

Искусство доказательства в математике

Доказательства играют центральную роль в высшей математике и теоретической информатике. Основная цель книги – помочь развить способности к математическому мышлению, в частности, способность читать и записывать доказательства.

Более 150 упражнений из формальной логики, теории множеств и теории чисел знакомят читателя с миром высшей математики через мастерство доказательства.

Третье издание бестселлера помогает перейти от механического решения задач к осмысленному доказательству теорем, обучаясь приемам, необходимым для чтения и написания доказательств.

- Тщательно подобранные примеры, демонстрирующие, как можно объединить несколько методов для построения комплексного доказательства
- Охватывает логику, теорию множеств, отношения и функции
- Идеально подходит для самостоятельного изучения курса математических доказательств или в качестве дополнительного чтения к курсу дискретной математики или математического анализа

Издание будет полезно всем, кто интересуется логикой и доказательствами: старшим школьникам, студентам, ИТ-специалистам, философам, лингвистам и др. Предполагается, что читатель не владеет знаниями, выходящими за рамки стандартного курса математики средней школы.

Интернет-магазин:
www.dmkpress.com

CAMBRIDGE
UNIVERSITY PRESS



Оптовая продажа:
КТК «Галактика»
e-mail: books@alians-kniga.ru

ISBN 978-5-97060-911-8
A standard linear barcode representing the ISBN number.
9 785970 609118 >

Искусство доказательства в математике

Дэниэл Веллеман



Искусство доказательства в математике



Дэниэл Веллеман

Искусство доказательства в математике

How to prove it

A Structured Approach

Third Edition

Daniel J. Velleman

*Department of Mathematics and Statistics
Amherst College*

*Department of Mathematics and Statistics
University of Vermont*



CAMBRIDGE
UNIVERSITY PRESS

Искусство доказательства в математике

Курс лекций с упражнениями

Дэниэл Веллеман



Москва, 2021

УДК 519.63

ББК 22.193

B27

Веллеман Д.

Б27 Искусство доказательства в математике / пер. с англ. В. С. Яценкова. – М.: ДМК Пресс, 2021. – 444 с.: ил.

ISBN 978-5-97060-911-8

Чего от вас ждут, когда просят что-то доказать? Что отличает правильное доказательство от неправильного? Эта книга поможет вам узнать ответы и разъяснит основные принципы, используемые при построении доказательств.

В отличие от школьного подхода к доказательствам как к пронумерованному списку утверждений и причин, в настоящем издании используется структурированный подход, характерный для программирования: математические доказательства также строятся путем объединения некоторых базовых структур. Выбор структуры определяется логической формой доказываемого утверждения, поэтому в начале книги рассматривается элементарная логика и читатель знакомится с различными формами математических выражений. Далее обсуждаются отношения, функции, математическая индукция и более сложные математические темы, в частности теория чисел. В конце разделов каждой главы представлен список упражнений, для части которых приводятся решения или подсказки.

Издание адресовано всем, кто интересуется логикой и доказательствами: математикам, специалистам по информатике, философам, лингвистам.

УДК 519.63

ББК 22.193

Copyright Original English language edition published by Cambridge University Press is part of the University of Cambridge. Russian language edition copyright © 2021 by DMK Press. All rights reserved.

Все права защищены. Любая часть этой книги не может быть воспроизведена в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения владельцев авторских прав.

ISBN 978-1-108-42418-9 (англ.)

ISBN 978-5-97060-911-8 (рус.)

© Daniel J. Velleman, 2020

© Оформление, издание, перевод,
ДМК Пресс, 2021

Содержание

От издательства.....	7
Предисловие к третьему изданию	8
Введение.....	11
Глава 1. Пропозициональная логика	17
1.1. Дедуктивное мышление и логические связки	17
1.2. Таблицы истинности.....	23
1.3. Переменные и множества	34
1.4. Операции над множествами.....	43
1.5. Условные и равнозначные связки.....	53
Упражнения.....	62
Глава 2. Кванторная логика.....	65
2.1. Кванторы.....	65
2.2. Эквивалентности, включающие кванторы	74
2.3. Другие операции с множествами.....	83
Глава 3. Доказательства	93
3.1. Стратегии доказательства	93
3.2. Доказательства, связанные с отрицаниями и условиями	104
3.3. Доказательства с использованием кванторов	116
3.4. Доказательства с использованием конъюнкций и равносильностей	133
3.5 Доказательство дизъюнкций	144
3.6. Доказательства существования и единственности	155
3.7. Более сложные примеры доказательств.....	164
Глава 4. Соответствия	174
4.1. Упорядоченные пары и декартовы произведения.....	174
4.2. Соответствия	182
4.3. Подробнее о соответствиях.....	190
4.4. Отношения порядка	199
4.5. Отношения эквивалентности	213
Глава 5. Функции.....	226
5.1. Определение функции.....	226
5.2. Однозначность и сюръективность	236
5.3. Инверсия функций	245

5.4. Замкнутые множества	254
5.5. Образы и прообразы: исследовательский проект	262
Глава 6. Математическая индукция	267
6.1. Доказательство путем математической индукции	267
6.2. Дополнительные примеры.....	274
6.3. Рекурсия	287
6.4. Сильная индукция	297
6.5. Вновь про замыкания	311
Глава 7. Теория чисел	317
7.1. Наибольшие общие делители	317
7.2. Простые множители	324
7.3. Модульная арифметика	333
7.4. Теорема Эйлера	341
7.5. Криптография с открытым ключом	349
Глава 8. Бесконечные множества.....	361
8.1. Равномощные множества	361
8.2. Счетные и несчетные множества	370
8.3. Теорема Кантора–Шредера–Бернштейна	377
Приложение. Решения некоторых упражнений	385
Дополнительные материалы	438
Краткое изложение методов доказательства	439
Предметный указатель.....	441

От издательства

Отзывы и пожелания

Мы всегда рады отзывам наших читателей. Расскажите нам, что вы думаете об этой книге – что понравилось или, может быть, не понравилось. Отзывы важны для нас, чтобы выпускать книги, которые будут для вас максимально полезны.

Вы можете написать отзыв на нашем сайте www.dmkpress.com, зайдя на страницу книги и оставив комментарий в разделе «Отзывы и рецензии». Также можно послать письмо главному редактору по адресу dmkpress@gmail.com; при этом укажите название книги в теме письма.

Если вы являетесь экспертом в какой-либо области и заинтересованы в написании новой книги, заполните форму на нашем сайте по адресу http://dmkpress.com/authors/publish_book/ или напишите в издательство по адресу dmkpress@gmail.com.

Список опечаток

Хотя мы приняли все возможные меры для того, чтобы обеспечить высокое качество наших текстов, ошибки все равно случаются. Если вы найдете ошибку в одной из наших книг, мы будем очень благодарны, если вы сообщите о ней главному редактору по адресу dmkpress@gmail.com. Сделав это, вы избавите других читателей от недопонимания и поможете нам улучшить последующие издания этой книги.

Нарушение авторских прав

Пиратство в интернете по-прежнему остается насущной проблемой. Издательства «ДМК Пресс» и Cambridge University Press очень серьезно относятся к вопросам защиты авторских прав и лицензирования. Если вы столкнетесь в интернете с незаконной публикацией какой-либо из наших книг, пожалуйста, пришлите нам ссылку на интернет-ресурс, чтобы мы могли применить санкции.

Ссылку на подозрительные материалы можно прислать по адресу электронной почты dmkpress@gmail.com.

Мы высоко ценим любую помощь по защите наших авторов, благодаря которой мы можем предоставлять вам качественные материалы.

Предисловие к третьему изданию

Читатели, изучающие математику и информатику, часто впадают в замешательство, когда их впервые просят серьезно потрудиться над математическими доказательствами, потому что они не знают «правил игры». Что от вас ждут, когда просят что-то доказать? Что отличает правильное доказательство от неправильного? Эта книга призвана помочь читателям узнать ответы на эти вопросы, разъясняя основные принципы, используемые при построении доказательств.

Многие читатели впервые знакомятся с математическими доказательствами на курсе геометрии в средней школе. К сожалению, школьников, изучающих геометрию, обычно учат думать о доказательстве как о пронумерованном списке утверждений и причин, а такое представление слишком ограниченно, чтобы быть полезным. Здесь есть поучительная параллель с информатикой. Ранние языки программирования поощряли аналогичный ограниченный взгляд на компьютерные программы в виде нумерованных списков инструкций. Теперь программисты-разработчики отошли от подобных языков и продвигают подход, называемый «структурным программированием». Обсуждение доказательств в этой книге основано на убеждении, что многие соображения, которые побудили программистов принять структурированный подход к программированию, применимы и к написанию доказательств. Можно сказать, что эта книга учит «структурированному доказательству».

В структурированном программировании компьютерная программа создается не путем перечисления инструкций друг за другом, а путем объединения определенных базовых структур, таких как конструкция `if-else` и цикл `do-while` языка программирования Java. Эти структуры объединяются не только путем перечисления по порядку, но и путем *вложения* друг в друга. Например, программа, созданная вложением конструкции `if-else` в цикл `do-while`, будет выглядеть так:

```
do
    if [условие]
        [Список операторов программы]
    else
        [Альтернативный список операторов программы]
    while [условие]
```

Отступы в такой программе не являются абсолютно необходимыми, но это удобный метод, часто используемый в информатике для отображения основной структуры программы.

Математические доказательства также строятся путем объединения некоторых базовых структур доказательства. Например, при доказательстве утверждения вида «если P , то Q » часто используется то, что можно было бы назвать структурой «предполагать, пока»: мы *предполагаем*, что P истинно, пока не сможем прийти к заключению, что Q истинно, в этот момент мы отказываемся от предположения и заключаем, что утверждение «если P , то Q » истинно. Другой пример – структура «доказательства для произвольного x »: чтобы доказать утверждение вида «для всех $x P(x)$ », мы *объявляем x как произвольный объект*, а затем *доказываем $P(x)$* . Как только мы приходим к выводу, что $P(x)$ истинно, мы отказываемся от объявления x как произвольного и заключаем, что утверждение «для всех $x P(x)$ » истинно. Более того, чтобы доказать более сложные утверждения, эти структуры часто объединяют, не только перечисляя одну за другой, но также вкладывая одну в другую. Например, чтобы доказать утверждение вида «для всех x если $P(x)$, то $Q(x)$ », мы, вероятно, вложим структуру «предполагать, пока» в структуру «доказательства для произвольного x », получив следующее доказательство:

Пусть x произвольно.

Предположим, что $P(x)$ истинно.

[Далее идет доказательство $Q(x)$.]

Таким образом, если $P(x)$, то $Q(x)$.

Таким образом, для всех x если $P(x)$, то $Q(x)$.

Как и раньше, мы использовали отступы, чтобы прояснить основную структуру доказательства.

Конечно, математики обычно не пишут свои доказательства в строгой форме с отступом. Наша цель в этой книге – научить читателей излагать доказательства обычным текстом, как это делают все математики. Тем не менее наш подход основан на убеждении, что если читатели хотят преуспеть в написании таких доказательств, они должны понимать основную структуру, которую имеют доказательства. Они должны усвоить, например, что выражения типа «Пусть x будет произвольным» и «Предположим, P » не являются изолированными шагами в доказательствах, а используются для введения структур доказательства «доказать для произвольного x » и «предполагать, пока». Начинающие математики нередко неправильно используют эти предложения в других целях. Такие ошибки аналогичны использованию в программе оператора `do` без парного оператора `while`.

Обратите внимание, что в наших примерах выбор структуры доказательства определяется логической формой доказываемого утверждения. По этой причине книга начинается с элементарной логики, чтобы познакомить читателей с различными формами математических выражений. В главе 1 обсуждаются логические связки, а в главе 2 представлены кванторы. В этих главах также представлены основы теории множеств, поскольку это важный предмет, который используется в остальной части книги (и во всей математике), а также потому, что он служит для иллюстрации многих логических выкладок, обсуждаемых в этих главах.

В главе 3 рассматриваются методы структурированного доказательства, упоминаются различные формы, которые могут принимать математиче-

ские утверждения, и обсуждаются структуры доказательства, подходящие для каждой формы. Примеры доказательств в этой главе по большей части выбраны не из-за их математического содержания, а из-за структур доказательства, которые они иллюстрируют. Это особенно верно в начале главы, когда мы только начинаем обсуждать некоторые методы, и в результате многие доказательства в этой части главы довольно тривиальны. По мере продвижения по главе доказательства становятся все более сложными и интересными с математической точки зрения.

Главы 4 и 5, посвященные отношениям и функциям, служат двум целям. Во-первых, они предоставляют материал, на котором читатели могут отрабатывать приемы доказательства из главы 3. И во-вторых, они знакомят читателей с некоторыми фундаментальными концепциями, используемыми во всех областях математики.

Глава 6 посвящена методу доказательства, который очень важен как в математике, так и в информатике: математической индукции. Изложение основано на методах из главы 3, которыми читатели должны были овладеть к этому моменту в книге.

После завершения главы 6 читатели должны быть готовы перейти к более существенным математическим темам. Две такие темы представлены в главах 7 и 8. Глава 7, новая в этом третьем издании, дает введение в теорию чисел, а в главе 8 мы обсуждаем бесконечные мощности. Эти главы развивают у читателей навык математических доказательств, а также дают представление о том, на что похожа более продвинутая математика.

Каждый раздел каждой главы заканчивается списком упражнений. Некоторые упражнения отмечены звездочкой; решения или подсказки для этих упражнений приведены в приложении. Упражнения, отмеченные символом P_D , можно выполнять с помощью программного обеспечения Proof Designer, которое бесплатно доступно в интернете.

Самыми большими изменениями в этом третьем издании являются добавление новой главы по теории чисел, а также более 150 дополнительных упражнений. Раздел о рефлексивных, симметричных и транзитивных замыканиях отношений был удален из главы 4 (хотя эти темы теперь включены в некоторые упражнения в разделе 4.4); он был заменен новым разделом в главе 5 о замыканиях множеств по функциям. По всему тексту также есть множество мелких изменений.

Я хотел бы поблагодарить всех, кто прислал мне комментарии к более ранним изданиям этой книги. В частности, Джон Коркоран и Раймонд Бут сделали несколько полезных предложений. Я также благодарен за советы Джонатану Сэнду и нескольким анонимным рецензентам.

Введение

Что такое математика? Математика в старших классах школы в основном занимается решением уравнений и вычислением ответов на числовые задачи. Математика в средних и высших учебных заведениях занимается более широким кругом вопросов, включая не только числа, но также множества, функции и другие математические объекты. Их объединяет использование *дедуктивного мышления* для поиска ответов на вопросы. Когда вы решаете уравнение относительно x , вы используете заданную в уравнении информацию, чтобы *вывести* (deduce) значение x . Точно так же, когда математики решают другие виды математических задач, они всегда обосновывают свои выводы дедуктивными рассуждениями.

Дедуктивные рассуждения в математике обычно представляют в виде *доказательства*. Одна из основных целей этой книги – помочь вам развить ваши способности к математическому мышлению в целом и, в частности, вашу способность читать и записывать доказательства. В следующих главах мы подробно изучим, как строятся доказательства, но сначала давайте рассмотрим несколько примеров.

Не волнуйтесь, если у вас возникнут проблемы с пониманием этих доказательств. Они просто предназначены для того, чтобы дать вам почувствовать, на что похожи математические доказательства. В некоторых случаях вы можете выполнить многие шаги доказательства, но будете озадачены тем, почему эти шаги объединены именно таким образом, или как кто-то смог прийти к такому доказательству. Если это так, мы просим вас проявить терпение. Ответы на многие из этих вопросов будут даны позже в этой книге, особенно в главе 3.

Все наши примеры доказательств во введении будут включать простые числа. Напомним, что целое число больше 1 называется *простым*, если оно не может быть записано как произведение двух меньших положительных целых чисел. Если его можно записать как произведение двух меньших положительных целых чисел, то оно *составное*. Например, 6 – составное число, поскольку $6 = 2 \cdot 3$, а 7 – простое число.

Прежде чем мы сможем привести пример доказательства с участием простых чисел, нам нужно найти объект доказательства – некоторый факт о простых числах, правильность которого можно проверить с помощью доказательства. Иногда можно найти интересные закономерности в математике, просто попробовав вычислить несколько чисел. Например, рассмотрим табл. В.1. Для каждого целого числа n от 2 до 10 таблица показывает, являются ли n и $2^n - 1$ простыми или нет, и возникает удивительная закономерность. Оказывается, $2^n - 1$ – простое число как раз в тех случаях, когда n простое!

Таблица В.1. Закономерность вычисления простых чисел

<i>n</i>	<i>n</i> четное?	$2^n - 1$	$2^n - 1$ четное?
2	Да	3	Да
3	Да	7	Да
4	Нет: $4 = 2 \cdot 2$	15	Нет: $15 = 3 \cdot 5$
5	Да	31	Да
6	Нет: $6 = 2 \cdot 3$	63	Нет: $63 = 7 \cdot 9$
7	Да	127	Да
8	Да: $8 = 2 \cdot 4$	255	Нет: $255 = 15 \cdot 17$
9	Нет: $9 = 3 \cdot 3$	511	Нет: $511 = 7 \cdot 73$
10	Нет: $10 = 2 \cdot 5$	1023	Нет: $1023 = 31 \cdot 33$

Будет ли эта закономерность продолжаться? Заманчиво предположить, что так и есть, но это лишь догадка. Математики называют такие догадки *гипотезами*. Таким образом, мы имеем следующие две гипотезы:

Гипотеза 1. Предположим, что n – целое число больше 1 и n простое. Тогда $2^n - 1$ – простое число.

Гипотеза 2. Предположим, что n – целое число больше 1 и n не является простым. Тогда $2^n - 1$ не является простым.

К сожалению, если мы продолжим табл. В.1, то сразу обнаружим, что гипотеза 1 неверна. Легко проверить, что число 11 простое, но $2^{11} - 1 = 2047 = 23 \cdot 89$, поэтому $2^{11} - 1$ составное. Таким образом, 11 является *контрпримером* к гипотезе 1. Существование хотя бы одного контрпримера доказывает, что гипотеза неверна, но интересно отметить, что в этом случае существует много контрпримеров. Если мы продолжим проверять числа до 30, то найдем еще два контрпримера к гипотезе 1: 23 и 29 – простые числа, но $2^{23} - 1 = 8\,388\,607 = 47 \cdot 178\,481$ и $2^{29} - 1 = 536\,870\,911 = 2089 \cdot 256\,999$. Однако никакое число до 30 не является контрпримером к гипотезе 2.

Считаете ли вы, что гипотеза 2 верна? Найдя контрпримеры к гипотезе 1, мы делаем вывод, что эта гипотеза неверна, но наша неспособность найти контрпример к гипотезе 2 еще не доказывает, что она верна. Возможно, для нее тоже есть контрпримеры, но самый маленький из них больше 30. Продолжение проверки примеров может выявить контрпример, а если его нет, то это может повысить нашу уверенность в гипотезе. Но мы никогда не можем быть уверены в правильности гипотезы, если только проверяем примеры. Сколько бы примеров мы ни проверили, всегда есть вероятность, что следующий окажется первым контрпримером. Единственный способ убедиться в правильности гипотезы 2 – это доказать ее.

На самом деле гипотеза 2 верна. Вот доказательство гипотезы:

Доказательство гипотезы 2. Поскольку n не простое число, существуют натуральные числа a и b такие, что $a < n$, $b < n$ и $n = ab$. Пусть $x = 2^b - 1$ и $y = 1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}$. Далее

$$\begin{aligned}
 xy &= (2^b - 1) \cdot (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) \\
 &= 2^b \cdot (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) - (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) \\
 &= (2^b + 2^{2b} + 2^{3b} + \dots + 2^{ab}) - (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) \\
 &= 2^{ab} - 1 \\
 &= 2^n - 1.
 \end{aligned}$$

Поскольку $b < n$, мы можем заключить, что $x = 2^b - 1 < 2^n - 1$. Кроме того, поскольку $ab = n > a$, отсюда следует, что $b > 1$. Следовательно, $x = 2^b - 1 > 2^1 - 1 = 1$, поэтому $y < xy = 2^n - 1$. Таким образом, мы показали, что $2^n - 1$ можно записать как произведение двух натуральных чисел x и y , оба из которых меньше $2^n - 1$, поэтому $2^n - 1$ не является простым.

Теперь, когда гипотеза доказана, мы можем назвать ее *теоремой*. Не вол-нуйтесь, если доказательство показалось вам непонятным. Мы вернемся к нему снова в конце главы 3, чтобы проанализировать, как оно было по-строено. На данный момент наиболее важно понять, что если n – любое целое число больше 1, которое может быть записано как произведение двух мень-ших положительных целых чисел a и b , то доказательство дает нам способ (по общему признанию, несколько загадочный) записать $2^n - 1$ как произведение двух меньших натуральных чисел x и y . Таким образом, если n не является простым, то $2^n - 1$ также не должно быть простым. Например, предположим, что $n = 12$, тогда $2^n - 1 = 4095$. Поскольку $12 = 3 \cdot 4$, мы можем подставить $a = 3$ и $b = 4$ в доказательство. Тогда согласно формулам для x и y , приведен-ным в доказательстве, мы будем иметь $x = 2^b - 1 = 2^4 - 1 = 15$ и $y = 1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b} = 1 + 2^4 + 2^8 = 273$. И как и предсказывают формулы в доказа-тельстве, мы имеем $xy = 15 \cdot 273 = 4095 = 2^n - 1$. Конечно, есть другие способы разложить 12 на произведение двух меньших целых чисел, и это может при-вести к другим способам факторизации 4095. Например, поскольку $12 = 2 \cdot 6$, мы могли бы использовать значения $a = 2$ и $b = 6$. Попробуйте вычислить со-ответствующие значения x и y и убедитесь, что их произведение равно 4095.

Хотя мы уже знаем, что гипотеза 1 неверна, мы все же можем задать ей интересные вопросы. Если мы продолжим проверять простые числа n , чтобы убедиться, что $2^n - 1$ простое, продолжим ли мы находить контрпримеры к гипотезе – примеры, для которых $2^n - 1$ не является простым? Будем ли мы продолжать находить примеры, для которых $2^n - 1$ простое? Если бы сущес-твовал только конечный набор простых чисел, мы могли бы исследовать эти вопросы, просто проверив $2^n - 1$ для каждого простого числа n . Но на самом деле простых чисел бесконечно много. Евклид (около 300 г. до н. э.) привел доказательство этого факта в книге IX своих «Элементов». Его доказатель-ство – одно из самых известных во всей математике¹:

Теорема 3. Простых чисел бесконечно много.

Доказательство. Предположим, что существует только конечное количество простых чисел. Пусть p_1, p_2, \dots, p_n – список всех простых чисел. Пусть $m = p_1 p_2 \cdots p_n + 1$. Заметим, что m не делится на p_1 , поскольку деление m на p_1 дает

¹ Евклид сформулировал теорему и доказательство несколько иначе. Для этой книги мы выбрали более современный подход.

частное $p_2 p_3 \cdots p_n$ и остаток 1. Аналогично, m не делится на любое число из списка p_2, p_3, \dots, p_n .

Теперь мы воспользуемся тем фактом, что каждое целое число больше 1 – либо простое, либо может быть записано как произведение двух или более простых чисел. (Мы увидим доказательство этого факта в главе 6 – см. теорему 6.4.2.) Ясно, что m больше 1, поэтому m либо простое, либо является произведением простых чисел. Предположим сначала, что m простое. Обратите внимание, что m больше, чем все числа в списке p_1, p_2, \dots, p_n , значит, мы обнаружили простое число, которого нет в этом списке. Но это противоречит нашему предположению, что это был список всех простых чисел.

Теперь предположим, что m – произведение простых чисел. Пусть q будет одним из простых чисел в этом произведении. Тогда m делится на q . Но мы уже видели, что m не делится ни на одно из чисел в списке p_1, p_2, \dots, p_n , поэтому мы снова приходим к противоречию с предположением, что в этот список включены все простые числа.

Поскольку предположение, что существует конечное число простых чисел, привело к противоречию, должно существовать бесконечно много простых чисел.

Напомним, что вы не должны беспокоиться, если некоторые аспекты этого доказательства кажутся загадочными. Прочитав главу 3, вы лучше подготовитесь к детальному пониманию доказательства. Затем мы вернемся к этому доказательству и проанализируем его структуру.

Мы видели, что если n не является простым, то $2^n - 1$ не может быть простым, но если n простое, то $2^n - 1$ может быть простым или составным. Поскольку простых чисел бесконечно много, существует бесконечно много чисел вида $2^n - 1$, которые, исходя из того, что мы знаем сейчас, могут быть простыми. Но сколько из них являются простыми?

Простые числа вида $2^n - 1$ называются *простыми числами Мерсенна* в честь отца Марёна Мерсённа (1588–1648), французского монаха и ученого, изучавшего эти числа. Хотя было найдено много простых чисел Мерсенна, до сих пор неизвестно, бесконечно ли их много. Многие из самых больших известных простых чисел – простые числа Мерсенна. На момент написания этой книги (февраль 2019 г.) наибольшее известное простое число – это простое число Мерсенна $2^{82\,589\,933} - 1$, состоящее из 24 862 048 цифр.

Простые числа Мерсенна связаны с совершенными числами, что является предметом другой известной нерешенной проблемы математики. Положительное целое число n называется *совершенным*, если n равно сумме всех положительных целых чисел, меньших n , которые делят n . (Для любых двух целых чисел m и n мы говорим, что m делит n , если n делится на m ; другими словами, если существует целое число q такое, что $n = qm$.) Например, существуют положительные целые числа меньше 6, которые делят 6. Это числа 1, 2 и 3, и при этом $1 + 2 + 3 = 6$. Следовательно, 6 – совершенное число. Следующее наименьшее совершенное число – 28. (Вы должны сами убедиться, что 28 совершенно, найдя все положительные целые числа меньше 28, которые делят 28, и сложив их.)

Евклид доказал, что если $2^n - 1$ – простое число, то $2^{n-1}(2^n - 1)$ совершенно. Таким образом, каждое простое число Мерсенна представляет собой совер-

шенное число. Более того, примерно через 2000 лет после доказательства Евклида швейцарский математик Леонард Эйлер (1707–1783), самый плодотворный математик в истории, доказал, что таким способом можно получить каждое четное совершенное число. Например, обратите внимание, что $6 = 2^1(2^2 - 1)$ и $28 = 2^2(2^3 - 1)$. Поскольку неизвестно, существует ли бесконечно много простых чисел Мерсенна, также неизвестно, существует ли бесконечно много четных совершенных чисел. Также неизвестно, существуют ли совершенные нечетные числа. Доказательства теорем Евклида и Эйлера см. в упражнениях 18 и 19 в разделе 7.4.

Хотя простых чисел бесконечно много, они встречаются тем реже, чем больше числа, которые мы рассматриваем. Например, существует 25 простых чисел от 1 до 100, 16 простых чисел от 1001 до 1100 и только шесть простых чисел от 1 000 001 до 1 000 100. В качестве нашего последнего вводного примера математического доказательства мы покажем, что существуют длинные отрезки последовательных положительных целых чисел, вообще не содержащие простых чисел. В этом доказательстве мы будем использовать следующую терминологию: для любого натурального числа n произведение всех целых чисел от 1 до n называется *факториалом n* и обозначается $n!$. Таким образом, $n! = 1 \cdot 2 \cdot 3 \cdots n$. Как и в случае с двумя предыдущими доказательствами, мы вернемся к этому доказательству в конце главы 3, чтобы проанализировать его структуру.

Теорема 4. Для каждого натурального числа n существует последовательность из n последовательных натуральных чисел, не содержащая простых чисел.

Доказательство. Предположим, что n – натуральное число. Пусть $x = (n + 1)! + 2$. Мы покажем, что ни одно из чисел $x, x + 1, x + 2, \dots, x + (n - 1)$ не является простым числом. Поскольку это последовательность из n последовательных натуральных чисел, это доказывает теорему.

Чтобы убедиться, что x не является простым, обратите внимание, что

$$x = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1) + 2 = 2 \cdot (1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1) + 1).$$

Таким образом, x можно записать как произведение двух меньших положительных целых чисел, поэтому x не является простым.

Аналогично имеем

$$x + 1 = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n + 1) + 3 = 3 \cdot (1 \cdot 2 \cdot 4 \cdots (n + 1) + 1),$$

поэтому $x + 1$ также не является простым. В общем, рассмотрим любое число $x + i$, где $0 < i < n - 1$. Отсюда имеем

$$x + 1 = \dots,$$

поэтому $x + i$ не является простым.

Теорема 4 показывает, что иногда между одним и другим простыми числами есть длинные отрезки. Но простые числа также иногда встречаются близко друг к другу. Поскольку 2 – единственное четное простое число, единственная пара последовательных целых чисел, которые являются простыми, – это

2 и 3. Но есть много пар простых чисел, которые отличаются только на два, например 5 и 7, 29 и 31, 7949 и 7951. Такие пары простых чисел называются *простыми числами-близнецами*. Неизвестно, есть ли бесконечно много простых чисел-близнецов.

Недавно был достигнут значительный прогресс в вопросе о простых числах-близнецах. В 2013 году Итан Чжан (род. 1955) доказал, что существует натуральное число $d < 70\,000\,000$ такое, что существует бесконечно много пар простых чисел, различающихся на d . Усилиями многих других математиков в 2013–2014 гг. удалось снизить диапазон возможных значений d до $d \leq 246$. Конечно, если утверждение верно при $d = 2$, то существует бесконечно много простых чисел-близнецов.

Упражнения

Примечание. Решения или подсказки для упражнений, отмеченных звездочкой (*), приведены в приложении.

- *1. (a) Разложите $2^{15} - 1 = 32\,767$ на произведение двух меньших натуральных чисел.
(b) Найдите целое число x такое, что $1 < x < 232\,767 - 1$ и $232\,767 - 1$ делится на x .
2. Сделайте несколько предположений о значениях n , для которых $3^n - 1$ – простое число, или о значениях n , для которых $3^n - 2^n$ – простое число. (Вы можете начать с создания таблицы, подобной В.1.)
- *3. Доказательство теоремы 3 дает метод нахождения простого числа, отличного от любого в данном списке простых чисел.
 - (a) Используйте этот метод, чтобы найти простое число, отличное от 2, 3, 5 и 7.
 - (b) Используйте этот метод, чтобы найти простое число, отличное от 2, 5 и 11.
4. Найдите пять последовательных целых чисел, которые не являются простыми.
5. Используйте табл. В.1 и последующее обсуждение, чтобы найти еще два совершенных числа.
6. Последовательность 3, 5, 7 – это список из трех простых чисел, где каждая пара соседних чисел в списке отличается на два. Есть ли еще такие «тройные простые числа»?
7. Два различных натуральных числа (m, n) называются *дружественными*, если сумма всех натуральных чисел меньше n , делящих n , равна m , а сумма всех положительных целых чисел меньше m , которые делят m , равна n . Покажите, что пара (220, 284) дружественная.

Глава 1

Пропозициональная логика

1.1. Дедуктивное мышление и логические связи

Как мы показали во введении, доказательства играют центральную роль в математике, а дедуктивные выкладки являются основой, на которую опираются доказательства. Поэтому мы начинаем изучение математических выводов и доказательств с изучения того, как работает дедуктивное мышление.

Пример 1.1.1. Вот три примера дедуктивного мышления:

1. Завтра будет дождь или снег.
Слишком тепло для снега.
Значит, пойдет дождь.
2. Если сегодня воскресенье, то сегодня мне не нужно идти на работу.
Сегодня воскресенье.
Поэтому сегодня мне не нужно идти на работу.
3. Я пойду на работу завтра или сегодня.
Я сегодня останусь дома.
Поэтому пойду на работу завтра.

В каждом случае мы пришли к *заключению* из предположения, что некоторые другие утверждения, называемые *допущениями* или *посылками*, верны. Например, посылки в рассуждении 3 – это утверждения «Я пойду на работу завтра или сегодня» и «Я сегодня останусь дома». Вывод такой: «Я пойду на работу завтра», и он вроде бы следует из посылок.

Но действительно ли этот вывод сделан верно? В конце концов, разве не может случиться так, что я останусь сегодня дома, а завтра проснусь больным и снова останусь дома? Если это произойдет, вывод окажется ложным. Но заметьте, что в этом случае первая посылка, которая гласила, что я пойду на работу завтра или сегодня, также будет ложной! Хотя у нас нет гарантии, что вывод истинный, он может быть ложным только в том случае, если хотя

бы одна из посылок также ложная. Если обе посылки истинны, мы можем быть уверены в истинности вывода. В этом смысле заключение навязано нам посылками, и это критерий, который мы будем использовать для оценки правильности дедуктивного рассуждения. Мы говорим, что рассуждение *действительно*, если все посылки не могут быть истинными без истинного заключения. Все три рассуждения в нашем примере – действительные.

Вот пример недействительного дедуктивного рассуждения:

Виноват или дворецкий, или горничная.

Или виновата горничная, или виноват повар.

Следовательно, виноват или дворецкий, или повар.

Рассуждение недействительно, потому что вывод может быть ложным, даже если истинны обе посылки. Например, если горничная виновна, а дворецкий и повар невиновны, то обе посылки будут истинными, но вывод будет ложным.

Мы можем узнать больше о том, что делает рассуждение действительным, сравнивая три рассуждения в примере 1.1.1. На первый взгляд может показаться, что рассуждения 2 и 3 имеют много общего, потому что оба они касаются одного и того же предмета: посещения работы. Но с точки зрения используемых рассуждений наиболее похожи рассуждения 1 и 3. Оба они вводят две *возможности* в первой посылке, исключают вторую возможность с помощью второй посылки и затем делают вывод, что первая возможность должна иметь место. Другими словами, оба рассуждения имеют вид:

P или Q .

Не Q .

Следовательно, P .

Именно эта *форма*, а не предмет обсуждения делает рассуждения действительными. Вы можете увидеть, что рассуждение 1 имеет такую форму, если принять, что буква P обозначает утверждение «Завтра будет дождь», а Q – «Завтра будет снег». Для рассуждения 3 P будет означать «Я пойду на работу завтра», а Q – «Я пойду на работу сегодня».

Замена определенных утверждений в каждом рассуждении буквами, как мы это сделали для рассуждений 1 и 3, дает два преимущества. Во-первых, это не позволяет нам отвлекаться на аспекты рассуждений, не влияющие на их обоснованность. Вам не нужно ничего знать о прогнозировании погоды или привычке ходить на работу, чтобы признать, что рассуждения 1 и 3 верны. Это потому, что оба рассуждения имеют форму, показанную ранее, и вы можете сказать, что эта форма рассуждения верна, даже не зная, что означают P и Q . Если вы не согласны с этим, рассмотрите следующее рассуждение:

Либо стробонатор пропускает зажигание, либо механизм друмпеля не отрегулирован.

Я проверил регулировку механизма друмпеля, и с ним все в порядке.

Следовательно, стробонатор неисправен.

Если механик даст такое объяснение после осмотра вашей машины, вы все равно не поймете, почему машина не заводится, но у вас не будет претензий к его логике!

Возможно, более важно то, что из анализа формы рассуждений 1 и 3 становится ясно, что влияет на их обоснованность: это слова *или* (*or*) и *не* (*not*). В большинстве дедуктивных рассуждений и, в частности, в математических рассуждениях значения всего нескольких слов дают нам ключ к пониманию того, что делает часть рассуждения правильной или ошибочной. (Какие слова являются важными в рассуждении 2 в примере 1.1.1?) Первые несколько глав этой книги посвящены изучению этих слов и того, как они используются в математических записях и рассуждениях.

В этой главе мы сконцентрируемся на словах, используемых для объединения простых утверждений в более сложные. Мы продолжим использовать буквы для обозначения утверждений, но только для однозначных утверждений, которые являются истинными или ложными. Вопросы, восклицания и расплывчатые заявления не допускаются. Также будет полезно использовать символы, иногда называемые *соединительными символами* или *связками* (*connective symbols*), для обозначения некоторых слов, применяемых для объединения утверждений. Вот наши первые три соединительных символа и слова, которые они обозначают:

Символ	Значение
\vee	или (<i>or</i>)
\wedge	и (<i>and</i>)
\neg	не (<i>not</i>)

Таким образом, если P и Q обозначают два утверждения, тогда мы будем писать $P \vee Q$ для обозначения утверждения « P или Q », $P \wedge Q$ для « P и Q » и $\neg P$ для «не P » или « P является ложным». Утверждение $P \vee Q$ иногда называют *дизъюнцией* P и Q , $P \wedge Q$ называют *конъюнцией* P и Q , а $\neg P$ называют *отрицанием* P .

Пример 1.1.2. Запишите логические формы следующих утверждений:

1. Или Джон пошел в магазин, или у нас закончились яйца.
2. Джо собирается уйти из дома и больше не вернется.
3. Или Билл на работе, а Джейн нет, или Джейн на работе, а Билл нет.

Решения

1. Если мы назначим P обозначать утверждение «Джон пошел в магазин», а Q – «у нас закончились яйца», то общее утверждение можно было бы символически представить как $P \vee Q$.
2. Если мы назначим P обозначать утверждение «Джо собирается уйти из дома», а Q – «Джо не вернется», то мы могли бы символически представить это утверждение как $P \wedge Q$. Но эта запись упускает важную особенность утверждения, потому что она не означает, что Q – отрицательное утверждение. Мы могли бы улучшить запись, обозначив как R утверждение «Джо собирается вернуться», а затем записав утверждение Q как $\neg R$.

как $\neg R$. Подставив это в нашу первую запись посылки, мы получаем улучшенную запись $P \wedge \neg R$.

3. Пусть B означает утверждение «Билл на работе», а J – утверждение «Джейн на работе». Тогда первая половина утверждения «Билл на работе, а Джейн нет» может быть представлена как $B \wedge \neg J$. Аналогично, вторая половина – это $J \wedge \neg B$. Чтобы записать все утверждение, мы должны использовать связку «или», образуя дизъюнкцию, так что полная запись будет иметь следующий вид: $(B \wedge \neg J) \vee (J \wedge \neg B)$.

Обратите внимание, что при анализе третьего утверждения в предыдущем примере мы добавили круглые скобки при формировании дизъюнкции $B \wedge \neg J$ и $J \wedge \neg B$, чтобы однозначно указать, какие утверждения были объединены. Это похоже на использование круглых скобок в алгебре, в которых, например, произведение $a + b$ и $a - b$ будет записано как $(a + b) \cdot (a - b)$, причем скобки служат для однозначного указания того, какие величины должны быть перемножены. Как и в алгебре, в логике принято опускать некоторые скобки, чтобы наши выражения были короче и удобнее для чтения. Однако мы должны договориться о некоторых соглашениях о том, как читать такие выражения, чтобы они оставались однозначными. Согласно одному соглашению, символ \neg всегда применяется только к утверждению, которое следует сразу после него. Например, $\neg P \wedge Q$ означает $(\neg P) \wedge Q$, а не $\neg(P \wedge Q)$. Позже мы увидим другие соглашения о скобках.

Пример 1.1.3. Какие английские предложения представлены следующими выражениями?

1. $(\neg S \wedge L) \vee S$, где S означает «Джон умен», а L означает «Джону повезло».
2. $\neg S \wedge (L \vee S)$, где S и L имеют те же значения, что и раньше.
3. $\neg(S \wedge L) \vee S$, причем S и L остаются прежними.

Решения

1. Джон не умен и ему повезло, или он умен.
2. Джон не умен, и ему повезло, или он умен. Обратите внимание, как расположение слова *или* в разговорном языке меняется в зависимости от того, где находятся круглые скобки.
3. Джон не умен и не удачлив, или Джон умен. Слово-союз *и* также зависит от различного возможного положения скобок.

Важно помнить, что символы \wedge , \vee и \neg на самом деле не соответствуют всем вариантам использования слов *и*, *или*, *не* в разговорном языке. Например, символ \wedge нельзя использовать для обозначения слова *и* в предложении «Джон и Билл – друзья», потому что в этом предложении слово *и* не используется для объединения двух утверждений. Символы \wedge и \vee могут использоваться только между двумя утверждениями, чтобы образовать их конъюнкцию или дизъюнкцию, а символ \neg может использоваться только перед утверждением, чтобы отрицать его. Это означает, что определенные строки букв и символов просто бессмысленны. Например, $P \neg \wedge Q$, $P \wedge \vee Q$ и $P \neg \neg Q$ – все это «неграмматические» выражения на языке логики. «Грамматические» выражения, подобные приведенным в примерах 1.1.2 и 1.1.3, иногда называют *правильно*

построенными формулами или просто *формулами*. И снова, здесь полезно подумать об аналогии с алгеброй, в которой символы $+$, $-$, \cdot и \div могут стоять между двумя числами в качестве операторов, а символ $-$ (минус) также может стоять перед числом, чтобы показать его отрицательность. Это единственный способ использования данных символов в алгебре, поэтому такие выражения, как $x - \div y$, не имеют смысла.

Иногда для записи выражений, представленных символами \wedge , \vee и \neg , используются слова, отличные от *и*, *или*, *не*. Например, рассмотрим первое утверждение в примере 1.1.3. Хотя мы использовали выражение «Джон не умен и ему повезло, или он умен», альтернативным способом передачи той же информации было бы выражение: «Либо Джон не умен, но ему повезло, либо он умен». Часто слово *но* используется в разговорном языке для обозначения связки *и*, особенно когда есть некоторый контраст или конфликт между объединяемыми утверждениями. В качестве более яркого примера представьте, что синоптик заканчивает свой прогноз заявлением «Дождь и снег – только эти варианты можно ждать от завтрашней погоды». Это просто окольный способ сказать, что завтра будет дождь *или* снег. Таким образом, даже несмотря на то, что синоптик использовал слово *и*, значение, выраженное в его утверждении, является дизъюнкцией. Урок из этих примеров состоит в том, что для определения логической формы утверждения вы должны думать о смысле утверждения, а не просто переводить слово за словом в символы.

Иногда логические слова скрыты в математических обозначениях. Например, рассмотрим утверждение $3 \leq \pi$. Хотя с виду оно кажется простым утверждением, не содержащим логических связок, если вы прочитаете его вслух, то услышите слово *или*. Если мы назначим P обозначать утверждение $3 < \pi$ и Q для утверждения $3 = \pi$, тогда утверждение $3 \leq \pi$ будет записано как $P \vee Q$. В этом примере утверждения, представленные буквами P и Q , настолько короткие, что вряд ли имеет смысл сокращать их до отдельных букв. В таких случаях мы иногда не будем беспокоиться о замене утверждений буквами, поэтому мы также можем записать это утверждение как $(3 < \pi) \vee (3 = \pi)$.

В качестве немного более сложного примера рассмотрим утверждение $3 < \pi < 4$. Это утверждение означает $3 < \pi$ и $\pi < 4$, так что снова логическая связка была скрыта в математической нотации. Дополняя запись, которую мы только что разработали для $3 \leq \pi$, мы можем записать выражение как $[(3 < \pi) \vee (3 = \pi)] \wedge (\pi < 4)$. Знание логической формы утверждения может быть важно для понимания части математических рассуждений, связанных с этим утверждением.

Упражнения

*1. Запишите логические формы следующих утверждений:

- У нас будут либо задания для самостоятельного чтения, либо домашняя работа, но у нас не будет одновременно домашней работы и теста.
- Вы не пойдете кататься на лыжах или пойдете, но снега не будет.
- $\sqrt{7} \leq 2$.

2. Запишите логические формы следующих утверждений:
- Либо Джон и Билл оба говорят правду, либо ни один из них не говорит правду.
 - Я буду есть либо рыбу, либо курицу, но не буду есть рыбу и картофельное пюре одновременно.
 - Число 3 является общим делителем чисел 6, 9 и 15.
3. Запишите логические формы следующих утверждений:
- Алиса и Боб не находятся в комнате одновременно.
 - Алисы и Боба одновременно нет в комнате.
 - Алисы или Боба нет в комнате.
 - Ни Алисы, ни Боба нет в комнате.
4. Запишите логические формы следующих утверждений:
- Либо Ральф и Эд оба высокие, либо оба красивые.
 - И Ральф, и Эд либо высокие, либо красивые.
 - И Ральф, и Эд оба невысокие и некрасивые.
 - Ни Ральф, ни Эд не являются одновременно высокими и красивыми.
5. Какие из следующих выражений являются правильными формулировками?
- $\neg(\neg P \vee \neg\neg R)$.
 - $\neg(P, Q, \wedge R)$.
 - $P \wedge \neg P$.
 - $(P \wedge Q) (P \vee R)$.
- *6. Пусть P означает утверждение «Я куплю брюки», а S – утверждение «Я куплю рубашку». Какие разговорные предложения представлены следующими формулами?
- $\neg(P \wedge \neg S)$.
 - $\neg P \wedge \neg S$.
 - $\neg P \vee \neg S$.
7. Пусть S означает утверждение «Стив счастлив», а G – «Джордж счастлив». Какие английские предложения представлены следующими формулами?
- $(S \vee G) \wedge (\neg S \vee \neg G)$.
 - $[S \vee (G \wedge \neg S)] \vee \neg G$.
 - $S \vee [G \wedge (\neg S \vee \neg G)]$.
8. Пусть T означает «Налоги вырастут», а D – «Дефицит вырастет». Какие английские предложения представлены следующими формулами?
- $T \vee D$.
 - $\neg(T \wedge D) \wedge \neg(\neg T \wedge \neg D)$.
 - $(T \wedge \neg D) \vee (D \wedge \neg T)$.
9. Определите посылки и выводы следующих дедуктивных рассуждений и запишите их логические формы. Как вы думаете, рассуждения верны? (Хотя при ответе на последний вопрос у вас будет только интуиция, в следующем разделе мы разработаем некоторые методы определения обоснованности рассуждений.)

- (а) Джейн и Пит оба не выиграют приз по математике. Пит выиграет либо приз по математике, либо по химии. Джейн получит приз по математике. Следовательно, Пит получит приз по химии.
- (б) Основное блюдо будет из говядины или рыбы. Гарниром будет либо горох, либо кукуруза. У нас не будет одновременно рыбы в качестве основного блюда и кукурузы в качестве гарнира. Поэтому у нас не будет одновременно говядины как основного блюда и гороха как гарнира.
- (с) Либо Джон, либо Билл говорят правду. Либо Сэм, либо Билл лгут. Следовательно, либо Джон говорит правду, либо Сэм лжет.
- (г) Либо продажи вырастут, и начальник будет доволен, либо расходы увеличатся, и начальник будет недоволен. Таким образом, продажи и расходы не могут увеличиться одновременно.

1.2. ТАБЛИЦЫ ИСТИННОСТИ

В разделе 1.1 мы показали, что рассуждение действительно, если все посылки не могут быть истинными без наличия истинного заключения. Поэтому, чтобы понять, как слова *и*, *или* и *не* влияют на обоснованность рассуждений, мы должны понять, как они способствуют истинности или ложности содержащих их утверждений.

Когда мы оцениваем истинность или ложность утверждения, мы присваиваем ему один из ярлыков – *истина* или *ложь*, – и этот ярлык называется его значением истинности. Вполне очевидно, как слово *и* способствует значению истинности содержащегося в нем утверждения. Утверждение в форме $P \wedge Q$ может быть истинным, только если одновременно истинны и P , и Q ; если либо P , либо Q является ложным, то $P \wedge Q$ также будет ложным. Поскольку мы предположили, что P и Q обозначают утверждения, которые либо истинны, либо ложны, мы можем свести все варианты возможных значений в табл. 1.1, называемую *таблицей истинности* для формулы $P \wedge Q$. Каждая строка в таблице истинности представляет одну из четырех возможных комбинаций значений истинности для утверждений P и Q . Хотя эти четыре возможности могут располагаться в таблице в любом порядке, лучше всего перечислять их систематически, чтобы мы могли быть уверены, что ни одна из возможностей не была упущена. Таблицу истинности для $\neg P$ также довольно легко построить, потому что для того, чтобы $\neg P$ было истинным, P должно быть ложным (табл. 1.2).

Таблица 1.1. Таблица истинности формулы $P \wedge Q$

P	Q	$P \wedge Q$
F	F	F
F	T	F
T	F	F
T	T	T

Таблица 1.2. Таблица истинности формулы $\neg P$

P	$\neg P$
F	T
T	F

Таблица истинности для $P \vee Q$ немного сложнее. Первые три строки, безусловно, должны быть заполнены, как показано в табл. 1.3, но могут возникнуть некоторые вопросы по поводу последней строки. Каким должно быть значение $P \vee Q$ – истинным или ложным в случае, когда P и Q оба истинны? Другими словами, какому из утверждений соответствует запись $P \vee Q$ – « P или Q , или оба» или же « P или Q , но не оба»? Первый способ интерпретации слова *или* называется *включающим или* (потому что он включает возможность того, что оба утверждения являются истинными), а второй – *исключающим или*. В математике *или* всегда включающее, если не указано иное, поэтому мы будем интерпретировать символ \vee как включающее или (табл. 1.4). См. упражнение 3, чтобы узнать больше об исключающем или.

Таблица 1.3. Таблица истинности формулы $P \vee Q$ с неоднозначностью

P	Q	$P \vee Q$
F	F	F
F	T	T
T	F	T
T	T	?

Таблица 1.4. Таблица истинности исключающего или

P	Q	$P \vee Q$
F	F	F
F	T	T
T	F	T
T	T	T

Используя правила, изложенные в этих таблицах истинности, теперь мы можем разработать таблицы истинности для более сложных формул. Все, что нам нужно сделать, – это определить значения истинности составных частей формулы, начиная с отдельных букв и постепенно переходя к более сложным формулам.

Пример 1.2.1. Составьте таблицу истинности для формулы $\neg(P \vee \neg Q)$.

Решение

P	Q	$\neg Q$	$P \vee \neg Q$	$\neg(P \vee \neg Q)$
F	F	T	T	F
F	T	F	F	T
T	F	T	T	F
T	T	F	T	F

В первых двух столбцах этой таблицы перечислены четыре возможные комбинации значений истинности P и Q . Третий столбец, в котором перечислены значения истинности для формулы $\neg Q$, находится путем простого отрицания значений истинности для Q во втором столбце. Четвертый столбец для формулы $P \vee \neg Q$ находится путем объединения значений истинности для P и $\neg Q$, перечисленных в первом и третьем столбцах, в соответствии с правилом значения истинности для \vee , приведенным в табл. 1.4. Согласно этому правилу, $P \vee \neg Q$ будет ложным, только если и P , и $\neg Q$ ложны. Глядя на первый и третий столбцы, мы видим, что это происходит только во второй строке таблицы, поэтому четвертый столбец содержит букву F во второй строке и букву T во всех остальных строках. Наконец, значения истинности для формулы $\neg(P \vee \neg Q)$ перечислены в пятом столбце, который находится путем отрицания значений истинности в четвертом столбце. (Обратите внимание, что эти столбцы нужно было пройти по порядку, потому что каждый текущий использовался при вычислении следующего.)

Пример 1.2.2. Составьте таблицу истинности для формулы $\neg(P \wedge Q) \vee \neg R$.

Решение

P	Q	R	$P \wedge Q$	$\neg(P \wedge Q)$	$\neg R$	$\neg(P \wedge Q) \vee \neg R$
F	F	F	F	T	T	T
F	F	T	F	T	F	T
F	T	F	F	T	T	T
F	T	T	F	T	F	T
T	F	F	F	T	T	T
T	F	T	F	T	F	T
T	T	F	T	F	T	T
T	T	T	T	F	F	F

Обратите внимание: поскольку эта формула содержит три буквы, требуется восемь строк, чтобы перечислить все возможные комбинации значений истинности для этих букв. (Если формула содержит n разных букв, сколько строк будет в ее таблице истинности?)

Существует способ сделать таблицы истинности более компактными. Вместо того чтобы использовать отдельные столбцы для перечисления значений истинности для составных частей формулы, просто перечислите эти значения истинности под соответствующим соединительным символом в исходной формуле. Это показано в табл. 1.5 для формулы из примера 1.2.1. На первом шаге мы перечислили значения истинности для P и Q под теми буквами, где они появляются в формуле. На втором шаге под символом \neg для $\neg Q$ были добавлены значения истинности для $\neg Q$. На третьем шаге мы объединили значения истинности для P и $\neg Q$, чтобы получить значения истинности для $P \vee \neg Q$, которые перечислены под символом \vee . Наконец, на последнем шаге эти значения истинности инвертируются и перечислены под начальным символом. Значения истинности, добавленные на последнем шаге, дают значение истинности для всей формулы, поэтому мы будем называть символ, под которым они перечислены (в данном случае первый

символ), главной связкой формулы. Обратите внимание, что значения истинности, перечисленные под главной связкой в этом случае, согласуются со значениями, которые мы нашли в примере 1.2.1.

Таблица 1.5. Пошаговое компактное представление

Шаг 1			Шаг 2		
P	Q	$\neg(P \vee \neg Q)$	$\neg R$	Q	$\neg(P \vee \neg Q)$
F	F	F F	F	F	F TF
F	T	T F	F	T	F FT
T	F	F F	T	F	T TF
T	T	T F	T	T	F FT

Шаг 3			Шаг 4		
P	Q	$\neg(P \vee \neg Q)$	$\neg R$	Q	$\neg(P \vee \neg Q)$
F	F	F T TF	F	F	F F T TF
F	T	F F FT	F	T	T F F FT
T	F	T T TF	T	F	F T T TF
T	T	T T FT	T	T	F T T FT

Теперь, когда мы знаем, как составлять таблицы истинности для сложных формул, мы готовы вернуться к анализу истинности рассуждений. Вернемся к первому примеру дедуктивного рассуждения:

Завтра будет дождь или снег.

Слишком тепло для снега.

Значит, пойдет дождь.

Как мы видели, если мы присвоим обозначение P утверждению «Завтра будет дождь», а Q – утверждению «Завтра пойдет снег», то мы можем символически представить рассуждение следующим образом:

$$\frac{P \vee Q \\ \neg Q}{\therefore P}$$

где символ \therefore означает *следовательно*.

Давайте посмотрим, как можно использовать таблицы истинности для проверки достоверности этого рассуждения. В табл. 1.6 представлена таблица истинности как для посылок, так и для вывода рассуждений. Напомним, что мы решили назвать рассуждение допустимым, если все предпосылки не могут быть истинными без истинного заключения. Глядя на табл. 1.6, мы видим, что единственная строка таблицы, в которой оба предположения оказываются верными, – это третья строка, и в этой строке вывод также верен. Таким образом, таблица истинности подтверждает, что если все посылки истинны, вывод также должен быть истинным, поэтому рассуждение действительно.

Таблица 1.6. Таблица истинности для посылок и вывода рассуждения

		Посылки		Заключение
P	Q	$P \vee Q$	$\neg Q$	P
F	F	F	T	F
F	T	T	F	F
T	F	T	T	T
T	T	T	F	T

Пример 1.2.3. Определите, действительны ли следующие рассуждения.

- Либо Джон не умен и просто везучий, либо он умен.
Джон умен.
Следовательно, Джон невезучий.
- Дворецкий и повар не являются оба одновременно невиновными.
Либо дворецкий лжет, либо повар невиновен.
Следовательно, дворецкий либо лжет, либо виноват.

Решения

- Как и в примере 1.1.3, пусть S означает утверждение «Джон умен», а L означает «Джон везучий». Тогда рассуждение имеет вид:

$$\begin{array}{c} (\neg S \wedge L) \vee S \\ S \\ \hline \therefore \neg L \end{array}$$

Теперь составим таблицу истинности как для посылок, так и для заключения. (Вам следует проработать промежуточные шаги при выводе третьего столбца этой таблицы, чтобы убедиться в его правильности.)

		Посылки		Заключение
S	L	$(\neg S \wedge L) \vee S$	S	$\neg L$
F	F	F	F	T
F	T	T	F	F
T	F	T	T	T
T	T	T	T	F

Обе посылки верны в третьей и четвертой строках этой таблицы. Заключение также верно в третьей строке, но неверно в четвертой строке. Таким образом, мы наблюдаем ситуацию, когда обе посылки истинные, а вывод – ложный, поэтому рассуждение недействительно. Фактически таблица показывает нам, почему это так. Проблема возникает в четвертой строке таблицы, в которой S и L истинны – иными словами, Джон и умен, и удачлив. Таким образом, если Джон и умен, и удачлив, то обе посылки будут истинными, но вывод будет ложным, поэтому было бы ошибкой делать вывод о том, что вывод должен быть истинным из предположения, что посылки истинны.

2. Пусть B означает утверждение «Дворецкий невиновен», C – утверждение «Повар невиновен» и L – утверждение «Дворецкий лжет». Тогда рассуждение имеет вид:

$$\begin{array}{c} \neg(B \wedge C) \\ L \vee C \\ \hline \therefore L \vee \neg B \end{array}$$

Вот таблица истинности для посылок и заключения:

			Посылки	Заключение	
B	C	L	$\neg(B \wedge C)$	$L \vee C$	$L \vee \neg B$
F	F	F	T	F	T
F	F	T	T	T	T
F	T	F	T	T	T
F	T	T	T	T	T
T	F	F	T	F	F
T	F	T	T	T	T
T	T	F	F	T	F
T	T	T	F	T	T

Обе посылки верны только во второй, третьей, четвертой и шестой строках, и в каждом из этих случаев верен и вывод. Следовательно, рассуждение действительно.

Если вы ожидали, что первое рассуждение в примере 1.2.3 окажется верным, возможно, это потому, что вас смутила первая посылка. Это довольно сложное утверждение, которое мы символически представили формулой $(\neg S \wedge L) \vee S$. Согласно нашей таблице истинности, эта формула ложна, если S и L ложны, и истинна в противном случае. Но обратите внимание, что это в точности то же самое, что и таблица истинности для более простой формулы $L \vee S$! Поэтому мы говорим, что формулы $(\neg S \wedge L) \vee S$ и $L \vee S$ эквивалентны. Эквивалентные формулы всегда имеют одинаковое значение истинности независимо от того, какие утверждения обозначают буквы в них, и независимо от того, каковы значения истинности этих утверждений. Эквивалентность посылки $(\neg S \wedge L) \vee S$ и более простой формулы $L \vee S$ может помочь вам понять, почему рассуждение ошибочно. Переводя формулу $L \vee S$ обратно на разговорный язык, мы видим, что первую предпосылку можно было бы сформулировать проще: «Джон либо удачив, либо умен (либо то и другое)». Но из этой посылки и второй посылки (что Джон умен) явно не следует, что он невезучий, потому что он может быть одновременно умен и удачив.

Пример 1.2.4. Какие из этих формул эквивалентны?

$$\neg(P \wedge Q), \neg P \wedge \neg Q, \neg P \vee \neg Q.$$

Решение

Вот таблица истинности для всех трех утверждений. (Вы должны ее проверить!)

P	Q	$\neg(P \wedge Q)$	$\neg P \wedge \neg Q$	$\neg P \vee \neg Q$
F	F	T	T	T
F	T	T	F	T
T	F	T	F	T
T	T	F	F	F

Третий и пятый столбцы в этой таблице идентичны, но они отличаются от четвертого столбца. Следовательно, формулы $\neg(P \wedge Q)$ и $\neg P \vee \neg Q$ эквивалентны, но ни одна из них не эквивалентна формуле $\neg P \wedge \neg Q$. Вы увидите в этом смысле, если задумаетесь о том, что означают формулы в реальной жизни. Например, предположим, что P означает «Yankee выиграли вчера вечером», а Q означает «Red Sox выиграли вчера вечером». Тогда формула $\neg(P \wedge Q)$ будет представлять утверждение «Yankee и Red Sox не выиграли вчера одновременно», а $\neg P \vee \neg Q$ будет представлять утверждение «Yankee или Red Sox не выиграли вчера вечером»; эти утверждения явно несут одну и ту же информацию. С другой стороны, $\neg P \wedge \neg Q$ будет представлять «Yankee и Red Sox оба не выиграли вчера вечером», что означает совершенно другое.

Вы можете сами убедиться, составив таблицу истинности, что формула $\neg P \wedge \neg Q$ из примера 1.2.4 эквивалентна формуле $\neg(P \vee Q)$. (Чтобы увидеть, что эта эквивалентность имеет смысл, обратите внимание, что утверждения «Yankee и Red Sox оба не выиграли вчера вечером» и «Это не тот случай, когда Yankee или Red Sox выиграли вчера вечером» означают одно и то же.) Эта эквивалентность, а также эквивалентность, обнаруженная в примере 1.2.4, называются *законами Де Моргана*. Они названы в честь британского математика Августа Де Моргана (1806–1871).

При анализе дедуктивных рассуждений и содержащихся в них утверждений полезно знать ряд часто встречающихся эквивалентностей. Самостоятельно составьте таблицы истинности для приведенных ниже эквивалентностей и убедитесь в том, что они имеют смысл, переведя формулы на разговорный язык, как мы сделали в примере 1.2.4.

Законы Де Моргана

$\neg(P \wedge Q)$ эквивалентно $\neg P \vee \neg Q$.

$\neg(P \vee Q)$ эквивалентно $\neg P \wedge \neg Q$.

Коммутативные законы

$P \wedge Q$ эквивалентно $Q \wedge P$.

$P \vee Q$ эквивалентно $Q \vee P$.

Ассоциативные законы

$P \wedge (Q \wedge R)$ эквивалентно $(P \wedge Q) \wedge R$.

$P \vee (Q \vee R)$ эквивалентно $(P \vee Q) \vee R$.

Идемпотентные законы

$P \wedge P$ эквивалентно P .

$P \vee P$ эквивалентно P .

Дистрибутивные законы

$P \wedge (Q \vee R)$ эквивалентно $(P \wedge Q) \vee (P \wedge R)$.

$P \vee (Q \wedge R)$ эквивалентно $(P \vee Q) \wedge (P \vee R)$.

Законы поглощения

$P \vee (P \wedge Q)$ эквивалентно P .

$P \wedge (P \vee Q)$ эквивалентно P .

Закон двойного отрицания

$\neg\neg P$ эквивалентно P .

Обратите внимание, что из-за ассоциативных законов мы можем опускать скобки в формулах $P \wedge Q \wedge R$ и $P \vee Q \vee R$, не беспокоясь о том, что полученная формула будет неоднозначной, потому что два возможных способа расстановки скобок приводят к эквивалентным формулам.

Многие эквиваленты в списке должны напомнить вам о похожих правилах, касающихся операций $+$, $-$ и \cdot в алгебре. Как и в алгебре, эти правила можно применять к более сложным формулам, и их можно комбинировать для выработки более сложных эквивалентностей. Любую из букв в этих эквивалентностях можно заменить более сложными формулами, и полученная эквивалентность останется верной. Например, заменив P в законе двойного отрицания формулой $Q \vee \neg R$, вы увидите, что $\neg(Q \vee \neg R)$ эквивалентно $Q \vee \neg R$. Кроме того, если две формулы эквивалентны, вы всегда можете заменить одну на другую в любом выражении, и результаты будут эквивалентными. Например, поскольку запись $\neg\neg P$ эквивалентна P , то, встретив $\neg\neg P$ в любой формуле, вы всегда можете заменить ее на P , и полученная формула будет эквивалентна исходной.

Пример 1.2.5. Найдите более простые формулы, эквивалентные этим формулам:

1. $\neg(P \vee \neg Q)$.
2. $\neg(Q \wedge \neg P) \vee P$.

Решения

1. $\neg(P \vee \neg Q)$

эквивалентно $\neg P \wedge \neg\neg Q$ (закон Де Моргана),

что эквивалентно $\neg P \wedge Q$ (закон двойного отрицания).

Вы можете проверить правильность этой эквивалентности, составив таблицу истинности для $\neg P \wedge Q$ и убедившись, что она такая же, как таблица истинности для $\neg(P \vee \neg Q)$, построенная в примере 1.2.1.

2. $\neg(Q \wedge \neg P) \vee P$

эквивалентно $(\neg Q \vee \neg\neg P) \vee P$ (закон Де Моргана),

что эквивалентно $(\neg Q \vee P) \vee P$ (закон двойного отрицания),

что эквивалентно $\neg Q \vee (P \vee P)$ (ассоциативный закон),

что эквивалентно $\neg Q \vee P$ (идемпотентный закон).

Некоторые эквивалентности основаны на том факте, что определенные формулы либо всегда истинны, либо всегда ложны. Например, вы можете проверить, составив таблицу истинности, что формула $Q \wedge (P \vee \neg P)$ эквивалентна просто Q . Но даже до того, как вы составите таблицу истинности, вы, вероятно, сможете понять, почему они эквивалентны. В каждой строке таблицы истинности $P \vee \neg P$ будет считаться истинным, и поэтому $Q \wedge (P \vee \neg P)$ будет считаться истинным, когда Q также истинно, и ложным, если Q ложно. Всегда верные формулы, такие как $P \vee \neg P$, называются *тавтологиями* (tautology). Точно так же формулы, которые всегда ложны, называются *контрадикциями* (contradiction). Например, формула $P \wedge \neg P$ представляет собой контрадикцию.

Пример 1.2.6. Являются ли эти формулы тавтологией или контрадикцией?

$$P \vee (Q \vee \neg P), P \wedge \neg(Q \vee \neg Q), P \vee \neg(Q \vee \neg Q).$$

Решение

Сначала мы составляем таблицу истинности для всех трех формул.

P	Q	$P \vee (Q \vee \neg P)$	$P \wedge \neg(Q \vee \neg Q)$	$P \vee \neg(Q \vee \neg Q)$
F	F	T	F	F
F	T	T	F	F
T	F	T	F	T
T	T	T	F	T

Из таблицы истинности видно, что первая формула является тавтологией, вторая – контрадикцией, а третья – ни то, ни другое. Фактически, поскольку последний столбец идентичен первому, третья формула эквивалентна P .

Теперь мы можем сформулировать еще несколько полезных законов, включающих тавтологию и контрадикции. Попробуйте самостоятельно убедить себя в правильности всех этих законов, разработав таблицы истинности для соответствующих утверждений.

Законы тавтологии

$P \wedge (\text{тавтология})$ эквивалентно P .

$P \vee (\text{тавтология})$ – это тавтология.

$\neg(\text{тавтология})$ – это контрадикция.

Законы контрадикции

$P \wedge (\text{контрадикция})$ – это контрадикция.

$P \vee (\text{контрадикция})$ эквивалентно P .

$\neg(\text{контрадикция})$ – это тавтология.

Пример 1.2.7. Найдите более простые формулы, эквивалентные следующим формулам:

1. $P \vee (Q \wedge \neg P)$.
2. $\neg(P \vee (Q \wedge \neg R)) \wedge Q$.

Решения

1. $P \vee (Q \wedge \neg P)$

эквивалентно $(P \vee Q) \wedge (P \vee \neg \neg P)$ (дистрибутивный закон),
что эквивалентно $P \vee Q$ (закон тавтологии).

Последний шаг основан на том факте, что $P \vee \neg P$ – тавтология.

2. $\neg(P \vee (Q \wedge \neg R)) \wedge Q$

эквивалентно $(\neg P \wedge \neg(Q \wedge \neg R)) \wedge Q$ (закон Де Моргана),
что эквивалентно $(\neg P \wedge (\neg Q \vee \neg \neg R)) \wedge Q$ (закон Де Моргана),
что эквивалентно $(\neg P \wedge (\neg Q \vee R)) \wedge Q$ (закон двойного отрицания),
что эквивалентно $\neg P \wedge ((\neg Q \vee R)) \wedge Q$ (ассоциативный закон),
что эквивалентно $\neg P \wedge (Q \wedge (\neg Q \vee R))$ (коммутативный закон),
что эквивалентно $\neg P \wedge ((Q \wedge \neg Q) \vee (Q \wedge R))$ (дистрибутивный закон),
что эквивалентно $\neg P \wedge (Q \wedge R)$ (закон контрадикции).

Последний шаг основан на том факте, что $Q \wedge \neg Q$ является контраполиксией. Наконец, по ассоциативному закону для \wedge мы можем убрать скобки, не делая формулу неоднозначной, поэтому исходная формула эквивалентна формуле $\neg P \wedge Q \wedge R$.

Упражнения

*1. Составьте таблицы истинности для следующих формул:

- (a) $\neg P \vee Q$.
(b) $(S \vee G) \wedge (\neg S \wedge \neg G)$.

2. Составьте таблицы истинности для следующих формул:

- (a) $\neg[P \wedge (Q \vee \neg P)]$.
(b) $(P \vee Q) \wedge (\neg P \vee R)$.

3. В этом упражнении мы будем использовать символ $+$ для обозначения *исключающего или*. Другими словами, $P + Q$ означает « P или Q , но не оба».

- (a) Составьте таблицу истинности для $P + Q$.
(b) Используя только связки \wedge , \vee и \neg , найдите формулу, эквивалентную $P + Q$. Обоснуйте свой ответ таблицей истинности.

4. Используя только связки \wedge и \neg , найдите формулу, эквивалентную $P \vee Q$. Подкрепите свой ответ таблицей истинности.

*5. Некоторые математики используют для обозначения операции НЕ-ИЛИ символ \downarrow . Другими словами, $P \downarrow Q$ означает «ни P , ни Q ».

- (a) Составьте таблицу истинности для $P \downarrow Q$.
(b) Используя только связки \wedge , \vee и \neg , найдите формулу, эквивалентную $P \downarrow Q$.
(c) Используя только связку \downarrow , найдите формулы, эквивалентные $\neg P$, $P \vee Q$ и $P \wedge Q$.

6. Некоторые математики используют запись $P | Q$, означающую, что « P и Q не являются оба истинными». (Эта связка называется И-НЕ и используется при описании схем в информатике.)

- (a) Составьте таблицу истинности для $P \mid Q$.
 (b) Используя только связки \wedge , \vee и \neg , найдите формулу, эквивалентную $P \mid Q$.
 (c) Используя только связку \mid , найдите формулы, эквивалентные $\neg P$, $P \vee Q$ и $P \wedge Q$.
- *7. Используйте таблицы истинности, чтобы определить, истинны ли рассуждения из упражнения 9 раздела 1.1.
8. Используйте таблицы истинности, чтобы определить, какие из следующих формул эквивалентны друг другу:
- $(P \wedge Q) \vee (\neg P \wedge \neg Q)$.
 - $\neg P \vee Q$.
 - $(P \vee \neg Q) \wedge (Q \vee \neg P)$.
 - $\neg(P \vee Q)$.
 - $(Q \wedge P) \vee \neg P$.
- *9. Используйте таблицы истинности, чтобы определить, какие из этих утверждений являются тавтологиями, какие – контрадикциями, а какие – ни тем, ни другим:
- $(P \vee Q) \wedge (\neg P \vee \neg Q)$.
 - $(P \vee Q) \wedge (\neg P \wedge \neg Q)$.
 - $(P \vee Q) \vee (\neg P \vee \neg Q)$.
 - $[P \wedge (Q \vee \neg R)] \vee (\neg P \vee R)$.
10. Используйте таблицы истинности, чтобы проверить эти законы:
- Второй закон Де Моргана. (Первый проверен в тексте выше.)
 - Распределительные законы.
- *11. Используйте законы, указанные выше, чтобы найти более простые формулы, эквивалентные этим формулам (см. примеры 1.2.5 и 1.2.7).
- $\neg(\neg P \wedge \neg Q)$.
 - $(P \wedge Q) \vee (P \wedge \neg Q)$.
 - $\neg(P \wedge \neg Q) \vee (\neg P \wedge Q)$.
12. Используйте законы, изложенные в тексте, чтобы найти более простые формулы, эквивалентные этим формулам (см. примеры 1.2.5 и 1.2.7).
- $\neg(\neg P \vee Q) \vee (P \wedge \neg R)$.
 - $\neg(\neg P \wedge Q) \vee (P \wedge \neg R)$.
 - $(P \wedge R) \vee [\neg R \wedge (P \vee Q)]$.
13. Используйте первый закон Де Моргана и закон двойного отрицания, чтобы вывести второй закон Де Моргана.
- *14. Обратите внимание, что ассоциативные законы говорят только о том, что скобки не нужны при объединении трех утверждений с \wedge или \vee . Фактически эти законы могут использоваться для оправдания отказа от скобок, когда объединено более трех утверждений. Используйте ассоциативные законы, чтобы показать, что $[P \wedge (Q \wedge R)] \wedge S$ эквивалентно $(P \wedge Q) \wedge (R \wedge S)$.
15. Сколько строк будет в таблице истинности для утверждения, содержащего n букв?

*16. Найдите формулу, включающую связки \wedge , \vee и \neg , которой соответствует следующая таблица истинности:

P	Q	???
F	F	T
F	T	F
T	F	T
T	T	T

17. Найдите формулу, включающую связки \wedge , \vee и \neg , которой соответствует следующая таблица истинности:

P	Q	???
F	F	F
F	T	T
T	F	T
T	T	F

18. Предположим, что вывод рассуждения является тавтологией. Что вы можете сказать о справедливости рассуждения? Что делать, если вывод является контрадикцией? Что, если одна из предпосылок – тавтология или контрадикция?

1.3. ПЕРЕМЕННЫЕ И МНОЖЕСТВА

В математических рассуждениях часто необходимо делать утверждения об объектах, представленных буквами, которые называют *переменными*. Например, если переменная x используется для обозначения числа в некоторой задаче, нас может заинтересовать утверждение « x – простое число». Хотя иногда мы будем использовать одну букву, например P , для обозначения этого утверждения, в других случаях мы немного изменим это обозначение и напишем $P(x)$, чтобы подчеркнуть, что это утверждение относится именно к x . Последнее обозначение позволяет говорить о присвоении значения x в утверждении. Например, $P(7)$ будет представлять утверждение «7 – простое число», а $P(a + b)$ будет означать « $a + b$ – простое число». Если утверждение содержит более одной переменной, наша сокращенная запись утверждения будет включать список всех задействованных переменных. Например, мы могли бы представить утверждение « p делится на q » в виде $D(p, q)$. В этом случае $D(12, 4)$ будет означать «12 делится на 4».

Хотя вы, вероятно, привыкли, что переменные чаще всего используются для обозначения чисел, они могут обозначать что угодно. Например, мы вполне можем позволить нотации $M(x)$ обозначать утверждение « x – мужчина», а $W(x)$ – « x – женщина». В этом случае мы используем переменную x для обозначения человека. Утверждение может даже содержать несколько пере-

менных, которые обозначают разные типы объектов. Например, в утверждении « x имеет у детей» переменная x обозначает человека, а y обозначает число.

Утверждения, включающие переменные, можно комбинировать с помощью связок, как и утверждения без переменных.

Пример 1.3.1. Запишите логические формы следующих утверждений:

1. x – простое число, и либо y , либо z делится на x .
2. x – мужчина, y – женщина, x любит y , но y не любит x .

Решения

1. Обозначим как P утверждение « x – простое число», через D – « y делится на x » и E для « z делится на x ». Тогда ответ будет представлен формулой $P \wedge (D \vee E)$. Но эта формула, хотя и не является неправильной, не помогает уловить взаимосвязь между утверждениями D и E . Мы поступим иначе и через $P(x)$ обозначим посылку « x – простое число», а через $D(y, x)$ – « y делится на x ». Тогда $D(z, x)$ будет означать « z делится на x », поэтому полная запись будет иметь вид $P(x) \wedge (D(y, x) \vee D(z, x))$.
2. Пусть $M(x)$ означает « x – мужчина», $W(y)$ означает « y – женщина» и $L(x, y)$ – « x любит y ». Тогда $L(y, x)$ будет означать « y любит x ». (Обратите внимание, что порядок переменных после L имеет значение!) Тогда искомое утверждение будет представлено формулой $M(x) \wedge W(y) \wedge L(x, y) \wedge \neg L(y, x)$.

В предыдущем разделе мы рассмотрели присвоение значений истинности утверждениям. Это не вызывает проблем, если утверждения не содержат переменных, поскольку такие утверждения либо истинны, либо ложны. Но если утверждение содержит переменные, мы больше не можем описать это утверждение как просто истинное или ложное. Его значение истинности может зависеть от значений задействованных переменных. Например, если $P(x)$ означает утверждение « x – простое число», тогда $P(x)$ будет истинным, если $x = 23$, и ложным, если $x = 22$. Чтобы справиться с этим осложнением, мы определим *множество истинности* (truth set) для утверждений, содержащих переменные. Однако перед тем, как дать это определение, было бы полезно рассмотреть некоторые основные определения из теории множеств.

Множество – это набор объектов. Объекты набора называются *элементами* множества. Самый простой способ определить конкретное множество – перечислить его элементы в фигурных скобках. Например, $\{3, 7, 14\}$ – это множество, элементами которого являются три числа: 3, 7 и 14. Чтобы показать, что элемент входит в множество, используют символ \in . Например, пусть A обозначает множество $\{3, 7, 14\}$, тогда мы можем написать $7 \in A$, чтобы показать, что 7 является элементом A . Чтобы показать, что 11 не является элементом A , пишут $11 \notin A$.

Множество полностью определено, если определены все его элементы. Следовательно, два множества с одинаковыми элементами всегда равны. Кроме того, когда множество определено путем перечисления элементов, то имеют значение только элементы в списке, а не порядок, в котором они

перечислены. Элемент может даже появляться в списке более одного раза. Таким образом, $\{3, 7, 14\}$, $\{14, 3, 7\}$ и $\{3, 7, 14, 7\}$ – три разных определения для одного и того же множества.

Разумеется, неудобно определять множество, содержащее очень большое количество элементов, путем прямого их перечисления, и невозможно дать такое определение для множества, содержащего бесконечно много элементов. Часто эту проблему можно решить, перечислив несколько элементов с многоточием (...) после них, если ясно, как следует продолжить список. Например, предположим, что мы определяем множество B , заявляя, что $B = \{2, 3, 5, 7, 11, 13, 17, \dots\}$. Как только вы узнаете, что элементы, перечисленные в определении B , являются простыми числами, вам станет ясно, что, например, $23 \in B$, даже несмотря на то, что этот элемент не указан в списке. Но этот метод требует понимания шаблона, заложенного в определении B , и вводит в наши обозначения двусмысленность и субъективность, которых следует избегать в математической записи. Поэтому обычно лучше определять такое множество, строго описывая принцип, определяющий элементы множества.

В нашем случае мы можем строго определить B следующим образом:

$$B = \{x \mid x \text{ – простое число}\}.$$

Это читается как « B равно множеству всех x , таких, что x является простым числом», и это означает, что элементы B являются значениями x , которые делают утверждение « x – простое число» истинным. Вы должны думать об утверждении « x – простое число» как о проверке на принадлежность к множеству. Любое значение x , которое делает это утверждение истинным, проходит проверку и является элементом множества. Все остальные значения не проходят проверку и не являются элементами объявленного множества. Конечно, в данном случае значения x , которые делают утверждение истинным, являются в точности простыми числами, поэтому такое определение говорит, что B – это множество, элементы которого являются простыми числами, как мы и говорили раньше.

Пример 1.3.2. Перепишите эти определения множеств, используя проверку принадлежности:

1. $E = \{2, 4, 6, 8, \dots\}$.
2. $P = \{\text{Джордж Вашингтон, Джон Адамс, Томас Джефферсон, Джеймс Мэдисон, ...}\}$.

Решения

Хотя могут быть и другие способы продолжить эти списки элементов, вероятно, наиболее естественными из них являются следующие определения:

1. $E = \{n \mid n \text{ – четное положительное число}\}$.
2. $P = \{z \mid z \text{ был президентом США}\}$.

Если множество было определено с использованием проверки на принадлежность, то эту проверку можно использовать для выяснения того, является ли что-либо элементом множества. Например, рассмотрим множество

$\{x \mid x^2 < 9\}$. Если мы хотим знать, является ли 5 элементом этого множества, мы просто применяем проверку на принадлежность в определении множества – другими словами, мы проверяем, действительно ли $5^2 < 9$. Поскольку $5^2 = 25 > 9$, это число не проходит проверку, следовательно, $5 \notin \{x \mid x^2 < 9\}$. С другой стороны, $(-2)^2 = 4 < 9$, поэтому $-2 \in \{x \mid x^2 < 9\}$. Те же самые рассуждения применимы к любому другому числу. Для любого числа y , чтобы узнать, действительно ли $y \in \{x \mid x^2 < 9\}$, мы просто проверяем, выполняется ли условие $y^2 < 9$. Фактически запись $y \in \{x \mid x^2 < 9\}$ – это просто окольный способ сказать, что $y^2 < 9$.

Обратите внимание, что поскольку утверждение $y \in \{x \mid x^2 < 9\}$ означает то же самое, что и $y^2 < 9$, это утверждение про y , но не про x ! Чтобы определить, действительно ли $y \in \{x \mid x^2 < 9\}$, вам нужно знать значение y (чтобы вы могли сравнить его квадрат с 9), но не то, что такое x . Мы говорим, что в данном утверждении y – *свободная переменная*, а x – *связанная* (или *фиктивная*) переменная. Свободные переменные в утверждении обозначают объекты, о которых это утверждение что-то говорит. Присвоение различных значений свободной переменной влияет на смысл утверждения и может изменить его значение истинности. Тот факт, что вы можете подставлять разные значения для свободной переменной, означает, что она может иметь произвольные значения. С другой стороны, связанные переменные – это просто буквы, которые используются для удобства, чтобы выразить идею, и не должны рассматриваться как обозначение какого-либо конкретного объекта. Связанная переменная всегда может быть заменена новой переменной без изменения смысла утверждения, и часто утверждение можно перефразировать так, чтобы связанные переменные были полностью удалены. Например, утверждения $y \in \{x \mid x^2 < 9\}$ и $y \in \{w \mid w^2 < 9\}$ означают одно и то же, потому что оба они означают: « y – элемент множества всех чисел, квадраты которых меньше 9». В этом последнем утверждении (в разговорной форме) все связанные переменные были исключены, и единственная переменная, которая там фигурирует, – это свободная переменная y .

Обратите внимание, что x является связанный переменной в записи $y \in \{x \mid x^2 < 9\}$, даже если это свободная переменная в записи $x^2 < 9$. Эта последняя запись является утверждением про x , которое будет истинным для одних значений x и ложным для других. Только когда это утверждение используется в нотации проверки на принадлежность к множеству, x становится связанный переменной. Можно сказать, что обозначение $\{x \mid \dots\}$ *связывает* переменную x .

Все, что мы сказали о множестве $\{x \mid x^2 < 9\}$, будет применяться к любому множеству, определенному проверкой на принадлежность элементов. В общем случае утверждение $y \in \{x \mid P(x)\}$ означает то же самое, что и $P(y)$, которое является утверждением относительно y , но не x . Точно так же $y \notin \{x \mid P(x)\}$ означает то же самое, что и $\neg P(y)$. Конечно, выражение $\{x \mid P(x)\}$ во все не является утверждением; это упоминание множества. По мере того как вы изучаете все больше математических обозначений, становится все более важным быть внимательным, чтобы различать выражения, которые являются математическими утверждениями, и выражения, которые являются упоминаниями математических объектов.

Пример 1.3.3. Что означают эти утверждения? Какие свободные переменные содержатся в каждом утверждении?

1. $a + b \notin \{x \mid x \text{ четное число}\}$.
2. $y \in \{x \mid x \text{ делится на } w\}$.
3. $2 \in \{w \mid 6 \notin \{x \mid x \text{ делится на } w\}\}$.

Решения

1. Эта запись говорит, что $a + b$ не является элементом множества всех четных чисел, или, другими словами, $a + b$ не является четным числом. И a , и b – свободные переменные, но x – связанная переменная. Утверждение будет истинным для одних значений a и b и ложным для других.
2. Эта запись говорит, что y делится на w . И y , и w – свободные переменные, но x – связанная переменная. Утверждение верно для одних значений y и w и ложно для других.
3. Эта запись выглядит довольно сложно, но если мы будем двигаться по шагам, то сможем ее расшифровать. Во-первых, обратите внимание, что утверждение $6 \notin \{x \mid x \text{ делится на } w\}$, которое присутствует внутри данной записи, означает то же самое, что и «6 не делится на w ». Представляя эквивалентную форму в исходную запись, мы находим, что исходное утверждение эквивалентно более простому утверждению $2 \in \{w \mid 6 \text{ не делится на } w\}$. Но это просто означает то же самое, что и «6 не делится на 2». Таким образом, в исходной записи нет свободных переменных, и обе переменные, x и w , – связанные. Поскольку свободных переменных нет, истинное значение утверждения не зависит от значений каких-либо переменных. Фактически, поскольку 6 делится на 2, утверждение ложно.

Возможно, вы уже догадались, как мы можем использовать теорию множеств, чтобы лучше понять значения истинности утверждений, содержащих свободные переменные. Как мы видели, утверждение, скажем, $P(x)$, содержащее свободную переменную x , может быть истинным для одних значений x и ложным для других. Чтобы отличить значения x , которые делают $P(x)$ истинным, от тех, которые делают его ложным, мы можем сформировать множество значений x , для которых $P(x)$ истинно. Мы будем называть его *множеством истинности* $P(x)$.

Определение 1.3.4. Множество истинности утверждения $P(x)$ – это множество всех значений x , которые делают утверждение $P(x)$ истинным. Другими словами, это множество, определенное с помощью утверждения $P(x)$ в качестве критерия принадлежности: $\{x \mid P(x)\}$.

Обратите внимание, что мы определили множества истинности только для утверждений, содержащих одну свободную переменную. В главе 4 мы обсудим множества истинности для утверждений с более чем одной свободной переменной.

Пример 1.3.5. Каковы множества истинности следующих утверждений?

1. Шекспир написал x .
2. n – четное простое число.

Решения

1. $\{x \mid \text{Шекспир написал } x\} = \{\text{Гамлет, Макбет, Двенадцатая ночь, ...}\}$.
2. $n \mid n$ четное простое число}. Поскольку единственное четное простое число – это 2, множество состоит из одного элемента {2}. Обратите внимание, что 2 и {2} – это не одно и то же! В первом случае это число, а во втором – это множество, единственным элементом которого является число. Таким образом, $2 \in \{2\}$, но $2 \neq \{2\}$.

Предположим, что A – это множество истинности утверждения $P(x)$. Согласно определению множества истинности, это означает, что $A = \{x \mid P(x)\}$. Мы уже видели, что для любого объекта у утверждение $y \in \{x \mid P(x)\}$ означает то же самое, что и $P(y)$. Следовательно, $y \in A$ означает то же, что и $P(y)$. Таким образом, в общем случае, если A является множеством истинности $P(x)$, то утверждение $y \in A$ означает то же самое, что и $P(y)$.

Когда утверждение содержит свободные переменные, из контекста часто ясно, что эти переменные обозначают объекты определенного типа. Множество всех объектов такого типа – другими словами, множество всех возможных значений переменных – называется *универсумом обсуждения* (universe of discourse, универсум дискурса, область рассуждений, предметная область) для этого утверждения, и мы говорим, что переменные *пробегают* (range over) этот универсум. Например, в большинстве случаев универсум для утверждения $x^2 < 9$ будет представлять собой множество всех действительных чисел; универсумом для утверждения « x – человек» служит множество всех людей.

Некоторые универсумы встречаются в математике чаще других, и для них удобно иметь постоянные названия. Вот несколько самых важных универсумов:

$$\mathbb{R} = \{x \mid x \text{ действительное число}\}.$$

$$\mathbb{Q} = \{x \mid x \text{ рациональное число}\}.$$

(Напомним, что *действительное* число – это любое число числового ряда, а *рациональное* число – это число, которое может быть записано как дробь p/q , где p и q – целые числа.)

$$\mathbb{Z} = \{x \mid x \text{ целое число}\} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}.$$

$$\mathbb{N} = \{x \mid x \text{ натуральное число}\} = \{0, 1, 2, 3, \dots\}.$$

(В некоторых книгах 0 является натуральным числом, а в некоторых нет. В этой книге мы считаем 0 натуральным числом.)

За символом \mathbb{R} , \mathbb{Q} и \mathbb{Z} может следовать верхний индекс + или -, чтобы указать, что в множество должны быть включены только положительные или отрицательные числа. Например, $\mathbb{R}^+ = \{x \mid x \text{ положительное действительное число}\}$, а $\mathbb{Z}^- = \{x \mid x \text{ отрицательное целое число}\}$.

Хотя универсум обсуждения обычно можно определить из контекста, иногда полезно идентифицировать его явно. Рассмотрим утверждение $P(x)$ со свободной переменной x , которая пробегает универсум U . Хотя мы записали множество истинности $P(x)$ как $\{x \mid P(x)\}$, если бы существовала какая-либо возможность неоднозначности в идентификации дискурса, мы могли бы указать его явно, написав $\{x \in U \mid P(x)\}$; эта запись читается как «множество всех x в U таких, что $P(x)$ ». Это обозначение указывает, что только элементы U должны рассматриваться как кандидаты на вхождение в множество истинности, а среди элементов U только прошедшие проверку соответствия $P(x)$ фактически войдут в это множество. Например, снова рассмотрим утверждение $x^2 < 9$. Если бы универсум для этого утверждения был множеством всех действительных чисел, то его множество истинности имело бы вид $\{x \in \mathbb{R} \mid x^2 < 9\}$, или, другими словами, множество всех действительных чисел от -3 до 3 . Но если бы универсум был множеством всех целых чисел, то множество истинности имело бы вид $\{x \in \mathbb{Z} \mid x^2 < 9\} = \{-2, -1, 0, 1, 2\}$. Так, например, $1,58 \in \{x \in \mathbb{R} \mid x^2 < 9\}$, но $1,58 \notin \{x \in \mathbb{Z} \mid x^2 < 9\}$. Очевидно, что выбор универсума может иметь значение!

Иногда эта явная нотация используется не для определения универсума, а для ограничения области внимания только частью универсума. Например, в случае утверждения $x^2 < 9$ мы можем рассматривать универсум как множество всех действительных чисел, но в ходе некоторых рассуждений, связанных с этим утверждением, мы можем решить временно ограничить наше внимание только положительными действительными числами. Тогда нас заинтересует множество $\{x \in \mathbb{R}^+ \mid x^2 < 9\}$. Как и раньше, эта нотация указывает, что только положительные действительные числа будут рассматриваться как кандидаты в элементы этого множества, а среди них только те, чей квадрат меньше 9 , войдут в множество. Таким образом, чтобы число стало элементом этого множества, оно должно пройти две проверки: оно должно быть положительным действительным числом, а его квадрат должен быть меньше 9 . Другими словами, утверждение $y \in \{x \in \mathbb{R}^+ \mid x^2 < 9\}$ означает то же самое, что $y \in \mathbb{R}^+ \wedge y^2 < 9$. В общем случае $y \in \{x \in A \mid P(x)\}$ означает то же, что и $y \in A \wedge P(y)$.

Как только появляется новая математическая концепция, математики обычно стараются исследовать все возможные ее крайности. Например, когда мы говорили о таблицах истинности, то рассматривали крайние утверждения, таблицы истинности которых содержали только Т (тавтологии) или только F (противоречия). Для концепции множества истинности утверждения, содержащего свободную переменную, соответствующими крайностями будут множества истинности утверждений, которые всегда истинны или всегда ложны. Предположим, что $P(x)$ – это утверждение, содержащее свободную переменную x , которая пробегает по универсуму U . Очевидно, что если $P(x)$ будет истинным для каждого значения x в U , то множество истинности $P(x)$ вберет в себя весь U . Например, поскольку утверждение $x^2 \geq 0$ истинно для любого действительного числа x , множество истинности этого утверждения имеет вид $\{x \in \mathbb{R} \mid x^2 \geq 0\} = \mathbb{R}$. Конечно, здесь не обошлось без тавтологии. Например, поскольку $P \vee \neg P$ является тавтологией, утверждение $P(x) \vee \neg P(x)$ будет истинным для каждого $x \in U$, независимо от того, что обо-

значает утверждение $P(x)$ или каков универсум U , и, следовательно, множеством истинности утверждения $P(x) \vee \neg P(x)$ будет U .

Для утверждения $P(x)$, которое является ложным для каждого возможного значения x , ничто в универсуме не может пройти проверку на принадлежность к множеству истинности $P(x)$, и поэтому оно не должно иметь элементов. Идея множества без элементов может показаться странной, но она возникает естественным образом, когда мы рассматриваем множества истинности для утверждений, которые всегда ложны. Поскольку множество полностью определено после определения его элементов, существует только одно множество, не имеющее элементов. Оно называется *пустым*, или *нулевым*, множеством и часто обозначается символом \emptyset . Например, $\{x \in \mathbb{Z} \mid x = x\} = \emptyset$. Поскольку пустое множество не имеет элементов, утверждение $x \in \emptyset$ является примером утверждения, которое всегда ложно, независимо от x .

Еще одно распространенное обозначение пустого множества основано на том факте, что любое множество можно объявить, перечислив его элементы в фигурных скобках. Поскольку пустое множество не имеет элементов, мы ничего не пишем между фигурными скобками, например $\emptyset = \{\}$. Обратите внимание, что $\{\emptyset\}$ – неправильная запись для пустого множества. Как мы видели ранее, 2 и {2} не одно и то же, а \emptyset – это не то же самое, что $\{\emptyset\}$. В первом случае это множество без элементов, а во втором это множество с одним элементом, и этот один элемент представляет собой \emptyset , то есть пустое множество.

Упражнения

*1. Запишите логические формы следующих утверждений:

- (a) 3 является общим делителем 6, 9 и 15. (Примечание: вы сделали это в упражнении 2 раздела 1.1, но теперь вы сможете дать более точный ответ.)
- (b) x делится как на 2, так и на 3, но не на 4.
- (c) x и y – натуральные числа, и ровно одно из них простое.

2. Запишите логические формы следующих утверждений:

- (a) x и y – мужчины, и либо x выше y , либо y выше x .
- (b) Либо x , либо y имеет карие глаза, и либо x , либо y имеет рыжие волосы.
- (c) Либо x , либо y имеет карие глаза и рыжие волосы.

*3. Напишите определения множеств, используя проверки принадлежности для следующих множеств:

- (a) {Меркурий, Венера, Земля, Марс, Юпитер, Сатурн, Уран, Нептун}.
- (b) {Браун, Колумбия, Корнелл, Дартмут, Гарвард, Принстон, Пенсильвянский университет, Йель}¹.
- (c) {Алабама, Аляска, Аризона, ..., Висконсин, Вайоминг}².

¹ Университеты Лиги плюща. – Прим. перев.

² Названия штатов в составе США. – Прим. перев.

- (d) {Альберта, Британская Колумбия, Манитоба, Нью-Брансуик, Ньюфаундленд и Лабрадор, Северо-Западные территории, Новая Шотландия, Нунавут, Онтарио, Остров Принца Эдуарда, Квебек, Саскачеван, Юкон}¹.
4. Напишите определения, используя проверки принадлежности для следующих множеств:
- {1, 4, 9, 16, 25, 36, 49, ...}.
 - {1, 2, 4, 8, 16, 32, 64, ...}.
 - {10, 11, 12, 13, 14, 15, 16, 17, 18, 19}.
- *5. Упростите следующие утверждения. Какие переменные свободны, а какие связаны? Если в утверждении нет свободных переменных, скажите, истинно оно или ложно.
- $-3 \in \{x \in \mathbb{R} \mid 13 - 2x > 1\}$.
 - $4 \in \{x \in \mathbb{R}^+ \mid 13 - 2x > 1\}$.
 - $4 \notin \{x \in \mathbb{R} \mid 13 - 2x > c\}$.
6. Упростите следующие утверждения. Какие переменные свободны, а какие связаны? Если в утверждении нет свободных переменных, скажите, истинно оно или ложно.
- $w \in \{x \in \mathbb{R} \mid 13 - 2x > c\}$.
 - $4 \in \{x \in \mathbb{R} \mid 13 - 2x \in \{y \mid y \text{ простое число}\}\}$. (Это утверждение можно сделать проще для чтения, если принять $P = \{y \mid y \text{ простое число}\}$; используя это обозначение, можно переписать утверждение как $4 \in \{x \in \mathbb{R} \mid 13 - 2x \in P\}$.)
 - $4 \in \{x \in \{y \mid y \text{ простое число}\} \mid 13 - 2x > 1\}$. (Используя те же обозначения, что и в части (b), мы могли бы записать это как $4 \in \{x \in P \mid 13 - 2x > 1\}$.)
7. Перечислите элементы следующих множеств:
- $\{x \in \mathbb{R} \mid 2x^2 + x - 1 = 0\}$.
 - $\{x \in \mathbb{R}^+ \mid 2x^2 + x - 1 = 0\}$.
 - $\{x \in \mathbb{Z} \mid 2x^2 + x - 1 = 0\}$.
 - $\{x \in \mathbb{N} \mid 2x^2 + x - 1 = 0\}$.
- *8. Каковы множества истинности следующих утверждений? Если можете, перечислите несколько элементов каждого множества истинности.
- Элизабет Тейлор когда-то была замужем за x .
 - x – логическая связка, изучаемая в разделе 1.1.
 - x является автором этой книги.
9. Каковы множества истинности следующих утверждений? Если можете, перечислите несколько элементов каждого множества истинности.
- x – действительное число, и $x^2 - 4x + 3 = 0$.
 - x – действительное число, и $x^2 - 2x + 3 = 0$.
 - x – действительное число, и $5 \in \{y \in \mathbb{R} \mid x^2 + y^2 < 50\}$.

¹ Провинции и территории Канады. – Прим. перев.

1.4. ОПЕРАЦИИ НАД МНОЖЕСТВАМИ

Предположим, что A – это множество истинности утверждения $P(x)$, а B – множество истинности утверждения $Q(x)$. Каковы множества истинности утверждений $P(x) \wedge Q(x)$, $P(x) \vee Q(x)$ и $\neg P(x)$? Чтобы ответить на эти вопросы, мы вводим некоторые основные операции над множествами.

Определение 1.4.1. Пересечение двух множеств A и B – это множество $A \cap B$, определенное следующим образом:

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

Объединение двух множеств A и B – это множество $A \cup B$, определенное следующим образом:

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

Разность двух множеств A и B – это множество $A \setminus B$, определенное следующим образом:

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

Помните, что утверждения, которые фигурируют в этих определениях, являются тестами на принадлежность к множеству. Так, например, определение $A \cap B$ говорит, что для того, чтобы объект был элементом множества $A \cap B$, он должен быть элементом как A , так и B . Другими словами, $A \cap B$ – это множество, состоящее из общих элементов A и B . Поскольку слово «или» в математике всегда интерпретируется как включающее или, все, что является элементом либо A , либо B , либо обоих, будет элементом множества $A \cup B$. Таким образом, мы можем думать о $A \cup B$ как о множестве, полученном в результате сваливания всех элементов A и B в одно множество. $A \setminus B$ – это множество, которое вы получили бы, если бы взяли множество A и удалили из него все элементы, которые также присутствуют в B .

Пример 1.4.2. Предположим, что $A = \{1, 2, 3, 4, 5\}$ и $B = \{2, 4, 6, 8, 10\}$. Перечислите элементы следующих множеств:

1. $A \cap B$.
2. $A \cup B$.
3. $A \setminus B$.
4. $(A \cup B) \setminus (A \cap B)$.
5. $(A \setminus B) \cup (B \setminus A)$.

Решения

1. $A \cap B = \{2, 4\}$.
2. $A \cup B = \{1, 2, 3, 4, 5, 6, 8, 10\}$.
3. $A \setminus B = \{1, 3, 5\}$.
4. Мы только что вычислили $A \cup B$ и $A \cap B$ в решениях 1 и 2, поэтому все, что нам нужно сделать, – это начать с множества $A \cup B$ из решения 2

и удалить из него все элементы, которые также находятся в $A \cap B$. Ответ: $(A \cup B) \setminus (A \cap B) = \{1, 3, 5, 6, 8, 10\}$.

5. У нас уже есть элементы $A \setminus B$, перечисленные в решении 3, и $B \setminus A = \{6, 8, 10\}$. Следовательно, их объединением будет множество $(A \setminus B) \cup (B \setminus A) = \{1, 3, 5, 6, 8, 10\}$. Как вы думаете, это множество случайно совпало с множеством из решения 4?

Пример 1.4.3. Предположим, что $A = \{x \mid x \text{ человек}\}$ и $B = \{x \mid x \text{ имеет каштановые волосы}\}$. Что такое $A \cap B$, $A \cup B$ и $A \setminus B$?

Решение

По определению $A \cap B = \{x \mid x \in A \text{ и } x \in B\}$. Как мы видели в последнем разделе, определения A и B говорят нам, что $x \in A$ означает то же самое, что « x – мужчина», а $x \in B$ означает то же самое, что « x имеет каштановые волосы». Вставляя эти значения в определение $A \cap B$, мы обнаруживаем, что

$$A \cap B = \{x \mid x \text{ мужчина, } x \text{ имеет каштановые волосы}\}.$$

Аналогичные рассуждения дают нам

$$A \cup B = \{x \mid \text{либо } x \text{ мужчина, либо } x \text{ имеет каштановые волосы}\},$$

а также

$$A \setminus B = \{x \mid x \text{ мужчина, и } x \text{ не имеет каштановых волос}\}.$$

Иногда бывает полезно при работе с операциями над множествами нарисовать изображения результатов этих операций. Один из способов сделать это – использовать диаграммы, подобные показанной на рис. 1.1. Они называются *диаграммами Венна*. Внутренняя часть прямоугольника, охватывающего диаграмму, представляет собой универсум U , а внутренние части двух кругов представляют два множества A и B . Другие множества, образованные той или иной комбинацией этих множеств, будут представлены различными областями на диаграмме. Например, заштрихованная область на рис. 1.2 является областью, общей для внутренних частей кругов, представляющих A и B , и поэтому она представляет множество $A \cap B$. На рис. 1.3 и 1.4 показаны области, представляющие $A \cup B$ и $A \setminus B$ соответственно.

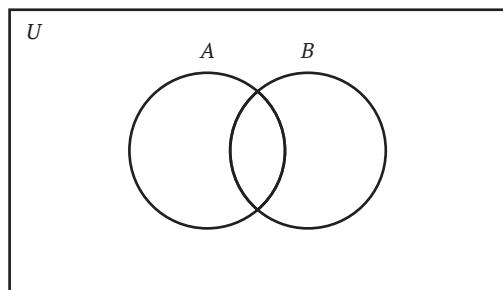
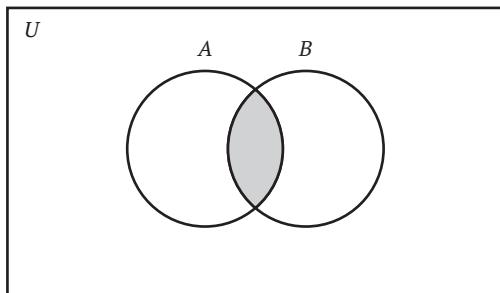
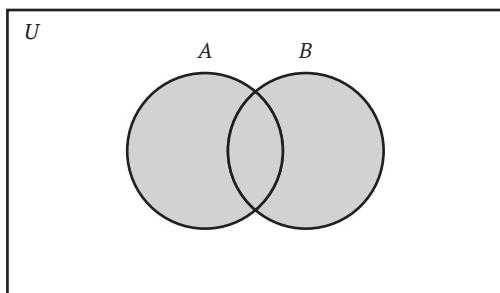
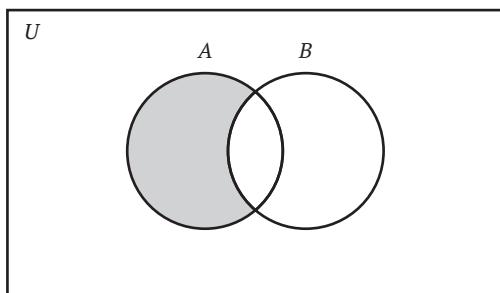


Рис. 1.1 ♦ Множества A и B в универсуме U

Рис. 1.2 ♦ Пересечение множеств $A \cap B$ Рис. 1.3 ♦ Объединение множеств $A \cup B$ Рис. 1.4 ♦ Разность множеств $A \setminus B$

Вот пример того, как диаграммы Венна могут помочь нам понять операции над множествами. В примере 1.4.2 множества $(A \cup B) \setminus (A \cap B)$ и $(A \setminus B) \cup (B \setminus A)$ оказались одинаковыми при конкретном наборе элементов множеств A и B . Построив диаграммы Венна для обоих множеств, вы можете убедиться, что это не было совпадением. Вы обнаружите, что обе диаграммы Венна выглядят как на рис. 1.5. Следовательно, эти множества всегда будут равны, независимо от того, из каких элементов состоят A и B , потому что оба множества всегда будут набором объектов, которые являются элементами либо A , либо B , но не обоих одновременно. Это множество называется *симметричной разностью* A и B и обозначается $A \Delta B$. Другими словами, $A \Delta B = (A \setminus B) \cup (B \setminus A)$.

$= (A \cup B) \setminus (A \cap B)$. Позже в этом разделе мы увидим другое объяснение того, почему эти множества всегда равны.

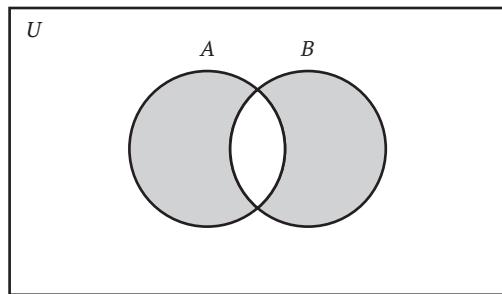


Рис. 1.5 ♦ $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$

Вернемся к вопросу, с которого мы начали этот раздел. Если A – множество истинности утверждения $P(x)$, а B – множество истинности $Q(x)$, то, как мы видели выше, $x \in A$ означает то же, что и $P(x)$, а $x \in B$ означает то же самое, что и $Q(x)$. Таким образом, множество истинности $P(x) \wedge Q(x)$ определяется записью $\{x \mid P(x) \wedge Q(x)\} = \{x \mid x \in A \wedge x \in B\} = A \cap B$. В эту запись заложен простой смысл. Она говорит нам, что множество истинности $P(x) \wedge Q(x)$ состоит из тех элементов, которые являются общими для множеств истинности $P(x)$ и $Q(x)$, – другими словами, значений x , которые делают истинными как $P(x)$, так и $Q(x)$. Мы уже видели пример этого. В примере 1.4.3 множества A и B были множествами истинности утверждений « x – мужчина» и « x имеет каштановые волосы», а $A \cap B$ оказалось множеством истинности « x – мужчина и x имеет каштановые волосы».

Аналогичные рассуждения показывают, что множеством истинности $P(x) \vee Q(x)$ является $A \cup B$. Чтобы найти множество истинности $\neg P(x)$, нам нужно обратиться к универсуму U . Множество истинности $\neg P(x)$ будет состоять из тех элементов универсума, для которых $P(x)$ ложно, и мы можем найти это множество, взяв U и удалив из него те элементы, для которых $P(x)$ истинно. Таким образом, множество истинности $\neg P(x)$ есть $U \setminus A$.

Эти наблюдения о множествах истинности иллюстрируют тот факт, что операции теории множеств \cap , \cup и \setminus имеют отношение к логическим связкам \wedge , \vee и \neg . Это не должно вызывать удивления, поскольку в конце концов в их определениях встречаются слова *и*, *или* и *не*. (Слово *не* скрыто в математическом символе \notin в определении разницы двух множеств.) Однако важно помнить, что хотя операции теории множеств и логические связки близки по смыслу, они не взаимозаменяемы. Логические связки могут использоваться только для связывания *утверждений*, тогда как операции теории множеств должны использоваться для операций со *множествами*. Например, если A – множество истинности $P(x)$, а B – множество истинности $Q(x)$, то мы можем сказать, что $A \cap B$ – множество истинности $P(x) \wedge Q(x)$, но такие выражения, как $A \wedge B$ или $P(x) \cap Q(x)$, совершенно бессмысленны и никогда не должны использоваться.

Связь между операциями теории множеств и логическими связками также становится очевидной, когда мы анализируем логические формы утверждений о пересечениях, объединениях и разностях множеств. Например, согласно определению пересечения, запись $x \in A \cap B$ означает то же самое, что $x \in A \wedge x \in B$. Аналогично, запись $x \in A \cup B$ означает то же самое, что $x \in A \vee x \in B$, а запись $x \in A \setminus B$ равнозначна $x \in A \wedge x \notin B$, или, немного иначе, $x \in A \wedge \neg(x \in B)$. Мы можем комбинировать эти правила при записи более сложных утверждений о множествах.

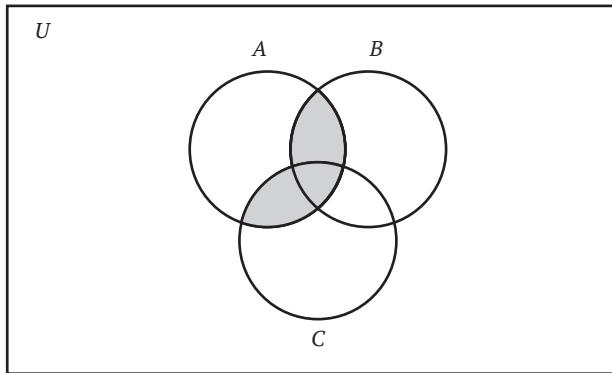
Пример 1.4.4. Запишите логические формы следующих утверждений:

1. $x \in A \cap (B \cup C)$.
2. $x \in A \setminus (B \cap C)$.
3. $x \in (A \cap B) \cup (A \cap C)$.

Решения

1. $x \in A \cap (B \cup C)$
эквивалентно $x \in A \wedge x \in (B \cup C)$ (определение \cap),
что эквивалентно $x \in A \wedge (x \in B \vee x \in C)$ (определение \cup).
2. $x \in A \setminus (B \cap C)$
эквивалентно $x \in A \wedge \neg(x \in B \cap C)$ (определение \setminus),
что эквивалентно $x \in A \wedge \neg(x \in B \wedge x \in C)$ (определение \cap).
3. $x \in (A \cap B) \cup (A \cap C)$
эквивалентно $x \in (A \cap B) \vee x \in (A \cap C)$ (определение \cup),
что эквивалентно $(x \in A \wedge x \in B) \vee (x \in A \wedge x \in C)$ (определение \cap).

Посмотрите еще раз на решения 1 и 3 примера 1.4.4. Вы должны признать, что утверждения, которые мы получили в этих двух частях, эквивалентны. (Если вы не согласны, вернитесь к дистрибутивным законам в разделе 1.2.) Эта эквивалентность означает, что утверждения $x \in A \cap (B \cup C)$ и $x \in (A \cap B) \cup (A \cap C)$ эквивалентны. Другими словами, объекты, являющиеся элементами множества $A \cap (B \cup C)$, будут точно такими же, как объекты, которые являются элементами $(A \cap B) \cup (A \cap C)$, независимо от того, каковы множества A , B и C . Но напомним, что множества с одинаковыми элементами равны, следовательно, для любых множеств A , B и C справедливо равенство $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Другой способ убедиться в этом – использовать диаграмму Венна на рис. 1.6. На наших предыдущих диаграммах Венна было два круга, потому что в предыдущих примерах объединялись только два множества. На этой диаграмме Венна есть три круга, которые представляют три множества A , B и C , которые в данном случае объединяются. Хотя можно создать диаграммы Венна для более чем трех множеств, это делается редко, потому что это невозможно сделать с перекрывающимися кругами. Подробнее о диаграммах Венна для более чем трех множеств см. в упражнении 12.

Рис. 1.6 ♦ $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

Таким образом, мы видим, что дистрибутивный закон для логических связок приводит к дистрибутивному закону для операций теории множеств. Вы можете догадаться, что поскольку существует два дистрибутивных закона для логических связок, причем \wedge и \vee играют противоположные роли в этих двух законах, могут существовать два дистрибутивных закона и для операций теории множеств. Второй дистрибутивный закон для множеств должен гласить, что для любых множеств A , B и C справедлива запись $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. Вы можете убедиться в этом сами, записав выражения $x \in A \cup (B \cap C)$ и $x \in (A \cup B) \cap (A \cup C)$, используя логические связки и установив, что они эквивалентны, используя второй закон распределения для логических связок \wedge и \vee . Еще один способ убедиться в этом – построить диаграмму Венна.

Мы можем вывести другое тождество теории множеств, найдя утверждение, эквивалентное утверждению, которое мы получили в части 2 примера 1.4.4:

$$x \in A \setminus (B \cap C)$$

- | | |
|---|-----------------------------|
| эквивалентно $x \in A \wedge \neg(x \in B \cap C)$ | (пример 1.4.4), |
| что эквивалентно $x \in A \wedge (x \notin B \vee x \notin C)$ | (закон Де Моргана), |
| что эквивалентно $(x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C)$ | (дистрибутивный закон), |
| что эквивалентно $(x \in A \setminus B) \vee (x \in A \setminus C)$ | (определение \setminus), |
| что эквивалентно $x \in (A \setminus B) \cup (A \setminus C)$ | (определение \cup). |

Таким образом, мы показали, что для любых множеств A , B и C справедливо $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$. И это вы тоже можете проверить с помощью диаграммы Венна.

Ранее мы обещали альтернативный способ проверки тождества $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$. Сейчас вы увидите, как это можно сделать. Сначала выпишем логические формы утверждений $x \in (A \cup B) \setminus (A \cap B)$ и $x \in (A \setminus B) \cup (B \setminus A)$:

- | | |
|--|---|
| $x \in (A \cup B) \setminus (A \cap B)$ | означает $(x \in A \vee x \in B) \wedge \neg(x \in A \wedge x \in B)$; |
| $x \in (A \setminus B) \cup (B \setminus A)$ | означает $(x \in A \wedge x \notin B) \vee \neg(x \in B \wedge x \notin A)$. |

Теперь вы можете проверить, что эти утверждения эквивалентны, используя эквивалентности из раздела 1.2. Альтернативный способ проверить эквивалентность – использовать таблицу истинности. Чтобы упростить таблицу истинности, давайте использовать P и Q в качестве сокращений для утверждений $x \in A$ и $x \in B$. Затем мы должны проверить, что формулы $(P \vee Q) \wedge \neg(P \wedge Q)$ и $(P \wedge \neg Q) \vee (Q \wedge \neg P)$ эквивалентны. Для этого составим таблицу истинности (табл. 1.7).

Таблица 1.7. Таблица истинности для проверки эквивалентности формул

P	Q	$(P \vee Q) \wedge \neg(P \wedge Q)$	$(P \wedge \neg Q) \vee (Q \wedge \neg P)$
F	F	F	F
F	T	T	T
T	F	T	T
T	T	F	F

Определение 1.4.5. Предположим, что A и B – множества. Мы будем говорить, что A является подмножеством B , если каждый элемент A также является элементом B . Мы пишем $A \subseteq B$, чтобы обозначать, что A является подмножеством B . Множества A и B называются непересекающимися, если они не имеют общих элементов. Обратите внимание: это то же самое, что сказать, что множество общих элементов, которые они имеют, является пустым множеством, или, другими словами, $A \cap B = \emptyset$.

Пример 1.4.6. Предположим, $A = \{\text{красный, зеленый}\}$, $B = \{\text{красный, желтый, зеленый, фиолетовый}\}$ и $C = \{\text{синий, фиолетовый}\}$. Тогда два элемента A , красный и зеленый, оба также находятся в B и, следовательно, $A \subseteq B$. Кроме того, $A \cap C = \emptyset$, поэтому A и C не пересекаются.

Если мы знаем, что $A \subseteq B$ или что A и B не пересекаются, мы можем нарисовать две разные диаграммы Венна, чтобы проиллюстрировать эти случаи (рис. 1.7 и 1.8).

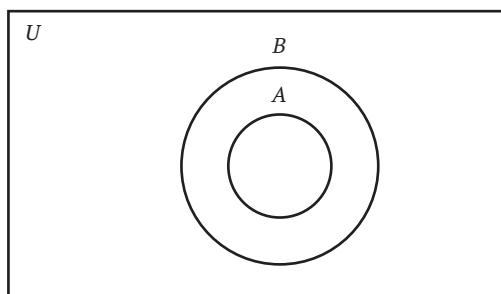
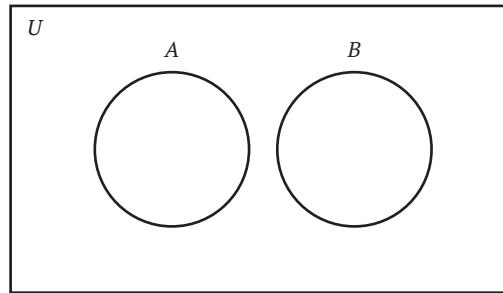


Рис. 1.7 ♦ $A \subseteq B$

Рис. 1.8 ♦ $A \cap B = \emptyset$

Подобно тому, как мы ранее выводили тождества, показывающие, что определенные множества всегда равны, также иногда можно показать, что определенные множества всегда не пересекаются или что одно множество всегда является подмножеством другого. Например, вы можете видеть на диаграмме Венна, что множества $A \cap B$ и $A \setminus B$ не перекрываются, и поэтому они всегда будут непересекающимися для любых множеств A и B . Другой способ показать это – написать логическими символами, что означает запись $x \in (A \cap B) \cap (A \setminus B)$:

$x \in (A \cap B) \cap (A \setminus B)$ означает $(x \in A \wedge x \in B) \wedge (x \in A \wedge x \notin B)$,
что эквивалентно $x \in A \wedge (x \in B \wedge x \notin B)$.

Но последнее утверждение содержит явное противоречие, поэтому утверждение $x \in (A \cap B) \cap (A \setminus B)$ всегда будет ложным независимо от x . Другими словами, ничто не может быть элементом множества $(A \cap B) \cap (A \setminus B)$, отсюда следует, что $(A \cap B) \cap (A \setminus B) = \emptyset$. Следовательно, $A \cap B$ и $A \setminus B$ не пересекаются.

Следующая теорема демонстрирует еще один пример общего факта, относящегося к операциям над множествами. Доказательство этой теоремы показывает, что принципы дедуктивного мышления, которые мы изучали, действительно используются в математических доказательствах.

Теорема 1.4.7. Для любых множеств A и B справедлива запись $(A \cup B) \setminus B \subseteq A$.

Доказательство. Мы должны показать, что если что-то является элементом $(A \cup B) \setminus B$, то оно также должно быть элементом A , поэтому предположим, что $x \in (A \cup B) \setminus B$. Это означает, что $x \in (A \cup B) \setminus B$ и $x \notin B$, или, другими словами, $x \in A \vee x \in B$ и $x \notin B$. Но обратите внимание, что эти утверждения имеют логическую форму $P \vee Q$ и $\neg Q$, и это в точности форма посылок нашего самого первого примера дедуктивного рассуждения в разделе 1.1! Как мы видели в этом примере, из посылок мы можем заключить, что $x \in A$ является истинным. Таким образом, все, что является элементом множества $(A \cup B) \setminus B$, также должно быть элементом A , следовательно, $(A \cup B) \setminus B \subseteq A$.

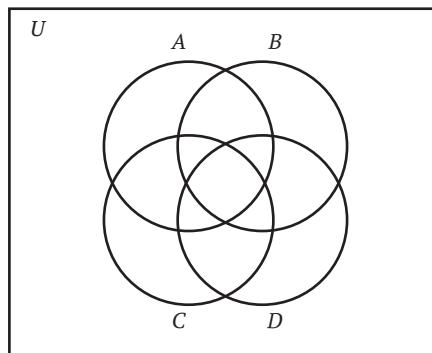
Вы можете сказать, что нам не требуется такое тщательное применение логических законов, чтобы понять, почему теорема 1.4.7 верна. Множество $(A \cup B) \setminus B$ можно рассматривать как результат последовательности действий,

когда мы начинаем с множества A , добавляем элементы B , а затем их удаляем. Здравый смысл подсказывает, что результатом будет просто исходное множество A ; другими словами, получается, что $(A \cup B) \setminus B = A$. Однако, как вас просят показать в упражнении 10 ниже, этот вывод неверен. Данний конфуз говорит о том, что в математике нельзя допускать, чтобы неточные рассуждения привели вас к поспешным выводам. Тщательное применение законов логики, как мы это делали в нашем доказательстве теоремы 1.4.7, поможет вам избежать поспешных выводов.

Упражнения

- *1. Пусть $A = \{1, 3, 12, 35\}$, $B = \{3, 7, 12, 20\}$ и $C = \{x \mid x \text{ простое число}\}$. Перечислите элементы следующих множеств. Не пересекаются ли какие-либо из приведенных ниже множеств с другими? Является ли какое-нибудь из перечисленных ниже множеств подмножеством другого множества?
 - (a) $A \cap B$.
 - (b) $(A \cup B) \setminus C$.
 - (c) $A \cup (B \setminus C)$.
- 2. Пусть $A = \{\text{США, Германия, Китай, Австралия}\}$, $B = \{\text{Германия, Франция, Индия, Бразилия}\}$ и $C = \{x \mid x \text{ страна в Европе}\}$. Перечислите элементы следующих множеств. Не пересекаются ли какие-либо из приведенных ниже множеств с другими? Является ли какое-нибудь из перечисленных ниже множеств подмножеством другого множества?
 - (a) $A \cup B$.
 - (b) $(A \cap B) \setminus C$.
 - (c) $(B \cap C) \setminus A$.
- 3. Убедитесь, что диаграммы Венна для $(A \cup B) \setminus (A \cap B)$ и $(A \setminus B) \cup (B \setminus A)$ выглядят как на рис. 1.5.
- *4. Используйте диаграммы Венна для проверки следующих идентичностей:
 - (a) $A \setminus (A \cap B) = A \setminus B$.
 - (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.
- 5. Проверьте идентичности в упражнении 4, написав с использованием логических символов, что означает принадлежность объекта x к каждому множеству, а затем используйте логические эквивалентности.
- 6. Используйте диаграммы Венна для проверки следующих идентичностей:
 - (a) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$.
 - (b) $A \cup (B \setminus C) = (A \cup B) \setminus (C \setminus A)$.
- 7. Проверьте идентичности в упражнении 6, написав с использованием логических символов, что означает принадлежность объекта x к каждому множеству, а затем используйте логические эквивалентности.

8. Используйте любой метод по своему выбору для подтверждения следующих идентичностей:
- $(A \setminus B) \cap C = (A \cap C) \setminus B$.
 - $(A \cap B) \setminus B = \emptyset$.
 - $A \setminus (A \setminus B) = A \cap B$.
- *9. Для каждого из следующих множеств запишите (используя логические символы), что означает принадлежность x к множеству. Затем определите, какие из этих множеств должны быть равны друг другу, определяя, какие утверждения эквивалентны.
- $(A \setminus B) \setminus C$.
 - $A \setminus (B \setminus C)$.
 - $(A \setminus B) \cup (A \cap C)$.
 - $(A \setminus B) \cap (A \setminus C)$.
 - $A \setminus (B \cup C)$.
10. В этом разделе было показано, что для любых множеств A и B $(A \cup B) \setminus B \subseteq A$.
- Приведите пример двух множеств A и B , для которых $(A \cup B) \setminus B = A$.
 - Покажите, что для всех множеств A и B $(A \cup B) \setminus B = A \setminus B$.
11. Предположим, что A и B – множества. Обязательно ли верно, что $(A \setminus B) \cup B = A$? Если нет, обязательно ли одно из этих множеств является подмножеством другого? Всегда ли $(A \setminus B) \cup B$ равно либо $A \setminus B$, либо $A \cup B$?
- *12. В этом разделе сказано, что вы не можете построить диаграмму Венна для четырех множеств, используя перекрывающиеся круги.
- Что не так в следующей диаграмме? Подсказка: где множество $(A \cap D) \setminus (B \cup C)$?



- Можете ли вы составить диаграмму Венна для четырех множеств, используя фигуры, отличные от окружностей?
13. (a) Составьте диаграммы Венна для множеств $(A \cup B) \setminus C$ и $A \cup (B \setminus C)$. Как вы можете сделать вывод о том, обязательно ли одно из этих множеств является подмножеством другого?

- (b) Приведите пример множеств A , B и C , для которых $(A \cup B) \setminus C \neq A \cup (B \setminus C)$.
- *14. Используйте диаграммы Венна, чтобы показать, что ассоциативный закон выполняется для симметричной разности; то есть для любых множеств A , B и C , $A(B \Delta C) = (A \Delta B)C$.
15. Подтвердите следующие идентичности любым удобным для вас методом:
- $(A \Delta B) \cup C = (A \cup C) \Delta (B \setminus C)$.
 - $(A \Delta B) \cap C = (A \cap C) \Delta (B \cap C)$.
 - $(A \Delta B) \setminus C = (A \setminus C) \Delta (B \setminus C)$.
16. Подтвердите следующие идентичности любым удобным для вас методом:
- $(A \cup B) \Delta C = (A \Delta C) \Delta (B \setminus A)$.
 - $(A \cap B) \Delta C = (A \Delta C) \Delta (A \cap B)$.
 - $(A \setminus B) \Delta C = (A \Delta C) \Delta (A \cap B)$.
17. Заполните пропуски, чтобы образовалась идентичность:
- $(A \Delta B) \cap C = (C \setminus A) \Delta \underline{\hspace{2cm}}$.
 - $C \setminus (A \Delta B) = (A \cap C) \Delta \underline{\hspace{2cm}}$.
 - $(B \setminus A) \Delta C = (A \Delta C) \Delta \underline{\hspace{2cm}}$.

1.5. УСЛОВНЫЕ И РАВНОЗНАЧНЫЕ СВЯЗКИ

Пора вернуться к вопросу, который мы оставили без ответа в разделе 1.1. Мы видели, как можно понять первое и третье рассуждения в примере 1.1.1, проанализировав связки \vee и \neg . Но как насчет справедливости второго рассуждения? Напомним, рассуждение было таким:

Если сегодня воскресенье, то сегодня мне не нужно идти на работу.
Сегодня воскресенье.

Поэтому сегодня мне не нужно идти на работу.

Что делает это рассуждение справедливым?

Похоже, что решающие слова здесь – *если* и *то*, которые встречаются в первой посылке. Поэтому мы вводим новую логическую связку \rightarrow и пишем $P \rightarrow Q$, чтобы представить утверждение «Если P , то Q ». Это утверждение иногда называют *условным утверждением*, где P является его *условием*, или *антecedентом*, а Q – его *следствием*. Если мы через P обозначим утверждение «Сегодня воскресенье», а Q – утверждение «Мне не нужно идти сегодня на работу», то логическая форма рассуждения будет такой:

$$\frac{\begin{array}{l} P \rightarrow Q \\ P \end{array}}{\therefore Q}$$

Наш анализ новой связки \rightarrow должен привести к выводу, что это рассуждение действительно.

Пример 1.5.1. Запишите логические формы следующих утверждений:

1. Если идет дождь и у меня нет зонтика, я промокну.
2. Если Мэри сделала домашнее задание, то учитель не соберет тетради, а если нет, то он попросит ее выполнить задание на доске.

Решения

1. Пусть R обозначает утверждение «идет дождь», U – «у меня есть зонтик», а W – «я промокну». Тогда утверждение 1 можно представить формулой $(R \wedge \neg U) \rightarrow W$.
2. Пусть H означает «Мэри сделала домашнее задание», C – «Учитель соберет тетради», а B – «Учитель попросит Мэри сделать домашнее задание на доске». Тогда второе утверждение можно представить формулой $(H \rightarrow \neg C) \wedge (\neg H \rightarrow B)$.

Чтобы проанализировать рассуждения, содержащие связку \rightarrow , мы должны составить таблицу истинности для формулы $P \rightarrow Q$. Поскольку $P \rightarrow Q$ должно означать, что если P истинно, то Q также истинно, мы, конечно, можем сказать, что если P истинно, а Q ложно, то $P \rightarrow Q$ ложно. Если P истинно и Q также истинно, то можно утверждать, что $P \rightarrow Q$ истинно. Это дает нам последние две строки таблицы истинности. Предыдущие две строки таблицы истинности заполнить сложнее, хотя, вероятно, большинство людей сказали бы, что если P и Q оба ложны, то $P \rightarrow Q$ следует считать истинным. Таким образом, мы можем резюмировать наши выводы с помощью табл. 1.8.

Таблица 1.8. Предварительная таблица истинности для формулы $P \rightarrow Q$

P	Q	$P \rightarrow Q$
F	F	T?
F	T	?
T	F	F
T	T	T

Чтобы понять, как заполнить неопределенные строки в этой таблице истинности, давайте рассмотрим пример. Возьмем утверждение «Если $x > 2$, то $x^2 > 4$ », которое мы могли бы представить формулой $P(x) \rightarrow Q(x)$, где $P(x)$ означает утверждение $x > 2$, а $Q(x)$ означает $x^2 > 4$. Конечно, утверждения $P(x)$ и $Q(x)$ содержат x как свободную переменную, и каждое из них будет истинным для одних значений x и ложным для других. Но, конечно же, независимо от значения x мы можем сказать, что верно, если $x > 2$, то $x^2 > 4$, поэтому условное утверждение $P(x) \rightarrow Q(x)$ должно быть истинным. Следовательно, таблица истинности должна быть заполнена так, чтобы независимо от значения x это условное утверждение получалось истинным.

Например, предположим, что $x = 3$. В этом случае $x > 2$ и $x^2 = 9 > 4$, поэтому $P(x)$ и $Q(x)$ истинны. Это соответствует четвертой строке таблицы истинности.

сти 1.8, и мы уже решили, что в этом случае утверждение $P(x) \rightarrow Q(x)$ должно выполняться. Но теперь рассмотрим случай $x = 1$. Тогда $x < 2$ и $x^2 = 1 < 4$, так что $P(x)$ и $Q(x)$ оба ложны, что соответствует первой строке в таблице истинности. Мы предварительно поставили букву Т в эту строку таблицы истинности и теперь видим, что этот интуитивный выбор должен быть правильным. Если мы поместим туда F, то утверждение $P(x) \rightarrow Q(x)$ окажется ложным в случае $x = 1$, а мы уже решили, что оно должно быть истинным для всех значений x .

Наконец, рассмотрим случай $x = -5$. Тогда $x < 2$, поэтому $P(x)$ ложно, но $x^2 = 25 > 4$, поэтому $Q(x)$ истинно. Этот случай соответствует второй строке таблицы истинности, и еще раз, если условное утверждение $P(x) \rightarrow Q(x)$ должно быть истинным в этом случае, мы должны поставить Т в этой строке. Получается, что все сомнительные строки в таблице истинности 1.8 должны быть заполнены буквами «Т», а заполненная таблица истинности для связки \rightarrow должна быть такой, как показано в табл. 1.9.

Таблица 1.9. Окончательная таблица истинности для формулы $P \rightarrow Q$

P	Q	$P \rightarrow Q$
F	F	T
F	T	T
T	F	F
T	T	T

Конечно, есть много других значений x , которые можно было бы включить в наше утверждение «Если $x > 2$, то $x^2 > 4$ »; но если вы попробуете их, то обнаружите, что все они ведут к первой, второй или четвертой строке таблицы истинности, как это делали наши примеры $x = 1, -5$ и 3. Никакое значение x не приведет к третьей строке, потому что вы никогда не найдете такой x , что $x > 2$, но $x^2 \leq 4$. В конце концов, именно поэтому мы сказали, что утверждение «Если $x > 2$, то $x^2 > 4$ » всегда истинно, несмотря ни на какое значение x ! Смысл того, что это условное утверждение всегда истинно, состоит в том, чтобы просто сказать, что вы никогда не найдете значение x такое, что $x > 2$ и $x^2 \leq 4$, – другими словами, не существует значения x , для которого $P(x)$ верно, но $Q(x)$ ложно. Таким образом, получается, что в таблице истинности для $P \rightarrow Q$ единственная ложная строка – это строка, в которой P истинно, а Q ложно.

Как показывает таблица истинности 1.10, формула $\neg P \vee Q$ также истинна во всех случаях, кроме тех случаев, когда P истинно, а Q ложно. Таким образом, если мы примем таблицу истинности на рис. 1.9 как правильную таблицу истинности для формулы $P \rightarrow Q$, тогда мы будем вынуждены принять вывод, что формулы $P \rightarrow Q$ и $\neg P \vee Q$ эквивалентны. Соответствует ли это тому, как слова *если* и *то* используются в обычном языке? Поначалу может показаться, что это не так, но, по крайней мере, для некоторых случаев использования слов *если* и *то* это так.

Таблица 1.10. Таблица истинности формулы $\neg P \vee Q$

P	Q	$\neg P \vee Q$
F	F	T
F	T	T
T	F	F
T	T	T

Например, представьте, что учитель говорит классу угрожающим тоном: «Не ленитесь делать домашнее задание, иначе провалите контрольную работу». Грамматически это утверждение имеет форму $\neg P \vee Q$, где P – это утверждение «Вы будете лениться делать домашнее задание», а Q – «Вы провалите контрольную работу». Но какое сообщение учитель пытается передать этим утверждением? Ясно, что подразумевается сообщение: «Если вы поленились делать домашнее задание, то провалите контрольную работу», или, другими словами, $P \rightarrow Q$. Таким образом, в этом примере формулы $\neg P \vee Q$ и $P \rightarrow Q$, кажется, означают одно и то же.

Аналогичная идея работает в первом утверждении из примера 1.1.2: «Или Джон пошел в магазин, или у нас закончились яйца». В разделе 1.1 мы представили это утверждение формулой $P \vee Q$, где P означает «Джон пошел в магазин», а Q – «У нас закончились яйца». Но кто-то, кто сделал это заявление, вероятно, пытался выразить мысль о том, что если Джон не пойдет в магазин, то у нас закончатся яйца, или, другими словами, $\neg P \rightarrow Q$. Таким образом, этот пример предполагает, что $\neg P \rightarrow Q$ означает то же, что и $P \vee Q$. Фактически мы можем вывести эту эквивалентность из предыдущего рассуждения, заменив $\neg P$ на P . Поскольку $P \rightarrow Q$ эквивалентно $\neg P \vee Q$, отсюда следует, что $\neg P \rightarrow Q$ эквивалентно $\neg\neg P \vee Q$, что эквивалентно $P \vee Q$ по закону двойного отрицания.

Мы можем вывести еще одну полезную эквивалентность следующим образом:

$\neg P \vee Q$ эквивалентно $\neg P \vee \neg\neg Q$ (закон двойного отрицания),
что эквивалентно $\neg(P \wedge \neg Q)$ (закон Де Моргана).

Таким образом, $P \rightarrow Q$ также эквивалентно $\neg(P \wedge \neg Q)$. Фактически именно к этому выводу мы пришли ранее при обсуждении утверждения «Если $x > 2$, то $x^2 > 4$ ». Тогда мы решили, что причина, по которой это утверждение верно для любого значения x , заключается в том, что не существует значения x , для которого $x > 2$ и $x^2 \leq 4$. Другими словами, утверждение $P(x) \wedge \neg Q(x)$ никогда не будет истинно, где, как и раньше, $P(x)$ означает $x > 2$, а $Q(x)$ означает $x^2 > 4$. Но это равносильно заявлению, что утверждение $\neg(P(x) \wedge \neg Q(x))$ всегда истинно. Таким образом, утверждение, что $P(x) \rightarrow Q(x)$ всегда истинно, равносильно утверждению, что $\neg(P(x) \wedge \neg Q(x))$ всегда истинно.

В качестве другого примера этой эквивалентности рассмотрим утверждение «Если пойдет дождь, то я возьму свой зонтик». Конечно, это утверждение имеет форму $P \rightarrow Q$, где P означает утверждение «Пойдет дождь», а Q означает «Я возьму свой зонтик». Но мы могли бы также рассматривать это заявление как заявление о том, что я не окажусь под дождем без зонта – другими словами, $\neg(P \wedge \neg Q)$.

Подводя итог, можно сказать, что на данный момент мы обнаружили следующие эквивалентности, связанные с условными утверждениями:

Законы условности

$$P \rightarrow Q \text{ эквивалентно } \neg P \vee Q.$$

$$P \rightarrow Q \text{ эквивалентно } \neg(P \wedge \neg Q).$$

Если вы все еще не уверены, что таблица истинности 1.9 верна, мы приводим еще одно обоснование. Мы знаем, что, используя эту таблицу истинности, теперь мы можем анализировать обоснованность дедуктивных рассуждений, включающих слова *если* и *то*. Когда мы проанализируем несколько простых рассуждений, то обнаружим, что таблица истинности 1.9 приводит к разумным выводам об их достоверности. Но если бы мы внесли какие-либо изменения в таблицу истинности, то пришли бы к явно неверным выводам. Например, вернемся к форме рассуждений, с которой мы начали этот раздел:

$$\begin{array}{c} P \rightarrow Q \\ P \\ \hline \therefore Q \end{array}$$

Мы уже решили, что такая форма рассуждений должна быть действительной, и таблица истинности 1.11 подтверждает это. Оба предположения истинны только в четвертой строке таблицы, и в этой строке также истинно заключение.

Таблица 1.11. Таблица истинности рассуждения по выводу заключения Q

		Посылки		Заключение	
P	Q	$P \rightarrow Q$	P	Q	
F	F	T	F	F	
F	T	T	F	T	
T	F	F	T	F	
T	T	T	T	T	

Из табл. 1.11 также следует, что для подтверждения этого рассуждения необходимы обе посылки. Но если бы мы изменили таблицу истинности для условного утверждения, сделав $P \rightarrow Q$ ложным в первой строке таблицы, то вторая посылка этого рассуждения больше не понадобилась бы. В итоге мы пришли бы к выводу, что только из одной посылки $P \rightarrow Q$ можно заключить, что Q должно быть истинным, поскольку в двух строках таблицы истинности, в которых посылка $P \rightarrow Q$ все еще будет истинной (во второй и четвертой строках), вывод Q также верен. Но это не выглядит правильным. Зная только, что *если P истинно, то Q истинно*, но не зная, что *P истинно на самом деле*, мы не можем сделать вывод, что *Q истинно*. Например, предположим, что мы знаем, что утверждение «*Если Джон не пошел в магазин, то у нас закончились яйца*» истинно. Но если мы при этом не знаем, пошел ли Джон в магазин, мы не сможем прийти к какому-либо выводу о том, закончились

ли у нас яйца. Таким образом, изменение первой строки таблицы истинности $P \rightarrow Q$ приведет к неправильному выводу о достоверности рассуждения.

Изменение второй строки таблицы истинности также приведет к неприемлемым выводам о достоверности рассуждений. Чтобы убедиться в этом, рассмотрим такую форму рассуждения:

$$\begin{array}{c} P \rightarrow Q \\ Q \\ \hline \therefore P \end{array}$$

Ее нельзя рассматривать как допустимую форму рассуждения. Например, рассмотрим следующее рассуждение:

Если Джонс был признан виновным в убийстве Смита, то он попадет в тюрьму.

Джонс попадет в тюрьму.

Таким образом, Джонс был признан виновным в убийстве Смита.

Даже если посылки этого рассуждения верны, из них вовсе не следует вывод о том, что Джонс был осужден за убийство Смита. Возможно, он попадет в тюрьму из-за того, что ограбил банк или не уплатил подоходный налог. Таким образом, заключение этого рассуждения может быть ложным, даже если посылки истинны, поэтому рассуждение ошибочно.

Запись таблицы истинности 1.12 согласуется с этим выводом. Во второй строке таблицы вывод P ложен, но обе посылки истинны, поэтому рассуждение ошибочно. Но обратите внимание: если бы мы изменили таблицу истинности $P \rightarrow Q$ и сделали ее ложной во второй строке, то анализ таблицы истинности сказал бы, что рассуждение верное. Следовательно, анализ этого рассуждения, судя по всему, согласуется с нашим решением поместить Т во вторую строку таблицы истинности для $P \rightarrow Q$.

Таблица 1.12. Таблица истинности рассуждения по выводу заключения P

Посылки		Заключение		
P	Q	$P \rightarrow Q$	Q	P
F	F	T	F	F
F	T	T	T	F
T	F	F	F	T
T	T	T	T	T

Последний пример показывает, что из посылок $P \rightarrow Q$ и Q нельзя вывести P . Но, безусловно, было бы правильным вывести P из посылок $Q \rightarrow P$ и Q . Это показывает, что формулы $P \rightarrow Q$ и $Q \rightarrow P$ не означают одно и то же. Вы можете проверить это, составив таблицу истинности для обеих формул и убедившись, что они не эквивалентны. Например, кто-то может полагать, что в целом утверждение «Если вы осужденный убийца, значит, вы не заслуживаете доверия» истинно, и это справедливо без того, чтобы истинным было утверждение «Если вы не заслуживаете доверия, значит, вы осужден-

ный убийца». Формула $Q \rightarrow P$ называется *обращением* $P \rightarrow Q$. Очень важно убедиться, что вы не путаете условное выражение с его обращением.

Контрапозицией (противопоставлением) $P \rightarrow Q$ является формула $\neg Q \rightarrow \neg P$, и она эквивалентна $P \rightarrow Q$. Сначала это может быть неочевидно, но вы можете проверить эквивалентность с помощью таблицы истинности. Например, утверждения «Если Джон обналичил выписанный мною чек, значит, на моем банковском счете овердрафт» и «Если на моем банковском счете нет овердрафта, то Джон не обналичил выписанный мной чек» эквивалентны. Я сказал бы и то, и другое при одинаковых обстоятельствах, а именно если бы выписал чек на сумму больше, чем у меня есть на счете. Эквивалентность условных утверждений и их контрапозиций часто используется в математических рассуждениях. Давайте добавим еще один пункт в наш список важных эквивалентов:

Закон конрапозиции

$P \rightarrow Q$ эквивалентно $\neg Q \rightarrow \neg P$.

Пример 1.5.2. Какие из следующих утверждений эквивалентны?

1. Если идет дождь или снег, то игра отменена.
2. Если игра не отменена, значит, сейчас не идет ни дождь, ни снег.
3. Если игра отменена, значит, идет дождь или снег.
4. Если идет дождь, то игра отменена, и если идет снег, то игра отменена.
5. Если нет ни дождя, ни снега, то игра не отменена.

Решение

Мы переводим все утверждения в логическую нотацию, используя следующие сокращения: R означает утверждение «идет дождь», S означает «идет снег», а C означает «игра отменена».

1. $(R \vee S) \rightarrow C$.
2. $\neg C \rightarrow (\neg R \wedge \neg S)$. По одному из законов Де Моргана это эквивалентно $\neg C \rightarrow \neg(R \vee S)$. Это противоположность утверждению 1, поэтому они эквивалентны.
3. $C \rightarrow (R \vee S)$. Это противоположность утверждению 1, которая ему *не* эквивалентна. Вы можете проверить это с помощью таблицы истинности или просто подумать, что означают эти утверждения. Утверждение 1 говорит, что дождь или снег приведут к отмене игры. В утверждении 3 говорится, что это *единственные* обстоятельства, при которых игра будет отменена.
4. $(R \rightarrow C) \wedge (S \rightarrow C)$. Это также эквивалентно утверждению 1, как показывают следующие рассуждения:

$$(R \rightarrow C) \wedge (S \rightarrow C)$$

эквивалентно $(\neg R \vee C) \wedge (\neg S \vee C)$

(условный закон),

что эквивалентно $(\neg R \wedge \neg S) \vee C$

(дистрибутивный закон),

что эквивалентно $\neg(R \vee S) \vee C$

(закон Де Моргана),

что эквивалентно $(R \vee S) \rightarrow C$

(условный закон).

Вам следует прочитать утверждения 1 и 4 еще раз и посмотреть, понятна ли вам их эквивалентность.

5. $\neg(R \vee S) \rightarrow \neg C$. Это контрапозиция утверждения 3, поэтому они эквивалентны. Но это не эквивалент утверждений 1, 2 и 4.

Утверждения, означающие $P \rightarrow Q$, очень часто встречаются в математике, но не всегда записываются в форме «если P , то Q ». Вот еще несколько способов выражения идеи $P \rightarrow Q$, которые часто используются в математике:

P влечет Q .

Q , если P .

P , только если Q .

P – достаточное условие для Q .

Q – необходимое условие для P .

Некоторые из них нуждаются в дополнительном объяснении. Второе выражение, « Q , если P », представляет собой слегка перефразированное утверждение «если P , то Q », поэтому достаточно очевидно, что оно означает $P \rightarrow Q$. В качестве примера утверждения формы « P , только если Q » можно привести предложение «Вы можете баллотироваться в президенты, только если вы гражданин этой страны». В этом случае P означает «Вы можете баллотироваться в президенты», а Q – «Вы гражданин этой страны». Это заявление означает, что если вы не гражданин, то вы не можете баллотироваться в президенты, или, другими словами, $\neg Q \rightarrow \neg P$. Но по закону контрапозиции это эквивалентно $P \rightarrow Q$.

Выражение « P – достаточное условие для Q » можно толковать как «Истинности P достаточно, чтобы гарантировать истинность Q », и представить формулой $P \rightarrow Q$. Наконец, « Q – необходимое условие для P » означает, что для того, чтобы P было истинным, необходимо, чтобы Q также было истинным. Это означает, что если Q не истинно, то P тоже не может быть истинным, или, другими словами, $\neg Q \rightarrow \neg P$. И снова по закону контрапозиции мы получаем $P \rightarrow Q$.

Пример 1.5.3. Запишите логические формы следующих утверждений:

1. Если придут не менее десяти человек, то будет прочитана лекция.
2. Лекция будет прочитана только при наличии не менее десяти человек.
3. Лекция будет прочитана при наличии не менее десяти человек.
4. Наличие не менее десяти человек является достаточным условием для чтения лекции.
5. Наличие не менее десяти человек – необходимое условие для чтения лекции.

Решения

Пусть T означает утверждение «Присутствуют как минимум десять человек», а L – «Будет прочитана лекция».

1. $T \rightarrow L$.
2. $L \rightarrow T$. Данное утверждение означает, что если там не будет хотя бы десяти человек, то лекция не будет проводиться, или, другими словами, $\neg T \rightarrow \neg L$. По закону контрапозиции это эквивалентно $L \rightarrow T$.

3. $T \rightarrow L$. Это просто перефразированное утверждение 1.
4. $T \rightarrow L$. В утверждении говорится, что наличия там не менее десяти человек достаточно, чтобы гарантировать, что лекция будет прочитана, а это означает, что если там будет не менее десяти человек, то лекция будет прочитана.
5. $L \rightarrow T$. Это утверждение означает то же, что и утверждение 2: если там не будет хотя бы десяти человек, то лекция не будет прочитана.

Мы уже видели, что условное выражение $P \rightarrow Q$ и обратное ему $Q \rightarrow P$ не эквивалентны. Часто в математике мы хотим сказать, что и $P \rightarrow Q$, и $Q \rightarrow P$ оба истинны, и для выражения этого факта удобно ввести новый символ логической связи « \leftrightarrow ». Вы можете считать $P \leftrightarrow Q$ сокращенной записью формулы $(P \rightarrow Q) \wedge (Q \rightarrow P)$. Утверждение вида $P \leftrightarrow Q$ называется *биусловным утверждением*, потому что оно представляет собой два условных утверждения. Создав таблицу истинности для $(P \rightarrow Q) \wedge (Q \rightarrow P)$, вы можете убедиться, что таблица истинности для $P \leftrightarrow Q$ такая, как показано на рис. 1.21. Обратите внимание, что по закону контрапозиции $P \leftrightarrow Q$ также эквивалентно $(P \rightarrow Q) \wedge (\neg P \rightarrow \neg Q)$.

Таблица 1.13. Таблица истинности формулы $P \leftrightarrow Q$

P	Q	$P \leftrightarrow Q$
F	F	T
F	T	F
T	F	F
T	T	T

Поскольку $Q \rightarrow P$ можно записать как « P , если Q », а $P \rightarrow Q$ можно записать как « P , только если Q », $P \leftrightarrow Q$ означает « P , если Q и P , только если Q », и утверждение часто пишут в виде «*P тогда и только тогда, когда Q*». Фраза *тогда и только тогда* (или ее эквивалент *если и только если*) встречается в математике так часто, что для нее есть общепринятое англоязычное сокращение *iff* (на русском языке – т.т.т.). Таким образом, $P \leftrightarrow Q$ часто пишут в виде «*P т.т.т. Q*» или «*P iff Q*». Другое аналогичное утверждение для $P \leftrightarrow Q$ звучит так: «*P является необходимым и достаточным условием для Q*».

Пример 1.5.4. Запишите логические формы следующих утверждений:

1. Игру отменят, если идет дождь или снег.
2. Наличие не менее десяти человек является необходимым и достаточным условием для чтения лекции.
3. Если Джон пошел в магазин, значит, у нас есть яйца, а если не пошел, то у нас их нет.

Решения

1. Пусть C означает «Игру отменят», R – «Идет дождь», а S – «Идет снег». Тогда утверждение можно представить формулой $C \leftrightarrow (R \vee S)$.
2. Пусть T означает «Присутствуют как минимум десять человек», а L – «Будет прочитана лекция». Тогда утверждение означает $T \leftrightarrow L$.

3. Пусть S означает «Джон пошел в магазин», а E – «У нас есть яйца». Тогда дословный перевод данного утверждения будет иметь вид $(S \rightarrow E) \wedge (\neg S \rightarrow \neg E)$. Это эквивалентно $S \leftrightarrow E$.

Одна из причин, по которой так легко спутать условное утверждение с обратным ему, состоит в том, что в повседневной речи мы иногда используем условное утверждение, когда мысль, которую мы хотим передать, на самом деле является биусловной. Например, вы вряд ли скажете: «Лекция будет прочитана, если придут не менее десяти человек», если припомните случай, когда было меньше десяти человек, а лекцию все равно прочитали. В конце концов, зачем вообще упоминать число десять, если это не минимальное количество? Следовательно, в утверждении фактически говорится, что лекция будет прочитана *тогда и только тогда*, когда на ней будет не менее десяти человек. В качестве другого примера предположим, что родители говорят ребенку: «Если ты не съешь свой обед, ты не получишь никакого десерта». Ребенок, безусловно, ожидает, что если он все-таки съест свой обед, то гарантировано получит десерт, хотя родители говорили не так буквально. Другими словами, ребенок интерпретирует утверждение как означающее: «Съесть свой обед – *необходимое и достаточное условие для получения десерта*».

Такое стирание различия между формами «если – то» и «тогда и только тогда» недопустимо в математике. Математики всегда используют такие фразы, как «тогда и только тогда» или «необходимое и достаточное условие», когда они хотят выразить биусловное утверждение. Никогда не следует интерпретировать утверждение «если – то» в математике как биусловное утверждение, присущее повседневной речи.

УПРАЖНЕНИЯ

- *1. Запишите логические формы следующих утверждений:
- Если этот газ имеет неприятный запах или не является взрывоопасным, то это не водород.
 - Для Джорджа наличие высокой температуры и головной боли является достаточным условием, чтобы пойти к врачу.
 - Наличие и жара, и головной боли – достаточное условие для того, чтобы Джордж пошел к врачу.
 - Если $x \neq 2$, то необходимое условие для того, чтобы число x было простым, – это нечетность x .
2. Запишите логические формы следующих утверждений:
- Мэри продаст свой дом, только если она сможет получить хорошую цену и найти хорошую квартиру.
 - Наличие хорошей кредитной истории и адекватного первоначального взноса является необходимым условием для получения ипотеки.
 - Джон будет прогуливать школу, пока его не исключат. (Подсказка: сначала попробуйте перефразировать утверждение, используя «если – то» вместо «пока».)
 - Если число x делится на 4 или 6, то оно не простое.

3. Запишите логическую форму следующего утверждения:
- Если идет дождь, то ветрено и солнце не светит. Теперь запишите следующие утверждения. Кроме того, для каждого утверждения определите, эквивалентно ли оно либо утверждению (а), либо его контраверсии.
 - Ветрено и не солнечно, только если идет дождь.
 - Дождь является достаточным условием для ветра и отсутствия солнечного света.
 - Дождь является необходимым условием для ветра и отсутствия солнечного света.
 - Дождь не идет, если светит солнце или нет ветра.
 - Ветер и отсутствие солнечного света являются необходимым условием дождя.
 - Либо ветрено, только если идет дождь, либо не солнечно, только если идет дождь.
- *4. Используйте таблицы истинности, чтобы определить, верны ли следующие рассуждения:
- Вырастут либо продажи, либо расходы. Если продажи пойдут вверх, начальник будет доволен. Если расходы увеличатся, начальник будет недоволен. Таким образом, продажи и расходы не увеличатся одновременно.
 - Если налоги, и уровень безработицы вырастут, наступит рецессия. Если ВВП вырастет, то рецессии не будет. ВВП и налоги растут. Поэтому уровень безработицы не растет.
 - Предупреждающая лампа загорится тогда и только тогда, когда давление будет слишком высоким и предохранительный клапан засорен. Предохранительный клапан не засорен. Следовательно, сигнальная лампа загорится тогда и только тогда, когда давление будет слишком высоким.
5. Используйте таблицы истинности, чтобы определить, верны ли следующие рассуждения:
- Если Джонс будет признан виновным, он попадет в тюрьму. Джонс будет признан виновным, только если Смит даст против него показания. Следовательно, Джонс не попадет в тюрьму, если Смит не даст показаний против него.
 - Либо демократы, либо республиканцы будут иметь большинство в сенате, но не те и другие вместе. Наличие демократического большинства – необходимое условие для принятия законопроекта. Следовательно, если республиканцы имеют большинство в сенате, законопроект не будет принят.
6. (а) Покажите, что $P \leftrightarrow Q$ эквивалентно $(P \wedge Q) \vee (\neg P \wedge \neg Q)$.
 (б) Покажите, что $(P \rightarrow Q) \vee (P \rightarrow R)$ эквивалентно $P - (Q \vee R)$.
- *7. (а) Докажите, что $(P \rightarrow R) \wedge (Q \rightarrow R)$ эквивалентно $P \rightarrow (Q \vee R)$.
 (б) Сформулируйте и проверьте аналогичную эквивалентность с использованием $(P \rightarrow R) \vee (Q \rightarrow R)$.

8. (a) Покажите, что $(P \rightarrow Q) \wedge (Q \rightarrow R)$ эквивалентно $(P \rightarrow R) \wedge [(P \leftrightarrow Q) \vee (R \leftrightarrow Q)]$.
(b) Покажите, что $(P \rightarrow Q) \vee (Q \rightarrow R)$ является тавтологией.
- *9. Найдите формулу, включающую только связки \neg и \rightarrow , которая эквивалентна $P \wedge Q$.
10. Найдите формулу, включающую только связки \neg и \rightarrow , которая эквивалентна $P \leftrightarrow Q$.
11. (a) Покажите, что $(P \vee Q) \leftrightarrow Q$ эквивалентно $P \rightarrow Q$.
(b) Покажите, что $(P \wedge Q) \leftrightarrow Q$ эквивалентно $Q \rightarrow P$.
12. Какие из следующих формул эквивалентны?
 - (a) $P \rightarrow (Q \rightarrow R)$.
 - (b) $Q \rightarrow (P \rightarrow R)$.
 - (c) $(P \rightarrow Q) \wedge (P \rightarrow R)$.
 - (d) $(P \wedge Q) \rightarrow R$.
 - (e) $P \rightarrow (Q \wedge R)$.

Глава 2

Кванторная логика

2.1. КВАНТОРЫ

Мы показали, что утверждение $P(x)$, содержащее свободную переменную x , может быть истинным для одних значений x и ложным для других. Иногда нам нужно сказать о том, сколько значений x делает $P(x)$ истинным. В частности, нам нередко приходится говорить, что или $P(x)$ истинно для каждого значения x , или оно истинно по крайней мере для одного значения x . Поэтому мы вводим еще два символа, называемых *кванторами*, чтобы иметь возможность выразить эти идеи.

Чтобы сказать, что $P(x)$ истинно для любого значения x в универсуме U , мы будем писать $\forall x P(x)$. Это читается как «Для всех $x P(x)$ ». Перевернутая буква А читается как слово «все». Символ \forall называется *универсальным квантором*, потому что запись $\forall x P(x)$ означает, что $P(x)$ *универсально* истинно. Как мы обсуждали в разделе 1.3, утверждение, что $P(x)$ истинно для любого значения x в универсуме, означает, что множество истинности $P(x)$ будет представлять собой весь универсум U . Следовательно, вы также можете передать смысл записи $\forall x P(x)$ утверждением о том, что множество истинности $P(x)$ равно U .

Мы используем запись $\exists x P(x)$, чтобы сказать, что в универсуме существует по крайней мере одно значение x , для которого $P(x)$ истинно. Это читается как «существует x такое, что $P(x)$ ». Перевернутая Е происходит от слова «существует» (exists) и называется *квантором существования*. Опять же, вы можете интерпретировать это утверждение как утверждение о множестве истинности $P(x)$. Утверждение, что $P(x)$ истинно хотя бы для одного значения x , означает, что в множестве истинности $P(x)$ есть хотя бы один элемент, или, другими словами, множество истинности не равно \emptyset .

Например, в разделе 1.5 мы обсуждали утверждение «если $x > 2$, то $x^2 > 4$ », где x пробегает множество всех действительных чисел, и мы утверждали, что оно верно для всех значений x . Теперь мы можем записать это утверждение символически как $\forall x(x > 2 \rightarrow x^2 > 4)$.

Пример 2.1.1. Что означают следующие формулы? Истинны они или ложны?

1. $\forall x(x^2 > 0)$, где универсумом дискурса является \mathbb{R} , множество всех действительных чисел.

2. $\exists x(x^2 - 2x + 3 = 0)$, снова с универсумом \mathbb{R} .
3. $\exists x(M(x) \wedge B(x))$, где универсум дискурса – это множество всех людей, $M(x)$ означает утверждение « x – мужчина», а $B(x)$ означает « x имеет каштановые волосы».
4. $\forall x(M(x) \rightarrow B(x))$ с тем же универсумом и одинаковыми значениями для $M(x)$ и $B(x)$.
5. $\forall xL(x, y)$, где универсум – это совокупность всех людей, а $L(x, y)$ означает «человеку x нравится y ».

Решения

1. Это означает, что для любого действительного числа x справедливо $x^2 > 0$. Это истинно.
2. Это означает, что существует по крайней мере одно действительное число x , благодаря которому уравнение $x^2 - 2x + 3 = 0$ оказывается истинным. Другими словами, уравнение имеет хотя бы одно действительное решение. Если вы решите уравнение, то обнаружите, что это утверждение неверно; уравнение не имеет действительных решений. (Попробуйте дополнить до полного квадрата или воспользоваться формулой корней квадратного уравнения.)
3. Существует по крайней мере один человек x такой, что x – мужчина и x имеет каштановые волосы. Другими словами, существует как минимум один мужчина с каштановыми волосами. Конечно, это утверждение истинно.
4. Для каждого x , если x – мужчина, то у x каштановые волосы. Другими словами, у всех мужчин каштановые волосы. Если вы не уверены, что формула означает именно это, вернитесь к таблице истинности условной связки. Согласно этой таблице истинности, утверждение $M(x) \rightarrow B(x)$ будет ложным, только если $M(x)$ истинно, а $B(x)$ ложно; то есть x – мужчина, но x не имеет каштановых волос. Таким образом, утверждение, что $M(x) \rightarrow B(x)$ истинно для каждого x , означает, что вышеупомянутой ситуации никогда не бывает, или, другими словами, не бывает мужчин без каштановых волос. Но именно это означает, что у всех мужчин каштановые волосы. Конечно, это ложное утверждение.
5. Каждому x нравится y . Другими словами, всем нравится y . Мы не можем сказать, истина это или ложь, если не знаем, кто такой y .

Обратите внимание, что в пятом утверждении в этом примере нам нужно знать, кем является y , чтобы определить, было ли утверждение истинным или ложным, но не кем является x . В примере говорится, что всем нравится y , и это утверждение касается y , но не x . Это означает, что y – свободная переменная в этом утверждении, а x – связанная.

Точно так же, хотя все другие утверждения содержат букву x , нам не нужно было знать значение x , чтобы определить их истинность, поэтому x во всех случаях является связанной переменной. В общем, даже если x является свободной переменной в некотором операторе $P(x)$, это связанная переменная в операторах $\forall xP(x)$ и $\exists xP(x)$. По этой причине мы говорим, что кванторы связывают переменную. Как и в разделе 1.3, это означает, что переменная,

связанная квантором, всегда может быть заменена новой переменной без изменения смысла утверждения, и часто можно перефразировать утверждение, вообще не упоминая связанную переменную. Например, утверждение $\forall xL(x, y)$ из примера 2.1.1 эквивалентно $\forall wL(w, y)$, потому что оба означают то же самое, что и «всем нравится y ». Такие слова, как «все», «кто-то», «кто угодно» или «что угодно», часто используются для выражения значений утверждений, содержащих кванторы. Если вы переводите разговорное утверждение в символы, эти слова часто подсказывают вам, что потребуется квантор.

Как и в случае с символом \neg , мы следуем соглашению, согласно которому выражения $\forall x$ и $\exists x$ применяются только к утверждениям, которые идут сразу после них. Например, $\forall xP(x) \rightarrow Q(x)$ означает $(\forall xP(x)) \rightarrow Q(x)$, а не $\forall x(P(x) \rightarrow Q(x))$.

Пример 2.1.2. Запишите логические формы следующих утверждений.

1. Кто-то не делал уроки.
2. Все в этом магазине либо по завышенной цене, либо некачественное.
3. Никто не идеален.
4. Сьюзан нравятся все, кто не любит Джо.
5. $A \subseteq B$.
6. $A \cap B \subseteq B \setminus C$.

Решения

1. Слово «кто-то» подсказывает нам, что нам следует использовать квантор существования. В качестве первого шага мы пишем $\exists x(x \text{ не сделал домашнее задание})$. Теперь, если мы обозначим через $H(x)$ утверждение « x сделал домашнее задание», то мы можем переписать исходную фразу как $\exists x \neg H(x)$.
 2. Перефразируем это утверждение: «если товар находится в этом магазине, значит, либо цена на него завышена, либо он некачественный (не важно, по какому критерию)». Таким образом, мы начинаем с записи $\forall x(\text{если } x \text{ находится в этом магазине, то либо цена } x \text{ завышена, либо } x \text{ некачественный})$. Чтобы перевести часть в круглых скобках в символическую форму, пусть $S(x)$ означает « x находится в этом магазине», $O(x)$ означает «цена x завышена» и $P(x)$ означает « x некачественный». Тогда наш окончательный ответ – $\forall x[S(x) \rightarrow (O(x) \vee P(x))]$.
- Обратите внимание, что, как и оператор 4 в примере 2.1.1, это утверждение имеет форму универсального квантора, применяемого к условному утверждению. Эта форма встречается довольно часто, и важно научиться понимать, что она означает и когда ее следует использовать. Мы можем проверить наш ответ на это задание, как и раньше, используя таблицу истинности для условной связки. Единственная ситуация, при которой утверждение $S(x) \rightarrow (O(x) \vee P(x))$ может быть ложным, – это если x находится в этом магазине, но не имеет завышенной цены или плохого качества. Таким образом, заявление, что данное утверждение истинно для всех значений x , означает, что этого никогда не произойдет, и именно это означает, что все товары в этом магазине либо с завышенной ценой, либо некачественные.

3. Это означает $\neg(\text{кто-то идеален})$, или, другими словами, $\neg\exists xP(x)$, где $P(x)$ означает « x идеален».
4. Как и в утверждении 2 в этом примере, мы можем сформулировать утверждение иначе: «Если человеку не нравится Джо, то Сьюзен нравится этот человек (независимо от того, кто это)». Таким образом, мы можем начать с переписывания данного утверждения как $\forall x(\text{если } x \text{ не любит Джо, то Сьюзен нравится } x)$. Пусть $L(x, y)$ означает « x любит y ». В утверждениях, которые говорят о конкретных элементах универсума дискурса, иногда удобно вводить буквы, обозначающие эти элементы. В данном случае мы говорим о Джо и Сьюзен, поэтому пусть j обозначает Джо, а s – Сьюзен. Таким образом, мы можем написать $L(s, x)$ для обозначения «Сьюзен нравится x » и $\neg L(x, j)$ для « x не любит Джо». Подставляя их, мы получаем ответ $\forall x(\neg L(x, j) \rightarrow L(s, x))$. Обратите внимание, что мы снова встретили универсальный квантор, применяемый к условному оператору. Как и прежде, вы можете проверить этот ответ, используя таблицу истинности условной связки.
5. Согласно определению 1.4.5, утверждение, что A является подмножеством B , означает, что все элементы A входят в B . Если вы уловили принцип того, как объединяются универсальные кванторы и условные выражения, вы должны согласиться, что символическая запись будет иметь вид $\forall x(x \in A \rightarrow x \in B)$.
6. Как и в предыдущем утверждении, сначала запишем это как $\forall x(x \in A \cap B \rightarrow x \in B \setminus C)$. Теперь, используя определения пересечения и разности, мы можем развернуть выражение, чтобы получить $\forall x[(x \in A \wedge x \in B) \rightarrow (x \in B \wedge x \notin C)]$.

Хотя до сих пор все наши примеры содержали только один квантор, нет причин, по которым в утверждении не может быть более одного квантора. Например, рассмотрим утверждение «Некоторые студенты женаты». Слово «некоторые» указывает на то, что это утверждение должно быть написано с использованием квантора существования, поэтому мы можем переписать его в форме $\exists x(x \text{ студент}, x \text{ женат})$. Пусть $S(x)$ означает « x – студент». Мы могли бы аналогичным образом выбрать букву для обозначения « x женат», но, возможно, лучшим подходом было бы признать, что «быть женатым» означает быть женатым *на ком-то*. Таким образом, если мы обозначим « x женат на y » как $M(x, y)$, то можем записать « x женат» как $\exists y M(x, y)$. Следовательно, мы можем представить все утверждение формулой $\exists x(S(x) \wedge \exists y M(x, y))$, формулой, содержащей два квантора существования.

В качестве другого примера давайте проанализируем утверждение «Все родители женаты». Начнем с записи $\forall x(\text{если } x \text{ – родитель, то } x \text{ женат})$. Родительство, как и брак, – это отношения между двумя людьми; быть родителем – значит быть *чym-to* родителем. Таким образом, было бы лучше всего представить утверждение « x – родитель» формулой $\exists y P(x, y)$, где $P(x, y)$ означает « x является родителем y ». Если мы снова представим « x женат» формулой $\exists y M(x, y)$, тогда запись исходного утверждения приобретет форму $\forall x(\exists y P(x, y) \rightarrow \exists y M(x, y))$. Хотя здесь нет ошибки, двойное использование переменной y может вызвать путаницу. Пожалуй, имеет смысл заменить

формулу $\exists y M(x, y)$ эквивалентной формулой $\exists z M(x, z)$. (Напомним, что они эквивалентны, потому что связанная переменная в любом утверждении может быть заменена другой без изменения смысла оператора.) Тогда доработанная символьная запись утверждения будет выглядеть следующим образом: $\forall x(\exists y P(x, y) \rightarrow \exists z M(x, z))$.

Распространенная ошибка новичков – пропускать кванторы. Например, у вас может возникнуть соблазн неправильно представить утверждение «Все родители женаты» формулой $\forall x(P(x, y) \rightarrow M(x, z))$, исключив $\exists y$ и $\exists z$. Хороший способ выявить такие ошибки – обратить внимание на свободные и связанные переменные. В неправильной формуле нет кванторов, связывающих переменные y и z , поэтому y и z являются свободными переменными. Но исходное утверждение «Все родители женаты» не является утверждением про y и z , поэтому эти переменные не должны быть свободными в ответе. Это намек на то, что кванторы y и z отсутствуют. Обратите внимание: если мы переведем неправильную формулу $\forall x(P(x, y) \rightarrow M(x, z))$ обратно на разговорный язык, мы получим следующее утверждение относительно y и z : «Каждый, кто является родителем y , женат на z ».

Пример 2.1.3. Запишите логические формы следующих утверждений.

1. У каждого в общежитии есть сосед по комнате, который ему не нравится.
2. Никому не нравятся больные неудачники.
3. Любой, у кого есть друг, болеющий корью, должен быть помещен в карантин.
4. Если у кого-то в общежитии есть друг, заболевший корью, то всех в общежитии следует поместить в карантин.
5. Если $A \subseteq B$, то A и $C \setminus B$ не пересекаются.

Решения

1. Это означает $\forall x$ (если x живет в общежитии, значит, у x есть сосед по комнате, который ему или ей не нравится). Чтобы сказать, что у x есть сосед по комнате, который ему или ей не нравится, мы могли бы написать $\exists y(x \text{ и } y - \text{соседи по комнате, а } x \text{ не любит } y)$. Если мы обозначим через $R(x, y)$ « x и y – соседи по комнате», а $L(x, y)$ – « x любит y », то получим формулу $\exists y(R(x, y) \wedge \neg L(x, y))$. Наконец, если через $D(x)$ мы обозначим « x живет в общежитии», то полная запись исходного утверждения будет выглядеть так: $\forall x[D(x) \rightarrow \exists y(R(x, y) \wedge \neg L(x, y))]$.
2. Это сложный вопрос, потому что фраза «заболевший неудачник» не относится к конкретному «заболевшему неудачнику», она относится ко всем «заболевшим неудачникам». Утверждение означает, что не нравятся все больные неудачники, или, другими словами, $\forall x$ (если x – неудачник, то x никому не нравится). Чтобы сказать, что никому не нравится x , мы пишем $\neg(\text{кому-то нравится } x)$, что означает $\neg \exists y L(y, x)$, где $L(y, x)$ означает « y нравится x ». Если через $S(x)$ мы обозначим « x – неудачник», то все утверждение примет вид $\forall x(S(x) \rightarrow \neg \exists y L(y, x))$.
3. Вы, наверное, уже поняли, что утверждения обычно легче всего переводить с разговорного языка на символьный в несколько этапов, лишь

понемногу за раз. Вот шаги, через которые мы можем пройти для перевода этого утверждения:

a. $\forall x$ (если x есть друг, болеющий корью, x следует поместить в карантин).

b. $\forall x[\exists y(y - \text{друг } x, \text{ и } y \text{ болен корью}) \rightarrow x \text{ следует поместить в карантин}]$.

Теперь, если $F(y, x)$ означает « $y - \text{друг } x$ », $M(y)$ означает « y болеет корью» и $Q(x)$ означает « x следует поместить в карантин», мы получим:

c. $\forall x[\exists y(F(y, x) \wedge M(y)) \rightarrow Q(x)]$.

4. Слово «любой» трудно интерпретировать, потому что в разных утверждениях оно означает разные вещи. В заявлении 3 это означает *всех*, но в данном утверждении – *кого-то*. Вот шаги нашего анализа:

1. $(\text{У кого-то в общежитии есть друг, болеющий корью}) \rightarrow (\text{всех в общежитии следует поместить в карантин})$.

2. $\exists x(x \text{ живет в общежитии, и у } x \text{ есть друг, болеющий корью}) \rightarrow \exists x(\text{если } z \text{ живет в общежитии, } z \text{ следует поместить в карантин})$.

Используя те же сокращения, что и в последнем утверждении, и обозначив через $D(x)$ « x живет в общежитии», мы получаем следующую формулу:

3. $\exists x[D(x) \wedge \exists y(F(y, x) \wedge M(y))] \rightarrow \forall z(D(z) \rightarrow Q(z))$.

5. Ясно, что ответ будет иметь форму условного утверждения: $(A \subseteq B) \rightarrow (A \text{ и } C \setminus B \text{ не пересекаются})$. Мы уже использовали символическую запись $A \subseteq B$ в примере 2.1.2. Утверждение, что A и $C \setminus B$ не пересекаются, означает, что у них нет общих элементов, или, другими словами, $\neg \exists x(x \in A \wedge x \in C \setminus B)$. Объединяя записи и подставляя определение $C \setminus B$, мы получаем $\forall x(x \in A \rightarrow x \in B) \rightarrow \neg \exists x(x \in A \wedge x \in C \wedge x \notin B)$.

Когда утверждение содержит более одного квантора, иногда трудно понять, что оно означает и является ли оно истинным или ложным. В этом случае лучше анализировать кванторы один за другим по порядку. Например, рассмотрим утверждение $\forall x \exists y(x + y = 5)$, где универсум дискурса – это множество всех действительных чисел. Рассматривая сначала только первый квантор $\forall x$, мы видим, что утверждение $\exists y(x + y = 5)$ истинно для каждого действительного числа x . Позже мы можем побеспокоиться о том, что означает $\exists y(x + y = 5)$; но думать о двух кванторах одновременно – это слишком запутанно.

Если мы хотим выяснить, истинно ли утверждение $\exists y(x + y = 5)$ для каждого значения x , можно попробовать несколько значений x . Например, предположим, что $x = 2$. Определим, истинно ли утверждение $\exists y(2 + y = 5)$. Пришло время подумать о следующем кванторе, $\exists y$. Это утверждение говорит, что существует по крайней мере одно значение y , для которого справедливо уравнение $2 + y = 5$. Другими словами, уравнение $2 + y = 5$ имеет хотя бы одно решение. Конечно, это истина, потому что уравнение имеет решение $y = 5 - 2 = 3$. Следовательно, утверждение $\exists y(2 + y = 5)$ тоже истинно.

Давайте попробуем еще одно значение x . Если $x = 7$, то нас интересует утверждение $\exists y(7 + y = 5)$, в котором говорится, что уравнение $7 + y = 5$ имеет

по крайней мере одно решение. И снова это истина, поскольку есть решение $y = 5 - 7 = -2$. Фактически вы, вероятно, уже поняли, что независимо от того, какое значение мы подставляем вместо x , уравнение $x + y = 5$ всегда будет иметь решение $y = 5 - x$, поэтому утверждение $\exists y(x + y = 5)$ будет истинным. Следовательно, исходное утверждение $\forall x \exists y(x + y = 5)$ истинно.

С другой стороны, утверждение $\exists y \forall x(x + y = 5)$ означает совсем другое – что существует по крайней мере одно значение y , для которого истинно утверждение $\forall x(x + y = 5)$. Можем ли мы найти такое значение y ? Попробуем, например, значение $y = 4$. Мы должны определить, истинно ли утверждение $\forall x(x + 4 = 5)$. В этом утверждении говорится, что независимо от того, какое значение мы подставляем вместо x , равенство $x + 4 = 5$ остается справедливым, и это явно неверно. Фактически в этом уравнении не работает никакое значение x , кроме $x = 1$. Следовательно, утверждение $\forall x(x + 4 = 5)$ ложно.

Мы убедились, что при $y = 4$ выражение $\forall x(x + y = 5)$ ложно, но, возможно, подойдет какое-то другое значение y ? Напомню, мы пытаемся определить, существует ли хотя бы одно подходящее значение y . Давайте попробуем еще раз, допустим $y = 9$. Отсюда вытекает утверждение $\forall x(x + 9 = 5)$, в котором говорится, что независимо от значения x справедливо уравнение $x + 9 = 5$. И снова это явно не так, поскольку для этого уравнения подходит только $x = -4$. Фактически к настоящему моменту вам должно быть ясно, что независимо от того, какое значение мы подставляем для y , уравнение $x + y = 5$ будет истинным только при одном значении x , а именно $x = 5 - y$, поэтому утверждение $\forall x(x + y = 5)$ будет ложным. Таким образом, *не существует* значений y , для которых $\forall x(x + y = 5)$ истинно, поэтому утверждение $\exists y \forall x(x + y = 5)$ ложно.

Обратите внимание: мы обнаружили, что утверждение $\forall x \exists y(x + y = 5)$ истинно, но $\exists y \forall x(x + y = 5)$ ложно. Очевидно, порядок кванторов имеет значение! Что отвечает за эту разницу? Первое утверждение говорит, что для каждого действительного числа x существует действительное число y такое, что $x + y = 5$. Например, когда мы попробовали $x = 2$, то обнаружили, что уравнение $x + y = 5$ становится истинным при $y = 3$, а при $x = 7$ подходит $y = -2$. Обратите внимание, что для разных значений x нам пришлось использовать разные значения y , чтобы уравнение получилось истинным. Вы можете толковать это как утверждение, что для каждого действительного числа x существует соответствующее действительное число y такое, что $x + y = 5$. С другой стороны, когда мы анализировали утверждение $\exists y \forall x(x + y = 5)$, мы искали единственное значение y , которое делало уравнение $x + y = 5$ истинным для всех значений x , и это оказалось невозможным. Для каждого значения x существует соответствующее значение y , которое делает уравнение истинным, но ни одно значение y не подходит для каждого x .

В качестве другого примера рассмотрим утверждение $\forall x \exists y L(x, y)$, где универсум дискурса – это совокупность всех людей, а $L(x, y)$ означает « x нравится y ». Это утверждение означает, что для каждого человека x истинно утверждение $\exists y L(x, y)$. Давайте переформулируем это утверждение как « x нравится кто-то», то есть исходное утверждение означает, что каждому x кто-то нравится. Другими словами, всем кто-то да нравится. С другой стороны, $\exists y \forall x L(x, y)$ означает, что существует некоторый человек y такой, что утверж-

дение $\forall xL(x, y)$ истинно. Как мы видели в примере 2.1.1, это утверждение означает «всем нравится y », поэтому $\exists y\forall xL(x, y)$ означает, что существует некоторый человек y , такой, что он нравится всем подряд. Эти утверждения не означают одно и то же. Вполне возможно, что для каждого человека найдется тот, кто ему нравится, но нет такого человека, который нравится абсолютно всем.

Пример 2.1.4. Что означают следующие утверждения? Истинны они или ложны? Универсум дискурса в каждом случае – это \mathbb{N} , множество всех натуральных чисел.

1. $\forall x\exists y(x < y)$.
2. $\exists y\forall x(x < y)$.
3. $\exists x\forall y(x < y)$.
4. $\forall y\exists x(x < y)$.
5. $\exists x\exists y(x < y)$.
6. $\forall x\forall y(x < y)$.

Решения

1. Это означает, что для любого натурального числа x истинно утверждение $\exists y(x < y)$. Другими словами, для каждого натурального числа x существует натуральное число больше x . Это верно. Например, $x + 1$ всегда больше x .
2. Это означает, что существует некоторое натуральное число y такое, что утверждение $\forall x(x < y)$ верно. Другими словами, существует такое натуральное число y , что все натуральные числа меньше y . Это ложное утверждение. Независимо от того, какое натуральное число y мы выберем, всегда найдутся натуральные числа больше y .
3. Это означает, что существует натуральное число x такое, что утверждение $\forall y(x < y)$ истинно. У вас может возникнуть соблазн сказать, что это утверждение будет истинным, если $x = 0$, но это не так. Поскольку 0 – наименьшее натуральное число, утверждение $0 < y$ истинно для всех значений y , кроме $y = 0$, но если $y = 0$, то утверждение $0 < y$ ложно, и поэтому $\forall y(0 < y)$ ложно. Аналогичное рассуждение показывает, что утверждение $\forall y(x < y)$ ложно для любого значения x , поэтому $\exists x\forall y(x < y)$ ложно.
4. Это означает, что для любого натурального числа y существует натуральное число меньше y . Это верно для любого натурального числа y , кроме $y = 0$, поскольку не существует натурального числа меньше 0 . Следовательно, это утверждение ложно.
5. Это означает, что существует натуральное число x такое, что $\exists y(x < y)$ истинно. Но, как мы показали в анализе первого утверждения, на самом деле это истинно для любого натурального числа x , значит, по определению истинно как минимум для одного числа. Таким образом, $\exists x\exists y(x < y)$ истинно.
6. Это означает, что для любого натурального числа x верно утверждение $\forall y(x < y)$. Но, как мы видели в анализе третьего утверждения, не существует ни одного значения x , для которого это утверждение истинно. Следовательно, утверждение $\forall x\forall y(x < y)$ ложно.

Упражнения

- *1. Запишите логические формы следующих утверждений.
- Любой, кто простил хотя бы одного человека, является святым.
 - Ни один студент из группы матанализа не умнее всех в группе дискретной математики.
 - Всем нравится Мэри, кроме самой Мэри.
 - Джейн видела полицейского, и Роджер тоже видел полицейского.
 - Джейн видела полицейского, и Роджер тоже видел этого полицейского.
2. Запишите логические формы следующих утверждений.
- У любого, кто купил Rolls Royce за наличные, должен быть богатый дядя.
 - Если кто-то в общежитии заболел корью, то всех, у кого есть друг в общежитии, следует поместить в карантин.
 - Если никто не провалил тест, то каждый, кто получил пятерку, будет обучать того, кто получил тройку.
 - Если кто-то может это сделать, то Джонс сможет.
 - Если Джонс может это сделать, то сможет любой.
3. Запишите логические формы следующих утверждений. Универсум дискурса – \mathbb{R} . Найдите свободные переменные в каждом утверждении.
- Каждое число, которое больше x , больше y .
 - Для каждого числа a уравнение $ax^2 + 4x - 2 = 0$ имеет хотя бы одно решение, если $a > -2$.
 - Все решения неравенства $x^3 - 3x < 3$ меньше 10.
 - Если существует число x такое, что $x^2 + 5x = w$, и существует число y такое, что $4 - y^2 = w$, то w строго находится между -10 и 10 .
- *4. Переведите следующие утверждения на обычный разговорный язык.
- $\forall x[(H(x) \wedge \neg \exists y M(x, y)) \rightarrow U(x)]$, где $H(x)$ означает « x – человек», $M(x, y)$ означает « x женат на y », а $U(x)$ означает « x несчастлив».
 - $\exists z(P(z, x) \wedge S(z, y) \wedge W(y))$, где $P(z, x)$ означает « z является родителем x », $S(z, y)$ означает « z и y – брат и сестра», а $W(y)$ означает « y – женщина».
5. Переведите следующие утверждения на обычный математический язык.
- $\forall x[(P(x) \wedge \neg(x = 2)) \rightarrow O(x)]$, где $P(x)$ означает « x – простое число», а $O(x)$ означает « x нечетное».
 - $\exists x[P(x) \wedge \forall y(P(y) \rightarrow y \leq x)]$, где $P(x)$ означает « x – идеальное число».
6. Переведите следующие утверждения на обычный математический язык. Истинны они или ложны? Универсум дискурса – \mathbb{R} .
- $\neg \exists x(x^2 + 2x + 3 = 0 \wedge x^2 + 2x - 3 = 0)$.
 - $\neg[\exists x(x^2 + 2x + 3 = 0) \wedge \exists x(x^2 + 2x - 3 = 0)]$.
 - $\neg \exists x(x^2 + 2x + 3 = 0) \wedge \neg \exists x(x^2 + 2x - 3 = 0)$.
7. Истинны ли эти утверждения? Универсум дискурса – это совокупность всех людей, а $P(x, y)$ означает « x – родитель y ».

- (a) $\exists x \forall y P(x, y)$.
(b) $\forall x \exists y P(x, y)$.
(c) $\neg \exists x \exists y P(x, y)$.
(d) $\exists x \neg \exists y P(x, y)$.
(e) $\exists x \exists y \neg P(x, y)$.
- *8. Верны ли эти утверждения? Универсум дискурса – это \mathbb{N} .
- (a) $\forall x \exists y (2x - y = 0)$.
(b) $\exists y \forall x (2x - y = 0)$.
(c) $\forall x \exists y (x - 2y = 0)$.
(d) $\forall x (x < 10 \rightarrow \forall y (y < x \rightarrow y < 9))$.
(e) $\exists y \exists z (y + z = 100)$.
(f) $\forall x \exists y (y > x \wedge \exists z (y + z = 100))$.
9. То же, что упражнение 8, но с универсумом дискурса \mathbb{R} .
10. То же, что и упражнение 8, но с но с универсумом дискурса \mathbb{Z} .

2.2. ЭКВИВАЛЕНТНОСТИ, ВКЛЮЧАЮЩИЕ КВАНТОРЫ

Изучая логические связки в главе 1, мы сочли полезным установить эквивалентность между различными формулами. В этом разделе мы покажем, что существует также ряд важных эквивалентностей, связанных с кванторами.

Например, в примере 2.1.2 мы представили утверждение «никто не совершенен» формулой $\neg \exists x P(x)$, где $P(x)$ означает « x совершенен». Но другой способ выразить ту же идею – сказать, что все не могут быть идеальными, или, другими словами, $\forall x \neg P(x)$. Это говорит о том, что эти две формулы эквивалентны, и достаточно простых рассуждений, чтобы показать, что это так. Независимо от того, что означает $P(x)$, формула $\neg \exists x P(x)$ означает, что в универсуме дискурса не существует значения x , для которого $P(x)$ истинно. Но это то же самое, что сказать, что для любого значения x в универсуме $P(x)$ ложно, или, другими словами, $\forall x \neg P(x)$. Следовательно, $\neg \exists x P(x)$ эквивалентно $\forall x \neg P(x)$.

Аналогичные рассуждения показывают, что $\neg \forall x P(x)$ эквивалентно $\exists x \neg P(x)$. Утверждение $\neg \forall x P(x)$ означает, что это не тот случай, когда для всех значений x истинно $P(x)$. Это эквивалентно утверждению, что существует хотя бы одно значение x , для которого $P(x)$ ложно, то есть $\exists x \neg P(x)$. Например, в примере 2.1.2 мы перевели «кто-то не сделал домашнее задание» на язык формул как $\exists x \neg H(x)$, где $H(x)$ означает « x сделал домашнее задание». Эквивалентом ему будет утверждение «не все сделали домашнее задание», которое можно представить формулой $\neg \forall x H(x)$.

Таким образом, мы сформулировали два закона, включающие отрицание и кванторы:

Законы отрицания кванторов

- $\neg \exists x P(x)$ эквивалентно $\forall x \neg P(x)$.
 $\neg \forall x P(x)$ эквивалентно $\exists x \neg P(x)$.

Комбинируя эти законы с законами Де Моргана и другими эквивалентностями, включающими логические связки, мы часто можем переформулировать отрицательное утверждение как эквивалентное, но более легкое для понимания положительное утверждение. Этот очень пригодится, когда мы начнем работать с отрицательными утверждениями в доказательствах.

Пример 2.2.1. Запишите отрицательные формы этих утверждений, а затем переформулируйте результаты как эквивалентные положительные утверждения.

1. $A \subseteq B$.
2. У каждого есть родственник, который ему не нравится.

Решения

1. Мы уже знаем, что $A \subseteq B$ означает $\forall x(x \notin A \vee x \in B)$. Чтобы повторно выразить отрицание этого утверждения как эквивалентное положительное утверждение, мы рассуждаем следующим образом:

$$\neg \forall x(x \in A \rightarrow x \in B)$$

эквивалентно $\exists x \neg(x \in A \rightarrow x \in B)$ (закон отрицания квантора),
 что эквивалентно $\exists x \neg(x \in A \rightarrow x \in B)$ (условный закон),
 что эквивалентно $\exists x(x \in A \wedge x \notin B)$ (закон Де Моргана).

Следовательно, $A \subseteq B$ означает то же, что и $\exists x(x \in A \wedge x \notin B)$. Если вы думаете об этом, значит, это должно иметь смысл. Сказать, что A не является подмножеством B , – значит сказать, что в A есть что-то, чего нет в B .

2. Прежде всего давайте запишем исходное утверждение в символической форме. Вы должны уже обладать достаточными навыками, чтобы удостовериться, что если мы обозначим « x связан с y » как $R(x, y)$ и « x нравится y » как $L(x, y)$, то исходное утверждение будет записано как $\forall x \exists y(R(x, y) \wedge \neg L(x, y))$. Теперь мы записываем его отрицание и пытаемся найти более простое эквивалентное положительное утверждение:

$$\neg \forall x \exists y(R(x, y) \wedge \neg L(x, y))$$

эквивалентно $\exists x \neg \exists y(R(x, y) \wedge \neg L(x, y))$ (закон отрицания квантора),
 что эквивалентно $\exists x \forall y \neg(R(x, y) \wedge \neg L(x, y))$ (закон отрицания квантора),
 что эквивалентно $\exists x \forall y(\neg R(x, y) \vee L(x, y))$ (закон Де Моргана),
 что эквивалентно $\exists x \forall y(\neg R(x, y) \rightarrow L(x, y))$ (условный закон).

Давайте переведем эту последнюю формулу обратно на разговорный язык. Если оставить в стороне первый квантор, формула $\forall y(R(x, y) \rightarrow L(x, y))$ означает, что для каждого y , если x находится родственником y , то x нравится y . Другими словами, x нравятся все его родственники. Прибавив $\exists x$ к началу, мы получим утверждение: «Существует кто-то, кому нравятся все его родственники». Вам следует потратить минуту-другую, чтобы убедиться, что это на самом деле эквивалентно отрицанию исходного утверждения: «У каждого есть родственник, который ему не нравится».

В качестве еще одного примера того, как законы отрицания кванторов помогают нам понять утверждения, рассмотрим утверждение «Все, кто нравится Патрисии, не нравятся Сью». Пусть $L(x, y)$ обозначает « x нравится y », и пусть p обозначает Патрисию, а s – Сью, тогда это утверждение будет представлено формулой $\forall x(L(p, x) \rightarrow \neg L(s, x))$. Теперь мы можем вывести формулу, эквивалентную этой:

$$\forall x(L(p, x) \rightarrow \neg L(s, x))$$

эквивалентно $\forall x(\neg L(p, x) \vee \neg L(s, x))$ (условный закон),

что эквивалентно $\forall x(\neg L(p, x) \wedge L(s, x))$ (закон Де Моргана),

что эквивалентно $\neg \exists x(L(p, x) \wedge L(s, x))$ (закон отрицания квантора).

Переводя последнюю формулу обратно на разговорный язык, мы получаем утверждение: «Нет никого, кто нравился бы одновременно Патрисии и Сью», и это действительно означает то же самое, что и утверждение, с которого мы начали.

В разделе 2.1 мы видели, что изменение порядка двух кванторов иногда может изменить смысл формулы. Однако если кванторы одного типа (оба \forall или оба \exists), оказывается, что порядок всегда можно изменить, не влияя на смысл формулы. Например, рассмотрим утверждение «У кого-то есть учитель, который моложе его». Чтобы записать это символически, мы сначала пишем $\exists x(y \text{ есть учитель младше } x)$. Теперь, чтобы сказать « y x есть учитель моложе x », мы пишем $\exists y(T(y, x) \wedge P(y, x))$, где $T(y, x)$ означает « y – учитель x », а $P(y, x)$ означает « y младше x ». Подставляя эти обозначения в исходное утверждение, получаем формулу $\exists x \exists y(T(y, x) \wedge P(y, x))$.

Что произойдет, если мы поменяем местами кванторы? Другими словами, что означает формула $\exists y \exists x(T(y, x) \wedge P(y, x))$? Вы должны самостоятельно удостовериться в том, что эта формула говорит о существовании человека y такого, что y является учителем кого-то старше x . Другими словами, существует ученик, который старше учителя. Но это утверждение истинно при тех же обстоятельствах, что и исходное утверждение: «существует учитель, который моложе ученика»! Оба означают, что существуют такие люди x и y , что y – учитель x и y моложе x . Фактически это говорит о том, что хорошим способом чтения пары кванторов $\exists y \exists x$ или $\exists x \exists y$ является фраза «существуют объекты x и y такие, что...».

Точно так же два универсальных квантора в строке всегда можно переключить без изменения значения формулы, потому что и $\forall x \forall y$, и $\forall y \forall x$ можно читать как означающие «для всех объектов x и y , ...». Например, рассмотрим формулу $\forall x \forall y(L(x, y) \rightarrow A(x, y))$, где $L(x, y)$ означает « x нравится y », а $A(x, y)$ означает « x восхищается y ». Вы можете трактовать эту формулу так, что «Для всех людей x и y если x нравится y , то x восхищается y ». Другими словами, люди всегда восхищаются теми, кто им нравится. Формула $\forall y \forall x(L(x, y) \rightarrow A(x, y))$ означает в точности то же самое.

Важно понимать, что когда мы говорим «существуют объекты x и y » или «для всех объектов x и y », мы не исключаем возможности того, что x и y являются одним и тем же объектом. Например, формула $\forall x \forall y(L(x, y) \rightarrow A(x, y))$ означает не только то, что человек, которому нравится другой человек, всег-

да восхищается этим человеком, но также и то, что люди, которые любят себя, также восхищаются собой. В качестве другого примера предположим, что мы хотим написать формулу, означающую « x – двоеженец». (Конечно, x будет свободной переменной в этой формуле.) Вы можете подумать, что утверждению соответствует формула $\exists y \exists z (M(x, y) \wedge M(x, z))$, где $M(x, y)$ означает « x женат на y ». Но чтобы сказать, что x – именно двоеженец, вы должны сказать, что есть два *разных* человека, на которых x женат, но ваша формула не говорит, что y и z разные. Правильный ответ: $\exists y \exists z (M(x, y) \wedge M(x, z) \wedge y \neq z)$.

Пример 2.2.2. Запишите логические формы следующих утверждений.

1. Все супружеские пары ссорятся.
2. Всем нравятся как минимум два человека.
3. Джону нравится ровно один человек.

Решения

1. $\forall x \forall y (M(x, y) \rightarrow F(x, y))$, где $M(x, y)$ означает « x и y женаты», а $F(x, y)$ означает « x и y ссорятся друг с другом».
2. $\forall x \exists y \exists z (L(x, y) \wedge L(x, z) \wedge y \neq z)$, где $L(x, y)$ означает « x нравится y ». Обратите внимание, что это утверждение означает, что всем нравятся как минимум два *разных* человека, поэтому было бы неправильно опускать « $y \neq z$ » в конце.
3. Пусть $L(x, y)$ означает « x любит y », а j обозначает Джона. Пошагово переведем исходное утверждение в символьную форму:
 - (a) $\exists x (\text{Джону нравится } x \text{, и Джону не нравится никто, кроме } x)$.
 - (b) $\exists x (L(j, x) \wedge \neg \exists y (\text{Джону нравится } y \text{ и } y \neq x))$.
 - (c) $\exists x (L(j, x) \wedge \neg \exists y (L(j, y) \wedge y \neq x))$.

Обратите внимание, что для третьего утверждения в этом примере мы не можем дать более простой ответ $\exists x L(j, x)$, потому что это означало бы, что Джону нравится *хотя бы один* человек, а не *ровно один* человек. Фраза «ровно один» встречается в математике так часто, что для нее есть специальное обозначение. Для представления в символьной форме утверждения «Существует ровно одно значение x такое, что $P(x)$ истинно» мы напишем $\exists! x P(x)$. Иногда его также читают: «Существует единственный x такой, что $P(x)$ ». Например, третий оператор в примере 2.2.2 можно было бы символически записать как $\exists! x L(j, x)$. Фактически это сокращенная запись формулы, приведенной в примере 2.2.2 как ответ на утверждение 3. Точно так же в целом мы можем рассматривать $\exists! x P(x)$ как сокращение формулы $\exists x (P(x) \wedge \neg \exists y (P(y) \wedge y \neq x))$.

Напомним, что когда мы обсуждали теорию множеств, иногда было полезно записать множество истинности $P(x)$ как $\{x \in U \mid P(x)\}$, а не $\{x \mid P(x)\}$, чтобы было понятно, что такое универсум дискурса. Точно так же вместо записи $\forall x P(x)$, чтобы указать, что $P(x)$ истинно для каждого значения x в некотором универсуме U , мы могли бы написать $\forall x \in U P(x)$. Это читается как «Для всех x в U $P(x)$ ». Точно так же мы можем написать $\exists x \in U P(x)$, чтобы сказать, что существует по крайней мере одно значение x во вселенной U такое, что $P(x)$ истинно. Например, утверждение $\forall x (x \geq 0)$ было бы ложным, если бы универсум был действительными числами, но истинным, если бы это были на-

туральные числа. Можно избежать неоднозначности при понимании этого утверждения, написав либо $\forall x \in \mathbb{R}(x \geq 0)$, либо $\forall x \in \mathbb{N}(x \geq 0)$, чтобы прояснить, что мы имели в виду.

Как и раньше, мы иногда используем эту нотацию не для определения универсума дискурса, а для того, чтобы ограничить внимание подмножеством универсума. Например, если наш универсум состоит из действительных чисел и мы хотим сказать, что некоторое действительное число x имеет квадратный корень, мы можем написать $\exists y(y^2 = x)$. Чтобы сказать, что каждое *положительное* действительное число имеет квадратный корень, мы бы написали $\forall x \in \mathbb{R}^+ \exists y(y^2 = x)$. Мы могли бы сказать, что каждое положительное действительное число имеет отрицательный квадратный корень, написав $\forall x \in \mathbb{R}^+ \exists y \in \mathbb{R}^-(y^2 = x)$. В общем, для любого множества A формула $\forall x \in A P(x)$ означает, что для *каждого* значения x в множестве A $P(x)$ истинно, а $\exists x \in A P(x)$ означает, что существует по крайней мере одно значение x в множестве A такое, что $P(x)$ истинно. Кванторы в этих формулах иногда называют *ограниченными кванторами*, потому что они устанавливают *границы* того, какие значения x должны рассматриваться. Иногда мы можем использовать вариации этой записи, чтобы наложить другие ограничения на количественные переменные. Например, утверждение о том, что каждое положительное действительное число имеет отрицательный квадратный корень, также можно записать как $\forall x > 0 \exists y < 0 (y^2 = x)$.

Формулы, содержащие ограниченные кванторы, также можно рассматривать как сокращенную запись более сложных формул, содержащих только обычные неограниченные кванторы. Запись $\exists x \in A P(x)$ означает, что существует некоторое значение x , которое находится в A и делает $P(x)$ истинным, и эту мысль можно выразить развернутой формулой $\exists x(x \in A \wedge P(x))$. Самостоятельно убедитесь, что $\forall x \in A P(x)$ означает то же самое, что и $\forall x(x \in A \rightarrow P(x))$. Например, рассмотренная нами ранее формула $\forall x \in \mathbb{R}^+ \exists y \in \mathbb{R}^-(y^2 = x)$ означает то же самое, что и $\forall x(x \in \mathbb{R}^+ \rightarrow \exists y \in \mathbb{R}^-(y^2 = x))$, которая, в свою очередь, может быть развернута как $\forall x(x \in \mathbb{R}^+ \rightarrow \exists y(y \in \mathbb{R}^- \wedge y^2 = x))$. По определениям \mathbb{R}^+ и \mathbb{R}^- эквивалентным способом сказать это будет $\forall x(x > 0 \rightarrow \exists y(y < 0 \wedge y^2 = x))$. Вы должны убедиться, что эта формула, как и исходная формула, означает, что каждое положительное действительное число имеет отрицательный квадратный корень. В качестве другого примера обратите внимание, что оператор $A \subseteq B$, который по определению означает $\forall x(x \in A \rightarrow x \in B)$, также может быть записан как $\forall x \in A(x \in B)$.

Интересно отметить, что законы отрицания кванторов работают и для ограниченных кванторов. Фактически мы можем вывести эти законы отрицания ограниченных кванторов из исходных законов, считая ограниченные кванторы сокращениями, как сказано выше. Например:

$$\neg \forall x \in A P(x)$$

эквивалентно $\neg \forall x(x \in A \rightarrow P(x))$ (расширенная запись),

что эквивалентно $\exists x \neg(x \in A \rightarrow P(x))$ (закон отрицания квантора),

что эквивалентно $\exists x \neg(x \notin A \vee P(x))$ (условный закон),

что эквивалентно $\exists x(x \in A \wedge \neg P(x))$ (закон Де Моргана),

что эквивалентно $\exists x \in A \neg P(x)$ (сокращенная запись).

Таким образом, мы показали, что $\neg\forall x \in A P(x)$ эквивалентно $\exists x \in A \neg P(x)$. В упражнении 5 вас попросят доказать другой закон отрицания ограниченного квантора – что $\neg\exists x \in A P(x)$ эквивалентно $\forall x \in A \neg P(x)$.

Совершенно очевидно, что если $A = \emptyset$, то $\exists x \in A P(x)$ будет ложным независимо от того, каково утверждение $P(x)$. В A не может быть ничего такого, что при подстановке x заставляет $P(x)$ становиться истинным, потому что в A вообще ничего нет! Может быть не столь очевидно, следует ли считать $\forall x \in A P(x)$ истинным или ложным, но мы можем найти ответ, используя законы отрицания кванторов:

$$\forall x \in A P(x)$$

эквивалентно $\neg\neg\forall x \in A P(x)$ (закон двойного отрицания),
что эквивалентно $\neg\exists x \in A \neg P(x)$ (закон отрицания квантора).

Теперь если $A = \emptyset$, то эта последняя формула будет истинной, независимо от содержания утверждения $P(x)$, потому что, как мы видели, $\exists x \in A \neg P(x)$ должно быть ложным. Таким образом, $\forall x \in A P(x)$ всегда истинно, если $A = \emptyset$. Математики иногда говорят, что такое утверждение является *пустым* истинным. Другой способ убедиться в этом – переписать оператор $\forall x \in A P(x)$ в эквивалентной форме $\forall x(x \in A \rightarrow P(x))$. Далее, согласно таблице истинности условной связки, это утверждение может быть ложным только тогда, когда существует некоторое значение x , такое что $x \in A$ истинно, а $P(x)$ ложно. Но такого значения x нет просто потому, что нет значения x , для которого истинно $x \in A$.

В качестве применения этого принципа отметим, что пустое множество является подмножеством каждого множества. Чтобы понять, почему, просто перепишите утверждение $A \subseteq B$ в эквивалентной форме $\forall x \in A(x \in B)$. Теперь если $A = \emptyset$, то, как мы только что заметили, это утверждение будет пустым. Таким образом, независимо от того, что представляет собой множество B , $\emptyset \subseteq B$. Другой пример пустого истинного утверждения – «Все единороги фиолетовые». Мы могли бы представить это утверждение формулой $\forall x \in A P(x)$, где A – множество всех единорогов, а $P(x)$ означает « x фиолетовый». Поскольку единорогов не существует, A – пустое множество, следовательно, утверждение истинно. (Обратите внимание, что утверждение «Все единороги зеленые» также истинно, что не противоречит тому факту, что все единороги фиолетовые!)

Возможно, вы уже заметили, что хотя в главе 1 мы всегда могли проверить эквивалентность с использованием логических связок, составляя таблицы истинности, у нас нет такого простого способа проверки эквивалентности с использованием кванторов. До сих пор мы доказывали эквивалентность записей с кванторами, просто глядя на примеры и руководствуясь здравым смыслом. По мере усложнения формул, с которыми мы работаем, этот метод станет ненадежным и трудным в использовании. К счастью, в главе 3 мы изучим более эффективные методы толкования формул, включающих кванторы. Чтобы натренироваться в анализе кванторов, мы разработаем несколько более сложных эквивалентов, используя здравый смысл. Если вы не до конца уверены, что эти эквивалентности верны, вы сможете проверить их более тщательно, когда перейдете к главе 3.

Рассмотрим утверждение: «Все люди светлоглазые и пышноволосые». Если мы примем, что $E(x)$ означает « x светлоглазый», а $T(x)$ – « x пышноволосый», то можем представить это утверждение формулой $\forall x(E(x) \wedge T(x))$. Эквивалентно ли это формуле $\forall xE(x) \wedge \forall xT(x)$? Последняя формула означает: «У всех светлые глаза, а также у всех пышные волосы», и интуитивно смысл тот же, что и в исходном утверждении. Следовательно, формула $\forall x(E(x) \wedge T(x))$ эквивалентна $\forall xE(x) \wedge \forall xT(x)$. Другими словами, можно сказать, что универсальный квантор распределяется по конъюнкции.

Однако данный закон распределения не работает для квантора существования. Рассмотрим формулы $\exists x(E(x) \wedge T(x))$ и $\exists xE(x) \wedge \exists xT(x)$. Первая формула означает, что существует кто-то и со светлыми глазами, и с пышными волосами, а вторая означает, что существует кто-то со светлыми глазами, и независимо от него существует еще кто-то с пышными волосами. Это совсем не одно и то же. Во втором утверждении не обязательно, чтобы человек со светлыми глазами и человек с пышными волосами были одной и той же персоной, но в первом утверждении они совпадают. Другой способ увидеть разницу между двумя утверждениями – проанализировать множества истинности. Пусть A – множество истинности $E(x)$, а B – множество истинности $T(x)$. Иными словами, A – это группа людей со светлыми глазами, а B – это группа людей с пышными волосами. Далее, второе утверждение говорит, что ни A , ни B не являются пустым множеством, но первое говорит, что $A \cap B$ не является пустым множеством, или, другими словами, что A и B не являются дизъюнктными.

В качестве примера применения закона распределения для универсально-го квантора и конъюнкции предположим, что A и B – это множества, и рассмотрим уравнение $A = B$. Мы знаем, что два множества равны, если они имеют полностью одинаковые элементы. Таким образом, равенство $A = B$ означает $\forall x(x \in A \leftrightarrow x \in B)$, что эквивалентно $\forall x[(x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A)]$. Поскольку универсальный квантор распределяется по конъюнкции, это эквивалентно формуле $\forall x(x \in A \rightarrow x \in B) \wedge \forall x(x \in B \rightarrow x \in A)$, и по определению подмножества это означает $A \subseteq B \wedge B \subseteq A$. Таким образом, мы показали, что уравнение $A = B$ также эквивалентно формуле $A \subseteq B \wedge B \subseteq A$.

Итак, мы ввели семь основных логических символов: связки \wedge , \vee , \neg , \rightarrow и \leftrightarrow , а также кванторы \forall и \exists . Замечательный факт заключается в том, что с помощью этих символов можно понять структуру всех математических утверждений и при условии правильного использования этих символов можно проанализировать все математические рассуждения. Чтобы проиллюстрировать всю мощь введенных нами символов, мы завершаем этот раздел записью еще нескольких математических утверждений в логической нотации.

Пример 2.2.3. Запишите логические формы следующих утверждений.

1. Утверждения о натуральных числах. Универсум дискурса – это \mathbb{N} .
 - (a) x – полный квадрат.
 - (b) x делится на y .
 - (c) x – простое число.
 - (d) x – наименьшее положительное число, кратное y и z .

2. Утверждения о действительных числах. Универсум дискурса – \mathbb{R} .
- Единичный элемент для сложения равен 0.
 - Каждое действительное число имеет аддитивное обратное.
 - Отрицательные числа не имеют квадратных корней.
 - Каждое положительное число имеет ровно два квадратных корня.

Решения

- (a) Это означает, что x – квадрат некоторого натурального числа, или, другими словами, $\exists y(x = y^2)$.
 (b) Это означает, что x равно y , умноженному на некоторое натуральное число, или, другими словами, $\exists z(x = yz)$.
 (c) Это означает, что $x > 1$ и x нельзя записать как произведение двух меньших натуральных чисел. В символьной записи: $x > 1 \wedge \neg \exists y \exists z (x = yz \wedge y < x \wedge z < x)$.
 (d) Переведем утверждение в символьную форму в несколько этапов:
 - x положительно, а x кратно как y , так и z , и не существует меньшего положительного числа, кратного как y , так и z .
 - $x > 0 \wedge \exists a(x = ya) \wedge \exists b(x = zb) \wedge \neg \exists w(w > 0 \wedge w < x \wedge (w \text{ делится как на } y, \text{ так и на } z))$.
 - $x > 0 \wedge \exists a(x = ya) \wedge \exists b(x = zb) \wedge \neg \exists w(w > 0 \wedge w < x \wedge \exists c(w = yc) \wedge \exists d(w = zd))$.
- (a) $\forall x(x + 0 = x)$.
 (b) $\forall x \exists y(x + y = 0)$.
 (c) $\forall x(x < 0 \rightarrow \neg \exists y(y^2 = x))$.
 (d) Переведем утверждение в символьную форму в несколько этапов:
 - $\forall x(x > 0 \rightarrow x)$ имеет ровно два квадратных корня).
 - $\forall x(x > 0 \rightarrow \exists y \exists z(y \text{ и } z \text{ – квадратные корни из } x \text{ и } y \neq z, \text{ и ничто другое не является квадратным корнем из } x))$.
 - $\forall x(x > 0 \rightarrow \exists y \exists z(y^2 = x \wedge z^2 = x \wedge y \neq z \wedge \neg \exists w(w^2 = x \wedge w \neq y \wedge w \neq z)))$.

Упражнения

- *1. Обратите эти утверждения, а затем повторно выразите результаты как эквивалентные положительные утверждения (см. пример 2.2.1.)
- У каждого, кто изучает математику, найдется друг, которому нужна помощь с домашним заданием.
 - У каждого есть сосед, которому никто не нравится.
 - $A \cup B \subseteq C \setminus D$.
 - $\exists x \forall y[y > x \rightarrow \exists z(z^2 + 5z = y)]$.
2. Обратите эти утверждения, а затем повторно выразите результаты как эквивалентные положительные утверждения (см. пример 2.2.1).
- В группе первокурсников есть кто-то, у кого нет соседа по комнате.
 - Всем кто-то нравится, но никому не нравятся все.
 - $\forall a \in A \exists b \in B(a \in C \leftrightarrow b \in C)$.
 - $\forall y > 0 \exists x(ax^2 + bx + c = y)$.

3. Истины или ложны следующие утверждения? Универсум дискурса – это \mathbb{N} .
- $\forall x(x < 7 \rightarrow \exists a \exists b \exists c(a^2 + b^2 + c^2 = x))$.
 - $\exists ! x(x^2 + 3 = 4x)$.
 - $\exists ! x(x^2 = 4x + 5)$.
 - $\exists x \exists y(x^2 = 4x + 5 \wedge y^2 = 4y + 5)$.
- *4. Покажите, что второй закон отрицания квантора, который гласит, что $\neg \forall x P(x)$ эквивалентно $\exists x \neg P(x)$, может быть получен из первого, который гласит, что $\neg \exists x P(x)$ эквивалентно $\exists x P(x) \vee \exists x Q(x)$. (Подсказка: используйте закон двойного отрицания.)
5. Покажите, что $\neg \exists x \in A P(x)$ эквивалентно $\forall x \in A \neg P(x)$.
- *6. Покажите, что квантор существования распространяется по дизъюнкции. Другими словами, покажите, что $\exists x(P(x) \vee Q(x))$ эквивалентно $\exists xP(x) \vee \exists xQ(x)$. (Подсказка: используйте факт, обсуждаемый в этом разделе, что универсальный квантор распространяется по конъюнкции.)
7. Покажите, что $\exists x(P(x) \rightarrow Q(x))$ эквивалентно $\forall xP(x) \rightarrow \exists xQ(x)$.
- *8. Покажите, что $(\forall x \in A P(x)) \wedge (\forall x \in B P(x))$ эквивалентно $\forall x \in (A \cup B) P(x)$. (Подсказка: начните с записи значений ограниченных кванторов в терминах неограниченных кванторов.)
9. Эквивалентны ли $\forall x(P(x) \vee Q(x))$ и $\forall xP(x) \vee \forall xQ(x)$? Объясните ответ. (Подсказка: попробуйте присвоить смысловые значения $P(x)$ и $Q(x)$.)
10. (a) Покажите, что $\exists x \in A P(x) \vee \exists x \in B P(x)$ эквивалентно $\exists x \in (A \cup B) P(x)$.
(b) Является ли $\exists x \in A P(x) \wedge \exists x \in B P(x)$ эквивалентом $\exists x \in (A \cap B) P(x)$?
Объясните ответ.
- *11. Покажите, что утверждения $A \subseteq B$ и $A \setminus B = \emptyset$ эквивалентны, записав каждое из них логическими символами и затем показав эквивалентность полученных формул.
12. Покажите, что утверждения $C \subseteq A \cup B$ и $C \setminus A \subseteq B$ эквивалентны, записав каждое из них логическими символами и затем продемонстрировав эквивалентность полученных формул.
13. (a) Покажите, что утверждения $A \subseteq B$ и $A \cup B = B$ эквивалентны, записав каждое из них логическими символами и затем продемонстрировав эквивалентность полученных формул. (Подсказка: вам может пригодиться упражнение 11 из раздела 1.5.)
(b) Покажите, что утверждения $A \subseteq B$ и $A \cap B = A$ эквивалентны.
- *14. Покажите, что утверждения $A \cap B = \emptyset$ и $A \setminus B = A$ эквивалентны.
15. Пусть $T(x, y)$ означает « x – учитель y ». Что означают следующие утверждения? При каких обстоятельствах каждое из них будет истинным? Какие-нибудь из них эквивалентны друг другу?
(a) $\exists ! y T(x, y)$.
(b) $\exists x \exists ! y T(x, y)$.

- (c) $\exists! x \exists y T(x, y)$.
- (d) $\exists y \exists! x T(x, y)$.
- (e) $\exists! x \exists! y T(x, y)$.
- (f) $\exists x \exists y [T(x, y) \wedge \neg \exists u \exists v (T(u, v) \wedge (u \neq x \vee v \neq y))]$.

2.3. ДРУГИЕ ОПЕРАЦИИ С МНОЖЕСТВАМИ

Теперь, когда мы знаем, как работать с кванторами, мы готовы обсудить более сложные темы теории множеств.

Пока что единственный способ, которым вы научились определять множества, кроме перечисления их элементов по одному, – это использовать нотацию проверки принадлежности $\{x \mid P(x)\}$. Иногда эту запись модифицируют, заменяя x перед вертикальной чертой более сложным выражением. Например, предположим, что мы хотим определить S как множество всех полных квадратов. Возможно, самый простой способ описать это множество – сказать, что оно состоит из всех чисел формы n^2 , где n – натуральное число. Это записывается как $S = \{n^2 \mid n \in \mathbb{N}\}$. Обратите внимание, что, используя наше решение для первого утверждения из примера 2.2.3, мы также можем определить это множество, написав $S = \{x \mid \exists n \in \mathbb{N} (x = n^2)\}$. Таким образом, $\{n^2 \mid n \in \mathbb{N}\} = \{x \mid \exists n \in \mathbb{N} (x = n^2)\}$, и, следовательно, $x \in \{n^2 \mid n \in \mathbb{N}\}$ означает то же, что и $\exists n \in \mathbb{N} (x = n^2)$.

Подобные обозначения часто используются, если элементы множества пронумерованы. Например, предположим, что мы хотим сформировать множество, элементами которого являются первые 100 простых чисел. Мы могли бы начать с нумерации простых чисел, назвав их p_1, p_2, p_3, \dots . Другими словами, $p_1 = 2, p_2 = 3, p_3 = 5$ и т. д. Тогда множество, которое мы ищем, можно объявить при помощи записи $P = \{p_1, p_2, p_3, \dots, p_{100}\}$. Другой способ описания этого множества – сказать, что оно состоит из всех чисел p_i , для i элемента множества $I = \{1, 2, 3, \dots, 100\} = \{i \in \mathbb{N} \mid 1 < i < 100\}$. Это можно было бы записать как $P = \{p_i \mid i \in I\}$. Каждый элемент p_i в этом множестве идентифицируется номером $i \in I$, который называется *индексом элемента*. Множество, определенное таким образом, иногда называют *индексированным семейством*, а I – *индексным множеством*.

Хотя индексы для индексированного семейства часто являются числами, это не обязательное условие. Например, предположим, что S – это множество всех студентов в группе. Если мы захотим сформировать множество всех матерей студентов, то можем через m_s обозначить мать любого студента s . Тогда множество всех матерей студентов можно было бы описать как $M = \{m_s \mid s \in S\}$. Это индексированное семейство, в котором индексным множеством является S , множество всех студентов. Каждая мать в множестве идентифицируется по имени студента, который является ее ребенком. Обратите внимание, что мы также можем определить это множество с помощью теста на принадлежность, написав $M = \{m \mid m \text{ – мать какого-то студента}\} = \{m \mid \exists s \in S (m = ms)\}$. В общем случае любое индексированное семейство $A = \{x_i \mid i \in I\}$ также можно определить как $A = \{x \mid \exists i \in I (x = x_i)\}$. Отсюда следует, что утверждение $x \in \{x_i \mid i \in I\}$ означает то же, что и $\exists i \in I (x = x_i)$.

Пример 2.3.1. Запишите логические формы следующих утверждений, используя обозначения соответствующих определений теории множеств.

1. $y \in \{\sqrt[3]{x} \mid x \in \mathbb{Q}\}$.
2. $\{x_i \mid i \in I\} \subseteq A$.
3. $\{n^2 \mid n \in \mathbb{N}\}$ и $\{n^3 \mid n \in \mathbb{N}\}$ не являются дизъюнктными.

Решения

1. $\exists x \in \mathbb{Q}(y = \sqrt[3]{x})$.
2. По определению подмножества мы должны сказать, что каждый элемент из $\{x_i \mid i \in I\}$ также является элементом A , поэтому мы могли бы начать с записи $\forall x(x \in \{x_i \mid i \in I\} \rightarrow x \in A)$. Подставляя уже известное нам значение $x \in \{x_i \mid i \in I\}$, мы получим $\forall x(\exists i \in I(x = x_i) \rightarrow x \in A)$. Но поскольку элементы $\{x_i \mid i \in I\}$ – это просто x_i для всех $i \in I$, возможно, более простым способом сказать, что каждый элемент $\{x_i \mid i \in I\}$ является элементом A , была бы запись $\forall i \in I(x_i \in A)$. Два приведенных нами ответа эквивалентны, но для доказательства этого потребуются методы, которые мы изучим в главе 3.
3. Мы должны сказать, что у этих двух множеств есть общий элемент, поэтому одно из решений – начать с записи $\exists x(x \in \{n^2 \mid n \in \mathbb{N}\} \wedge x \in \{n^3 \mid n \in \mathbb{N}\})$. Однако, как и в последнем утверждении, есть более простой способ. Элемент, общий для двух множеств, должен быть квадратом некоторого натурального числа, а также кубом некоторого (возможно, другого) натурального числа. Таким образом, мы могли бы сказать, что существует такой общий элемент, написав $\exists n \in \mathbb{N} \exists m \in \mathbb{N}(n^2 = m^3)$. Обратите внимание, что было бы неправильно писать $\exists n \in \mathbb{N}(n^2 = n^3)$, потому что это не учитывает возможность того, что два натуральных числа будут разными. Кстати, это утверждение верно, поскольку $64 = 8^2 = 4^3$, поэтому 64 является элементом обоих множеств.

Элементом множества может быть что угодно. Некоторые интересные и полезные идеи возникают, когда мы рассматриваем множество, элементами которого являются другие множества. Например, предположим, что $A = \{1, 2, 3\}$, $B = \{4\}$ и $C = \emptyset$. Нет причин, по которым мы не могли бы сформировать множество $\mathcal{F} = \{A, B, C\}$, состоящее из трех множеств A , B и C . Подставив определения A , B и C , мы могли бы записать определение множества \mathcal{F} иначе: $\mathcal{F} = \{\{1, 2, 3\}, \{4\}, \emptyset\}$. Обратите внимание, что $1 \in A$ и $A \in \mathcal{F}$, но $1 \notin \mathcal{F}$. Дело в том, что \mathcal{F} состоит только из трех элементов, и все они являются множествами, а не числами. Такие множества, как \mathcal{F} , все элементы которых являются множествами, иногда называют *семействами* множеств.

Часто бывает удобно определять семейства множеств как индексированные семейства. Например, предположим, что S снова обозначает множество всех студентов, и для каждого студента C_s обозначает множество курсов, которые он прослушал. Тогда множество всех этих множеств C_s будет индексированным семейством множеств $\mathcal{F} = \{C_s \mid s \in S\}$. Помните, что элементы этого семейства – не курсы, а множества курсов. Если мы обозначим буквой t какую-то конкретную ученицу Тину и если Тина изучала математический

анализ, начертательную геометрию и историю, то $C_t = \{\text{матанализ, геометрия, история}\}$ и $C_t \in \mathcal{F}$, но матанализ $\notin \mathcal{F}$.

Важным примером семейства множеств является *степенное множество* (power set).

Определение 2.3.2. Предположим, что A – множество. Степенное множество множества A , обозначаемое $\mathcal{P}(A)$, – это множество, элементами которого являются все подмножества A . Другими словами,

$$\mathcal{P}(A) = \{x \mid x \subseteq A\}.$$

Например, множество $A = \{7, 12\}$ имеет четыре подмножества: $\emptyset, \{7\}, \{12\}$ и $\{7, 12\}$. Следовательно, $\mathcal{P}(A) = \{\emptyset, \{7\}, \{12\}, \{7, 12\}\}$. А как насчет $\mathcal{P}(\emptyset)$? Хотя \emptyset не имеет элементов, у него есть одно подмножество, а именно \emptyset . Поэтому $\mathcal{P}(\emptyset) = \{\emptyset\}$. Обратите внимание, что, как мы указали в разделе 1.3, $\{\emptyset\}$ не тоже самое, что \emptyset .

Каждый раз, работая с некоторыми подмножествами множества X , полезно помнить, что все эти подмножества X являются элементами $\mathcal{P}(X)$ по определению степенного множества. Например, если мы обозначим через C множество всех курсов, предлагаемых в вашем учебном заведении, тогда каждое из упомянутых ранее множеств C_s является подмножеством C . Таким образом, для каждого студента s справедливо $C_s \in \mathcal{P}(C)$. Это означает, что каждый элемент семейства $\mathcal{F} = \{C_s \mid s \in S\}$ является элементом $\mathcal{P}(C)$, поэтому $\mathcal{F} \subseteq \mathcal{P}(C)$.

Пример 2.3.3. Запишите логические формы следующих утверждений.

1. $x \in \mathcal{P}(A)$.
2. $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
3. $B \in \{\mathcal{P}(A) \mid A \in \mathcal{F}\}$.
4. $x \in \mathcal{P}(A \cap B)$.
5. $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$.

Решение

1. По определению степенного множества элементы $\mathcal{P}(A)$ являются подмножествами A . Таким образом, утверждение $x \in \mathcal{P}(A)$ означает, что $x \subseteq A$, что, как мы уже знаем, можно записать как $\forall y(y \in x \rightarrow y \in A)$.
2. По определению подмножества это означает $\forall x(x \in \mathcal{P}(A) \rightarrow x \in \mathcal{P}(B))$. Теперь, расписывая $x \in \mathcal{P}(A)$ и $x \in \mathcal{P}(B)$, как уже делали выше, мы получаем $\forall x[\forall y(y \in x \rightarrow y \in A) \rightarrow \forall y(y \in x \rightarrow y \in B)]$.
3. Как и раньше, это означает $\exists A \in \mathcal{F}(B = \mathcal{P}(A))$. Далее, выражение $B = \mathcal{P}(A)$ означает, что элементы B являются в точности подмножествами A , или, другими словами, $\forall x(x \in B \leftrightarrow x \subseteq A)$. Подставляя это выражение и расписывая определение подмножества, мы получаем наш окончательный ответ: $\exists A \in \mathcal{F} \forall x(x \in B \leftrightarrow \forall y(y \in x \rightarrow y \in A))$.
4. Как и в первом утверждении, мы начинаем с записи $\forall y(y \in x \rightarrow y \in A \cap B)$. Теперь, подставляя это в определение пересечения, мы получаем $\forall y(y \in x \rightarrow (y \in A \wedge y \in B))$.

5. По определению пересечения это означает $(x \in \mathcal{P}(A)) \wedge (x \in \mathcal{P}(B))$. Теперь, расписывая определение степенного множества, как и раньше, мы получаем $\forall y(y \in x \rightarrow y \in A) \wedge \forall y(y \in x \rightarrow y \in B)$.

Обратите внимание, что для утверждения 5 в этом примере мы сначала записали определение пересечения, а затем использовали определение степенного множества, тогда как в утверждении 4 мы начали с записи определения степенного множества, а затем использовали определение пересечения. По мере того как вы постигаете все больше математических терминов и обозначений, становится все более важным научиться выбирать, какое определение толковать в первую очередь при определении значения сложного математического утверждения. Хорошее практическое правило – всегда начинать с «самого внешнего» символа. В утверждении 4 в примере 2.3.3 символ пересечения встречается внутри обозначения степенного множества, поэтому мы сначала выписали определение степенного множества. В утверждении 5 обозначение степенного множества расположено внутри обозначения пересечения двух множеств, поэтому мы начали с определения пересечения. Аналогичные соображения привели нас к тому, что в утверждении 2 мы использовали сначала определение подмножества, а не степенного множества.

Интересно отметить, что наши ответы на утверждения 4 и 5 в примере 2.3.3 эквивалентны. (Мы попросим вас проверить это в упражнении 11.) Как и в разделе 1.4, это следует из того, что для любых множеств A и B существует эквивалентность $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$. В упражнении 12 мы попросим вас показать, что это уравнение в целом неверно, если мы изменим \cap на \cup .

Обратимся еще раз к семейству множеств $\mathcal{F} = \{C_s \mid s \in S\}$, где S – это множество всех студентов, а для каждого студента s C_s – это множество всех учебных курсов, которые прошел s . Если бы мы захотели знать, какие курсы изучали все студенты, нам пришлось бы найти те элементы, которые являются общими для всех множеств в \mathcal{F} . Множество всех этих общих элементов называется пересечением семейства \mathcal{F} и обозначается $\bigcap \mathcal{F}$. Точно так же объединение семейства \mathcal{F} , обозначаемое как $\bigcup \mathcal{F}$, – это множество, полученное в результате объединения всех элементов всех множеств в \mathcal{F} в одно множество. В этом случае $\bigcup \mathcal{F}$ будет множеством всех курсов, которые прошел любой студент.

Пример 2.3.4. Пусть $\mathcal{F} = \{1, 2, 3, 4\}, \{2, 3, 4, 5\}, \{3, 4, 5, 6\}$. Найдите $\bigcap \mathcal{F}$ и $\bigcup \mathcal{F}$.

Решение

$$\begin{aligned}\bigcap \mathcal{F} &= \{1, 2, 3, 4\} \cap \{2, 3, 4, 5\} \cap \{3, 4, 5, 6\} = [3, 4], \\ \bigcup \mathcal{F} &= \{1, 2, 3, 4\} \cup \{2, 3, 4, 5\} \cup \{3, 4, 5, 6\} = [1, 2, 3, 4, 5, 6].\end{aligned}$$

Хотя эти примеры могут в какой-то мере прояснить, что мы подразумеваем под $\bigcap \mathcal{F}$ и $\bigcup \mathcal{F}$, мы до сих пор не дали точные определения для этих множеств. В целом если \mathcal{F} – любое семейство множеств, то мы определяем множество $\bigcap \mathcal{F}$ как содержащее элементы, которые являются общими для всех множеств в \mathcal{F} . Таким образом, чтобы быть элементом $\bigcap \mathcal{F}$, объект должен

быть элементом каждого множества в \mathcal{F} . С другой стороны, все, что является элементом любого из множеств в \mathcal{F} , должно быть в $\bigcup \mathcal{F}$, поэтому, чтобы войти в $\bigcup \mathcal{F}$, объекту достаточно быть элементом хотя бы одного множества в \mathcal{F} . Таким образом, мы приходим к следующим общим определениям.

Определение 2.3.5. Предположим, что \mathcal{F} – семейство множеств. Тогда *пересечение* и *объединение* \mathcal{F} – это множества $\bigcap \mathcal{F}$ и $\bigcup \mathcal{F}$, определенные следующим образом:

$$\begin{aligned}\bigcap \mathcal{F} &= \{x \mid \forall A \in \mathcal{F} (x \in A)\} = \{x \mid \forall A (A \in \mathcal{F} \rightarrow x \in A)\}. \\ \bigcup \mathcal{F} &= \{x \mid \exists A \in \mathcal{F} (x \in A)\} = \{x \mid \exists A (A \in \mathcal{F} \wedge x \in A)\}.\end{aligned}$$

Некоторые математики считают $\bigcap \mathcal{F}$ неопределенным, если $\mathcal{F} = \emptyset$. Объяснение причины этого дано в упражнении 15. Мы будем использовать нотацию $\bigcap \mathcal{F}$ только тогда, когда $\mathcal{F} \neq \emptyset$.

Обратите внимание, что если A и B – любые два множества и $\mathcal{F} = \{A, B\}$, то $\bigcap \mathcal{F} = A \cap B$ и $\bigcup \mathcal{F} = A \cup B$. Таким образом, определения пересечения и объединения семейства множеств на самом деле являются обобщениями наших прежних определений пересечения и объединения двух множеств.

Пример 2.3.6. Запишите логические формы следующих утверждений.

1. $x \in \bigcap \mathcal{F}$.
2. $\bigcap \mathcal{F} \not\subseteq \bigcup \mathcal{G}$.
3. $x \in \mathcal{P}(\bigcup \mathcal{F})$.
4. $x \in \bigcup \{\mathcal{P}(A) \mid A \in \mathcal{F}\}$.

Решения

1. По определению пересечения семейства множеств это означает $\forall A \in \mathcal{F} (x \in A)$ или, что то же самое, $\forall A (A \in \mathcal{F} \rightarrow x \in A)$.
2. Как мы показали в примере 2.2.1, утверждение, что одно множество не является подмножеством другого, означает, что существует элемент, входящий в первое множество и не входящий во второе. Следовательно, мы начинаем с записи $\exists x (x \in \bigcap \mathcal{F} \wedge x \notin \bigcup \mathcal{G})$. Мы уже расписали, что означает $x \in \bigcap \mathcal{F}$ в решении 1. По определению объединения семейства множеств $x \in \bigcup \mathcal{G}$ означает $\exists A \in \mathcal{G} (x \in A)$, поэтому $x \notin \bigcup \mathcal{G}$ означает $\neg \exists A \in \mathcal{G} (x \in A)$. Согласно законам отрицания кванторов это эквивалентно $\forall A \in \mathcal{G} (x \notin A)$. Подставляя эквивалентные записи, получаем $\exists x [\forall A \in \mathcal{F} (x \in A) \wedge \forall A \in \mathcal{G} (x \notin A)]$.
3. Поскольку символ объединения встречается в нотации степенного множества, мы начинаем с записи его определения. Как и в примере 2.3.3, получаем $x \subseteq \bigcup \mathcal{F}$, или, другими словами, $\forall y (y \in x \rightarrow y \in \bigcup \mathcal{F})$. Теперь воспользуемся определением объединения, чтобы записать $y \in \bigcup \mathcal{F}$ как $\exists A \in \mathcal{F} (y \in A)$. Окончательный ответ – $\forall y (y \in x \rightarrow \exists A \in \mathcal{F} (y \in A))$.
4. На этот раз мы сначала напишем определение объединения. Согласно этому определению, утверждение означает, что x является элементом хотя бы одного из множеств $\mathcal{P}(A)$ для $A \in \mathcal{F}$. Другими словами, $\exists A \in \mathcal{F} (x \in \mathcal{P}(A))$. Подставляя запись утверждения $x \in \mathcal{P}(A)$ из примера 2.3.3, мы получаем $\exists A \in \mathcal{F} \forall y (y \in x \rightarrow y \in A)$.

Запись сложных математических утверждений в виде логических символов, как мы это делали в последнем примере, иногда помогает понять, что означают утверждения и являются ли они истинными или ложными. Например, предположим, что мы снова обозначим через C_s множество всех курсов, которые прошел студент s . Пусть M – множество математических курсов, E – множество лингвистических курсов, и пусть $\mathcal{F} = \{C_s \mid s \in M\}$ и $\mathcal{G} = \{C_s \mid s \in E\}$. Что означает утверждение 2 из примера 2.3.6 с учетом этих определений, и при каких обстоятельствах оно будет верным? Согласно нашему решению для этого примера, утверждение означает $\exists x[\forall A \in \mathcal{F}(x \in A) \wedge \forall A \in \mathcal{G}(x \notin A)]$, или, другими словами, есть что-то, что является элементом каждого множества в \mathcal{F} , но не может быть элементом каждого множества в \mathcal{G} . Принимая во внимание определения \mathcal{F} и \mathcal{G} , которые мы используем, это означает, что существует некоторый курс, который изучали все студенты-математики, но не изучал ни один студент-лингвист. Если, например, все студенты-математики изучали матанализ, но ни один лингвист его не изучал, то утверждение будет верным.

В качестве другого примера предположим, что $\mathcal{F} = \{\{1, 2, 3\}, \{2, 3, 4\}, \{3, 4, 5\}\}$ и $x = \{4, 5, 6\}$. Будет ли утверждение 3 примера 2.3.6 истинным при таком определении? Вы можете узнать это, найдя $\mathcal{P}(\bigcap \mathcal{F})$, а затем проверив, является ли x его элементом, но это займет очень много времени, потому что оказывается, что $\mathcal{P}(\bigcap \mathcal{F})$ имеет 32 элемента. Попробуйте использовать перевод в логические символы, приведенный в нашем решении для этого примера. Согласно этому переводу утверждение означает $\forall y(y \in x \rightarrow \exists A \in \mathcal{F}(y \in A))$; другими словами, каждый элемент x входит по крайней мере в одно множество в \mathcal{F} . Оглядываясь на наши определения \mathcal{F} и x , нетрудно увидеть, что это не так, потому что $6 \in x$, но 6 не содержится ни в одном из множеств семейства \mathcal{F} .

Для объединения или пересечения индексированного семейства множеств иногда используется альтернативное обозначение. Предположим, что $\mathcal{F} = \{A_i \mid i \in I\}$, где каждый элемент A_i является множеством. Тогда $\bigcup \mathcal{F}$ будет множеством всех элементов, общих для всех A_i , для $i \in I$, и это также можно записать как $\bigcap_{i \in I} A_i$. Другими словами,

$$\bigcap \mathcal{F} = \bigcap_{i \in I} A_i = \{x \mid \forall i \in I(x \in A_i)\}.$$

Аналогично, альтернативная запись для $\bigcup \mathcal{F}$ – это $\bigcup_{i \in I} A_i$, следовательно,

$$\bigcup \mathcal{F} = \bigcup_{i \in I} A_i = \{x \mid \exists i \in I(x \in A_i)\}.$$

Возвращаясь к нашему примеру курсов, изучаемых студентами, мы могли бы использовать эту нотацию, чтобы определить множество курсов, проходимых всеми студентами, как $\bigcap_{s \in S} C_s$. Вы можете толковать эту запись как обозначение результата прохождения отбора всех элементов s в S , формирования множества C_s для каждого из них, а затем пересечения всех этих множеств.

Пример 2.3.7. Пусть $I = \{1, 2, 3\}$, и для каждого $i \in I$ пусть $A_i = \{i, i + 1, i + 2, i + 3\}$. Найдите $\bigcap_{i \in I} A_i$ и $\bigcup_{i \in I} A_i$.

Решение

Сначала перечислим элементы множеств A_i для $i \in I$:

$$A_1 = \{1, 2, 3, 4\}, A_2 = \{2, 3, 4, 5\}, A_3 = \{3, 4, 5, 6\};$$

затем

$$\bigcap_{i \in I} A_i = A_1 \cap A_2 \cap A_3 = \{1, 2, 3, 4\} \cap \{2, 3, 4, 5\} \cap \{3, 4, 5, 6\} = \{3, 4\};$$

и аналогично

$$\bigcup_{i \in I} A_i = \{1, 2, 3, 4\} \cup \{2, 3, 4, 5\} \cup \{3, 4, 5, 6\} = \{1, 2, 3, 4, 5, 6\}.$$

Теперь вы можете видеть, что вопрос, заданный в этом примере, полностью идентичен вопросу из примера 2.3.4, но с другими обозначениями.

Пример 2.3.8. В этом примере наш универсум дискурса будет множеством S всех студентов. Пусть $L(x, y)$ означает « x нравится y », а $A(x, y)$ – « x восхищается y ». Для каждого студента s пусть L_s будет множеством всех студентов, которые ему нравятся. Другими словами, $L_s = \{t \in S \mid L(s, t)\}$. Аналогично, пусть $A_s = \{t \in S \mid A(s, t)\}$ – множество всех студентов, которыми восхищаются. Опишите следующие множества:

1. $\bigcap_{s \in S} L_s$.
2. $\bigcup_{s \in S} L_s$.
3. $\bigcup_{s \in S} L_s \setminus \bigcup_{s \in S} A_s$.
4. $\bigcup_{s \in S} (L_s \setminus A_s)$.
5. $(\bigcap_{s \in S} L_s) \cap (\bigcap_{s \in S} A_s)$.
6. $\bigcup_{s \in S} (L_s \cap A_s)$.
7. $\bigcup_{b \in B} L_b$, где $B = \bigcap_{s \in S} A_s$.

Решения

Прежде всего обратите внимание, что в общем случае $t \in L_s$ означает то же самое, что и $L(s, t)$; аналогично $t \in A_s$ означает $A(s, t)$.

1. $\bigcap_{s \in S} L_s = \{t \mid \forall s \in S (t \in L_s)\} = \{t \in S \mid \forall s \in S L(s, t)\}$ = множество всех студентов, которые нравятся всем студентам.
2. $\bigcup_{s \in S} L_s = \{t \mid \exists s \in S (t \in L_s)\} = \{t \in S \mid \exists s \in S L(s, t)\}$ = множество всех студентов, которым нравится хотя бы один студент.
3. Как мы видели в решении 2, $\bigcup_{s \in S} L_s$ = совокупность всех студентов, которые нравятся хотя бы одному студенту. Точно так же $\bigcup_{s \in S} A_s$ = совокупность всех студентов, которыми восхищается хотя бы один студент. Таким образом, $\bigcup_{s \in S} L_s \setminus \bigcup_{s \in S} A_s = \{t \mid t \in \bigcup_{s \in S} L_s \text{ и } t \notin \bigcup_{s \in S} A_s\} = \{t \mid \forall s \in S (L(s, t) \wedge \neg A(s, t))\}$ = множество всех студентов, которым нравится хотя бы один студент, но они не восхищаются никакими другими студентами.
4. $\bigcup_{s \in S} (L_s \setminus A_s) = \{t \mid \exists s \in S (t \in L_s \setminus A_s)\} = \{t \in S \mid \exists s \in S (L(s, t) \wedge \neg A(s, t))\}$ = множество всех студентов t таких, что определенному студенту нравится t , но не вызывает восхищения. Обратите внимание, что это множество отличается от множества в пункте 3. Чтобы студент t оказался в этом множестве, должен быть студент, которому он нравится, но который

не восхищается им, но могут быть и другие студенты, которым он нравится. Чтобы попасть в множество в пункте 3, t не должен вызывать восхищения ни у кого.

5. $(\bigcap_{s \in S} L_s) \cap (\bigcap_{s \in S} A_s) = \{t \mid t \in \bigcap_{s \in S} L_s \text{ и } t \in \bigcap_{s \in S} A_s\} = \{t \mid \forall s \in S (t \in L_s) \wedge \forall s \in S (t \in A_s)\} = \{t \in S \mid \forall s \in S L(s, t) \wedge \forall s \in S A(s, t)\}$ = множество всех студентов, которые нравятся всем студентам, а также вызывают восхищение у всех студентов.
6. $\bigcap_{s \in S} (L_s \cap A_s) = \{t \mid \forall s \in S (t \in L_s \cap A_s)\} = \{t \in S \mid \forall s \in S (L(s, t) \wedge A(s, t))\}$ = множество всех студентов, которые всем нравятся и которыми восхищаются все студенты. Это то же самое, что и множество в пункте 5. Фактически вы можете использовать закон распределения для применения квантора общности и конъюнкции, чтобы показать, что условия принадлежности для двух множеств эквивалентны.
7. $\bigcup_{b \in B} L_b = \{t \mid \exists b \in B (t \in L_b)\} = \{t \in S \mid \exists b (b \in B \wedge L(b, t))\}$. Но B был определен как множество студентов, которыми восхищаются все студенты, поэтому $b \in B$ означает $b \in S \wedge \forall s \in S A(s, b)$. Подставляя, мы получаем $\bigcup_{b \in B} L_b = \{t \in S \mid \exists b (b \in S \wedge \forall s \in S A(s, b) \wedge L(b, t))\}$ = множество всех студентов, которые нравятся какому-то студенту; в свою очередь, этим студентом восхищаются все студенты.

Упражнения

- *1. Запишите логические формы следующих утверждений. Вы можете использовать в своих ответах символы \in , \notin , $=$, \neq , \wedge , \vee , \rightarrow , \leftrightarrow , \forall и \exists , но не \subseteq , $\not\subseteq$, \mathcal{P} , \cap , \cup , \setminus , $\{ \}$ или \neg . (Следовательно, вы должны расписать определения некоторых обозначений теории множеств, а также использовать эквивалентности, чтобы избавиться от любых вхождений \neg .)
 - (a) $\mathcal{F} \subseteq \mathcal{P}(A)$.
 - (b) $A \subseteq \{2n + 1 \mid n \in \mathbb{N}\}$.
 - (c) $\{n^2 + n + 1 \mid n \in \mathbb{N}\} \subseteq \{2n + 1 \mid n \in \mathbb{N}\}$.
 - (d) $\mathcal{P}(\bigcup_{i \in I} A_i) \not\subseteq \bigcup_{i \in I} \mathcal{P}(A_i)$.
2. Запишите логические формы следующих утверждений. Вы можете использовать в своих ответах символы \in , \notin , $=$, \neq , \wedge , \vee , \rightarrow , \leftrightarrow , \forall и \exists , но не \subseteq , $\not\subseteq$, \mathcal{P} , \cap , \cup , \setminus , $\{ \}$ или \neg . (Следовательно, вы должны расписать определения некоторых обозначений теории множеств, а также использовать эквивалентности, чтобы избавиться от любых вхождений \neg .)
 - (a) $x \in \bigcup \mathcal{F} \setminus \bigcup \mathcal{G}$.
 - (b) $\{x \in B \mid x \notin C\} \in \mathcal{P}(A)$.
 - (c) $x \in \bigcap_{i \in I} (A_i \cup B_i)$.
 - (d) $x \in \bigcap_{i \in I} A_i \cup (\bigcap_{i \in I} B_i)$.
3. Мы показали, что $\mathcal{P}(\emptyset) = \{\emptyset\}$ и $\{\emptyset\} = \emptyset$. Что такое $\mathcal{P}(\{\emptyset\})$?
- *4. Предположим, $\mathcal{F} = \{\{\text{красный}, \text{зеленый}, \text{синий}\}, \{\text{оранжевый}, \text{красный}, \text{синий}\}, \{\text{фиолетовый}, \text{красный}, \text{зеленый}, \text{синий}\}\}$. Найдите $\bigcap \mathcal{F}$ и $\bigcup \mathcal{F}$.
5. Предположим, что $\mathcal{F} = \{\{3, 7, 12\}, \{5, 7, 16\}, \{5, 12, 23\}\}$. Найдите $\bigcap \mathcal{F}$ и $\bigcup \mathcal{F}$.

6. Пусть $I = \{2, 3, 4, 5\}$, и для каждого $i \in I$ пусть $A_i = \{i, i + 1, i - 1, 2i\}$.
- Перечислите элементы всех множеств A_i для $i \in I$.
 - Найдите $\bigcap_{i \in I} A_i$ и $\bigcup_{i \in I} A_i$.
7. Пусть $P = \{\text{Иоганн Себастьян Бах, Наполеон Бонапарт, Иоганн Вольфганг фон Гете, Давид Юм, Вольфганг Амадей Моцарт, Исаак Ньютон, Джордж Вашингтон}\}$, и пусть $Y = \{1750, 1751, 1752, \dots, 1759\}$. Для каждого $y \in Y$ пусть $A_y = \{p \in P \mid \text{человек } p \text{ был жив какое-то время в течение года } y\}$. Найдите $\bigcup_{y \in Y} A_y$ и $\bigcap_{y \in Y} A_y$.
- *8. Пусть $I = \{2, 3\}$, и для каждого $i \in I$ пусть $A_i = \{i, 2i\}$ и $B_i = \{i, i + 1\}$.
- Перечислите элементы множеств A_i и B_i для $i \in I$.
 - Найдите $\bigcap_{i \in I} (A_i \cup B_i)$ и $(\bigcap_{i \in I} A_i) \cup (\bigcap_{i \in I} B_i)$. Это одно и то же?
 - В частях (c) и (d) упражнения 2 вы проанализировали утверждения $x \in \bigcap_{i \in I} (A_i \cup B_i)$ и $x \in (\bigcap_{i \in I} A_i) \cup (\bigcap_{i \in I} B_i)$. Какой можно сделать вывод из вашего ответа на предыдущий вопрос (b) о том, эквивалентны ли эти утверждения?
9. (a) Запишите логические формы утверждений $x \in \bigcup_{i \in I} (A_i \setminus B_i)$, $x \in (\bigcup_{i \in I} A_i) \setminus (\bigcup_{i \in I} B_i)$ и $x \in (\bigcup_{i \in I} A_i) \setminus (\bigcap_{i \in I} B_i)$. Как вы думаете, эквивалентны ли все эти утверждения друг другу?
- (b) Пусть I, A_i и B_i определены как в задании 8. Найдите $\bigcup_{i \in I} (A_i \setminus B_i)$, $(\bigcup_{i \in I} A_i) \setminus (\bigcup_{i \in I} B_i)$ и $(\bigcup_{i \in I} A_i) \setminus (\bigcap_{i \in I} B_i)$. А что вы теперь думаете насчет эквивалентности каких-либо утверждений в части (a)?
10. Приведите пример индексного множества I и индексированных семейств множеств $\{A_i \mid i \in I\}$ и $\{B_i \mid i \in I\}$ таких, что $\bigcup_{i \in I} (A_i \cap B_i) \neq (\bigcup_{i \in I} A_i) \cap (\bigcup_{i \in I} B_i)$.
11. Покажите, что для любых множеств A и B справедлива идентичность $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$, показав, что утверждения $x \in \mathcal{P}(A \cap B)$ и $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$ эквивалентны (см. пример 2.3.3).
- *12. Приведите примеры множеств A и B , для которых $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.
13. Проверьте следующие идентичности, записав (с помощью логических символов), что означает, что объект x является элементом каждого множества, а затем используя логические эквивалентности.
- $\bigcup_{i \in I} (A_i \cap B_i) = (\bigcup_{i \in I} A_i) \cup (\bigcup_{i \in I} B_i)$.
 - $(\bigcap \mathcal{F}) \cap (\bigcap \mathcal{G}) = \bigcap (\mathcal{F} \cup \mathcal{G})$.
 - $\bigcap_{i \in I} (A_i \setminus B_i) = (\bigcap_{i \in I} A_i) \setminus (\bigcup_{i \in I} B_i)$.
- *14. Иногда каждое множество в индексированном семействе множеств имеет *два* индекса. В этой задаче мы используем следующие определения: $I = \{1, 2\}$, $J = \{3, 4\}$. Для каждого $i \in I$ и $j \in J$ пусть $A_{i,j} = \{i, j, i + j\}$. Так, например, $A_{2,3} = \{2, 3, 5\}$.
- Для каждого $j \in J$ пусть $B_j = \bigcup_{i \in I} A_{i,j} = A_{1,j} \cup A_{2,j}$. Найдите B_3 и B_4 .
 - Найдите $\bigcap_{j \in J} B_j$. (Обратите внимание, что, заменив B_j его определением, мы могли бы сказать, что $\bigcap_{j \in J} B_j = \bigcap_{j \in J} (\bigcup_{i \in I} A_{i,j})$.)
 - Найдите $\bigcup_{i \in I} (\bigcap_{j \in J} A_{i,j})$ (Подсказка: вы можете сделать это в два шага, соответствующие частям (a) и (b).) Эквивалентны ли $\bigcap_{j \in J} (\bigcup_{i \in I} A_{i,j})$ и $\bigcup_{i \in I} (\bigcap_{j \in J} A_{i,j})$?

- (d) Запишите логические формы утверждений $x \in \bigcap_{j \in J} (\bigcup_{i \in I} A_{i,j})$ и $x \in \bigcup_{i \in I} (\bigcap_{j \in J} A_{i,j})$. Эквивалентны ли они?
15. (a) Покажите, что если $\mathcal{F} = \emptyset$, то утверждение $x \in \bigcup \mathcal{F}$ будет ложным независимо от любого x . Отсюда следует, что $\bigcup \emptyset = \emptyset$.
- (b) Покажите, что если $\mathcal{F} = \emptyset$, то утверждение $x \in \bigcap \mathcal{F}$ будет истинным независимо от любого x . В ситуации, когда нам ясно, что представляет собой универсум дискурса U , мы могли бы сказать, что $\bigcap \emptyset = U$. Однако это грозит неприятными последствиями, так как обозначение $\bigcap \emptyset$ будет означать разные вещи в разных контекстах. Более того, работая с множествами, элементами которых являются множества, математики часто вообще не используют универсум дискурса. (Подробнее об этом см. в следующем упражнении.) По этим причинам некоторые математики считают запись $\bigcap \emptyset$ бессмысленной. Мы избежим этой проблемы в данной книге, используя запись $\bigcap \mathcal{F}$ только в тех случаях, когда можем быть уверены, что $\mathcal{F} \neq \emptyset$.
16. В разделе 2.3 мы говорили о том, что множества сами могут быть элементами множества. При обсуждении множеств, элементами которых являются множества, может показаться наиболее естественным рассматривать универсум дискурса как совокупность всех множеств. Однако, как мы увидим в этой задаче, предположение, что такое множество существует, ведет к противоречиям.
- Предположим, что U было множеством всех множеств. Обратите внимание, что, в частности, U – это множество, из чего следует, что $U \in U$. Это еще не противоречие; хотя большинство множеств не являются элементами самих себя, возможно, некоторые множества являются таковыми. Но это предполагает, что множества в универсуме U можно разделить на две категории: необычные множества, которые, как и само U , являются элементами самих себя, и более типичные множества, которые таковыми не являются. Пусть R будет множеством множеств второй категории. Другими словами, $R = \{A \in U \mid A \notin A\}$. Это означает, что для любого множества A в универсуме U , A будет элементом R тогда и только тогда, когда $A \notin A$. Другими словами, мы имеем $\forall A \in U (A \in R \leftrightarrow A \notin A)$.
- (a) Покажите, что применение этого последнего факта к самому множеству R (другими словами, включение R вместо A) приводит к противоречию. Это противоречие было обнаружено Берtrandом Расселом (1872–1970) в 1901 году и известно как *парадокс Рассела*.
- (b) Поразмыслите еще немного о парадоксе в части (a). Как вы думаете, что это говорит нам о множествах?

Глава 3

Доказательства

3.1. СТРАТЕГИИ ДОКАЗАТЕЛЬСТВА

Математики всегда настроены скептически. В поисках ответов на математические вопросы они используют множество приемов, включая метод проб и ошибок, эксперименты с примерами и догадки, но обычно они не уверены в правильности ответа, если не могут его доказать. Наверняка вы уже видели математические доказательства раньше (несколько примеров было во введении), но вряд ли у вас есть достаточный опыт их написания. В этой главе вы узнаете больше о том, как выстраивать доказательства, чтобы начать разрабатывать их самостоятельно.

Доказательства очень похожи на пазлы. Нет никаких правил для того, как нужно собирать пазл. Единственное правило касается конечного продукта: все детали должны подходить друг к другу, а рисунок должен выглядеть правильно. То же самое и с доказательствами.

Хотя нет правил для сборки пазлов, некоторые методы работают лучше, чем другие. Например, вы никогда не составите пазл, разложив случайные детали в меру своего разумения, а затем вернувшись назад и заполнив пустые места! Но вы ведь также не делаете этого, начиная сверху и заполняя ряды строго по порядку, пока не дойдете до низа. Вы, вероятно, сначала строите границу рисунка, а затем постепенно соединяете вместе другие детали пазла и выясняете, куда они подходят. Иногда вы пытаетесь вставить детали не в те места, понимаете, что они не подходят, и чувствуете, что не движетесь вперед. Но время от времени вы обнаруживаете в приятном озарении, что два больших фрагмента рисунка подходят друг к другу, и чувствуете, что неожиданно добились большого прогресса. По мере того как фрагменты пазла встают на свои места, вырисовывается картина. Вы внезапно понимаете, что собранное вами синее пятно – это озеро или часть неба. Но только когда пазл будет собран, вы сможете увидеть всю картину целиком.

То же можно сказать и о процессе поиска доказательства. И я думаю, следует отметить еще одно сходство. Собрав пазл, не стоит сразу разбирать его, не так ли? Вы, вероятно, оставите его на день или два, чтобы полюбоваться. Вы должны сделать то же самое с доказательством. Вы сами придумали, как собрать детали вместе, и как только все будет готово, стоит этим полюбоваться, не так ли?

В этой главе мы обсудим методы построения доказательств, которые математики используют чаще всего, и объясним, как их использовать, чтобы самому начать разрабатывать доказательства. Понимание этих методов также может помочь вам правильно прочитать и понять доказательства, найденные другими людьми. К сожалению, методы, описанные в данной главе, не дадут вам готовое описание пошаговой процедуры для построения каждого доказательства. В поиске доказательства вы можете сделать несколько неудачных попыток, прежде чем найдете правильный путь, а некоторые доказательства могут потребовать изрядной сообразительности или проницательности. По-степенно вы разовьете свои навыки доказательства и сможете решать все более сложные задачи.

Математики обычно формулируют ответ на математический вопрос в форме *теоремы*, которая гласит, что если определенные предположения, называемые *гипотезами* теоремы, истинны, то некоторый вывод также должен быть истинным. Часто гипотезы и выводы содержат свободные переменные, и в этом случае подразумевается, что эти переменные могут обозначать любые элементы универсума дискурса. Присвоение конкретных значений этим переменным называется экземпляром теоремы, и для того, чтобы теорема была правильной, должен быть случай, когда для каждого экземпляра теоремы, который делает гипотезы истинными, вывод также является истинным. Если существует хотя бы один случай, когда гипотезы истинны, а вывод ложен, то теорема неверна. Такой пример называется *контрпримером* (опровержением) к теореме.

Пример 3.1.1. Рассмотрим следующую теорему:

Теорема. Предположим, что $x > 3$ и $y < 2$. Тогда $x^2 - 2y > 5$.

Эта теорема верна (вы будете доказывать это в упражнении 15 данной главы). Гипотезы теоремы: $x > 3$ и $y < 2$, а вывод: $x^2 - 2y > 5$. В качестве примера теоремы мы можем подставить 5 вместо x и 1 вместо y . Ясно, что при этих значениях переменных гипотезы $x > 3$ и $y < 2$ истинны, поэтому теорема говорит нам, что вывод $x^2 - 2y > 5$ также должен быть истинным. Действительно, подставляя значения x и y , мы обнаруживаем, что $x^2 - 2y = 25 - 2 = 23$ и, конечно, $23 > 5$. Обратите внимание, что это вычисление не является доказательством теоремы. Мы проверили только один пример теоремы, но доказательство должно показать, что *все* примеры верны.

Если отбросить вторую гипотезу, то получится ошибочная теорема:

Ошибкачная теорема. Предположим, что $x > 3$. Тогда $x^2 - 2y > 5$.

Мы можем увидеть, что эта теорема ошибочна, найдя контрпример. Например, предположим, что $x = 4$ и $y = 6$. Тогда единственная оставшаяся гипотеза, $x > 3$, верна, но $x^2 - 2y = 16 - 12 = 4$, поэтому вывод $x^2 - 2y > 5$ неверен.

Если вы найдете хотя бы один контрпример к теореме, то можете быть уверены, что теорема неверна, но единственный способ узнать наверняка, что теорема верна, – это доказать ее. *Доказательство теоремы* – это просто дедуктивный аргумент, предпосылки которого являются гипотезами теоре-

мы, а заключение – выводом теоремы. На протяжении всего доказательства мы держим в голове, что любые свободные переменные в гипотезах и выводы теоремы обозначают некоторые конкретные, но неуказанные элементы универсума дискурса. Другими словами, мы воображаем, что рассуждаем о каком-то примере теоремы, но на самом деле не выбираем конкретный случай; аргументация доказательства должна быть применима ко *всем* случаям. Конечно, аргумент должен быть верным, поэтому мы можем быть уверены, что если гипотезы теоремы верны для любого случая, то вывод будет верным и для данного воображаемого случая.

То, как вы придумаете и запишете доказательство теоремы, будет в основном зависеть от логической формы вывода. Часто это также будет зависеть от логической формы гипотез. Методы доказательства, которые мы обсудим в этой главе, расскажут вам, какие стратегии доказательства с наибольшей вероятностью подойдут для различных форм гипотез и выводов.

Методы доказательства, основанные на логических формах гипотез, обычно предлагают способы сделать выводы из гипотез. Когда вы делаете вывод из гипотез, вы используете предположение, что гипотезы истинны, чтобы обосновать утверждение, что какое-то другое утверждение также истинно. После того как вы показали, что утверждение истинно, вы можете использовать его позже в доказательстве точно так же, как если бы это была гипотеза. Возможно, самое важное правило, которое следует учитывать при составлении таких выводов, заключается в следующем: *никогда ничего не утверждать, пока вы не сможете полностью доказать это*, используя гипотезы или выводы, сделанные на их основе ранее в доказательстве. Ваш девиз должен быть таким: «Я не буду делать никаких заявлений раньше времени». Следование этому правилу предотвратит использование беспочвенных логических обоснований или поспешных выводов и гарантирует, что если гипотезы верны, то и вывод также должен быть верным. И это основная цель любого доказательства: гарантировать, что вывод верен, если гипотезы верны.

Чтобы убедиться, что ваши утверждения адекватно обоснованы, вы должны скептически относиться к каждому заключению в вашем доказательстве. Если вы сомневаетесь в адекватности обоснования, на которое опирается ваше утверждение, значит, оно не адекватно. В конце концов, если ваше собственное рассуждение даже вас не убеждает, как вы можете ожидать, что оно убедит кого-то еще?

Методы доказательства, основанные на логической форме вывода, зачастую несколько отличаются от методов, основанных на формах гипотез. Обычно они предлагают способы преобразования проблемы в эквивалентную, но более простую для решения. Способ решения задачи путем преобразования ее в более простую форму должен быть вам знаком. Например, прибавление одного и того же числа к обеим сторонам уравнения преобразует его в эквивалентное уравнение, которое иногда легче решить, чем исходное. Студенты, изучавшие математический анализ, могут быть знакомы с методами вычисления интегралов, такими как подстановка или интегрирование по частям, которые можно использовать для преобразования сложной задачи интегрирования в более простую.

Доказательства, написанные с использованием этих стратегий преобразования, часто включают шаги, на которых вы в качестве аргумента предполагаете, что какое-то утверждение истинно, без предоставления какого-либо обоснования для этого предположения. Сначала может показаться, что такое рассуждение нарушает правило, согласно которому утверждения всегда должны быть оправданы, но это не так, потому что *предполагать что-либо* – не то же самое, что *утверждать* это. Утверждать что-либо – значит настаивать, что это истинно, и такое утверждение никогда не приемлемо в доказательстве, если оно не может быть подкреплено. Однако цель предположения в доказательстве состоит не в том, чтобы заявлять, что утверждение является истинным, а в том, чтобы позволить вам выяснить, что *было бы* истинным в итоге, *если бы* предположение было истинным. Вы всегда должны помнить, что любой вывод, который вы делаете на основании предположения, может оказаться ложным, если предположение ошибочно. Каждый раз, когда вы приводите утверждение в доказательстве, важно быть уверенными, что вы твердо знаете, утверждение это или предположение.

Следующий пример внесет больше ясности. Допустим, что в ходе доказательства вы решили предположить истинность какого-то утверждения, назовем его P , и используете это утверждение, чтобы сделать вывод, что другое утверждение Q истинно. Было бы неправильно называть это доказательством того, что Q истинно, потому что вы не можете быть уверены, что ваше предположение об истинности P было правильным. Все, что можно сказать на этом этапе, – это лишь то, что если P истинно, то вы можете быть уверены, что Q также истинно. Другими словами, вы знаете, что утверждение $P \rightarrow Q$ верно. Если Q представляет собой вывод доказываемой теоремы, то доказательство в лучшем случае неполное. Но если вы стремились доказать, что $P \rightarrow Q$, то доказательство завершено. Это подводит нас к нашей первой стратегии доказательства.

Чтобы доказать заключение вида $P \rightarrow Q$:

Предположим, что P истинно, а затем докажем Q .

Вот еще одна точка зрения на этот способ доказательства. Предположение, что P истинно, равносильно добавлению P к вашему списку гипотез. Хотя изначально P могло и не быть одной из ваших гипотез, как только вы это предположили, вы можете использовать утверждение P точно так же, как любую другую гипотезу. Доказать Q – значит рассматривать Q как новый вывод и забыть об исходном выводе. Следовательно, этот метод говорит, что если вывод теоремы, которую вы пытаетесь доказать, имеет форму $P \rightarrow Q$, вы можете *преобразовать задачу*, добавив P в свой список гипотез и изменив свой вывод с $P \rightarrow Q$ на Q . Это ставит перед вами новую, возможно, более простую задачу доказательства. Если вы сможете решить новую задачу, то вы покажете, что если P истинно, то Q также истинно, тем самым решив исходную задачу доказательства $P \rightarrow Q$. Способ решения этой новой задачи теперь будет определяться логической формой нового вывода Q (который сам по

себе может быть сложным утверждением), а также, возможно, логической формой новой гипотезы P .

Обратите внимание, что этот метод не говорит вам, как построить полное доказательство, он просто дает вам возможность сделать один шаг, предостав员я новую задачу, которую нужно решить, чтобы завершить доказательство. Доказательства обычно не пишутся сразу, а создаются постепенно, путем последовательного применения нескольких методов. Часто использование этих методов приводит к тому, что вы несколько раз меняете задачу. При обсуждении этого процесса будет полезно найти способ отслеживать результаты последовательности преобразований. Поэтому мы вводим следующую более общую терминологию. Мы будем называть утверждения, которые известны или считаются истинными в какой-то момент в ходе поиска доказательства, *исходными посылками* или *данным* (*givens*), а утверждение, которое еще предстоит доказать на этом этапе, как *цель* (*goal*). Когда вы начинаете искать доказательство, исходные посылки представляют собой просто гипотезы теоремы, которую вы доказываете, но позже к ним могут присоединиться другие утверждения, которые были выведены из гипотез или добавлены как новые предположения в результате некоторого преобразования задачи. Первоначальной целью будет вывод теоремы, но она может быть изменена несколько раз в ходе поиска доказательства.

Чтобы подчеркнуть, что все наши стратегии доказательства применимы не только к исходной задаче доказательства, но также и к результатам любого преобразования задачи, с этого момента при обсуждении стратегии мы будем говорить лишь о текущих посылках и целях, а не о гипотезах и выводах. Например, изложенную ранее стратегию на самом деле следует называть стратегией доказательства *цели* в форме $P \rightarrow Q$, а не вывода в этой форме. Даже если вывод теоремы, которую вы доказываете, не является условным утверждением, трансформировав задачу таким образом, что целью становится условное утверждение, вы можете применить эту стратегию в качестве следующего шага в поиске доказательства.

Пример 3.1.2. Предположим, что a и b – действительные числа. Докажите, что если $0 < a < b$, то $a^2 < b^2$.

Рассуждение

Нам дана гипотеза, что a и b – действительные числа. Наш вывод имеет вид $P \rightarrow Q$, где P – это утверждение $0 < a < b$, а Q – утверждение $a^2 < b^2$. Таким образом, мы начинаем с этих утверждений как исходной посылки и цели:

Посылки	Цель
a и b – действительные числа	$(0 < a < b) \rightarrow (a^2 < b^2)$

Согласно нашей методике мы должны предположить, что $0 < a < b$, и попытаться использовать это предположение, чтобы доказать, что $a^2 < b^2$. Другими словами, мы трансформируем задачу, добавляя $0 < a < b$ в список исходных посылок и делая $a^2 < b^2$ целью доказательства:

Посылки	Цель
a и b – действительные числа	$a^2 < b^2$
$0 < a < b$	

Сравнение неравенств $a < b$ и $a^2 < b^2$ говорит о том, что умножение обеих сторон неравенства $a < b$ на a или b может приблизить нас к нашей цели. Поскольку нам дано, что a и b положительны, нам не придется менять знак неравенства, если мы это сделаем. Умножение $a < b$ на a дает нам $a^2 < ab$, а умножение на b дает $ab < b^2$. Таким образом, $a^2 < ab < b^2$, поэтому $a^2 < b^2$.

Решение

Теорема. Предположим, что a и b – действительные числа. Если $0 < a < b$, то $a^2 < b^2$.

Доказательство. Предположим, что $0 < a < b$. Умножая неравенство $a < b$ на положительное число a , получаем $a^2 < ab$, и аналогичным образом умножая на b , получаем $ab < b^2$. Следовательно, $a^2 < ab < b^2$, значит, $a^2 < b^2$, что и требовалось доказать. Таким образом, если $0 < a < b$, то $a^2 < b^2$.

Как видно из предыдущего примера, рассуждения, которые вы используете, когда ищете доказательство, отличаются от шагов, которые вы записываете, когда пишете окончательную версию доказательства. В частности, хотя мы часто будем говорить об исходных посылках и целях, пытаясь найти доказательства, окончательная версия доказательства, как правило, на них не ссылается. На протяжении всей этой главы, а иногда и в последующих главах, мы будем предварять доказательство рассуждениями, но это только для того, чтобы помочь вам понять, как строятся доказательства. Когда математики записывают доказательства, они обычно просто перечисляют шаги, необходимые для обоснования своих выводов, без объяснения того, как они до этого додумались. Некоторые из этих шагов будут утверждениями, свидетельствующими, что задача была преобразована (обычно в соответствии с некоторой стратегией, основанной на логической форме цели); некоторые шаги будут утверждениями, которые опираются на выводы из исходных посылок (часто с использованием некоторой стратегии доказательства, основанной на логической форме посылок). Однако обычно доказательства не отражают ход мысли математика об этих преобразованиях и выводах. Например, доказательство в примере 3.1.2 начинается с предложения «Предположим, что $0 < a < b$ », свидетельствующего, что задача была преобразована в соответствии с нашей стратегией, а затем продолжается последовательностью выкладок, приводящих к выводу, что $a^2 < b^2$. Чтобы обосновать окончательный вывод в последнем предложении «если $0 < a < b$, то $a^2 < b^2$ », не потребовалось никаких дополнительных объяснений.

Хотя такое отсутствие объяснений иногда затрудняет чтение доказательств, оно разделяет две разные цели: *объяснение ваших мыслительных процессов и обоснование ваших выводов*. Первая цель – это психология; вторая – математика. Основная цель доказательства – обосновать утверждение, что вывод следует из гипотез, и никакое объяснение ваших мыслительных

процессов не может заменить адекватное обоснование этого утверждения. Сведение к минимуму любого упоминания мыслительных процессов в доказательстве помогает сохранить четкость этого различия. Иногда в очень сложное доказательство математик может включить упоминание стратегии, лежащей в основе доказательства, чтобы его было легче читать. Однако обычно читатели не нуждаются в пояснениях. Не волнуйтесь, если вы не сразу поймете стратегию, лежащую в основе доказательства, которое вы читаете. Просто пройдите доказательство шаг за шагом, и стратегия в конечном итоге станет понятной. Если нет, перечитайте доказательство еще раз.

Чтобы сохранить четкое различие между доказательством и стратегией, лежащей в основе доказательства, в дальнейшем, формулируя стратегию доказательства, мы будем часто описывать как предварительные рассуждения, которые пригодятся при составлении доказательства, так и форму, которую вы можете использовать в окончательной версии доказательства. Например, вот повторное изложение стратегии доказательства, которое мы обсуждали ранее, в том виде, который мы будем использовать для представления стратегий доказательства с этого момента.

Чтобы доказать цель вида $P \rightarrow Q$:

Предположим, что P истинно, а затем докажем Q .

Стратегия доказательства

Перед использованием стратегии:

<i>Посылки</i>	<i>Цель</i>
–	$P \rightarrow Q$
–	

После использования стратегии:

<i>Посылки</i>	<i>Цель</i>
–	
–	Q
P	

Форма окончательного доказательства

Предположим, что P .

[Здесь приводим доказательство Q .]

Следовательно, $P \rightarrow Q$.

Обратите внимание, что предложенная здесь форма окончательного доказательства говорит вам, как выглядят начало и конец доказательства, но в середине нужно будет добавить свои шаги. Список исходных посылок и целей под заголовком «После использования стратегии» сообщает вам, что известно или можно предположить и что необходимо доказать, чтобы заполнить этот пробел в доказательстве. Многие из наших стратегий доказательства сообщают вам, как сформулировать начало или конец доказательства, оставляя пробел, который необходимо заполнить дальнейшими рассуждениями.

Существует второй метод, который иногда используется для доказательства целей вида $P \rightarrow Q$. Поскольку любое условное утверждение $P \rightarrow Q$ эквивалентно своему контрапозитиву $\neg Q \rightarrow \neg P$, вы можете доказать $P \rightarrow Q$, доказав $\neg Q \rightarrow \neg P$, используя стратегию, показанную ранее. Другими словами:

Чтобы доказать цель вида $P \rightarrow Q$:

Предположим, что Q ложно, и докажем, что P ложно.

Стратегия доказательства

Перед использованием стратегии:

<i>Посылки</i>	<i>Цель</i>
—	$P \rightarrow Q$
—	

После использования стратегии:

<i>Посылки</i>	<i>Цель</i>
—	$\neg P$
—	
$\neg Q$	

Форма окончательного доказательства

Предположим, что Q ложно.

[Здесь приводим доказательство $\neg P$.]

Следовательно, $P \rightarrow Q$.

Пример 3.1.3. Предположим, что a , b и c – действительные числа и $a > b$. Докажите, что если $ac \leq bc$, то $c \leq 0$.

Стратегия доказательства

<i>Посылки</i>	<i>Цель</i>
a, b и c – действительные числа	$(ac \leq bc) \rightarrow (c \leq 0)$
$a > b$	

Контрапозитив цели имеет вид $\neg(c \leq 0) \rightarrow \neg(ac \leq bc)$, или, другими словами $(c > 0) \rightarrow (ac > bc)$, поэтому мы можем доказать это, добавив $c > 0$ к исходным посылкам и сделав $ac > bc$ нашей новой целью:

<i>Посылки</i>	<i>Цель</i>
a, b и c – действительные числа	$ac > bc$
$a > b$	
$c > 0$	

Теперь мы можем написать первое и последнее предложения доказательства. Согласно стратегии, окончательное доказательство должно иметь следующий вид:

Предположим, что $c > 0$.

[Здесь приводим доказательство $ac > bc$.]

Следовательно, если $ac < bc$, то $c < 0$.

Используя новую посылку $c > 0$, мы видим, что цель $ac > bc$ немедленно следует из посылки $a > b$ путем умножения обеих частей на положительное число c . Добавление этого шага между первым и последним предложениями образует полное доказательство.

Решение

Теорема. Предположим, что a , b и c – действительные числа и $a > b$. Если $ac < bc$, то $c < 0$.

Доказательство. Докажем контрапозитив. Предположим, что $c > 0$. Тогда мы можем умножить обе части исходного неравенства $a > b$ на c и заключить, что $ac > bc$. Следовательно, если $ac \leq bc$, то $c \leq 0$.

Обратите внимание, что, хотя мы свободно использовали символы логики в ходе рассуждений, мы не использовали их в окончательной записи доказательства. Хотя было бы неплохо использовать логические символы в доказательстве, математики обычно стараются избегать этого. Использование обозначений и правил логики может быть очень полезным, когда вы выясняете стратегию доказательства, но в финальной версии вы должны стараться как можно больше придерживаться обычного языка.

Вам может быть интересно, откуда мы узнали в примере 3.1.3, что для доказательства цели вида $P \rightarrow Q$ нам следует использовать второй метод, а не первый. Ответ прост: мы попробовали оба метода, и второй сработал. Когда существует более одной стратегии для доказательства цели определенного вида, вам, возможно, придется попробовать несколько разных стратегий, прежде чем вы найдете ту, которая работает. Со временем вы научитесь угадывать, какая стратегия с наибольшей вероятностью сработает для конкретного доказательства.

Обратите внимание, что в каждом из приведенных нами примеров наша стратегия заключалась в изменении наших посылок и цели – это попытка облегчить задачу. Начало и конец доказательства, которые были предоставлены нами в формулировке метода, служат для того, чтобы рассказать читателю о том, что эти изменения были внесены, и о том, как решение этой пересмотренной версии решает исходную задачу. Остальная часть доказательства содержит решение этой упрощенной исправленной задачи.

Большинство других методов доказательства в этой главе также предполагают, что вы каким-то образом пересмотрите свои исходные посылки и цель. Эти изменения приводят к новой задаче доказательства, и в каждом случае изменения были разработаны таким образом, чтобы решение новой задачи в сочетании с некоторыми начальными или конечными утверждениями, объясняющими эти изменения, также решало исходную задачу. Это означает, что всякий раз, когда вы используете одну из этих стратегий, вы можете написать одно или два предложения в начале или в конце доказательства,

а затем забыть об исходной задаче и вместо этого работать над новой задачей, что обычно бывает проще. Часто вы сможете найти доказательство, используя методы, описанные в этой главе, чтобы неоднократно пересматривать свои посылки и цель, делая оставшуюся задачу все проще и проще, пока вы не достигнете точки, в которой станет совершенно очевидно, что цель следует из посылок.

Упражнения

- *1. Рассмотрим следующую теорему. (Эта теорема доказана во введении.)

Теорема. Предположим, что n – целое число больше 1 и n не является простым. Тогда $2^n - 1$ не является простым числом.

- (a) Определите гипотезы и вывод теоремы. Верны ли гипотезы при $n = 6$? Что говорит вам в этом случае теорема? Верно ли это?
 - (b) Какой вывод можно сделать из теоремы в случае $n = 15$? Проверьте правильность этого вывода подстановкой.
 - (c) Какой вывод можно сделать из теоремы в случае $n = 11$?
2. Рассмотрим следующую теорему. (Теорема верна, но мы не будем просить вас доказывать ее здесь.)

Теорема. Предположим, что $b^2 > 4ac$. Тогда квадратное уравнение $ax^2 + bx + c = 0$ имеет ровно два действительных решения.

- (a) Определите гипотезы и вывод теоремы.
 - (b) Чтобы привести пример теоремы, вы должны указать значения для a , b и c , но не для x . Почему?
 - (c) Какой вывод можно сделать из теоремы в случае $a = 2$, $b = -5$, $c = 3$? Проверьте правильность этого вывода подстановкой.
 - (d) Какой вывод можно сделать из теоремы в случае $a = 2$, $b = 4$, $c = 3$?
3. Рассмотрим следующую ошибочную теорему.

Ошибкачная теорема. Предположим, что n – натуральное число, большее 2, и n – не простое число. Тогда $2n + 13$ не является простым числом.

Каковы исходные посылки и вывод этой теоремы? Покажите, что теорема неверна, найдя контрпример.

- *4. Завершите следующее альтернативное доказательство теоремы из примера 3.1.2.

Доказательство. Предположим, что $0 < a < b$. Тогда $b - a > 0$.

[Впишите здесь доказательство $b^2 - a^2 > 0$.]

Поскольку $b^2 - a^2 > 0$, то $a^2 < b^2$. Следовательно, если $0 < a < b$, то $a^2 < b^2$.

5. Предположим, что a и b – действительные числа. Докажите, что если $a < b < 0$, то $a^2 > b^2$.

6. Предположим, что a и b – действительные числа. Докажите, что если $0 < a < b$, то $1/b < 1/a$.
7. Предположим, что a – действительное число. Докажите, что если $a^5 > a$, то $a^5 > a$. (Подсказка: один из подходов – начать с заполнения следующего уравнения: $a^5 - a = (a^5 - a) \cdot ?$.)
- *8. Предположим, что $A \setminus B \subseteq C \cap D$ и $x \in A$. Докажите, что если $x \notin D$, то $x \in B$.
9. Предположим, что $A \cap B \subseteq C \setminus D$. Докажите, что если $x \in A$, то если $x \in D$, то $x \notin B$.
- *10. Предположим, что a и b – действительные числа. Докажите, что если $a < b$, то $(a + b)/2 < b$.
11. Предположим, что x – действительное число и $x \neq 0$. Докажите, что если $(\sqrt[3]{x} +)/(x^2 + 6) = 1/x$, то $x \neq 8$.
- *12. Предположим, что a, b, c и d – действительные числа, $0 < a < b$ и $d > 0$. Докажите, что если $ac \geq bd$, то $c > d$.
13. Предположим, что x и y – действительные числа и $3x + 2y \leq 5$. Докажите, что если $x > 1$, то $y < 1$.
14. Предположим, что x и y – действительные числа. Докажите, что если $x^2 + y = -3$ и $2x - y = 2$, то $x = -1$.
- *15. Докажите первую теорему из примера 3.1.1. (Подсказка: вам может быть полезно применить теорему из примера 3.1.2.)
16. Рассмотрим следующую теорему.

Теорема. Предположим, что x – действительное число и $x \neq 4$. Если $(2x - 5)/(x - 4) = 3$, то $x = 7$.

- (a) Что не так в следующем доказательстве теоремы?

Доказательство. Предположим, что $x = 7$. Тогда $(2x - 5)/(x - 4) = (2(7) - 5)/(7 - 4) = 9/3 = 3$. Следовательно, если $(2x - 5)/(x - 4) = 3$, тогда $x = 7$.

- (b) Дайте правильное доказательство теоремы.

17. Рассмотрим следующую ошибочную теорему.

Ошибкачная теорема. Предположим, что x и y – действительные числа и $x \neq 3$. Если $x^2y = 9y$, то $y = 0$.

- (a) Что не так в следующем доказательстве теоремы?

Доказательство. Предположим, что $x^2y = 9y$. Тогда $(x^2 - 9)y = 0$. Поскольку $x/3 = x^2/9$, поэтому $x^2 - 9 = 0$. Следовательно, мы можем разделить обе части уравнения $(x^2 - 9)y = 0$ на $x^2 - 9$, что приводит к выводу, что $y = 0$. Таким образом, если $x^2y = 9y$, то $y = 0$.

- (b) Покажите, что теорема неверна, найдя контрпример.

3.2. ДОКАЗАТЕЛЬСТВА, СВЯЗАННЫЕ С ОТРИЦАНИЯМИ И УСЛОВИЯМИ

Перейдем к доказательствам, в которых цель представлена в форме $\neg P$. Обычно легче доказать положительное утверждение, чем отрицательное, поэтому часто бывает полезно переформулировать цель, прежде чем доказывать ее. Вместо того чтобы пытаться доказать цель, которая говорит о том, что *не должно* быть истиной, попробуйте перефразировать ее как цель, которая говорит о том, что *должно* быть истиной. К счастью, мы уже изучили несколько эквивалентов, которые помогут в этом. Таким образом, мы приходим к первой стратегии доказательства отрицательных утверждений.

Чтобы доказать цель в форме $\neg P$:

Если возможно, повторно выразите цель в какой-либо другой форме, а затем используйте одну из стратегий доказательства для этой новой формы.

Пример 3.2.1. Предположим, что $A \cap C \subseteq B$ и $a \in C$. Докажите, что $a \notin A \setminus B$.

Стратегия доказательства

Посылки	Цель
$A \cap C \subseteq B$	$a \notin A \setminus B$
$a \in C$	

Чтобы доказать цель, мы должны показать, что не существует случая, когда $a \in A$ и $a \notin B$. Поскольку это отрицательная цель, мы пытаемся повторно выразить ее как положительное утверждение:

$a \notin A \setminus B$ эквивалентно ($a \in A \wedge a \notin B$) (определение $A \setminus B$),
что эквивалентно $a \notin A \vee a \in B$ (закон Де Моргана),
что эквивалентно $a \in A \rightarrow a \in B$ (условный закон).

Переписывая цель таким образом, мы получаем:

Посылки	Цель
$A \cap C \subseteq B$	$a \in A \rightarrow a \in B$
$a \in C$	

Теперь докажем цель в этой новой форме, используя первую стратегию из раздела 3.1. Итак, мы добавляем $a \in A$ в наш список исходных посылок и делаем $a \in B$ нашей целью:

Посылки	Цель
$A \cap C \subseteq B$	$a \in B$
$a \in C$	
$a \in A$	

Теперь найти доказательство намного легче: из посылок $a \in A$ и $a \in C$ мы можем заключить, что $a \in A \cap C$, а поскольку $A \cap C \subseteq B$, отсюда следует, что $a \in B$.

Решение

Теорема. Предположим, что $A \cap C \subseteq B$ и $a \in C$. Тогда $a \notin A \setminus B$.

Доказательство. Предположим, что $a \in A$. Тогда поскольку $a \in C$, то $a \in A \cap C$. Но тогда из исходной посылки $A \cap C \subseteq B$ следует, что $a \in B$. Таким образом, не может быть случая, чтобы a было элементом A , но не B , поэтому $a \notin A \setminus B$.

Иногда цель в форме $\neg P$ невозможно переформулировать в положительное утверждение, и поэтому эту стратегию нельзя использовать. В этом случае обычно лучше проводить доказательство от противного. Начните с предположения, что P истинно, и попытайтесь использовать это предположение, чтобы доказать то, что, как вы знаете, ложно. Часто это делается путем доказательства утверждения, которое противоречит одной из исходных посылок. Поскольку вы знаете, что доказанное вами утверждение ложно, то и предположение о том, что P было истинным, должно быть ложным. Единственная оставшаяся возможность состоит в том, что P ложно.

Чтобы доказать цель в форме $\neg P$:

Предположим, что P истинно, и попытаемся прийти к противоречию. Как только вы пришли к противоречию, вы можете сделать вывод, что утверждение P должно быть ложным.

Стратегия доказательства

Перед использованием стратегии:

Посылки	Цель
–	$\neg P$
–	

После использования стратегии:

Посылки	Цель
–	Противоречие
–	
P	

Форма окончательного доказательства

Предположим, что P истинно.

[Здесь добавьте доказательство противоречия.]

Таким образом, P ложно.

Пример 3.2.2. Докажите, что если $x^2 + y = 13$ и $y \neq 4$, то $x \neq 3$.

Стратегия доказательства

Цель – это условное утверждение, поэтому в соответствии с первой стратегией доказательства в разделе 3.1 мы можем рассматривать антецедент как исходную посылку и сделать следствие нашей новой целью:

<i>Посылки</i>	<i>Цель</i>
$x^2 + y = 13$	$x \neq 3$
$y \neq 4$	

Эта стратегия доказательства также подсказывает, какую форму должно принять окончательное доказательство. Согласно стратегии, доказательство должно выглядеть так:

Предположим, что $x^2 + y = 13$ и $y \neq 4$.

[Здесь приводим доказательство $x \neq 3$.]

Таким образом, если $x^2 + y = 13$ и $y \neq 4$, то $x \neq 3$.

Другими словами, первое и последнее предложения окончательного доказательства уже написаны, и задача, которую предстоит решить, – это добавить доказательство $x \neq 3$ между этими двумя предложениями. Список посылок и целей обобщает то, что мы знаем и что нам нужно доказать, чтобы решить эту задачу.

Цель $x \neq 3$ означает $\neg(x = 3)$, но поскольку $x = 3$ не имеет логических связок, ни одна из известных нам эквивалентностей не может быть использована для повторного выражения этой цели в положительной форме. Поэтому мы пробуем доказательство от противного и преобразуем задачу следующим образом:

<i>Посылки</i>	<i>Цель</i>
$x^2 + y = 13$	Противоречие
$y \neq 4$	
$x = 3$	

Опять же, стратегия доказательства, предложившая это преобразование, также говорит нам, как заполнить еще несколько предложений окончательного доказательства. Как мы упоминали выше, эти предложения идут между первым и последним предложениями доказательства, которые были написаны ранее.

Предположим, что $x^2 + y = 13$ и $y \neq 4$.

Предположим, что $x = 3$.

[Здесь приводим доказательство противоречия.]

Следовательно, $x \neq 3$.

Таким образом, если $x^2 + y = 13$ и $y \neq 4$, то $x \neq 3$.

Отступы в этой схеме доказательства не являются частью окончательного доказательства. Мы добавили их здесь, чтобы показать основную структуру доказательства. Первая и последняя строки идут на одном уровне и показы-

вают, что мы доказываем условное утверждение, предполагая антецедент и доказывая следствие. Между этими строками находится доказательство консеквента $x \neq 3$, которое мы выделили отступом относительно первой и последней строк. Это внутреннее доказательство имеет форму доказательства от противного, на что указывают его первая и последняя строки. Между этими строками нам еще нужно добавить доказательство противоречия.

На данный момент у нас нет конкретного утверждения в качестве цели; подойдет любой невозможный вывод. Поэтому мы должны более внимательно присмотреться к исходным посылкам, чтобы увидеть, не противоречат ли одни из них другим. В данном случае первая и третья посылки вместе означают, что $y = 4$, а это противоречит второй посылке.

Решение

Теорема. Если $x^2 + y = 13$ и $y \neq 4$, то $x \neq 3$.

Доказательство. Предположим, что $x^2 + y = 13$ и $y \neq 4$. Предположим также, что $x = 3$. Подставляя это в уравнение $x^2 + y = 13$, мы получаем $9 + y = 13$, значит, $y = 4$. Но это противоречит исходной посылке $y \neq 4$. Следовательно, $x \neq 3$. Таким образом, если $x^2 + y = 13$ и $y \neq 4$, то $x \neq 3$.

Здесь вы можете спросить, почему мы решили в заключении, когда мы достигли противоречия в доказательстве, что $x \neq 3$? В конце концов, второй список исходных посылок в нашей работе содержит три пункта. Почему мы решили, что виновником противоречия была именно третья посылка, $x = 3$? Чтобы ответить на этот вопрос, взгляните на первые посылки и анализ целей для этого примера. Согласно этому анализу, у нас было две посылки, $x^2 + y = 13$ и $y \neq 4$, опираясь на которые, мы должны были прийти к выводу $x \neq 3$. Эти посылки были введены как предположения в первом предложении доказательства. Наше доказательство того, что $x \neq 3$, существует в контексте, в котором эти предположения справедливы, на что указывает отступ в схеме доказательства в наших предварительных рассуждениях. Таким образом, нам нужно было только показать, что $x \neq 3$ в *предположении, что $x^2 + y = 13$ и $y \neq 4$* . Когда мы пришли к противоречию, нам не нужно было выяснять, какое из трех утверждений во втором списке посылок было ложным. Мы, безусловно, были вправе заключить, что если ни одна из первых двух посылок заведомо не виновата в противоречии, то все дело в третьей посылке, и это все, что нужно для завершения доказательства.

У доказательства цели с помощью противоречия есть преимущество в том, что оно позволяет предположить ложность одного вывода и перейти к работе с другим. Но у него есть и недостаток, заключающийся в том, что он оставляет вам довольно неоднозначную цель: вызвать противоречие, доказав то, что, как вы знаете, является ложным. Поскольку все стратегии доказательства, которые мы обсуждали до сих пор, зависят от анализа логической формы цели, похоже, что ни одна из них не поможет вам достичь цели – создать противоречие. В предыдущем доказательстве мы были вынуждены более внимательно присмотреться к нашим данным, чтобы найти противоречие. В данном случае мы сделали это, доказав, что $y = 4$, что противоречит ис-

ходному $y \neq 4$. Это иллюстрирует закономерность, которая часто встречается в доказательствах от противоречия: если одно из данных имеет вид $\neg P$, то вы можете получить противоречие с помощью доказательства P . Это наша первая стратегия, основанная на логической форме исходных посылок.

Чтобы использовать исходные посылки в форме $\neg P$:

Если вы проводите доказательство от противного, попробуйте сделать своей целью P . Если вы можете доказать P , то доказательство будет полным, потому что P противоречит исходному $\neg P$.

Стратегия доказательства

До использования стратегии:

Посылки	Цель
$\neg P$	Противоречие
—	
—	

После использования стратегии:

Посылки	Цель
$\neg P$	P
—	
—	

Форма окончательного доказательства

[Здесь приводится доказательство P .]

Поскольку мы уже знаем $\neg P$, это противоречие.

Хотя мы рекомендовали доказательство от противного для доказательства целей вида $\neg P$, его можно использовать для любых целей. Обычно лучше сначала попробовать другие стратегии, если они применимы; но если вы застряли, то можете попробовать добиться противоречия в любом доказательстве.

Следующий пример иллюстрирует это, а также еще одно важное правило составления доказательства: во многих случаях логическая форма утверждения может быть обнаружена путем записи *определения* некоторого математического слова или символа, которое встречается в утверждении. По этой причине при работе над доказательством чрезвычайно важно знать точные формулировки определений всех математических терминов.

Пример 3.2.3. Предположим, что A , B и C – множества, $A \setminus B \subseteq C$ и x – вообще что угодно. Докажите, что если $x \in A \setminus C$, то $x \in B$.

Стратегия доказательства

Нам дано, что $A \setminus B \subseteq C$, и наша цель – доказать связку $x \in A \setminus C \rightarrow x \in B$. Поскольку цель является условным утверждением, наш первый шаг – преобразовать проблему, добавив $x \in A \setminus C$ в качестве второй посылки и сделав своей целью $x \in B$:

Посылки	Цель
$A \setminus B \subseteq C$	$x \in B$
$x \in A \setminus C$	

Таким образом, форма окончательного доказательства будет следующей:

Предположим, что $x \in A \setminus C$.

[Здесь приводим доказательство $x \in B$.]

Таким образом, если $x \in A \setminus C$, то $x \in B$.

Цель $x \in B$ не содержит логических связок, поэтому ни один из методов, которые мы изучили до сих пор, не применим, и не очевидно, почему цель следует из посылок. Не имея другого выхода, мы попытаемся построить доказательство от противного:

Посылки	Цель
$A \setminus B \subseteq C$	Противоречие
$x \in A \setminus C$	
$x \notin B$	

Как и прежде, такая трансформация проблемы позволяет нам дополнить еще несколько предложений доказательства:

Предположим, что $x \in A \setminus C$.

Предположим, что $x \notin B$.

[Здесь приводим доказательство противоречия.]

Следовательно, $x \in B$.

Таким образом, если $x \in A \setminus C$, то $x \in B$.

Поскольку мы проводим доказательство от противного, а наша последняя посылка теперь является отрицательным утверждением, мы могли бы попробовать использовать нашу стратегию при наличии исходных посылок формы $\neg P$. К сожалению, эта стратегия предлагает сделать нашей целью $x \in B$, что возвращает нас к тому, с чего мы начали. Мы должны посмотреть на другие посылки, чтобы попытаться найти противоречие.

В этом случае расписывание определения второй посылки является ключом к доказательству, поскольку это определение также содержит отрицательное утверждение. По определению, $x \in A \setminus C$ означает $x \in A$ и $x \notin C$. Замена этой посылки определением дает нам:

Посылки	Цель
$A \setminus B \subseteq C$	Противоречие
$x \in A$	
$x \notin C$	
$x \notin B$	

Теперь третья посылка также имеет форму $\neg P$, где P – это утверждение $x \in C$, поэтому мы можем применить стратегию использования посылок

в форме $\neg P$ и сделать своей целью $x \in C$. Доказав это утверждение, мы завершим доказательство в целом, потому что оно противоречит исходному $x \notin C$.

Посылки	Цель
$A \setminus B \subseteq C$	
$x \in A$	
$x \notin C$	
$x \notin B$	

Еще раз: мы приблизились к искомому доказательству, когда раскрыли тот факт, что можно получить противоречие, доказывая $x \in C$. Мы также добавили к доказательству определение $x \in A \setminus C$, вставляя его в наиболее логичном месте сразу после того, как мы заявили, что $x \in A \setminus C$:

Предположим, что $x \in A \setminus C$. Это означает, что $x \in A$ и $x \notin C$.

Предположим, что $x \notin B$.

[Здесь приводим доказательство $x \in C$.]

Это противоречит тому, что $x \notin C$.

Следовательно, $x \in B$.

Таким образом, если $x \in A \setminus C$, то $x \in B$.

Мы наконец достигли точки, в которой цель легко вытекает из исходных посылок. Из $x \in A$ и $x \notin B$ заключаем, что $x \in A \setminus B$. Поскольку $A \setminus B \subseteq C$, следует, что $x \in C$.

Решение

Теорема. Предположим, что A , B и C – множества, $A \setminus B \subseteq C$ и x – вообще что угодно. Если $x \in A \setminus C$, то $x \in B$.

Доказательство. Предположим, что $x \in A \setminus C$. Это означает, что $x \in A$ и $x \notin C$. Предположим, что $x \notin B$. Тогда $x \in A \setminus B$, и поскольку $A \setminus B \subseteq C$, отсюда следует, что $x \in C$. Но это противоречит тому факту, что $x \notin C$. Следовательно, $x \in B$. Таким образом, если $x \in A \setminus C$, то $x \in B$.

Стратегия, которую мы рекомендовали для использования исходных посылок в форме $\neg P$, применима только в том случае, если вы проводите доказательство от противного. Для других видов доказательств можно использовать следующую стратегию. Эта стратегия основана на том факте, что исходные посылки в форме $\neg P$, как и цели в этой форме, могут лучше сработать, если они переформулированы как положительные утверждения.

Чтобы использовать исходные посылки в форме $\neg P$:

Если возможно, выражите исходные посылки в другой форме.

Мы обсудили стратегии работы как с исходными посылками, так и с целями в форме $\neg P$, но упустили из внимания цели формы $P \rightarrow Q$. Теперь мы восполним этот пробел, предложив две стратегии использования исходных посылок формы $P \rightarrow Q$. Ранее мы говорили, что многие стратегии использо-

вания посылок предлагают способы делать из них выводы. Такие стратегии называются *правилами вывода*. Обе наши стратегии использования посылок вида $P \rightarrow Q$ являются примерами правил вывода.

Чтобы использовать исходные посылки в форме $P \rightarrow Q$:

Если вам также дано P или если вы можете доказать, что P истинно, то вы можете использовать эту посылку, чтобы заключить, что Q истинно. Поскольку это эквивалентно $\neg Q \rightarrow \neg P$, если вы можете доказать, что Q ложно, вы можете использовать это данное, чтобы сделать вывод, что P ложно.

Первое из этих правил вывода гласит: если известно, что и P , и $P \rightarrow Q$ истинны, отсюда следует, что Q также должно быть истинным. Логики называют это правило *modus ponens*. Мы видели это правило в действии в одном из наших первых примеров правильного дедуктивного рассуждения в главе 1, в аргументе 2 примера 1.1.1. Справедливость этой формы рассуждений была проверена с помощью таблицы истинности условной связки в разделе 1.5.

Второе правило, называемое *modus tollens*, гласит: если известно, что $P \rightarrow Q$ истинно, а Q ложно, вы можете сделать вывод, что P также должно быть ложным. Справедливость этого правила также можно проверить с помощью таблиц истинности, как вас просят показать в упражнении 14. Обычно вы не извлечете заметной пользы из посылок в форме $P \rightarrow Q$, пока не докажете P или $\neg Q$. Однако если вы когда-нибудь достигнете в своем доказательстве момента, когда вы определили, что P истинно, вам, вероятно, следует немедленно использовать это утверждение, чтобы сделать вывод, что Q истинно. Точно так же, если вы когда-нибудь установите $\neg Q$, немедленно воспользуйтесь этим, чтобы заключить $\neg P$.

Хотя большинство наших примеров будут включать конкретные математические утверждения, иногда мы будем приводить примеры доказательств с буквами, обозначающими неопределенные утверждения. Позже в этой главе мы воспользуемся этим методом для проверки некоторых эквивалентностей из главы 2, которые на тот момент опирались только на интуитивное обоснование. Вот такой пример, иллюстрирующий использование *modus ponens* и *modus tollens*.

Пример 3.2.4. Предположим, что $P \rightarrow (Q \rightarrow R)$. Докажите, что $\neg R \rightarrow (P \rightarrow \neg Q)$.

Стратегия доказательства

На самом деле это можно сделать с помощью таблицы истинности, как вас просят показать в упражнении 15, но давайте найдем доказательство, используя стратегии, которые мы обсуждали. Начнем со следующей ситуации:

Посылки	Цель
$P \rightarrow (Q \rightarrow R)$	$\neg R \rightarrow (P \rightarrow \neg Q)$

Единственное, что нам дано, – это условное утверждение. Согласно только что упомянутым правилам вывода, если бы мы знали P , мы могли бы использовать *modus ponens* для вывода $Q \rightarrow R$, а если бы мы знали $\neg(Q \rightarrow R)$, мы

могли бы использовать *modus tollens* для вывода $\neg P$. Поскольку на данный момент мы не знаем ни того, ни другого, мы не можем ничего сделать с исходными посылками. Если в ходе работы над доказательством получится добавить в список исходных посылок P или $\neg(Q \rightarrow R)$, то мы рассмотрим возможность использования *modus ponens* или *modus tollens*. А пока нам нужно сосредоточиться на цели.

Цель также является условным выражением, поэтому мы предполагаем антецедент и устанавливаем следствие в качестве нашей новой цели:

<i>Посылки</i>	<i>Цель</i>
$P \rightarrow (Q \rightarrow R)$	$P \rightarrow \neg Q$
$\neg R$	

Теперь мы можем записать часть доказательства:

Предположим, что $\neg R$.

[Здесь приводим доказательство $P \rightarrow \neg Q$.]

Следовательно, $\neg R \rightarrow (P \rightarrow \neg Q)$.

Мы по-прежнему ничего не можем сделать с исходными посылками, однако новая цель – тоже условная, поэтому мы снова используем ту же стратегию:

<i>Посылки</i>	<i>Цель</i>
$P \rightarrow (Q \rightarrow R)$	$\neg Q$
$\neg R$	
P	

Теперь доказательство выглядит так:

Предположим $\neg R$.

Предположим P .

[Здесь приводим доказательство $\neg Q$.]

Следовательно, $P \rightarrow \neg Q$.

Следовательно, $\neg R \rightarrow (P \rightarrow \neg Q)$.

Мы ждали возможности использовать наши исходные посылки, применяя либо *modus ponens*, либо *modus tollens*, и теперь мы можем это сделать. Поскольку мы знаем $P \rightarrow (Q \rightarrow R)$ и P , по *modus ponens* мы можем вывести $Q \rightarrow R$. Любой вывод, сделанный из исходных посылок, может быть добавлен в столбец посылок:

<i>Посылки</i>	<i>Цель</i>
$P \rightarrow (Q \rightarrow R)$	$\neg Q$
$\neg R$	
P	
$Q \rightarrow R$	

К доказательству добавляем еще одну строчку:

Предположим $\neg R$.

Предположим P .

Поскольку P и $P \rightarrow (Q \rightarrow R)$, то $Q \rightarrow R$.

[Здесь приводим доказательство $\neg Q$.]

Следовательно, $P \rightarrow \neg Q$.

Следовательно, $\neg R \rightarrow (P \rightarrow \neg Q)$.

Наконец, наш последний шаг – использовать modus tollens. Теперь мы знаем $Q \rightarrow R$ и $\neg R$, поэтому по modus tollens мы можем заключить $\neg Q$. Это наша цель, так что доказательство готово.

Решение

Теорема. Предположим, что $P \rightarrow (Q \rightarrow R)$. Тогда $\neg R \rightarrow (P \rightarrow \neg Q)$.

Доказательство. Предположим $\neg R$. Предположим P . Так как P и $P \rightarrow (Q \rightarrow R)$, то $Q \rightarrow R$. Но тогда, поскольку $\neg R$, мы приходим к $\neg Q$. Таким образом, $P \rightarrow \neg Q$. Следовательно, $\neg R \rightarrow (P \rightarrow \neg Q)$.

Иногда, если вы зашли в тупик, вы можете использовать правила вывода, чтобы пойти в обратном направлении. Например, предположим, что одна из ваших посылок имеет форму $P \rightarrow Q$, и ваша цель Q . Если бы вы только могли доказать P , вы могли бы использовать modus ponens для достижения своей цели. Поэтому было бы разумно рассматривать как цель P , а не Q . Если вы сможете доказать P , вам останется сделать еще один шаг, чтобы доказать Q .

Пример 3.2.5. Предположим, что $A \subseteq B$, $a \in A$ и $a \notin B \setminus C$. Докажите, что $a \in C$.

Стратегия доказательства

Посылки	Цель
$A \subseteq B$	
$a \in A$	
$a \notin B \setminus C$	

Наша третья исходная посылка – отрицательное утверждение, поэтому мы начнем с преобразования его в эквивалентное положительное утверждение. Согласно определению разности двух множеств, эта посылка означает $\neg(a \in B \wedge a \notin C)$, а согласно одному из законов Де Моргана это эквивалентно $a \notin B \vee a \in C$. Поскольку нашей целью является $a \in C$, вероятно, будет полезно переписать ее в эквивалентной форме $a \in B \rightarrow a \in C$:

Посылки	Цель
$A \subseteq B$	
$a \in A$	
$a \in B \rightarrow a \in C$	

Теперь мы можем использовать нашу стратегию для использования посылок в форме $P \rightarrow Q$. Наша цель – $a \in C$, и нам дано, что $a \in B \rightarrow a \in C$. Если докажем, что $a \in B$, то сможем использовать modus ponens, чтобы достичь цели доказательства. Итак, давайте попробуем рассматривать $a \in B$ как цель и посмотрим, облегчит ли это задачу:

Посылки	Цель
$A \subseteq B$	$a \in B$
$a \in A$	
$a \in B \rightarrow a \in C$	

Теперь понятно, как достичь цели. Поскольку $a \in A$ и $A \subseteq B$, то $a \in B$.

Решение

Теорема. Предположим, что $A \subseteq B$, $a \in A$ и $a \notin B \setminus C$. Тогда $a \in C$.

Доказательство. Поскольку $a \in A$ и $A \subseteq B$, мы можем заключить, что $a \in B$. Но $a \notin B \setminus C$, отсюда следует, что $a \in C$.

Упражнения

- *1. Эту задачу можно решить, используя таблицы истинности, но вы вместо этого используйте методы написания доказательств, которые уже обсуждались в этой главе (см. пример 3.2.4).
 - (a) Предположим, что $P \rightarrow Q$ и $Q \rightarrow R$ истинны. Докажите, что $P \rightarrow R$ верно.
 - (b) Предположим, что $\neg R \rightarrow (P \rightarrow \neg Q)$ истинно. Докажите, что $P \rightarrow (Q \rightarrow R)$ верно.
2. Эту задачу можно решить, используя таблицы истинности, но вы вместо этого используйте методы написания доказательств, которые уже обсуждались в этой главе (см. пример 3.2.4).
 - (a) Предположим, что $P \rightarrow Q$ и $R \rightarrow \neg Q$ истинны. Докажите, что $P \rightarrow \neg R$ истинно.
 - (b) Предположим, что P истинно. Докажите, что $Q \rightarrow \neg(Q \rightarrow \neg P)$ истинно.
3. Предположим, что $A \subseteq C$ и B и C не пересекаются. Докажите, что если $x \in A$, то $x \notin B$.
4. Предположим, что $A \setminus B$ не пересекается с C и $x \in A$. Докажите, что если $x \in C$, то $x \in B$.
- *5. Докажите, что не может быть вместе $x \in A \setminus B$ и $x \in B \setminus C$.
- *6. Воспользуйтесь методом доказательства от противного, чтобы доказать теорему из примера 3.2.1.

7. Воспользуйтесь методом доказательства от противного, чтобы доказать теорему из примера 3.2.5.
8. Предположим, что $y + x = 2y - x$, причем x и y не равны нулю. Докажите, что $y \neq 0$.
- *9. Предположим, что a и b – ненулевые действительные числа. Докажите, что если $a < 1/a < b < 1/b$, то $a < -1$.
10. Предположим, что x и y – действительные числа. Докажите, что если $x^2y = 2x + y$, то если $y \neq 0$, то $x \neq 0$.
11. Предположим, что x и y – действительные числа. Докажите, что если $x \neq 0$, то если $y = (3x^2 + 2y) / (x^2 + 2)$, то $y = 3$.
- *12. Рассмотрим следующую ошибочную теорему.

Ошибкачная теорема. Предположим, что x и y – действительные числа и $x + y = 10$. Тогда $x \neq 3$ и $y \neq 8$.

(a) Где ошибка в следующем доказательстве теоремы?

Доказательство. Предположим, что вывод теоремы ошибочен. Тогда $x = 3$ и $y = 8$. Но тогда $x + y = 11$, что противоречит исходной посылке о том, что $x + y = 10$. Следовательно, вывод должен быть верным.

(b) Покажите, что теорема ошибочна, найдя контрпример.

13. Рассмотрим следующую ошибочную теорему.

Ошибкачная теорема. Предположим, что $A \subseteq C, B \subseteq C$ и $x \in A$. Тогда $x \in B$.

(a) Где ошибка в следующем доказательстве теоремы?

Доказательство. Предположим, что $x \notin B$. Поскольку $x \in A$ и $A \subseteq C$, то $x \in C$. Поскольку $x \notin B$ и $B \subseteq C$, то $x \notin C$. Но теперь мы доказали и $x \in C$, и $x \notin C$, поэтому мы пришли к противоречию. Следовательно, $x \in B$.

(b) Покажите, что теорема ошибочна, найдя контрпример.

14. Используйте таблицы истинности, чтобы показать, что modus tollens является допустимым правилом вывода.

- *15. Используйте таблицы истинности, чтобы проверить правильность теоремы из примера 3.2.4.

16. Используйте таблицы истинности, чтобы проверить правильность утверждений в упражнении 1.

17. Используйте таблицы истинности, чтобы проверить правильность утверждений в упражнении 2.

18. Можно ли изменить доказательство из примера 3.2.2, чтобы доказать, что если $x^2 + y = 13$ и $x \neq 3$, то $y \neq 4$? Объясните ответ.

3.3. ДОКАЗАТЕЛЬСТВА С ИСПОЛЬЗОВАНИЕМ КВАНТОРОВ

Взгляните снова на пример 3.2.3. В этом примере мы сказали, что x может быть каким угодно, и доказали утверждение $x \in A \setminus C \rightarrow x \in B$. Поскольку рассуждения, которые мы использовали, применимы независимо от того, что представляет собой x , наше доказательство фактически показывает, что $x \in A \setminus C \rightarrow x \in B$ истинно для всех значений x . Другими словами, мы можем заключить $\forall x(x \in A \setminus C \rightarrow x \in B)$.

Это рассуждение иллюстрирует самый простой и понятный способ доказательства цели в форме $\forall xP(x)$. Если вы можете предоставить доказательство цели $P(x)$, которое будет работать независимо от x , то вы можете сделать вывод, что $\forall xP(x)$ должно быть истинным. Чтобы убедиться, что ваше доказательство будет работать для любого значения x , важно начинать доказательство без каких-либо предположений относительно x . Математики выражают это, говоря, что x должен быть *произвольным* объектом. В частности, вы не должны предполагать, что x равен любому другому объекту, уже обсуждаемому в доказательстве. Следовательно, если буква x уже используется в доказательстве для обозначения некоторого конкретного объекта, то вы не можете использовать ее для обозначения произвольного объекта. В этом случае вы должны выбрать другую переменную, которая еще не используется в доказательстве, например y , и заменить цель $\forall xP(x)$ эквивалентным выражением $\forall yP(y)$. Теперь вы можете продолжить, используя y для обозначения произвольного объекта и доказав $P(y)$.

Чтобы доказать цель вида $\forall xP(x)$:

Пусть x обозначает произвольный объект; докажем $P(x)$. Буква x должна быть новой переменной в доказательстве. Если x уже используется в доказательстве для обозначения чего-либо, тогда вы должны выбрать неиспользуемую переменную, скажем y , чтобы обозначить произвольный объект, и доказать $P(y)$.

Стратегия доказательства

Перед использованием стратегии:

<i>Посылки</i>	<i>Цель</i>
—	$\forall xP(x)$
—	

После использования стратегии:

<i>Посылки</i>	<i>Цель</i>
—	$P(x)$
—	

Форма окончательного доказательства

Пусть x – произвольный объект.

[Здесь приводится доказательство $P(x)$.]

Поскольку x было произвольным, мы можем заключить, что $\forall x P(x)$.

Пример 3.3.1. Предположим, что A , B и C – множества и $A \setminus B \subseteq C$. Докажите, что $A \setminus C \subseteq B$.

Стратегия доказательства

Посылки	Цель
$A \setminus B \subseteq C$	$A \setminus C \subseteq B$

Как обычно, мы сначала смотрим на логическую форму цели для планирования нашей стратегии. В этом случае мы должны выписать определение \subseteq , чтобы определить логическую форму цели.

Посылки	Цель
$A \setminus B \subseteq C$	$\forall x(x \in A \setminus C \rightarrow x \in B)$

Поскольку цель имеет вид $\forall x P(x)$, где $P(x)$ – это утверждение $x \in A \setminus C \rightarrow x \in B$, мы введем в доказательство новую переменную x , которая будет обозначать произвольный объект, а затем попытаемся доказать $x \in A \setminus C \rightarrow x \in B$. Отметим, что x – новая переменная в доказательстве. Она появилась в логической форме цели как связанная переменная, но помните, что связанные переменные не означают ничего конкретного. Мы еще не использовали x как свободную переменную ни в одном операторе, поэтому он не использовался для обозначения какого-либо конкретного объекта. Чтобы убедиться, что x произвольно, мы должны быть осторожны, дабы не добавлять никаких предположений касаемо x в столбец данных. Однако мы меняем нашу цель:

Посылки	Цель
$A \setminus B \subseteq C$	$x \in A \setminus C \rightarrow x \in B$

Согласно нашей стратегии, окончательное доказательство должно выглядеть так:

Пусть x произвольно.

[Здесь помещаем доказательство $x \in A \setminus C \rightarrow x \in B$.]

Поскольку x был произвольным, мы можем заключить, что $\forall x(x \in A \setminus C \rightarrow x \in B)$, поэтому $A \setminus C \subseteq B$.

Теперь проблема в точности такая же, как в примере 3.2.3, так что оставшаяся часть решения аналогичная. Другими словами, мы можем просто вставить доказательство, которое мы написали в примере 3.2.3, между первым и последним предложениями доказательства, написанного здесь.

Решение

Теорема. Предположим, что A , B и C – множества и $A \setminus B \subseteq C$. Тогда $A \setminus C \subseteq B$.

Доказательство. Пусть x означает произвольный объект. Предположим, что $x \in A \setminus C$. Это означает, что $x \in A$ и $x \notin C$. Предположим, что $x \notin B$. Тогда $x \in A \setminus B$, и поскольку $A \setminus B \subseteq C$, то $x \in C$. Но это противоречит тому факту, что $x \notin C$. Следовательно, $x \in B$. Таким образом, если $x \in A \setminus C$, то $x \in B$. Поскольку x произвольно, мы можем заключить, что $\forall x(x \in A \setminus C \rightarrow x \in B)$, поэтому $A \setminus C \subseteq B$.

Обратите внимание: хотя это доказательство показывает, что каждый элемент $A \setminus C$ также является элементом B , оно не содержит таких фраз, как «каждый элемент $A \setminus C$ » или «все элементы $A \setminus C$ ». На протяжении большей части доказательства мы просто рассуждаем о x , который рассматривается как единственный фиксированный элемент $A \setminus C$. Мы соглашаемся, что x обозначает некоторый конкретный элемент $A \setminus C$, стараясь не делать никаких предположений о том, какой это элемент. Только в конце доказательства мы замечаем, что, поскольку x был произвольным, наши выводы об x были бы верными независимо от того, что представляет собой x . Это главное преимущество использования данной стратегии для доказательства цели вида $\forall x P(x)$. Оно позволяет вам доказать цель относительно всех объектов, рассуждая только об одном объекте, если этот объект является произвольным. Если вы доказываете цель в форме $\forall x P(x)$ и обнаруживаете, что много говорите о «всех x » или «каждом x », вы, вероятно, излишне усложняете свое доказательство, не используя эту стратегию.

Как мы показали в главе 2, утверждения вида $\forall x(P(x) \rightarrow Q(x))$ довольно распространены в математике. Поэтому, возможно, стоит подумать о том, как можно объединить стратегии, которые мы обсуждали, для доказательства цели в этой форме. Поскольку цель начинается с $\forall x$, первый шаг – считать x произвольным и попытаться доказать $P(x) \rightarrow Q(x)$. Чтобы доказать эту цель, вы, вероятно, захотите предположить, что $P(x)$ истинно, и доказать $Q(x)$. Ваше доказательство, вероятно, начнется так: «Пусть x произвольно. Предположим, что $P(x)$ ». Затем последуют шаги, необходимые для достижения цели $Q(x)$. Часто в этом типе доказательства утверждение, что x произвольно, опускается, и доказательство просто начинается словами «Предположим $P(x)$ ». Когда таким образом в доказательство вводится новая переменная x , обычно подразумевается, что она обозначает произвольный элемент. Другими словами, относительно x не делается никаких предположений, кроме заявления, что $P(x)$ истинно.

Важным примером этого типа доказательства является доказательство, в котором цель имеет вид $\forall x \in A P(x)$. Напомним, что эта запись означает то же самое, что и $\forall x(x \in A \rightarrow P(x))$, поэтому в соответствии с нашей стратегией доказательство должно начинаться с «Предположим $x \in A$ », а затем переходить к шагам, необходимым для заключения, что $P(x)$ истинно. Еще раз: нам понятно, что относительно x не делается никаких предположений, кроме явного предположения, что $x \in A$, поэтому x обозначает произвольный элемент A .

Математики иногда пропускают и другие шаги в доказательствах, если можно ожидать, что знающие читатели сами восстановят их. В частности,

многие из наших стратегий доказательства предполагают, что доказательство заканчивается предложением, в котором резюмируется, почему рассуждения, приведенные в доказательстве, приводят к желаемому выводу. В доказательстве, в котором были объединены несколько из этих стратегий, в конце доказательства может быть несколько таких суммирующих предложений, одно за другим. Математики часто сводят эти выводы в одно предложение или даже полностью их пропускают. Когда вы читаете доказательство, написанное кем-то другим, вам может быть полезно восстановить эти пропущенные шаги.

Пример 3.3.2. Предположим, что A и B – множества. Докажите, что если $A \cap B = A$, то $A \subseteq B$.

Стратегия доказательства

Наша цель – $A \cap B = A \rightarrow A \subseteq B$. Поскольку цель является условным выражением, мы добавляем антецедент в список исходных посылок и делаем следствие целью. Мы также выпишем определение \subseteq в новой цели, чтобы увидеть, какова ее логическая форма.

Посылки	Цель
$A \cap B = A$	$\forall x(x \in A \rightarrow x \in B)$

Теперь цель имеет вид $\forall x(P(x) \rightarrow Q(x))$, где $P(x)$ – это утверждение $x \in A$, а $Q(x)$ – утверждение $x \in B$. Поэтому пусть x произвольно, предположим $x \in A$ и докажем $x \in B$:

Посылки	Цель
$A \cap B = A$	$x \in B$
$x \in A$	

Комбинируя стратегии доказательства, которые мы использовали, мы видим, что окончательное доказательство будет иметь следующий вид:

Предположим, что $A \cap B = A$.

Пусть x произвольно.

Предположим, что $x \in A$.

[Здесь приводим доказательство $x \in B$.]

Следовательно, $x \in A \rightarrow x \in B$.

Поскольку x был произвольным, мы можем заключить, что $\forall x(x \in A \rightarrow x \in B)$, поэтому $A \subseteq B$.

Следовательно, если $A \cap B = A$, то $A \subseteq B$.

Как говорилось ранее, когда мы пишем окончательное доказательство, то можем пропустить предложение «Пусть x произвольно», а также некоторые или все из последних трех предложений.

Мы подошли к тому моменту, когда уже не можем анализировать логическую форму цели. К счастью, когда мы смотрим на исходные посылки, то обнаруживаем, что цель легко достижима. Поскольку $x \in A$ и $A \cap B = A$, отсюда

следует, что $x \in A \cap B$, поэтому $x \in B$. (На этом последнем шаге мы используем определение \cap : $x \in A \cap B$ означает $x \in A$ и $x \in B$.)

Решение

Теорема. Предположим, что A и B – множества. Если $A \cap B = A$, то $A \subseteq B$.

Доказательство. Предположим, что $A \cap B = A$, и предположим, что $x \in A$. Тогда поскольку $A \cap B = A$, то $x \in A \cap B$, поэтому $x \in B$. Поскольку x был произвольным элементом A , мы можем заключить, что $A \subseteq B$.

Доказательство цели вида $\exists x P(x)$ также предусматривает введение новой переменной x в рассуждения и доказательство $P(x)$, но в этом случае x не будет произвольным. Поскольку вам нужно только доказать, что $P(x)$ истинно хотя бы для одного x , достаточно присвоить конкретное значение x и доказать $P(x)$ для этого значения x .

Чтобы доказать цель вида $\exists x P(x)$:

Попробуйте найти значение x , для которого, по вашему мнению, будет истинным $P(x)$. Затем начните доказательство со слов «Пусть x = (значение, которое вы выбрали)» и перейдите к доказательству $P(x)$ для этого значения x . Еще раз подчеркнем, что x должен быть новой переменной. Если буква x уже используется в доказательстве для какой-либо другой цели, тогда вам следует выбрать неиспользуемую переменную, скажем y , и переписать цель в эквивалентной форме $\exists y P(y)$. Теперь продолжайте, как и раньше, начиная доказательство с «Пусть y = (значение, которое вы выбрали)», и докажите $P(y)$.

Стратегия доказательства

Перед использованием стратегии:

Посылки	Цель
–	$\exists x P(x)$
–	

После использования стратегии:

Посылки	Цель
–	$P(x)$
–	
$x = (\text{значение, которое вы выбрали})$	

Форма окончательного доказательства

Пусть $x = (\text{значение, которое вы выбрали})$.

[Здесь приводится доказательство $P(x)$.]

Таким образом, $\exists x P(x)$.

В некоторых случаях найти подходящее значение для x может быть сложно. Один из способов, который иногда бывает полезен, – это предположить,

что $P(x)$ истинно, а затем посмотреть, сможете ли вы выяснить, каким должен быть x , основываясь на этом предположении. Если $P(x)$ – уравнение, включающее x , это равносильно решению уравнения относительно x . Однако если это не сработает, вы можете использовать любой другой метод, который вам нравится, чтобы попытаться найти значение x , включая предположения и метод проб и ошибок. Причина, по которой у вас есть такая свобода действий на этом этапе, заключается в том, что рассуждения, которые вы используете для поиска значения x , не появятся в окончательном доказательстве. Это из-за нашего правила, согласно которому доказательство должно содержать только рассуждения, необходимые для обоснования вывода доказательства, а не объяснение того, как вы пришли к этим рассуждениям. Чтобы обосновать вывод о том, что $\exists x P(x)$ истинно, необходимо только проверить, что $P(x)$ оказывается истинным, когда x присваивается определенное значение. Как вы до этого додумались – это ваше личное дело, а не часть обоснования вывода.

Пример 3.3.3. Докажите, что для любого действительного числа x если $x > 0$, то существует действительное число y такое, что $y(y + 1) = x$.

Стратегия доказательства

В символической записи наша цель имеет вид $\forall x(x > 0 \rightarrow \exists y[y(y + 1) = x])$, где предполагается, что переменные x и y в этом утверждении лежат в диапазоне \mathbb{R} . Мы начинаем с предположения, что x – произвольное действительное число, а затем предполагаем, что $x > 0$, и пытаемся доказать, что $\exists y[y(y + 1) = x]$. Таким образом, теперь у нас есть следующая исходная посылка и цель:

Посылки	Цель
$x > 0$	$\exists y[y(y + 1) = x]$

Поскольку наша цель имеет вид $\exists y P(y)$, где $P(y)$ – это утверждение $y(y + 1) = x$, в соответствии с нашей стратегией мы должны попытаться найти значение y , для которого $P(y)$ истинно. В данном случае мы можем сделать это, решив уравнение $y(y + 1) = x$ относительно y . Это квадратное уравнение, которое можно решить с помощью формулы корней квадратного уравнения:

$$y(y + 1) = x \Leftrightarrow y^2 + y - x = 0 \Leftrightarrow y = \frac{-1 \pm \sqrt{1 + 4x}}{2}.$$

Обратите внимание, что $\sqrt{1 + 4x}$ определено, поскольку мы имеем $x > 0$ как данность. Фактически мы нашли два решения для y , но, чтобы доказать, что $\exists y[y(y + 1) = x]$, нам нужно показать только одно значение y , которое делает уравнение $y(y + 1) = x$ истинным. В доказательстве можно использовать любое из двух решений. Воспользуемся решением $y = (-1 + \sqrt{1 + 4x})/2$.

Шаги, которые мы использовали для нахождения y , не должны появляться в окончательном доказательстве. В окончательном доказательстве мы просто скажем «Пусть $y = (-1 + \sqrt{1 + 4x})/2$ », а затем докажем, что $y(y + 1) = x$. Другими словами, окончательное доказательство будет иметь следующий вид:

Пусть x – произвольное действительное число.

Предположим, что $x > 0$.

Пусть $y = (-1 + \sqrt{1 + 4x})/2$.

[Здесь доказываем истинность $y(y + 1) = x$.]

Таким образом, $\exists y[y(y + 1) = x]$.

Следовательно, $x > 0 \rightarrow \exists y[y(y + 1) = x]$.

Поскольку x был произвольным, мы можем заключить, что $\forall x(x > 0 \rightarrow \exists y[y(y + 1) = x])$.

Чтобы понять, что нужно сделать, чтобы заполнить оставшийся пробел в доказательстве, мы добавляем $y = (-1 + \sqrt{1 + 4x})/2$ в список исходных посылок и делаем $y(y + 1) = x$ целью:

Посылки	Цель
$x > 0$	$y(y + 1) = x$
$y = (-1 + \sqrt{1 + 4x})/2$	

Теперь мы можем доказать, что равенство $y(y + 1) = x$ выполняется, просто подставив $(-1 + \sqrt{1 + 4x})/2$ вместо y и убедившись в истинности полученного равенства.

Решение

Теорема. Для каждого действительного числа x , если $x > 0$, существует действительное число y такое, что $y(y + 1) = x$.

Доказательство. Пусть x – произвольное действительное число, и пусть $x > 0$.
Пусть

$$y = \frac{-1 + \sqrt{1 + 4x}}{2},$$

которое определено, поскольку $x > 0$. Тогда

$$\begin{aligned} y(y + 1) &= \left(\frac{-1 + \sqrt{1 + 4x}}{2} \right) \cdot \left(\frac{-1 + \sqrt{1 + 4x}}{2} + 1 \right) \\ &= \left(\frac{\sqrt{1 + 4x} - 1}{2} \right) \cdot \left(\frac{\sqrt{1 + 4x} + 1}{2} \right) \\ &= \frac{1 + 4x - 1}{4} = \frac{4x}{4} = x. \end{aligned}$$

Иногда, доказывая цель в форме $\exists y Q(y)$, вы не сможете определить, просто взглянув на утверждение $Q(y)$, какое значение вам следует подставить вместо y . В этом случае вы можете более внимательно изучить исходные посылки, чтобы понять, предлагают ли они значение для подстановки вместо y . В частности, в этой ситуации может оказаться полезной исходная посылка в виде $\exists x P(x)$. Она означает, что объект с определенным свойством существует

ет. Вероятно, удобно было бы представить, что выбран конкретный объект с этим свойством, и ввести в доказательство новую переменную, скажем x_0 , которая будет обозначать этот объект. Таким образом, в оставшейся части доказательства вы будете использовать x_0 для обозначения некоторого конкретного объекта, и вы можете предположить, что с x_0 , обозначающим этот объект, $P(x_0)$ истинно. Другими словами, вы можете добавить $P(x_0)$ в свой список исходных посылок. Этот объект x_0 или что-то вытекающее из него может пригодиться для подстановки вместо y , чтобы показать истинность $Q(y)$.

Чтобы использовать исходную посылку в форме $\exists xP(x)$:

Ведите в доказательство новую переменную x_0 , чтобы обозначить объект, для которого истинно $P(x_0)$. Это означает, что теперь вы можете предположить, что $P(x_0)$ истинно. Логики называют это правило вывода *экзистенциальным подтверждением*.

Обратите внимание, что использование посылки в форме $\exists xP(x)$ сильно отличается от доказательства цели в форме $\exists xP(x)$, потому что при использовании посылки в этой форме *вы не можете выбрать конкретное значение для подстановки вместо x* . Вы можете предположить, что x_0 обозначает некоторый объект, для которого $P(x_0)$ истинно, но вы не можете предполагать что-либо еще относительно x_0 . С другой стороны, посылка в форме $\forall xP(x)$ говорит, что $P(x)$ будет истинным независимо от того, какое значение присвоено x . Следовательно, вы можете выбрать любое значение, которое хотите подставить вместо x , и использовать это значение, чтобы сделать вывод, что $P(x)$ истинно.

Чтобы использовать исходную посылку в форме $\forall xP(x)$:

Вы можете подставить вместо x любое значение, например a , и использовать его, чтобы сделать вывод, что $P(a)$ истинно. Это правило называется *универсальным подтверждением*.

Обычно, если у вас есть посылка в форме $\exists xP(x)$, вы должны немедленно применить к ней экзистенциальное подтверждение. Полезный совет: если вы знаете, что что-то существует, вы должны дать этому название. С другой стороны, вы не сможете применить универсальное подтверждение к посылке в форме $\forall xP(x)$, если у вас нет определенного значения a для подстановки вместо x , поэтому вы можете подождать, пока в доказательстве не представится подходящий случай. Например, рассмотрим посылку в форме $\forall x(P(x) \rightarrow Q(x))$. Вы можете использовать эту посылку, чтобы заключить, что $P(a) \rightarrow Q(a)$ для любого a , но согласно нашему правилу использования посылок, которые являются условными операторами, этот вывод, вероятно, не будет очень полезным, если вы не знаете $P(a)$ или $\neg Q(a)$. Вероятно, вам следует подождать, пока в доказательстве не появится объект a , для которого вы знаете либо $P(a)$, либо $\neg Q(a)$, и подставить a вместо x .

Мы уже использовали этот прием в некоторых из наших предыдущих доказательств, имея дело с посылками в форме $A \subseteq B$. Так, в примере 3.2.5 мы использовали посылки $A \subseteq B$ и $a \in A$, чтобы заключить, что $a \in B$. Обоснование

этого рассуждения заключается в том, что $A \subseteq B$ означает $\forall x(x \in A \rightarrow x \in B)$, поэтому согласно правилу универсального подтверждения мы можем подставить a вместо x и заключить, что $a \in A \rightarrow a \in B$. Поскольку мы также знаем, что $a \in A$, по modus ponens следует, что $a \in B$.

Пример 3.3.4. Предположим, что \mathcal{F} и \mathcal{G} – семейства множеств и $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Докажите, что $\bigcap \mathcal{F} \subseteq \bigcup \mathcal{G}$.

Стратегия доказательства

Наш первый шаг в анализе логической формы цели – расписать значение символа подмножества, что дает нам утверждение $\forall x(x \in \bigcap \mathcal{F} \rightarrow x \in \bigcup \mathcal{G})$. Мы могли бы пойти дальше, расписав определения объединения и пересечения, но той записи, которую мы уже сделали, будет достаточно, чтобы мы могли решить, как начать доказательство. Определения объединения и пересечения потребуются позже в доказательстве, но сейчас мы не будем спешить с подстановкой. При анализе логических форм данностей и целей, чтобы найти доказательство, обычно лучше всего делать ровно столько записей, сколько необходимо для определения следующего шага доказательства. Продолжение логического анализа обычно лишь вносит ненужные сложности, не принося никакой пользы.

Поскольку наша цель имеет вид $\forall x(x \in \bigcap \mathcal{F} \rightarrow x \in \bigcup \mathcal{G})$, мы считаем x произвольным объектом, предполагаем, что $x \in \bigcap \mathcal{F}$, и пытаемся доказать $x \in \bigcup \mathcal{G}$.

Посылки	Цель
$\mathcal{F} \cap \mathcal{G} \neq \emptyset$	
$x \in \bigcap \mathcal{F}$	$x \in \bigcup \mathcal{G}$

Новая цель в логической записи имеет вид $\exists A \in \mathcal{G}(x \in A)$, поэтому, чтобы доказать ее, мы должны попытаться найти значение A , которое будет здесь «работать». Беглый взгляд на цель не проясняет, как выбрать A , поэтому мы присмотримся более внимательно к исходным посылкам. Начнем с записи их логическими символами:

Посылки	Цель
$\exists A(A \in \mathcal{F} \cap \mathcal{G})$	
$\forall A \in \mathcal{F}(x \in A)$	$\exists A \in \mathcal{G}(x \in A)$

Вторая посылка начинается с $\forall A$, поэтому мы не сможем использовать его до тех пор, пока в ходе доказательства не появится подходящее значение для подстановки вместо A . В частности, мы должны иметь в виду, что если мы когда-нибудь в поисках доказательства найдем элемент \mathcal{F} , мы можем подставить его вместо A во второй посылке и заключить, что он содержит x как элемент. Однако первая посылка начинается с $\exists A$, поэтому мы должны немедленно пустить ее в дело. Она говорит, что существует некоторый объект, который является элементом $\mathcal{F} \cap \mathcal{G}$. Исходя из правила экзистенциального подтверждения, мы можем ввести имя, скажем A_0 , для этого объекта. Таким образом, с этого момента мы можем рассматривать $A_0 \in \mathcal{F} \cap \mathcal{G}$ как данность.

Поскольку теперь у нас есть имя A_0 для определенного элемента $\mathcal{F} \cap \mathcal{G}$, было бы излишним продолжать обсуждение исходного утверждения $\exists A (A \in \mathcal{F} \cap \mathcal{G})$, поэтому мы исключим его из нашего списка данных. Поскольку наша новая посылка $A_0 \in \mathcal{F} \cap \mathcal{G}$ означает $A_0 \in \mathcal{F}$ и $A_0 \in \mathcal{G}$, теперь мы имеем следующую ситуацию:

Посылки	Цель
$A_0 \in \mathcal{F}$	$\exists A \in \mathcal{G} (x \in A)$
$A_0 \in \mathcal{G}$	
$\forall A \in \mathcal{F} (x \in A)$	

Если вы достаточно глубоко изучили методику доказательства, то должны знать, каким должен быть следующий шаг. Раньше мы решили внимательно следить за любыми элементами \mathcal{F} , которые могут возникнуть во время доказательства, чтобы подставить вместо A в последнюю исходную посылку. И вот у нас есть элемент \mathcal{F} : это A_0 ! Подставляя A_0 вместо A , мы можем заключить, что $x \in A_0$. Любые выводы из этого можно рассматривать в будущем как исходную посылку, поэтому вы можете смело добавить это утверждение в столбец исходных посылок, если пожелаете.

Как вы помните, мы решили присмотреться к посылкам, потому что не знали, какое значение присвоить A в цели. Нам нужно подставить значение A , которое входит в \mathcal{G} , и это сделает утверждение $x \in A$ истинным. Помог ли нам анализ исходных посылок найти значение для подстановки A ? Да! Используйте $A = A_0$.

Хотя мы перевели исходные утверждения $x \in \bigcap \mathcal{F}$, $x \in \bigcup \mathcal{G}$ и $\mathcal{F} \cap \mathcal{G} \neq \emptyset$ в логическую символьную форму, чтобы понять, как использовать их в доказательстве, эти преобразования обычно не записывают в окончательной форме доказательства. В окончательном доказательстве мы просто записываем все утверждения в их первоначальной форме и оставляем за читателем доказать самостоятельную запись логических форм, чтобы следовать нашим рассуждениям.

Решение

Теорема. Предположим, что \mathcal{F} и \mathcal{G} – семейства множеств и $\mathcal{F} \cap \mathcal{G} \neq \emptyset$. Тогда $\bigcap \mathcal{F} \subseteq \bigcup \mathcal{G}$.

Доказательство. Предположим, что $x \in \bigcap \mathcal{F}$. Поскольку $\mathcal{F} \cap \mathcal{G} \neq \emptyset$, мы можем обозначить через A_0 элемент $\mathcal{F} \cap \mathcal{G}$. Таким образом, $A_0 \in \mathcal{F}$ и $A_0 \in \mathcal{G}$. Поскольку $x \in \bigcap \mathcal{F}$ и $A_0 \in \mathcal{F}$, отсюда следует, что $x \in A_0$. Но мы также знаем, что $A_0 \in \mathcal{G}$, поэтому можем заключить, что $x \in \bigcup \mathcal{G}$.

Доказательства, включающие кванторы всеобщности и существования, часто вызывают у них затруднения.

Это последнее предложение сбило вас с толку, не так ли? Вы, наверное, задаетесь вопросом: «У них – это у кого?» Читатели ваших доказательств испытывают такое же замешательство, если вы будете использовать переменные, не объясняя, что они означают. Начинающие составители доказательств иногда

небрежно относятся к пояснениям, и поэтому доказательства, включающие кванторы всеобщности и существования, часто вызывают затруднения у читателей. (На этот раз в предложении больше смысла, не так ли?) Используя стратегии, которые мы обсуждали в этом разделе, вы будете вводить новые переменные в свое доказательство, и когда вы это делаете, вы всегда должны аккуратно пояснить читателю, что они обозначают.

Например, доказывая цель в форме $\forall x \in A P(x)$, вы, вероятно, начнете с введения переменной x для обозначения произвольного элемента A . Ваш читатель не будет знать, что означает x , если вы не начнете свое доказательство со слов «Пусть x – произвольный элемент из A » или «Предположим, $x \in A$ ». Эти предложения говорят читателю, что с этого момента он должен воспринимать x как обозначение некоторого конкретного элемента A , хотя какой элемент он обозначает, остается неуказанным. Конечно, вы должны четко понимать, что означает x . В частности, поскольку x должен быть произвольным, вам следует аккуратно формулировать мысли, чтобы случайно не предположить об x ничего иного, кроме того факта, что $x \in A$. Попробуйте представить, что значение x выбрано *кем-то другим*; вы не можете контролировать, какой элемент A он выберет. Использование посылок в форме $\exists x P(x)$ выглядит аналогично. Эта форма говорит о том, что вы можете ввести в доказательство новую переменную x_0 , чтобы обозначить некоторый объект, для которого $P(x_0)$ истинно, но вы не можете предполагать что-либо еще относительно x_0 . С другой стороны, если вы *доказываете* $\exists x P(x)$, ваше доказательство, вероятно, будет начинаться со слов «Пусть $x = \dots$ ». На этот раз вы можете выбрать значение x и должны прямо сообщить читателю, что вы выбираете значение x и какое значение вы выбрали.

Также важно при объявлении новой переменной x твердо знать, *какого рода* объект обозначает x . Это число? множество? функция? матрица? Лучше не писать $a \in X$, например, если X не является множеством. Если вы не будете очень аккуратны, то можете написать чушь. Вам также иногда необходимо знать, какой объект представляет собой переменная, чтобы выяснить логическую форму оператора, включающего эту переменную. Например, запись $A = B$ означает $\forall x (x \in A \leftrightarrow x \in B)$, если A и B – множества, но не в том случае, если они числа.

Самая важная вещь, о которой следует помнить при введении переменных в доказательство, – это простое правило, что переменные всегда должны вводиться перед их использованием. Если вы приведете утверждение об x (т. е. утверждение, в котором x встречается как свободная переменная) без предварительного объяснения того, что означает x , читатель вашего доказательства не поймет, о чем вы говорите, – и есть большой шанс, что вы и сами запутаетесь в том, что хотели сказать!

Поскольку доказательства с использованием кванторов обычно требуют больше практики, чем другие доказательства, которые мы обсуждали до сих пор, мы заканчиваем этот раздел еще двумя примерами.

Пример 3.3.5. Предположим, что B – множество, а \mathcal{F} – семейство множеств. Докажите, что если $\bigcup \mathcal{F} \subseteq B$, то $\mathcal{F} \subseteq \mathcal{P}(B)$.

Стратегия доказательства

Мы предполагаем $\bigcup \mathcal{F} \subseteq B$ и пытаемся доказать $\mathcal{F} \subseteq \mathcal{P}(B)$. Поскольку эта цель означает $\forall x(x \in \mathcal{F} \rightarrow x \in \mathcal{P}(B))$, мы вводим переменную x , обозначающую произвольный элемент, предполагаем $x \in \mathcal{F}$ и назначаем $x \in \mathcal{P}(B)$ в качестве нашей цели. Напомним, что \mathcal{F} – семейство множеств, и поскольку $x \in \mathcal{F}$, то x – множество.

Таким образом, теперь у нас есть следующие посылки и цель:

Посылки	Цель
$\bigcup \mathcal{F} \subseteq B$	
$x \in \mathcal{F}$	$x \in \mathcal{P}(B)$

Чтобы выяснить, как доказать эту цель, мы должны использовать определение степенного множества. Утверждение $x \in \mathcal{P}(B)$ означает $x \subseteq B$, или, другими словами, $\forall y(y \in x \rightarrow y \in B)$. Поэтому мы должны ввести в доказательство еще один произвольный объект. Пусть y обозначает произвольный объект, пусть $y \in x$, и попытаемся доказать $y \in B$.

Посылки	Цель
$\bigcup \mathcal{F} \subseteq B$	
$x \in \mathcal{F}$	$y \in B$
$y \in x$	

Цель не поддается дальнейшему анализу, поэтому мы должны более внимательно присмотреться к посылкам. Наша цель – $y \in B$, и единственное место, где встречается B , – это первая строка в перечне посылок. Фактически первая посылка позволила бы нам достичь цели, если бы мы только знали, что $y \in \bigcup \mathcal{F}$. Отсюда следует, что мы могли бы попытаться рассматривать $y \in \bigcup \mathcal{F}$ как нашу цель. Если мы сможем достичь этой цели, то нам останется добавить еще один шаг, применяя первую посылку, и доказательство будет завершено.

Посылки	Цель
$\bigcup \mathcal{F} \subseteq B$	
$x \in \mathcal{F}$	$y \in \bigcup \mathcal{F}$
$y \in x$	

И снова у нас есть цель, которую можно записать в логической форме, поэтому мы используем логическую форму цели, чтобы выбрать стратегию. Логическая запись цели имеет вид $\exists A \in \mathcal{F}(y \in A)$, и чтобы доказать ее, мы должны найти такое множество A , что $A \in \mathcal{F}$ и $y \in A$. Присмотревшись к посылкам, мы видим, что x является таким множеством, поэтому доказательство закончено.

Решение

Теорема. Предположим, что B – множество, а \mathcal{F} – семейство множеств. Если $\bigcup \mathcal{F} \subseteq B$, то $\mathcal{F} \subseteq \mathcal{P}(B)$.

Доказательство. Предположим, $\bigcup \mathcal{F} \subseteq B$. Пусть x – произвольный элемент \mathcal{F} . Пусть y – произвольный элемент x . Поскольку $y \in x$ и $x \in \mathcal{F}$, по определению $\bigcup \mathcal{F}, y \in \bigcup \mathcal{F}$. Но тогда, поскольку $\bigcup \mathcal{F} \subseteq B, y \in B$. Поскольку y был произвольным элементом x , мы можем заключить, что $x \subseteq B$, поэтому $x \in \mathcal{P}(B)$. Но x был произвольным элементом \mathcal{F} , следовательно, $\mathcal{F} \subseteq \mathcal{P}(B)$, что и требовалось доказать.

Диаграмма Венна на рис. 3.1 поможет вам понять, почему теорема из примера 3.3.5 верна, и мы рекомендуем обратиться к рисунку, когда вы перечитываете доказательство. Но обратите внимание, что мы не доказывали теорему, просто объясняя рисунок; доказательство было построено в соответствии со стратегиями. Существует множество приемов, таких как рисование картинок или предоставление примеров, способствующих пониманию того, почему теорема верна. Но формирование такого понимания еще не является доказательством. Чтобы доказать теорему, вы должны следовать стратегиям, описанным в этой главе.

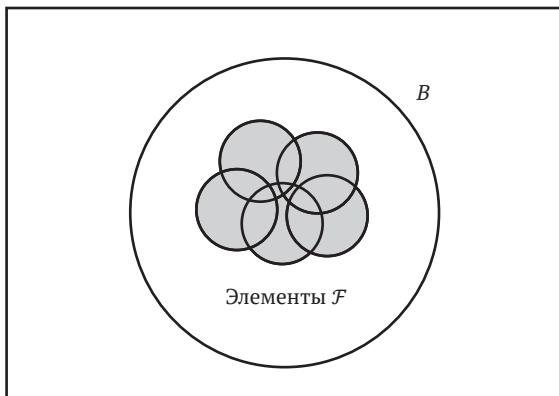


Рис. 3.1 ♦ Маленькие кружки представляют собой элементы \mathcal{F} , а закрашенная область – $\bigcup \mathcal{F}$. Большой кружок представляет B

Доказательство в примере 3.3.5, вероятно, является самым сложным доказательством из всех, которые мы разработали до сих пор. Прочтите его еще раз и убедитесь, что вы понимаете его структуру и цель каждого предложения. Разве не удивительно, как много сложной логики было упаковано всего в несколько строк?

Короткое доказательство нередко имеет такую богатую логическую структуру. Эта эффективность изложения является одной из самых привлекательных черт доказательств, но также часто делает их трудными для чтения. Хотя до сих пор мы концентрировались на *написании* доказательств, также важно научиться *читать* доказательства, написанные другими людьми. Чтобы дать вам немного попрактиковаться в этом, мы представляем наше последнее доказательство в этом разделе без предварительных рассуждений. Посмотрите, сможете ли вы следовать структуре доказательства, читая его. После доказательства мы предоставим комментарий, который поможет вам понять его.

Для этого доказательства нам понадобится следующее определение:

Определение 3.3.6. Для любых целых чисел x и y мы будем говорить, что x делит y (или y делится на x), если $\exists k \in \mathbb{Z} (kx = y)$. Запись $x | y$ означает « x делит y », а $x \nmid y$ означает « x не делит y ». Например, $4 | 20$, поскольку $5 \cdot 4 = 20$, но $4 \nmid 21$.

Теорема 3.3.7. Для всех целых чисел a, b и c если $a | b$ и $b | c$, то $a | c$.

Доказательство. Пусть a, b и c – произвольные целые числа, и пусть $a | b$ и $b | c$. Поскольку $a | b$, мы можем выбрать такое целое m , что $ma = b$. Аналогично, поскольку $b | c$, мы можем выбрать такое целое число n , что $nb = c$. Следовательно, $c = nb = nma$, и поскольку nm – целое число, то $a | c$.

Комментарий. В теореме говорится, что $\forall a \in \mathbb{Z} \forall b \in \mathbb{Z} \forall c \in \mathbb{Z} (a | b \wedge b | c \rightarrow a | c)$, поэтому наиболее естественный способ продолжить – объявить, что a, b и c – произвольные целые числа, предположить, что $a | b$ и $b | c$, а затем доказать, что $a | c$. Первое предложение доказательства указывает на использование этой стратегии, поэтому цель оставшейся части доказательства должна состоять в том, чтобы доказать, что $a | c$. Тот факт, что это цель остальной части доказательства, явно не указывается. Ожидается, что вы сами поймете это, применив свои знания о стратегиях доказательства. Возможно, вы даже захотите составить список посылок и целей, который поможет вам отслеживать то, что известно и что еще предстоит доказать, пока вы продолжаете читать доказательство. На этом этапе доказательства список будет выглядеть так:

Посылки	Цель
a, b и c – целые числа	
$a b$	
$b c$	$a c$

Поскольку новая цель означает $\exists k \in \mathbb{Z} (ka = c)$, доказательство можно продолжить путем нахождения целого числа k такого, что $ka = c$. Как и во многих доказательствах экзистенциальных утверждений, первый шаг в нахождении такого k включает более внимательное изучение посылок. В следующем предложении доказательства используется заданное $a | b$, чтобы сделать вывод, что мы можем выбрать такое целое число m , что $ma = b$. Доказательство не говорит, на каком правиле основан этот вывод. Догадайтесь об этом сами, разработав логическую форму данного утверждения $a | b$ на основании определения делимости. Поскольку это данное означает $\exists k \in \mathbb{Z} (ka = b)$, вы должны понимать, что используемое правило вывода – это экзистенциальное подтверждение. Экзистенциальное подтверждение также используется в следующем предложении доказательства, чтобы оправдать выбор целого числа n – такого, что $nb = c$. Уравнения $ma = b$ и $nb = c$ теперь могут быть добавлены к списку посылок.

Некоторые шаги также были пропущены в последнем предложении доказательства. Мы ожидали, что цель $a | c$ можно было бы доказать, найдя такое целое число k , что $ka = c$. Из уравнения $c = nma$ и того факта, что nm является целым числом, следует, что $k = nm$ подходит, но в доказательстве

явно не говорится, что это значение k используется; на самом деле переменная k вообще не фигурирует в доказательстве. Разумеется, переменная k не фигурирует и в формулировке теоремы. Читатель доказательства ожидает, что мы докажем, что $a \mid c$, путем нахождения целого числа, которое при умножении на a дает значение c , но исходя из формулировки теоремы у читателя нет причин ожидать, что этому целому числу будет присвоено имя k . Следовательно, присвоение этого имени целому числу nm не облегчило бы понимание доказательства, поэтому мы этого не сделали.

Упражнения

Примечание. Упражнения, отмеченные символом P_D , можно выполнять с помощью компьютерной программы Proof Designer, доступной для бесплатного скачивания в интернете.

- *1. В упражнении 7 раздела 2.2 вы использовали логические эквивалентности, чтобы показать, что $\exists x(P(x) \rightarrow Q(x))$ эквивалентно $\forall xP(x) \rightarrow \exists xQ(x)$. Теперь используйте методы этого раздела, чтобы доказать, что если $\exists x(P(x) \rightarrow Q(x))$ истинно, то $\forall xP(x) \rightarrow \exists xQ(x)$ истинно. (Примечание: другое направление эквивалентности доказать немного сложнее. См. упражнение 30 в разделе 3.5.)
2. Докажите, что если A и $B \setminus C$ не пересекаются, то $A \cap B \subseteq C$.
- *3. Докажите, что если $A \subseteq B \setminus C$, то A и C не пересекаются.
- P_D 4. Предположим, что $A \subseteq \mathcal{P}(A)$. Докажите, что $\mathcal{P}(A) \subseteq \mathcal{P}(\mathcal{P}(A))$.
5. Гипотеза теоремы, доказанной в упражнении 4, – это $A \subseteq \mathcal{P}(A)$.
 - (a) Можете ли вы придумать множество A , для которого эта гипотеза верна?
 - (b) Можете ли вы придумать множество A , для которого эта гипотеза *не* верна?
6. Предположим, что x – действительное число.
 - (a) Докажите, что если $x \neq 1$, то существует действительное число y такое, что $\frac{y+1}{y-2} = x$.
 - (b) Докажите, что если существует действительное число y такое, что $\frac{y+1}{y-2} = x$, то $x \neq 1$.
- *7. Докажите, что для любого действительного числа x , если $x > 2$, существует действительное число y такое, что $y + 1/y = x$.
- P_D 8. Докажите, что если \mathcal{F} – семейство множеств и $A \in \mathcal{F}$, то $A \subseteq \bigcup \mathcal{F}$.
- *9. Докажите, что если \mathcal{F} – семейство множеств и $A \in \mathcal{F}$, то $\bigcap \mathcal{F} \subseteq A$.
10. Пусть \mathcal{F} – непустое семейство множеств, B – множество и $\forall A \in \mathcal{F}(B \subseteq A)$. Докажите, что $B \subseteq \bigcap \mathcal{F}$.

11. Предположим, что \mathcal{F} – семейство множеств. Докажите, что если $\emptyset \in \mathcal{F}$, то $\bigcap \mathcal{F} = \emptyset$.
- P_D *12. Предположим, что \mathcal{F} и \mathcal{G} – семейства множеств. Докажите, что если $\mathcal{F} \subseteq \mathcal{G}$, то $\bigcup \mathcal{F} \subseteq \mathcal{G}$.
13. Предположим, что \mathcal{F} и \mathcal{G} – непустые семейства множеств. Докажите, что если $\mathcal{F} \subseteq \mathcal{G}$, то $\bigcap \mathcal{G} \subseteq \bigcap \mathcal{F}$.
- *14. Предположим, что $\{A_i \mid i \in I\}$ – индексированное семейство множеств. Докажите, что $\bigcup_{i \in I} \mathcal{P}(A_i) \subseteq \mathcal{P}(\bigcup_{i \in I} A_i)$. (Подсказка: сначала убедитесь, что вы помните значение всех символов!)
15. Предположим, что $\{A_i \mid i \in I\}$ – индексированное семейство множеств и $I = \emptyset$. Докажите, что $\bigcup_{i \in I} A_i \in \bigcup_{i \in I} \mathcal{P}(A_i)$.
- P_D 16. Докажите утверждение, обратное утверждению, доказанному в примере 3.3.5. Другими словами, докажите, что если $\mathcal{F} \subseteq \mathcal{P}(B)$, то $\bigcup \mathcal{F} \subseteq B$.
- *17. Предположим, что \mathcal{F} и \mathcal{G} – непустые семейства множеств, и каждый элемент \mathcal{F} является подмножеством каждого элемента \mathcal{G} . Докажите, что $\bigcup \mathcal{F} \subseteq \bigcap \mathcal{G}$.
18. В этой задаче все переменные имеют значение \mathbb{Z} , множество всех целых чисел.
- Докажите, что если $a \mid b$ и $a \mid c$, тогда $a \mid (b + c)$.
 - Докажите, что если $ac \mid bc$ и $c \neq 0$, то $a \mid b$.
19.
 - Докажите, что для всех действительных чисел x и y существует действительное число z такое, что $x + z = y - z$.
 - Будет ли утверждение в части (a) истинным, если «действительное число» заменить на «целое»? Обоснуйте ответ.
- *20. Рассмотрим следующую теорему.

Теорема. Для любого действительного числа x справедливо неравенство $x^2 \geq 0$.

Где ошибка в следующем доказательстве теоремы?

Доказательство. Предположим, что теорема неверна. Тогда для любого действительного числа x справедливо неравенство $x^2 < 0$. В частности, подставив $x = 3$, мы получим $9 < 0$, что явно неверно. Это противоречие показывает, что для любого числа x справедливо неравенство $x^2 \geq 0$.

21. Рассмотрим следующую ошибочную теорему.

Ошибкачная теорема. Если $\forall x \in A(x \neq 0)$ и $A \subseteq B$, то $\forall x \in B(x \neq 0)$.

(а) Где ошибка в следующем доказательстве теоремы?

Доказательство. Предположим, что $\forall x \in A(x \neq 0)$ и $A \subseteq B$. Пусть x – произвольный элемент A . Поскольку $\forall x \in A(x \neq 0)$, мы можем заключить, что $x \neq 0$. Кроме того, поскольку $A \subseteq B$, то $x \in B$. Поскольку $x \in B$, $x \neq 0$ и x – произвольный элемент, мы можем заключить, что $\forall x \in B(x \neq 0)$.

- (b) Найдите контрпример к теореме. Другими словами, найдите пример множеств A и B , для которых предположения теоремы верны, но вывод неверен.

*22. Рассмотрим следующую ошибочную теорему.

Ошибкачная теорема. $\exists x \in \mathbb{R} \forall y \in \mathbb{R} (xy^2 = y - x)$.

Где ошибка в следующем доказательстве теоремы?

Доказательство. Пусть $x = y / (y^2 + 1)$, тогда

$$y - x = y - \frac{y}{y^2 + 1} = \frac{y^3}{y^2 + 1} = \frac{y}{y^2 + 1} \cdot y^2 = xy^2.$$

23. Рассмотрим следующую ошибочную теорему.

Ошибкачная теорема. Предположим, что \mathcal{F} и \mathcal{G} – семейства множеств. Если $\bigcup \mathcal{F}$ и $\bigcup \mathcal{G}$ не пересекаются, то и \mathcal{F} и \mathcal{G} тоже не пересекаются.

- (a) Где ошибка в следующем доказательстве теоремы?

Доказательство. Предположим, что $\bigcup \mathcal{F}$ и $\bigcup \mathcal{G}$ не пересекаются. Предположим, что \mathcal{F} и \mathcal{G} не пересекаются. Тогда мы можем выбрать такое множество A , что $A \in \mathcal{F}$ и $A \in \mathcal{G}$. Поскольку $A \in \mathcal{F}$, согласно упражнению 8, $A \subseteq \bigcup \mathcal{F}$, поэтому каждый элемент A входит в $\bigcup \mathcal{F}$. Аналогично, поскольку $A \in \mathcal{G}$, каждый элемент A входит в $\bigcup \mathcal{G}$. Но тогда каждый элемент A входит как в $\bigcup \mathcal{F}$, так и в $\bigcup \mathcal{G}$, а это невозможно, поскольку $\bigcup \mathcal{F}$ и $\bigcup \mathcal{G}$ не пересекаются. Таким образом, мы пришли к противоречию, поэтому \mathcal{F} и \mathcal{G} не должны пересекаться.

- (b) Найдите контрпример к теореме.

24. Рассмотрим следующую предположительную теорему.

Предположительная теорема. Для всех действительных чисел x и y справедливо $x^2 + xy - 2y^2 = 0$.

- (a) Что не так в следующем доказательстве теоремы?

Доказательство. Пусть x и y равны некоторому произвольному действительному числу r . Тогда $x^2 + xy - 2y^2 = r^2 + r \cdot r - 2r^2 = 0$.

Поскольку x и y были произвольными, это показывает, что для всех действительных чисел x и y верно $x^2 + xy - 2y^2 = 0$.

- (b) Верна ли теорема? Обоснуйте свой ответ либо доказательством, либо контрпримером.

*25. Докажите, что для каждого действительного числа x существует действительное число y такое, что для любого действительного числа z верно $yz = (x + z)^2 - (x^2 + z^2)$.

26. (a) Сравнивая различные правила работы с кванторами в доказательствах, вы должны увидеть сходство между правилами для целей

в форме $\forall xP(x)$ и посылок в форме $\exists xP(x)$. В чем это сходство? Как насчет правил для целей в форме $\exists xP(x)$ и посылок в форме $\forall xP(x)$?

- (b) Можете ли вы назвать причину, по которой наблюдается такое сходство? (Подсказка: вспомните о том, как работает доказательство от противоречия, если цель начинается с квантора.)

3.4. ДОКАЗАТЕЛЬСТВА С ИСПОЛЬЗОВАНИЕМ КОНЪЮНКЦИЙ И РАВНОСИЛЬНОСТЕЙ

Метод доказательства цели вида $P \wedge Q$ очень прост.

Чтобы доказать цель вида $P \wedge Q$:

Докажите отдельно P и Q .

Другими словами, цель вида $P \wedge Q$ рассматривается как две отдельные цели P и Q . То же самое верно и для посылок вида $P \wedge Q$.

Чтобы использовать посылки вида $P \wedge Q$:

Используйте по отдельности посылки P и Q .

Мы уже использовали эти идеи без явного упоминания в некоторых из наших предыдущих примеров. Скажем, в примере 3.2.3 посылка $x \in A \setminus C$ была расписана как $x \in A \wedge x \notin C$, но мы рассматривали ее как две отдельные посылки $x \in A$ и $x \notin C$.

Пример 3.4.1. Предположим, что $A \subseteq B$ и A и C не пересекаются. Докажите, что $A \subseteq B \setminus C$.

Стратегия доказательства

Посылки	Цель
$A \subseteq B$	$A \subseteq B \setminus C$
$A \cap C = \emptyset$	

Логическая форма цели имеет вид $\forall x(x \in A \rightarrow x \in B \setminus C)$, поэтому пусть x будет произвольным, предположим $x \in A$ и попытаемся доказать, что $x \in B \setminus C$. Новая цель $x \in B \setminus C$ означает $x \in B \wedge x \notin C$, поэтому в соответствии с нашей стратегией мы должны разделить ее на две цели, $x \in B$ и $x \notin C$, и доказать их по отдельности.

Посылки	Цель
$A \subseteq B$	$x \in B$
$A \cap C = \emptyset$	$x \notin C$
$x \in A$	

Окончательное доказательство будет иметь следующий вид.

Пусть x будет произвольным элементом.

Предположим, что $x \in A$.

[Здесь помещаем доказательство $x \in B$.]

[Здесь помещаем доказательство $x \notin C$.]

Таким образом, $x \in B \wedge x \notin C$, поэтому $x \in B \setminus C$.

Следовательно, $x \in A \rightarrow x \in B \setminus C$.

Поскольку x – произвольный элемент, $\forall x(x \in A \rightarrow x \in B \setminus C)$, значит, $A \subseteq B \setminus C$.

Первая цель $x \in B$ явно следует из того факта, что $x \in A$ и $A \subseteq B$. Вторая цель, $x \notin C$, следует из $x \in A$ и $A \cap C = \emptyset$. Вы можете увидеть это, проанализировав логическую форму утверждения $A \cap C = \emptyset$. Это оператор отрицания, но его можно переписать как эквивалентный оператор утверждения:

$A \cap C = \emptyset$ эквивалентно $\neg \exists y(y \in A \wedge y \in C)$ (определения \cap и \emptyset),
что эквивалентно $\forall y(\neg(y \in A \wedge y \in C))$ (правило отрицания кванторов),
что эквивалентно $\forall y(y \notin A \vee y \notin C)$ (закон Де Моргана),
что эквивалентно $\forall y(y \in A \rightarrow y \notin C)$ (условный закон).

Подставляя x вместо y в этом последнем утверждении, мы видим, что $x \in A \rightarrow x \notin C$, и, поскольку мы уже знаем, что $x \in A$, мы можем заключить, что $x \notin C$.

Решение

Теорема. Предположим, что $A \subseteq B$ и A и C не пересекаются. Тогда $A \subseteq B \setminus C$.

Доказательство. Предположим, что $x \in A$. Поскольку $A \subseteq B$, отсюда следует, что $x \in B$, и поскольку A и C не пересекаются, справедливо $x \notin C$. Таким образом, $x \in B \setminus C$. Поскольку x был произвольным элементом A , мы заключаем, что $A \subseteq B \setminus C$.

Используя наши стратегии работы с конъюнкциями, мы теперь можем выработать правильный способ работы с биусловными утверждениями или равносильностями вида $P \leftrightarrow Q$ при составлении доказательства. Поскольку $P \leftrightarrow Q$ равносильно $(P \rightarrow Q) \wedge (Q \rightarrow P)$, в соответствии с нашими стратегиями посылку или цель вида $P \leftrightarrow Q$ следует рассматривать как две отдельные посылки или цели: $P \rightarrow Q$ и $Q \rightarrow P$.

Чтобы доказать цель вида $P \leftrightarrow Q$:

Докажите отдельно $P \rightarrow Q$ и $Q \rightarrow P$.

Чтобы использовать посылку в форме $P \leftrightarrow Q$:

Считайте ее двумя отдельными посылками $P \rightarrow Q$ и $Q \rightarrow P$.

Эти стратегии проиллюстрированы в следующем примере, в котором мы используем новые определения.

Определение 3.4.2. Целое число x является четным, если $\exists k \in \mathbb{Z}(x = 2k)$, и нечетным, если $\exists k \in \mathbb{Z}(x = 2k + 1)$.

Мы также используем тот факт, что каждое целое число либо четное, либо нечетное, но не то и другое одновременно. Доказательство этого факта см. в упражнении 16 в разделе 6.1.

Пример 3.4.3. Предположим, что x – целое число. Докажите, что x четно тогда и только тогда, когда x^2 четно.

Рассуждение

Цель (x четно) \leftrightarrow (x^2 четно), поэтому мы докажем две цели (x четно) \rightarrow (x^2 четно) и (x^2 четно) \rightarrow (x четно) по отдельности. Сначала предположим, что x четно, и докажем, что x^2 четно:

Посылки	Цель
$x \in \mathbb{Z}$	x^2 четно
x четно	

Подстановка определения четности в посылку и в цель раскроет их логические формы:

Посылки	Цель
$x \in \mathbb{Z}$	$\exists k \in \mathbb{Z}(x^2 = 2k)$
$\exists k \in \mathbb{Z}(x = 2k)$	

Поскольку вторая посылка начинается с $\exists k$, мы немедленно используем ее, и пусть k обозначает какое-то конкретное целое число, для которого истинно утверждение $x = 2k$. Таким образом, у нас есть два новых исходных утверждения: $k \in \mathbb{Z}$ и $x = 2k$.

Посылки	Цель
$x \in \mathbb{Z}$	$\exists k \in \mathbb{Z}(x^2 = 2k)$
$k \in \mathbb{Z}$	
$x = 2k$	

Цель начинается с $\exists k$, но поскольку k уже используется для обозначения определенного числа, мы не можем присвоить k новое значение для доказательства цели. Поэтому мы должны использовать другую букву, скажем j . Однако нам недостаточно переписать цель в эквивалентной форме $\exists j \in \mathbb{Z}(j^2 = 2j)$. Чтобы доказать эту цель, мы должны придумать значение для j . Оно должно быть целым числом и удовлетворять уравнению $x^2 = 2j$. Исходя из посылки $x = 2k$, мы видим, что $x^2 = (2k)^2 = 4k^2 = 2(2k^2)$, поэтому похоже, что правильным значением является $j = 2k^2$. Очевидно, что $2k^2$ – целое число, поэтому данное значение j подходит для завершения доказательства нашей первой цели.

Чтобы доказать вторую цель (x^2 четно) \rightarrow (x четно), мы докажем вместо этого контрапозицию (x нечетно) \rightarrow (x^2 нечетно). Поскольку любое целое число является четным или нечетным, но не тем и другим сразу, это равносильно утверждению (x нечетно) \rightarrow (x^2 нечетно).

Посылки	Цель
$x \in \mathbb{Z}$	x^2 нечетно
x нечетно	

Последующие шаги теперь очень похожи на первую часть доказательства. Как и раньше, мы начнем с написания определения нечетного числа как во второй посылке, так и в цели. На этот раз, чтобы избежать конфликта имен переменных, с которым мы столкнулись в первой части доказательства, мы используем разные имена для связанных переменных в двух утверждениях.

Посылки	Цель
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z} (x^2 = 2j + 1)$
$\exists k \in \mathbb{Z} (x = 2k + 1)$	

Затем мы воспользуемся второй посылкой, и пусть k обозначает конкретное целое число, для которого $x = 2k + 1$.

Посылки	Цель
$x \in \mathbb{Z}$	$\exists j \in \mathbb{Z} (x^2 = 2j + 1)$
$k \in \mathbb{Z}$	
$x = 2k + 1$	

Теперь мы должны найти целое число j такое, что $x^2 = 2j + 1$. Подставляя $2k + 1$ вместо x , мы получаем $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, поэтому $j = 2k^2 + 2k$ выглядит правильным выбором.

Прежде чем дать окончательное изложение доказательства, сделаем несколько пояснений. Два условных утверждения, которые мы доказали, можно рассматривать как представление двух направлений \rightarrow и \leftarrow биусловного оператора \leftrightarrow в исходной цели. Эти две части доказательства иногда обозначаются символами \rightarrow и \leftarrow . Мы заканчиваем каждую часть доказательством утверждения, которое заявляет о существовании числа с определенными свойствами. Мы обозначили это число буквой j в рассуждении, но заметим, что j не упоминается явно в формулировке задачи. Как и в доказательстве теоремы 3.3.7, мы решили не упоминать j явно и в окончательном доказательстве.

Решение

Теорема. Предположим, что x – целое число. Это число x четно тогда и только тогда, когда x^2 четно.

Доказательство. (\rightarrow) Предположим, что x четно. Тогда для некоторого целого k выполняется $x = 2k$. Следовательно, $x^2 = 4k^2 = 2(2k^2)$, поэтому, поскольку $2k^2$ – целое число, x^2 четно. Таким образом, если x четно, то x^2 четно.

(\leftarrow) Предположим, что x нечетно. Тогда $x = 2k + 1$ для некоторого целого k . Следовательно, $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, поэтому, поскольку $2k^2 + 2k$ – целое число, x^2 нечетно. Таким образом, если x^2 четно, то x четно.

Используя разработанные нами методы доказательства, теперь мы можем проверить некоторые из равносильностей, которые в главе 2 мы смогли обосновать только на интуитивном уровне. В качестве примера давайте докажем, что формулы $\forall x\neg P(x)$ и $\neg\exists xP(x)$ равносильны. Утверждение, что эти формулы равносильны, означает, что они всегда будут иметь одинаковое значение истинности. Другими словами, независимо от того, какое утверждение обозначает запись $P(x)$, утверждение $\forall x\neg P(x) \leftrightarrow \neg\exists xP(x)$ будет истинным. Мы можем доказать это, используя нашу технику доказательства биусловных утверждений.

Пример 3.4.4. Докажите, что $\forall x\neg P(x) \leftrightarrow \neg\exists xP(x)$.

Стратегия доказательства

(\rightarrow) Мы должны доказать $\forall x\neg P(x) \leftrightarrow \neg\exists xP(x)$, поэтому мы принимаем $\forall x\neg P(x)$ и пытаемся доказать $\neg\exists xP(x)$. Наша цель теперь – утверждение с отрицанием, и попытка его переписать потребует использования той самой равносильности, которую мы пытаемся доказать!

Поэтому мы прибегаем к нашей единственной оставшейся стратегии борьбы с целями, содержащими отрицание, доказывая их через противоречие. Теперь у нас есть следующая ситуация:

Посылки	Цель
$\forall x\neg P(x)$	Противоречие
$\exists xP(x)$	

Вторая посылка начинается с квантора существования, поэтому мы сразу же используем ее и через x_0 обозначаем некоторый объект, для которого верно утверждение $P(x_0)$. Но теперь, подставляя x_0 вместо x в первую посылку, мы получаем $\neg P(x_0)$, что дает нам необходимое противоречие.

(\leftarrow) Для этого направления биусловия мы должны принять $\neg\exists xP(x)$ и попытаться доказать $\forall x\neg P(x)$. Поскольку эта цель начинается с универсального квантора, мы обозначаем через x произвольный элемент и пытаемся доказать $\neg P(x)$. И снова у нас есть отрицаемая цель, которую нельзя выразить иначе, поэтому мы используем доказательство через противоречие:

Посылки	Цель
$\neg\exists xP(x)$	Противоречие
$P(x)$	

Наша первая посылка также является отрицаемым утверждением, и это предполагает, что мы можем получить нужное противоречие, доказав $\exists xP(x)$. Назначим это своей целью.

Посылки	Цель
$\neg\exists xP(x)$	$\exists xP(x)$
$P(x)$	

Чтобы не путать x , который появляется как свободная переменная во второй посылке (произвольный элемент x , введенный ранее в доказательстве), с x , который присутствует как связанная переменная в цели, вам следует переписать цель в эквивалентной форме $\exists y P(y)$. Чтобы доказать эту цель, мы должны найти значение y , при котором $P(y)$ станет истинным. Но это просто! Вторая посылка, $P(x)$, говорит нам, что произвольный x – именно то значение, которое нам нужно.

Решение

Теорема. $\forall x \neg P(x) \leftrightarrow \neg \exists x P(x)$.

Доказательство. (\rightarrow) Предположим, что $\forall x \neg P(x)$, и предположим, что $\exists x P(x)$. Тогда мы можем выбрать некоторое значение x_0 такое, что $P(x_0)$ истинно. Но поскольку $\forall x \neg P(x)$, мы можем заключить, что $\neg P(x_0)$, и это противоречие. Следовательно, $\forall x \neg P(x) \rightarrow \neg \exists x P(x)$.

(\leftarrow) Предположим, $\neg \exists x P(x)$. Пусть x имеет произвольное значение, и пусть $P(x)$. Поскольку у нас есть конкретный x , для которого верно $P(x)$, следует, что $\exists x P(x)$, а это противоречие. Следовательно, $\neg P(x)$. Поскольку x был произвольным, мы можем заключить, что $\forall x \neg P(x)$, поэтому $\neg \exists x P(x) \rightarrow \forall x \neg P(x)$.

Иногда при доказательстве цели вида $P \leftrightarrow Q$ шаги в доказательстве $Q \rightarrow P$ такие же, как шаги, используемые для доказательства $P \rightarrow Q$, но в обратном порядке. В этом случае вы можете упростить доказательство, записав его в виде строки эквивалентностей, начиная с P и заканчивая Q . Например, предположим, что вы обнаружили, что можете доказать $P \rightarrow Q$, сначала предположив P , а затем из P вывести какое-то другое утверждение R и далее использовать R , чтобы вывести Q ; и предположим, что те же шаги в обратном порядке можно использовать для доказательства того, что $Q \rightarrow P$. Другими словами, вы можете предположить Q , использовать это предположение, чтобы сделать вывод, что R истинно, а затем использовать R , чтобы доказать P . Поскольку вы утверждали как $P \rightarrow R$, так и $R \rightarrow P$, вы можете суммировать эти два шага, заявив $P \leftrightarrow R$. Аналогично, два других шага доказательства говорят вам, что $R \leftrightarrow Q$. Эти два утверждения означают, что доказана цель $P \leftrightarrow Q$. Математики иногда приводят такого рода доказательства, просто записывая строку равносильностей:

P тогда и только тогда, когда R тогда и только тогда, когда Q .

Это сокращенная запись строки « P , если и только если R и R , если и только если Q (и, следовательно, P , если и только если Q)». Это показано в следующем примере.

Пример 3.4.5. Предположим, что A , B и C – множества. Докажите, что $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Стратегия доказательства

Как мы видели в главе 2, уравнение $A \cap (B \setminus C) = (A \cap B) \setminus C$ означает $\forall x (x \in A \cap (B \setminus C) \leftrightarrow x \in (A \cap B) \setminus C)$, но оно также эквивалентно утверждению $[A \cap$

$(B \setminus C) \subseteq (A \cap B) \setminus C] \wedge [(A \cap B) \setminus C \subseteq A \cap (B \setminus C)]$. Это предполагает два подхода к доказательству. Мы могли бы обозначить через x произвольный элемент, а затем доказать $x \in A \cap (B \setminus C) \leftrightarrow x \in (A \cap B) \setminus C$, или мы могли бы доказать два утверждения $A \cap (B \setminus C) \subseteq (A \cap B) \setminus C$ и $(A \cap B) \setminus C \subseteq A \cap (B \setminus C)$. Фактически почти каждое доказательство равенства двух множеств будет включать один из этих двух подходов. В данном случае мы будем использовать первый подход, поэтому, как только мы введем произвольный x , у нас будет цель вида «если и только если».

В первой половине доказательства (\rightarrow) мы предполагаем, что $x \in A \cap (B \setminus C)$, и пытаемся доказать $x \in (A \cap B) \setminus C$:

Посылки	Цель
$x \in A \cap (B \setminus C)$	$x \in (A \cap B) \setminus C$

Чтобы получить логические формы посылки и цели, запишем их определения следующим образом:

$x \in A \cap (B \setminus C)$, если и только если $x \in A \wedge x \in B \setminus C$, если и только если
 $x \in A \wedge x \in B \wedge x \notin C$;

$x \in (A \cap B) \setminus C$, если и только если $x \in A \cap B \wedge x \notin C$, если и только если
 $x \in A \wedge x \in B \wedge x \notin C$.

Здесь ясно, что посылка определяет цель, поскольку последние шаги в обеих строках эквивалентностей оказались идентичными. Фактически также ясно, что рассуждения, связанные со вторым направлением доказательства (\leftarrow), будут точно такими же, только столбцы посылок и цели поменяются местами. Таким образом, мы могли бы попытаться сократить доказательство, записав его в виде строки равносильностей, начиная с $x \in A \cap (B \setminus C)$ и заканчивая $x \in (A \cap B) \setminus C$. В этом случае, если мы начнем с $x \in A \cap (B \setminus C)$ и следуя первой строке эквивалентностей, показанной выше, мы приходим к утверждению, которое совпадает с последним утверждением во второй строке. Затем мы можем продолжить, проследив вторую строку равносильностей назад до $x \in (A \cap B) \setminus C$.

Решение

Теорема. Предположим, что A , B и C – множества. Тогда $A \cap (B \setminus C) = (A \cap B) \setminus C$.

Доказательство. Пусть x – произвольный элемент. Тогда

$x \in A \cap (B \setminus C)$, если и только если $x \in A \wedge x \in B \setminus C$,
если и только если $x \in A \wedge x \in B \wedge x \notin C$,
если и только если $x \in (A \cap B) \wedge x \notin C$,
если и только если $x \in (A \cap B) \setminus C$.

Таким образом, $\forall x(x \in A \cap (B \setminus C) \leftrightarrow x \in (A \cap B) \setminus C)$, следовательно, $A \cap (B \setminus C) = (A \cap B) \setminus C$.

В доказательствах довольно часто используется методика записи последовательности равносильностей в одном порядке с последующей ее записью

в обратном порядке. Порядок, в котором должны быть записаны шаги в окончательном доказательстве, определяется нашим правилом, согласно которому утверждение никогда не следует делать, пока оно не будет обосновано. В частности, если вы пытаетесь доказать $P \leftrightarrow Q$, было бы неправильно начинать описание доказательства с неоправданного утверждения $P \leftrightarrow Q$, а затем выяснять значения двух сторон P и Q , показывая, что они одинаковые. Вместо этого вам следует начать с равносильностей, которые вы можете обосновать, и связать их вместе, чтобы получить обоснование цели $P \leftrightarrow Q$, прежде чем вы будете это утверждать. Подобный метод иногда можно использовать для получения доказательств уравнений, как показывает следующий пример.

Пример 3.4.6. Докажите, что для любых действительных чисел a и b справедливо

$$(a + b)^2 - 4(a - b)^2 = (3b - a)(3a - b).$$

Стратегия доказательства

Цель имеет вид $\forall a \forall b ((a + b)^2 - 4(a - b)^2 = (3b - a)(3a - b))$, поэтому мы начнем с того, что a и b – произвольные действительные числа, и попытаемся доказать уравнение. Выполнив умножение с обеих сторон, мы получим:

$$\begin{aligned}(a + b)^2 - 4(a - b)^2 &= a^2 + 2ab + b^2 - 4(a^2 - 2ab + b^2) \\ &= -3a^2 + 10ab - 3b^2;\end{aligned}$$

$$(3b - a)(3a - b) = 9ab - 3a^2 - 3b^2 + ab = -3a^2 + 10ab - 3b^2.$$

Очевидно, что обе стороны равны. Самый простой способ сформулировать доказательство этого – написать строку равенств, начинающуюся с $(a + b)^2 - 4(a - b)^2$ и заканчивающуюся $(3b - a)(3a - b)$. Мы можем сделать это, скопировав первую строку равенств, показанных выше, а затем продолжив ее последней строкой, записанной в обратном порядке.

Решение

Теорема. Для любых действительных чисел a и b справедливо уравнение

$$(a + b)^2 - 4(a - b)^2 = (3b - a)(3a - b).$$

Доказательство. Пусть a и b – произвольные действительные числа. Тогда

$$\begin{aligned}(a + b)^2 - 4(a - b)^2 &= a^2 + 2ab + b^2 - 4(a^2 - 2ab + b^2) \\ &= -3a^2 + 10ab - 3b^2 \\ &= 9ab - 3a^2 - 3b^2 + ab = (3b - a)(3a - b).\end{aligned}$$

В конце этого раздела мы представим еще одно доказательство без предварительных рассуждений, но с комментарием, который поможет вам прочитать доказательство.

Теорема 3.4.7. Для каждого целого n справедливо утверждение $6 \mid n$, если и только если $2 \mid n$ и $3 \mid n$.

Доказательство. Пусть n – произвольное целое число.

(\rightarrow) Предположим, что $6 \mid n$. Тогда мы можем выбрать такое целое число k , что $6k = n$. Следовательно, $n = 6k = 2(3k)$, поэтому $2 \mid n$, и аналогично $n = 6k = 3(2k)$, поэтому $3 \mid n$.

(\leftarrow) Предположим, $2 \mid n$ и $3 \mid n$. Тогда мы можем выбрать целые числа j и k такие, что $n = 2j$ и $n = 3k$. Следовательно, $6(j - k) = 6j - 6k = 3(2j) - 2(3k) = 3n - 2n = n$, поэтому $6 \mid n$.

Комментарий. Мы доказываем утверждение $\forall n \in \mathbb{Z} [6 \mid n \leftrightarrow ((2 \mid n) \wedge (3 \mid n))]$, и наиболее естественная стратегия для доказательства цели в такой форме состоит в том, чтобы объявить значение n произвольным, а затем по отдельности доказать оба направления биусловия. Очевидно, что это наиболее подходящая и простая стратегия доказательства.

Для доказательства биусловного утверждения слева направо полагаем $6 \mid n$, а затем доказываем $2 \mid n$ и $3 \mid n$, рассматривая их как две отдельные цели. Введение целого числа k оправдано экзистенциальным подтверждением, поскольку предположение $6 \mid n$ означает $\exists k \in \mathbb{Z} (6k = n)$. На этом этапе доказательства у нас есть следующие посылки и цели:

Посылки	Цель
$n \in \mathbb{Z}$	$2 \mid n$
$k \in \mathbb{Z}$	$3 \mid n$
$6k = n$	

Первая цель $2 \mid n$ означает $\exists j \in \mathbb{Z} (2j = n)$, поэтому мы должны найти такое целое число j , что $2j = n$. Хотя доказательство не говорит об этом явно, уравнение $n = 2(3k)$, которое выводится в доказательстве, предполагает, что мы используем значение $j = 3k$. Ясно, что $3k$ – целое число (этот шаг в доказательстве тоже пропущен), поэтому такой выбор j вполне обоснован. Доказательство $3 \mid n$ работает аналогично.

Для доказательства в обратном направлении полагаем $2 \mid n$ и $3 \mid n$ и доказываем $6 \mid n$. Повторим, что введение j и k оправдано экзистенциальным подтверждением. Никакого объяснения того, почему мы должны вычислить $6(j - k)$, не дается, но доказательство и не требует таких объяснений. Причина вычисления станет очевидной, когда, к удивлению читателя, выяснится, что $6(j - k) = n$. Такие сюрпризы приносят удовольствие от работы с доказательствами. Как и в первой половине доказательства, поскольку $j - k$ – целое число, это показывает, что $6 \mid n$.

Упражнения

*1. Используйте методы этой главы, чтобы доказать, что $\forall x(P(x) \wedge Q(x))$ равносильно $\forall xP(x) \wedge \forall xQ(x)$.

P_D2. Докажите, что если $A \subseteq B$ и $A \subseteq C$, то $A \subseteq B \cap C$.

P_D3. Предположим, $A \subseteq B$. Докажите, что для любого множества C справедливо $C \setminus B \subseteq C \setminus A$.

- P_D*4. Докажите, что если $A \subseteq B$ и $A \not\subseteq C$, то $B \not\subseteq C$.
- P_D5. Докажите, что если $A \subseteq B \setminus C$ и $A \neq \emptyset$, то $B \not\subseteq C$.
6. Докажите, что для любых множеств A, B и C справедливо $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$, найдя строку равносильностей, начинающуюся с $x \in A \setminus (B \cap C)$ и заканчивающуюся $x \in (A \setminus B) \cup (A \setminus C)$ (см. пример 3.4.5).
- P_D*7. Используйте методы этой главы, чтобы доказать, что для любых множеств A и B справедливо $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.
- P_D8. Докажите, что $A \subseteq B$ тогда и только тогда, когда $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.
- *9. Докажите, что если x и y – нечетные целые числа, то xy – нечетное.
10. Докажите, что если x и y – нечетные целые числа, то $x - y$ – четное.
11. Докажите, что для любого целого n , n^3 четно тогда и только тогда, когда n четно.
12. Рассмотрим следующую предположительную теорему.

Предположительная теорема. Предположим, что m – четное целое число, а n – нечетное целое число. Тогда $n^2 - m^2 = n + m$.

(a) Что не так в следующем доказательстве теоремы?

Доказательство. Поскольку m четно, мы можем выбрать некоторое целое k такое, что $m = 2k$. Аналогично, поскольку n нечетно, имеем $n = 2k + 1$. Следовательно, $n^2 - m^2 = (2k + 1)^2 - (2k)^2 = 4k^2 + 4k + 1 - 4k^2 = 4k + 1 = (2k + 1) + (2k) = n + m$.

(b) Верна ли теорема? Обоснуйте свой ответ либо доказательством, либо контрпримером.

- *13. Докажите, что $\forall x \in \mathbb{R} [\exists y \in \mathbb{R} (x + y = xy) \leftrightarrow x = 1]$.
14. Докажите, что $\exists z \in \mathbb{R} \forall x \in \mathbb{R}^+ [\exists y \in \mathbb{R} (y - x = y/x) \leftrightarrow x = z]$.
- P_D15. Предположим, что B – множество, а \mathcal{F} – семейство множеств. Докажите, что $\bigcup \{A \setminus B \mid A \in \mathcal{F}\} \subseteq \bigcup (\mathcal{F} \setminus \mathcal{P}(B))$.
- *16. Предположим, что \mathcal{F} и \mathcal{G} – непустые семейства множеств и каждый элемент \mathcal{F} не пересекается с некоторым элементом \mathcal{G} . Докажите, что $\bigcup \mathcal{F}$ и $\bigcap \mathcal{G}$ не пересекаются.

P_D17. Докажите, что для любого множества A справедливо $A = \bigcup \mathcal{P}(A)$.

P₀*18. Предположим, что \mathcal{F} и \mathcal{G} – семейства множеств.

(a) Докажите, что $\bigcup (\mathcal{F} \cap \mathcal{G}) \subseteq (\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G})$.

(b) Где ошибка в следующем доказательстве утверждения: $(\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G}) \subseteq \bigcup (\mathcal{F} \cap \mathcal{G})$?

Доказательство. Предположим, что $x \in (\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G})$. Это означает, что $x \in \bigcup \mathcal{F}$ и $x \in \bigcup \mathcal{G}$, поэтому $\exists A \in \mathcal{F} (x \in A)$ и $\exists A \in \mathcal{G} (x \in A)$. Таким образом, мы можем выбрать множество A такое, что $A \in \mathcal{F}, A \in \mathcal{G}$ и $x \in A$. Поскольку $A \in \mathcal{F}$ и $A \in \mathcal{G}$, то $A \in \mathcal{F} \cap \mathcal{G}$. Следовательно, $\exists A \in \mathcal{F} \cap \mathcal{G} (x \in A)$, поэтому $x \in \bigcup (\mathcal{F} \cap \mathcal{G})$.

$\cap \mathcal{G}$). Поскольку x было произвольным, мы можем заключить, что $(\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G}) \subseteq \bigcup(\mathcal{F} \cap \mathcal{G})$.

(c) Найдите пример семейств мноожеств \mathcal{F} и \mathcal{G} , для которых $\bigcup(\mathcal{F} \cap \mathcal{G}) \neq (\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G})$.

P_D19. Предположим, что \mathcal{F} и \mathcal{G} – семейства множеств. Докажите, что $(\bigcup \mathcal{F}) \cap (\bigcup \mathcal{G}) \subseteq \bigcup(\mathcal{F} \cap \mathcal{G})$, если и только если $\forall A \in \mathcal{F} \ \forall B \in \mathcal{G} (A \cap B \subseteq \bigcup(\mathcal{F} \cap \mathcal{G}))$.

P_D20. Предположим, что \mathcal{F} и \mathcal{G} – семейства множеств. Докажите, что $\bigcup \mathcal{F}$ и $\bigcup \mathcal{G}$ не пересекаются тогда и только тогда, когда для всех $A \in \mathcal{F}$ и $B \in \mathcal{G}$ A и B не пересекаются.

P_D21. Предположим, что \mathcal{F} и \mathcal{G} – семейства множеств.

(a) Докажите, что $(\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G}) \subseteq \bigcup(\mathcal{F} \setminus \mathcal{G})$.

(b) Где ошибка в следующем доказательстве того, что $\bigcup(\mathcal{F} \setminus \mathcal{G}) \subseteq (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$?

Доказательство. Предположим, что $x \in \bigcup(\mathcal{F} \setminus \mathcal{G})$. Тогда мы можем выбрать некоторое множество $A \in \mathcal{F} \setminus \mathcal{G}$ такое, что $x \in A$. Поскольку $A \in \mathcal{F} \setminus \mathcal{G}$, это значит, что $A \in \mathcal{F}$ и $A \notin \mathcal{G}$. Поскольку $x \in A$ и $A \in \mathcal{F}$, то $x \in \bigcup \mathcal{F}$. Поскольку $x \in A$ и $A \notin \mathcal{G}$, то $x \notin \bigcup \mathcal{G}$. Следовательно, $x \in (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$.

(c) Докажите, что $\bigcup(\mathcal{F} \setminus \mathcal{G}) \subseteq (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$, если и только если $\forall A \in (\mathcal{F} \setminus \mathcal{G}) \forall B \in \mathcal{G} (A \cap B = \emptyset)$.

(d) Найдите пример семейств мноожеств \mathcal{F} и \mathcal{G} , для которых $\bigcup(\mathcal{F} \setminus \mathcal{G}) \neq (\bigcup \mathcal{F}) \setminus (\bigcup \mathcal{G})$.

P_D*22. Предположим, что \mathcal{F} и \mathcal{G} – семейства множеств. Докажите, что если $\bigcup \mathcal{F} \cup \bigcup \mathcal{G}$, то существует $A \in \mathcal{F}$ такое, что для всех $B \in \mathcal{G}$ справедливо $A \cup B$.

23. Предположим, что B – множество, $\{A_i \mid i \in I\}$ – индексированное семейство множеств, а $I \neq \emptyset$.

(a) Какие стратегии используются в следующем доказательстве уравнения $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$?

Доказательство. Пусть x – произвольный объект. Предположим, что $x \in B \cap (\bigcup_{i \in I} A_i)$. Тогда $x \in B$ и $x \in \bigcup_{i \in I} A_i$, так что мы можем выбрать некоторое $i_0 \in I$ такое, что $x \in A_{i_0}$. Поскольку $x \in B$ и $x \in A_{i_0}$, то $x \in B \cap A_{i_0}$. Следовательно, $x \in \bigcup_{i \in I} (B \cap A_i)$.

Теперь предположим, что $x \in \bigcup_{i \in I} (B \cap A_i)$. Тогда мы можем выбрать $i_0 \in I$ такое, что $x \in B \cap A_{i_0}$. Следовательно, $x \in B$ и $x \in A_{i_0}$. Поскольку $x \in A_{i_0}$, то $x \in \bigcup_{i \in I} A_i$. Поскольку $x \in B$ и $x \in \bigcup_{i \in I} A_i$, то $x \in B \cap (\bigcup_{i \in I} A_i)$.

Так как x взят произвольно, мы показали, что $\forall x [x \in B \cap (\bigcup_{i \in I} A_i) \leftrightarrow x \in \bigcup_{i \in I} (B \cap A_i)]$, следовательно, $B \cap (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \cap A_i)$.

(b) Докажите, что $B \setminus (\bigcup_{i \in I} A_i) = \bigcup_{i \in I} (B \setminus A_i)$.

(c) Можете ли вы сформулировать и доказать аналогичную теорему о $B \setminus (\bigcup_{i \in I} A_i)$? (Подсказка: попробуйте предположить теорему, а затем попытайтесь ее доказать. Если вы не можете закончить доказательство, возможно, ваша догадка была неверной. Измените свое предположение и попробуйте еще раз.)

- *24. Предположим, что $\{A_i \mid i \in I\}$ и $\{B_i \mid i \in I\}$ – это индексированные семейства множеств и $I \neq \emptyset$.
- Докажите, что $\bigcup_{i \in I} (A_i \setminus B_i) \subseteq (\bigcup_{i \in I} A_i) \setminus (\bigcup_{i \in I} B_i)$.
 - Найдите пример, для которого $\bigcup_{i \in I} (A_i \setminus B_i) \neq (\bigcup_{i \in I} A_i) \setminus (\bigcup_{i \in I} B_i)$.
25. Предположим, что $\{A_i \mid i \in I\}$ и $\{B_i \mid i \in I\}$ – индексированные семейства множеств.
- Докажите, что $\bigcup_{i \in I} (A_i \cap B_i) \subseteq (\bigcup_{i \in I} A_i) \cap (\bigcup_{i \in I} B_i)$.
 - Найдите пример, для которого $\bigcup_{i \in I} (A_i \cap B_i) \neq (\bigcup_{i \in I} A_i) \cap (\bigcup_{i \in I} B_i)$.
26. Докажите, что для всех целых чисел a и b существует такое целое число c , что $a \mid c$ и $b \mid c$.
27. (a) Докажите, что для любого целого n выполняется условие: $15 \mid n$, если и только если $3 \mid n$ и $5 \mid n$.
- (b) Докажите, что для любого целого n выполняется условие: $60 \mid n$, если и только если $6 \mid n$ и $10 \mid n$.

3.5 ДОКАЗАТЕЛЬСТВО ДИЗЬЮНКЦИЙ

Предположим, что одна из ваших исходных посылок в доказательстве имеет форму $P \vee Q$. Такая запись говорит вам, что либо P , либо Q истинно, и ничего более конкретного. Таким образом, вы должны принять во внимание два варианта. Один из способов провести доказательство – рассмотреть эти два варианта по очереди. Другими словами, сначала предположите, что утверждение P истинно, и используйте это предположение для доказательства своей цели. Затем предположите, что Q истинно, и найдите еще одно доказательство того, что цель истинна. Хотя вы не знаете, какое из двух предположений истинно, исходная гипотеза $P \vee Q$ говорит вам, что одно из них обязательно должно быть истинным. Какой бы из вариантов вы ни доказали, это означает доказательство цели. Следовательно, цель должна быть истинной в любом случае.

Две возможности, которые рассматриваются по отдельности в этом типе доказательства, – возможность того, что утверждение P истинно, и того, что утверждение Q истинно, – называются *случаями*. Исходная посылка $P \vee Q$ объединяет два случая, гарантируя, что они охватывают все возможности. В такой ситуации математики говорят, что случаи *исчерпывающие*. Если случаи являются исчерпывающими, доказательство можно в любой момент разбить на два случая или более.

Чтобы использовать посылки в форме $P \vee Q$:

Разбейте доказательство на случаи. Для случая 1 предположите, что утверждение P истинно, и используйте это предположение для доказательства цели. Для случая 2 предположите, что утверждение Q истинно, и приведите другое доказательство цели.

Стратегия доказательства

Перед использованием стратегии:

<i>Посылки</i>	<i>Цель</i>
$P \vee Q$	–
–	

После использования стратегии:

Случай 1:	<i>Посылки</i>	<i>Цель</i>
	P	–
	–	
Случай 2:	<i>Посылки</i>	<i>Цель</i>
	Q	–
	–	

Форма окончательного доказательства

Случай 1. Утверждение P истинно.

[Здесь приводится доказательство цели.]

Случай 2. Утверждение Q истинно.

[Здесь приводится доказательство цели.]

Поскольку мы знаем, что $P \vee Q$, эти случаи покрывают все возможные варианты. Следовательно, цель должна быть истинной.

Пример 3.5.1. Предположим, что A, B и C – множества. Докажите, что если $A \subseteq C$ и $B \subseteq C$, то $A \cup B \subseteq C$.

Стратегия доказательства

Предположим, что $A \subseteq C$ и $B \subseteq C$, и докажем, что $A \cup B \subseteq C$. Запись цели в логической форме дает нам следующие посылки и цель:

<i>Посылки</i>	<i>Цель</i>
$A \subseteq C$	$\forall x(x \in A \cup B \rightarrow x \in C)$
$B \subseteq C$	

Пусть x будет произвольным, предположим, что $x \in A \cup B$, и попытаемся доказать $x \in C$. Таким образом, теперь у нас есть новая посылка $x \in A \cup B$, которую мы записываем как $x \in A \vee x \in B$, а наша цель теперь – $x \in C$.

<i>Посылки</i>	<i>Цель</i>
$A \subseteq C$	$x \in C$
$B \subseteq C$	
$x \in A \vee x \in B$	

Поскольку на данном этапе мы не можем дальше анализировать цель, мы более внимательно смотрим на исходные посылки. Первая посылка приго-

дится, если нам попадется объект, который является элементом множества A , поскольку это позволит нам сразу сделать вывод, что этот объект также должен быть элементом множества C . Аналогично, вторая посылка пригодится, если мы найдем элемент множества B . Помня, что мы должны следить за любыми элементами A или B , которые могут оказаться в процессе рассуждений, мы переходим к третьей посылке. Поскольку она имеет вид $P \vee Q$, мы пробуем применить доказательство по отдельным случаям. Для первого случая мы предполагаем $x \in A$, а для второго мы полагаем $x \in B$. Следовательно, в первом случае мы имеем следующие посылки и цель:

Посылки	Цель
$A \subseteq C$	$x \in C$
$B \subseteq C$	
$x \in A$	

Мы уже решили, что если мы когда-нибудь встретим элемент A , то можем использовать первую посылку, чтобы сделать вывод, что он также является элементом C . Поскольку теперь у нас есть $x \in A$ как данность, мы можем заключить, что наша цель $x \in C$ доказана. Рассуждения для второго случая очень похожи, только мы используем вторую посылку вместо первой.

Решение

Теорема. Предположим, что A, B и C – множества. Если $A \subseteq C$ и $B \subseteq C$, то $A \cup B \subseteq C$.

Доказательство. Предположим, что $A \subseteq C$ и $B \subseteq C$, и пусть x – произвольный элемент из $A \cup B$. Тогда либо $x \in A$, либо $x \in B$.

Случай 1. $x \in A$. Тогда, поскольку $A \subseteq C$, $x \in C$.

Случай 2. $x \in B$. Тогда, поскольку $B \subseteq C$, $x \in C$.

Поскольку мы знаем, что либо $x \in A$, либо $x \in B$, эти случаи охватывают все возможности, следовательно, мы можем заключить, что $x \in C$. Поскольку x был произвольным элементом $A \cup B$, это означает, что $A \cup B \subseteq C$.

Обратите внимание, что случаи в этом доказательстве не являются исключительными. Другими словами, оба случая, $x \in A$ и $x \in B$, могут быть истинными, поэтому некоторые значения x могут подпадать под оба случая. В этом нет ничего плохого. Случаи в доказательстве должны охватывать все возможности, но нет ничего плохого в том, чтобы охватить некоторые возможности более одного раза. Другими словами, случаи должны быть исчерпывающими, но не обязательно исключительными.

Доказательство по отдельным случаям иногда бывает полезно, если вы доказываете цель в форме $P \vee Q$. Если вы можете доказать P в одном случае и Q в другом, то, пока ваши случаи являются исчерпывающими, вы можете сделать вывод, что $P \vee Q$ истинно. Этот метод особенно полезен, если одна из посылок также имеет форму дизъюнкции, потому что тогда вы можете использовать случаи, предложенные этой посылкой.

Чтобы доказать цель вида $P \vee Q$:

Разбейте доказательства на случаи. В каждом случае докажите P или Q .

Пример 3.5.2. Предположим, что A, B и C – множества. Докажите, что $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$.

Стратегия доказательства

Поскольку цель в логической форме имеет вид $\forall x(x \in A \setminus (B \setminus C) \rightarrow x \in (A \setminus B) \cup C)$, мы будем считать x произвольным элементом, предположим, что $x \in A \setminus (B \setminus C)$, и попытаемся доказать $x \in (A \setminus B) \cup C$. Запись этих утверждений в логической форме дает нам:

$$\begin{array}{ll} \text{Посылки} & \text{Цель} \\ x \in A \wedge \neg(x \in B \wedge x \notin C) & (x \in A \wedge x \notin B) \vee x \in C \end{array}$$

Мы разделяем посылку на два отдельных случая, $x \in A$ и $\neg(x \in B \wedge x \notin C)$, и, поскольку второй случай является отрицанием, мы используем один из законов Де Моргана, чтобы переписать его как положительное утверждение $x \notin B \vee x \in C$.

$$\begin{array}{ll} \text{Посылки} & \text{Цель} \\ x \in A & (x \in A \wedge x \notin B) \vee x \in C \\ x \notin B \vee x \in C & \end{array}$$

Теперь вторая посылка и цель являются дизъюнкциями, поэтому мы попытаемся рассмотреть два случая $x \notin B$ и $x \in C$, предложенные второй посылкой. Согласно нашей стратегии доказательства целей в форме $P \vee Q$, если в каждом случае мы можем либо доказать $x \in A \wedge x \notin B$, либо доказать $x \in C$, то доказательство будет завершено. В первом случае полагаем $x \notin B$.

$$\begin{array}{ll} \text{Посылки} & \text{Цель} \\ x \in A & (x \in A \wedge x \notin B) \vee x \in C \\ x \notin B & \end{array}$$

В этом случае утверждение цели явно истинное, потому что в данном случае мы можем заключить, что $x \in A \wedge x \notin B$. Во втором случае мы предполагаем, что $x \in C$, и снова очевидна истинность цели.

Решение

Теорема. Предположим, что A, B и C – множества. Тогда $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$.

Доказательство. Предположим, что $x \in A \setminus (B \setminus C)$. Тогда $x \in A$ и $x \notin B \setminus C$. Поскольку $x \notin B \setminus C$, то либо $x \notin B$, либо $x \in C$. Мы рассмотрим эти случаи по отдельности.

Случай 1. $x \notin B$. Тогда поскольку $x \in A$, то $x \in A \setminus B$, поэтому $x \in (A \setminus B) \cup C$.

Случай 2. $x \in C$. Тогда очевидно, что $x \in (A \setminus B) \cup C$.

Поскольку x был произвольным элементом из $A \setminus (B \setminus C)$, мы можем заключить, что $A \setminus (B \setminus C) \subseteq (A \setminus B) \cup C$.

Иногда бывает полезно разбить доказательство на случаи, даже если случаи не предполагаются посылками в форме $P \vee Q$. Любое доказательство при желании можно разбить на случаи, если эти случаи охватывают все возможности.

Пример 3.5.3. Докажите, что для любого целого числа x остаток от деления x^2 на 4 равен 0 или 1.

Стратегия доказательства

Мы начинаем с того, что принимаем за x произвольное целое число, а затем пытаемся доказать, что остаток от деления x^2 на 4 равен 0 или 1.

$$\begin{array}{ll} \text{Посылки} & \text{Цель} \\ x \in \mathbb{Z} & (x^2 \div 4, \text{ остаток } 0) \vee (x^2 \div 4, \text{ остаток } 1) \end{array}$$

Поскольку целью является дизъюнкция, наиболее разумной стратегией представляется разбиение доказательства на случаи, но пока не ясно, какие случаи использовать. Однако если мы рассмотрим несколько значений x , это подскажет нам правильные случаи:

x	x^2	Частное от $x^2 \div 4$	Остаток от $x^2 \div 4$
1	1	0	1
2	4	1	0
3	9	2	1
4	16	4	0
5	25	6	1
6	36	9	0

Похоже, что остаток равен 0, когда x четно, и 1, когда нечетно. Воспользуемся этими случаями. Таким образом, для случая 1 мы предполагаем, что x четно, и пытаемся доказать, что остаток от деления равен 0, а для случая 2 мы предполагаем, что x нечетно, и доказываем, что остаток равен 1. Поскольку каждое целое число либо четное, либо нечетное, эти случаи являются исчерпывающими.

Расписав определение четности, получим посылки и цель для случая 1:

$$\begin{array}{ll} \text{Посылки} & \text{Цель} \\ x \in \mathbb{Z} & x^2 \div 4, \text{ остаток } 0 \\ \exists k \in \mathbb{Z} (x = 2k) & \end{array}$$

Мы сразу используем вторую посылку, и пусть k обозначает некоторое конкретное целое число, для которого $x = 2k$. Тогда $x^2 = (2k)^2 = 4k^2$, поэтому ясно, что при делении x^2 на 4 частное равно k^2 , а остаток равен 0.

Случай 2 очень похож на предыдущий:

<i>Посылки</i>	<i>Цель</i>
$x \in \mathbb{Z}$	$x^2 \div 4$, остаток 1
$\exists k \in \mathbb{Z} (x = 2k + 1)$	

И снова мы сразу используем вторую посылку, и пусть k обозначает некоторое конкретное целое число, для которого $x = 2k + 1$. Тогда $x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, поэтому, когда x^2 делится на 4, частное равно $k^2 + k$, а остаток равен 1.

Решение

Теорема. Для каждого целого числа x остаток от деления x^2 на 4 равен 0 или 1.

Доказательство. Предположим, что x – целое число. Рассмотрим два случая.

Случай 1. x четно. Тогда $x = 2k$ для некоторого целого k , поэтому $x^2 = 4k^2$. Очевидно, что остаток от деления x^2 на 4 равен 0.

Случай 2. x нечетно. Тогда $x = 2k + 1$ для некоторого целого k , поэтому $x^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$. Ясно, что в этом случае остаток от деления x^2 на 4 равен 1.

Иногда при поиске доказательства цели, имеющей вид $P \vee Q$, трудно понять, как разбить доказательство на случаи. Вот способ, который часто бывает полезным. Просто предположим, что P истинно в случае 1 и ложно в случае 2. Конечно, P либо истинно, либо ложно, поэтому эти случаи являются исчерпывающими. В первом случае вы предположили, что P истинно, поэтому, безусловно, цель $P \vee Q$ истинна. Таким образом, в случае 1 никаких дополнительных рассуждений не требуется. Во втором случае вы предположили, что P ложно, поэтому единственная возможность для цели $P \vee Q$ оказаться истинной – если Q истинно. Следовательно, чтобы завершить доказательство, вы должны попытаться доказать Q .

Чтобы доказать цель в форме $P \vee Q$:

Если P истинно, то очевидно, что цель $P \vee Q$ истинна, поэтому вам нужно беспокоиться только о том случае, когда P ложно. В этом случае вы можете завершить доказательство, доказав, что Q истинно.

Стратегия доказательства

Перед использованием стратегии:

<i>Посылки</i>	<i>Цель</i>
–	$P \vee Q$
–	

После использования стратегии:

Посылки	Цель
—	Q
—	
$\neg P$	

Форма окончательного доказательства

Если P истинно, то очевидно, что $P \vee Q$ истинно. Теперь предположим, что P ложно.

[Здесь следует привести доказательство Q .]

Таким образом, $P \vee Q$ истинно.

Итак, эта стратегия доказательства $P \vee Q$ предполагает, что вы трансформируете проблему, добавляя $\neg P$ как новую посылку и меняя цель на Q . Интересно отметить, что это в точности то же самое, что и преобразование, которое вы использовали бы, если бы вы доказывали цель $\neg P \rightarrow Q$! В этом нет ничего удивительного, потому что мы уже знаем, что утверждения $P \vee Q$ и $\neg P \rightarrow Q$ эквивалентны. Но мы вывели эту эквивалентность ранее из таблицы истинности для условной связки, и эту таблицу истинности поначалу было трудно понять. Возможно, приведенное нами рассуждение делает эту эквивалентность и, следовательно, таблицу истинности условной связки более очевидной.

Конечно, при использовании данной стратегии роли P и Q можно поменять местами. Иными словами, вы также можете доказать $P \vee Q$, предполагая, что Q ложно, и доказывая P .

Пример 3.5.4. Докажите, что для любого действительного числа x если $x^2 > x$, то либо $x < 0$, либо $x > 1$.

Стратегия доказательства

Наша цель — $\forall x(x^2 \geq x \rightarrow (x \leq 0 \vee x \geq 1))$, поэтому для начала пусть x будет произвольным действительным числом, предположим, что $x^2 \geq x$, и установим $x \leq 0 \vee x \geq 1$ в качестве нашей цели:

Посылки	Цель
$x^2 \geq x$	$x \leq 0 \vee x \geq 1$

Согласно нашей стратегии, чтобы доказать эту цель, мы можем либо предположить, что $x > 0$, и доказать $x \geq 1$, либо предположить, что $x < 0$, и доказать $x \leq 0$. Предположение о положительности x выглядит более удобным при рассмотрении неравенства, поэтому мы используем первый подход.

Посылки	Цель
$x^2 \geq x$	$x \geq 1$
$x > 0$	

Поиск доказательства теперь не составит труда. Поскольку $x > 0$, мы можем разделить исходное неравенство $x^2 \geq x$ на x , чтобы получить искомое утверждение $x \geq 1$.

Решение

Теорема. Для любого действительного числа x если $x^2 \geq x$, то либо $x \leq 0$, либо $x \geq 1$.

Доказательство. Предположим, что $x^2 \geq x$. Если $x \leq 0$, то, разумеется, $x \leq 0$ или $x \geq 1$. Предположим теперь, что $x > 0$. Тогда мы можем разделить обе части неравенства $x^2 \geq x$ на x , чтобы заключить, что $x \geq 1$. Таким образом, либо $x \leq 0$, либо $x \geq 1$.

Эквивалентность $P \vee Q$ и $\neg P \rightarrow Q$ также предлагает правило вывода, называемое *дизъюнктивным силлогизмом*, для использования исходного утверждения формы $P \vee Q$.

Чтобы использовать посылку в форме $P \vee Q$:

Если вам также дано $\neg P$ или вы можете доказать, что P ложно, то можете воспользоваться этим условием, чтобы заключить, что Q истинно. Точно так же, если вам дано $\neg Q$ или вы можете доказать, что Q ложно, вы можете сделать вывод, что P истинно.

Фактически это правило мы использовали в нашем первом примере deductивного мышления в главе 1!

Мы заканчиваем этот раздел доказательством, которое вы можете прочитать без предварительного анализа.

Теорема 3.5.5. Предположим, что m и n – целые числа. Если произведение mn четно, то либо m четно, либо n четно.

Доказательство. Предположим, что mn четное. Тогда мы можем выбрать такое целое число k , что $mn = 2k$. Если m четно, то доказывать больше нечего, поэтому предположим, что m нечетно. Тогда $m = 2j + 1$ для некоторого целого j . Подставляя его в уравнение $mn = 2k$, мы получаем $(2j + 1)n = 2k$, поэтому $2jn + n = 2k$, и, следовательно, $n = 2k - 2jn = 2(k - jn)$. Поскольку $(k - jn)$ – целое число, отсюда следует, что n четно.

Комментарий. Доказательство в общем виде устроено следующим образом:

Предположим, что mn четно.

Если m четно, то очевидно, что либо m четно, либо n четно. Теперь предположим, что m не является четным. Тогда m только нечетно.

[Здесь приводится доказательство того, что n четно.]

Следовательно, либо m четно, либо n четно.

Следовательно, если mn четно, то либо m четно, либо n четно.

Предположения о том, что mn четно, а m нечетно, приводят, посредством экзистенциального подтверждения, к уравнениям $mn = 2k$ и $m = 2j + 1$. В доказательстве этого явно не говорится, но подразумевается, что вы сами решите, что для доказательства четности n достаточно найти такое целое число c , что $n = 2c$. Прямые преобразования приводят к уравнению $n = 2(k - jn)$, поэтому выбор $c = k - jn$ вполне обоснован.

Упражнения

- P_D*1. Предположим, что A, B и C – множества. Докажите, что $A \cap (B \cup C) \subseteq (A \cap B) \cup C$.
- P_D2. Предположим, что A, B и C – множества. Докажите, что $(A \cup B) \setminus C \subseteq A \cup (B \setminus C)$.
- P_D3. Предположим, что A, B и C – множества. Докажите, что $A \setminus (A \setminus B) = A \cap B$.
- P_D4. Предположим, что A, B и C – множества. Докажите, что $A \setminus (B \setminus C) = (A \setminus B) \cup (A \cap C)$.
- P_D*5. Предположим, что $A \cap C \subseteq B \cap C$ и $A \cup C \subseteq B \cup C$. Докажите, что $A \subseteq B$.
- P_D6. Вспомните раздел 1.4, где сказано, что симметрическая разность двух множеств A и B – это множество $AB = (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B)$. Докажите, что если $AB \subseteq A$, то $B \subseteq A$.
- P_D7. Предположим, что A, B и C – множества. Докажите, что $A \cup C \subseteq B \cup C$, если и только если $A \setminus C \subseteq B \setminus C$.
- P_D*8. Докажите, что для любых множеств A и B справедливо $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$.
- P_D9. Докажите, что для любых множеств A и B если $\mathcal{P}(A) \cup \mathcal{P}(B) = \mathcal{P}(A \cup B)$, то либо $A \subseteq B$, либо $B \subseteq A$.
10. Предположим, что x и y – действительные числа и $x = 0$. Докажите, что $y + 1/x = 1 + y/x$ тогда и только тогда, когда или $x = 1$, или $y = 1$.
11. Докажите, что для любого действительного числа x если $|x - 3| > 3$, тогда $x^2 > 6x$. (Подсказка: согласно определению $|x - 3|$, если $x - 3 \geq 0$, то $|x - 3| = x - 3$, а если $x - 3 < 0$, то $|x - 3| = 3 - x$. Самый простой способ использовать этот факт – разбить ваше доказательство на случаи. Предположим, что $x - 3 \geq 0$ в случае 1 и $x - 3 < 0$ в случае 2.)
- *12. Докажите, что для любого действительного числа x неравенство $|2x - 6| > x$ справедливо тогда и только тогда, когда $|x - 4| > 2$. (Прочтите подсказку к упражнению 11.)
13. (a) Докажите, что для всех действительных чисел a и b неравенство $|a| \leq b$ справедливо, если и только если $-b \leq a \leq b$.
(b) Докажите, что для любого действительного числа x справедливо $-|x| \leq x \leq |x|$. (Подсказка: используйте часть (a).)
(c) Докажите, что для всех действительных чисел x и y справедливо неравенство $|x + y| \leq |x| + |y|$. (Это называется *неравенством треугольника*. Один из способов доказать это – объединить части (a) и (b), но вы также можете сделать это, рассмотрев ряд случаев.)
(d) Докажите, что для всех действительных чисел x и y справедливо неравенство $|x + y| \geq |x| - |y|$. (Подсказка: начните с уравнения $|x| = |(x + y) + (-y)|$, а затем примените неравенство треугольника к правой части.)

14. Докажите, что для любого целого числа x значение $x^2 + x$ четно.
15. Докажите, что для любого целого числа x остаток от деления x^4 на 8 равен 0 или 1.
- *16. Предположим, что \mathcal{F} и \mathcal{G} – непустые семейства множеств.
- P_D(a) Докажите, что $\bigcup(\mathcal{F} \cup \mathcal{G}) = (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$.
- (b) Докажите, что $B \cup (\bigcup \mathcal{F}) = \bigcup_{A \in \mathcal{F}}(B \cup A)$.
- (c) Можете ли вы сформулировать и доказать аналогичную теорему о $\bigcap(\mathcal{F} \cup \mathcal{G})$?
17. Предположим, что \mathcal{F} – непустое семейство множеств, а B – множество.
- P_D(a) Докажите, что $B \cup (\bigcup \mathcal{F}) = \bigcup(\mathcal{F} \cup \{B\})$.
- (b) Докажите, что $B \cup (\bigcap \mathcal{F}) = \bigcap_{A \in \mathcal{F}}(B \cup A)$.
- (c) Можете ли вы сформулировать и доказать аналогичные теоремы о $B \cap (\bigcup \mathcal{F})$ и $\cap(\bigcap \mathcal{F})$?
18. Предположим, что \mathcal{F}, \mathcal{G} и \mathcal{H} – непустые семейства множеств и для любого $A \in \mathcal{F}$ и любого $B \in \mathcal{G}$ справедливо $A \cup B \in \mathcal{H}$. Докажите, что $\bigcap \mathcal{H} \subseteq (\bigcap \mathcal{F}) \cup (\bigcap \mathcal{G})$.
- P_D19. Предположим, что A и B – множества. Докажите, что $\forall x(x \in A \Delta B \leftrightarrow (x \in A \leftrightarrow x \notin B))$.
- P_D*20. Предположим, что A, B и C – множества. Докажите, что $A \Delta B$ и C не пересекаются тогда и только тогда, когда $A \cap C = B \cap C$.
- P_D21. Предположим, что A, B и C – множества. Докажите, что $A \cap B \subseteq C$ тогда и только тогда, когда $A \cup C = B \cup C$.
- P_D22. Предположим, что A, B и C – множества. Докажите, что $C \subseteq A \Delta B$ тогда и только тогда, когда $C \subseteq A \cup B$ и $A \cap B \cap C = \emptyset$.
- P_D*23. Предположим, что A, B и C – множества.
- (a) Докажите, что $A \setminus C \subseteq (A \setminus B) \cup (B \setminus C)$.
- (b) Докажите, что $A \cap C \subseteq (A \setminus B) \cup (B \setminus C)$.
- P_D*24. Предположим, что A, B и C – множества.
- (a) Докажите, что $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$.
- (b) Найдите пример множеств A, B и C таких, что $(A \cup B) \cap C \neq (A \Delta C) \cup (B \Delta C)$.
- P_D25. Предположим, что A, B и C – множества.
- (a) Докажите, что $(A \Delta C) \cap (B \Delta C) \subseteq (A \cap B) \Delta C$.
- (b) Всегда ли верно, что $(A \cap B) \Delta C \subseteq (A \Delta C) \cap (B \Delta C)$? Приведите доказательство или контрпример.
- P_D26. Предположим, что A, B и C – множества. Рассмотрим множества $(A \setminus B) \Delta C$ и $(A \Delta C) \setminus (B \Delta C)$. Можете ли вы доказать, что одно из них является подмножеством другого? Обоснуйте свои выводы либо доказательствами, либо контрпримерами.
- *27. Рассмотрим следующую предположительную теорему.

Предположительная теорема. Для любого действительного числа x если $|x - 3| < 3$, то $0 < x < 6$.

Правильно ли следующее доказательство? Если да, то какие стратегии доказательства в нем задействованы? Если нет, можно ли это исправить? Верна ли теорема?

Доказательство. Пусть x – произвольное действительное число, и предположим, что $|x - 3| < 3$. Рассмотрим два случая.

Случай 1. $x - 3 \geq 0$. Тогда $|x - 3| = x - 3$. Подставляя это в предположение, что $|x - 3| < 3$, мы получаем $x - 3 < 3$, поэтому ясно, что $x < 6$.

Случай 2. $x - 3 < 0$. Тогда $|x - 3| = 3 - x$, поэтому предположение $|x - 3| < 3$ означает, что $3 - x < 3$. Следовательно, $3 < 3 + x$, поэтому $0 < x$.

Поскольку мы доказали и $0 < x$, и $x < 6$, можем заключить, что $0 < x < 6$.

28. Рассмотрим следующую предположительную теорему.

Предположительная теорема. Для любых множеств A, B и C если $A \setminus B \subseteq C$ и $A \subset C$, то $A \cap B = \emptyset$.

Правильно ли следующее доказательство? Если да, то какие стратегии доказательства в нем задействованы? Если нет, можно ли это исправить? Верна ли теорема?

Доказательство. Предположим, что $A \setminus B \subseteq C$ и $A \subset C$. Имея $A \subset C$, мы можем выбрать некоторый x таким образом, что $x \in A$ и $x \notin C$. Поскольку $x \notin C$ и $A \setminus B \subseteq C$, то $x \notin A \setminus B$. Поэтому либо $x \notin A$, либо $x \in B$. Но мы уже знаем, что $x \in A$, следовательно, $x \in B$. Поскольку $x \in A$ и $x \in B$, то $x \in A \cap B$. Следовательно, $A \cap B \neq \emptyset$.

- *29. Рассмотрим следующую предположительную теорему.

Предположительная теорема. $\forall x \in \mathbb{R} \exists y \in \mathbb{R} (xy^2 \neq y - x)$.

Правильно ли следующее доказательство? Если да, то какие стратегии доказательства в нем задействованы? Если нет, можно ли это исправить? Верна ли теорема?

Доказательство. Пусть x – произвольное действительное число.

Случай 1. $x = 0$. Пусть $y = 1$. Тогда $xy^2 = 0$ и $y - x = 1 - 0 = 1$, поэтому $xy^2 \neq y - x$.

Случай 2. $x \neq 0$. Пусть $y = 0$. Тогда $xy^2 = 0$ и $y - x \neq -x = 0$, поэтому $xy^2 \neq y - x$. Поскольку эти случаи являются исчерпывающими, мы показали, что справедливо $\exists y \in \mathbb{R} (xy^2 \neq y - x)$. Поскольку x был произвольным, это показывает, что истинно $\forall x \in \mathbb{R} \exists y \in \mathbb{R} (xy^2 \neq y - x)$.

30. Докажите, что если $\forall x P(x) \rightarrow \exists x Q(x)$, то $\exists x (P(x) \rightarrow Q(x))$. (Подсказка: помните, что $P \rightarrow Q$ эквивалентно $\neg P \vee Q$.)

- *31. Рассмотрим следующую предположительную теорему.

Предположительная теорема. Предположим, что A, B и C – множества и $A \subseteq B \cup C$. Тогда либо $A \subseteq B$, либо $A \subseteq C$.

Правильно ли следующее доказательство? Если да, то какие стратегии доказательства в нем задействованы? Если нет, можно ли это исправить? Верна ли теорема?

Доказательство. Пусть x – произвольный элемент из A . Поскольку $A \subseteq B \cup C$, то либо $x \in B$, либо $x \in C$.

Случай 1. $x \in B$. Поскольку x был произвольным элементом из A , отсюда следует, что $\forall x \in A(x \in B)$, то есть истинно утверждение $A \subseteq B$.

Случай 2. $x \in C$. Аналогично, поскольку x был произвольным элементом из A , мы можем заключить, что $A \subseteq C$.

Таким образом, либо $A \subseteq B$, либо $A \subseteq C$.

- P_D32. Предположим, что A, B и C – множества и $A \subseteq B \cup C$. Докажите, что или $A \subseteq B$, или $A \cap C \neq \emptyset$.
33. Докажите $\exists x(P(x) \rightarrow \forall y P(y))$. (Примечание: предположим, что универсум дискурса не является пустым множеством.)

3.6. ДОКАЗАТЕЛЬСТВА СУЩЕСТВОВАНИЯ И ЕДИНСТВЕННОСТИ

В этом разделе мы рассматриваем доказательства, в которых цель имеет вид $\exists! xP(x)$. Напомним, что эта формула означает «существует ровно один x такой, что $P(x)$ », и, как мы видели в разделе 2.2, ее можно рассматривать как сокращенную запись формулы $\exists x(P(x) \wedge \neg y(P(y) \wedge y \neq x))$. Согласно стратегиям доказательства, рассмотренным в предыдущих разделах, мы могли бы доказать эту цель, найдя конкретное значение x , для которого мы могли бы доказать как $P(x)$, так и $\neg y(P(y) \wedge y \neq x)$. Последняя часть этого доказательства будет включать доказательство отрицательного утверждения, но мы можем переписать его как эквивалентное положительное утверждение:

$$\begin{aligned} & \neg \exists y(P(y) \wedge y \neq x) \\ & \text{эквивалентно } \forall y \neg(P(y) \wedge y \neq x) \quad (\text{правило отрицания квантора}), \\ & \text{что эквивалентно } \forall y(\neg P(y) \vee y = x) \quad (\text{закон Де Моргана}), \\ & \text{что эквивалентно } \forall y(P(y) \rightarrow y = x) \quad (\text{условный закон}). \end{aligned}$$

Таким образом, мы видим, что $\exists! xP(x)$ можно также записать как $\exists x(P(x) \wedge \forall y(P(y) \rightarrow y = x))$. Фактически, как показывает следующий пример, несколько других формул также эквивалентны $\exists! xP(x)$, и они предлагают другие подходы к доказательству целей в этой форме.

Пример 3.6.1. Докажите, что все следующие формулы эквивалентны:

1. $\exists x(P(x) \wedge \forall y(P(y) \rightarrow y = x))$.
2. $\exists x \forall y(P(y) \leftrightarrow y = x)$.
3. $\exists xP(x) \wedge \forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$.

Стратегия доказательства

Если мы возьмемся доказывать напрямую эквивалентность каждого из этих утверждений всем остальным, то нам придется доказать три биусловия: утверждение 1 истинно, если и только если истинно утверждение 2; утверждение 1 истинно, если и только если истинно утверждение 3; утверждение 2 истинно, если и только если истинно утверждение 3. Если мы докажем каждое биусловие методами раздела 3.4, то каждое доказательство будет включать по два условных доказательства, поэтому нам потребуется шесть условных доказательств. К счастью, есть более простой способ. Мы докажем, что из утверждения 1 следует утверждение 2, из утверждения 2 следует утверждение 3, а из утверждения 3 следует утверждение 1, – всего три условия. Хотя мы не будем приводить отдельное доказательство того, что из утверждения 2 следует утверждение 1, оно будет следовать из того факта, что из утверждения 2 следует утверждение 3, а из утверждения 3 следует утверждение 1. Точно так же и два остальных условия последуют из тех трех, которые мы докажем. Математики почти всегда используют такой метод, чтобы доказать, что несколько утверждений эквивалентны. Поскольку мы будем доказывать три условных утверждения, наше доказательство будет состоять из трех частей, которые мы обозначим $1 \rightarrow 2$, $2 \rightarrow 3$ и $3 \rightarrow 1$. Нам нужно будет разработать стратегию доказательства для трех частей по отдельности.

$1 \rightarrow 2$. Мы предполагаем утверждение 1 и доказываем утверждение 2. Поскольку утверждение 1 начинается с квантора существования, мы выбираем имя, скажем x_0 , для некоторого объекта, для которого истинны утверждения $P(x_0)$ и $\forall y(P(y) \rightarrow y = x_0)$. Таким образом, теперь мы имеем следующую ситуацию:

Посылки	Цель
$P(x_0)$	
$\forall y(P(y) \rightarrow y = x_0)$	$\exists x \forall y(P(y) \leftrightarrow y = x)$

Наша цель также начинается с квантора существования, поэтому, чтобы доказать ее, мы должны попытаться найти значение x , которое делает остальную часть утверждения истинной. Конечно, очевидный выбор – $x = x_0$. Подставляя x_0 вместо x , мы видим, что теперь должны доказать $\forall y(P(y) \leftrightarrow y = x_0)$. Примем y за произвольный объект и докажем оба направления биусловия. Истинность для направления \rightarrow очевидна из второй посылки. Для направления \leftarrow предположим, что $y = x_0$. У нас также есть $P(x_0)$ как посылка, и, подставляя в эту посылку y вместо x_0 , мы получаем $P(y)$.

$2 \rightarrow 3$. Утверждение 2 является экзистенциальным, поэтому пусть x_0 – некоторый объект такой, что $\forall y(P(y) \leftrightarrow y = x_0)$. Цель, утверждение 3, представляет собой конъюнкцию, поэтому мы рассматриваем ее как две отдельные цели.

Посылки	Цель
$\forall y(P(y) \leftrightarrow y = x_0)$	$\exists x P(x)$
	$\forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$

Чтобы доказать первую цель, мы должны выбрать значение для x , и, конечно, это снова будет $x = x_0$. Таким образом, мы должны доказать $P(x_0)$. Естественно,

венный способ использовать нашу единственную посылку – это подставить что-либо вместо y ; чтобы доказать цель $P(x_0)$, очевидно, нужно подставить x_0 . Это дает нам $P(x_0) \leftrightarrow x_0 = x_0$. Конечно, $x_0 = x_0$ истинно, а по направлению \leftarrow биусловия получаем $P(x_0)$.

Для второй цели пусть y и z произвольны, предположим, что истинны $P(y)$ и $P(z)$, и попытаемся доказать, что $y = z$.

Посылки	Цель
$\forall y(P(y) \leftrightarrow y = x_0)$	$y = z$
$P(y)$	
$P(z)$	

Подставляя y и z в первую посылку, мы получаем $P(y) \leftrightarrow y = x_0$ и $P(z) \leftrightarrow z = x_0$. Поскольку мы предположили $P(y)$ и $P(z)$, на этот раз используем направление \rightarrow этих биусловий, чтобы сделать вывод, что $y = x_0$ и $z = x_0$, из чего следует наша цель $y = z$.

$3 \rightarrow 1$. Поскольку утверждение 3 является конъюнкцией, мы рассматриваем его как две отдельные посылки. Первая – экзистенциальное утверждение, поэтому мы обозначаем за x_0 некоторый объект, такой что $P(x_0)$ истинно. Чтобы доказать утверждение 1, мы снова положим $x = x_0$, и получим следующие посылки и цель:

Посылки	Цель
$P(x_0)$	$P(x_0) \wedge \forall y(P(y) \leftrightarrow y = x_0)$
$\forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$	

Мы уже знаем первую половину цели, поэтому нам нужно доказать только вторую. Для этого пусть y будет произвольным, пусть истинно $P(y)$ и нашей целью будет $y = x_0$.

Посылки	Цель
$P(x_0)$	$y = x_0$
$\forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$	
$P(y)$	

Но теперь мы знаем как $P(y)$, так и $P(x_0)$, поэтому цель $y = x_0$ следует из второй посылки.

Решение

Теорема. Следующие варианты эквивалентны:

1. $\exists x(P(x) \wedge \forall y(P(y) \rightarrow y = x))$.
2. $\exists x \forall y(P(y) \leftrightarrow y = x)$.
3. $\exists x P(x) \wedge \forall y \forall z((P(y) \wedge P(z)) \rightarrow y = z)$.

Доказательство. $1 \rightarrow 2$. Исходя из утверждения 1, мы можем считать, что x_0 – некоторый объект такой, что $P(x_0)$ и $\forall y(P(y) \rightarrow y = x_0)$. Для доказательства утверждения 2 покажем, что $\forall y(P(y) \leftrightarrow y = x_0)$. Пусть y – произвольный объект. Мы уже знаем направление \rightarrow биусловного выражения. Для доказательства в на-

правлении \leftarrow предположим, что $y = x_0$. Тогда, поскольку мы знаем истинность $P(x_0)$, можем заключить, что $P(y)$ истинно.

2 \rightarrow 3. Исходя из утверждения 2, выберем x_0 так, чтобы $\forall y(P(y) \leftrightarrow y = x_0)$. Тогда, в частности, $P(x_0) \leftrightarrow x_0 = x_0$, и поскольку очевидно, что $x_0 = x_0$, отсюда следует, что $P(x_0)$ истинно. Таким образом, $\exists xP(x)$. Чтобы доказать вторую половину утверждения 3, пусть y и z обозначают произвольные объекты, и пусть $P(y)$ и $P(z)$ истинны. Тогда из нашего выбора x_0 (как чего-то, для чего $\forall y(P(y) \leftrightarrow y = x_0)$ истинно) следует, что $y = x_0$ и $z = x_0$, поэтому $y = z$.

3 \rightarrow 1. Пусть согласно первой половине утверждения 3 x_0 – некоторый объект такой, что $P(x_0)$. Утверждение 1 следует из условия, если мы сможем показать, что $\forall y(P(y) \rightarrow y = x_0)$, поэтому предположим, что $P(y)$. Поскольку теперь у нас есть и $P(x_0)$, и $P(y)$, во второй половине утверждения 3 мы можем прийти к выводу, что $y = x_0$, что и требовалось доказать.

Поскольку все три утверждения теоремы эквивалентны $\exists! xP(x)$, мы можем доказать цель в такой форме, доказав любое из трех утверждений теоремы. Вероятно, самый распространенный метод доказательства цели $\exists! xP(x)$ – это доказательство утверждения 3 теоремы.

Чтобы доказать цель в форме $\exists! xP(x)$:

Докажите цели $\exists xP(x)$ и $\forall y\forall z((P(y) \wedge P(z)) \rightarrow y = z)$. Первая из этих целей показывает, что существует x такое, что $P(x)$ истинно, а вторая показывает, что это значение x уникально. Поэтому две части доказательства иногда называют *существованием и единственностью*. Каждая часть доказывается с использованием описанных ранее стратегий.

Форма окончательного доказательства

Существование: [Здесь приведите доказательство $\exists xP(x)$.]

Единственность: [Здесь приведите доказательство $\forall y\forall z((P(y) \wedge P(z)) \rightarrow y = z)$.]

Пример 3.6.2. Докажите, что существует единственное множество A такое, что для каждого множества B истинно $A \cup B = B$.

Стратегия доказательства

Наша цель – $\exists! AP(A)$, где $P(A)$ представляет собой утверждение $\forall B(A \cup B = B)$. В соответствии с нашей стратегией мы можем доказать его, отдельно доказывая существование и единственность. Для доказательства существования мы должны доказать $\exists AP(A)$, поэтому пытаемся найти значение A , которое делает $P(A)$ истинным. Не существует формулы для нахождения этого множества A , но если вы задумаетесь о том, что означает утверждение $P(A)$, то должны понять, что правильный выбор – $A = \emptyset$. Подставляя это значение вместо A , мы видим, что для завершения доказательства существования B мы должны показать, что $\forall B(\emptyset \cup B = B)$. Это действительно так. (Если вы не уверены в этом, разработайте доказательство!)

Доказательством единственности послужит доказательство утверждения $\forall C\forall D((P(C) \wedge P(D)) \rightarrow C = D)$. Пусть C и D – произвольные множества. Предпо-

ложим, что $P(C)$ и $P(D)$ истинны, и докажем, что $C = D$. Расписав, что означают утверждения $P(C)$ и $P(D)$, мы получим следующие посылки и цель:

Посылки	Цель
$\forall B(C \cup B = B)$	$C = D$
$\forall B(D \cup B = B)$	

Чтобы воспользоваться посылками, мы должны попытаться найти что-то, что можно было бы подставить в каждой из них вместо B . Вот разумный подход, который упрощает остальную часть доказательства: мы подставляем D вместо B в первую посылку и C вместо B во вторую. Это дает нам $C \cup D = D$ и $D \cup C = C$. Но ясно, что $C \cup D = D \cup C$. (Если вы не понимаете почему, докажите это!) Отсюда прямо следует цель $C = D$.

Решение

Теорема. Существует уникальное множество A такое, что для каждого множества B истинно $A \cup B = B$.

Доказательство

Существование: очевидно, $\forall B(\emptyset \cup B = B)$, поэтому \emptyset обладает требуемым качеством.

Уникальность: предположим, что $\forall B(C \cup B = B)$ и $\forall B(D \cup B = B)$ истинны. Применяя первое из этих предположений к D , мы видим, что $C \cup D = D$, а применяя второе к C , получаем $D \cup C = C$. Но ясно, что $C \cup D = D \cup C$, поэтому $C = D$.

Иногда утверждение в форме $\exists! xP(x)$ доказывается путем доказательства утверждения 1 из примера 3.6.1. Это приводит к следующей стратегии доказательства.

Чтобы доказать цель в форме $\exists! xP(x)$:

Докажите $\exists x(P(x) \wedge \forall y(P(y) \rightarrow y = x))$, используя стратегии из предыдущих разделов.

Пример 3.6.3. Докажите, что для каждого действительного числа x , если $x \neq 2$, существует уникальное действительное число y такое, что $2y/(y + 1) = x$.

Стратегия доказательства

Наша цель – $\forall x(x \neq 2 \rightarrow \exists! y(2y/(y + 1) = x))$. Поэтому пусть x произвольно, предположим, что $x \neq 2$, и докажем $\exists! y(2y/(y + 1) = x)$. Согласно предыдущей стратегии, мы можем доказать эту цель, доказав эквивалентное утверждение

$$\exists y \left(\frac{2y}{y+1} = x \wedge \forall z \left(\frac{2z}{z+1} = x \rightarrow z = y \right) \right).$$

Начнем с попытки найти значение y , при котором уравнение $2y/(y + 1) = x$ окажется истинным. Другими словами, мы решаем это уравнение относительно y :

$$\frac{2y}{y+1} = x \Rightarrow 2y = x(y+1) \Rightarrow y(2-x) = x \Rightarrow y = \frac{x}{2-x}.$$

Обратите внимание, что $x \neq 2$ дано как условие, так что деление на $2-x$ на последнем шаге вполне допустимо. Конечно, в доказательстве эти шаги не приводятся. Мы просто полагаем $y = x/(2-x)$ и пытаемся доказать как $2y/(y+1) = x$, так и $\forall z(2z/(z+1) = x \rightarrow z = y)$.

Посылки	Цель
$x \neq 2$	$\frac{2y}{y+1} = x$
$y = \frac{x}{2-x}$	$\forall z \left(\frac{2z}{z+1} = x \rightarrow z = y \right)$

В истинности первой цели легко убедиться, просто подставив $x/(2-x)$ вместо y . Во втором случае, пусть z произвольно, предположим, что $2z/(z+1) = x$, и докажем, что $z = y$.

Доказательства существования и единственности

Посылки	Цель
$x \neq 2$	$z = y$
$y = \frac{x}{2-x}$	
$\frac{2z}{z+1} = x$	

Теперь мы можем показать, что $z = y$, решив относительно z уравнение в третьей посылке:

$$\frac{2z}{z+1} = x \Rightarrow 2z = x(z+1) \Rightarrow z(2-x) = x \Rightarrow z = \frac{x}{2-x} = y.$$

Обратите внимание, что шаги, которые мы использовали здесь, точно такие же, как шаги, которые мы использовали ранее при решении относительно y . Это обычная закономерность в доказательствах существования и единственности. Хотя предварительные рассуждения по поиску доказательства существования не должны появляться в доказательстве, эти или аналогичные доводы иногда могут использоваться, чтобы доказать, что объект, показанный как существующий, уникален.

Решение

Теорема. Для каждого действительного числа x если $x \neq 2$, то существует unique действительное число y такое, что $2y/(y+1) = x$.

Доказательство. Пусть x – произвольное действительное число, и пусть $x \neq 2$. Пусть $y = x/(2-x)$, что определено, поскольку $x \neq 2$. Тогда

$$\frac{2y}{y+1} = \frac{\frac{2x}{2-x}}{\frac{x}{2-x} + 1} = \frac{\frac{2x}{2-x}}{\frac{2}{2-x}} = \frac{2x}{2} = x.$$

Чтобы убедиться в единственности этого решения, предположим, что $2z/(z+1) = x$. Тогда $2z = x(z+1)$, поэтому $z(2-x) = x$. Поскольку $x \neq 2$, мы можем разделить обе части на $2-x$, чтобы получить $z = x/(2-x) = y$.

Теорема из примера 3.6.1 также может быть использована для формулировки стратегии использования посылок в форме $\exists!xP(x)$. И снова утверждение 3 этой теоремы используется чаще всего.

Использование посылок в форме $\exists!xP(x)$:

Рассматривайте эту запись как два исходных утверждения, $\exists xP(x)$ и $\forall y\forall z((P(y) \wedge P(z)) \rightarrow y = z)$. Чтобы использовать первое утверждение, вам, вероятно, следует выбрать имя, скажем x_0 , для обозначения некоторого объекта, такого что $P(x_0)$ истинно. Второе говорит вам, что если вы когда-нибудь найдете два объекта y и z такие, что утверждения $P(y)$ и $P(z)$ оба истинны, вы можете заключить, что $y = z$.

Пример 3.6.4. Предположим, что A , B и C – множества, A и B пересекаются, A и C пересекаются и A имеет ровно один элемент. Докажите, что B и C пересекаются.

Стратегия доказательства

Посылки	Цель
$A \cap B \neq \emptyset$	$B \cap C \neq \emptyset$
$A \cap C \neq \emptyset$	
$\exists! x(x \in A)$	

В соответствии с нашей стратегией мы относимся к последней посылке как к двум отдельным посылкам. Расписывая значения других посылок и цели, мы получаем следующее:

Посылки	Цель
$\exists x(x \in A \wedge x \in B)$	$\exists x(x \in B \wedge x \in C)$
$\exists x(x \in A \wedge x \in C)$	
$\exists x(x \in A)$	
$\forall y\forall z((P(y) \wedge P(z)) \rightarrow y = z)$	

Чтобы доказать цель, мы должны найти такой объект, который является элементом как B , так и C . Для этого мы обратимся к посылкам. Первая из них говорит нам, что мы можем выбрать имя, скажем b , для какого-то объекта, такого, что $b \in A$ и $b \in B$. Аналогично, согласно второй посылке мы можем обозначить за c такой объект, что $c \in A$ и $c \in C$. На этом шаге третья посылка является избыточной. Мы уже знаем, что в A есть элементы, потому что нам

известно, что $b \in A$ и $c \in A$. Мы также можем обратиться к четвертой посылке, в которой говорится, что если мы найдем два объекта, которые являются элементами A , мы можем сделать вывод, что они идентичны. Но, как мы только что заметили, нам известно, что $b \in A$ и $c \in A$! Поэтому мы можем заключить, что $b = c$. Поскольку $b \in B$ и $b = c \in C$, мы нашли объект, который является элементом как B , так и C , что является доказательством цели.

Решение

Теорема. Предположим, что A , B и C – множества, A и B пересекаются, A и C пересекаются, а A имеет ровно один элемент. Тогда B и C пересекаются.

Доказательство. Поскольку A и B не являются дизъюнктными, мы можем выбрать объект b такой, что $b \in A$ и $b \in B$. Аналогично, поскольку A и C не являются дизъюнктными, существует некоторый объект c такой, что $c \in A$ и $c \in C$. Поскольку A имеет только один элемент, то справедлива идентичность $b = c$. Таким образом, $b = c \in B \cap C$, и, следовательно, B и C пересекаются.

Упражнения

- *1. Докажите, что для каждого действительного числа x существует уникальное действительное число y такое, что $x^2y = x - y$.
2. Докажите, что существует единственное действительное число x такое, что для любого действительного числа y справедливо равенство $xy + x - 4 = 4y$.
3. Докажите, что для любого действительного числа x если $x \neq 0$ и $x \neq 1$, то существует единственное действительное число y такое, что $y/x = y - x$.
- *4. Докажите, что для каждого действительного числа x если $x \neq 0$, существует единственное действительное число y такое, что для каждого действительного числа z справедливо равенство $zy = z/x$.
5. Напомним, что если \mathcal{F} – семейство множеств, то $\bigcup \mathcal{F} = \{x \mid \exists A(A \in \mathcal{F} \wedge x \in A)\}$. Предположим, мы определяем новое множество $\bigcup !\mathcal{F}$ по формуле $\bigcup !\mathcal{F} = \{x \mid \exists !A(A \in \mathcal{F} \wedge x \in A)\}$.
 - (a) Докажите, что для любого семейства множеств \mathcal{F} истинно $\bigcup !\mathcal{F} \subseteq \bigcup \mathcal{F}$.
 - (b) Семейство множеств \mathcal{F} называется *попарно непересекающимся*, если каждая пара различных элементов \mathcal{F} не пересекается; то есть $\forall A \in \mathcal{F} \forall B \in \mathcal{F} (A \neq B \rightarrow A \cap B = \emptyset)$. Докажите, что для любого семейства множеств \mathcal{F} утверждение $\bigcup !\mathcal{F} = \bigcup \mathcal{F}$ истинно тогда и только тогда, когда \mathcal{F} попарно не пересекается.
- P_D*6. Пусть U – произвольное множество.
 - (a) Докажите, что существует единственное $A \in \mathcal{P}(U)$ такое, что для любого $B \in \mathcal{P}(U)$ истинно утверждение $A \cup B = B$.
 - (b) Докажите, что существует единственное $A \in \mathcal{P}(U)$ такое, что для любого $B \in \mathcal{P}(U)$ истинно утверждение $A \cup B = A$.

P_D*7. Пусть U – произвольное множество.

- (а) Докажите, что существует единственное $A \in \mathcal{P}(U)$ такое, что для любого $B \in \mathcal{P}(U)$ истинно утверждение $A \cap B = B$.
- (б) Докажите, что существует единственное $A \in \mathcal{P}(U)$ такое, что для любого $B \in \mathcal{P}(U)$ истинно утверждение $A \cap B = A$.

P_D*8. Пусть U – произвольное множество.

- (а) Докажите, что для любого $A \in \mathcal{P}(U)$ существует единственное $B \in \mathcal{P}(U)$ такое, что для любого $C \in \mathcal{P}(U)$ истинно утверждение $C \setminus A = C \cap B$.
- (б) Докажите, что для любого $A \in \mathcal{P}(U)$ существует единственное $B \in \mathcal{P}(U)$ такое, что для любого $C \in \mathcal{P}(U)$ истинно утверждение $C \cap A = C \setminus B$.

P_D9. Вспомните, как вы показали в упражнении 14 раздела 1.4, что *симметрическая разность* (строгая дизъюнкция – прим. перев.) ассоциативна; другими словами, для всех множеств A, B и C справедливо утверждение $A \Delta (B \Delta C) = (A \Delta B) \Delta C$. Вам также полезно иметь в виду, что симметрическая разность коммутативна; другими словами, для всех множеств A и B справедливо утверждение $A \Delta B = B \Delta A$.

- (а) Докажите, что существует единственный единичный элемент для симметрической разности. Другими словами, существует единственное множество X такое, что для каждого множества A справедливо утверждение $A \Delta X = A$.
- (б) Докажите, что каждое множество имеет единственное обратное множество для операции симметрической разности. Другими словами, для каждого множества A существует уникальное множество B такое, что $A \Delta B = X$, где X – единичный элемент из пункта (а).
- (с) Докажите, что для любых множеств A и B существует единственное множество C такое, что $A \Delta C = B$.
- (д) Докажите, что для каждого множества A существует единственное множество $B \subseteq A$ такое, что для каждого множества $C \subseteq A$ справедливо утверждение $B \Delta C = A \setminus C$.

P_D10. Предположим, что A – множество, и для любого семейства множеств \mathcal{F} если $\bigcup \mathcal{F} = A$, то $A \in \mathcal{F}$. Докажите, что в A ровно один элемент.

P_D*11. Предположим, что \mathcal{F} – семейство множеств, обладающее тем свойством, что для любого $\mathcal{G} \subseteq \mathcal{F}$ справедливо $\bigcup \mathcal{G} \in \mathcal{F}$. Докажите, что существует единственное множество A такое, что $A \in \mathcal{F}$ и $\forall B \in \mathcal{F} (B \subseteq A)$.

12. (а) Предположим, что $P(x)$ – утверждение со свободной переменной x . Используя изученные нами логические символы, запишите формулу, которая означает, что «существуют ровно два значения x , для которых истинно $P(x)$ ».
- (б) Основываясь на вашем ответе на пункт (а), разработайте стратегию доказательства для утверждения вида «существуют ровно два значения x , для которых истинно $P(x)$ ».
- (с) Докажите, что существует ровно два решения уравнения $x^3 = x^2$.

13. (a) Докажите, что существует единственное действительное число c такое, что ему соответствует единственное действительное число x такое, что $x^2 + 3x + c = 0$. (Другими словами, существует единственное действительное число c такое, что уравнение $x^2 + 3x + c = 0$ имеет ровно одно решение.)
- (b) Покажите, что это *не* тот случай, когда существует единственное действительное число x такое, что ему соответствует единственное действительное число c , при котором $x^2 + 3x + c = 0$. (Подсказка: вы должны суметь доказать, что для *каждого* действительного числа x существует уникальное действительное число c такое, что $x^2 + 3x + c = 0$.)

3.7. БОЛЕЕ СЛОЖНЫЕ ПРИМЕРЫ ДОКАЗАТЕЛЬСТВ

До сих пор в большинстве наших доказательств использовались довольно простые приложения рассмотренных нами методов. Мы закончим эту главу несколькими примерами более сложных доказательств. В этих доказательствах тоже используются приемы, описанные в данной главе, но они по разным причинам немного сложнее, чем большинство наших предыдущих доказательств. Некоторые доказательства просто длиннее и требуют применения большего количества стратегий. Иные требуют грамотного выбора стратегий. В некоторых случаях ясно, какую стратегию использовать, но требуются небольшие усилия, чтобы понять, как именно ее использовать. Наши предыдущие примеры, которые были предназначены только для иллюстрации и пояснения методов доказательства, могли произвести впечатление механической скучной работы. Мы надеемся, что, изучив эти более сложные примеры, вы начнете понимать, что математические рассуждения также могут быть удивительными и красивыми.

Некоторые методы доказательства особенно трудно применить. Например, когда вы доказываете цель формы $\exists x P(x)$, очевидный способ продолжить – попытаться найти значение x , которое делает утверждение $xP(x)$ истинным, но иногда совсем не очевидно, как найти это значение x . Аналогичная проблема возникает при использовании исходных данных в форме $\forall x P(x)$. Вы, вероятно, захотите подставить конкретное значение вместо x , но для этого вам придется сделать осмысленный выбор объекта подстановки. Также иногда трудно разработать доказательства, требующие разбиения на случаи. Иногда бывает трудно понять, когда следует использовать разбиение на случаи и какие случаи задействовать.

Начнем с того, что снова вернемся к доказательствам из введения к этой книге. Некоторые аспекты этих доказательств, вероятно, слегка вас озадачили, когда вы читали введение. А теперь, когда вы лучше понимаете, как строятся доказательства, они стали для вас более понятными? Далее мы представляем каждое доказательство в точности так, как это было сделано во введении, а затем сопровождаем его комментарием, в котором поясняются использованные методы.

Теорема 3.7.1. Предположим, что n – целое число больше 1 и n не является простым. Тогда $2^n - 1$ не является простым.

Доказательство. Поскольку n не является простым, существуют натуральные числа a и b такие, что $a < n$, $b < n$ и $n = ab$. Пусть $x = 2^b - 1$ и $y = 1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}$. Отсюда

$$\begin{aligned} xy &= (2^b - 1) \cdot (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) \\ &= 2^b \cdot (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) - (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) \\ &= (2^b + 2^{2b} + 2^{3b} + \dots + 2^{ab}) - (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) \\ &= 2^{ab} - 1 \\ &= 2^n - 1. \end{aligned}$$

Поскольку $b < n$, мы можем заключить, что $x = 2^b - 1 < 2^n - 1$. Также поскольку $ab = n > a$, то $b > 1$. Следовательно, $x = 2^b - 1 > 2^1 - 1 = 1$, поэтому $y < xy = 2^n - 1$. Таким образом, мы показали, что $2^n - 1$ может быть записано как произведение двух натуральных чисел x и y , оба из которых меньше $2^n - 1$, поэтому $2^n - 1$ не является простым.

Комментарий. Нам дано, что n не является простым, и мы должны доказать, что $2^n - 1$ не является простым. Оба эти утверждения являются отрицаниями, но, к счастью, их легко переформулировать в утвердительной форме. Утверждение, что целое число больше 1, не является простым, означает, что оно может быть записано как произведение двух меньших положительных целых чисел. Таким образом, гипотеза о том, что n не является простым, означает $\exists a \in \mathbb{Z}^+ \exists b \in \mathbb{Z}^+ (ab = n \wedge a < n \wedge b < n)$, и фактически мы должны доказать, что $2^n - 1$ не является простым, что означает $\exists x \in \mathbb{Z}^+ \exists y \in \mathbb{Z}^+ (xy = 2^n - 1 \wedge x < 2^n - 1 \wedge y < 2^n - 1)$. Во втором предложении доказательства мы применяем экзистенциальное подтверждение к гипотезе о том, что n не является простым, а оставшаяся часть доказательства посвящена демонстрации чисел x и y со свойствами, необходимыми для доказательства того, что $2^n - 1$ не является простым.

Как обычно бывает в случае экзистенциальных подтверждений, доказательство не объясняет, как были выбраны значения x и y , оно просто демонстрирует, что эти значения работают. После того как приняты значения x и y , остается доказать цель $xy = 2^n - 1 \wedge x < 2^n - 1 \wedge y < 2^n - 1$. Конечно, это рассматривается как три отдельные цели, которые доказаны один за раз. Доказательства этих трех целей включают только элементарную алгебру.

Одна из привлекательных особенностей этого доказательства – вычисление, показывающее, что $xy = 2^n - 1$. Формулы для x и y несколько сложны, и сначала их произведение выглядит еще сложнее. Приятный сюрприз случается позже, когда большая часть членов произведения сокращается и как по волшебству возникает ответ $2^n - 1$. Конечно, задним числом мы можем увидеть, что именно расчетом на это и был мотивирован выбор x и y . Однако есть один аспект этого расчета, который может вас беспокоить. Наличие в формулах символа троеточия «...» указывает на то, что доказательство зависит от фрагмента, который не раскрывается. Мы дадим более строгое доказательство того, что $xy = 2^n - 1$, в главе 6, после того как вы ознакомитесь с методом доказательства математической индукцией (см. теорему 6.5.2).

Теорема 3.7.2. Простых чисел бесконечно много.

Доказательство. Предположим, что существует только конечное количество простых чисел. Пусть p_1, p_2, \dots, p_n – список всех простых чисел. Пусть $m = p_1 p_2 \cdots p_n + 1$. Заметим, что m не делится на p_1 , поскольку деление m на p_1 дает частное $p_2 p_3 \cdots p_n$ и остаток 1. Аналогично, m не делится на любое число из последовательности p_2, p_3, \dots, p_n .

Теперь мы используем тот факт, что каждое целое число больше 1 либо простое, либо может быть записано как произведение простых чисел. (Мы приведем доказательство этого факта в главе 6 – см. теорему 6.4.2.) Ясно, что m больше 1, поэтому m – либо простое, либо произведение простых чисел. Предположим сначала, что m простое. Обратите внимание, что m больше, чем все числа в списке p_1, p_2, \dots, p_n , значит, мы обнаружили простое число, которого нет в этом списке. Но это противоречит нашему предположению, что это был список *всех* простых чисел.

Теперь предположим, что m – произведение простых чисел. Пусть q будет одним из простых чисел в этом произведении. Тогда m делится на q . Но мы уже видели, что m не делится ни на одно из чисел в списке p_1, p_2, \dots, p_n , поэтому мы снова приходим к противоречию с предположением, что в этот список включены все простые числа.

Поскольку предположение, что количество простых чисел ограничено, привело к противоречию, должно существовать бесконечно много простых чисел.

Комментарий. Поскольку бесконечность означает *не конечность*, утверждение теоремы можно рассматривать как отрицание. Поэтому неудивительно, что доказательство выстроено на противоречии. Предположение, что существует конечное число простых чисел, означает, что существует натуральное число n такое, что имеется n простых чисел, а утверждение, что существует n простых чисел, означает, что существует список различных чисел p_1, p_2, \dots, p_n таких, что каждое число в списке является простым и не существует простых чисел, которых нет в списке. Таким образом, во втором предложении доказательства применяется экзистенциальное подтверждение для введения чисел n и p_1, p_2, \dots, p_n в доказательство. На этом этапе доказательства мы имеем следующую ситуацию:

Посылки	Цель
p_1, p_2, \dots, p_n – список простых чисел	Противоречие
$\neg \exists q (q \text{ простое} \wedge q \notin \{p_1, p_2, \dots, p_n\})$	

Вторую посылку можно было бы переформулировать как положительное утверждение, но, поскольку мы проводим доказательство от противного, другим разумным подходом было бы попытаться прийти к противоречию, доказав истинность утверждения $\exists q (q \text{ простое} \wedge q \notin \{p_1, p_2, \dots, p_n\})$. Это стратегия, используемая в доказательстве. Таким образом, цель оставшейся части доказательства – показать, что существует простое число, не указанное в списке p_1, p_2, \dots, p_n .

Поскольку наша цель теперь является экзистенциальным утверждением, неудивительно, что следующим шагом доказательства является введение нового числа t без каких-либо объяснений того, как оно было выбрано. Что удивительно, так это то, что t может быть, а может и не быть тем простым числом, которое мы ищем. Загвоздка в том, что t может не быть простым. Все, в чем мы можем быть уверены, – это то, что t либо простое, либо произведение простых чисел. Поскольку это утверждение является дизъюнкцией, оно допускает доказательство с разбиением на случаи, и этот метод используется в остальной части доказательства. Хотя эти случаи явно не отмечены в доказательстве, важно понимать, что остальная часть рассуждений имеет форму доказательства по случаям. В случае 1 мы предполагаем, что t – простое число, а в случае 2 предполагаем, что оно является произведением простых чисел. В обоих случаях мы можем отыскать простое число, не указанное в списке и необходимое для завершения доказательства.

В нашем следующем доказательстве используется факториальная запись. Напомним, что для любого натурального числа n факториалом $n!$ является число $n! = 1 \cdot 2 \cdot 3 \cdots n$.

Теорема 3.7.3. Для каждого положительного целого числа n существует ряд из n последовательных натуральных целых чисел, не содержащих простых чисел.

Доказательство. Предположим, что n – натуральное целое число. Пусть $x = (n+1)! + 2$. Мы покажем, что ни одно из чисел $x, x+1, x+2, \dots, x+(n-1)$ не является простым числом. Поскольку это ряд из n последовательных натуральных чисел, это доказывает теорему.

Чтобы убедиться, что x не является простым числом, обратите внимание, что

$$x = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + 2 = 2 \cdot (1 \cdot 3 \cdot 4 \cdots (n+1) + 1).$$

Таким образом, x можно записать как произведение двух меньших положительных целых чисел, поэтому x не является простым.

Аналогично имеем

$$x+1 = 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + 3 = 3 \cdot (1 \cdot 2 \cdot 4 \cdots (n+1) + 1),$$

поэтому $x+1$ также не является простым. В общем случае можно рассмотреть любое число $x+i$, где $0 \leq i \leq n-1$. Тогда имеем

$$\begin{aligned} x+i &= 1 \cdot 2 \cdot 3 \cdot 4 \cdots (n+1) + (i+2) \\ &= (i+2) \cdot (1 \cdot 2 \cdot 3 \cdots (i+1) \cdot (i+3) \cdots (n+1) + 1), \end{aligned}$$

поэтому $x+i$ не является простым.

Комментарий. Ряд из n последовательных натуральных чисел – это последовательность вида $x, x+1, x+2, \dots, x+(n-1)$, где x – натуральное число. Следовательно, логическая форма утверждения, которое необходимо доказать, имеет вид $\forall n > 0 \exists x > 0 \forall i (0 \leq i \leq n-1 \rightarrow x+i \text{ не является простым})$, где все переменные принимают целочисленные значения. Наш план доказательства вполне

предсказуем и очевиден: пусть $n > 0$ будет произвольным, присвоим значение x , пусть i будет произвольным, а затем предположим, что $0 \leq i \leq n - 1$, и докажем, что $x + i$ не является простым. Как и в доказательстве теоремы 3.7.1, чтобы доказать, что $x + i$ не является простым, мы покажем, что его можно записать как произведение двух меньших натуральных чисел.

Перед демонстрацией того, что $x + i$ не является простым, где i – произвольное целое число от 0 до $n - 1$, доказательство включает проверки того, что x и $x + 1$ не являются простыми числами. Они совершенно не нужны и включены только для облегчения чтения доказательства.

Пример 3.7.4. Докажите, что существует единственное действительное число m со следующими двумя свойствами:

1. Для любого действительного числа x справедливо утверждение $x^2 + 2x + 3 \geq m$.
2. Если y – любое действительное число, обладающее таким свойством, что для любого действительного числа x справедливо утверждение $x^2 + 2x + 3 \geq y$, то $m \geq y$.

Стратегия доказательства

Было бы удобно назначить определение для свойства 1. Мы будем говорить, что m – это *нижняя граница* для выражения $x^2 + 2x + 3$, если выполняется свойство 1; то есть если для любого действительного числа x справедливо $x^2 + 2x + 3 \geq m$. Тогда свойство 2 говорит, что если y – любая нижняя грань для $x^2 + 2x + 3$, то $m \geq y$. Другими словами, никакая нижняя граница не может быть больше m , поэтому m – *наибольшая нижняя граница* (или *точная нижняя грань* – прим. перев.). (О низких и наибольших нижних границах мы поговорим подробнее в разделе 4.4 главы 4.)

Нам нужно будет доказать существование и единственность числа m . Что касается доказательства существования, то самая сложная его часть – найти правильное значение m . Решив следующее квадратное уравнение, мы найдем подсказку, как выбрать m :

$$x^2 + 2x + 3 = x^2 + 2x + 1 + 2 = (x + 1)^2 + 2.$$

Поскольку $(x + 1)^2$ не может быть отрицательным, для каждого действительного числа x у нас будет справедливо $x^2 + 2x + 3 = (x + 1)^2 + 2 \geq 2$, поэтому $m = 2$ соответствует свойству 1 – другими словами, число 2 является нижней гранью для $x^2 + 2x + 3$. Конечно, любое меньшее число также будет нижней гранью, но свойство 2 требует, чтобы m было *наибольшей* нижней границей, поэтому m не может быть меньше 2. Судя по всему, $m = 2$ – это правильный выбор. Посмотрим, сможем ли мы доказать свойство 2 с таким значением m .

Чтобы доказать, что свойство 2 выполняется при $m = 2$, мы должны доказать $\forall y[\forall x(x^2 + 2x + 3 \geq y) \rightarrow 2 \geq y]$. Очевидный способ продолжить доказательство – объявить у произвольным, предположить истинность утверждения $\forall x(x^2 + 2x + 3 \geq y)$, а затем доказать, что $2 \geq y$, и прийти к следующей ситуации:

Посылки	Цель
$\forall x(x^2 + 2x + 3 \geq y)$	$2 \geq y$

Естественный способ использовать эту посылку – подставить что-то вместо x . Глядя на цель, мы видим, что если бы нашлось значение x , для которого $x^2 + 2x + 3 = 2$, то подстановка этого значения x в посылку привела бы непосредственно к цели. Решая уравнение $x^2 + 2x + 3 = 2$, мы обнаруживаем, что подстановка $x = -1$ завершит доказательство.

Нам еще предстоит доказать единственность m . Для этого мы должны предположить, что m_1 и m_2 – это два числа, обладающие свойствами 1 и 2, а затем доказать, что $m_1 = m_2$. Таким образом, мы получаем следующие посылки и цель:

Посылки	Цель
$\forall x(x^2 + 2x + 3 \geq m_1)$	$m_1 = m_2$
$\forall x(x^2 + 2x + 3 \geq m_2)$	
$\forall y[\forall x(x^2 + 2x + 3 \geq y) \rightarrow m_1 \geq y]$	
$\forall y[\forall x(x^2 + 2x + 3 \geq y) \rightarrow m_2 \geq y]$	

Вероятно, нам следует применить универсальное подтверждение к одной или нескольким посылкам, но к каким именно и какие значения мы должны подставить? Ключевой момент состоит в том, что первые две посылки предполагают, что было бы полезно подставить m_1 или m_2 вместо y в третьей и четвертой посылках. Фактически мы подставляем $y = m_2$ в третьей посылке и $y = m_1$ в четвертой. (Вы можете сравнить это со стратегией, которую мы использовали для доказательства единственности в примере 3.6.2.) Это дает нам $m_1 \geq m_2$ и $m_2 \geq m_1$, откуда следует цель $m_1 = m_2$.

Решение

Теорема. Существует единственное действительное число m со следующими двумя свойствами:

1. Для любого действительного числа x справедливо утверждение $x^2 + 2x + 3 \geq m$.
2. Если y – любое действительное число, обладающее таким свойством, что для любого действительного числа x справедливо утверждение $x^2 + 2x + 3 \geq y$, то $m \geq y$.

Доказательство

Существование: пусть $m = 2$. Чтобы доказать свойство 1, пусть x – произвольное действительное число. Отсюда

$$x^2 + 2x + 3 = (x + 1)^2 + 2 \geq 2 = m,$$

как требуется по условию. Это показывает, что 2 является нижней гранью для $x^2 + 2x + 3$.

Для свойства 2 пусть y будет произвольным числом, таким, что для любого x справедливо $x^2 + 2x + 3 \geq y$. В частности, полагая $x = -1$, находим, что

$$y \leq (-1)^2 + 2(-1) + 3 = 2 = m.$$

Поскольку y был произвольным, это доказывает свойство 2.

Уникальность: предположим, что есть два числа m_1 и m_2 , обладающих свойствами 1 и 2. Другими словами, m_1 и m_2 являются нижними гранями для $x^2 + 2x + 3$, а также если y – любая нижняя грань, то $m_1 \geq y$ и $m_2 \geq y$. Применяя этот последний факт к $y = m_1$ и $y = m_2$, мы получаем $m_1 \geq m_2$ и $m_2 \geq m_1$, так что $m_1 = m_2$.

Для читателей, знакомых с определением пределов из курса матанализа, мы продемонстрируем, как с использованием методов этой главы можно разработать доказательства, включающие пределы. Читатели, которые не знакомы с определением пределов, должны пропустить этот пример.

Пример 3.7.5. Покажите, что

$$\lim_{x \rightarrow 3} \frac{2x^2 - 5x - 3}{x - 3} = 7.$$

Стратегия доказательства

Согласно определению пределов, наша цель означает, что для каждого положительного числа существует такое положительное число δ , что если x – любое число такое, что $0 < |x - 3| < \delta$, то $|(\frac{2x^2 - 5x - 3}{x - 3}) - 7| < \epsilon$. Переводя это неравенство в логические символы, мы получаем

$$\forall \epsilon > 0 \exists \delta > 0 \forall x \left(0 < |x - 3| < \delta \rightarrow \left| \frac{2x^2 - 5x - 3}{x - 3} - 7 \right| < \epsilon \right).$$

Поэтому начинаем с того, что объявляем ϵ произвольным положительным числом, а затем пытаемся найти положительное число δ , для которого мы можем доказать

$$\forall x \left(0 < |x - 3| < \delta \rightarrow \left| \frac{2x^2 - 5x - 3}{x - 3} - 7 \right| < \epsilon \right).$$

Наша работа за кулисами, связанная с нахождением δ , конечно же, не появится в доказательстве. В окончательном доказательстве мы просто напишем «Пусть $\delta =$ (некоторое положительное число)», а затем приступим к доказательству утверждения

$$\forall x \left(0 < |x - 3| < \delta \rightarrow \left| \frac{2x^2 - 5x - 3}{x - 3} - 7 \right| < \epsilon \right).$$

Прежде чем вычислить значение δ , давайте подумаем, как будет выглядеть остальная часть доказательства. Исходя из формы цели на этом этапе, мы должны продолжить, приняв x произвольным, предполагая, что $0 < |x - 3| < \delta$, а затем доказывая $|(\frac{2x^2 - 5x - 3}{x - 3}) - 7| < \epsilon$. Таким образом, полное доказательство будет иметь следующий вид:

Пусть ϵ – произвольное положительное число.

Пусть δ = (некоторое положительное число).

Пусть x – произвольное число.

Предположим, что $0 < |x - 3| < \delta$.

[Здесь приводится доказательство $|(2x^2 - 5x - 3)/(x - 3) - 7| < \epsilon$.]

Следовательно, $0 < |x - 3| < \delta \rightarrow |(2x^2 - 5x - 3)/(x - 3) - 7| < \epsilon$.

Поскольку x был произвольным, мы можем заключить, что

$\forall x (0 < |x - 3| < \delta \rightarrow |(2x^2 - 5x - 3)/(x - 3) - 7| < \epsilon)$.

Следовательно, $\exists \delta > 0 \forall x (0 < |x - 3| < \delta \rightarrow |(2x^2 - 5x - 3)/(x - 3) - 7| < \epsilon)$.

Поскольку ϵ произвольно, отсюда следует, что $\forall \epsilon > 0 \exists \delta > 0 \forall x (0 < |x - 3| < \delta \rightarrow |(2x^2 - 5x - 3)/(x - 3) - 7| < \epsilon)$.

Осталось проработать два шага. Мы должны решить, какое значение присвоить δ , и реализовать доказательство $|(2x^2 - 5x - 3)/(x - 3) - 7| < \epsilon$. Сначала мы зайдемся вторым шагом, и в ходе проработки этого шага станет ясно, какое значение мы должны использовать для δ . Посылки и цели для второго шага имеют следующий вид:

Посылки	Цель
$\epsilon > 0$	$\left \frac{2x^2 - 5x - 3}{x - 3} - 7 \right < \epsilon$
δ = (некоторое положительное число)	
$0 < x - 3 < \delta$	

Прежде всего заметим, что у нас есть $0 < |x - 3|$ как условие, поэтому $x = 3$ и, следовательно, дробь $(2x^2 - 5x - 3)/(x - 3)$ определена. Разложив числитель этой дроби на множители, находим, что

$$\left| \frac{2x^2 - 5x - 3}{x - 3} - 7 \right| = \left| \frac{(2x + 1)(x - 3)}{x - 3} - 7 \right| = |2x + 1 - 7| = |2x - 6| = 2|x - 3|.$$

Также мы имеем как условие $|x - 3| < \delta$, поэтому $2|x - 3| < 2\delta$. Объединяя это неравенство с предыдущим уравнением, мы получаем $|(2x^2 - 5x - 3)/(x - 3) - 7| < 2\delta$, и наша цель – $|(2x^2 - 5x - 3)/(x - 3) - 7| < \epsilon$. Таким образом, если мы выберем δ так, что $2\delta = \epsilon$, доказательство будет готово. Другими словами, мы должны принять $\delta = \epsilon/2$. Обратите внимание, что, поскольку $\epsilon > 0$, это положительное число, как и требовалось.

Решение

Теорема.

$$\lim_{x \rightarrow 3} \frac{2x^2 - 5x - 3}{x - 3} = 7.$$

Доказательство. Предположим, что $\epsilon > 0$. Пусть $\delta = \epsilon/2$, что также явно положительное число. Пусть x – произвольное действительное число, и предположим, что $0 < |x - 3| < \delta$. Тогда

$$\begin{aligned} \left| \frac{2x^2 - 5x - 3}{x - 3} - 7 \right| &= \left| \frac{(2x + 1)(x - 3)}{x - 3} - 7 \right| = |2x + 1 - 7| = |2x - 6| = 2|x - 3| < 2\delta \\ &= 2\left(\frac{\epsilon}{2}\right) = \epsilon. \end{aligned}$$

Упражнения

- P_D*1. Предположим, что \mathcal{F} – семейство множеств. Докажите, что существует единственное множество A , обладающее следующими двумя свойствами:
- $\mathcal{F} \subseteq \mathcal{P}(A)$.
 - $\forall B (\mathcal{F} \subseteq \mathcal{P}(B) \rightarrow A \subseteq B)$.
- (Подсказка: сначала рассмотрите пример. Пусть $\mathcal{F} = \{\{1, 2, 3\}, \{2, 3, 4\}, \{3, 4, 5\}\}$. Можете ли вы найти множество A , у которого есть свойства (a) и (b)?)
2. Докажите, что существует единственное положительное вещественное число m , которое обладает следующими двумя свойствами:
- Для любого положительного действительного числа x справедливо $\frac{x}{x+1} < m$.
 - Если y – любое положительное действительное число, обладающее таким свойством, что для любого положительного действительного числа x справедливо $\frac{x}{x+1} < m$, то $m \leq y$.
- P_D3. Предположим, что A и B – множества. Что вы можете доказать относительно $\mathcal{P}(A \setminus B) \setminus (\mathcal{P}(A) \setminus \mathcal{P}(B))$? (Нет, это выражение не равно \emptyset . Попробуйте несколько примеров и посмотрите, что у вас получится.)
- P_D4. Предположим, что A, B и C – множества. Докажите, что следующие утверждения эквивалентны:
- $(A \Delta C) \cap (B \Delta C) = \emptyset$.
 - $A \cap B \subseteq C \subseteq A \cup B$. (Примечание: это сокращенный способ записать, что $A \cap B \subseteq C$ и $C \subseteq A \cup B$.)
 - $A \Delta C \subseteq A \Delta B$.
- *5. Предположим, что $\{A_i \mid i \in I\}$ – это семейство множеств. Докажите, что если $P(\bigcup_{i \in I} A_i) \subseteq \bigcup_{i \in I} \mathcal{P}(A_i)$, то существует такое $i \in I$, что $\forall j \in I (A_j \subseteq A_i)$.
6. Предположим, что \mathcal{F} – непустое семейство множеств. Пусть $I = \bigcup \mathcal{F}$ и $J = \bigcup \mathcal{F}$. Предположим также, что $J \neq \emptyset$, и заметим, что из этого следует, что для любого $X \in \mathcal{F}$ $X \neq \emptyset$, а также $I \neq \emptyset$. Наконец, пусть $\{A_i \mid i \in I\}$ – индексированное семейство множеств.
- Докажите, что $\bigcup_{i \in I} A_i = \bigcup_{x \in \mathcal{F}} (\bigcup_{i \in X} A_i)$.
 - Докажите, что $\bigcup_{i \in I} A_i = \bigcup_{x \in \mathcal{F}} (\bigcup_{i \in X} A_i)$.

- (c) Докажите, что $\bigcup_{i \in J} A_i \subseteq \bigcup_{x \in F} (\bigcup_{i \in X} A_i)$. Всегда ли $\bigcup_{i \in J} A_i = \bigcup_{x \in F} (\bigcup_{i \in X} A_i)$? Приведите доказательство или контрпример, чтобы оправдать свой ответ.
- (d) Найдите и докажите теорему, связывающую $\bigcup_{i \in I} A_i$ и $\bigcup_{x \in F} (\bigcup_{i \in X} A_i)$.
7. Докажите, что $\lim_{x \rightarrow 2} \frac{3x^2 - 12}{x - 2} = 12$.
- *8. Докажите, что если $\lim_{x \rightarrow c} f(x) = L$ и $L > 0$, то существует такое число $\delta > 0$, что для всех x если $0 < |x - c| < \delta$, то $f(x) > 0$.
9. Докажите, что если $\lim_{x \rightarrow c} f(x) = L$, то $\lim_{x \rightarrow c} 7f(x) = 7L$.
- *10. Рассмотрим следующую предположительную теорему.

Предположительная теорема. Существуют иррациональные числа a и b такие, что a^b рационально.

Правильно ли следующее доказательство? Если да, то какие стратегии доказательства оно использует? Если доказательство ошибочно, можно ли исправить ошибку? Верна ли теорема? (Примечание: в доказательстве используется тот факт, что $\sqrt{2}$ иррационален. Мы докажем это в главе 6 – см. теорему 6.4.5.)

Доказательство. Либо число $\sqrt{2}^{\sqrt{2}}$ рационально, либо иррационально.

Случай 1. $\sqrt{2}^{\sqrt{2}}$ рационально. Пусть $a = b = \sqrt{2}$. Тогда a и b иррациональны, и $a^b = \sqrt{2}^{\sqrt{2}}$, которое мы полагаем в этом случае рациональным.

Случай 2. $\sqrt{2}^{\sqrt{2}}$ иррационально. Пусть $a = \sqrt{2}^{\sqrt{2}}$ и $b = \sqrt{2}$. Тогда a иррационально по условию, и мы знаем, что b также иррационально. Также

$$a^b = \left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^{(\sqrt{2} \cdot \sqrt{2})} = (\sqrt{2})^2 = 2,$$

что является рациональным числом.

Глава 4

Соответствия

4.1. УПОРЯДОЧЕННЫЕ ПАРЫ И ДЕКАРТОВЫ ПРОИЗВЕДЕНИЯ

В главе 1 мы обсудили множества истинности для утверждений, содержащих одну свободную переменную. В данной главе мы расширяем это понятие и включаем в него утверждения с более чем одной свободной переменной.

Например, предположим, что $P(x, y)$ – это утверждение с двумя свободными переменными x и y . Мы не можем говорить об этом утверждении как об истинном или ложном, пока не укажем два значения – одно для x и другое для y . Следовательно, если мы хотим, чтобы множество истинности определяло, какие значения свободных переменных делают утверждение истинным, то множество истинности должно содержать не отдельные значения, а пары значений. Мы будем указывать пары значений, записывая два значения в скобках, разделенных запятой. Например, пусть $D(x, y)$ означает « x делит y ». Тогда утверждение $D(6, 18)$ истинно, так как $6 \mid 18$, а пара значений $(6, 18)$ представляет собой присвоение значений переменным x и y , что делает утверждение $D(x, y)$ истинным. Обратите внимание, что 18 не делит 6 , поэтому пара значений $(18, 6)$ делает утверждение $D(x, y)$ ложным. Поэтому мы должны различать пары $(18, 6)$ и $(6, 18)$. Поскольку расстановка значений в паре имеет значение, мы будем называть пару (a, b) *упорядоченной парой с первой координатой a и второй координатой b* .

Вы, вероятно, встречали упорядоченные пары раньше, когда изучали точки на плоскости xy . Использование координат x и y для идентификации точек на плоскости работает путем назначения каждой точке на плоскости упорядоченной пары, координаты которой являются координатами x и y точки. Пары должны быть упорядочены, потому что, например, точки $(2, 5)$ и $(5, 2)$ – это разные точки на плоскости. В данном случае координаты упорядоченных пар – действительные числа, но упорядоченные пары могут иметь что угодно в качестве своих координат. Например, предположим, что мы используем $C(x, y)$ для записи утверждения « x имеет у детей». В этом утверждении переменная x охватывает множество всех людей, а y – множество всех натуральных чисел. Таким образом, единственными упорядоченными пары, которые

имеет смысл учитывать при обсуждении значений переменных x и y в этом утверждении, – это пары, в которых первая координата – это человек, а вторая – натуральное число. Например, присвоение (Принц Чарльз, 2) делает утверждение $C(x, y)$ истинным, потому что у принца Чарльза действительно двое детей, тогда как присваивание (Анджелина Джоли, 37) делает утверждение ложным. Обратите внимание, что назначение (2, принц Чарльз) не имеет смысла, потому что оно приводит к бессмысленному утверждению «у 2 детей имеется принц Чарльз».

В общем, если $P(x, y)$ – это утверждение, в котором x располагается в некотором множестве A , а y – в множестве B , то лишь значения x и y , имеющие смысл в $P(x, y)$ будут упорядоченными парами, в которых первая координата является элементом A , а вторая – элементом B . Поэтому мы даем следующее определение:

Определение 4.1.1. Предположим, что A и B – множества. Тогда *декартово произведение* A и B , обозначаемое $A \times B$, – это множество всех упорядоченных пар, в которых первая координата является элементом A , а вторая – элементом B . Другими словами,

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

Пример 4.1.2.

1. Если $A = \{\text{красный}, \text{зеленый}\}$ и $B = \{2, 3, 5\}$, то $A \times B = \{(\text{красный}, 2), (\text{красный}, 3), (\text{красный}, 5), (\text{зеленый}, 2), (\text{зеленый}, 3), (\text{зеленый}, 5)\}$.
2. Если $P = \{\text{человек}\}$ – множество всех людей, то $P \times \mathbb{N} = \{(p, n) \mid p - \text{человек}, n - \text{натуральное число}\} = \{(\text{Принц Чарльз}, 0), (\text{Принц Чарльз}, 1), (\text{Принц Чарльз}, 2), (\text{Анджелина Джоли}, 0), (\text{Анджелина Джоли}, 1), \dots\}$. Это упорядоченные пары, значения которых имеет смысл присваивать свободным переменным x и y в утверждении $C(x, y)$.
3. $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \text{ и } y - \text{действительные числа}\}$. Это координаты всех точек на плоскости. По понятным причинам это множество иногда обозначают как \mathbb{R}^2 .

Введение нового математического понятия дает нам возможность попрактиковаться в методике доказательства, доказав некоторые основные свойства новой концепции. Вот теорема, излагающая некоторые основные свойства декартовых произведений.

Теорема 4.1.3. Предположим, что A, B, C и D – множества. Тогда

1. $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
2. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
3. $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D)$.
4. $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.
5. $A \times \emptyset = \emptyset \times A = \emptyset$.

Доказательство 1. Пусть p – произвольный элемент из $A \times (B \cap C)$. Тогда по определению декартова произведения p должна быть упорядоченной парой, первая координата которой является элементом A , а вторая координата – элементом $B \cap C$. Другими словами, $p = (x, y)$ для некоторых $x \in A$ и $y \in B \cap C$. Поскольку

$y \in B \cap C$, то $y \in B$ и $y \in C$. Так как $x \in A$ и $y \in B$, то $p = (x, y) \in A \times B$, и аналогично $p \in A \times C$. Таким образом, $p \in (A \times B) \cap (A \times C)$. Поскольку p был произвольным элементом $A \times (B \cap C)$, отсюда следует, что $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$.

Пусть теперь p – произвольный элемент из $(A \times B) \cap (A \times C)$. Тогда $p \in A \times B$, поэтому $p = (x, y)$ для некоторых $x \in A$ и $y \in B$. Кроме того, $(x, y) = p \in A \times C$, поэтому $y \in C$. Так как $y \in B$ и $y \in C$, то $y \in B \cap C$. Таким образом, $p = (x, y) \in A \times (B \cap C)$. Поскольку p был произвольным элементом из $(A \times B) \cap (A \times C)$, мы можем заключить, что $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$, поэтому $A \times (B \cap C) = (A \times B) \cap (A \times C)$.

Комментарий. Прежде чем продолжить доказательство остальных частей, дадим краткий комментарий к только что приведенному доказательству. Утверждение 1 представляет собой уравнение связи между двумя множествами, поэтому, как мы показали в примере 3.4.5, есть два естественных подхода, которые мы могли бы использовать для его доказательства. Мы могли бы доказать $\forall p [p \in A \times (B \cap C) \leftrightarrow p \in (A \times B) \cap (A \times C)]$ или два отдельных утверждения $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$ и $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$. В этом доказательстве мы использовали второй подход. В первом абзаце мы доказываем $A \times (B \cap C) \subseteq (A \times B) \cap (A \times C)$, а во втором – $(A \times B) \cap (A \times C) \subseteq A \times (B \cap C)$.

В первом из этих двух доказательств мы используем обычный подход, принимая за p произвольный элемент из $A \times (B \cap C)$, а затем доказываем $p \in (A \times B) \cap (A \times C)$. Поскольку $p \in A \times (B \cap C)$ означает $\exists x \exists y (x \in A \wedge y \in B \cap C \wedge p = (x, y))$, мы немедленно вводим переменные x и y путем экзистенциального подтверждения. Остальная часть доказательства включает простое развертывание определений задействованных операций теории множеств. Доказательство противоположной инклузии во втором абзаце производится аналогично.

Обратите внимание, что в обеих частях этого доказательства мы ввели произвольный объект p , который оказался упорядоченной парой, и поэтому мы могли сказать, что $p = (x, y)$ для некоторых объектов x и y . В большинстве доказательств, связанных с декартовыми произведениями, математики игнорируют этот шаг. Если с самого начала ясно, что объект окажется упорядоченной парой, обычно он с самого начала просто называется (x, y) . Мы будем следовать этой практике в наших доказательствах.

Мы оставляем доказательства утверждений 2 и 3 в качестве упражнений (см. упражнение 5).

Доказательство 4. Пусть (x, y) – произвольный элемент из $(A \times B) \cup (C \times D)$. Тогда либо $(x, y) \in A \times B$, либо $(x, y) \in C \times D$.

Случай 1. $(x, y) \in A \times B$. Тогда $x \in A$ и $y \in B$, поэтому ясно, что $x \in A \cup C$ и $y \in B \cup D$. Следовательно, $(x, y) \in (A \cup C) \times (B \cup D)$.

Случай 2. $(x, y) \in C \times D$. Аналогичное рассуждение показывает, что $(x, y) \in (A \cup C) \times (B \cup D)$.

Поскольку (x, y) был произвольным элементом из $(A \times B) \cup (C \times D)$, отсюда следует, что $(A \times B) \cup (C \times D) \subseteq (A \cup C) \times (B \cup D)$.

Доказательство 5. Предположим, что $A \times \emptyset \neq \emptyset$. Тогда $A \times \emptyset$ имеет по крайней мере один элемент, и по определению декартова произведения этот элемент должен быть упорядоченной парой (x, y) для некоторых $x \in A$ и $y \in \emptyset$. Но это

невозможно, потому что \emptyset не имеет элементов. Следовательно, $A \times \emptyset = \emptyset$. Доказательство того, что $\emptyset \times A = \emptyset$, аналогично.

Комментарий. В утверждении 4 говорится, что одно множество является подмножеством другого, и доказательство строится по обычному шаблону для утверждений этого типа: мы начинаем с произвольного элемента первого множества, а затем доказываем, что это элемент второго множества. Ясно, что произвольный элемент первого множества должен быть упорядоченной парой, поэтому мы записали его как упорядоченную пару с самого начала.

Таким образом, для остальной части доказательства мы имеем $(x, y) \in (A \times B) \cup (C \times D)$ как посылку, и цель состоит в том, чтобы доказать, что $(x, y) \in (A \cup C) \times (B \cup D)$. Посылка означает $(x, y) \in A \times B \vee (x, y) \in C \times D$, поэтому подходящей стратегией будет доказательство по случаям. В каждом случае цель легко доказать.

Утверждение 5 означает, что $A \times \emptyset = \emptyset \wedge \emptyset \times A = \emptyset$, поэтому мы рассматриваем это как две цели и по отдельности доказываем $A \times \emptyset = \emptyset$ и $\emptyset \times A = \emptyset$. Утверждение, что множество равно пустому множеству, на самом деле является отрицательным утверждением, хотя на первый взгляд не выглядит таковым, потому что оно означает, что множество не имеет никаких элементов. Поэтому неудивительно, что доказательство $A \times \emptyset = \emptyset$ проводится от противного. Предположение, что $A \times \emptyset \neq \emptyset$, означает $\exists p(p \in A \times \emptyset)$, поэтому наш следующий шаг – ввести имя для элемента $A \times \emptyset$. Здесь тоже ясно, что новый объект, представленный в доказательстве, является упорядоченной парой, поэтому мы с самого начала записываем его как упорядоченную пару (x, y) . Расшифровка смысла записи $(x, y) \in A \times \emptyset$ сразу приводит к противоречию.

Доказательство утверждения $\emptyset \times A = \emptyset$ устроено аналогично, но сказать об этом – еще не значит доказать. Таким образом, слова о том, что эта часть доказательства аналогична, на самом деле указывают лишь на то, что вторая половина доказательства остается в качестве упражнения. Вы должны проработать детали этого доказательства в уме (или, если необходимо, записать их на бумаге), чтобы убедиться, что доказательство, аналогичное рассмотренному в первой половине, действительно сработает.

Поскольку порядок координат в упорядоченной паре имеет значение, $A \times B$ и $B \times A$ означают разные вещи. Бывает ли, что $A \times B = B \times A$? Что ж, это возможно, если $A = B$. Ясно, что если $A = B$, то $A \times B = A \times A = B \times A$. Есть ли другие возможности?

Рассмотрим неправильное доказательство того, что $A \times B = B \times A$, только если $A = B$: первые координаты упорядоченных пар в $A \times B$ берутся из A , а первые координаты упорядоченных пар в $B \times A$ берутся из B . Если $A \times B = B \times A$, то первые координаты в этих двух множествах должны быть одинаковыми, поэтому $A = B$.

Это хороший пример того, почему важно придерживаться правил составления доказательств, которые мы изучили, вместо того чтобы убеждать самого себя в любых доводах, которые кажутся правдоподобными. Неформальные рассуждения в предыдущем абзаце неверны, и мы можем найти ошибку, переформулировав это рассуждение как формальное доказательство. Предположим, что $A \times B = B \times A$. Чтобы доказать, что $A = B$, мы можем принять за

x произвольный элемент, а затем попытаться доказать утверждения $x \in A \rightarrow x \in B$ и $x \in B \rightarrow x \in A$. Для первого из них мы предполагаем $x \in A$ и пытаемся доказать $x \in B$. Теперь в соответствии с ходом неправильного доказательства нам следует попытаться показать, что x является первой координатой некоторой упорядоченной пары в $A \times B$, а затем использовать тот факт, что $A \times B = B \times A$. Мы могли бы сделать это, попытавшись найти некоторый объект $y \in B$ и затем сформировав упорядоченную пару (x, y) . Тогда у нас было бы $(x, y) \in A \times B$ и $A \times B = B \times A$, и из этого следовало бы, что $(x, y) \in B \times A$ и, следовательно, $x \in B$. Но как мы можем найти объект $y \in B$? У нас нет никакой информации о B , кроме того факта, что $A \times B = B \times A$. Фактически B может быть пустым множеством! Это недостаток доказательства. Если $B = \emptyset$, то выбрать $y \in B$ будет невозможно, и доказательство развалится. По тем же причинам другая половина доказательства не будет работать, если $A = \emptyset$.

Мы не только нашли ошибку в доказательстве, но теперь можем понять, что с ней делать. Мы должны принять во внимание возможность того, что A или B могут быть пустым множеством.

Теорема 4.1.4. Предположим, что A и B – множества. Тогда $A \times B = B \times A$, если и только если либо $A = \emptyset$ и $B = \emptyset$, либо $A = B$.

Доказательство. (\rightarrow) Предположим, что $A \times B = B \times A$. Если $A = \emptyset$ или $B = \emptyset$, то доказывать больше нечего, поэтому предположим, что $A \neq \emptyset$ и $B \neq \emptyset$. Мы покажем, что $A = B$. Пусть x – произвольный элемент, и предположим, что $x \in A$. Поскольку $B \neq \emptyset$, мы можем выбрать некоторое $y \in B$. Тогда $(x, y) \in A \times B = B \times A$, поэтому $x \in B$.

Теперь предположим, что $x \in B$. Поскольку $A \neq \emptyset$, мы можем выбрать некоторый $z \in A$. Следовательно, $(x, z) \in B \times A = A \times B$, поэтому $x \in A$. Таким образом, $A = B$, что и требовалось доказать.

(\leftarrow) Предположим, что либо $A = \emptyset$, $B = \emptyset$, либо $A = B$.

Случай 1. $A = \emptyset$. Тогда $A \times B = \emptyset \times B = \emptyset = B \times \emptyset = B \times A$.

Случай 2. $B = \emptyset$. Аналогично случаю 1.

Случай 3. $A = B$. Тогда $A \times B = A \times A = B \times A$.

Комментарий. Конечно, доказываемое утверждение является утверждением типа «если и только если», поэтому мы доказываем оба направления по отдельности. Для направления \rightarrow наша цель – $A = \emptyset \vee B = \emptyset \vee A = B$, что можно записать как $(A = \emptyset \vee B = \emptyset) \vee A = B$, поэтому с помощью одной из наших стратегий дизъюнкций из главы 3 мы можем предположить $\neg(A = \emptyset \vee B = \emptyset)$ и доказать, что $A = B$. Обратите внимание, что по одному из законов Де Моргана $\neg(A = \emptyset \vee B = \emptyset)$ эквивалентно $A = \emptyset \wedge B = \emptyset$, поэтому мы рассматриваем это как два предположения – $A = \emptyset$ и $B = \emptyset$. Конечно, мы могли поступить иначе, например предположив $A = B$ и $B = \emptyset$ и затем доказав $A = \emptyset$. Но вспомним из комментария к части 5 теоремы 4.1.3, что $A = \emptyset$ и $B = \emptyset$ на самом деле являются отрицательными утверждениями, поэтому, поскольку обычно лучше работать с положительными, чем с отрицательными утверждениями, нам лучше отрицать их оба, чтобы получить предположения $A = \emptyset$ и $B = \emptyset$, а затем доказать положительное утверждение $A = B$. Предположения $A = \emptyset$ и $B = \emptyset$ являются экзистенциальными утверждениями, поэтому они используются

в доказательстве для обоснования введения u и z . Доказательство того, что $A = B$, проводится очевидным образом, вводится произвольный объект x и затем доказывается $x \in A \leftrightarrow x \in B$.

Для направления доказательства \leftarrow мы имеем $A = \emptyset \vee B = \emptyset \vee A = B$ как посылку, поэтому естественно использовать доказательство по случаям. В любом случае цель легко доказать.

Эта теорема – лучшая иллюстрация того, как на самом деле работает математика, чем большинство примеров, которые мы видели до сих пор. Обычно, когда вы пытаетесь найти ответ на математический вопрос, вы заранее не знаете, каким будет ответ. Возможно, вы сможете угадать ответ и будете иметь представление о том, как могло бы пройти доказательство, но ваше предположение может быть неверным, а ваша идея доказательства может быть ошибочной. Только превратив свою идею в формальное доказательство в соответствии с правилами главы 3, вы можете быть уверены, что ваш ответ верен. Часто в процессе разработки формального доказательства вы обнаруживаете изъян в своих рассуждениях, как мы это делали ранее, и вам, возможно, придется пересмотреть свои идеи, чтобы устраниить этот недостаток. Окончательная теорема и доказательство часто являются результатом целой череды проб, ошибок и исправлений. Конечно, когда математики пишут свои теоремы и доказательства, они следуют нашему правилу, согласно которому доказательства нужны для обоснования теорем, а не для объяснения мыслительных процессов, и поэтому они не описывают все ошибки, которые они сделали. И хотя математики не объясняют свои ошибки в доказательствах, вы не должны заблуждаться, думая, что они их не делают!

Теперь, когда мы знаем, как использовать упорядоченные пары и декартовы произведения, чтобы рассуждать о присвоении значений свободным переменным, мы готовы определить множества истинности для утверждений, содержащих две свободные переменные.

Определение 4.1.5. Предположим, что $P(x, y)$ – это оператор с двумя свободными переменными, в котором x принадлежит множеству A , а y – множеству B . Тогда $A \times B$ – это множество всех значений x и y , которые имеют смысл в утверждении $P(x, y)$. *Множество истинности* $P(x, y)$ – это подмножество $A \times B$, состоящее из тех значений, которые делают утверждение истинным. Другими словами, множество истинности $P(x, y)$ – это множество $\{(a, b) \in A \times B \mid P(a, b)\}$.

Пример 4.1.6. Каковы множества истинности следующих утверждений?

1. « x имеет y детей», где x пробегает множество P всех людей, а y пробегает \mathbb{N} .
2. « x находится в y », где x распространяется на множество C всех городов, а y распространяется на множество N всех стран.
3. « $y = 2x - 3$ », где x и y пробегают \mathbb{R} .

Решения

1. $\{(p, n) \in P \times \mathbb{N} \mid y$ человека p есть n детей $\} = \{(принц Чарльз, 2), \dots\}$.
2. $\{(c, n) \in C \times N \mid$ город c расположен в стране $n\} = \{(Нью-Йорк, США), (Токио, Япония), (Париж, Франция), \dots\}$.

3. $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 2x - 3\} = \{(0, -3), (1, -1), (2, 1), \dots\}$. Вы, вероятно, уже знакомы с тем фактом, что упорядоченные пары в этом множестве представляют собой координаты точек на плоскости, лежащих вдоль определенной прямой линии, называемой графиком уравнения $y = 2x - 3$. Таким образом, вы можете считать график уравнения изображением его множества истинности!

Многие факты о множествах истинности для утверждений с одной свободной переменной, которые мы обсуждали в главе 1, переносятся на множества истинности для утверждений с двумя свободными переменными. Например, предположим, что T – это множество истинности утверждения $P(x, y)$, где x пробегает некоторое множество A , а y – множество B . Тогда для любых $a \in A$ и $b \in B$ утверждение $(a, b) \in T$ означает то же самое, что и $P(a, b)$. Кроме того, если $P(x, y)$ истинно для всех $x \in A$ и $y \in B$, то $T = A \times B$, а если $P(x, y)$ ложно для любых $x \in A$ и $y \in B$, то $T = \emptyset$. Если S – это множество истинности другого утверждения $Q(x, y)$, тогда множеством истинности утверждения $P(x, y) \wedge Q(x, y)$ является $T \cap S$, а множество истинности $P(x, y) \vee Q(x, y)$ – это $T \cup S$.

Хотя до конца этой главы мы будем рассматривать только упорядоченные пары, можно работать с упорядоченными тройками, упорядоченными четверками и т. д. Их можно использовать, чтобы говорить о множествах истинности для утверждений, содержащих три или более свободных переменных. Например, пусть $L(x, y, z)$ означает утверждение « x прожил в y в течение z лет», где x пробегает множество P всех людей, y пробегает множество C всех городов, а $z \in \mathbb{N}$. Тогда множества значений свободных переменных, имеющих смысл в этом утверждении, будут упорядоченными тройками (p, c, n) , где p – человек, c – город, а n – натуральное число. Множество всех таких упорядоченных троек будет записано как $P \times C \times \mathbb{N}$, а множество истинности утверждения $L(x, y, z)$ можно объявить как $\{(p, c, n) \in P \times C \times \mathbb{N} \mid \text{человек } p \text{ прожил в городе } c \text{ лет}\}$.

Упражнения

- *1. Каковы множества истинности следующих утверждений? Перечислите несколько элементов каждого множества истинности.
 - (a) « x – родитель y », где x и y пробегают множество P всех людей.
 - (b) «Есть кто-то, кто живет в x и посещает y », где x пробегает множество C всех городов, а y пробегает множество U всех университетов.
- 2. Каковы множества истинности следующих утверждений? Перечислите несколько элементов каждого множества истинности.
 - (a) « x живет в y », где x пробегает множество P всех людей, а y пробегает множество C всех городов.
 - (b) «Население x равно y », где x распространяется на множество C всех городов, а y пробегает \mathbb{N} .
- 3. Множества истинности следующих утверждений являются подмножествами \mathbb{R}^2 . Перечислите несколько элементов каждого множества ис-

тинности. Изобразите графически все точки на плоскости, координаты которых находятся в множестве истинности.

- (a) $y = x^2 - x - 2$.
- (b) $y < x$.
- (c) Либо $y = x^2 - x - 2$, либо $y = 3x - 2$.
- (d) $y < x$, и либо $y = x^2 - x - 2$, либо $y = 3x - 2$.

*4. Пусть $A = \{1, 2, 3\}$, $B = \{1, 4\}$, $C = \{3, 4\}$ и $D = \{5\}$. Вычислите все множества, упомянутые в теореме 4.1.3, и убедитесь, что все части теоремы верны.

5. Докажите п. 2 и 3 теоремы 4.1.3.

*6. Что неправильно в следующем доказательстве того, что для любых множеств A , B , C и D справедливо $(A \cup C) \times (B \cup D) \subseteq (A \times B) \cup (C \times D)$? (Отметим, что это обратная версия инклузии в части 4 теоремы 4.1.3.)

Доказательство. Пусть $(x, y) \in (A \cup C) \times (B \cup D)$. Тогда $x \in A \cup C$ и $y \in B \cup D$, поэтому либо $x \in A$, либо $x \in C$ и либо $y \in B$, либо $y \in D$. Мы рассматриваем эти случаи отдельно.

Случай 1. $x \in A$ и $y \in B$. Тогда $(x, y) \in A \times B$.

Случай 2. $x \in C$ и $y \in D$. Тогда $(x, y) \in C \times D$.

Таким образом, либо $(x, y) \in A \times B$, либо $(x, y) \in C \times D$, поэтому $(x, y) \in (A \times B) \cup (C \times D)$.

7. Если A имеет m элементов, а B имеет n элементов, сколько элементов у $A \times B$?

P_D*8. Верно ли, что для любых множеств A , B и C справедливо равенство $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$? Приведите доказательство или контрпример, чтобы обосновать свой ответ.

P_D9. Докажите, что для любых множеств A , B и C справедливо равенство $A \times (B \Delta C) = (A \times B) \Delta (A \times C)$.

P_D*10. Докажите, что для любых множеств A , B , C и D справедливо выражение $(A \setminus C) \times (B \setminus D) \subseteq (A \times B) \setminus (C \times D)$.

P_D11. Докажите, что для любых множеств A , B , C и D справедливо равенство $(A \times B) \setminus (C \times D) = [A \times (B \setminus D)] \cup [(A \setminus C) \times B]$.

P_D12. Докажите, что для любых множеств A , B , C и D , если $A \times B$ и $C \times D$ не пересекаются, то либо A и C не пересекаются, либо B и D не пересекаются.

13. Предположим, что $I = \emptyset$. Докажите, что для любого индексированного семейства множеств $\{A_i \mid i \in I\}$ и любого множества B справедливо равенство $(\bigcap_{i \in I} A_i) \times B = \bigcap_{i \in I} (A_i \times B)$. Где в доказательстве используется предположение, что $I = \emptyset$?

14. Пусть $\{A_i \mid i \in I\}$ и $\{B_i \mid i \in I\}$ – индексированные семейства множеств.

(a) Докажите, что $\bigcap_{i \in I} (A_i \times B_i) \subseteq (\bigcap_{i \in I} A_i) \times (\bigcap_{i \in I} B_i)$.

(b) Для каждого $(i, j) \in I \times I$ пусть $C_{i,j} = A_i \times B_j$, и пусть $P = I \times I$. Докажите, что $\bigcup_{p \in P} C_p = \bigcup_{i \in I} B_i$.

*15. Этую проблему предложил профессор Алан Тейлор из Юнион-колледжа, штат Нью-Йорк. Рассмотрим следующую предположительную теорему.

Предположительная теорема. Для любых множеств A, B, C и D если $A \times B \subseteq C \times D$, то $A \subseteq C$ и $B \subseteq D$.

Правильно ли следующее доказательство? Если да, то какие стратегии доказательства в нем задействованы? Если нет, можно ли его исправить? Верна ли теорема?

Доказательство. Предположим, что $A \times B \subseteq C \times D$. Пусть a – произвольный элемент из A и b – произвольный элемент из B . Тогда $(a, b) \in A \times B$, и поскольку $A \times B \subseteq C \times D$, то $(a, b) \in C \times D$. Следовательно, $a \in C$ и $b \in D$. Поскольку a и b были произвольными элементами A и B , соответственно, из этого следует, что $A \subseteq C$ и $B \subseteq D$.

4.2. Соответствия

Предположим, что $P(x, y)$ – это оператор с двумя свободными переменными x и y . Часто такое утверждение можно рассматривать как выражение *соответствия* (или *отношения*) между x и y . Множество истинности утверждения $P(x, y)$ – это множество упорядоченных пар, которые записывают, когда это соответствие выполняется. Возможно, вам будет удобно думать о некотором множестве упорядоченных пар как о реестре записей всех случаев, когда существует какое-либо соответствие. В этом заключается смысл следующего определения.

Определение 4.2.1. Предположим, что A и B – множества. Тогда множество $R \subseteq A \times B$ называется *соответствием из A в B*.

Если x пробегает A , а y пробегает B , то очевидно, что множество истинности любого утверждения $P(x, y)$ будет соответствием из A в B . Однако обратите внимание, что определение 4.2.1 не требует, чтобы множество упорядоченных пар было определено как множество истинности некоторого утверждения про множество, которое является соответствием. Хотя размышления о множествах истинности послужили основой для этого определения, оно ничего явно не говорит о таковых. Согласно определению, любое подмножество $A \times B$ следует называть соответствием из A в B .

Пример 4.2.2. Вот несколько примеров соответствий из одного множества в другое.

- Пусть $A = \{1, 2, 3\}$, $B = \{3, 4, 5\}$ и $R = \{(1, 3), (1, 5), (3, 3)\}$. Тогда $R \subseteq A \times B$, поэтому R является соответствием из A в B .
- Пусть $G = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x > y\}$. Тогда G – соответствие из \mathbb{R} в \mathbb{R} .
- Пусть $A = \{1, 2\}$ и $B = \mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$. Пусть $E = \{(x, y) \in A \times B \mid x \in y\}$. Тогда E является соответствием из A в B . В этом случае $E = \{(1, \{1\}), (1, \{1, 2\}), (2, \{2\}), (2, \{1, 2\})\}$.

В следующих трех примерах пусть S – это множество всех студентов в вашем учебном заведении, R – множество всех комнат в общежитии, P – множество всех профессоров, а C – множество всех курсов.

4. Пусть $L = \{(s, r) \in S \times R \mid \text{студент живет в комнате общежития } r\}$. Тогда L – соответствие из S в R .
5. Пусть $E = \{(s, c) \in S \times C \mid \text{студент } s \text{ зачислен на курс } c\}$. Тогда E – соответствие из S в C .
6. Пусть $T = \{(c, p) \in C \times P \mid \text{курс } c \text{ ведет профессор } p\}$. Тогда T – соответствие из C в P .

До сих пор мы занимались в основном развитием ваших навыков доказательства. Еще один важный навык в математике – это способность понимать и применять новые определения. Вот определения нескольких новых понятий, связанных с соответствиями. Вскоре мы приведем примеры, иллюстрирующие эти понятия, но сначала посмотрим, умеете ли вы понимать концепции, исходя из определений.

Определение 4.2.3. Предположим, что R является соответствием из A в B . Тогда *область определения* (domain) R – это множество

$$\text{Dom}(R) = \{a \in A \mid \exists b \in B ((a, b) \in R)\}.$$

Множество значений (range) R – это множество

$$\text{Ran}(R) = \{b \in B \mid \exists a \in A ((a, b) \in R)\}.$$

Обратным к R является соответствие R^{-1} из B в A , определяемое следующим образом:

$$R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}.$$

Наконец, предположим, что R – это соответствие из A в B , а S – это соответствие из B в C . Тогда *композиция* S и R – это соответствие $S \circ R$ из A в C , определенное следующим образом:

$$S \circ R = \{(a, c) \in A \times C \mid \exists b \in B ((a, b) \in R \text{ и } (b, c) \in S)\}.$$

Обратите внимание, что мы предположили, что вторые координаты пар в R и первые координаты пар в S происходят из одного и того же множества B , потому что это ситуация, в которой нас чаще всего будет интересовать $S \circ R$. Однако в этом ограничении нет необходимости, как мы просим вас показать в упражнении 15.

Согласно определению 4.2.3 область определения соответствия из A в B – это множество, содержащее все первые координаты упорядоченных пар в соответствии. В общем, это будет подмножество A , но не обязательно все A . Например, рассмотрим соответствие L из части 4 примера 4.2.2, которое объединяет студентов с комнатами общежития, в которых они живут. Область определения L будет содержать всех студентов, которые фигурируют в качестве первой координаты в какой-либо упорядоченной паре в L – другими словами, всех студентов, которые живут в какой-либо комнате общежития, –

но не будет содержать, например, студентов, которые живут в квартирах за пределами кампуса. Уточнив исходное определение, мы получим:

$$\begin{aligned}\text{Dom}(L) &= \{s \in S \mid \exists r \in R((s, r) \in L)\} \\ &= \{s \in S \mid \exists r \in R(\text{студент } s \text{ живет в комнате общежития } r)\} \\ &= \{s \in S \mid \text{студент } s \text{ живет в какой-то комнате общежития}\}.\end{aligned}$$

Точно так же множество значений – это множество, содержащее все вторые координаты упорядоченных пар. Например, множество значений соответствия L будет множеством всех комнат общежития, в которых живет какой-то студент. Любые незанятые комнаты в общежитии не попадают в зону охвата L .

Обратное соответствие содержит точно такие же упорядоченные пары, что и исходное, но с обратным порядком координат каждой пары. Таким образом, в случае соответствия L , если студент Джо Смит живет в комнате 213 общежития Дэвис-Холл, то $(\text{Джо Смит}, 213 \text{ Дэвис-Холл}) \in L$ и $(213 \text{ Дэвис-Холл}, \text{Джо Смит}) \in L^{-1}$. В общем, для любого студента s и комнаты в общежитии r у нас будет $(r, s) \in L^{-1}$ тогда и только тогда, когда $(s, r) \in L$. В качестве другого примера рассмотрим соответствие G из части 2 примера 4.2.2. Оно содержит все упорядоченные пары действительных чисел (x, y) , в которых x больше y . Мы могли бы назвать это соответствие «больше». Обратное ему:

$$\begin{aligned}G^{-1} &= ((x, y) \in \mathbb{R} \times \mathbb{R} \mid (y, x) \in G) \\ &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y > x\} \\ &= \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}.\end{aligned}$$

Другими словами, обратным соответствуя «больше» является соответствие «меньше»!

Самым сложным понятием, введенным в определении 4.2.3, является понятие композиции двух соответствий. В качестве примера этого понятия рассмотрим соответствие E и T из частей 5 и 6 примера 4.2.2. Напомним, что E – это соответствие из множества S всех студентов во множество C всех курсов, а T – соответствие из C во множество P всех преподавателей. Согласно определению 4.2.3 композиция $T \circ E$ – это соответствие из S в P , определяемое следующим образом:

$$\begin{aligned}T \circ E &= \{\{s, p\} \in S \times P \mid \exists c \in C(\{s, c\} \in E \text{ и } (c, p) \in T)\} \\ &= \{(s, p) \in S \times P \mid \exists c \in C (\text{студент } s \text{ зачислен на курс } c, \text{ и курс } c \text{ ведет профессор } p)\} \\ &= \{\{s, p\} \in S \times P \mid \text{студент } s \text{ зачислен на какой-либо курс, преподаваемый профессором } p\}.\end{aligned}$$

Таким образом, если Джо Смит изучает биологию и биологию преподает профессор Эванс, то $(\text{Джо Смит}, \text{биология}) \in E$ и $(\text{биология}, \text{профессор Эванс}) \in T$, и, следовательно, $(\text{Джо Смит}, \text{профессор Эванс}) \in T \circ E$. В общем случае если s – некоторый конкретный студент, а p – конкретный профессор, то $(s, p) \in T \circ E$ тогда и только тогда, когда существует некоторый курс с такой, что $(s, c) \in E$ и $(c, p) \in T$. Поначалу эта запись может показаться перевернутой.

той. Если $(s, c) \in E$ и $(c, p) \in T$, то у вас может возникнуть соблазн написать $(s, p) \in E \circ T$, но, согласно нашему определению, правильное обозначение – $(s, p) \in T \circ E$. Причина, по которой мы решили записывать композиции соответствий таким образом, станет ясна в главе 5. На данный момент вам просто нужно аккуратно обращаться с этой нотацией при работе с композициями соответствий.

Пример 4.2.4. Пусть S, R, C и P будут множествами студентов, комнат общежития, курсов и профессоров в вашем учебном заведении, как и раньше, и пусть L , E и T будут соответствиями, определенными в частях 4–6 примера 4.2.2. Опишите следующие соответствия.

1. E^{-1} .
2. $E \circ L^{-1}$.
3. $E^{-1} \circ E$.
4. $E \circ E^{-1}$.
5. $T \circ (E \circ L^{-1})$.
6. $(T \circ E) \circ L^{-1}$.

Решения

1. $E^{-1} = \{(c, s) \in C \times S \mid (s, c) \in E\} = \{(c, s) \in C \times S \mid \text{студент } s \text{ записан на курс } c\}$. Например, если Джо Смит записался на курс биологии, то $(Джо Смит, биология) \in E$ и $(биология, Джо Смит) \in E^{-1}$.
2. Поскольку L^{-1} – это соответствие из R в S , а E – соответствие из S в C , то $E \circ L^{-1}$ будет соответствием из R в C , определенным следующим образом:

$$\begin{aligned} E \circ L^{-1} &= \{(r, c) \in R \times C \mid \exists s \in S((r, s) \in L^{-1} \text{ и } (s, c) \in E)\} \\ &= \{(r, c) \in R \times C \mid \exists s \in S((s, r) \in L \text{ и } (s, c) \in E)\} \\ &= \{(r, c) \in R \times C \mid \exists s \in S(\text{студент } s \text{ живет в комнате } r \text{ и записан на курс } c)\} \\ &= \{(r, c) \in R \times C \mid \text{какой-то студент, который живет в комнате } r, \text{ записан на курс } c\}. \end{aligned}$$

Вернемся к нашему любимому ученику Джо Смиту, который изучает биологию и живет в комнате 213 общежития Дэвис-Холл. У нас есть пары $(213 \text{ Дэвис-Холл}, Джо Смит) \in L^{-1}$ и $(Джо Смит, биология) \in E$. Из определения композиции следует, что $(213 \text{ Дэвис Холл}, биология) \in E \circ L^{-1}$.

3. Поскольку E – это соответствие из S в C , а E^{-1} – это соответствие из C в S , то $E^{-1} \circ E$ – это соответствие из S в S , определяемое следующим образом:

$$\begin{aligned} E^{-1} \circ E &= \{(s, t) \in S \times S \mid \exists c \in C((s, c) \in E \text{ и } (c, t) \in E^{-1})\} \\ &= \{(s, t) \in S \times S \mid \exists c \in C(\text{студент } s \text{ записан на курс } c, \text{ как и студент } t)\} \\ &= \{(s, t) \in S \times S \mid \text{есть курс, на который одновременно обучаются студенты } s \text{ и } t\}. \end{aligned}$$

(Обратите внимание, что произвольный элемент $S \times S$ записывается (s, t) , а не (s, s) , потому что мы не предполагаем, что две координаты равны.)

4. Это не то же самое, что предыдущий пример! Поскольку E^{-1} – это отношение от C к S , а E – это отношение от S к C , то $E \circ E^{-1}$ – это отношение от C к C . Оно определяется следующим образом:

$$\begin{aligned}E \circ E^{-1} &= \{(c, d) \in C \times C \mid \exists s \in S((c, s) \in E^{-1} \text{ и } (s, d) \in E)\} \\&= \{(c, d) \in C \times C \mid \exists s \in S(\text{студент } s \text{ записан на курс } c, \text{ а также} \\&\quad \text{записан на курс } d)\} \\&= \{(c, d) \in C \times C \mid \text{есть студент, который записан на оба курса } c \text{ и } d\}.\end{aligned}$$

5. В п. 2 мы видели, что $E \circ L^{-1}$ – это соответствие из R в C , а T – это соответствие из C в P , поэтому $T \circ (E \circ L^{-1})$ – это соответствие из R в P , определенное следующим образом:

$$\begin{aligned}T \circ (E \circ L^{-1}) &= \{(r, p) \in R \times P \mid \exists c \in C((r, c) \in E \circ L^{-1} \text{ и } (c, p) \in T)\} \\&= \{(r, p) \in R \times P \mid \exists c \in C(\text{студент, проживающий в комнате } r \\&\quad \text{и записанный на курс } c \text{ профессора } p)\} \\&= \{(r, p) \in R \times P \mid \text{есть студент, проживающий в комнате } r \\&\quad \text{и записанный на курс } c \text{ профессора } p\}.\end{aligned}$$

6. $(T \circ E) \circ L^{-1} = \{(r, p) \in R \times P \mid \exists s \in S((r, s) \in L^{-1} \text{ и } (s, p) \in T \circ E)\}$
 $= \{(r, p) \in R \times P \mid \exists s \in S (\text{студент, живущий в комнате } r \\&\quad \text{и записанный на какой-то курс профессора } p)\} \\= \{(r, p) \in R \times P \mid \text{какой-то студент, живущий в комнате } r \\&\quad \text{и записанный на какой-то курс профессора } p\}.$

Обратите внимание, что наши ответы на части 3 и 4 примера 4.2.4 были разными, поэтому композиция отношений не коммутативна. Однако наши ответы на части 5 и 6 оказались одинаковыми. Это случайное совпадение или композиция соответствий в целом ассоциативна? Часто, глядя на примеры нового понятия, можно предложить общие правила, которые могли бы к нему применяться. Хотя одного контрпримера достаточно, чтобы опровергнуть правило, мы никогда не должны принимать правило на веру без доказательства в случае, если не знаем контрпример. Следующая теорема суммирует некоторые из основных свойств введенных нами новых понятий.

Теорема 4.2.5. Предположим, что R – это соответствие из A в B , S – это соответствие из B в C , а T – это соответствие из C в D . Тогда:

1. $(R^{-1})^{-1} = R$.
2. $\text{Dom}(R^{-1}) = \text{Ran}(R)$.
3. $\text{Ran}(R^{-1}) = \text{Dom}(R)$.
4. $T \circ (S \circ R) = (T \circ S) \circ R$.
5. $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Доказательство. Мы докажем п. 1, 2 и половину из п. 4, а остальные оставим как упражнения (см. упражнение 7).

1. Прежде всего обратите внимание, что R^{-1} – это соответствие из B в A , поэтому $(R^{-1})^{-1}$ – это соответствие из A в B , как и R . Чтобы убедиться, что $(R^{-1})^{-1} = R$, пусть (a, b) – произвольная упорядоченная пара из $A \times B$.

Тогда

$(a, b) \in (R^{-1})^{-1}$ тогда и только тогда, когда $(b, a) \in R^{-1}$ тогда и только тогда, когда $(a, b) \in R$.

2. Сначала отметим, что $\text{Dom}(R^{-1})$ и $\text{Ran}(R)$ являются подмножествами B . Пусть теперь b – произвольный элемент B . Тогда

$b \in \text{Dom}(R^{-1})$ тогда и только тогда, когда $\exists a \in A ((b, a) \in R^{-1})$
тогда и только тогда, когда $\exists a \in A ((a, b) \in R)$
тогда и только тогда, когда $b \in \text{Ran}(R)$.

4. Ясно, что $T \circ (S \circ R)$ и $(T \circ S) \circ R$ являются соответствиями из A в D . Пусть (a, d) – произвольный элемент из $A \times D$.

Сначала предположим, что $(a, d) \in T \circ (S \circ R)$. По определению композиции это означает, что мы можем выбрать некоторый элемент $c \in C$ такой, что $(a, c) \in S \circ R$ и $(c, d) \in T$. Поскольку $(a, c) \in S \circ R$, мы снова можем использовать определение композиции и выберем некоторые $b \in B$ такие, что $(a, b) \in R$ и $(b, c) \in S$. Теперь, поскольку $(b, c) \in S$ и $(c, d) \in T$, мы можем заключить, что $(b, d) \in T \circ S$. Аналогично, поскольку $(a, b) \in R$ и $(b, d) \in T \circ S$, следует, что $(a, d) \in (T \circ S) \circ R$.

Теперь предположим, что $(a, d) \in (T \circ S) \circ R$. Аналогичное рассуждение, формулировку которого мы оставляем читателю, показывает, что $(a, d) \in T \circ (S \circ R)$. Таким образом, $T \circ (S \circ R) = (T \circ S) \circ R$.

Комментарий. Утверждение 1 означает $\forall p (p \in (R^{-1})^{-1} \leftrightarrow p \in R)$, поэтому мы должны ввести в доказательство произвольный элемент p , а затем доказательства $p \in (R^{-1})^{-1} \leftrightarrow p \in R$. Но поскольку R и $(R^{-1})^{-1}$ оба представляют собой соответствия из A в B , мы можем трактовать универсум, который пробегает p , как $A \times B$, поэтому p должна быть упорядоченной парой. Поэтому в предыдущем доказательстве мы с самого начала использовали упорядоченную пару (a, b) . Доказательство биусловного утверждения $(a, b) \in (R^{-1})^{-1} \leftrightarrow (a, b) \in R$ использует метод, представленный в примере 3.4.5, для объединения последовательности эквивалентностей.

Доказательства утверждений 2 и 4 аналогичны, за исключением того, что биусловное доказательство утверждения 4 не может быть легко выполнено путем объединения эквивалентностей, поэтому мы доказываем оба направления по отдельности. Было доказано только одно направление. Ключом к этому доказательству является понимание того, что посылка $(a, d) \in T \circ (S \circ R)$ является экизистенциальным утверждением, поскольку она означает $\exists c \in C ((a, c) \in S \circ R \text{ и } (c, d) \in T)$, поэтому мы должны ввести в доказательство новую переменную c , обозначающую некоторый элемент из C , такой что $(a, c) \in S \circ R$ и $(c, d) \in T$. Аналогично, $(a, c) \in S \circ R$ тоже является экизистенциальным утверждением, поэтому следует ввести переменную b . После введения этих новых переменных мы легко приходим к цели $(a, d) \in (T \circ S) \circ R$.

Утверждение 5 теоремы 4.2.5, возможно, заслуживает отдельного комментария. Прежде всего обратите внимание, что правая часть уравнения – это $R^{-1} \circ S^{-1}$, а не $S^{-1} \circ R^{-1}$; порядок отношений был обращен. Вам будет предло-

жено доказать утверждение 5 в упражнении 7, но, возможно, сначала стоит попробовать пример. Мы уже видели, что для отношений E и T из п. 5 и 6 примера 4.2.2

$$T \circ E = \{(s, p) \in S \times P \mid \text{студент } s \text{ зачислен на какой-то курс профессора } p\}$$

следует, что

$$(T \circ E)^{-1} = \{(p, s) \in P \times S \mid \text{студент } s \text{ зачислен на какой-либо курс профессора } p\}.$$

Чтобы вычислить $E^{-1} \circ T^{-1}$, сначала заметим, что T^{-1} – это соответствие из P в C , а E^{-1} – это соответствие из C в S , поэтому $E^{-1} \circ T^{-1}$ – это соответствие из P в S . Теперь, применяя определение композиции, получаем:

$$\begin{aligned} E^{-1} \circ T^{-1} &= \{(p, s) \in P \times S \mid \exists c \in C((p, c) \in T^{-1} \text{ и } (c, s) \in E^{-1})\} \\ &= \{(p, s) \in P \times S \mid \exists c \in C((c, p) \in T \text{ и } (s, c) \in E)\} \\ &= \{(p, s) \in P \times S \mid \exists c \in C(\text{курс } c \text{ профессора } p, \text{ и студент } s \text{ записан на курс } c)\} \\ &= \{(p, s) \in P \times S \mid \text{студент } s \text{ зачислен на какой-либо курс профессора } p\}. \end{aligned}$$

Таким образом, $(T \circ E)^{-1} = E^{-1} \circ T^{-1}$.

Упражнения

- *1. Найдите области определения и множества значений следующих соответствий.
 - (a) $\{(p, q) \in P \times P \mid \text{человек } p \text{ является родителем человека } q\}$, где P – множество всех живущих людей.
 - (b) $\{(x, y) \in \mathbb{R}^2 \mid y > x^2\}$.
2. Найдите области определения и множества значений следующих соответствий.
 - (a) $\{(p, q) \in P \times P \mid \text{человек } p \text{ – брат человека } q\}$, где P – множество всех живущих людей.
 - (b) $\{(x, y) \in \mathbb{R}^2 \mid y^2 = 1 - 2/(x^2 + 1)\}$.
3. Пусть L и E – соответствия, определенные в п. 4 и 5 примера 4.2.2. Опишите следующие отношения:
 - (a) $L^{-1} \circ L$.
 - (b) $E \circ (L^{-1} \circ L)$.
4. Пусть E и T – соответствия, определенные в п. 5 и 6 примера 4.2.2. Так же, как в этом примере, пусть C будет множеством всех курсов в вашем учебном заведении, и пусть $D = \{\text{понедельник, вторник, среда, четверг, пятница}\}$. Пусть $M = \{(c, d) \in C \times D \mid \text{курс } c \text{ встречается в день } d\}$. Опишите следующие соответствия:
 - (a) $M \circ E$.
 - (b) $M \circ T^{-1}$.

- *5. Предположим, что $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$, $R = \{(1, 4), (1, 5), (2, 5), (3, 6)\}$ и $S = \{(4, 5), (4, 6), (5, 4), (6, 6)\}$. Обратите внимание, что R – это соответствие из A в B , а S – это соответствие из B в B . Найдите следующие отношения:
- $S \circ R$.
 - $S \circ S^{-1}$.
6. Предположим, что $A = \{1, 2, 3\}$, $B = \{4, 5\}$, $C = \{6, 7, 8\}$, $R = \{(1, 7), (3, 6), (3, 7)\}$ и $S = \{(4, 7), (4, 8), (5, 6)\}$. Обратите внимание, что R – это соответствие из A в C , а S – это соответствие из B в C . Найдите следующие соответствия:
- $S^{-1} \circ R$.
 - $R^{-1} \circ S$.
7. (a) Докажите часть 3 теоремы 4.2.5, повторяя доказательство п. 2 в тексте.
- (b) Приведите альтернативное доказательство части 3 теоремы 4.2.5, показав, что оно следует из утверждений 1 и 2.
- (c) Завершите доказательство части 4 теоремы 4.2.5.
- (d) Докажите часть 5 теоремы 4.2.5.
8. Пусть $E = \{(p, q) \in P \times P \mid \text{человек } p \text{ является врагом человека } q\}$ и $F = \{(p, q) \in P \times P \mid \text{человек } p - \text{ друг человека } q\}$, где P – множество всех людей. Как можно представить выражение «враг моего врага – мой друг» соответствиями между E и F ?
9. Предположим, что R – это соответствие из A в B , а S – это соответствие из B в C .
- Докажите, что $\text{Dom}(S \circ R) \subseteq \text{Dom}(R)$.
 - Докажите, что если $\text{Ran}(R) \subseteq \text{Dom}(S)$, то $\text{Dom}(S \circ R) = \text{Dom}(R)$.
 - Сформулируйте и докажите аналогичные теоремы о $\text{Ran}(S \circ R)$.
10. Предположим, что R и S – соответствия из A в B . Истинны ли следующие утверждения? Обоснуйте свои ответы доказательствами или контрпри мерами.
- $R \subseteq \text{Dom}(R) \times \text{Ran}(R)$.
 - Если $R \subseteq S$, то $R^{-1} \subseteq S^{-1}$.
 - $(R \cup S)^{-1} = R^{-1} \cup S^{-1}$
- *11. Предположим, что R – соответствие из A в B , а S – это соответствие из B в C . Докажите, что $S \circ R = \emptyset$ тогда и только тогда, когда $\text{Ran}(R)$ и $\text{Dom}(S)$ не пересекаются.
- P_D12. Пусть R – соответствие из A в B , а S и T – соответствия из B в C .
- Докажите, что $(S \circ R) \setminus (T \circ R) \subseteq (S \setminus T) \circ R$.
 - Где ошибка в следующем доказательстве того, что $(S \setminus T) \circ R \subseteq (S \circ R) \setminus (T \circ R)$?
- Доказательство.* Предположим, что $(a, c) \in (S \setminus T) \circ R$. Тогда мы можем выбрать некоторый $b \in B$ такой, что $(a, b) \in R$ и $(b, c) \in S \setminus T$, так что $(b, c) \in S$ и $(b, c) \notin T$. Поскольку $(a, b) \in R$ и $(b, c) \in S$, то $(a, c) \in S \circ R$. Точно так же, поскольку $(a, b) \in R$ и $(b, c) \notin T$, то $(a, c) \notin T \circ R$. Поэтому $(a, c) \in (S \circ R) \setminus (T \circ R)$. Поскольку (a, c) произвольно, это значит, что $(S \setminus T) \circ R \subseteq (S \circ R) \setminus (T \circ R)$.

- (c) Верно ли, что $(S \setminus T) \circ R \subseteq (S \circ R) \setminus (T \circ R)$? Обоснуйте свой ответ либо доказательством, либо контрпримером.
13. Пусть R и S – соответствия из A в B , а T – соответствие из B в C . Истины ли следующие утверждения? Обоснуйте свои ответы доказательствами или контрпримерами.
- Если R и S не пересекаются, то R^{-1} и S^{-1} тоже не пересекаются.
 - Если R и S не пересекаются, то $T \circ R$ и $T \circ S$ тоже не пересекаются.
 - Если $T \circ R$ и $T \circ S$ не пересекаются, то R и S тоже не пересекаются.
- P_D14. Пусть R – соответствие из A в B , а S и T – соответствия из B в C . Истины ли следующие утверждения? Обоснуйте свои ответы доказательствами или контрпримерами.
- Если $S \subseteq T$, то $S \circ R \subseteq T \circ R$.
 - $(S \cap T) \circ R \subseteq (S \circ R) \cap (T \circ R)$.
 - $(S \cap T) \circ R = (S \circ R) \cap (T \circ R)$.
 - $(S \cup T) \circ R = (S \circ R) \cup (T \circ R)$.
15. Пусть R – соответствие из A в B , а S – это соответствие из C в D . Покажите, что существует множество E , такое что R – соответствие из A в E , а S – соответствие из E в D , и поэтому применима формулировка $S \circ R$ из определения 4.2.3. Более того, это определение дает один и тот же результат независимо от того, какое именно множество E используется.

4.3. ПОДРОБНЕЕ О СООТВЕТСТВИЯХ

Хотя мы определили соответствия как множества упорядоченных пар, иногда бывает полезно взглянуть на них по-другому. Часто даже небольшое изменение обозначений может помочь нам взглянуть на вещи иначе. Одно из альтернативных обозначений, которое математики иногда используют для соответствий, объясняется тем фактом, что в математике мы часто выражаем отношения между двумя объектами x и y , помещая между ними некоторый символ. Например, обозначения $x = y$, $x < y$, $x \in y$ и $x \subseteq y$ выражают четыре важных математических отношения между x и y . Подражая этим обозначениям, если R является соответствием из A в B , где $x \in A$ и $y \in B$, математики иногда пишут xRy для обозначения $(x, y) \in R$.

Например, если L – соответствие, определенное в п. 4 примера 4.2.2, то для любого студента s и комнаты общежития r запись sLr означает $(s, r) \in L$, или, другими словами, студент s живет в комнате общежития r . Аналогично, если E и T – соответствия, определенные в п. 5 и 6 примера 4.2.2, то запись sEc означает, что студент s записался на курс c , а cTr означает, что курс c преподает профессор r . Определение композиции соответствий можно было бы сформулировать, сказав, что если R – это соответствие из A в B , а S – это соответствие из B в C , то $S \circ R = \{(a, c) \in A \times C \mid \exists b \in B (aRb \text{ и } bSc)\}$.

Еще один способ представить соответствия – нарисовать их. На рис. 4.1 показано соответствие $R = \{(1, 3), (1, 5), (3, 3)\}$ из п. 1 примера 4.2.2. Напомним, что это было соответствие из множества $A = \{1, 2, 3\}$ в множество $B = \{3, 4, 5\}$.

На рисунке каждое из этих множеств представлено овалом, а элементы множества представлены точками внутри овала. Каждая упорядоченная пара $(a, b) \in R$ представлена стрелкой от точки, представляющей a , до точки, представляющей b . Например, есть стрелка от точки внутри A с меткой 1 до точки внутри B с меткой 5, потому что упорядоченная пара $(1, 5)$ является элементом R .

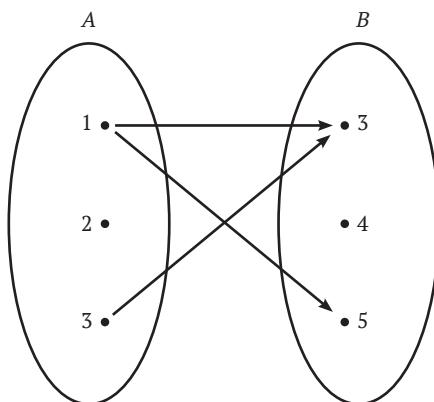


Рис. 4.1 ♦ Графическое представление соответствия

В общем, таким изображением может быть представлено любое соответствие R из множества A в множество B . Точки, представляющие элементы A и B на рисунке, называются *вершинами*, а стрелки, представляющие упорядоченные пары в R , называются *ребрами*. Не важно, как именно вершины, представляющие элементы A и B , расположены на странице; важно, чтобы ребра точно соответствовали упорядоченным парам в R . Рисование этих изображений поможет вам понять идеи, обсуждаемые в последнем разделе. Например, вы должны быть уверены, что можете найти область определения R , обнаружив те вершины в A , для которых есть ребра, исходящие от них. Точно так же множество значений R будет состоять из тех элементов B , вершины которых имеют ребра, входящие к ним. Для соответствия R , показанного на рис. 4.1, имеем $\text{Dom}(R) = \{1, 3\}$ и $\text{Ran}(R) = \{3, 5\}$. Изображение R^{-1} выглядело бы так же, как изображение R , но с обратным направлением всех стрелок.

Рисунки, иллюстрирующие состав двух соответствий, понять немного сложнее. Например, снова рассмотрим соответствия E и T из п. 5 и 6 примера 4.2.2. На рис. 4.2 показано, как может выглядеть часть обоих соответствий. (Полная схема может быть довольно большой, если в вашем учебном заведении много студентов, курсов и профессоров.) На этом рисунке мы можем видеть, что, например, Джо Смит изучает биологию и математику, что биологию преподает профессор Эванс и что математику преподает профессор Эндрюс. Отсюда, применяя определение композиции, мы видим, что пары (Джо Смит, проф. Эванс) и (Джо Смит, проф. Эндрюс) являются элементами соответствия $T \circ E$.

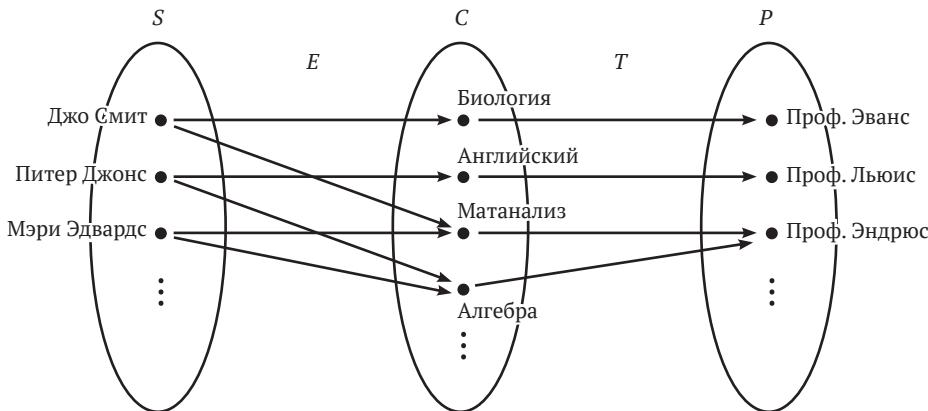


Рис. 4.2 ♦ Пример графического представления двух соответствий

Чтобы лучше разглядеть, как композиция $T \circ E$ представлена на этом рисунке, сначала обратите внимание, что для любого студента s , курса c и профессора p есть стрелка от s до c , если и только если sEc , и стрелка от c до p , если и только если cTp . Таким образом, согласно определению композиции:

$$\begin{aligned} T \circ E &= \{(s, p) \in S \times P \mid \exists c \in C (sEc \text{ и } cTp)\} \\ &= \{(s, p) \in S \times P \mid \exists c \in C \text{ (на рис. 4.2 есть стрелка от } s \text{ до } c \text{ и стрелка от } c \text{ до } p)\} \\ &= \{(s, p) \in S \times P \mid \text{на рис. 4.2 вы можете перейти от } s \text{ к } p \text{ в два этапа, следуя стрелкам}\}. \end{aligned}$$

Например, начиная с вершины, обозначающей Мэри Эдвардс, мы можем добраться до профессора Эндрюса за два шага (пройдя через матанализ или алгебру), поэтому мы можем заключить, что $(\text{Мэри Эдвардс}, \text{проф. Эндрюс}) \in T \circ E$.

В некоторых ситуациях мы рисуем соответствия несколько иначе. Например, если A – множество и $R \subseteq A \times A$, то согласно определению 4.2.1 R будет являться соответствием из A в A . Такое отношение также иногда называют *отношением на A* (или *бинарным отношением на A*). Соответствия этого типа часто встречаются в математике; фактически мы уже видели некоторые из них. Например, мы описали отношение на G в п. 2 примера 4.2.2 как соответствие из \mathbb{R} в \mathbb{R} , но в нашей новой терминологии мы могли бы назвать его просто отношением (или бинарным отношением) на \mathbb{R} . Соответствие $E^{-1} \circ E$ из примера 4.2.4 было отношением к S , а $E \circ E^{-1}$ было отношением к C .

Пример 4.3.1. Вот еще несколько примеров отношений множеств.

- Пусть $A = \{1, 2\}$ и $B = \mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$, как в п. 3 примера 4.2.2. Пусть

$$\begin{aligned} S &= \{(x, y) \in B \times B \mid x \subseteq y\} \\ &= \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{1\}), (\{1\}, \{1, 2\}), (\{2\}, \{2\}), (\{2\}, \{1, 2\}), (\{1, 2\}, \{1, 2\})\}. \end{aligned}$$

Тогда S – отношение на B .

2. Пусть A – множество. Пусть $i_A = \{(x, y) \in A \times A \mid x = y\}$. Тогда i_A является отношением на A . (Оно называется *отношением тождества на A*.) Например, если $A = \{1, 2, 3\}$, то $i_A = \{(1, 1), (2, 2), (3, 3)\}$. Обратите внимание, что i_A можно также определить, написав $i_A = \{(x, x) \mid x \in A\}$.
3. Для каждого положительного действительного числа r пусть $D_r = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |x - y| < r\}$. Тогда D_r – отношение на \mathbb{R} .

Пусть R является отношением на A . Если бы мы использовали метод, описанный ранее, чтобы графически представить R , то нам пришлось бы нарисовать две копии множества A , а затем нарисовать ребра от одной копии A к другой, чтобы представить упорядоченные пары в R . Более простой способ изобразить схему – нарисовать только одну копию A , а затем соединить вершины, представляющие элементы A , ребрами, чтобы представить упорядоченные пары в R . Например, на рис. 4.3 показано изображение отношения S из п. 1 примера 4.3.1. Схемы, подобные изображенной на рис. 4.3, называются *ориентированными графиками*.

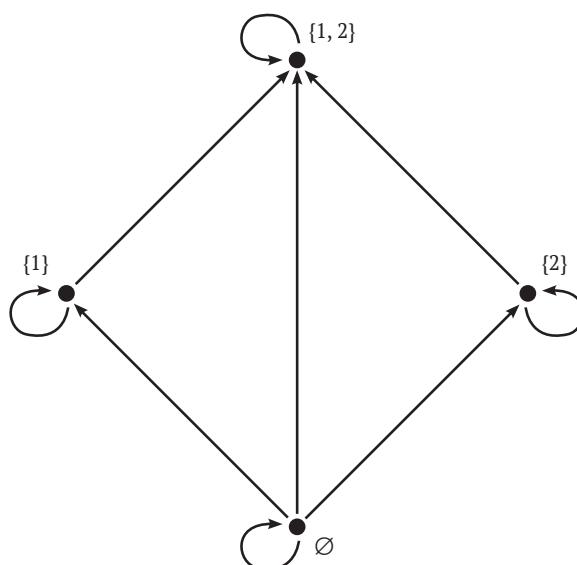


Рис. 4.3 ♦ Пример ориентированного графа

Обратите внимание, что в этом ориентированном графе есть ребро от \emptyset до самого себя, потому что $(\emptyset, \emptyset) \in S$. Ребра, подобные этому, которые направлены от вершины к ней же, называются *петлями*. Фактически на рис. 4.3 есть петля в каждой вершине, потому что S обладает свойством $\forall x \in B((x, x) \in S)$. Мы описываем эту ситуацию, говоря, что S является *рефлексивным*.

Определение 4.3.2. Предположим, что R – отношение на A .

1. R называется *рефлексивным* к A (или просто *рефлексивным*, если A ясно из контекста), если $\forall x \in A(xRx)$, или, другими словами, $\forall x \in A((x, x) \in R)$.

2. R симметрично, если $\forall x \in A \forall y \in A (xRy \rightarrow yRx)$.
3. R транзитивно, если $\forall x \in A \forall y \in A \forall z \in A ((xRy \wedge yRz) \rightarrow xRz)$.

Как мы видели в примере 4.3.1, если R рефлексивно к A , то ориентированный граф, представляющий R , будет иметь петли во всех вершинах. Если R симметрично, то всякий раз, когда есть ребро от x до y , также будет ребро от y до x . Если x и y различны, то будет два ребра, соединяющих x и y , по одному в каждом направлении. Таким образом, если R симметрично, то все ребра, кроме петель, попадут в такие пары. Если R транзитивно, то всякий раз, когда есть ребро от x до y и от y до z , существует также ребро от x до z .

Пример 4.3.3. Является ли соответствие G из п. 2 примера 4.2.2 рефлексивным? Симметричным? Транзитивным? Являются ли соответствия в примере 4.3.1 рефлексивными, симметричными или транзитивными?

Решение

Напомним, что соответствие G из примера 4.2.2 является отношением на \mathbb{R} и что для любых действительных чисел x и y запись xGy означает $x > y$. Таким образом, сказать, что G рефлексивно, означало бы, что $\forall x \in \mathbb{R} (xGx)$, или, другими словами, $\forall x \in \mathbb{R} (x > x)$, и это явно неверно. Сказать, что G симметрично, означало бы, что $\forall x \in \mathbb{R} \forall y \in \mathbb{R} (x > y \rightarrow y > x)$, и это также явно неверно. Наконец, сказать, что G транзитивно, означало бы, что $\forall x \in \mathbb{R} \forall y \in \mathbb{R} \forall z \in \mathbb{R} ((x > y \wedge y > z) \rightarrow x > z)$, и это истинно. Следовательно, G транзитивно, но не рефлексивно или симметрично.

Анализ отношений в примере 4.3.1 аналогичен. Для отношения S в части 1 мы используем тот факт, что для любых x и y в B , xSy означает $x \leq y$. Как мы уже заметили, S рефлексивно, поскольку $\forall x \in B (x \leq x)$, но неверно, что $\forall x \in B \forall y \in B (x \leq y \rightarrow y \leq x)$. Например, $\{1\} \subseteq \{1, 2\}$, но $\{1, 2\} \not\subseteq \{1\}$. Вы можете увидеть это, взглянув на рис. 4.3 и отметив, что есть ребро от $\{1\}$ до $\{1, 2\}$, но нет ребра от $\{1, 2\}$ до $\{1\}$. Таким образом, S не симметрично. S транзитивно, потому что утверждение $\forall x \in B \forall y \in B \forall z \in B ((x \leq y \wedge y \leq z) \rightarrow x \leq z)$ истинно.

Для любого множества A отношение тождества i_A будет рефлексивным, симметричным и транзитивным, поскольку все утверждения $\forall x \in A (x = x)$, $\forall x \in A \forall y \in A (x = y \rightarrow y = x)$ и $\forall x \in A \forall y \in A \forall z \in A ((x = y \wedge y = z) \rightarrow x = z)$ явно истинны. Наконец, пусть r – положительное действительное число, и рассмотрим отношение D_r . Для любого действительного числа x истинно утверждение $|x - x| = 0 < r$, поэтому $(x, x) \in D_r$. Следовательно, D_r рефлексивно. Кроме того, для любых действительных чисел x и y $|x - y| = |y - x|$, поэтому если $|x - y| < r$, тогда $|y - x| < r$. Следовательно, если $(x, y) \in D_r$, то $(y, x) \in D_r$, поэтому D_r симметрично. Но D_r не транзитивно. Чтобы понять, почему, пусть x будет любым действительным числом. Пусть $y = x + 2r/3$ и $z = y + 2r/3 = x + 4r/3$. Тогда $|x - y| = 2r/3 < r$ и $|y - z| = 2r/3 < r$, но $|x - z| = 4r/3 > r$. Следовательно, $(x, y) \in D_r$ и $(y, z) \in D_r$, но $(x, z) \notin D_r$.

Возможно, вы уже догадались, что свойства отношений, заявленные в определении 4.3.2, связаны с операциями, представленными в определении 4.2.3. Сказать, что отношение R является симметричным, означает поменять местами две переменные таким образом, который напоминает

определение R^{-1} . Определение транзитивности отношения включает объединение двух упорядоченных пар, как и определение композиции соответствий. Следующая теорема разъясняет эти связи более строго.

Теорема 4.3.4. Предположим, что R – отношение на A .

1. R рефлексивно тогда и только тогда, когда $i_A \subseteq R$, где, как и раньше, i_A – тождественное отношение на A .
2. R симметрично тогда и только тогда, когда $R = R^{-1}$.
3. R транзитивно тогда и только тогда, когда $R \circ R \subseteq R$.

Доказательство. Мы докажем п. 2 и оставим доказательства п. 1 и 3 в качестве упражнений (см. упражнения 7 и 8).

2. (\rightarrow) Предположим, что R симметрично. Пусть (x, y) – произвольный элемент R . Тогда xRy , и поскольку R симметрично, то yRx . Таким образом, $(y, x) \in R$, поэтому из определения R^{-1} следует $(x, y) \in R^{-1}$. Поскольку (x, y) произвольно, то $R \subseteq R^{-1}$.

Теперь предположим, что $(x, y) \in R^{-1}$. Тогда $(y, x) \in R$, и так как R симметрично, то $(x, y) \in R$. Таким образом, $R^{-1} \subseteq R$, поэтому $R = R^{-1}$.

(\leftarrow) Пусть $R = R^{-1}$, и пусть x и y – произвольные элементы A . Предположим, что xRy . Тогда $(x, y) \in R$, и поскольку $R = R^{-1}$, то $(x, y) \in R^{-1}$. По определению R^{-1} это означает $(y, x) \in R$, поэтому yRx . Таким образом, $\forall x \in A \forall y \in A (xRy \rightarrow yRx)$, поэтому R симметрично.

Комментарий. Это доказательство довольно простое. Утверждение, которое нужно доказать, является утверждением типа «тогда и только тогда», поэтому мы доказываем оба направления по отдельности. В половине \rightarrow мы должны доказать, что $R = R^{-1}$, и это делается путем доказательства как $R \subseteq R^{-1}$, так и $R^{-1} \subseteq R$. Каждая из этих целей доказывается, если взять произвольный элемент из первого множества и показать, что он присутствует во втором множестве. В половине \leftarrow мы должны доказать, что R симметрично, что означает $\forall x \in A \forall y \in A (xRy \rightarrow yRx)$. Мы используем очевидную стратегию, назначая x и y произвольными элементами из A , предполагая xRy и доказывая yRx .

Упражнения

- *1. Пусть $L = \{a, b, c, d, e\}$ и $W = \{\text{bad}, \text{bed}, \text{cab}\}$. Пусть $R = \{(l, w) \in L \times W \mid$ буква l встречается в слове $w\}$. Нарисуйте диаграмму R (как на рис. 4.1).
- 2. Пусть $A = \{\text{cat}, \text{dog}, \text{bird}, \text{rat}\}$, и пусть $R = \{(x, y) \in A \times A \mid$ в обоих словах x и y встречается хотя бы одна буква $\}$. Нарисуйте ориентированный граф (как на рис. 4.3) для отношения R . Является ли R рефлексивным? Симметричным? Транзитивным?
- *3. Пусть $A = \{1, 2, 3, 4\}$. Нарисуйте ориентированный граф для i_A , отношение тождества на A .
- 4. Перечислите упорядоченные пары в соответствиях, представленных ориентированными графиками на рис. 4.4. Определите, является ли каждое соответствие рефлексивным, симметричным или транзитивным.

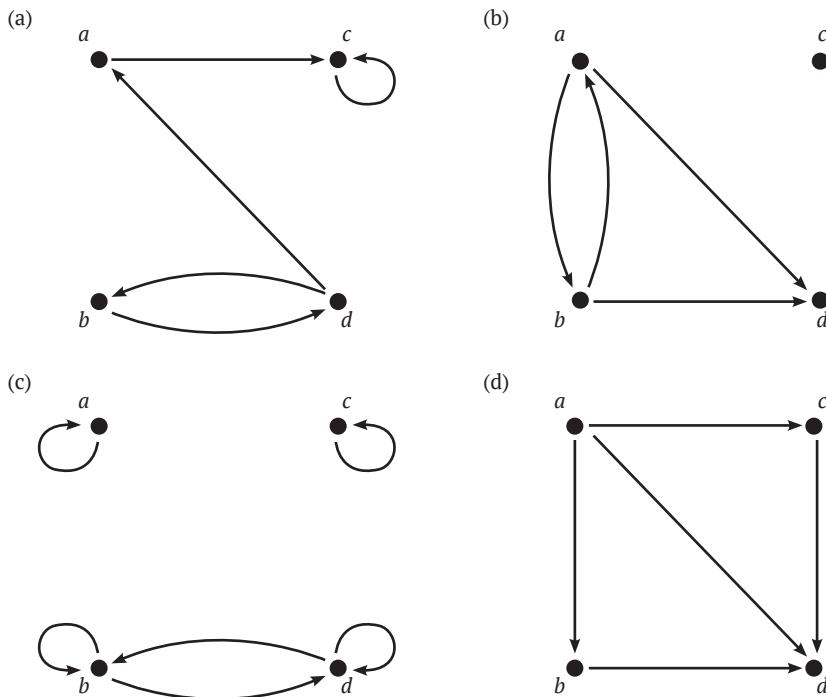


Рис. 4.4 ♦ Примеры соответствий, представленных ориентированными графами

*5. На рис. 4.5 показаны два соответствия R и S . Найдите $S \circ R$.

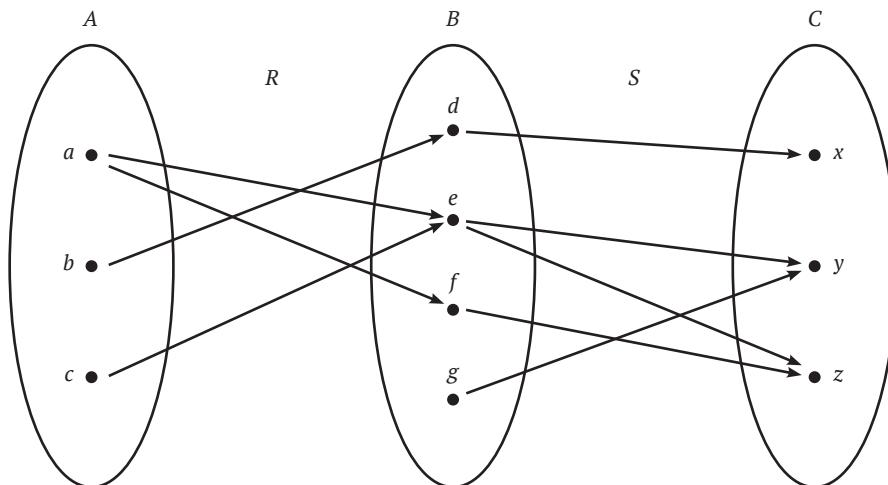


Рис. 4.5 ♦ Пример композиции соответствий R и S

6. Предположим, что r и s – два положительных действительных числа. Пусть D_r и D_s определены, как в п. 3 примера 4.3.1. Что такое $D_r \circ D_s$? Обоснуйте свой ответ доказательством. (Подсказка: в вашем доказательстве может пригодиться неравенство треугольника; см. упражнение 13(с) раздела 3.5.)
- *7. Докажите п. 1 теоремы 4.3.4.
8. Докажите п. 3 теоремы 4.3.4.
9. Пусть A и B – множества.
- Покажите, что для любого соответствия R из A в B справедливо $R \circ i_A = R$.
 - Покажите, что для любого соответствия R из A в B справедливо $i_B \circ R = R$.
- *10. Предположим, что S – отношение на A . Пусть $D = \text{Dom}(S)$ и $R = \text{Ran}(S)$. Докажите, что $i_D \subseteq S^{-1} \circ S$ и $i_R \subseteq S \circ S^{-1}$.
11. Предположим, что R – отношение на A . Докажите, что если R рефлексивно, то $R \subseteq R \circ R$.
12. Предположим, что R – отношение на A .
- Докажите, что если R рефлексивно, то R^{-1} тоже рефлексивно.
 - Докажите, что если R симметрично, то R^{-1} тоже симметрично.
 - Докажите, что если R транзитивно, то R^{-1} тоже транзитивно.
- *13. Пусть R_1 и R_2 – отношения на A . Для каждого пункта задания приведите доказательство или контрпример, чтобы обосновать свой ответ.
- Если R_1 и R_2 рефлексивны, должно ли $R_1 \cup R_2$ быть рефлексивным?
 - Если R_1 и R_2 симметричны, должно ли $R_1 \cup R_2$ быть симметричным?
 - Если R_1 и R_2 транзитивны, должно ли $R_1 \cup R_2$ быть транзитивным?
14. Пусть R_1 и R_2 – отношения на A . Для каждого пункта задания приведите доказательство или контрпример, чтобы обосновать свой ответ.
- Если R_1 и R_2 рефлексивны, должно ли $R_1 \cap R_2$ быть рефлексивным?
 - Если R_1 и R_2 симметричны, должно ли $R_1 \cap R_2$ быть симметричным?
 - Если R_1 и R_2 транзитивны, должно ли $R_1 \cap R_2$ быть транзитивным?
15. Пусть R_1 и R_2 – отношения на A . Для каждого пункта задания приведите доказательство или контрпример, чтобы обосновать свой ответ.
- Если R_1 и R_2 рефлексивны, должно ли $R_1 \setminus R_2$ быть рефлексивным?
 - Если R_1 и R_2 симметричны, должно ли $R_1 \setminus R_2$ быть симметричным?
 - Если R_1 и R_2 транзитивны, должно ли $R_1 \setminus R_2$ быть транзитивным?
16. Пусть R и S – рефлексивные отношения на A . Докажите, что $R \circ S$ рефлексивно.
- *17. Пусть R и S – симметричные отношения на A . Докажите, что $R \circ S$ симметрично тогда и только тогда, когда $R \circ S = S \circ R$.
18. Пусть R и S – транзитивные отношения на A . Докажите, что если $S \circ R \subseteq R \circ S$, то $R \circ S$ транзитивно.

19. Рассмотрим следующую предположительную теорему.

Предположительная теорема. Предположим, что R – отношение на A , и определим отношение S на $\mathcal{P}(A)$ следующим образом:

$$S = \{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid \exists X \in X \exists y \in Y (xRy)\}.$$

Если R транзитивно, то и S тоже транзитивно.

(а) Где ошибка в следующем доказательстве теоремы?

Доказательство. Предположим, что R транзитивно. Пусть $(X, Y) \in S$ и $(Y, Z) \in S$. Тогда по определению S , xRy и yRz , где $x \in X$, $y \in Y$ и $z \in Z$. Поскольку xRy , yRz и R транзитивны, xRz . Но тогда, поскольку $x \in X$ и $z \in Z$, из определения S следует, что $(X, Z) \in S$. Таким образом, S транзитивно.

(б) Верна ли теорема? Обоснуйте свой ответ либо доказательством, либо контрпримером.

*20. Пусть R – отношение на A . Пусть $B = \{X \in \mathcal{P}(A) \mid X \neq \emptyset\}$, и определим отношение S на B следующим образом:

$$S = \{(X, Y) \in B \times B \mid \forall x \in X \forall y \in Y (xRy)\}.$$

Докажите, что если R транзитивно, то транзитивно и S . Почему нужно было исключить пустое множество из множества B , чтобы это доказательство сработало?

21. Пусть R – отношение на A ; определим отношение S на $\mathcal{P}(A)$ следующим образом:

$$S = \{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid \forall x \in X \exists y \in Y (xRy)\}.$$

Для каждого пункта задания приведите доказательство или контрпример, чтобы обосновать свой ответ.

(а) Если R рефлексивно, должно ли S быть рефлексивным?

(б) Если R симметрично, должно ли S быть симметричным?

(в) Если R транзитивно, должно ли S быть транзитивным?

22. Рассмотрим следующую предположительную теорему.

Предположительная теорема. Пусть R – отношение на A . Если R симметрично и транзитивно, то R рефлексивно.

Правильно ли следующее доказательство? Если да, то какие стратегии доказательства оно использует? Если нет, можно ли это исправить? Верна ли теорема?

Доказательство. Пусть x – произвольный элемент из A . Пусть y – любой элемент из A , такой что xRy . Поскольку R симметрично, то yRx . Но тогда по определению транзитивности, поскольку xRy и yRx , мы можем заключить, что xRx . Поскольку x произвольно, мы показали, что $\forall x \in A (xRx)$, поэтому R рефлексивно.

*23. Эту задачу предложил профессор Уильям Цвикер из Юнион-колледжа, штат Нью-Йорк. Предположим, что A – множество и $\mathcal{F} \subseteq \mathcal{P}(A)$. Пусть =

$\{(a, b) \in A \times A \mid \text{для любого } X \subseteq A \setminus \{a, b\}, \text{ если } X \cup \{a\} \in \mathcal{F}, \text{ тогда } X \cup \{b\} \in \mathcal{F}\}$. Покажите, что R транзитивно.

24. Пусть $R = \{(m, n) \in \mathbb{N} \times \mathbb{N} \mid |m - n| \leq 1\}$, которое является отношением на \mathbb{N} . Обратите внимание, что $R \subseteq \mathbb{Z} \times \mathbb{Z}$, поэтому R также является отношением на \mathbb{Z} . Это упражнение проиллюстрирует, почему в п. 1 определения 4.3.2 мы использовали фразу « R рефлексивно на A », а не просто « R рефлексивно».
- (a) Рефлексивно ли R на \mathbb{N} ?
 - (b) Рефлексивно ли R на \mathbb{Z} ?

4.4. Отношения порядка

Рассмотрим соотношение $L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$. Вы должны сами убедиться, что оно рефлексивно и транзитивно, но не симметрично. Оно не может быть симметричным хотя бы потому, что существует много пар (x, y) , таких что xLy истинно, а yLx ложно. Фактически единственная ситуация, при которой xLy и yLx могут быть истинными одновременно, – если $x \leq y$ и $y \leq x$, то есть $x = y$. Поэтому мы говорим, что L *антисимметрично* (или *кососимметрично*). Вот общее определение.

Определение 4.4.1. Предположим, что R – отношение на множестве A . Тогда R называется *антисимметричным*, если $\forall x \in A \forall y \in A ((xRy \wedge yRx) \rightarrow x = y)$.

Мы уже видели отношение, у которого многие свойства совпадают с L . Взгляните еще раз на отношение S , определенное в п. 1 примера 4.3.1. Напомним, что в этом примере мы приняли $A = \{1, 2\}$, $B = \mathcal{P}(A)$ и $S = \{(x, y) \in B \times B \mid x \subseteq y\}$. Таким образом, если x и y являются элементами B , то xSy означает $x \subseteq y$. В предыдущем разделе мы убедились, что S рефлексивно и транзитивно, но не симметрично. Фактически S также антисимметрично, потому что для любых множеств x и y если $x \subseteq y$ и $y \subseteq x$, то $x = y$. Возможно, вам будет полезно вернуться к рис. 4.3 в предыдущем разделе, на котором показан ориентированный граф, представляющий S .

Интуитивно понятно, что L и S – отношения, которые как-то связаны с со-поставлением размеров двух объектов. Каждое из утверждений $x \leq y$ и $x \subseteq y$ можно рассматривать как утверждение, что в некотором смысле множество y «по крайней мере такого же размера» как x . Вы можете также справедливо заметить, что каждое из этих утверждений указывает, в каком порядке идут x и y . Отсюда вытекает следующее определение.

Определение 4.4.2. Предположим, что R является отношением на множестве A . Тогда R называется *частичным порядком*¹ на A (или просто *частичным порядком*, если A ясно из контекста), если оно рефлексивно, транзитивно и антисимметрично. Оно называется *полным порядком*² на A (или просто *полным*

¹ Так же говорят «*отношение, частично упорядоченное на A* ». – Прим. перев.

² Так же говорят «*отношение, полностью упорядоченное на A* ». – Прим. перев.

порядком), если представляет собой частичный порядок, и, кроме того, имеет следующее свойство:

$$\forall x \in A \ \forall y \in A (xRy \vee yRx).$$

Только что рассмотренные отношения L и S являются частичными порядками. S не является полным порядком, потому что утверждение $\forall x \in B \forall y \in B (x \leq y \vee y \leq x)$ не истинно. Например, если мы примем $x = \{1\}$ и $y = \{2\}$, тогда $x \not\leq y$ и $y \not\leq x$. Таким образом, хотя мы можем рассматривать отношение S как указание на то, в каком смысле один элемент B может быть не меньше другого, оно не дает нам способа сравнения каждой пары элементов B . Для некоторых пар, таких как $\{1\}$ и $\{2\}$, S не говорит ни про одну из них, что она как минимум такого же размера, как другая. В этом смысле порядок *частичный*. С другой стороны, L – это полный порядок, потому что если x и y – любые два действительных числа, то либо $x \leq y$, либо $y \leq x$. Таким образом, L дает нам способ сравнения любых двух действительных чисел.

Пример 4.4.3. Какие из следующих отношений являются частично упорядоченными, а какие – полностью?

1. Пусть A – произвольное множество, и пусть $B = \mathcal{P}(A)$ и $S = \{(x, y) \in B \times B \mid x \subseteq y\}$.
2. Пусть $A = \{1, 2\}$ и $B = \mathcal{P}(A)$, как и раньше. Примем

$$R = \{(x, y) \in B \times B \mid y \text{ содержит по крайней мере столько же элементов, сколько } x\} = \{(\emptyset, \emptyset), (\emptyset, \{1\}), (\emptyset, \{2\}), (\emptyset, \{1, 2\}), (\{1\}, \{1\}), (\{1\}, \{2\}), (\{1\}, \{1, 2\}), (\{2\}, \{1\}), (\{2\}, \{2\}), (\{2\}, \{1, 2\}), (\{1, 2\}, \{1, 2\})\}.$$

3. $D = \{(x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \mid x \text{ делит } y\}$.
4. $G = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \geq y\}$.

Решения

1. Это просто обобщение одного из рассмотренных ранее примеров, и легко убедиться, что это частичный порядок. Пока A имеет хотя бы два элемента, это отношение не будет полностью упорядоченным. Чтобы понять, почему, просто отметьте, что если a и b – разные элементы A , то $\{a\}$ и $\{b\}$ – элементы B , для которых $\{a\} \not\subseteq \{b\}$ и $\{b\} \not\subseteq \{a\}$.
2. Обратите внимание, что $(\{1\}, \{2\}) \in R$ и $(\{2\}, \{1\}) \in R$, но, конечно, $\{1\} \neq \{2\}$. Таким образом, R не антисимметрично, поэтому это не частичный порядок. Хотя R был определен путем выбора пар (x, y) , в которых y в определенном смысле не меньше x , он не удовлетворяет определению частичного порядка. Этот пример показывает, что наше описание частичных порядков как отношений, которые указывают на то, что один объект по крайней мере такой же величины, как другой, не следует воспринимать слишком серьезно. Это было предпосылкой для определения частичного порядка, но это не само определение.
3. Ясно, что каждое натуральное число делится само на себя, поэтому D рефлексивно. Кроме того, как мы показали в теореме 3.3.7, если $x \mid y$ и $y \mid z$, то $x \mid z$. Таким образом, если $(x, y) \in D$ и $(y, z) \in D$, то $(x, z) \in D$, по-

этому D транзитивно. Наконец, предположим, что $(x, y) \in D$ и $(y, x) \in D$. Тогда $x \mid y$ и $y \mid x$, и поскольку x и y положительны, следует, что $x \leq y$ и $y \leq x$, поэтому $x = y$. Таким образом, D антисимметрично, значит, это частичный порядок. Легко найти примеры, показывающие, что D не является полным порядком. Например, $(3, 5) \notin D$ и $(5, 3) \notin D$.

Возможно, вы были удивлены, обнаружив, что D – это частичный порядок. Похоже, здесь не сравниваются размеры, как в случае с другими частичными порядками, которые мы видели. Но мы показали, что этот случай разделяет с другими отношениями важные свойства рефлексивности, транзитивности и антисимметрии. Фактически это одна из причин для формулирования таких определений, как 4.4.2. Они помогают нам увидеть сходство между вещами, которые на первый взгляд могут показаться совсем не похожими.

4. Вы должны сами убедиться, что G – это полный порядок. Обратите внимание, что в этом случае более разумно будет трактовать запись xGy как обозначение, что y не превышает x , а не так, что y меньше x . Определение частичного порядка, хотя и основано на размышлениях о порядках, направленных в одну сторону, на самом деле применимо к порядкам в любом направлении. Фактически этот пример может привести вас к предположению, что если R является частичным порядком на A , то и R^{-1} является таким же порядком. Мы попросим вас доказать эту гипотезу в упражнении 13.

До сих пор в качестве имен для наших отношений мы всегда использовали буквы, но иногда математики представляют отношения с помощью символов, а не букв. Например, в п. 4 примера 4.4.3 мы использовали букву G в качестве имени отношения. Но в этом примере для всех действительных чисел x и y запись xGy означала то же самое, что и $x \geq y$. Это говорит о том, что на самом деле не было необходимости вводить букву G ; мы могли бы просто рассматривать символ \geq как имя отношения. Используя эти обозначения, мы могли бы сказать, что \geq – полный порядок на \mathbb{R} .

Вот еще один пример частичного порядка. Пусть A – множество всех слов английского языка, и пусть $R = \{(x, y) \in A \times A \mid$ все буквы из слова x присутствуют в правильном порядке в слове $y\}$. Например, пары $(can, cannot)$, $(tar, start)$ и $(ball, ball)$ – элементы R , но $(can, anchor)$ и $(can, carnival)$ – нет. Вы должны самостоятельно убедиться, что R рефлексивно, транзитивно и антисимметрично, поэтому R является частичным порядком. Теперь рассмотрим множество $B = \{me, men, tame, mental\} \subseteq A$. Ясно, что многие упорядоченные пары слов в B входят в отношение R , но обратите внимание, в частности, что упорядоченные пары (me, me) , (me, men) , $(me, tame)$ и $(me, mental)$ – все входят в R . Если мы трактуем xRy в том смысле, что y в некотором смысле не меньше x , то мы могли бы сказать, что слово me – это *наименьший* элемент B в том смысле, что он меньше всех остальных в множестве.

Не в каждом множестве слов будет элемент, самый маленький в этом смысле. Например, рассмотрим множество $C = \{a, me, men, tame, mental\} \subseteq A$. Каждое из слов *men*, *tame* и *mental* больше, чем хотя бы одно другое слово в множестве, но ни *a*, ни *me* не больше всех остальных слов в множестве.

Мы будем называть *a* и *te* *минимальными* элементами множества *C*. Но обратите внимание, что ни *a*, ни *te* не являются наименьшими элементами *C* в смысле, описанном в последнем абзаце, потому что ни один из них не меньше другого. Множество *C* имеет два минимальных элемента, но не имеет наименьшего элемента.

Эти примеры могут вызвать у вас ряд вопросов о наименьших и минимальных элементах. Множество *C* имеет два минимальных элемента, но *B* имеет только один наименьший элемент. Может ли множество содержать более одного наименьшего элемента? Если в множестве есть только один минимальный элемент, должен ли он быть наименьшим элементом? Может ли множество иметь наименьший элемент и минимальный элемент, которые отличаются? Были бы ответы на эти вопросы другими, если бы мы ограничили наше внимание только *полными*, а не всеми частичными порядками? Прежде чем мы попытаемся ответить на любой из этих вопросов, мы должны более тщательно сформулировать определения терминов *наименьший* и *минимальный*.

Определение 4.4.4. Предположим, что *R* является частичным порядком на множестве *A*, $B \subseteq A$ и $b \in B$. Тогда *b* называется *R*-наименьшим элементом *B* (или просто наименьшим элементом, если *R* ясен из контекста), если $\forall x \in B (bRx)$. Он называется *R*-минимальным элементом (или просто минимальным элементом), если $\neg \exists x \in B (xRb \wedge x = b)$.

Пример 4.4.5

- Пусть $L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$, как и раньше. Пусть $B = \{x \in \mathbb{R} \mid x \geq 7\}$. Есть ли в *B* какие-либо *L*-наименьшие или *L*-минимальные элементы? А как насчет множества $C = \{x \in \mathbb{R} \mid x > 7\}$? Как упоминалось ранее, мы могли бы обойтись здесь без буквы *L* и упоминать \leq -наименьшие или \leq -минимальные элементы *B* и *C*.
- Пусть *D* – отношение делимости, определенное в п. 3 примера 4.4.3. Пусть $B = \{3, 4, 5, 6, 7, 8, 9\}$. Есть ли в *B* какие-либо *D*-наименьшие или *D*-минимальные элементы?
- Пусть $S = \{(X, Y) \in \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \mid X \subseteq Y\}$, который является частичным порядком на множестве $\mathcal{P}(\mathbb{N})$. Пусть $\mathcal{F} = \{X \in \mathcal{P}(\mathbb{N}) \mid 2 \in X \text{ и } 3 \in X\}$. Обратите внимание, что элементы \mathcal{F} являются не натуральными числами, а *множествами* натуральных чисел. Например, множества $\{1, 2, 3\}$ и $\{n \in \mathbb{N} \mid n \text{ простое число}\}$ оба являются элементами \mathcal{F} . Есть ли у \mathcal{F} какие-либо *S*-наименьшие или *S*-минимальные элементы? А как насчет множества $G = \{X \in \mathcal{P}(\mathbb{N}) \mid \text{либо } 2 \in X, \text{ либо } 3 \in X\}$?

Решения

- Ясно, что $7 \leq x$ для каждого $x \in B$, поэтому $\forall x \in B (7Lx)$ и, следовательно, 7 является наименьшим элементом *B*. Это также минимальный элемент, поскольку ничто в *B* не меньше 7, поэтому $\neg \exists x \in B (xL7 \wedge x \neq 7)$. Нет никаких других наименьших или минимальных элементов. Обратите внимание, что 7 не является наименьшим или минимальным элементом *C*, так как $7 \notin C$. В соответствии с определением 4.4.4 наименьший или

минимальный элемент множества должен фактически быть элементом множества. По сути, C не имеет наименьшего или минимального элемента.

2. Прежде всего обратите внимание, что 6 и 9 не минимальны, потому что оба делятся на 3, а 8 не минимальный, потому что делится на 4. Все остальные элементы B являются минимальными элементами, но ни один из них не является наименьшим элементом.
3. Множество $\{2, 3\}$ является наименьшим элементом \mathcal{F} , поскольку 2 и 3 являются элементами каждого множества в \mathcal{F} , и, следовательно, $\forall X \in \mathcal{F} (\{2, 3\} \subseteq X)$. Это также минимальный элемент, поскольку никакой другой элемент \mathcal{F} не является его подмножеством, и нет других наименьших или минимальных элементов. Множество \mathcal{G} имеет два минимальных элемента: {2} и {3}. Любое другое множество в \mathcal{G} должно содержать одно из них как подмножество, поэтому никакое другое множество не может быть минимальным. Ни одно множество не является наименьшим, поскольку ни один из них не является подмножеством другого.

Теперь мы готовы ответить на некоторые вопросы, которые мы подняли перед определением 4.4.4.

Теорема 4.4.6. *Предположим, что R – частичный порядок на множестве A и $B \subseteq A$.*

1. *Если B имеет наименьший элемент, то этот наименьший элемент уникalen. Таким образом, мы можем говорить о наименьшем элементе **множества B** , а не о самом маленьком элементе среди всех.*
2. *Предположим, что b – наименьший элемент B . Тогда b также является минимальным элементом B , и это единственный минимальный элемент.*
3. *Если R – полный порядок, а b – минимальный элемент B , то b – наименьший элемент B .*

Стратегия доказательства

Эти доказательства несколько сложнее, чем предыдущие в этой главе, поэтому мы немного поработаем, перед тем как составить окончательную формулировку.

1. Конечно, мы начинаем с предположения, что B имеет наименьший элемент, и, поскольку это экзистенциальное утверждение, мы сразу вводим имя, скажем b , для наименьшего элемента B . Мы должны доказать, что b является единственным наименьшим элементом. Как мы видели в разделе 3.6, это можно записать как $\forall c (c - \text{наименьший элемент } B \rightarrow b = c)$, поэтому следующим шагом будет назначение произвольного элемента c . Предположим, что это также наименьший элемент, и докажем, что $b = c$.

На данный момент мы мало что знаем о b и c . Мы знаем, что они оба являются элементами B , но мы даже не знаем, какие типы объектов находятся в B – будь то числа, множества или какой-либо другой тип объекта, – так что это не очень помогает нам в поиске доказательства, что $b = c$. Единственный полезный факт, который мы знаем о b и c ,

заключается в том, что они оба являются наименьшими элементами B , что означает $\forall x \in B(bRx)$ и $\forall x \in B(cRx)$. Самый многообещающий способ использовать эти утверждения – подставить что-нибудь вместо x в каждое утверждение. То, что мы подставляем, должно быть элементом B , и на данный момент мы знаем только два элемента, b и c . Подставив их в оба утверждения, мы получим bRb , bRc , cRb и cRc . Конечно, мы уже знали bRb и cRc , поскольку R рефлексивно. Но когда вы видите bRc и cRb , вам следует вспомнить об антисимметрии. Поскольку R – частичный порядок, он антисимметричен, поэтому из bRc и cRb следует, что $b = c$.

2. Прежде всего мы должны доказать, что b – минимальный элемент в B , что означает $\neg\exists x \in B(xRb \wedge x \neq b)$. Поскольку это отрицательное утверждение, его можно переписать как эквивалентное положительное утверждение:

$\neg\exists x \in B(xRb \wedge x \neq b)$ тогда и только тогда, когда $\forall x \in B \neg(xRb \wedge x \neq b)$
 тогда и только тогда, когда $\forall x \in B(\neg xRb \vee x = b)$
 тогда и только тогда, когда $\forall x \in B(xRb \rightarrow x = b)$.

Таким образом, чтобы доказать, что b минимально, мы могли бы обозначить за x произвольный элемент B , предположить, что xRb , и доказать, что $x = b$.

Итак, неплохо было бы еще раз подвести итоги того, что мы знаем на данный момент о b и x . Мы знаем xRb , и мы знаем, что b – наименьший элемент B , что означает $\forall x \in B(bRx)$. Если мы применим этот последний факт к нашему произвольному x , то, как и в части 1, мы можем использовать антисимметрию для завершения доказательства.

Мы все еще должны доказать, что b – единственный минимальный элемент, и, как и в части 1, это означает $\forall c(c$ – минимальный элемент $B \rightarrow b = c)$. Итак, мы обозначаем за c произвольный элемент B , предполагаем, что c – минимальный элемент B , и стараемся доказать, что $b = c$. Предположение, что c – минимальный элемент B , означает, что $c \in B$ и $\neg x \in B(xRc \wedge x = c)$, но, как и раньше, мы можем переписать это последнее утверждение в эквивалентной положительной форме $\forall x \in B(xRc \rightarrow x = c)$. Чтобы использовать это утверждение, мы должны подставить что-то вместо x , и поскольку наша цель – показать, что $b = c$, подстановка b вместо x выглядит хорошей идеей. Это дает нам $bRc \rightarrow b = c$, поэтому если мы сможем доказать bRc , то завершим доказательство, используя *modus ponens*, чтобы сделать вывод, что $b = c$. Но мы знаем, что b – наименьший элемент B , поэтому, конечно, bRc истинно.

3. Разумеется, мы начинаем с предположения, что R – это полный порядок, а b – минимальный элемент B . Мы должны доказать, что b – наименьший элемент B , что означает $\forall x \in B(bRx)$, поэтому пусть x будет произвольный элемент из B и попытаемся доказать bRx .

Мы знаем из рассмотренных нами примеров, что минимальные элементы в частичных порядках не всегда являются наименьшими элементами, поэтому предположение, что R является полным порядком, должно иметь решающее значение. Предположение о полном порядке

R означает $\forall x \in A \forall y \in A (xRy \vee yRx)$, поэтому, чтобы использовать его, мы должны что-то подставить вместо x и y . Единственные вероятные кандидаты для подстановки – это b и наш произвольный объект x , и, подставив их, мы получим $xRb \vee bRx$. Наша цель – bRx , так что это определенно похоже на прогресс. Нам было бы достаточно только исключить возможность xRb . Итак, давайте посмотрим, сможем ли мы доказать обратное утверждение $\neg xRb$.

Поскольку это отрицательное утверждение, мы попытаемся доказать его от противного. Предположим, что истинно утверждение xRb . Кому утверждению оно может противоречить? Единственное, что мы еще не использовали, – это то, что b минимально, и поскольку это отрицательное утверждение, это естественное место для поиска противоречия. Чтобы опровергнуть тот факт, что b минимально, мы должны попытаться показать, что $\exists x \in B (xRb \wedge x \neq b)$. Но мы уже предполагали xRb , поэтому достаточно доказать $x \neq b$.

На этом этапе вы должны попытаться доказать $x = b$. Другого пути у вас нет. Дело в том, что мы начали с того, что обозначили за x произвольный элемент B , а это означает, что это может быть любой элемент B , включая b . Затем мы предположили, что справедливо xRb , но поскольку R рефлексивно, это не исключает возможности того, что $x = b$. На самом деле у нас нет никакой надежды доказать $x \neq b$. Кажется, мы застряли. Давайте окнем взглядом общий план доказательства. Нам нужно было показать $\forall x \in B (bRx)$, поэтому мы приняли за x произвольный элемент B и пытались доказать bRx . Теперь мы столкнулись с проблемами из-за вероятности того, что $x = b$. Но если наша конечная цель – доказать bRx , то возможность того, что $x = b$ действительно, не является проблемой. Поскольку R рефлексивно, если $x = b$, то, конечно, bRx будет истинно! Итак, как мы должны построить окончательное доказательство? Пожалуйста, что наши рассуждения относительно bRx должны быть разными в зависимости от того, $x = b$ или нет. Это предполагает разделение доказательства на случаи. В случае 1 мы предполагаем, что $x = b$, и используем тот факт, что R рефлексивно, чтобы завершить доказательство. В случае 2 мы предполагаем, что $x \neq b$, и тогда мы можем использовать нашу исходную линию атаки, начиная с того факта, что R является полным порядком.

Доказательство

1. Пусть b является наименьшим элементом B , и пусть c также является наименьшим элементом B . Поскольку b является наименьшим элементом, справедливо утверждение $\forall x \in B (bRx)$, то есть, в частности, bRc . Аналогично, поскольку c – наименьший элемент, то справедливо cRb . Но теперь, поскольку R – частичный порядок, он должен быть антисимметричным, поэтому из bRc и cRb мы можем заключить, что $b = c$.
2. Пусть x – произвольный элемент из B , и пусть xRb . Поскольку b – наименьший элемент B , мы должны иметь bRx , и теперь из антисимметрии следует, что $x = b$. Таким образом, не может быть $x \in B$ такого, что xRb и $x \neq b$, поэтому b – минимальный элемент.

Чтобы убедиться, что это единственный элемент, предположим, что c также является минимальным элементом. Поскольку b – наименьший элемент B , то справедливо bRc . Но тогда, поскольку c минимально, должно быть $b = c$. Таким образом, b – единственный минимальный элемент B .

3. Предположим, что R – полный порядок, а b – минимальный элемент в B . Пусть x – произвольный элемент B . Если $x = b$, то, поскольку R рефлексивно, bRx . Теперь предположим, что $x \neq b$. Поскольку R является полным порядком, мы знаем, что или xRb , или bRx . Но xRb не может быть истинным, поскольку, комбинируя xRb с нашим предположением, что $x \neq b$, мы можем заключить, что b не является минимальным, тем самым противоречи нашему предположению о минимальности. Таким образом, утверждение bRx должно быть истинным. Поскольку x был произвольным, мы можем заключить, что $\forall x \in B(bRx)$, поэтому b – наименьший элемент B .

При сравнении подмножеств некоторого множества A математики часто используют частичный порядок $S = \{(X, Y) \in \mathcal{P}(A) \times \mathcal{P}(A) \mid X \subseteq Y\}$, хотя это не всегда выражено в явном виде. Напомним, что если $\mathcal{F} \subseteq \mathcal{P}(A)$ и $X \in \mathcal{F}$, то согласно определению 4.4.4 X является S -наименьшим элементом \mathcal{F} тогда и только тогда, когда $\forall Y \in \mathcal{F}(X \subseteq Y)$. Другими словами, утверждение, что элемент \mathcal{F} является наименьшим элементом, означает, что это подмножество каждого элемента \mathcal{F} . Точно так же математики иногда говорят, что множество является наименьшим с учетом определенного свойства. Обычно это означает, что у множества есть рассматриваемое свойство, и, кроме того, оно является подмножеством каждого множества, обладающего таким свойством. Например, мы могли бы описать наш вывод в части 3 примера 4.4.5, сказав, что $\{2, 3\}$ – это наименьшее множество $X \subseteq \mathbb{N}$ со свойством $2 \in X$ и $3 \in X$. Вы встретите другие примеры этого подхода в следующих главах.

Пример 4.4.7

1. Найдите наименьшее множество действительных чисел X таких, что $5 \in X$ и для всех действительных чисел x и y если $x \in X$ и $x < y$, то $y \in X$.
2. Найдите наименьшее множество действительных чисел X таких, что $X \neq \emptyset$ и для всех действительных чисел x и y если $x \in X$ и $x < y$, то $y \in X$.

Решения

1. Другой способ сформулировать задачу – сказать, что мы ищем наименьший элемент семейства множеств $\mathcal{F} = \{X \subseteq \mathbb{R} \mid 5 \in X \text{ и } \forall x \forall y((x \in X \wedge x < y) \rightarrow y \in X)\}$, где подразумевается, что *наименьшее* означает наименьший элемент по отношению к частичному порядку подмножества. Теперь для любого множества $x \in \mathcal{F}$ мы знаем, что $5 \in X$, и мы знаем, что $\forall x \forall y((x \in X \wedge x < y) \rightarrow y \in X)$. В частности, так как $5 \in X$, мы можем сказать, что $\forall y(5 < y \rightarrow y \in X)$. Таким образом, если мы положим $A = \{y \in \mathbb{R} \mid 5 < y\}$, то можно заключить, что $\forall X \in \mathcal{F}(A \subseteq X)$. Но легко видеть, что $A \in \mathcal{F}$, поэтому A – наименьший элемент \mathcal{F} .
2. Мы должны найти наименьший элемент семейства множеств $\mathcal{F} = \{X \subseteq \mathbb{R} \mid X \neq \emptyset \text{ и } \forall x \forall y((x \in X \wedge x < y) \rightarrow y \in X)\}$. Множество $A = \{y \in \mathbb{R} \mid 5 \leq y\}$

из п. 1 является элементом \mathcal{F} , но это не самый маленький элемент или даже минимальный элемент, потому что множество $A = \{y \in \mathbb{R} \mid 6 \leq y\}$ меньше – другими словами, $A \subseteq A$ и $A = A$. Но A также не наименьший элемент, поскольку $A = \{y \in \mathbb{R} \mid 7 \leq y\}$ еще меньше. Фактически в этом семействе нет наименьшего или даже минимального элемента. Мы попросим вас проверить это в упражнении 12. Этот пример показывает, что мы должны быть осторожны, говоря о наименьшем множестве с некоторым свойством. Такого наименьшего множества может и не быть!

Вы, наверное, уже догадались, как определять максимальные и наибольшие элементы в частично упорядоченных множествах. Пусть R – частичный порядок на A , $B \subseteq A$ и $b \in B$. Мы говорим, что b – *наибольший элемент* B , если $\forall x \in B (xRb)$, и *максимальный элемент* B , если $\neg \exists x \in B (bRx \wedge b \neq x)$. Конечно, эти определения очень похожи на определения 4.4.4. В упражнении 14 мы попросим вас определить некоторые связи между этими определениями. Другая полезная идея из этой области – концепция верхней или нижней границы множества.

Определение 4.4.8. Предположим, что R – частичный порядок на A , $B \subseteq A$ и $a \in A$. Тогда a называется *нижней границей* для B , если $\forall x \in B (aRx)$. Точно также a называется *верхней границей* для B , если $\forall x \in B (xRa)$.

Обратите внимание, что нижняя граница для B не обязательно должна быть элементом B . Это единственное различие между нижними границами и наименьшими элементами. Наименьший элемент B – это просто нижняя граница, которая также является элементом B . Например, в п. 1 примера 4.4.5 мы пришли к выводу, что число 7 не было наименьшим элементом множества $C = \{x \in \mathbb{R} \mid x > 7\}$, потому что $7 \notin C$. Но 7 – это нижняя граница для C . Фактически это можно сказать и про любое действительное число меньше 7, но не любое число больше 7. Таким образом, множество всех нижних границ C представляет собой множество $\{x \in \mathbb{R} \mid x \leq 7\}$, причем 7 – его наибольший элемент. Мы говорим, что 7 – *точная нижняя граница* множества C .

Определение 4.4.9. Предположим, что R – частичный порядок на A и $B \subseteq A$. Пусть U – множество всех верхних границ для B , а L – множество всех нижних границ. Если U имеет наименьший элемент, то этот наименьший элемент называется *наименьшей верхней границей* B . Если L имеет наибольший элемент, то он называется *наибольшей нижней границей* B . Термины «наименьшая верхняя граница» и «наибольшая нижняя граница» иногда сокращаются до н.в.г. и н.н.г.

Пример 4.4.10

- Пусть $L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$, полный порядок на \mathbb{R} . Пусть $B = \{1/n \mid n \in \mathbb{Z}^+\} = \{1, 1/2, 1/3, 1/4, 1/5, \dots\} \subseteq \mathbb{R}$. Есть ли у B какие-либо верхние или нижние границы? Есть ли у него наименьшая верхняя граница или наибольшая нижняя граница?
- Пусть A – множество всех английских слов, и пусть \mathbb{R} – частичный порядок на A , описанный после примера 4.4.3. Пусть $B = \{\text{hold}, \text{up}\}$. Есть ли

у B верхняя или нижняя граница? Есть ли у него наименьшая верхняя граница или наибольшая нижняя граница?

Решения

1. Очевидно, что наибольший элемент B равен 1. Это также верхняя граница для B , как и любое число, большее 1. По определению верхняя граница для B должна быть не меньше, чем каждый элемент B , поэтому, в частности, оно должно быть не меньше 1. Таким образом, никакое число меньше 1 не является верхней границей для B , поэтому множество верхних границ для B можно описать как $\{x \in \mathbb{R} \mid x \geq 1\}$. Очевидно, что наименьший элемент этого множества равен 1, следовательно, 1 – это н.в.г. для B . Ясно, что 0, как и любое отрицательное число, является нижней границей для B . С другой стороны, предположим, что a – положительное число. Тогда для достаточно большого n будет $1/n < a$. (Вы можете убедиться, что подойдет любое целое число n , большее $1/a$.) Таким образом, нельзя сказать, что $\forall x \in B(a \leq x)$, и, следовательно, a не является нижней границей для B . Итак, множество всех нижних границ для B равно $\{x \in \mathbb{R} \mid x \leq 0\}$, а н.н.г. для B равно 0.
2. Ясно, что слова *holdup* и *uphold* являются верхними границами для B . Фактически никакое более короткое слово не может быть верхней границей, поэтому они оба являются минимальными элементами множества всех верхних границ. Согласно п. 2 теоремы 4.4.6, множество, которое имеет более одного минимального элемента, не может иметь наименьшего элемента, поэтому множество всех верхних границ для B не имеет наименьшего элемента, и, следовательно, B не имеет наименьшей верхней границы.
Слова *hold* и *up* не имеют общих букв, поэтому у B нет нижней границы.

Обратите внимание, что в части 1 примера 4.4.10 самый большой элемент B также оказался его наименьшей верхней границей. Вы можете спросить, всегда ли самые большие элементы являются наименьшими верхними границами и всегда ли наименьшие элементы являются наибольшими нижними границами. Мы попросим вас доказать, что это так, в упражнении 20. Еще один интересный факт об этом примере заключается в том, что хотя у B не было наименьшего элемента, у него была наибольшая нижняя граница. Это не совпадение. Что касается действительных чисел, то это важный факт: каждое непустое множество действительных чисел, имеющих нижнюю границу, имеет точную нижнюю границу, и, аналогично, каждое непустое множество действительных чисел, имеющих верхнюю границу, имеет наименьшую верхнюю границу. Доказательство этого факта выходит за рамки данной книги, но важно понимать, что это особый факт о действительных числах; он не распространяется на все частичные порядки или даже на все полные порядки в целом. Например, множество B во второй части примера 4.4.10 имело верхние границы, но не имело наименьшей верхней границы.

Мы заканчиваем этот раздел, еще раз рассмотрев, как эти новые понятия применяются к частичному порядку подмножества на $\mathcal{P}(A)$ для любого множества A . Оказывается, что в этом частичном порядке наименьшие верхние

границы и наибольшие нижние границы – наши старые знакомые объединения и пересечения.

Теорема 4.4.11. Пусть A – множество, $\mathcal{F} \subseteq \mathcal{P}(A)$ и $\mathcal{F} \neq \emptyset$. Тогда точная верхняя граница \mathcal{F} (в частичном порядке подмножества) равна $\bigcap \mathcal{F}$, а точная нижняя граница \mathcal{F} равна $\bigcap \mathcal{F}$.

Доказательство. См. упражнение 23.

Упражнения

- *1. В каждом случае скажите, является ли R частичным порядком на A . Если да, то является ли оно полным порядком?
 - (а) $A = \{a, b, c\}$, $R = \{(a, a), (b, a), (b, b), (b, c), (c, c)\}$.
 - (б) $A = \mathbb{R}$, $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |x| < |y|\}$.
 - (в) $A = \mathbb{R}$, $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid |x| < |y| \text{ или } x = y\}$.
- 2. В каждом случае скажите, является ли R частичным порядком на A . Если да, то является ли оно полным порядком?
 - (а) A – множество всех слов английского языка, $R = \{(x, y) \in A \times A \mid \text{слово } y \text{ встречается по крайней мере так же поздно в алфавитном порядке, как слово } x\}$.
 - (б) A – множество всех слов английского языка, $R = \{(x, y) \in A \times A \mid \text{первая буква слова } y \text{ встречается в алфавите по крайней мере так же поздно, как и первая буква слова } x\}$.
 - (в) A – множество всех стран мира, $R = \{(x, y) \in A \times A \mid \text{население страны } y \text{ по крайней мере равно населению страны } x\}$.
- 3. В каждом случае найдите все минимальные и максимальные элементы B . Также найдите, если они существуют, наибольший и наименьший элементы B , а также наименьшую верхнюю границу и наибольшую нижнюю границу B .
 - (а) R – отношение, показанное на ориентированном графе на рис. 4.6, $B = \{2, 3, 4\}$.

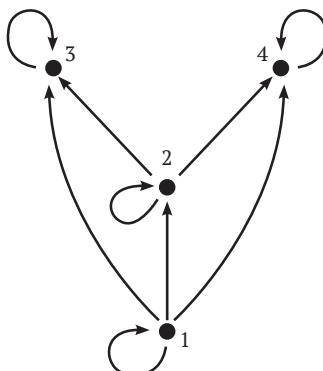


Рис. 4.6 ♦ Ориентированный граф отношения к заданию 3(а)

- (b) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \leq y\}$, $B = \{x \in \mathbb{R} \mid 1 \leq x < 2\}$.
(c) $R = \{(x, y) \in \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \mid x \subseteq y\}$, $B = \{x \in \mathcal{P}(\mathbb{N}) \mid x \text{ имеет не более } 5 \text{ элементов}\}$.
- *4. Предположим, что R – отношение на A . Вы можете подумать, что R не может быть одновременно антисимметричным и симметричным, но это неверно. Докажите, что R одновременно антисимметрично и симметрично тогда и только тогда, когда $R \subseteq i_A$.
5. Предположим, что R – частичный порядок на A и $B \subseteq A$. Докажите, что $R \cap (B \times B)$ – частичный порядок на B .
6. Предположим, что R_1 и R_2 – частичные порядки на A . Для каждой части приведите доказательство или контрпример, чтобы обосновать свой ответ.
- (a) Должно ли $R_1 \cap R_2$ быть частичным порядком на A ?
 - (b) Должно ли $R_1 \cup R_2$ быть частичным порядком на A ?
7. Предположим, что R_1 – частичный порядок на A_1 , R_2 – частичный порядок на A_2 и $A_1 \cap A_2 = \emptyset$.
- (a) Докажите, что $R_1 \cup R_2$ – частичный порядок на $A_1 \cup A_2$.
 - (b) Докажите, что $R_1 \cup R_2 \cup (A_1 \times A_2)$ является частичным порядком на $A_1 \cup A_2$.
 - (c) Предположим, что R_1 и R_2 – полные порядки. Являются ли частичные порядки в п. (a) и (b) также полными порядками?
- *8. Предположим, что R – частичный порядок на A , а S – частичный порядок на B . Определим соответствие из T в $A \times B$ следующим образом: $T = \{((a, b), (a', b')) \in (A \times B) \times (A \times B) \mid aRa' \text{ и } bSb'\}$. Покажите, что T – это частичный порядок на $A \times B$. Будет ли T также полным порядком, если и R , и S являются полными порядками?
9. Предположим, что R – частичный порядок на A , а S – частичный порядок на B . Определим соответствие из L в $A \times B$ следующим образом: $L = \{((a, b), (a', b')) \in (A \times B) \times (A \times B) \mid aRa', \text{ и если } a = a' \text{ то } bSb'\}$. Покажите, что L является частичным порядком на $A \times B$. Будет ли L также полным порядком, если и R , и S являются полными порядками?
10. Предположим, что R – частичный порядок на A . Для каждого $x \in A$ пусть $P_x = \{a \in A \mid aRx\}$. Докажите, что $\forall x \in A \ \forall y \in A (xRy \leftrightarrow P_x \subseteq P_y)$.
- *11. Пусть D – отношение делимости, определенное в п. 3 примера 4.4.3. Пусть $B = \{x \in Z \mid x > 1\}$. Есть ли у B минимальные элементы? Если да, то какие? Есть ли у B наименьший элемент? Если да, то какой?
12. Покажите, что, как было сказано в п. 2 примера 4.4.7, $\{X \subseteq R \mid X \neq \emptyset \text{ и } \forall x \forall y ((x \in X \wedge x < y) \rightarrow y \in X)\}$ не имеет минимального элемента.
13. Предположим, что R – частичный порядок на A . Докажите, что R^{-1} также является частичным порядком на A . Если R – полный порядок, будет ли R^{-1} также полным порядком?
- *14. Предположим, что R – частичный порядок на A , $B \subseteq A$ и $b \in B$. В упражнении 13 доказано, что R^{-1} также является частичным порядком на A .

- (a) Докажите, что b является R -наибольшим элементом B тогда и только тогда, когда это R^{-1} -наименьший элемент B .
- (b) Докажите, что b является R -максимальным элементом B тогда и только тогда, когда он является R^{-1} -минимальным элементом B .
15. Предположим, что R_1 и R_2 – частичные порядки на A , $R_1 \subseteq R_2$, $B \subseteq A$ и $b \in B$.
- (a) Докажите, что если b является R_1 -наименьшим элементом B , то он также является R_2 -наименьшим элементом B .
- (b) Докажите, что если b является R_2 -минимальным элементом в B , то он также является R_1 -минимальным элементом в B .
16. Предположим, что R – частичный порядок на A , $B \subseteq A$ и $b \in B$. Докажите, что если b – наибольший элемент B , то b также является максимальным элементом B , и это единственный максимальный элемент.
- *17. Если подмножество частично упорядоченного множества имеет ровно один минимальный элемент, должен ли этот элемент быть наименьшим элементом? Приведите доказательство или контрпример, чтобы обосновать свой ответ.
18. Предположим, что R – частичный порядок на A , $B_1 \subseteq A$, $B_2 \subseteq A$, $\forall x \in B_1 \exists y \in B_2 (xRy)$ и $\forall x \in B_2 \exists y \in B_1 (xRy)$.
- (a) Докажите, что для всех $x \in A$ элемент x является верхней границей B_1 тогда и только тогда, когда x является верхней границей B_2 .
- (b) Докажите, что если B_1 и B_2 не пересекаются, то ни один из них не имеет максимального элемента.
19. Рассмотрим следующую предположительную теорему.
- Предположительная теорема.** Предположим, что R – полный порядок на A и $B \subseteq A$. Тогда каждый элемент B является либо наименьшим элементом B , либо наибольшим элементом B .
- (a) Где ошибка в следующем доказательстве теоремы?
- Доказательство.* Предположим, что $b \in B$. Пусть x – произвольный элемент из B . Так как R – полный порядок, либо bRx , либо xRb .
- Случай 1. bRx . Поскольку x был произвольным, мы можем заключить, что $\forall x \in B (bRx)$, так что b является наименьшим элементом R .
- Случай 2. xRb . Поскольку x был произвольным, мы можем заключить, что $\forall x \in B (xRb)$, поэтому b является наибольшим элементом R .
- Таким образом, b является либо наименьшим элементом B , либо наибольшим элементом B . Поскольку b было произвольным, каждый элемент B является либо его наименьшим элементом, либо его наибольшим элементом.
- (b) Верна ли теорема? Обоснуйте свой ответ либо доказательством, либо контрпримером.
20. Предположим, что R – частичный порядок на A , $B \subseteq A$ и $b \in B$.
- (a) Докажите, что если b – наименьший элемент B , то он также является точной нижней границей B .

- (b) Докажите, что если b – наибольший элемент B , то он также является наименьшей верхней границей B .
- *21. Предположим, что R – частичный порядок на A и $B \subseteq A$. Пусть U – множество всех верхних границ для B .
- Докажите, что U ограничено вверх; то есть докажите, что если $x \in U$ и xRy , то $y \in U$.
 - Докажите, что каждый элемент B является нижней границей для U .
 - Докажите, что если x – точная нижняя граница U , то x – точная верхняя граница B .
22. Предположим, что R – частичный порядок на A , $B_1 \subseteq A$, $B_2 \subseteq A$, x_1 – точная верхняя граница B_1 , а x_2 – точная верхняя граница B_2 . Докажите, что если $B_1 \subseteq B_2$, то x_1Rx_2 .
23. Докажите теорему 4.4.11.
- *24. Пусть R – отношение на A . Пусть $S = R \cup R^{-1}$.
- Покажите, что S – симметричное отношение на A и $R \subseteq S$.
 - Покажите, что если T – симметричное отношение на A и $R \subseteq T$, то $S \subseteq T$.
- Обратите внимание, что это упражнение показывает, что S – наименьший элемент множества $\mathcal{F} = \{T \subseteq A \times A \mid R \subseteq T \text{ и } T \text{ симметрично}\}$; другими словами, это наименьшее симметричное отношение на A , которое содержит R как подмножество. Отношение S называется *симметричным замыканием* R .
25. Предположим, что R – отношение на A . Пусть $\mathcal{F} = \{T \subseteq A \times A \mid R \subseteq T \text{ и } T \text{ транзитивно}\}$.
- Покажите, что $\mathcal{F} \neq \emptyset$.
 - Покажите, что $\bigcap \mathcal{F}$ – транзитивное отношение на A и $R \subseteq \bigcap \mathcal{F}$.
 - Покажите, что $\bigcap \mathcal{F}$ – наименьшее транзитивное отношение на A , содержащее R как подмножество. Отношение $\bigcap \mathcal{F}$ называется *транзитивным замыканием* R .
26. Пусть R_1 и R_2 – отношения на A и $R_1 \subseteq R_2$.
- Пусть S_1 и S_2 – симметричные замыкания R_1 и R_2 соответственно. Докажите, что $S_1 \subseteq S_2$ (см. определение симметричного замыкания в упражнении 24).
 - Пусть T_1 и T_2 – транзитивные замыкания R_1 и R_2 соответственно. Докажите, что $T_1 \subseteq T_2$ (см. определение транзитивного замыкания в упражнении 25).
- *27. Пусть R_1 и R_2 – отношения на A , и пусть $R = R_1 \cup R_2$.
- Пусть S_1 , S_2 и S – симметричные замыкания R_1 , R_2 и R соответственно. Докажите, что $S_1 \cup S_2 = S$ (см. определение симметричного замыкания в упражнении 24).
 - Пусть T_1 , T_2 и T – транзитивные замыкания R_1 , R_2 и R соответственно. Докажите, что $T_1 \cup T_2 \subseteq T$, и приведите пример, показывающий, что возможна ситуация, когда $T_1 \cup T_2 \neq T$ (см. определение транзитивного замыкания в упражнении 25).

28. Пусть A – множество.
- Докажите, что если A имеет хотя бы два элемента, то не существует наибольшего антисимметричного отношения на A . Другими словами, не существует такого отношения R на A , что R антисимметрично, и для любого антисимметричного отношения S на A истинно $S \subseteq R$.
 - Предположим, что R – полный порядок на A . Докажите, что R – максимальное антисимметричное отношение на A . Другими словами, не существует антисимметричного отношения S на A такого, что $R \subseteq S$ и $R \neq S$.
29. Предположим, что R – отношение на A . Мы говорим, что R нерефлексивно, если $\forall x \in A ((x, x) \notin R)$. Отношение R называется *строгим частичным порядком* на A , если оно нерефлексивно и транзитивно. Оно называется *строгим полным порядком*, если является строгим частичным порядком и, кроме того, $\forall x \in A \forall y \in A (xRy \vee yRx \vee x = y)$. (Обратите внимание, что используемая здесь терминология несколько вводит в заблуждение, потому что строгий частичный порядок не является особым видом частичного порядка. Это вообще не частичный порядок, поскольку он не рефлексивен!)
- Пусть $L = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x < y\}$. Покажите, что L – строгий полный порядок на \mathbb{R} .
 - Покажите, что если R – частичный порядок на A , то $R \setminus i_A$ – строгий частичный порядок на A , и если R – полный порядок на A , то $R \setminus i_A$ – строгий полный порядок на A .
 - Покажите, что если R – строгий частичный порядок на A , то $R \cup i_A$ – частичный порядок на A , а если R – строгий полный порядок на A , то $R \cup i_A$ – полный порядок на A .
30. Предположим, что R – отношение на A , и пусть T – транзитивное замыкание R . Докажите, что если R симметрично, то и T симметрично. (Подсказка: предположим, что R симметрично. Докажите, что $R \subseteq T^{-1}$ и T^{-1} транзитивны. Что вы можете заключить относительно T и T^{-1} ? См. определение транзитивного замыкания в упражнении 25.)

4.5. Отношения эквивалентности

В примере 4.3.3 мы видели, что отношение тождества i_A на любом множестве A всегда рефлексивно, симметрично и транзитивно. Отношения с этой комбинацией свойств часто возникают в математике, и у них есть некоторые важные свойства, которые мы исследуем в этом разделе. Эти отношения называются *отношениями эквивалентности*.

Определение 4.5.1. Предположим, что R – отношение на множестве A . Тогда R называется *отношением эквивалентности на A* (или просто *отношением эквивалентности*, если A ясно из контекста), если оно рефлексивно, симметрично и транзитивно.

Как мы заметили ранее, отношение тождества i_A на множестве A является отношением эквивалентности. В качестве другого примера пусть T будет множеством всех треугольников, и пусть C будет отношением конгруэнтности треугольников. Другими словами, $C = \{(s, t) \in T \times T \mid \text{треугольник } s \text{ конгруэнтен треугольнику } t\}$. (Напомним, что если один треугольник можно, не искажая, переместить таким образом, чтобы он совпал с другим треугольником, то такие треугольники конгруэнтны.) Ясно, что каждый треугольник конгруэнтен сам себе, поэтому C рефлексивно. Кроме того, если треугольник s конгруэнтен треугольнику t , то t конгруэнтен s , поэтому C симметрично; и если r конгруэнтно s и s конгруэнтен t , то r конгруэнтен t , поэтому C транзитивно. Таким образом, C является отношением эквивалентности на T .

В качестве еще одного примера пусть P – множество всех людей, и пусть $B = \{(p, q) \in P \times P \mid \text{человек } p \text{ имеет тот же день рождения, что и человек } q\}$. (Под «одним днем рождения» мы подразумеваем один и тот же месяц и день, но не обязательно один и тот же год.) У всех один и тот же день рождения, так что B рефлексивно. Если p имеет тот же день рождения, что и q , то q имеет тот же день рождения, что и p , поэтому B симметрично. И если p имеет тот же день рождения, что и q , а q имеет тот же день рождения, что и r , то p имеет тот же день рождения, что и r , поэтому B транзитивно. Следовательно, B – отношение эквивалентности.

Возможно, будет поучительно более внимательно взглянуть на отношение B . Мы можем трактовать его как разбиение множества P всех людей на 366 категорий, по одной для каждого возможного дня рождения. (Помните, некоторые люди родились 29 февраля!) Упорядоченная пара людей будет элементом B , если люди принадлежат к одной категории, но не будет элементом B , если люди происходят из разных категорий. Мы можем считать, что эти категории образуют семейство подмножеств P , которые мы могли бы записать как индексированное семейство следующим образом. Прежде всего пусть D будет множеством всех возможных дней рождения. Другими словами, $D = \{1 \text{ янв.}, 2 \text{ янв.}, 3 \text{ янв.}, \dots, 30 \text{ дек.}, 31 \text{ дек.}\}$. Теперь для каждого $d \in D$ пусть $P_d = \{p \in P \mid \text{человек } p \text{ родился в день } d\}$. Тогда семейство $\mathcal{F} = \{P_d \mid d \in D\}$ – это индексированное семейство подмножеств P . Элементы \mathcal{F} называются *классами эквивалентности* для отношения B , и каждый человек является элементом ровно одного из этих классов эквивалентности. Отношение B состоит из таких пар $(p, q) \in P \times P$, что люди p и q находятся в одном классе эквивалентности. Другими словами:

$$\begin{aligned} B &= \{(p, q) \in P \times P \mid \exists d \in D(p \in P_d \text{ и } q \in P_d)\} \\ &= \{(p, q) \in P \times P \mid \exists d \in D((p, q) \in P_d \times P_d)\} \\ &= \bigcup_{d \in D}(P_d \times P_d). \end{aligned}$$

Мы будем называть семейство \mathcal{F} *разбиением* P , потому что оно разбивает множество P на непересекающиеся части. Оказывается, каждое отношение эквивалентности на множестве A определяет разбиение A , элементы которого являются классами эквивалентности для отношения эквивалентности. Но прежде чем мы сможем выяснить, почему это так, мы должны более тщательно определить термины «разбиение» и «класс эквивалентности».

Определение 4.5.2. Предположим, что A – множество и $\mathcal{F} \subseteq \mathcal{P}(A)$. Мы будем говорить, что \mathcal{F} попарно не пересекается, если каждая пара различных элементов \mathcal{F} не пересекается, или, другими словами, $\forall X \in \mathcal{F} \forall Y \in \mathcal{F} (X = Y \rightarrow X \cap Y = \emptyset)$. (Эта концепция обсуждалась в упражнении 5 раздела 3.6.) \mathcal{F} называется разбиением A , если оно обладает следующими свойствами:

1. $\bigcup \mathcal{F} = A$.
2. \mathcal{F} попарно не пересекается.
3. $\forall x \in \mathcal{F} (X \neq \emptyset)$.

Например, предположим, что $A = \{1, 2, 3, 4\}$ и $\mathcal{F} = \{\{2\}, \{1, 3\}, \{4\}\}$. Тогда $\bigcap \mathcal{F} = \{2\} \cup \mathcal{F} \{1, 3\} \cup \{4\} = \{1, 2, 3, 4\} = A$, так что \mathcal{F} удовлетворяет первому предложению в определении разбиения. Кроме того, никакие два множества в \mathcal{F} не имеют общих элементов, поэтому \mathcal{F} попарно не пересекается, и ясно, что все множества в \mathcal{F} непусты. Таким образом, \mathcal{F} является разбиением A . С другой стороны, семейство $G = \{\{1, 2\}, \{1, 3\}, \{4\}\}$ не является попарно дизъюнктным, поскольку $\{1, 2\} \cap \{1, 3\} = \{1\} \neq \emptyset$, поэтому это не разделение A . Семейство $H = \{\{0, 2\}, \{1, 3\}, \{4\}\}$ также не является разбиением A , поскольку оно не соответствует третьему требованию в определении.

Определение 4.5.3. Предположим, что R – отношение эквивалентности на множестве A и $x \in A$. Тогда класс эквивалентности x относительно R – это множество

$$[x]_R = \{y \in A \mid yRx\}.$$

Если R ясно из контекста, тогда мы просто пишем $[x]$ вместо $[x]_R$. Множество всех классов эквивалентности элементов A называется A по модулю R и обозначается A/R . Таким образом:

$$A/R = \{[x]_R \mid x \in A\} = \{X \subseteq A \mid \exists x \in A (X = [x]_R)\}.$$

В случае отношения «одинаковый день рождения» B если p – любой человек, то согласно определению 4.5.3:

$$\begin{aligned} [p]_B &= \{q \in P \mid qBp\} \\ &= \{q \in P \mid \text{человек } q \text{ имеет тот же день рождения, что и человек } p\}. \end{aligned}$$

Например, если Джон родился 10 августа, то

$$\begin{aligned} [\text{Джон}]_B &= (q \in P \mid \text{у человека } q \text{ тот же день рождения, что и у Джона}) \\ &= \{q \in P \mid \text{человек } q \text{ родился 10 августа}\}. \end{aligned}$$

В обозначениях, которые мы ввели ранее, это просто множество P_d для $d = 10$ августа. Фактически теперь должно быть ясно, что для любого человека p , если мы обозначим за d день рождения p , то $[p]_B = P_d$. Это согласуется с нашим предыдущим утверждением, что множества P_d являются классами эквивалентности для отношения эквивалентности B . Согласно определению 4.5.3, множество всех этих классов эквивалентности называется P по модулю B :

$$P/B = \{[p]_B \mid p \in P\} = \{P_d \mid d \in D\}.$$

В упражнении 6 вас попросят более тщательно доказать это уравнение. Как мы заметили ранее, это семейство является разбиением P .

Рассмотрим еще один пример. Пусть S – отношение на \mathbb{R} , определенное следующим образом:

$$S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x - y \in \mathbb{Z}\}.$$

Например, $(5,73, 2,73) \in S$ и $(-1,27, 2,73) \in S$, так как $5,73 - 2,73 = 3 \in \mathbb{Z}$ и $-1,27 - 2,73 = -4 \in \mathbb{Z}$, но $(1,27, 2,73) \notin S$, поскольку $1,27 - 2,73 = -1,46 \notin \mathbb{Z}$. Ясно, что для любого $x \in \mathbb{R}$ истинно $x - x = 0 \in \mathbb{Z}$, поэтому $(x, x) \in S$, и поэтому S рефлексивно. Чтобы убедиться, что S симметрично, предположим, что $(x, y) \in S$. По определению S это означает, что $x - y \in \mathbb{Z}$. Но тогда $y - x = -(x - y) \in \mathbb{Z}$ тоже, поскольку отрицательное значение любого целого числа также является целым числом, поэтому $(y, x) \in S$. Поскольку (x, y) был произвольным элементом S , это показывает, что S симметрично. Наконец, чтобы доказать, что S транзитивно, предположим, что $(x, y) \in S$ и $(y, z) \in S$. Тогда $x - y \in \mathbb{Z}$ и $y - z \in \mathbb{Z}$. Поскольку сумма любых двух целых чисел является целым числом, отсюда следует, что $x - z = (x - y) + (y - z) \in \mathbb{Z}$, поэтому $(x, z) \in S$, как требуется. Таким образом, S – отношение эквивалентности на \mathbb{R} .

Как выглядят классы эквивалентности для этого отношения эквивалентности? Мы уже наблюдали, что $(5,73, 2,73) \in S$ и $(-1,27, 2,73) \in S$, поэтому $5,73 \in [2,73]$ и $-1,27 \in [2,73]$. Фактически нетрудно увидеть, какими будут другие элементы этого класса эквивалентности:

$$[2,73] = \{\dots, -1,27, -0,27, 0,73, 1,73, 2,73, 3,73, 4,73, 5,73, \dots\}.$$

Иными словами, класс эквивалентности содержит все положительные действительные числа в форме « $_-, 73$ » и все отрицательные действительные числа в форме « $-_, 27$ ». В общем, для любого действительного числа x класс эквивалентности x будет содержать все действительные числа, которые отличаются от x на целое число:

$$[x] = \{\dots, x - 3, x - 2, x - 1, x, x + 1, x + 2, x + 3, \dots\}.$$

Вот несколько фактов об этих классах эквивалентности, которые вы можете попытаться доказать самостоятельно. Как вы можете видеть в последнем уравнении, x всегда является элементом $[x]$. Если мы выберем любое число x G $[2,73]$, то $[x]$ будет точно таким же, как $[2,73]$. Например, если $x = 4,73$, мы находим, что

$$[4,73] = \{\dots, -1,27, -0,27, 0,73, 1,73, 2,73, 3,73, 4,73, 5,73, \dots\} = [2,73].$$

Таким образом, $[4,73]$ и $[2,73]$ – это просто два разных названия одного и того же множества. Но если мы выберем $x \notin [2,73]$, то $[x]$ будет отличаться от $[2,73]$. Например,

$$[1,3] = \{\dots, 1,7, -0,7, 0,3, 1,3, 2,3, 3,3, 4,3, \dots\}.$$

Фактически из этих уравнений видно, что $[1,3]$ и $[2,73]$ не имеют общих элементов. Другими словами, $[1,3]$ не пересекается с $[2,73]$. В общем, для лю-

бых двух действительных чисел x и y классы эквивалентности $[x]$ и $[y]$ либо идентичны, либо не пересекаются. Каждый класс эквивалентности имеет много разных имен, но разные классы эквивалентности не пересекаются. Поскольку $[x]$ всегда содержит x как элемент, каждый класс эквивалентности не пуст, и каждое действительное число x находится ровно в одном классе эквивалентности, а именно $[x]$. Другими словами, множество всех классов эквивалентности \mathbb{R}/S является разбиением \mathbb{R} . Это еще одна иллюстрация того факта, что классы эквивалентности, определяемые отношением эквивалентности, всегда образуют разбиение.

Теорема 4.5.4. Предположим, что R – отношение эквивалентности на множестве A . Тогда A/R – разбиение A .

Доказательство теоремы 4.5.4 будет легче понять, если мы сначала докажем несколько фактов о классах эквивалентности. Факты, которые доказываются в первую очередь с целью использования их для доказательства теорем, обычно называют **леммами**.

Лемма 4.5.5. Предположим, что R – отношение эквивалентности на A . Тогда:

1. Для любого $x \in A$ истинно $x \in [x]$.
2. Для любых $x \in A$ и $y \in A$ утверждение $y \in [x]$ истинно тогда и только тогда, когда $[y] = [x]$.

Доказательство

1. Пусть $x \in A$ произвольно. Поскольку R рефлексивно, то xRx . Следовательно, по определению класса эквивалентности $x \in [x]$.
2. (\rightarrow) Предположим, что $y \in [x]$. Тогда по определению класса эквивалентности yRx . Теперь предположим, что $z \in [y]$. Тогда zRy . Поскольку истинны zRy и yRx , транзитивность R позволяет заключить, что истинно zRx , поэтому $z \in [x]$. Поскольку z был произвольным, это показывает, что $[y] \subseteq [x]$.

Теперь предположим, что $z \in [x]$, поэтому zRx . Мы уже знаем yRx , и поскольку R симметрично, мы можем заключить, что xRy . Применяя транзитивность к zRx и xRy , мы можем заключить, что zRy истинно, поэтому $z \in [y]$. Следовательно, $[x] \subseteq [y]$, поэтому $[x] = [y]$.

(\leftarrow) Предположим, что $[y] = [x]$. Из п. 1 мы знаем, что $y \in [y]$, поэтому из $[y] = [x]$ следует, что $y \in [x]$.

Комментарий

1. Согласно определению классов эквивалентности $x \in [x]$ означает xRx . Вот почему мы используем тот факт, что R рефлексивно.
2. Конечно, форма цели «*тогда и только тогда*» заставляет нас доказывать оба направления по отдельности. Для направления \rightarrow цель – $[y] = [x]$, и, поскольку $[y]$ и $[x]$ – множества, мы можем доказать это, доказав $[y] \subseteq [x]$ и $[x] \subseteq [y]$. Мы докажем каждое из этих утверждений обычным методом, беря произвольный элемент из одного множества и доказывая, что он входит в другое. На протяжении всего доказательства мы неоднократно используем определение классов эквивалентности, как делали это при доказательстве утверждения 1.

Доказательство теоремы 4.5.4. Чтобы доказать, что A/R является разбиением A , мы должны доказать три свойства из определения 4.5.2. Во-первых, мы должны показать, что $\bigcup(A/R) = A$, или, другими словами, что $\bigcup_{x \in A} [x] = A$. Теперь каждый класс эквивалентности в A/R является подмножеством A , поэтому очевидно, что их объединение также является подмножеством A . Таким образом, $\bigcup(A/R) \subseteq A$, поэтому для завершения доказательства нам осталось показать лишь, что $A \subseteq \bigcup(A/R)$. Чтобы доказать это, предположим, что $x \in A$. Тогда по лемме 4.5.5 $x \in [x]$ и, конечно, $[x] \in A/R$, поэтому $x \in \bigcup(A/R)$. Таким образом, $\bigcup(A/R) = A$.

Чтобы убедиться, что A/R попарно не пересекаются, предположим, что X и Y – два элемента A/R и $X \cap Y \neq \emptyset$. По определению A/R , X и Y являются классами эквивалентности, поэтому мы должны иметь $X = [x]$ и $Y = [y]$ для некоторых $x, y \in A$. Поскольку $X \cap Y \neq \emptyset$, мы можем выбрать некоторый z такой, что $z \in X \cap Y = [x] \cap [y]$. Теперь по лемме 4.5.5, поскольку $z \in [x]$ и $z \in [y]$, следует, что $[x] = [z] = [y]$. Таким образом, $X = Y$. Это показывает, что если $X \neq Y$, то $X \cap Y = \emptyset$, поэтому A/R попарно не пересекается.

Наконец, что касается последнего пункта определения разбиения, предположим, что $X \in A/R$. Как и раньше, это означает, что $X = [x]$ для некоторого $x \in A$. Теперь по лемме 4.5.5 $x \in [x] = X$, поэтому $X \neq \emptyset$, что и требовалось доказать.

Комментарий. Мы по интуитивным соображениям использовали формулу $\bigcup(A/R) \subseteq A$, но если вы не уверены, почему это правильно, вам следует написать формальное доказательство. (Вы также можете посмотреть упражнение 16 в разделе 3.3.) Доказательство того, что $A \subseteq \bigcup(A/R)$, вас не затруднит.

Определение попарной дизъюнктиности (несовместности) предполагает, что для доказательства того, что A/R попарно не пересекается, мы должны объявить X и Y произвольными элементами A/R , а затем доказать, что $X \neq Y \rightarrow X \cap Y = \emptyset$. Напомним, что утверждение, что множество пустое, – на самом деле утверждение отрицания, поэтому и антецедент, и следствие этого условного выражения отрицательны. Это говорит о том, что, вероятно, будет легче доказать контрапозитив, поэтому мы предполагаем $X \cap Y \neq \emptyset$ и доказываем, что $X = Y$. Все посылки $X \in A/R$, $Y \in A/R$ и $X \cap Y \neq \emptyset$ являются экзистенциальными утверждениями, поэтому мы должны ввести переменные x , y и z . Лемма 4.5.5 теперь применяется для доказательства того, что $X = Y$, а также доказательства последнего предложения в определении разбиения.

Теорема 4.5.4 гласит, что если R – отношение эквивалентности на A , то A/R – это разбиение A . Фактически оказывается, что каждое разбиение A возникает таким образом.

Теорема 4.5.6. Предположим, что A – множество, а \mathcal{F} – разбиение A . Тогда существует отношение эквивалентности R на A такое, что $A/R = \mathcal{F}$.

Прежде чем доказывать эту теорему, возможно, стоит кратко обсудить стратегию доказательства. Поскольку заключение теоремы является экзистенциальным утверждением, мы должны попытаться найти отношение эквивалентности R такое, что $A/R = \mathcal{F}$. Очевидно, что для разных вариантов выбора \mathcal{F} нам нужно будет найти разные R , в какой-то степени зависящие

от \mathcal{F} . Если вспомнить пример с днем рождения в начале этого раздела, это поможет вам понять, как действовать дальше. Напомним, что в этом примере отношение эквивалентности B состояло из всех пар людей (p, q) таких, что p и q находились в одном множестве в разбиении $\{P_d \mid d \in D\}$. Фактически мы обнаружили, что можем также выразить это, сказав, что $B = \bigcup_{d \in D} (P_d \times P_d)$. Это говорит о том, что в доказательстве теоремы 4.5.6 мы можем обозначить за R множество всех пар $(x, y) \in A \times A$ таких, что x и y находятся в одном множестве в разбиении \mathcal{F} . Альтернативная запись имеет вид $R = \bigcup_{X \in \mathcal{F}} (X \times X)$.

Вернемся на минуту к примеру разбиения, приведенному после определения 4.5.2. В этом примере у нас было $A = \{1, 2, 3, 4\}$ и $\mathcal{F} = \{\{2\}, \{1, 3\}, \{4\}\}$. Теперь давайте определим отношение R на A , как предложено в последнем абзаце. Это дает нам следующее:

$$\begin{aligned} R &= \bigcup_{X \in \mathcal{F}} (X \times X) \\ &= (\{2\} \times \{2\}) \cup (\{1, 3\} \times \{1, 3\}) \cup (\{4\} \times \{4\}) \\ &= \{(2, 2)\} \cup \{(1, 1), (1, 3), (3, 1), (3, 3)\} \cup \{(4, 4)\} \\ &= \{(2, 2), (1, 1), (1, 3), (3, 1), (3, 3), (4, 4)\}. \end{aligned}$$

Ориентированный граф для этого отношения показан на рис. 4.7. Самостоятельно убедитесь, что R является отношением эквивалентности и что классы эквивалентности таковы:

$$[2] = \{2\}, [1] = [3] = \{1, 3\}, [4] = \{4\}.$$

Таким образом, множество всех классов эквивалентности есть $A/R = \{\{2\}, \{1, 3\}, \{4\}\}$, что в точности совпадает с разбиением \mathcal{F} , с которого мы начали.

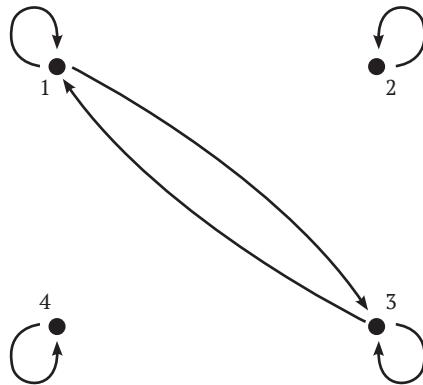


Рис. 4.7 ♦ Ориентированный граф отношения $R = \bigcup_{X \in \mathcal{F}} (X \times X)$

Конечно, рассуждения, которые привели нас к формуле $R = \bigcup_{X \in \mathcal{F}} (X \times X)$, не являются частью доказательства теоремы 4.5.6. Когда мы пишем доказательство, мы можем просто определить R таким образом, а затем проверить, что это отношение эквивалентности на A и что $A/R = \mathcal{F}$. Если мы докажем некоторые новые леммы, это может еще больше упростить доказательство.

Лемма 4.5.7. Предположим, A – множество, а \mathcal{F} – разбиение A . Пусть $R = \bigcup_{x \in \mathcal{F}} (X \times X)$. Тогда R – отношение эквивалентности на A . Мы будем называть R отношением эквивалентности, определяемым \mathcal{F} .

Доказательство. Мы докажем, что R рефлексивно, а остальное оставим вам в упражнении 8. Пусть x – произвольный элемент A . Поскольку \mathcal{F} – разбиение A , то $\bigcup \mathcal{F} = A$, поэтому $x \in \bigcup \mathcal{F}$. Таким образом, мы можем выбрать некоторый $X \in \mathcal{F}$, так что $x \in X$. Но тогда $(x, x) \in X \times X$, поэтому $(x, x) \in \bigcup_{x \in \mathcal{F}} (X \times X) = R$. Следовательно, R рефлексивно.

Комментарий. Обозначив за x произвольный элемент из A , мы должны доказать $(x, x) \in R$. Поскольку $R = \bigcup_{x \in \mathcal{F}} (X \times X)$, это означает, что мы должны доказать $\exists X \in \mathcal{F} (x, x) \in X \times X$, или, другими словами, $\exists X \in \mathcal{F} (x \in X)$. Но это просто означает, что $x \in \bigcup \mathcal{F}$, поэтому в доказательстве предлагается использовать первое предложение в определении раздела, в котором говорится, что $\bigcup \mathcal{F} = A$.

Лемма 4.5.8. Предположим, что A – множество, а \mathcal{F} – разбиение A . Пусть R – отношение эквивалентности, определяемое \mathcal{F} . Предположим, что $X \in \mathcal{F}$ и $x \in X$. Тогда $[x]_R = X$.

Доказательство. Предположим, что $y \in [x]_R$. Тогда $(y, x) \in R$, поэтому по определению R должен существовать некоторый $Y \in \mathcal{F}$, такой что $(y, x) \in Y \times Y$, и, следовательно, $y \in Y$ и $x \in Y$. Поскольку $x \in X$ и $x \in Y$, $X \cap Y \neq \emptyset$, а поскольку \mathcal{F} попарно не пересекается, то $X = Y$. Таким образом, так как $y \in Y$, то $y \in X$. Поскольку y был произвольным элементом из $[x]_R$, мы можем заключить, что $[x]_R \subseteq X$.

Теперь пусть $y \in X$. Тогда $(y, x) \in X \times X$, поэтому $(y, x) \in R$ и, следовательно, $y \in [x]_R$. Таким образом, $X \subseteq [x]_R$, поэтому $[x]_R = X$.

Комментарий. Чтобы доказать $[x]_R = X$, докажем $[x]_R \subseteq X$ и $X \subseteq [x]_R$. Мы начнем с произвольного $y \in [x]_R$ и докажем $y \in X$. Записав определение $[x]_R$, мы получим $(y, x) \in R$, и поскольку R было определено как $\bigcup_{Y \in \mathcal{F}} (Y \times Y)$, это означает $\exists Y \in \mathcal{F} (y, x) \in Y \times Y$. Конечно, поскольку это экзистенциальное утверждение, мы немедленно вводим новую переменную Y . Так как это дает нам $y \in Y$ и наша цель – $y \in X$, неудивительно, что доказательство завершается доказательством $Y = X$.

Доказательство того, что $X \subseteq [x]_R$, также использует определения $[x]_R$ и R , но более прямолинейно.

Доказательство теоремы 4.5.6. Пусть $R = \bigcup_{x \in \mathcal{F}} (X \times X)$. Мы уже видели, что R является отношением эквивалентности, поэтому нам нужно лишь удостовериться, что $A/R = \mathcal{F}$. Чтобы убедиться в этом, предположим, что $X \in A/R$. Это означает, что $X = [x]$ для некоторого $x \in A$. Поскольку \mathcal{F} является разбиением, мы знаем, что $\bigcup \mathcal{F} = A$, поэтому $x \in \bigcup \mathcal{F}$, и, следовательно, мы можем выбрать некоторый $Y \in \mathcal{F}$, такой, что $x \in Y$. Но тогда согласно лемме 4.6.8 $[x] = Y$. Таким образом, $X = Y \in \mathcal{F}$, поэтому $A/R \subseteq \mathcal{F}$.

Теперь предположим, что $X \in \mathcal{F}$. Тогда, поскольку \mathcal{F} – разбиение, $X \neq \emptyset$, мы можем выбрать некоторый $x \in X$. Следовательно, по лемме 4.6.8 $X = [x] \in A/R$, поэтому $\mathcal{F} \subseteq A/R$. Таким образом, $A/R = \mathcal{F}$.

Комментарий. Докажем, что $A/R = \mathcal{F}$, доказав, что $A/R \subseteq \mathcal{F}$ и $\mathcal{F} \subseteq A/R$. В качестве первого доказательства мы берем произвольный $X \in A/R$ и доказываем, что $X \in \mathcal{F}$. Поскольку $X \in A/R$ означает $\exists x \in A (X = [x])$, мы немедленно вводим новую переменную x для обозначения элемента A , такого что $X = [x]$. Доказательство того, что $x \in \mathcal{F}$, в данном случае следует слегка окольным путем нахождения множества $Y \in \mathcal{F}$, такого что $X = Y$. Это мотивировано леммой 4.5.8, которая предлагает способ показать, что элемент \mathcal{F} равен $[x] = X$. Доказательство того, что $\mathcal{F} \in A/R$, также опирается на лемму 4.5.8.

Вы уже видели, что отношение эквивалентности R на множестве A можно использовать для определения разбиения A/R множества A , а также что разбиение \mathcal{F} на A можно использовать для определения отношения эквивалентности $\bigcup_{X \in \mathcal{F}} (X \times X)$ на A . Доказательство теоремы 4.5.6 демонстрирует интересную связь между этими операциями. Если вы начнете с разбиения \mathcal{F} на A , воспользуетесь \mathcal{F} для определения отношения эквивалентности $R = \bigcup_{X \in \mathcal{F}} (X \times X)$, а затем используете R для определения разбиения A/R , то вы вернетесь туда, откуда начали. Другими словами, окончательное разбиение A/R такое же, как исходное разбиение \mathcal{F} . Вы можете задаться вопросом, сработает ли та же идея в обратном порядке. Другими словами, предположим, что вы начали с отношения эквивалентности R на A , использовали R для определения разбиения $\mathcal{F} = A/R$, а затем использовали \mathcal{F} для определения отношения эквивалентности $S = \bigcup_{X \in \mathcal{F}} (X \times X)$. Будет ли окончательное отношение эквивалентности S таким же, как исходное отношение эквивалентности R ? В упражнении 10 вам нужно показать, что это так.

В конце этого раздела мы рассмотрим еще несколько примеров отношений эквивалентности. Следующее определение описывает очень полезное семейство таких отношений.

Определение 4.5.9. Предположим, что m – натуральное число. Для любых целых чисел x и y мы будем говорить, что x конгруэнтно y по модулю m , если $\exists k \in \mathbb{Z} (x - y = km)$. Другими словами, x конгруэнтно y по модулю m тогда и только тогда, когда $m \mid (x - y)$. Мы будем использовать обозначение $x \equiv y \pmod{m}$, чтобы обозначать, что x конгруэнтно y по модулю m .

Например, $12 \equiv 27 \pmod{5}$, так как $12 - 27 = -15 = (-3) \cdot 5$. Теперь для любого натурального числа m мы можем рассмотреть соотношение $\{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \equiv y \pmod{m}\}$. Как мы упоминали в последнем разделе, математики иногда используют символы, а не буквы в качестве имен отношений. В этом случае, исходя из обозначений в определении 4.5.9, мы будем использовать символ \equiv_m в качестве названия этого отношения. Таким образом, для любых целых чисел x и y запись $x \equiv_m y$ означает то же, что $x \equiv y \pmod{m}$. Оказывается, это отношение является еще одним примером отношения эквивалентности.

Теорема 4.5.10. Для любого натурального числа m отношение \equiv_m является отношением эквивалентности на \mathbb{Z} .

Доказательство. Мы проверим транзитивность для \equiv_m и оставим вам проверку рефлексивности и симметрии в упражнении 11. Чтобы увидеть, что \equiv_m транзитивно, предположим, что $x \equiv_m y$ и $y \equiv_m z$. Это означает, что $x \equiv y \pmod{m}$ и $y \equiv z \pmod{m}$.

и $y \equiv z \pmod{m}$, или, другими словами, $m \mid (x - y)$ и $m \mid (y - z)$. Следовательно, согласно упражнению 18(а) раздела 3.3, $m \mid [(x - y) + (y - z)]$. Но $(x - y) + (y - z) = x - z$, поэтому $m \mid (x - z)$, а значит, $x \equiv_m z$.

Об этих отношениях эквивалентности мы еще поговорим позже в этой книге, особенно в главе 7.

Отношения эквивалентности часто возникают, когда мы хотим сгруппировать вместе элементы множества, которые имеют что-то общее. Например, если вы изучали векторы в предыдущем курсе математики или физики, то вам, возможно, сказали, что векторы можно рассматривать как стрелки. Но вам, вероятно, также сказали, что разные стрелки, указывающие в одном направлении и имеющие одинаковую длину, следует рассматривать как один и тот же вектор. Вот более строгое объяснение взаимосвязи между векторами и стрелками. Пусть A – множество всех стрелок, и пусть $R = \{(x, y) \in A \times A \mid$ стрелки x и y указывают в одном направлении и имеют одинаковую длину}. Мы предлагаем вам самостоятельно убедиться, что R является отношением эквивалентности на A . Каждый класс эквивалентности состоит из стрелок, которые имеют одинаковую длину и указывают в одном направлении. Теперь мы можем представлять векторы не стрелками, а классами эквивалентности стрелок.

Студентам, знакомым с компьютерным программированием, может быть интересен наш следующий пример. Предположим, мы обозначили за P множество всех компьютерных программ, и для любых компьютерных программ p и q мы говорим, что они эквивалентны, если они всегда производят один и тот же результат при одинаковом вводе. Пусть $R = \{(p, q) \in P \times P \mid$ программы p и q эквивалентны}. Нетрудно убедиться, что R является отношением эквивалентности на P . Классы эквивалентности группируют вместе программы, которые производят одинаковый результат при одинаковом вводе.

Упражнения

- *1. Найдите все разбиения множества $A = \{1, 2, 3\}$.
2. Найдите все отношения эквивалентности на множестве $A = \{1, 2, 3\}$.
- *3. Пусть W – множество всех слов английского языка. Какие из следующих отношений на W являются отношениями эквивалентности? Для тех из них, которые являются отношениями эквивалентности, каковы классы эквивалентности?
 - (a) $R = \{(x, y) \in W \times W \mid$ слова x и y начинаются с одной буквы}.
 - (b) $S = \{(x, y) \in W \times W \mid$ слова x и y имеют хотя бы одну общую букву}.
 - (c) $T = \{(x, y) \in W \times W \mid$ слова x и y имеют одинаковое количество букв}.
4. Какие из следующих отношений на \mathbb{R} являются отношениями эквивалентности? Каковы для них классы эквивалентности?
 - (a) $R = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x - y \in \mathbb{N}\}$.
 - (b) $S = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x - y \in \mathbb{Q}\}$.
 - (c) $T = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid \exists n \in \mathbb{Z} (y = x \cdot 10^n)\}$.

5. Пусть L – множество всех невертикальных прямых на плоскости. Какие из следующих отношений на L являются отношениями эквивалентности? Каковы для них классы эквивалентности?
- $R = \{(k, l) \in L \times L \mid$ прямые k и l имеют одинаковый наклон $\}$.
 - $S = \{(k, l) \in L \times L \mid$ прямые k и l перпендикулярны $\}$.
 - $T = \{(k, l) \in L \times L \mid k \cap x = l \cap x$ и $k \cap y = l \cap y\}$, где x и y – это ось x и ось y .
(Здесь мы рассматриваем прямые как множества точек.)
- *6. При обсуждении отношения эквивалентности B для одинакового дня рождения в соответствии с определением 4.5.3 мы утверждали, что $P/B = \{P_d \mid d \in D\}$. Приведите строгое доказательство этого утверждения. В ходе разработки доказательства вы обнаружите, что существует предположение, которое вы должны сделать о днях рождения людей (очень разумное предположение), чтобы доказательство сработало. Что это за предположение?
7. Пусть T – множество всех треугольников, и пусть $S = \{(s, t) \in T \times T \mid$ треугольники s и t подобны $\}$. (Напомним, что два треугольника подобны, если углы одного треугольника равны соответствующим углам другого.) Убедитесь, что S является отношением эквивалентности.
8. Завершите доказательство леммы 4.5.7.
9. Пусть R и S – отношения эквивалентности на A и $A/R = A/S$. Докажите, что $R = S$.
- *10. Предположим, что R – отношение эквивалентности на A . Пусть $\mathcal{F} = A/R$, и пусть S – отношение эквивалентности, определяемое \mathcal{F} . Другими словами, $S = \bigcup_{X \in \mathcal{F}} (X \times X)$. Докажите, что $S = R$.
11. Пусть \equiv_m будет отношением «конгруэнтность по модулю m », определенным выше, для положительного целого числа m .
 - Завершите доказательство теоремы 4.5.10, показав, что \equiv_m рефлексивно и симметрично.
 - Найдите все классы эквивалентности для \equiv_2 и \equiv_3 . Сколько классов эквивалентности существует в каждом случае? Как вы думаете, сколько в целом классов эквивалентности существует для \equiv_m ?
12. Докажите, что для любого целого n либо $n^2 \equiv 0 \pmod{4}$, либо $n^2 \equiv 1 \pmod{4}$.
- *13. Предположим, что m – натуральное число. Докажите, что для всех целых чисел a, a', b и b' если $a' \equiv a \pmod{m}$ и $b' \equiv b \pmod{m}$, то $a' + b' \equiv a + b \pmod{m}$ и $ab \equiv a'b' \pmod{m}$.
14. Предположим, что R – отношение эквивалентности на A и $B \subseteq A$. Пусть $S = R \cap (B \times B)$.
 - Докажите, что S – отношение эквивалентности на B .
 - Докажите, что для всех $x \in B$ истинно $[x]_S = [x]_R \cap B$.
15. Предположим, что $B \subseteq A$, и определим отношение R на $P(A)$ следующим образом:

$$R = \{(X, Y) \in P(A) \times P(A) \mid X \subseteq Y\}.$$

- (a) Докажите, что R – отношение эквивалентности на $\mathcal{P}(A)$.
 (b) Докажите, что для любого $X \in \mathcal{P}(A)$ существует ровно один $Y \in [X]_R$ такой, что $Y \cap B = \emptyset$.
- *16. Предположим, что \mathcal{F} – разбиение A , \mathcal{G} – разбиение B , а A и B не пересекаются. Докажите, что $\mathcal{F} \cup \mathcal{G}$ – разбиение $A \cup B$.
17. Предположим, что R – отношение эквивалентности на A , S – отношение эквивалентности на B , а A и B не пересекаются.
 (a) Докажите, что $R \cup S$ является отношением эквивалентности на $A \cup B$.
 (b) Докажите, что для всех $x \in A$ $[x]_{R \cup S} = [x]_R$ и для всех $y \in B$ $[y]_{R \cup S} = [y]_S$.
 (c) Докажите, что $(A \cup B)/(R \cup S) = (A/R) \cup (B/S)$.
18. Предположим, что \mathcal{F} и \mathcal{G} – разбиения множества A . Определим новое семейство множеств $\mathcal{F} \cdot \mathcal{G}$ следующим образом:
- $$\mathcal{F} \cdot \mathcal{G} = \{Z \in \mathcal{P}(A) \mid Z \neq \emptyset \text{ и } \exists X \in \mathcal{F} \exists Y \in \mathcal{G} (Z = X \cap Y)\}.$$
- Докажите, что $\mathcal{F} \cdot \mathcal{G}$ – разбиение A .
19. Пусть $\mathcal{F} = \{\mathbb{R}^-, \mathbb{R}^+, \{0\}\}$ и $\mathcal{G} = \{\mathbb{Z}, \mathbb{R} \setminus \mathbb{Z}\}$, и обратите внимание, что и \mathcal{F} , и \mathcal{G} являются разбиениями \mathbb{R} . Перечислите элементы $\mathcal{F} \cdot \mathcal{G}$ (см. в упражнении 18 значение используемых здесь обозначений).
- *20. Предположим, что R и S – отношения эквивалентности на множестве A . Пусть $T = R \cap S$.
 (a) Докажите, что T – отношение эквивалентности на A .
 (b) Докажите, что для всех $x \in A$, $[x]_T = [x]_R \cap [x]_S$.
 (c) Докажите, что $A/T = (A/R) \cdot (A/S)$. (Значение используемых здесь обозначений см. в упражнении 18.)
21. Пусть \mathcal{F} – разбиение A , а \mathcal{G} – разбиение B . Определим новое семейство множеств $\mathcal{F} \otimes \mathcal{G}$ следующим образом:
- $$\mathcal{F} \otimes \mathcal{G} = \{Z \in \mathcal{P}(A \times B) \mid \exists X \in \mathcal{F} \exists Y \in \mathcal{G} (Z = X \times Y)\}.$$
- Докажите, что $\mathcal{F} \otimes \mathcal{G}$ является разбиением $A \times B$.
- *22. Пусть $\mathcal{F} = \{\mathbb{R}^-, \mathbb{R}^+, \{0\}\}$, который является разбиением \mathbb{R} . Перечислите элементы $\mathcal{F} \otimes \mathcal{F}$ и опишите их геометрически как подмножества плоскости xy . (Значение используемых здесь обозначений см. в упражнении 21.)
23. Предположим, что R – отношение эквивалентности на A , а S – отношение эквивалентности на B . Определим отношение T на $A \times B$ следующим образом:
- $$T = \{((a, b), (a', b')) \in (A \times B) \times (A \times B) \mid aRa' \text{ и } bSb'\}.$$
- (a) Докажите, что T – отношение эквивалентности на $A \times B$.
 (b) Докажите, что если $a \in A$ и $b \in B$, то $[(a, b)]_T = [a]_R \times [b]_S$.
 (c) Докажите, что $(A \times B)/T = (A/R) \otimes (B/S)$. (Значение используемых здесь обозначений см. в упражнении 21.)

- *24. Предположим, что R и S – отношения на множестве A , а S – отношение эквивалентности. Мы будем говорить, что R совместимо с S , если для всех x, y, x' и y' в A , если xSx' и ySy' , то xRy , если и только если $x'Ry'$.
- Докажите, что если R совместимо с S , то существует единственное отношение T на A/S такое, что для всех x и y в A $[x]_S T [y]_S$ тогда и только тогда, когда xRy .
 - Предположим, что T – отношение на A/S и для всех x и y в A $[x]_S T [y]_S$ тогда и только тогда, когда xRy . Докажите, что R совместимо с S .
25. Пусть R – отношение на A и R рефлексивно и транзитивно. (Такое отношение называется *предпорядком* на A .) Пусть $S = R \cap R^{-1}$.
- Докажите, что S – отношение эквивалентности на A .
 - Докажите, что существует единственное отношение T на A/S такое, что для всех x и y в A $[x]_S T [y]_S$ тогда и только тогда, когда xRy . (Подсказка: используйте упражнение 24.)
 - Докажите, что T – частичный порядок на A/S , где T – отношение из части (b).
26. Пусть $I = \{1, 2, \dots, 100\}$, $A = \mathcal{P}(I)$ и $R = \{(X, Y) \in A \times A \mid Y$ имеет как минимум столько же элементов, сколько $X\}$.
- Докажите, что R является предпорядком на A . (См. определение предпорядка в упражнении 25.)
 - Пусть S и T определены, как в упражнении 25. Опишите элементы A/S и частичный порядок T . Сколько элементов в A/S ? Это полный порядок?
27. Предположим, что A – множество. Если \mathcal{F} и \mathcal{G} являются разбиениями A , то мы говорим, что \mathcal{F} уточняет \mathcal{G} , если $\forall X \in \mathcal{F} \exists Y \in \mathcal{G} (X \subseteq Y)$. Пусть P – множество всех разбиений A , и пусть $R = \{(\mathcal{F}, \mathcal{G}) \in P \times P \mid \mathcal{F}$ уточняет $\mathcal{G}\}$.
- Докажите, что R – частичный порядок на P .
 - Предположим, что S и T – отношения эквивалентности на A . Пусть $\mathcal{F} = A/S$ и $\mathcal{G} = A/T$. Докажите, что $S \subseteq T$ тогда и только тогда, когда \mathcal{F} уточняет \mathcal{G} .
 - Предположим, что \mathcal{F} и \mathcal{G} – разбиения A . Докажите, что $\mathcal{F} \cdot \mathcal{G}$ – наибольшая нижняя граница множества $\{\mathcal{F}, \mathcal{G}\}$ в частичном порядке R . (Значение используемых здесь обозначений см. в упражнении 18.)

Глава 5

ФУНКЦИИ

5.1. ОПРЕДЕЛЕНИЕ ФУНКЦИИ

Предположим, что P – это множество всех людей, и пусть $H = \{(p, n) \in P \times \mathbb{N} \mid$ у человека p есть n детей}. Тогда H является отношением из P в \mathbb{N} и обладает следующим важным свойством. Для каждого $p \in P$ существует ровно одно $n \in \mathbb{N}$ такое, что $(p, n) \in H$. Математики выражают эту идею, говоря, что H является функцией от P к \mathbb{N} .

Определение 5.1.1. Предположим, что F является отношением из A в B . Тогда F называется функцией от A к B , если для каждого $a \in A$ существует ровно одно значение $b \in B$ такое, что $(a, b) \in F$. Другими словами, утверждение, что F является функцией от A к B , означает:

$$\forall a \in A \exists! b \in B((a, b) \in F).$$

Чтобы указать, что F является функцией от A к B , мы будем писать $F: A \rightarrow B$.

Пример 5.1.2

- Пусть $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$ и $F = \{(1, 5), (2, 4), (3, 5)\}$. Является ли F функцией от A к B ?
- Пусть $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$ и $G = \{(1, 5), (2, 4), (1, 6)\}$. Является ли G функцией от A к B ?
- Пусть C – множество всех городов, а N – множество всех стран, и пусть $L = \{(c, n) \in C \times N \mid$ город c находится в стране $n\}$. Является ли L функцией от C к N ?
- Пусть P – множество всех людей, и пусть $C = \{(p, q) \in P \times P \mid$ человек p является родителем человека $q\}$. Является ли C функцией от P к P ?
- Пусть P – множество всех людей, и пусть $D = \{(p, x) \in P \times \mathcal{P}(P) \mid x =$ множество всех дочерних элементов $p\}$. Является ли D функцией от P к $\mathcal{P}(P)$?
- Пусть A – произвольное множество. Напомним, что $i_A = \{(a, a) \mid a \in A\}$ называется отношением тождества на A . Является ли оно функцией от A к A ?
- Пусть $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = x^2\}$. Является ли f функцией от \mathbb{R} к \mathbb{R} ?

Решения

1. Да. Обратите внимание, что элемент 1 связан отношением F с элементом 5 и больше ни с каким другим элементом B . Точно так же 2 связан только с 4, а 3 с 5. Другими словами, каждый элемент A фигурирует как первая координата ровно одной упорядоченной пары в F . Следовательно, F является функцией от A к B . Обратите внимание, что определение функции *не* требует, чтобы *каждый* элемент B составлял пару ровно с одним элементом A . Поэтому не имеет значения, что 5 встречается как вторая координата двух разных пар в F , а 6 вообще не встречается ни в одной упорядоченной паре.
2. Нет. G нельзя назвать функцией от A к B по двум причинам. Во-первых, элемент 3 не образует пару ни с одним элементом B в отношении G , что нарушает требование, чтобы каждый элемент A был сопоставлен с некоторым элементом B . Во-вторых, элемент 1 образует пару с двумя разными элементами B (5 и 6), что нарушает требование, чтобы каждый элемент A входил в пару *только с одним* элементом B .
3. Если мы сделаем разумное предположение, что каждый город находится ровно в одной стране, то L будет функцией от C к N .
4. Поскольку у некоторых людей нет детей, а у некоторых есть более одного ребенка, C не является функцией от P к P .
5. Да, D – это функция от P к $\mathcal{P}(P)$. Каждому человеку p соответствует ровно одно множество $x \subseteq P$, а именно множество всех дочерних элементов p . Обратите внимание, что в отношении D человек p связан с *множеством*, состоящим из всех детей p , а *не* с самими детьми. Даже если p не имеет ровно одного дочернего элемента, все же верно, что существует ровно одно множество, которое содержит в точности дочерние элементы p и ничего больше.
6. Да. Каждый $a \in A$ связан в отношении i_A ровно с одним элементом A , а именно с самим a . Другими словами, $(a, a) \in i_A$, но для любого $a' \neq a$ истинно $(a, a') \notin i_A$. Следовательно, мы можем назвать i_A функцией тождества на A .
7. Да. Для каждого действительного числа x существует ровно одно значение y , а именно $y = x^2$, такое, что $(x, y) \in f$.

Пусть $f: A \rightarrow B$. Если $a \in A$, то мы знаем, что существует ровно один элемент $b \in B$ такой, что $(a, b) \in f$. Этот уникальный элемент b называется «значением f в точке a », или «отображением точки a относительно f », или «результатом применения f к a », или просто « f от a », и записывается как $f(a)$. Другими словами, для любых $a \in A$ и $b \in B$ утверждение $b = f(a)$ истинно тогда и только тогда, когда $(a, b) \in f$. Например, для функции $F = \{(1, 5), (2, 4), (3, 5)\}$ из п. 1 примера 5.1.2 мы могли бы сказать, что $F(1) = 5$, поскольку $(1, 5) \in F$. Аналогично, $F(2) = 4$ и $F(3) = 5$. Если L – функция из п. 3, а c – любой город, то $L(c)$ будет единственной страной n такой, что $(c, n) \in L$. Другими словами, $L(c) =$ страна, в которой находится c . Например, $L(\text{Париж}) = \text{Франция}$. Для функции D из части 5 мы могли бы сказать, что для любого человека p истинно утверждение, что $D(p) =$ множество всех дочерних элементов p . Если A – любое множество и $a \in A$, то $(a, a) \in i_A$, поэтому $i_A(a) = a$. И если f – функция из п. 7, то для любого действительного числа x справедливо равенство $f(x) = x^2$.

Функция f по множеству A на другом множестве B часто задается правилом, которое можно использовать для определения $f(a)$ для любого $a \in A$. Например, если A – это множество всех людей и $B = \mathbb{R}^+$, тогда мы могли бы определить функцию f от A к B по правилу, что для каждого $a \in A$ справедливо равенство $f(a) =$ высота a в дюймах. Хотя это определение не говорит явно, какие упорядоченные пары являются элементами f , мы можем установить это, используя наше правило, что для всех $a \in A$ и $b \in B$ утверждение $(a, b) \in f$ истинно тогда и только тогда, когда $b = f(a)$. Таким образом:

$$\begin{aligned}f &= \{(a, b) \in A \times B \mid (b = f(a))\} \\&= \{(a, b) \in A \times B \mid b = \text{высота } a \text{ в дюймах}\}.\end{aligned}$$

Например, если рост Джо Смита 68 дюймов, то $(\text{Джо Смит}, 68) \in f$ и $f(\text{Джо Смит}) = 68$.

Пример 5.1.3. Вот еще несколько примеров функций, определенных при помощи правил.

- Предположим, каждому студенту назначен научный руководитель, который является профессором. Пусть S – множество студентов, а P – множество профессоров. Тогда мы можем определить функцию f от S к P по правилу, что для каждого студента s имеется $f(s) =$ руководитель s . Другими словами:

$$\begin{aligned}f &= \{(s, p) \in S \times P \mid p = f(s)\} \\&= \{(s, p) \in S \times P \mid \text{профессор } p \text{ является научным руководителем} \\&\quad \text{студента } s\}.\end{aligned}$$

- Мы можем определить функцию g от \mathbb{Z} к \mathbb{R} по правилу, что для любого $x \in \mathbb{Z}$ $g(x) = 2x + 3$. Тогда

$$\begin{aligned}g &= \{(x, y) \in \mathbb{Z} \times \mathbb{R} \mid y = g(x)\} \\&= \{(x, y) \in \mathbb{Z} \times \mathbb{R} \mid y = 2x + 3\} \\&= \{\dots, (-2, -1), (-1, 1), (0, 3), (1, 5), (2, 7), \dots\}.\end{aligned}$$

- Пусть h – функция от \mathbb{R} к \mathbb{R} , определенная правилом, что для каждого $x \in \mathbb{R}$, $h(x) = 2x + 3$. Обратите внимание, что формула для $h(x)$ такая же, как формула для $g(x)$ в п. 2. Однако h и g – разные функции. Вы можете убедиться в этом, заметив, что, например, $(\pi, 2\pi + 3) \in h$, но $(\pi, 2\pi + 3) \notin g$, поскольку $\pi \notin \mathbb{Z}$. Подробнее о взаимосвязи между g и h см. упражнение 7(с).

Обратите внимание, что когда функция f от A к B задается правилом нахождения $f(a)$, оно должно определять значение $f(a)$ для *каждого* $a \in A$. Иногда, когда математики формулируют такое правило, они не говорят явно, что правило применяется ко всем $a \in A$. Например, математик мог бы сказать: «пусть f будет функцией от \mathbb{R} к \mathbb{R} , определенной формулой $f(x) = x^2 + 7$ ». В этом случае понятно, что уравнение $f(x) = x^2 + 7$ применимо ко всем $x \in \mathbb{R}$, даже если об этом не было сказано явно. Это означает, что вы можете подставить любое действительное число для x в это уравнение, и полученное

уравнение будет истинным. Например, вы можете сделать вывод, что $f(3) = 3^2 + 7 = 16$. Аналогично, если w – действительное число, вы можете написать $f(w) = w^2 + 7$ или даже $f(2w - 3) = (2w - 3)^2 + 7 = 4w^2 - 12w + 16$.

Поскольку функция f от A к B полностью определяется правилом нахождения $f(a)$, две функции, определенные эквивалентными правилами, должны совпадать. Точнее, мы имеем следующую теорему.

Теорема 5.1.4. *Предположим, что f и g – функции от A к B . Если $\forall a \in A(f(a) = g(a))$, то $f = g$.*

Доказательство. Предположим, что $\forall a \in A(f(a) = g(a))$, и пусть (a, b) – произвольный элемент f . Тогда $b = f(a)$. Но по нашему предположению $f(a) = g(a)$, поэтому $b = g(a)$ и, следовательно, $(a, b) \in g$. Таким образом, $f \subseteq g$. Аналогичное рассуждение показывает, что $g \subseteq f$, поэтому $f = g$.

Комментарий. Поскольку f и g – множества, мы докажем, что $f = g$, показав, что $f \subseteq g$ и $g \subseteq f$. Для каждой из этих целей мы в качестве доказательства показываем, что произвольный элемент одного множества должен быть элементом другого. Обратите внимание, что теперь, когда мы доказали теорему 5.1.4, у нас есть другой метод доказательства равенства двух функций f и g от множества A к другому множеству B . В будущем для доказательства $f = g$ мы обычно будем доказывать $\forall a \in A(f(a) = g(a))$, а затем применять теорему 5.1.4.

Поскольку функции – это просто отношения особого типа, концепции, представленные в главе 4 для отношений, могут быть применены и к функциям. Например, предположим, что $f: A \rightarrow B$. Тогда f является отношением из A в B , поэтому имеет смысл говорить об области определения f , которая является подмножеством A , и диапазоне значений f , который является подмножеством B . Согласно определению функции, каждый элемент A должен фигурировать как первая координата некоторой (фактически ровно одной) упорядоченной пары в f , поэтому область определения f фактически полностью перекрывает A . Но диапазон значений f не обязательно должен полностью охватывать B . Элементы диапазона f будут вторыми координатами всех упорядоченных пар в f , а вторая координата упорядоченной пары в f – это то, что мы назвали отображением ее первой координаты. Таким образом, диапазон f можно также описать как множество всех отображений элементов A через f :

$$\text{Ran}(f) = \{f(a) \mid a \in A\}.$$

Например, для функции f , определенной в части 1 примера 5.1.3, $\text{Ran}(f) = \{f(s) \mid s \in S\}$ – множество всех руководителей студентов.

Мы можем рисовать диаграммы функций точно так же, как рисовали диаграммы отношений в главе 4. Если $f: A \rightarrow B$, то, как и раньше, каждая упорядоченная пара $(a, b) \in f$ будет представлена на диаграмме ребром, соединяющим a с b . По определению функции каждый элемент $a \in A$ встречается как первая координата ровно одной упорядоченной пары в f , а вторая координата этой упорядоченной пары – $f(a)$. Таким образом, для каждого $a \in A$ будет существовать ровно одно ребро, выходящее из a , и оно будет соединять a

с $f(a)$. Например, на рис. 5.1 показано, как будет выглядеть диаграмма для функции L , определенной в п. 3 примера 5.1.2.

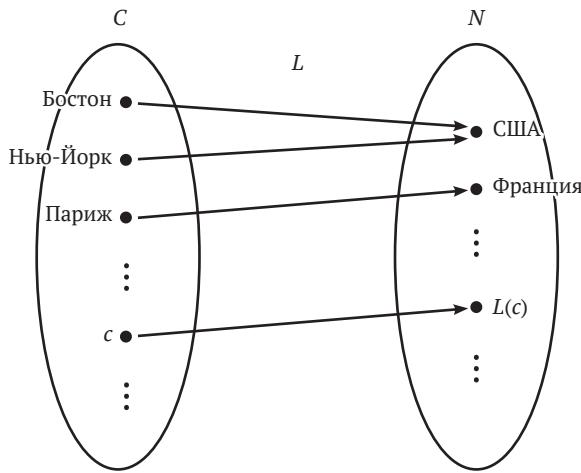


Рис. 5.1 ♦ Диаграмма связей для функции L , определенной в п. 3 примера 5.1.2

Определение композиции отношений также применимо и к функциям. Если $f: A \rightarrow B$ и $g: B \rightarrow C$, при этом f – отношение из A в B , а g – отношение из B в C , поэтому $g \circ f$ будет отношением из A в C . Оказывается, $g \circ f$ является функцией от A к C , как показывает следующая теорема.

Теорема 5.1.5. Предположим, что $f: A \rightarrow B$ и $g: B \rightarrow C$. Тогда $g \circ f: A \rightarrow C$, и для любого $a \in A$ значение $g \circ f$ в точке a определяется формулой $(g \circ f)(a) = g(f(a))$.

Стратегия доказательства

Перед тем как доказывать эту теорему, было бы полезно обсудить стратегию доказательства. Согласно определению функции, чтобы показать, что $g \circ f: A \rightarrow C$, мы должны доказать, что $\forall a \in A \exists! c \in C ((a, c) \in g \circ f)$, поэтому мы начнем с того, что обозначим за a произвольный элемент из A , а затем попытаемся доказать, что $\exists! c \in C ((a, c) \in g \circ f)$. Как мы показали в разделе 3.6, мы можем доказать это утверждение, отдельно доказывая существование и единственность. Чтобы доказать существование, мы должны попытаться найти $c \in C$ такое, что $(a, c) \in g \circ f$. Для доказательства единственности следует предположить, что $(a, c_1) \in g \circ f$ и $(a, c_2) \in g \circ f$, а затем попытаться доказать, что $c_1 = c_2$.

Доказательство. Пусть a – произвольный элемент из A . Мы должны показать, что существует единственный элемент $c \in C$ такой, что $(a, c) \in g \circ f$.

Существование: пусть $b = f(a) \in B$. Пусть $c = g(b) \in C$. Тогда $(a, b) \in f$ и $(b, c) \in g$, поэтому по определению композиции отношений $(a, c) \in g \circ f$. Следовательно, $\exists c \in C((a, c) \in g \circ f)$.

Единственность. Пусть $(a, c_1) \in g \circ f$ и $(a, c_2) \in g \circ f$. Тогда по определению композиции мы можем выбрать элемент $b_1 \in B$ такой, чтобы $(a, b_1) \in f$ и $(b_1, c_1) \in g$, и мы также можем выбрать $b_2 \in B$ такой, чтобы $(a, b_2) \in f$ и $(b_2, c_2) \in g$. Поскольку f – функция, может быть только один элемент $b \in B$ такой, что $(a, b) \in f$. Таким образом, поскольку (a, b_1) и (a, b_2) являются элементами f , отсюда следует, что $b_1 = b_2$. Применяя аналогичные рассуждения к g , поскольку $(b_1, c_1) \in g$ и $(b_1, c_2) = (b_2, c_2) \in g$, приходим к выводу, что $c_1 = c_2$, что и требовалось доказать.

Этот вывод завершает доказательство того, что $g \circ f$ является функцией от A к C . Наконец, чтобы вывести формулу для $(g \circ f)(a)$, вспомните, что в доказательстве существования мы показали, что для любого $a \in A$ если принять $b = f(a)$ и $c = g(b)$, то $(a, c) \in g \circ f$. Таким образом:

$$(g \circ f)(a) = c = g(b) = g(f(a)).$$

Когда мы впервые представили идею композиции двух отношений в главе 4, то отметили определенное своеобразие обозначений и пообещали объяснить причину этого позже. Теперь мы можем дать это объяснение. Обозначения, которые мы использовали для композиции соотношений, объясняются тем, что они приводят к удобной формуле $(g \circ f)(x) = g(f(x))$, полученной в теореме 5.1.5. Обратите внимание: поскольку функции – это просто отношения особого типа, все, что мы доказали относительно композиции отношений, применимо к композиции функций. В частности, из теоремы 4.2.5 мы знаем, что композиция функций ассоциативна.

Пример 5.1.6. Вот несколько примеров композиций функций.

- Пусть C и N – множества всех городов и стран соответственно, и пусть $L: C \rightarrow N$ – функция, определенная в п. 3 примера 5.1.2. Таким образом, для каждого города c запись $L(c)$ означает страну, в которой находится c . Пусть B будет множеством всех зданий, расположенных в городах. Определим $F: B \rightarrow C$ по формуле $F(b) =$ город, в котором находится здание b . Тогда $L \circ F: B \rightarrow N$. Например, $F(\text{Эйфелева башня}) = \text{Париж}$, поэтому согласно формуле, полученной в теореме 5.1.5:

$$(L \circ F)(\text{Эйфелева башня}) = L(F(\text{Эйфелева башня})) = L(\text{Париж}) = \text{Франция}.$$

В целом для каждого здания $b \in B$:

$$\begin{aligned} (L \circ F)(b) &= L(F(b)) = L(\text{город, в котором находится } b) \\ &= \text{страна, в которой находится } b. \end{aligned}$$

Эта функция представлена схематически на рис. 5.2.

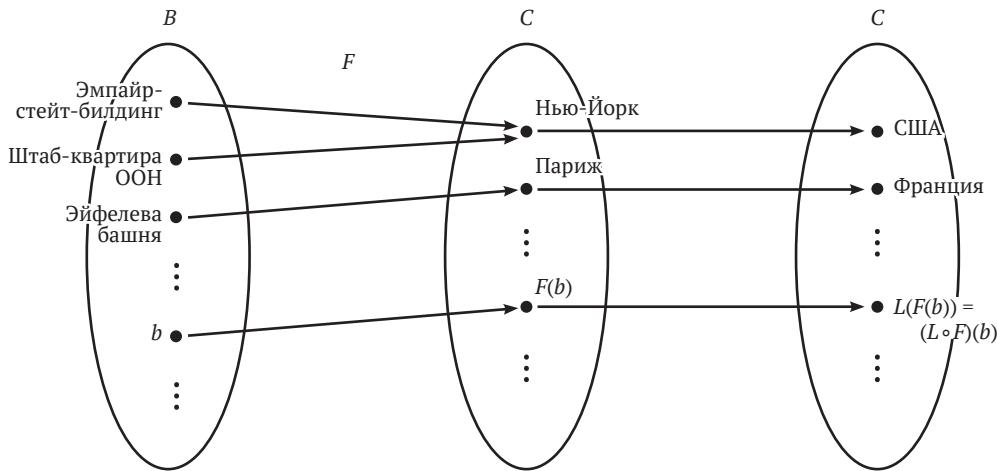


Рис. 5.2 ♦ Схематическое представление функции $(L \circ F)(b) = L(F(b)) = L(\text{город, в котором находится } b) = \text{страна, в которой находится } b$

2. Пусть $g: \mathbb{Z} \rightarrow \mathbb{R}$ – функция из п. 2 примера 5.1.3, которая была определена формулой $g(x) = 2x + 3$. Пусть $f: \mathbb{Z} \rightarrow \mathbb{Z}$ определяется формулой $f(n) = n^2 - 3n + 1$. Тогда $g \circ f: \mathbb{Z} \rightarrow \mathbb{R}$. Например, $f(2) = 2^2 - 3 \cdot 2 + 1 = -1$, поэтому $(g \circ f)(2) = g(f(2)) = g(-1) = 1$. В общем случае для любого $n \in \mathbb{Z}$

$$(g \circ f)(n) = g(f(n)) = g(n^2 - 3n + 1) = 2(n^2 - 3n + 1) + 3 = 2n^2 - 6n + 5.$$

Упражнения

- *1. (a) Пусть $A = \{1, 2, 3\}$, $B = \{4\}$ и $f = \{(1, 4), (2, 4), (3, 4)\}$. Является ли f функцией от A к B ?
- (b) Пусть $A = \{1\}$, $B = \{2, 3, 4\}$ и $f = \{(1, 2), (1, 3), (1, 4)\}$. Является ли f функцией от A до B ?
- (c) Пусть C будет множеством всех автомобилей, зарегистрированных в вашем регионе, и пусть S будет множеством всех конечных последовательностей букв и цифр. Пусть $L = \{(c, s) \in C \times S \mid \text{номерной знак автомобиля } c - \text{ это } s\}$. Является ли L функцией от C к S ?
- 2. (a) Пусть f – отношение, представленное графом на рис. 5.3. Является ли f функцией от A к B ?
- (b) Пусть W – множество всех слов английского языка, и пусть A – множество всех букв алфавита. Пусть $f = \{(w, a) \in W \times A \mid \text{буква } a \text{ встречается в слове } w\}$, и пусть $g = \{(w, a) \in W \times A \mid \text{буква } a \text{ является первой буквой слова } w\}$. Является ли f функцией от W к A ? Что вы можете сказать про g ?
- (c) Джон, Мэри, Сьюзен и Фред идут обедать и садятся за круглый стол. Пусть $P = \{\text{Джон, Мэри, Сьюзен, Фред}\}$, и пусть $R = \{(p, q) \in P \times P \mid \text{человек } p \text{ сидит сразу справа от человека } q\}$. Является ли R функцией от P к P ?

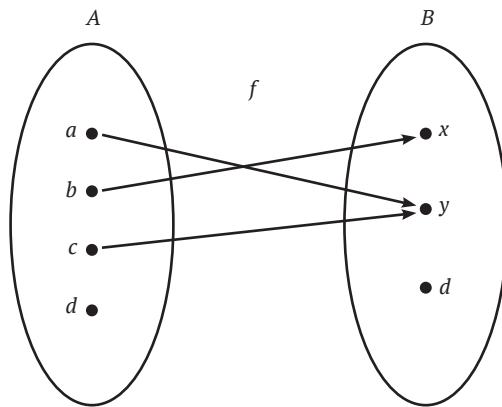


Рис. 5.3 ♦ Пример отношения между множествами

- *3. (a) Пусть $A = \{a, b, c\}$, $B = \{a, b\}$ и $f = \{(a, b), (b, b), (c, a)\}$. Тогда $f: A \rightarrow B$. Что вы можете сказать про $f(a)$, $f(b)$ и $f(c)$?
 - (b) Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ – функция, определяемая формулой $f(x) = x^2 - 2x$. Чему равно $f(2)$?
 - (c) Пусть $f = \{(x, n) \in \mathbb{R} \times \mathbb{Z} \mid n \leq x < n + 1\}$. Тогда $f: \mathbb{R} \rightarrow \mathbb{Z}$. Чему равно $f(\pi)$? Чему равно $f(-\pi)$?
4. (a) Пусть N – это множество всех стран, а C – множество всех городов. Пусть $H: N \rightarrow C$ – функция, определяемая правилом, согласно которому для каждой страны n запись $H(n)$ означает столицу страны n . Чему равняется $H(\text{Италия})$?
- (b) Пусть $A = \{1, 2, 3\}$ и $B = \mathcal{P}(A)$. Пусть $F: B \rightarrow B$ – функция, определяемая формулой $F(X) = A \setminus X$. Чему равняется $F(\{1, 3\})$?
- (c) Пусть $f: \mathbb{R} \rightarrow \mathbb{R} \times \mathbb{R}$ – функция, определенная формулой $f(x) = (x + 1, x - 1)$. Чему равняется $f(2)$?
- *5. Пусть L – функция, определенная в п. 3 примера 5.1.2, и пусть H – функция, определенная в упражнении 4(а). Напишите формулы для $L \circ H$ и $H \circ L$.
6. Пусть f и g – функции от \mathbb{R} к \mathbb{R} , определенные следующими формулами:

$$f(x) = \frac{1}{x^2 + 2}, \quad g(x) = 2x - 1.$$

Найдите формулы для $(f \circ g)(x)$ и $(g \circ f)(x)$.

- *7. Пусть $f: A \rightarrow B$ и $C \subseteq A$. Множество $f \cap (C \times B)$, которое является отношением из C в B , называется *ограничением* f на C и иногда обозначается $f \upharpoonright C$. Другими словами:

$$f \upharpoonright C = f \cap (C \times B).$$

- (а) Докажите, что $f \upharpoonright C$ является функцией от C к B и что для всех $c \in C$ справедливо равенство $f(c) = (f \upharpoonright C)(c)$.

- (b) Предположим, что $g: C \rightarrow B$. Докажите, что $g = f \upharpoonright C$ тогда и только тогда, когда $g \sqsubseteq f$.
- (c) Пусть g и h – функции, определенные в п. 2 и 3 примера 5.1.3. Покажите, что $g = h \upharpoonright \mathbb{Z}$.
8. Предположим, что $f: A \rightarrow B$ и $g \sqsubseteq f$. Докажите, что существует множество $A' \subseteq A$ такое, что $g: A' \rightarrow B$.
9. Предположим, что $f: A \rightarrow B$, $B \neq \emptyset$ и $A \subseteq A'$. Докажите, что существует функция $g: A' \rightarrow B$ такая, что $f \sqsubseteq g$.
- *10. Предположим, что f и g – функции от A до B и $f = g$. Покажите, что fg не является функцией.
11. Предположим, что A – множество. Покажите, что i_A – единственное отношение на A , которое одновременно является отношением эквивалентности на A , а также является функцией от A к A .
12. Предположим, что $f: A \rightarrow C$ и $g: B \rightarrow C$.
- Докажите, что если A и B не пересекаются, то $f \cup g: A \cup B \rightarrow C$.
 - Докажите, что $f \cup g: A \cup B \rightarrow C$ тогда и только тогда, когда $f \upharpoonright (A \cap B) = g \upharpoonright (A \cap B)$. (Пояснение к символу \upharpoonright см. в упражнении 7.)
- *13. Предположим, что R – это отношение от A к B , S – это отношение от B к C , $\text{Ran}(R) = \text{Dom}(S) = B$ и $S \circ R: A \rightarrow C$.
- Докажите, что $S: B \rightarrow C$.
 - Приведите пример, подтверждающий, что $R: A \rightarrow B$.
14. Предположим, что $f: A \rightarrow B$ и S – отношение на B . Определим отношение R на A следующим образом:
- $$R = \{(x, y) \in A \times A \mid (f(x), f(y)) \in S\}.$$
- Докажите, что если S рефлексивно, то и R тоже.
 - Докажите, что если S симметрично, то и R тоже.
 - Докажите, что если S транзитивно, то и R тоже.
- *15. Предположим, что $f: A \rightarrow B$ и R – отношение на A . Определим отношение S на B следующим образом:
- $$S = \{(x, y) \in B \times B \mid \exists u \in A \exists v \in A (f(u) = x \wedge f(v) = y \wedge (u, v) \in R)\}.$$
- Обоснуйте свои ответы на следующие вопросы либо доказательствами, либо контрпримерами.
- Если R рефлексивно, должно ли S быть рефлексивным?
 - Если R симметрично, должно ли S быть симметричным?
 - Если R транзитивно, должно ли S быть транзитивным?
16. Предположим, что A и B – множества, и пусть $\mathcal{F} = \{f \mid f: A \rightarrow B\}$. Также предположим, что R является отношением на B , и определим отношение S на \mathcal{F} следующим образом:
- $$S = \{(f, g) \in \mathcal{F} \times \mathcal{F} \mid \forall x \in A ((f(x), g(x)) \in R)\}.$$

Обоснуйте свои ответы на следующие вопросы либо доказательствами, либо контрпримерами.

- (а) Если R рефлексивно, должно ли S быть рефлексивным?
- (б) Если R симметрично, должно ли S быть симметричным?
- (с) Если R транзитивно, должно ли S быть транзитивным?

17. Пусть A – непустое множество и $f: A \rightarrow A$.

- (а) Предположим, что существует $a \in A$ такое, что $\forall x \in A (f(x) = a)$. (В этом случае f называется *постоянной* функцией.) Докажите, что для всех $g: A \rightarrow A$ справедливо $f \circ g = f$.
- (б) Предположим, что для всех $g: A \rightarrow A$ справедливо $f \circ g = f$. Докажите, что f – постоянная функция. (Подсказка: что будет, если g – постоянная функция?)

18. Пусть $\mathcal{F} = \{f \mid f: \mathbb{R} \rightarrow \mathbb{R}\}$. Пусть $R = \{(f, g) \in \mathcal{F} \times \mathcal{F} \mid \exists a \in \mathbb{R} \forall x > a (f(x) = g(x))\}$.

- (а) Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ и $g: \mathbb{R} \rightarrow \mathbb{R}$ – функции, определенные формулами $f(x) = |x|$ и $g(x) = x$. Покажите, что $(f, g) \in R$.
- (б) Докажите, что R – отношение эквивалентности.

*19. Пусть $\mathcal{F} = \{f \mid f: \mathbb{Z}^+ \rightarrow \mathbb{R}\}$. Для $g \in \mathcal{F}$ определим множество $O(g)$ следующим образом:

$$O(g) = \{f \in \mathcal{F} \mid \exists a \in \mathbb{Z}^+ \exists c \in \mathbb{R}^+ \forall x > a (|f(x)| \leq c|g(x)|)\}.$$

(Если $f \in O(g)$, математики говорят, что « f является асимптотой g »).

- (а) Пусть $f: \mathbb{Z}^+ \rightarrow \mathbb{R}$ и $g: \mathbb{Z}^+ \rightarrow \mathbb{R}$ определены формулами $f(x) = 7x + 3$ и $g(x) = x^2$. Докажите, что $f \in O(g)$, но $g \notin O(f)$.
- (б) Пусть $S = \{(f, g) \in \mathcal{F} \times \mathcal{F} \mid f \in O(g)\}$. Докажите, что S предварительный, но не частичный порядок. (См. определение предварительного порядка в упражнении 25 раздела 4.5.)
- (с) Предположим, что $f_1 \in O(g)$ и $f_2 \in O(g)$, а s и t – действительные числа. Определим функцию $f: \mathbb{Z}^+ \rightarrow \mathbb{R}$ формулой $f(x) = sf_1(x) + tf_2(x)$. Докажите, что $f \in O(g)$. (Подсказка: вам может пригодиться неравенство треугольника. См. упражнение 13(с) раздела 3.5.)

20. (а) Предположим, что $g: A \rightarrow B$ и $R = \{(x, y) \in A \times A \mid g(x) = g(y)\}$.

Покажите, что R – отношение эквивалентности на A .

- (б) Предположим, что R – отношение эквивалентности на A , и пусть $g: A \rightarrow A/R$ – функция, определенная формулой $g(x) = [x]_R$. Покажите, что $R = \{(x, y) \in A \times A \mid g(x) = g(y)\}$.

*21. Предположим, что $f: A \rightarrow B$ и R – отношение эквивалентности на A . Мы будем говорить, что f называется *совместной* с R , если $\forall x \in A \forall y \in A (xRy \rightarrow f(x) = f(y))$. (Вы можете сравнить это упражнение с упражнением 24 из раздела 4.5.)

- (а) Предположим, что f совместна с R . Докажите, что существует единственная функция $h: A/R \rightarrow B$ такая, что для всех $x \in A$ справедливо $h([x]_R) = f(x)$.
- (б) Предположим, что $h: A/R \rightarrow B$ и для всех $x \in A$ справедливо $h([x]_R) = f(x)$. Докажите, что f совместна с R .

22. Пусть $R = \{(x, y) \in \mathbb{N} \times \mathbb{N} \mid x \equiv y_{(\text{mod } 5)}\}$. Обратите внимание, что по теореме 4.5.10 и упражнению 14 из раздела 4.5 R является отношением эквивалентности на \mathbb{N} .
- Докажите, что существует единственная функция $h: \mathbb{N}/R \rightarrow \mathbb{N}/R$ такая, что для любого натурального числа x справедливо $h([x]_R) = [x^2]_R$. (Подсказка: используйте упражнение 21.)
 - Покажите, что не существует такой функции $h: \mathbb{N}/R \rightarrow \mathbb{N}/R$, что для любого натурального числа x справедливо $h([x]_R) = [2^x]_R$.

5.2. Однозначность и сюръективность

В последнем разделе мы видели, что композиция двух функций тоже является функцией. А как насчет обратных функций? Если $f: A \rightarrow B$, то f^{-1} является отношением из B в A , поэтому f^{-1} является отношением из B в A . Но является ли это отношение функцией от B к A ? Мы ответим на этот вопрос в следующем разделе. Как мы увидим, ответ зависит от следующих двух свойств функций.

Определение 5.2.1. Предположим, что $f: A \rightarrow B$. Мы будем говорить, что f *взаимно однозначна* (one-to-one), если

$$\neg \exists a_1 \in A \exists a_2 \in A (f(a_1) = f(a_2) \wedge a_1 \neq a_2).$$

Мы говорим, что f *отображается на* B (или просто *отображается*, если B ясно из контекста), если

$$\forall b \in B \exists a \in A (f(a) = b).$$

Первые функции иногда также называют *инъекциями*, а вторые – *сюръекциями*.

Обратите внимание, что наше определение взаимной однозначности начинается с символа отрицания \neg . Другими словами, когда мы говорим, что f взаимно однозначна, мы подразумеваем, что определенной ситуации *не* возникает. Ситуация, которая *не* должна возникать, заключается в том, что существует два разных элемента области определения f , a_1 и a_2 , таких, что $f(a_1) = f(a_2)$. Эта ситуация проиллюстрирована на рис. 5.4(a). Таким образом, функция на рис. 5.4(a) не взаимно однозначна. Рисунок 5.4(b) показывает взаимно однозначную функцию.

Если $f: A \rightarrow B$, то утверждение что f сюръективна, означает, что каждый элемент B является отображением некоторого элемента A посредством f . Другими словами, на диаграмме f каждый элемент B имеет указывающее на него ребро. Ни одна из функций на рис. 5.4 не сюръективна, потому что в обоих случаях есть элементы B без ребер, указывающих на них. На рис. 5.5 показаны две сюръективные функции.

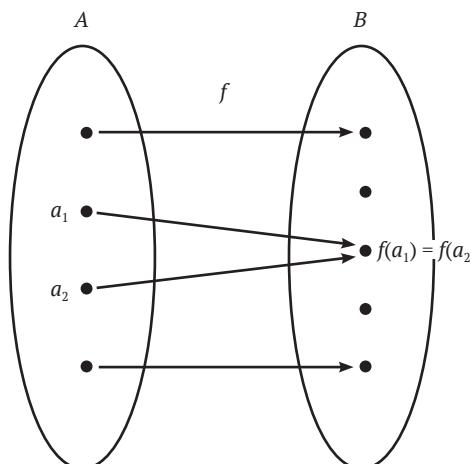
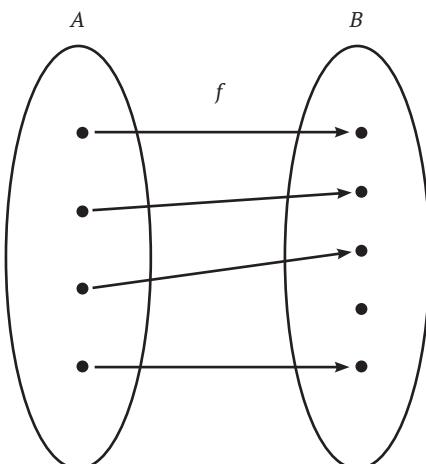
(a) f не однозначна(b) f однозначна

Рис. 5.4 ♦ Примеры неоднозначной (а) и однозначной (б) функций

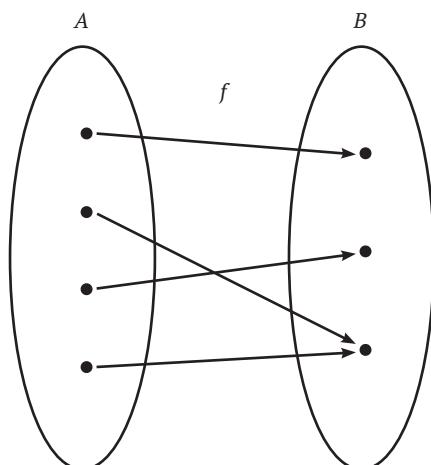
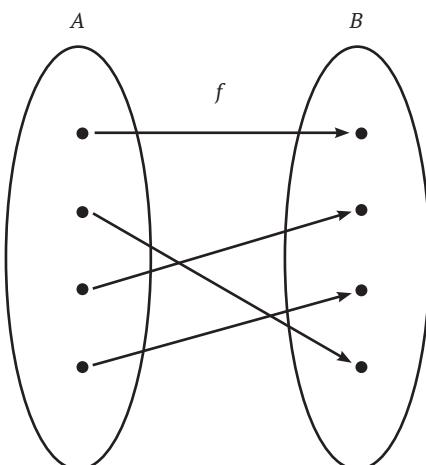
(a) f сюръективна, но не однозначна(б) f сюръективна и однозначна

Рис. 5.5 ♦ Примеры неоднозначной (а) и однозначной (б) сюръективных функций

Пример 5.2.2. Однозначны ли следующие функции? Сюръективны ли они?

1. Функция F из п. 1 примера 5.1.2.
2. Функция L из п. 3 примера 5.1.2.
3. Функция тождества i_A для любого множества A .
4. Функция g из п. 2 примера 5.1.3.
5. Функция h из п. 3 примера 5.1.3.

Решения

1. F не взаимно однозначна, потому что $F(1) = 5 = F(3)$. Она также не сюръективна, потому что $6 \in B$, но не существует $a \in A$ такого, что $F(a) = 6$.
2. L не взаимно однозначна, потому что существует много пар различных городов c_1 и c_2 , для которых $L(c_1) = L(c_2)$. Например, $L(\text{Чикаго}) = \text{США} = L(\text{Сиэтл})$. Утверждение что L сюръективна, соответствует формуле $\forall n \in N \exists c \in C(L(c) = n)$, или, другими словами, для каждой страны n существует такой город c , что город c расположен в стране n . Вероятно, это правда, поскольку маловероятно, что существует страна, в которой вообще нет городов. Таким образом, функция L , вероятно, сюръективна.
3. Чтобы решить, является ли i_A взаимно однозначным, мы должны определить, найдутся ли в A два элемента a_1 и a_2 такие, что $i_A(a_1) = i_A(a_2)$ и $a_1 \neq a_2$.

Но, как сказано в разделе 5.1, для любого $a \in A$ справедливо $i_A(a) = a$, поэтому $i_A(a_1) = i_A(a_2)$ означает $a_1 = a_2$. Значит, не может быть элементов a_1 и a_2 из множества A таких, что $i_A(a_1) = i_A(a_2)$ и $a_1 \neq a_2$, поэтому i_A взаимно однозначна.

Утверждение, что i_A сюръективна, означает, что для любого $a \in A$ найдется такой $b \in A$, что справедливо $a = i_A(b)$. Это, очевидно, верно, потому что $a = i_A(a)$. Значит, i_A сюръективна.

4. Как и в решении 3, чтобы узнать, является ли функция g взаимно однозначной, мы должны определить, существуют ли такие целые числа n_1 и n_2 , что $g(n_1) = g(n_2)$ и $n_1 \neq n_2$. Согласно определению g мы имеем:

$$\begin{aligned} g(n_1) = g(n_2) \text{ тогда и только тогда, когда } 2n_1 + 3 = 2n_2 + 3 \\ \text{тогда и только тогда, когда } 2n_1 = 2n_2 \\ \text{тогда и только тогда, когда } n_1 = n_2. \end{aligned}$$

Следовательно, не может быть целых чисел n_1 и n_2 , для которых $g(n_1) = g(n_2)$ и $n_1 \neq n_2$. Другими словами, функция g однозначна. Однако она не сюръективна, потому что, например, не существует целого числа n , для которого $g(n) = 0$. Чтобы понять, почему, предположим, что n – целое число и $g(n) = 0$. Тогда по определению g мы имеем $2n + 3 = 0$, поэтому $n = -3/2$. Но это противоречит тому факту, что n – целое число. Обратите внимание, что область определения g – это \mathbb{Z} , поэтому для того, чтобы g была сюръективной, для каждого действительного числа y должно существовать целое число n такое, что $g(n) = y$. Поскольку мы убедились, что не существует такого целого числа n , что $g(n) = 0$, мы можем заключить, что g не сюръективна.

5. Эта функция является как взаимно однозначной, так и сюръективной. Проверка того, что h взаимно однозначна, очень похожа на проверку однозначности g в решении 4 и оставляется читателю. Чтобы убедиться, что h сюръективна, мы должны показать, что $\forall y \in \mathbb{R} \exists x \in \mathbb{R} (h(x) = y)$. Вот краткое доказательство этого утверждения. Пусть y – произвольное действительное число. Пусть $x = (y - 3)/2$. Тогда $g(x) = 2x + 3 = 2 \cdot ((y - 3)/2) + 3 = y - 3 + 3 = y$. Следовательно, $\forall y \in \mathbb{R} \exists x \in \mathbb{R} (h(x) = y)$, значит, функция h сюръективна.

Хотя определение взаимной однозначности легче всего понять, когда оно сформулировано как отрицательное утверждение, как в определении 5.2.1, мы знаем из главы 3, что определение проще использовать в доказательствах, если переписать его как эквивалентное положительное утверждение. Следующая теорема показывает, как это сделать. Она также дает полезную эквивалентность для определения сюръективности.

Теорема 5.2.3. Предположим, что $f: A \rightarrow B$.

1. f взаимно однозначна тогда и только тогда, когда $\forall a_1 \in A \forall a_2 \in A (f(a_1) = f(a_2) \rightarrow a_1 = a_2)$.
2. f сюръективна тогда и только тогда, когда $\text{Ran}(f) = B$.

Доказательство

1. Мы воспользуемся правилами из глав 1 и 2 для преобразования отрицательных утверждений в положительные формы.

f взаимно однозначна тогда и только тогда,
 когда $\neg \exists a_1 \in A \exists a_2 \in A (f(a_1) = f(a_2) \wedge a_1 \neq a_2)$
 тогда и только тогда, когда $\forall a_1 \in A \forall a_2 \in A \neg (f(a_1) = f(a_2) \wedge a_1 \neq a_2)$
 тогда и только тогда, когда $\forall a_1 \in A \forall a_2 \in A (f(a_1) \neq f(a_2) \vee a_1 = a_2)$
 тогда и только тогда, когда $\forall a_1 \in A \forall a_2 \in A (f(a_1) = f(a_2) \rightarrow a_1 = a_2)$.

2. Сначала мы свяжем определение сюръективности с определением множества значений.

f сюръективна тогда и только тогда, когда $\forall b \in B \exists a \in A (f(a) = b)$
 тогда и только тогда, когда $\forall b \in B \exists a \in A ((a, b) \in f)$
 тогда и только тогда, когда $\forall b \in B (b \in \text{Ran}(f))$
 тогда и только тогда, когда $B \subseteq \text{Ran}(f)$.

Теперь мы готовы доказать часть 2 теоремы.

(\rightarrow) Предположим, что f сюръективна. По только что полученной эквивалентности $B \subseteq \text{Ran}(f)$, а по определению множества значений $\text{Ran}(f) \subseteq B$. Отсюда следует, что $\text{Ran}(f) = B$.

(\leftarrow) Предположим, что $\text{Ran}(f) = B$. Тогда, безусловно, $B \subseteq \text{Ran}(f)$, так что с учетом эквивалентности можно заключить, что f сюръективна.

Комментарий. Обычно наиболее выгодно записывать доказательство оператором «тогда и только тогда, когда» в виде строки эквивалентностей, если это возможно. В случае утверждения 1 это легко сделать, используя правила логики. Для утверждения 2 эта стратегия не совсем работает, но она дает нам эквивалентность, которая оказывается полезной при доказательстве.

Пример 5.2.4. Пусть $A = R \setminus \{-1\}$, а функция $f: A \rightarrow R$ определена формулой

$$f(a) = \frac{2a}{a + 1}.$$

Докажите, что f взаимно однозначна, но не сюръективна.

Стратегия доказательства

Согласно п. 1 теоремы 5.2.3 мы можем доказать, что f взаимно однозначна, доказывая эквивалентное утверждение $\forall a_1 \in A \forall a_2 \in A (f(a_1) = f(a_2) \rightarrow a_1 = a_2)$. Итак, пусть a_1 и a_2 – произвольные элементы из A , предположим, что $f(a_1) = f(a_2)$, а затем докажем, что $a_1 = a_2$. Это стратегия, которая почти всегда используется при доказательстве взаимной однозначности функции. Остальные детали доказательства касаются только простой алгебры и приводятся позже.

Чтобы показать, что f не сюръективна, мы должны доказать истинность утверждения $\neg \forall x \in \mathbb{R} \exists a \in A (f(a) = x)$. Переписав его как положительное утверждение, мы видим, что должны доказать $\exists x \in \mathbb{R} \forall a \in A (f(a) \neq x)$, поэтому мы должны попытаться найти конкретное определенное число x такое, что $\forall a \in A (f(a) \neq x)$. К сожалению, совсем не ясно, какое значение мы должны взять для x . Чтобы преодолеть эту трудность, мы воспользуемся несколько необычной процедурой. Вместо того чтобы пытаться доказать, что f не сюръективна, давайте попробуем доказать, что она сюръективна! Конечно, мы ожидаем, что это доказательство не сработает, но, возможно, понимание того, почему оно не работает, поможет нам выяснить, какое значение x использовать в доказательстве того, что функция f не сюръективна.

Чтобы доказать, что f сюръективна, нам нужно будет доказать утверждение $\forall x \in \mathbb{R} \exists a \in A (f(a) = x)$, поэтому мы должны принять за x произвольное действительное число и попытаться найти такое $a \in A$, что $f(a) = x$. Заполняя определение f , мы видим, что должны найти элемент $a \in A$ такой, что

$$\frac{2a}{a+1} = x.$$

Чтобы найти это значение, мы просто решаем уравнение относительно a :

$$\frac{2a}{a+1} = x \Rightarrow 2a = ax + x \Rightarrow a(2 - x) = x \Rightarrow a = \frac{x}{2 - x}.$$

Вот оно! Последний шаг в этом выводе не сработает, если $x = 2$, потому что тогда мы будем делить на 0. Это единственное значение x , которое вызывает проблемы, когда мы пытаемся найти значение a , для которого $f(a) = x$. Возможно, $x = 2$ – это значение, которое нужно использовать в доказательстве того, что f не сюръективна.

Теперь вернемся к доказательству того, что f не сюръективна. Если мы примем $x = 2$, то для завершения доказательства мы должны показать, что $\forall a \in A (f(a) \neq 2)$. Мы сделаем это, объявив a произвольным элементом из A , полагая $f(a) = 2$, а затем пытаясь получить противоречие. Остальные детали доказательства несложны.

Решение

Доказательство. Чтобы убедиться, что f взаимно однозначна, пусть a_1 и a_2 – произвольные элементы из A , и предположим, что $f(a_1) = f(a_2)$. Применяя определение f , получаем, что $2a_1/(a_1 + 1) = 2a_2/(a_2 + 1)$. Таким образом, $2a_1(a_2 + 1) = 2a_2(a_1 + 1)$. Умножение обеих частей дает нам $2a_1a_2 + 2a_1 = 2a_1a_2 + 2a_2$, поэтому $2a_1 = 2a_2$ и, следовательно, $a_1 = a_2$.

Чтобы показать, что f не сюръективна, докажем, что $\forall a \in A (f(a) \neq 2)$. Предположим, что $a \in A$ и $f(a) = 2$. Применяя определение f , получаем $2a/(a+1) = 2$. Таким образом, $2a = 2a + 2$, что явно невозможно. Следовательно, $2 \notin \text{Ran}(f)$, поэтому $\text{Ran}(f) \neq \mathbb{R}$ и f не сюръективна.

Как мы видели в предыдущем примере, при доказательстве взаимной однозначности функции f обычно проще всего доказать эквивалентное утверждение $\forall a_1 \in A \forall a_2 \in A (f(a_1) = f(a_2) \rightarrow a_1 = a_2)$ из п. 1 теоремы 5.2.3. Конечно, это всего лишь пример того, что обычно легче доказать положительное утверждение, чем отрицательное. Эта эквивалентность также часто используется в доказательствах, где нам дано, что функция взаимно однозначна, как вы увидите в доказательстве части 1 следующей теоремы.

Теорема 5.2.5. Предположим, что $f: A \rightarrow B$ и $g: B \rightarrow C$. Как мы показали в теореме 5.1.5, отсюда следует, что $g \circ f: A \rightarrow C$.

1. Если f и g взаимно однозначны, то этим же свойством обладает $g \circ f$.
2. Если f и g сюръективны, то этим же свойством обладает $g \circ f$.

Доказательство

1. Предположим, что f и g взаимно однозначны. Пусть a_1 и a_2 – произвольные элементы из A , и предположим, что $(g \circ f)(a_1) = (g \circ f)(a_2)$. Согласно теореме 5.1.5 это означает, что $g(f(a_1)) = g(f(a_2))$. Так как g взаимно однозначно, то $f(a_1) = f(a_2)$, и аналогично, поскольку f взаимно однозначно, мы можем заключить, что $a_1 = a_2$. Таким образом, композиция $g \circ f$ также взаимно однозначна.
2. Предположим, что f и g сюръективны, и пусть c – произвольный элемент из C . Поскольку g сюръективна, мы можем найти некоторый элемент $b \in B$ такой, что $g(b) = c$. Аналогично, поскольку f сюръективна, существует некоторый элемент $a \in A$ такой, что $f(a) = b$. Тогда $(g \circ f)(a) = g(f(a)) = g(b) = c$. Таким образом, композиция $g \circ f$ тоже сюръективна.

Комментарий

1. Как и в примере 5.2.4, мы доказываем, что композиция $g \circ f$ взаимно однозначна, доказав, что $\forall a_1 \in A \forall a_2 \in A (f(a_1) = f(a_2) \rightarrow a_1 = a_2)$. Итак, пусть a_1 и a_2 – произвольные элементы из A , предположим, что $(g \circ f)(a_1) = (g \circ f)(a_2)$, что означает $g(f(a_1)) = g(f(a_2))$, а затем докажем, что $a_1 = a_2$. В следующем предложении доказательства говорится про предположение, что g взаимно однозначно, но может быть не ясно, как оно используется. Чтобы понять этот шаг, давайте запишем, что значит однозначность g . Как мы заметили ранее, вместо того чтобы использовать исходное определение, которое является отрицательным утверждением, нам, вероятно, будет лучше использовать эквивалентное положительное утверждение $\forall b_1 \in B \forall b_2 \in B (g(b_1) = g(b_2) \rightarrow b_1 = b_2)$. Естественный способ использовать посылку в этой форме – подставить что-нибудь вместо b_1 и b_2 . Подставляя $f(a_1)$ и $f(a_2)$, мы получаем $g(f(a_1)) = g(f(a_2)) \rightarrow f(a_1) = f(a_2)$, и, поскольку мы знаем, что $g(f(a_1)) = g(f(a_2))$, по modus ponens следует $f(a_1) = f(a_2)$. Эти шаги не были раскрыты в доказательстве; читатели доказательства должны догадаться об этом сами. Убедитесь, что вы

понимаете, как, используя аналогичные рассуждения, можно перейти от $f(a_1) = f(a_2)$ к $a_1 = a_2$, применив тот факт, что f взаимно однозначна.

2. После предположения, что f и g сюръективны, форма остальной части доказательства полностью определяется логической формой цели. Поскольку это означает, что $\forall c \in C \exists a \in A ((g \circ f)(a) = c)$, обозначим за c произвольный элемент из C , а затем найдем некоторый элемент $a \in A$, для которого мы можем доказать $(g \circ f)(a) = c$.

Функции, которые взаимно однозначны и в то же время сюръективны, особенно важны в математике. Такие функции иногда называют *взаимно однозначными соответствиями*, или *биекциями*. На рис. 5.5(b) показан пример однозначного соответствия. Обратите внимание, что на этом рисунке и A , и B состоят из четырех элементов. На самом деле вы должны понять простую вещь: если существует взаимно однозначное соответствие между двумя конечными множествами, то эти множества должны иметь одинаковое количество элементов. Это одна из причин, почему так важны однозначные соответствия. Мы обсудим взаимно однозначные соответствия между бесконечными множествами в главе 8.

Вот еще один пример однозначного соответствия. Предположим, что A – это множество всех зрителей на аншлаговом концерте, а S – множество всех мест в концертном зале. Пусть $f: A \rightarrow S$ – функция, заданная правилом

$$f(a) = \text{сиденье, на котором сидит } a.$$

Поскольку разные люди не сидят на одном и том же месте, функция f взаимно однозначна. Так как билеты на концерт распроданы и все места заняты, функция f сюръективна. Следовательно, f является взаимно однозначным соответствием. Даже не пересчитывая людей или места, мы можем сказать, что количество зрителей в концертном зале должно быть ровно таким же, как количество мест.

Упражнения

1. Какие функции в упражнении 1 раздела 5.1 взаимно однозначны? Какие сюръективны?
- *2. Какие функции в упражнении 2 раздела 5.1 взаимно однозначны? Какие сюръективны?
3. Какие функции в упражнении 3 раздела 5.1 взаимно однозначны? Какие сюръективны?
4. Какие функции в упражнении 4 раздела 5.1 взаимно однозначны? Какие сюръективны?
- *5. Пусть $A = \mathbb{R} \setminus \{1\}$, и пусть $f: A \rightarrow A$ определено следующим образом:

$$f(x) = \frac{x+1}{x-1}.$$

- (a) Докажите, что f взаимно однозначна и сюръективна.
 (b) Докажите, что $f \circ f = i_A$.
6. Пусть a и b – действительные числа и $a \neq 0$. Определим $f: \mathbb{R} \rightarrow \mathbb{R}$ формулой $f(x) = ax + b$. Покажите, что f взаимно однозначна и сюръективна.
7. Определим функцию $f: \mathbb{R}^+ \rightarrow \mathbb{R}$ по формуле $f(x) = 1/x - x$.
- Докажите, что f взаимно однозначна. (Подсказка: вы можете сначала доказать, что если $0 < a < b$, то $f(a) > f(b)$.)
 - Покажите, что f сюръективна.
 - Пусть функция $g: \mathbb{R}^+ \rightarrow \mathbb{R}$ определена формулой $g(x) = 1/x + x$. Эта функция взаимно однозначна? Эта функция сюръективна?
8. Пусть $A = \mathcal{P}(\mathbb{R})$. Определим функцию $f: \mathbb{R} \rightarrow A$ по формуле $f(x) = \{y \in \mathbb{R} \mid y^2 < x\}$.
- Найдите $f(2)$.
 - Является ли f взаимно однозначной? Сюръективной?
- *9. Пусть $A = \mathcal{P}(\mathbb{R})$ и $B = \mathcal{P}(A)$. Определим $f: B \rightarrow A$ по формуле $f(\mathcal{F}) = \bigcup \mathcal{F}$.
- Найдите $f(\{\{1, 2\}, \{3, 4\}\})$.
 - Является ли f взаимно однозначной? Сюръективной?
10. Пусть $f: A \rightarrow B$ и $g: B \rightarrow C$.
- Докажите, что если $g \circ f$ сюръективна, то g сюръективна.
 - Докажите, что если $g \circ f$ взаимно однозначна, то f взаимно однозначна.
11. Пусть $f: A \rightarrow B$ и $g: B \rightarrow C$.
- Докажите, что если f сюръективна и g не взаимно однозначна, то $g \circ f$ не взаимно однозначна.
 - Докажите, что если f не сюръективна и g взаимно однозначна, то $g \circ f$ не сюръективна.
12. Пусть $f: A \rightarrow B$. Определим функцию $g: B \rightarrow \mathcal{P}(A)$ формулой $g(b) = \{a \in A \mid f(a) = b\}$. Докажите, что если f сюръективна, то g взаимно однозначна. Что, если f не сюръективна?
- *13. Пусть $f: A \rightarrow B$ и $C \subseteq A$. В упражнении 7 раздела 5.1 мы определили $f \upharpoonright C$ (ограничение f на C), и вы показали, что $f \upharpoonright C : C \rightarrow B$.
- Докажите, что если f взаимно однозначна, то и $f \upharpoonright C$ обладает таким же свойством.
 - Докажите, что если $f \upharpoonright C$ сюръективна, то f обладает таким же свойством.
 - Приведите примеры, показывающие, что обратное утверждение для частей (a) и (b) не всегда истинно.
14. Пусть $f: A \rightarrow B$ и существует некоторый элемент $b \in B$ такой, что $\forall x \in A (f(x) = b)$. (Поэтому f – постоянная функция.)
- Докажите, что если A имеет более одного элемента, то f не взаимно однозначна.
 - Докажите, что если B имеет более одного элемента, то f не сюръективна.

15. Пусть $f: A \rightarrow C$, $g: B \rightarrow C$, а A и B не пересекаются. В упражнении 12(а) раздела 5.1 вы доказали, что $f \cup g: A \cup B \rightarrow C$. Теперь предположим, что f и g взаимно однозначны. Докажите, что $f \cup g$ взаимно однозначно тогда и только тогда, когда $\text{Ran}(f)$ и $\text{Ran}(g)$ не пересекаются.
16. Пусть R – отношение из A в B , S – отношение из B в C , $\text{Ran}(R) = \text{Dom}(S) = B$ и $S \circ R: A \rightarrow C$. В упражнении 13(а) в разделе 5.1 вы доказали, что $S: B \rightarrow C$. Теперь докажите, что если S взаимно однозначно, то $R: A \rightarrow B$.
- *17. Пусть $f: A \rightarrow B$ и R – отношение на A . Как и в упражнении 15 раздела 5.1, определим отношение S на B следующим образом:
- $$S = \{(x, y) \in B \times B \mid \exists u \in A \exists v \in A (f(u) = x \wedge f(v) = y \wedge (u, v) \in R)\}.$$
- (a) Докажите, что если R рефлексивно и f сюръективна, то S рефлексивно.
(b) Докажите, что если R транзитивно и f взаимно однозначна, то S транзитивно.
18. Пусть R является отношением эквивалентности на A , и пусть $g: A/R \rightarrow A/R$ определяется формулой $g([x]) = [x]$, как в упражнении 20(б) в разделе 5.1.
- (a) Покажите, что g сюръективна.
(b) Покажите, что g взаимно однозначна тогда и только тогда, когда $R = i_A$.
19. Пусть $f: A \rightarrow B$, R – отношение эквивалентности на A , и f совместно с R (определение совместности см. в упражнении 21 раздела 5.1). В упражнении 21(а) раздела 5.1 вы доказали, что существует единственная функция $h: A/R \rightarrow B$ такая, что для всех $x \in A$ справедливо $h([x]) = f(x)$. Теперь докажите, что h взаимно однозначна тогда и только тогда, когда $\forall x \in A \forall y \in A (f(x) = f(y) \rightarrow xRy)$.
- *20. Пусть A , B и C – множества и $f: A \rightarrow B$.
- (a) Докажите, что если f сюръективна, $g: B \rightarrow C$, $h: B \rightarrow C$ и $g \circ f = h \circ f$, то $g = h$.
(b) Пусть C имеет не менее двух элементов, и для всех функций g и h от B к C если $g \circ f = h \circ f$, то $g = h$. Докажите, что f сюръективна.
21. Пусть A , B и C – множества и $f: B \rightarrow C$.
- (a) Докажите, что если f взаимно однозначна, $g: A \rightarrow B$, $h: A \rightarrow B$ и $f \circ g = f \circ h$, то $g = h$.
(b) Пусть $A = \emptyset$, и для всех функций g и h от A к B если $f \circ g = f \circ h$, то $g = h$. Докажите, что f взаимно однозначна.
22. Пусть $\mathcal{F} = \{f \mid f: \mathbb{R} \rightarrow \mathbb{R}\}$, и определим отношение R на \mathcal{F} следующим образом:

$$R = \{(f, g) \in \mathcal{F} \times \mathcal{F} \mid \exists h \in \mathcal{F} (f = h \circ g)\}.$$

- (a) Пусть f , g и h – функции от \mathbb{R} до \mathbb{R} , определенные формулами $f(x) = x^2 + 1$, $g(x) = x^3 + 1$ и $h(x) = x^4 + 1$. Докажите, что это тот случай, когда hRf , но не gRf .

- (b) Докажите, что R – предпорядок. (См. определение предпорядка в упражнении 25 раздела 4.5.)
- (c) Докажите, что для всех $f \in \mathcal{F}$ справедливо $f R i_R$.
- (d) Докажите, что для всех $f \in \mathcal{F}$ $i_R R f$ тогда и только тогда, когда f взаимно однозначна. (Подсказка для направления справа налево: предположим, что f взаимно однозначна. Пусть $A = \text{Ran}(f)$, и пусть $h = f^{-1} \cup ((\mathbb{R} \setminus A) \times \{0\})$. Теперь докажите, что $h: \mathbb{R} \rightarrow \mathbb{R}$ и $i_{\mathbb{R}} = h \circ f$.)
- (e) Предположим, что $g \in \mathcal{F}$ – постоянная функция; другими словами, существует некоторое действительное число c такое, что $\forall x \in \mathbb{R} (g(x) = c)$. Докажите, что для всех $f \in \mathcal{F}$ истинно утверждение $g R f$. (Подсказка: см. упражнение 17 в разделе 5.1.)
- (f) Предположим, что $g \in \mathcal{F}$ – постоянная функция. Докажите, что для всех $f \in \mathcal{F}$ $f R g$ тогда и только тогда, когда f – постоянная функция.
- (g) Как и в упражнении 25 раздела 4.5, если мы положим $S = R \cap R^{-1}$, то S будет отношением эквивалентности на \mathcal{F} . Кроме того, существует единственное отношение T на \mathcal{F}/S такое, что для всех f и g в \mathcal{F} утверждение $[f]_S T [g]_S$ тогда и только тогда, когда $f R g$, и T – частичный порядок на \mathcal{F}/S . Докажите, что множество всех взаимно однозначных функций от \mathbb{R} к \mathbb{R} является наибольшим элементом \mathcal{F}/S в частичном порядке T , а множество всех постоянных функций от \mathbb{R} к \mathbb{R} является наименьшим элементом.
23. Пусть $f: \mathbb{N} \rightarrow \mathbb{N}$ определяется формулой $f(n) = n$. Обратите внимание, что мы также можем сказать, что $f: \mathbb{N} \rightarrow \mathbb{Z}$. Это упражнение покажет, почему в определении 5.2.1 мы использовали фразу « f отображается на B », а не просто « f сюръективна».
- (a) Отображается ли f на \mathbb{N} ?
- (b) Отображается ли f в \mathbb{Z} ?

5.3. ИНВЕРСИЯ ФУНКЦИЙ

Теперь мы готовы вернуться к вопросу о том, всегда ли обратная функция от A к B является функцией от B к A . Рассмотрим снова функцию F из п. 1 примера 5.1.2. Напомним, что в этом примере у нас было $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$ и $F = \{(1, 5), (2, 4), (3, 5)\}$. Как мы убедились в примере 5.1.2, F является функцией от A к B . Согласно определению, обратное отношение имеет вид $F^{-1} = \{(5, 1), (4, 2), (5, 3)\}$, что, очевидно, является отношением от B на A . Но F^{-1} не может быть функцией от B к A по двум причинам. Прежде всего $6 \in B$, но 6 не образует пару ни с одним элементом A в отношении F^{-1} . Во-вторых, 5 образует пару с двумя разными элементами A , 1 и 3 . Таким образом, этот пример показывает, что функция, обратная функции от A к B , не всегда является функцией от B к A .

Вы могли заметить, что причины, по которым F^{-1} не является функцией от B к A , связаны с причинами, по которым F не является ни взаимно однозначной, ни сюръективной, упомянутыми в части 1 примера 5.2.2. Это наводит на мысль о следующей теореме.

Теорема 5.3.1. Предположим, что $f: A \rightarrow B$. Если f взаимно однозначна и сюръективна, то существует $f^{-1}: B \rightarrow A$.

Доказательство. Предположим, что f взаимно однозначна и сюръективна, и пусть b – произвольный элемент B . Чтобы показать, что f^{-1} является функцией от B к A , мы должны доказать, что $\exists! a \in A ((b, a) \in f^{-1})$, поэтому существование и единственность докажем отдельно.

Существование: поскольку f сюръективна, существует некоторый элемент $a \in A$ такой, что $f(a) = b$. Таким образом, $(a, b) \in f$, значит, $(b, a) \in f^{-1}$.

Единственность: предположим, что $(b, a_1) \in f^{-1}$ и $(b, a_2) \in f^{-1}$ для некоторых $a_1, a_2 \in A$. Тогда $(a_1, b) \in f$ и $(a_2, b) \in f$, поэтому $f(a_1) = b = f(a_2)$. Поскольку f взаимно однозначна, отсюда следует, что $a_1 = a_2$.

Комментарий. Форма доказательства определяется логической формой утверждения, что $f^{-1}: B \rightarrow A$. Поскольку это означает $\forall b \in B \exists! a \in A ((b, a) \in f^{-1})$, пусть b – произвольный элемент из B , а затем отдельно докажем существование и единственность нужного $a \in A$. Обратите внимание, что предположение о том, что f сюръективна, является ключом к доказательству существования, а предположение, что f взаимно однозначна, является ключом к доказательству уникальности.

Предположим, что f – некоторая функция из множества A к множеству B . Теорема 5.3.1 утверждает, что достаточным условием, для того чтобы f^{-1} была функцией из B к A , является взаимно однозначное соответствие f . Но является ли это необходимым условием? Другими словами, верно ли обратное к теореме 5.3.1? (Если вы не помните, что означают слова «достаточный», «необходимый» и «обратный», вам следует вернуться к разделу 1.5!) Мы покажем в теореме 5.3.4, что ответ на этот вопрос утвердительный. Другими словами, если f^{-1} – это функция от B к A , то f должна быть взаимно однозначной и сюръективной.

Если $f^{-1}: B \rightarrow A$, то по определению функции для каждого $b \in B$ существует ровно один элемент $a \in A$ такой, что $(b, a) \in f^{-1}$, и

$$\begin{aligned} f^{-1}(b) &= \text{единственный } a \in A \text{ такой, что } (b, a) \in f^{-1} \\ &= \text{единственный } a \in A \text{ такой, что } (a, b) \in f \\ &= \text{единственное } a \in A \text{ такой, что } f(a) = b. \end{aligned}$$

Это дает нам еще одну полезную точку зрения на f^{-1} . Если f^{-1} является функцией от B к A , то это функция, которая сопоставляет каждому элементу $b \in B$ уникальный элемент $a \in A$, такой что $f(a) = b$. Предположение в теореме 5.3.1 о взаимной однозначности f гарантирует, что существует ровно один такой a .

В качестве примера снова рассмотрим функцию f , которая назначает каждому человеку в зрительном зале на концерте с аншлагом место, на котором этот человек сидит. Как мы видели в конце предыдущего раздела, f является взаимно однозначной функцией от множества A всех зрителей к множеству S всех мест в концертном зале. Следовательно, f^{-1} должна быть функцией от S к A , и для каждого $s \in S$

$f^{-1}(s) =$ единственный $a \in A$ такой, что $f(a) = s$
 $=$ уникальный человек a такой, что место, на котором сидит a ,
 \quad является s
 $=$ человек, сидящий на месте s .

Другими словами, функция f назначает каждому человеку место, на котором этот человек сидит, а функция f^{-1} назначает каждому месту человека, сидящего на этом месте.

Поскольку $f: A \rightarrow S$ и $f^{-1}: S \rightarrow A$, по теореме 5.1.5 следует, что $f^{-1} \circ f: A \rightarrow A$ и $f \circ f^{-1}: S \rightarrow S$. Что это за функции? Чтобы выяснить, что из себя представляет первая функция, обозначим за a произвольный элемент A и вычислим $(f^{-1} \circ f)(a)$.

$$\begin{aligned}(f^{-1} \circ f)(a) &= f^{-1}(f(a)) \\&= f^{-1}(\text{сиденье, на котором сидит } a) \\&= \text{человек, сидящий на месте, на котором сидит } a \\&= a.\end{aligned}$$

Но напомним, что для любого $a \in A$ справедливо $i_A(a) = a$. Таким образом, мы показали, что $\forall a \in A ((f^{-1} \circ f)(a) = i_A(a))$, поэтому по теореме 5.1.4 $f^{-1} \circ f = i_A$. Аналогично, вы должны иметь возможность проверить, что $f \circ f^{-1} = i_S$.

Когда математики обнаруживают подобное необычное явление на примере, они всегда задаются вопросом, простое ли это совпадение или часть более общей закономерности. Другими словами, можем ли мы доказать теорему, которая гласит, что то, что произошло в этом примере, произойдет и в других примерах? В этом случае оказывается, что можем.

Теорема 5.3.2. Предположим, что f – функция от A к B , и предположим, что f^{-1} – функция от B к A . Тогда $f^{-1} \circ f = i_A$ и $f \circ f^{-1} = i_B$.

Доказательство. Пусть a – произвольный элемент из A . Пусть $b = f(a) \in B$. Тогда $(a, b) \in f$, поэтому $(b, a) \in f^{-1}$ и, следовательно, $f^{-1}(b) = a$. Таким образом:

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a = i_A(a).$$

Поскольку a произвольно, мы показали, что $\forall a \in A ((f^{-1} \circ f)(a) = i_A(a))$, следовательно, $f^{-1} \circ f = i_A$. Доказательство второй половины теоремы аналогично и остается в качестве упражнения (см. упражнение 8).

Комментарий. Чтобы доказать равенство двух функций, мы обычно применяем теорему 5.1.4. Таким образом, поскольку $f^{-1} \circ f$ и i_A являются функциями от A к A , для доказательства их равенства мы докажем, что $\forall a \in A ((f^{-1} \circ f)(a) = i_A(a))$.

Теорема 5.3.2 утверждает, что если $f: A \rightarrow B$ и $f^{-1}: B \rightarrow A$, то каждая функция отменяет действие другой. Для любого $a \in A$ применение функции f дает $f(a) \in B$. Согласно теореме 5.3.2, $f^{-1}(f(a)) = (f^{-1} \circ f)(a) = i_A(a) = a$. Как видите, применение f^{-1} к $f(a)$ отменяет эффект применения f , возвращая нам исходный элемент a . Аналогично, для любого $b \in B$, применяя f^{-1} , мы получаем $f^{-1}(b) \in A$, и мы можем отменить эффект применения f^{-1} , применяя f , поскольку $f(f^{-1}(b)) = b$.

Например, пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ определяется формулой $f(x) = 2x$. Вы должны удостовериться, что f взаимно однозначна и сюръективна, поэтому $f^{-1}: \mathbb{R} \rightarrow \mathbb{R}$, и для любого $x \in \mathbb{R}$ справедливо

$$f^{-1}(x) = \text{единственный } y \text{ такой, что } f(y) = x.$$

Поскольку $f^{-1}(x)$ является единственным решением для y в уравнении $f(y) = x$, мы можем найти формулу для $f^{-1}(x)$, решив это уравнение для y . Заполнение определения f в уравнении дает нам $2y = x$, поэтому $y = x/2$. Таким образом, для любого $x \in \mathbb{R}$ $f^{-1}(x) = x/2$. Обратите внимание, что применение f к любому числу удваивает число, а применение f^{-1} уменьшает его вдвое, и каждая из этих операций отменяет действие другой. Другими словами, если вы удвоите число, а затем уменьшите результат вдвое, вы вернетесь к тому числу, с которого начали. Точно так же уменьшение вдвое любого числа и последующее удвоение результата вернет вам исходное число.

Существуют ли другие обстоятельства, при которых композиция двух функций равна функции идентичности? Исследование этого вопроса приводит к следующей теореме.

Теорема 5.3.3. Возьмем функцию $f: A \rightarrow B$.

1. Если существует функция $g: B \rightarrow A$ такая, что $g \circ f = i_A$, то f взаимно однозначна.
2. Если существует функция $g: B \rightarrow A$ такая, что $f \circ g = i_B$, то f сюръективна.

Доказательство

1. Предположим, что $g: B \rightarrow A$ и $g \circ f = i_A$. Пусть a_1 и a_2 – произвольные элементы из A , и предположим, что $f(a_1) = f(a_2)$. Применяя функцию g к обеим частям этого равенства, получаем $g(f(a_1)) = g(f(a_2))$. Но $g(f(a_1)) = (g \circ f)(a_1) = i_A(a_1) = a_1$, и аналогично $g(f(a_2)) = a_2$. Таким образом, мы можем заключить, что $a_1 = a_2$, и, следовательно, f взаимно однозначна.
2. См. упражнение 9.

Комментарий. Предположение, что существует функция $g: B \rightarrow A$ такая, что $g \circ f = i_A$, является экзистенциальным утверждением, поэтому мы сразу представляем, что была выбрана конкретная функция g . Доказательство взаимной однозначности f следует обычному шаблону для таких доказательств, основанному на теореме 5.2.3.

Итак, круг замкнулся. В теореме 5.3.1 мы доказали, что если f взаимно однозначная и сюръективная функция от A к B , то f^{-1} является функцией от B к A . Из этого заключения следует, как мы показали в теореме 5.3.2, что композиция f с обратной ей функцией должна быть функцией тождества. А в теореме 5.3.3 мы обнаружили, что когда композиция двух функций является функцией тождества, мы возвращаемся к свойствам взаимной однозначности и сюръективности! Таким образом, комбинируя теоремы 5.3.1–5.3.3, мы получаем следующую теорему.

Теорема 5.3.4. Предположим, что $f: A \rightarrow B$. Тогда следующие утверждения эквивалентны.

1. f взаимно однозначна и сюръективна.
2. $f^{-1}: B \rightarrow A$.
3. Существует функция $g: B \rightarrow A$ такая, что $g \circ f = i_A$ и $f \circ g = i_B$.

Доказательство

1 → 2. Именно об этом говорит теорема 5.3.1.

2 → 3. Предположим, что $f^{-1}: B \rightarrow A$. Пусть $g = f^{-1}$, и применим теорему 5.3.2.

3 → 1. Применим теорему 5.3.3.

Комментарий. Как мы показали в разделе 3.6, самый простой способ доказать, что несколько утверждений эквивалентны, – это доказать круг импликаций. В этом случае мы доказали круг $1 \rightarrow 2 \rightarrow 3 \rightarrow 1$. Отметим, что доказательства этих импликаций весьма схематичны. Вы должны самостоятельно дополнить их деталями.

Например, пусть f и g – функции от \mathbb{R} к \mathbb{R} , определенные следующими формулами:

$$f(x) = \frac{x+7}{5}, \quad g(x) = 5x - 7.$$

Тогда для любого действительного числа x

$$(g \circ f)(x) = g(f(x)) = g\left(\frac{x+7}{5}\right) = 5 \cdot \frac{x+7}{5} - 7 = x + 7 - 7 = x.$$

Таким образом, $g \circ f = i_{\mathbb{R}}$. Аналогичное рассуждение показывает, что $f \circ g = i_{\mathbb{R}}$. Таким образом, из теоремы 5.3.4 следует, что f должна быть взаимно однозначной и сюръективной и что f^{-1} также должна быть функцией от \mathbb{R} к \mathbb{R} . Что такое f^{-1} ? Конечно, было бы логично предположить, что $f^{-1} = g$, но на самом деле это не следует из доказанных теорем. Вы можете проверить это напрямую, вычислив $f^{-1}(x)$ с учетом того факта, что $f^{-1}(x)$ должно быть единственным решением для y в уравнении $f(y) = x$. Однако в этой проверке нет необходимости. Следующая теорема показывает, что f^{-1} должно быть равно g .

Теорема 5.3.5. Предположим, что $f: A \rightarrow B$, $g: B \rightarrow A$, $g \circ f = i_A$ и $f \circ g = i_B$. Тогда $g = f^{-1}$.

Доказательство. По теореме 5.3.4 $f^{-1}: B \rightarrow A$. Следовательно, по теореме 5.3.2 $f^{-1} \circ f = i_A$. Таким образом:

$$\begin{aligned} g &= i_A \circ g && \text{(упражнение 9 раздела 43)} \\ &= (f^{-1} \circ f) \circ g \\ &= f^{-1} \circ (f \circ g) && \text{(теорема 4.2.5)} \\ &= f^{-1} \circ i_B \\ &= f^{-1} && \text{(упражнение 9 раздела 43).} \end{aligned}$$

Комментарий. Это доказательство быстро приводит к желаемому заключению благодаря эффективному использованию предыдущих теорем и упражнений. Более прямое, но несколько более длинное доказательство фигурирует в упражнении 10.

Пример 5.3.6. В каждой части определите, является ли f взаимно однозначной и сюръективной. Если это так, найдите f^{-1} .

- Пусть $A = \mathbb{R} \setminus \{0\}$ и $B = \mathbb{R} \setminus \{2\}$, и функция $f: A \rightarrow B$ определена формулой

$$f(x) = \frac{1}{x} + 2.$$

(Обратите внимание, что для всех $x \in A$ значение $1/x$ определено и не равно нулю, поэтому $f(x) \neq 2$ и, следовательно, $f(x) \in B$.)

- Пусть $A = \mathbb{R}$ и $B = \{x \in \mathbb{R} \mid x \geq 0\}$ и функция $f: A \rightarrow B$ определена формулой

$$f(x) = x^2.$$

Решения

- Вы можете напрямую проверить, что f взаимно однозначна, но мы не будем это делать. Вместо этого мы просто попытаемся найти функцию $g: B \rightarrow A$ такую, что $g \circ f = i_A$ и $f \circ g = i_B$. Мы знаем из теорем 5.3.4 и 5.3.5, что если мы найдем такую g , то сможем сделать вывод, что f взаимно однозначна и сюръективна и $g = f^{-1}$.

Поскольку мы собираемся получить $g = f^{-1}$, мы знаем, что для любого $x \in B = \mathbb{R} \setminus \{2\}$ значение $g(x)$ должно быть единственным $y \in A$ таким, что $f(y) = x$. Таким образом, чтобы найти формулу для $g(x)$, мы решаем уравнение $f(y) = x$ относительно y . Заполняя определение f , мы видим, что уравнение, которое мы должны решить, имеет вид:

$$\frac{1}{y} + 2 = x.$$

Решая это уравнение, получаем:

$$\frac{1}{y} + 2 = x \Rightarrow \frac{1}{y} = x - 2 \Rightarrow y = \frac{1}{x-2}.$$

Таким образом, мы определяем функцию $g: B \rightarrow A$ формулой

$$g(x) = \frac{1}{x-2}.$$

(Обратите внимание, что для всех $x \in B$ по условию $x \neq 2$, поэтому $1/(x-2)$ определено и не равно нулю и, следовательно, $g(x) \in A$.) Давайте убедимся, что g обладает нужными свойствами. Для любого $x \in A$ мы имеем:

$$g(f(x)) = g\left(\frac{1}{x} + 2\right) = \frac{1}{1/x + 2 - 2} = \frac{1}{1/x} = x.$$

Таким образом, $g \circ f = i_A$. Аналогично, для любого $x \in B$

$$f(g(x)) = f\left(\frac{1}{x-2}\right) = \frac{1}{1/(x-2)} + 2 = x - 2 + 2 = x,$$

поэтому $f \circ g \neq i_B$. Следовательно, как мы заметили ранее, f должно быть взаимно однозначной и сюръективной, и $g = f^{-1}$.

2. Повторяя решение п. 1, попробуем найти функцию $g: B \rightarrow A$ такую, что $g \circ f = i_A$ и $f \circ g = i_B$. Поскольку применение f к числу приводит к возведению этого числа в квадрат, а мы хотим, чтобы g отменила эффект f , разумным предложением было бы извлечение квадратного корня $g(x) = \sqrt{x}$. Посмотрим, сработает ли эта идея.

Для любого $x \in B$ получаем:

$$f(g(x)) = f(\sqrt{x}) = (\sqrt{x})^2 = x,$$

поэтому $f \circ g = i_B$. Но для $x \in A$ получаем выражение

$$g(f(x)) = g(x^2) = \sqrt{x^2},$$

и оно не всегда равно x . Например, $g(f(-3)) = \sqrt{(-3)^2} = \sqrt{9} = 3 \neq -3$. Следовательно, $g \circ f = i_A$. Этот пример показывает, что вы должны проверить оба варианта, как $f \circ g = i_B$, так и $g \circ f = i_A$. Один вариант может сработать, а другой – нет.

Что пошло не так? Мы знаем, что если f^{-1} является функцией от B к A , то для любого $x \in B$ функция $f^{-1}(x)$ должна быть единственным решением относительно y в уравнении $f(y) = x$. Применение определения f дает нам $y^2 = x$, поэтому $y = \pm\sqrt{x}$. Следовательно, в уравнении $y^2 = x$ есть два решения вместо одного. Например, когда $x = 9$, мы получаем $y = \pm 3$. Другими словами, $f(3) = f(-3) = 9$. Но это означает, что f не является взаимно однозначной! Значит, f^{-1} не является функцией от B к A .

Функции, которые отменяют действие друг друга, часто встречаются в математике. Например, если вы знакомы с логарифмами, вы узнаете формулы $10^{\log x} = x$ и $\log 10^x = x$. (Здесь мы используем логарифмы с основанием 10.) Мы можем переписать эти формулы на языке текущего раздела, определив функции $f: \mathbb{R} \rightarrow \mathbb{R}^+$ и $g: \mathbb{R}^+ \rightarrow \mathbb{R}$ следующим образом:

$$f(x) = 10^x, \quad g(x) = \log x.$$

Тогда для любого $x \in \mathbb{R}$ имеем $g(f(x)) = \log 10^x = x$, а для любого $x \in \mathbb{R}^+$ $f(g(x)) = 10^{\log x} = x$. Таким образом, $g \circ f = i_{\mathbb{R}}$ и $f \circ g = i_{\mathbb{R}^+}$, поэтому $g = f^{-1}$. Другими словами, логарифмическая функция обратна функции «возвести 10 в степень».

Мы видели еще один пример функций, отменяющих действие друг друга, в разделе 4.5. Предположим, что A – любое множество, пусть \mathbb{E} – множество всех отношений эквивалентности на A , и пусть \mathcal{P} – множество всех разбиений A . Определим функцию $f: \mathbb{E} \rightarrow \mathcal{P}$ формулой $f(R) = A/R$ и определим другую функцию $g: \mathcal{P} \rightarrow \mathbb{E}$ формулой

$$\begin{aligned} g(\mathcal{F}) &= \text{отношение эквивалентности, определяемое } \mathcal{F} \\ &= \bigcup_{X \in \mathcal{F}} (X \times X). \end{aligned}$$

Убедитесь в том, что из доказательства теоремы 4.5.6 следует, что $f \circ g = i_{\mathbb{E}}$, а из упражнения 10 в разделе 4.5 следует, что $g \circ f = i_{\mathcal{P}}$. Таким образом, f вза-

имно однозначна и сюръективна, и $g = f^{-1}$. Одно интересное следствие этого состоит в том, что если A имеет конечное число элементов, то мы можем сказать, что количество отношений эквивалентности на A точно такое же, как количество разбиений A , даже если мы не знаем, какое это число.

Упражнения

- *1. Пусть R – функция, определенная в упражнении 2(с) раздела 5.1. В упражнении 2 раздела 5.2 вы показали, что R взаимно однозначна и сюръективна, поэтому $R^{-1}: P \rightarrow P$. Если $p \in P$, какова обратная функция $R^{-1}(p)$?
- 2. Пусть F – функция, определенная в упражнении 4(б) раздела 5.1. В упражнении 4 раздела 5.2 вы показали, что F взаимно однозначна и сюръективна, так что $F^{-1}: B \rightarrow B$. Если $X \in B$, какова обратная функция $F^{-1}(X)$?
- *3. Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ определяется формулой

$$f(x) = \frac{2x + 5}{3}.$$

Покажите, что f взаимно однозначна и сюръективна, и найдите формулу для $f^{-1}(x)$. (Вы можете скопировать метод, использованный в примере после теоремы 5.3.2 или в примере 5.3.6.)

- 4. Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ определяется формулой $f(x) = 2x^3 - 3$. Покажите, что f взаимно однозначна и сюръективна, и найдите формулу для $f^{-1}(x)$.
- 5. Пусть $f: \mathbb{R} \rightarrow \mathbb{R}^+$ определяется формулой $f(x) = 10^{2-x}$. Покажите, что f взаимно однозначна и сюръективна, и найдите формулу для $f^{-1}(x)$.
- 6. Пусть $A = \mathbb{R} \setminus \{2\}$, и пусть f – функция с областью определения A , определенной формулой

$$f(x) = \frac{3x}{x - 2}.$$

- (a) Покажите, что f – взаимно однозначная сюръективная функция от A к B для некоторого множества $B \subseteq \mathbb{R}$. Что такое множество B ?
- (b) Найдите формулу для $f^{-1}(x)$.
- 7. В примере после теоремы 5.3.4 мы задали $f(x) = (x + 7)/5$ и нашли, что $f^{-1}(x) = 5x - 7$. Пусть f_1 и f_2 – функции от \mathbb{R} к \mathbb{R} , определенные по формулам

$$f_1(x) = x + 7, \quad f_2(x) = \frac{x}{5}.$$

- (a) Докажите, что $f = f_2 \circ f_1$.
- (b) Согласно части 5 теоремы 4.2.5, $f^{-1} = (f_2 \circ f_1)^{-1} = f_1^{-1} \circ f_2^{-1}$. Убедитесь, что это так, вычислив $f_1^{-1} \circ f_2^{-1}$ напрямую.
- 8. (a) Докажите вторую половину теоремы 5.3.2, копируя доказательство первой половины.

- (b) Приведите альтернативное доказательство второй половины теоремы 5.3.2, применив первую половину к f^{-1} .
- *9. Докажите часть 2 теоремы 5.3.3.
10. Используйте следующую стратегию, чтобы дать альтернативное доказательство теоремы 5.3.5: пусть (b, a) – произвольный элемент из $B \times A$. Предположите $(b, a) \in g$ и докажите $(b, a) \in f^{-1}$. Затем предположите $(b, a) \in f^{-1}$ и докажите $(b, a) \in g$.
- *11. Пусть $f: A \rightarrow B$ и $g: B \rightarrow A$.
- Докажите, что если f взаимно однозначна и $f \circ g = i_B$, то $g = f^{-1}$.
 - Докажите, что если f сюръективна и $g \circ f = i_A$, то $g = f^{-1}$.
 - Докажите, что если $f \circ g = i_B$, но $g \circ f = i_A$, то f сюръективна, но не взаимно однозначна, а g взаимно однозначна, но не сюръективна.
12. Пусть $f: A \rightarrow B$ и f взаимно однозначна. Докажите, что существует некоторое множество $B' \subseteq B$ такое, что $f^{-1}: B' \rightarrow A$.
13. Предположим, что $f: A \rightarrow B$ и f сюръективна. Пусть $R = \{(x, y) \in A \times A \mid f(x) = f(y)\}$. Согласно упражнению 20(а) раздела 5.1, R является отношением эквивалентности на A .
- Докажите, что существует функция $h: A/R \rightarrow B$ такая, что для всех $x \in A$ справедливо $h([x]_R) = f(x)$. (Подсказка: см. упражнение 21 в разделе 5.1.)
 - Докажите, что функция h взаимно однозначна и сюръективна. (Подсказка: см. упражнение 19 в разделе 5.2.)
 - Из пункта (b) следует, что $h^{-1}: B \rightarrow A/R$. Докажите, что для всех $b \in B$ справедливо $h^{-1}(b) = \{x \in A \mid f(x) = b\}$.
 - Предположим, что $g: B \rightarrow A$. Докажите, что $f \circ g = i_B$ тогда и только тогда, когда $\forall b \in B(g(b) \in h^{-1}(b))$.
- *14. Предположим, что $f: A \rightarrow B$, $g: B \rightarrow A$ и $f \circ g = i_B$. Пусть $A' = \text{Ran}(g) \subseteq A$.
- Докажите, что для всех $x \in A'$ справедливо $(g \circ f)(x) = x$.
 - Докажите, что $f \upharpoonright A'$ является взаимно однозначной сюръективной функцией от A' к B и $g = (f \upharpoonright A')^{-1}$. (Значение используемых здесь обозначений см. в упражнении 7 раздела 5.1.)
15. Пусть $B = \{x \in \mathbb{R} \mid x \geq 0\}$. Пусть $f: \mathbb{R} \rightarrow B$ и $g: B \rightarrow \mathbb{R}$ определены формулами $f(x) = x^2$ и $g(x) = \sqrt{x}$. Как мы видели в п. 2 примера 5.3.6, $g \neq f^{-1}$. Покажем, что $g = (f \upharpoonright B)^{-1}$. (Подсказка: см. упражнение 14.)
- *16. Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ определяется формулой $f(x) = 4x - x^2$. Пусть $B = \text{Ran}(f)$.
- Найдите B .
 - Найдите множество $A \subseteq \mathbb{R}$ такое, что $f \upharpoonright A$ – взаимно однозначная сюръективная функция от A , и найдите формулу для $(f \upharpoonright A)^{-1}(x)$. (Подсказка: см. упражнение 14.)
17. Пусть A – некоторое множество, и пусть $\mathcal{F} = \{f \mid f: A \rightarrow A\}$ и $\mathcal{P} = \{f \in \mathcal{F} \mid f$ взаимно однозначна и сюръективна $\}$. Определим отношение R на \mathcal{F} следующим образом:

$$R = \{(f, g) \in \mathcal{F} \times \mathcal{F} \mid \exists h \in \mathcal{P}(f = h^{-1} \circ g \circ h)\}.$$

- (a) Докажите, что R – отношение эквивалентности.
- (b) Докажите, что если fRg , то $(f \circ f) R (g \circ g)$.
- (c) Для любых $f \in \mathcal{F}$ и $a \in A$, если $f(a) = a$, мы говорим, что a – *неподвижная (фиксированная) точка* f . Докажите, что если f имеет неподвижную точку и fRg , то g также имеет неподвижную точку.
- *18. Предположим, что $f: A \rightarrow C$, $g: B \rightarrow C$ и g взаимно однозначна и сюръективна. Докажите, что существует функция $h: A \rightarrow B$ такая, что $g \circ h = f$.

5.4. ЗАМКНУТЫЕ МНОЖЕСТВА

Часто в математике мы работаем с функцией от множества к самому себе. В этой ситуации может быть полезна следующая концепция.

Определение 5.4.1. Пусть дана функция $f: A \rightarrow A$ и множество $C \subseteq A$. Мы будем говорить, что множество C замкнуто относительно f , если $\forall x \in C (f(x) \in C)$.

Пример 5.4.2

- Пусть $A = \{a, b, c, d\}$ и $f = \{(a, c), (b, b), (c, d), (d, c)\}$. Тогда $f: A \rightarrow A$. Пусть $C_1 = \{a, c, d\}$ и $C_2 = \{a, b\}$. Замкнуто ли C_1 относительно f ? Замкнуто ли C_2 ?
- Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ и $g: \mathbb{R} \rightarrow \mathbb{R}$ определены формулами $f(x) = x + 1$ и $g(x) = x - 1$. Замкнуто ли множество \mathbb{N} относительно f ? Замкнуто ли оно относительно g ?
- Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ определяется формулой $f(x) = x^2$. Пусть $C_1 = \{x \in \mathbb{R} \mid 0 < x < 1\}$ и $C_2 = \{x \in \mathbb{R} \mid 0 < x < 2\}$. Замкнуто ли C_1 относительно f ? Замкнуто ли C_2 ?

Решения

- Множество C_1 замкнуто относительно f , потому что $f(a) = f(d) = c \in C_1$ и $f(c) = d \in C_1$. Однако C_2 не замкнуто относительно f , потому что $a \in C_2$, но $f(a) = c \notin C_2$.
- Для любого натурального числа n сумма $n + 1$ также является натуральным числом, поэтому \mathbb{N} замкнуто относительно f . Однако \mathbb{N} не замкнуто относительно g , потому что $0 \in \mathbb{N}$, но $g(0) = -1 \notin \mathbb{N}$.
- Для любого действительного числа x если $0 < x < 1$, то $0 < x^2 < 1$ (см. пример 3.1.2), поэтому C_1 замкнуто относительно f . Но $1,5 \in C_2$ и $f(1,5) = 1,5^2 = 2,25 \notin C_2$, поэтому C_2 не замкнуто относительно f .

В п. 2 примера 5.4.2 мы видели, что \mathbb{N} не замыкается относительно функции $g: \mathbb{R} \rightarrow \mathbb{R}$, определенной формулой $g(x) = x - 1$. Предположим, мы хотим добавить элементы к \mathbb{N} , чтобы получить множество, замкнутое относительно g . Поскольку $0 \in \mathbb{N}$, нам нужно добавить $g(0) = -1$. Но если к множеству добавить -1 , то оно также должно содержать $g(-1) = -2$, а если мы добавим -2 , то нам придется добавить $g(-2) = -3$. Вероятно, вы уже поняли, что нам придется сложить все отрицательные целые числа с \mathbb{N} , получив множество всех целых чисел \mathbb{Z} . Но обратите внимание, что \mathbb{Z} замкнуто относительно g , потому что для каждого целого числа n найдется разность $n - 1$, которая так-

же является целым числом. Итак, мы преуспели в нашей задаче увеличения \mathbb{N} , чтобы замкнуть множество относительно g .

Когда мы увеличили \mathbb{N} до \mathbb{Z} , добавленные числа – отрицательные целые числа – были числами, которые *пришло* добавить, поскольку мы хотели, чтобы результирующее множество было замкнуто относительно g . Отсюда следует, что \mathbb{Z} – наименьшее замкнутое относительно g множество, содержащее \mathbb{N} . Здесь мы используем слово «наименьший» точно так, как мы определили его в разделе 4.4. Если мы положим $\mathcal{F} = \{C \subseteq R \mid N \subseteq C \text{ и } C \text{ замкнуто относительно } g\}$, тогда \mathbb{Z} – наименьший элемент \mathcal{F} , где, как обычно, подразумевается, что мы имеем в виду «наименьший» в смысле подмножества частичного порядка. Другими словами, \mathbb{Z} является элементом \mathcal{F} , и это подмножество каждого элемента \mathcal{F} . Мы будем говорить, что \mathbb{Z} является *замыканием* \mathbb{N} относительно g .

Определение 5.4.3. Предположим, что $f: A \rightarrow A$ и $B \subseteq A$. Тогда *замыкание* B относительно f – это наименьшее множество $C \subseteq A$ такое, что $B \subseteq C$ и C замкнуто относительно f , если существует такое наименьшее множество. Другими словами, множество $C \subseteq A$ является замыканием B относительно f , если оно обладает следующими свойствами:

1. $B \subseteq C$.
2. C замкнуто относительно f .
3. Для любого множества $D \subseteq A$ если $B \subseteq D$ и D замкнуто относительно f , то $C \subseteq D$.

Согласно теореме 4.4.6 если в множестве есть наименьший элемент, то в нем может быть только один наименьший элемент. Таким образом, если множество B имеет замыкание относительно функции f , то это замыкание должно быть уникальным, поэтому имеет смысл называть его, например, *точным* замыканием, а не просто замыканием. Однако, как мы видели в примере 4.4.7, некоторые семейства множеств не имеют наименьших элементов, поэтому не сразу понятно, всегда ли множества имеют замыкания по функциям. На самом деле это так, как мы покажем в нашем доказательстве теоремы 5.4.5 ниже. Но сначала давайте рассмотрим еще несколько примеров замыканий.

Пример 5.4.4

1. В п. 1 примера 5.4.2 множество $C_2 = \{a, b\}$ не было замкнутым относительно f . Что означает замыкание C_2 относительно f ?
2. Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ определяется формулой $f(x) = x + 1$, и пусть $B = \{0\}$. Что означает замыкание B при f ?

Решения

1. Поскольку $a \in C_2$, чтобы получить множество, замкнутое относительно f , нам нужно добавить $f(a) = c$. Но тогда нам также придется добавить $f(c) = d$, что даст нам полное множество $A = \{a, b, c, d\}$. Ясно, что A замкнуто относительно f , поэтому замыкание C_2 относительно f есть A .
2. Поскольку $0 \in B$, замыкание B относительно f должно содержать $f(0) = 1$. Но тогда оно также должно содержать $f(1) = 2, f(2) = 3, f(3) = 4$ и факти-

чески все положительные целые числа. Добавление всех натуральных чисел к B дает нам множество \mathbb{N} , которое, как мы уже знаем из части 2 примера 5.4.2, замкнуто относительно f . Таким образом, замыкание $\{0\}$ относительно f равно \mathbb{N} .

Вот пример, иллюстрирующий полезность обсуждаемых нами понятий. Пусть P – множество людей, и предположим, что у каждого человека в множестве P есть лучший друг, который также находится в P . Тогда мы можем определить функцию $f: P \rightarrow P$ с помощью формулы $f(p)$ – лучший друг p . Предположим, что всякий раз, когда кто-то из множества P слышит сплетню, он рассказывает ее своему лучшему другу (но никому другому). Теперь рассмотрим любое множество $C \subseteq P$ и предположим, что C замкнуто относительно f . Тогда для любого человека $p \in C$ его лучший друг также находится в C . Таким образом, если кто-то из C услышит сплетню, единственный человек, которому он расскажет сплетню, также находится в C . Никто из C никогда не передаст сплетню человеку, который не находится в C . Таким образом, если мы расскажем некоторым людям в C какие-то сплетни, они могут распространиться на других людей в C , но никогда не оставят C . Если вы хотите отслеживать распространение сплетен в этой популяции, вам следует заранее узнать, какие подмножества P замкнуты относительно f .

Предположим, мы рассказываем сплетню всем людям в некотором множестве $B \subseteq P$. Как сплетня будет распространяться? Люди из B расскажут своим лучшим друзьям, а затем те расскажут своим лучшим друзьям, которые расскажут своим лучшим друзьям, и так далее. Основываясь на наших предыдущих примерах, вы можете догадаться, что множество H людей, которые в конечном итоге услышат сплетни, будут замыканием B относительно f . Посмотрим, сможем ли мы корректно доказать, что H обладает тремя свойствами, перечисленными в определении 5.4.3.

Очевидно, будет истинно утверждение $B \subseteq H$, поскольку люди в B слышат сплетни в самом начале процесса. Это подтверждает свойство 1 определения 5.4.3. Если p – произвольный элемент H , то в конце концов p слышит сплетню. Но как только p услышит сплетню, он перескажет ее $f(p)$, так что $f(p) \in H$. Таким образом, H замкнуто относительно f , как того требует свойство 2 определения. Наконец, предположим, что $B \subseteq C \subseteq P$ и C замкнуто относительно f . Как мы заметили ранее, любые сплетни, которые рассказывают людям в B , могут распространяться на других людей в C , но они никогда не покинут C . Таким образом, каждый, кто когда-либо слышал сплетни, должен принадлежать к C , что означает $H \subseteq C$. Это подтверждает свойство 3, поэтому H действительно является замыканием B относительно f .

Теперь перейдем к доказательству того, что замыкания существуют всегда. Предположим, что $f: A \rightarrow A$ и $B \subseteq A$. Один из способов доказать существование замыкания B относительно f – добавить к B те элементы, которые нужны, чтобы сделать его замкнутым относительно f , как мы это делали в предыдущих примерах, а затем доказать, что результат замкнут относительно f . Некоторые аспекты этого доказательства опираются на метод математической индукции, который мы еще не обсуждали. Мы представим это доказательство в разделе 6.5 после обсуждения математической индукции. Но есть другой

подход к доказательству, использующий только те понятия, которые мы уже изучили. Мы знаем, что замыкание B относительно f , если оно существует, должно быть наименьшим элементом семейства $\mathcal{F} = \{C \subseteq A \mid B \subseteq C \text{ и } C \text{ замкнуто относительно } f\}$.

Согласно упражнению 20 раздела 4.4, наименьший элемент множества также всегда является точной нижней границей множества, а по теореме 4.4.11 точной нижней гранью любого непустого семейства множеств \mathcal{F} является $\bigcap \mathcal{F}$. Это скелет нашего следующего доказательства.

Теорема 5.4.5. Пусть $f: A \rightarrow A$ и $B \subseteq A$. Тогда B имеет замыкание относительно f .

Доказательство. Пусть $\mathcal{F} = \{C \subseteq A \mid B \subseteq C \text{ и } C \text{ замкнуто относительно } f\}$. Вы уже должны суметь проверить, что $A \in \mathcal{F}$, и, следовательно, $\mathcal{F} \neq \emptyset$. Значит, мы можем принять $C = \bigcap \mathcal{F}$ и, исходя из упражнения 9 раздела 3.3, утверждать, что $C \subseteq A$. Мы покажем, что C является замыканием B относительно f , доказав три свойства из определения 5.4.3.

Чтобы доказать первое свойство, предположим, что $x \in B$. Пусть D – произвольный элемент \mathcal{F} . Тогда из определения \mathcal{F} следует $B \subseteq D$, поэтому $x \in D$. Поскольку D был выбран произвольно, это означает, что $\forall D \in \mathcal{F}(x \in D)$, поэтому $x \in \bigcap \mathcal{F} = C$. Следовательно, $B \subseteq C$.

Далее, предположим, что $x \in C$, и снова пусть D – произвольный элемент \mathcal{F} . Тогда $x \in D$, поскольку $x \in C = \bigcap \mathcal{F}$. Но поскольку $D \in \mathcal{F}$, множество D замкнуто относительно f , значит, $f(x) \in D$. Поскольку D произвольно, мы можем заключить, что $\forall D \in \mathcal{F}(f(x) \in D)$, поэтому $f(x) \in \bigcap \mathcal{F} = C$. Таким образом, мы показали, что C замкнуто относительно f , что является вторым свойством в определении 5.4.3.

Наконец, чтобы доказать третье свойство, предположим, что $B \subseteq D \subseteq A$ и D замкнуто относительно f . Тогда $D \in \mathcal{F}$, и, снова вспомнив упражнение 9 раздела 3.3, мы можем заключить, что $C = \bigcap \mathcal{F} \subseteq D$.

Комментарий. Наша цель – $\exists C(C – это замыкание B относительно f)$, поэтому мы должны начать с определения C . Однако определение $C = \bigcap \mathcal{F}$ не имеет смысла, если мы не уверены, что $\mathcal{F} \neq \emptyset$, поэтому сначала мы должны это доказать. Поскольку $\mathcal{F} \neq \emptyset$ означает $\exists D(D \in \mathcal{F})$, мы докажем это, приведя пример элемента из \mathcal{F} . Примером является A , поэтому мы должны доказать, что $A \in \mathcal{F}$. Фраза в доказательстве, что «вы должны суметь проверить», что $A \in \mathcal{F}$ действительно означает, что вы должны провести проверку. Согласно определению \mathcal{F} , утверждение, что $A \in \mathcal{F}$, означает, что $A \subseteq A$, $B \subseteq A$ и A замкнуто относительно f . Вы должны чувствовать, что хорошо понимаете, почему все три утверждения верны.

Определив C и убедившись, что $C \subseteq A$, мы должны доказать, что C обладает тремя свойствами, указанными в определении замыкания B относительно f . Чтобы доказать первое утверждение, $B \subseteq C$, обозначим за x произвольный элемент из B и докажем, что $x \in C$. Поскольку $C = \bigcap \mathcal{F}$, цель $x \in C$ означает $\forall D \in \mathcal{F}(x \in D)$, поэтому возьмем за D произвольный элемент из \mathcal{F} и докажем, что $x \in D$. Чтобы доказать, что C замкнуто относительно f , мы предположим, что $x \in C$ и докажем, что $f(x) \in C$. Напомним, что по определению C эта цель означает $\forall D \in \mathcal{F}(f(x) \in D)$, поэтому примем за D произвольный элемент из \mathcal{F} ,

докажем, что $f(x) \in D$. Наконец, для доказательства третьей цели мы предполагаем, что $D \subseteq A$, $B \subseteq D$ и D замкнуто относительно f , и доказываем, что $C \subseteq D$. К счастью, это доказательство фигурирует в упражнении из предыдущего раздела.

Замкнутые множества и замыкания также встречаются при изучении функций более чем одной переменной. Если $f: A \times A \rightarrow A$, то f называется *функцией двух переменных*. Элементом области определения f может быть упорядоченная пара (x, y) , где $x, y \in A$. Результат применения f к этой паре должен быть записан как $f((x, y))$, но обычно оставляют одну пару скобок и просто пишут $f(x, y)$.

Определение 5.4.6. Пусть $f: A \times A \rightarrow A$ и $C \subseteq A$. Мы будем говорить, что C замкнуто относительно f , если $\forall x \in C \forall y \in C (f(x, y) \in C)$.

Пример 5.4.7

- Пусть $f: \mathbb{R}^+ \times \mathbb{R}^+ \rightarrow \mathbb{R}^+$ и $g: \mathbb{R}^+ \times \mathbb{R}^+ \rightarrow \mathbb{R}^+$ определены формулами $f(x, y) = x/y$ и $g(x, y) = x^y$. Замкнуто ли множество \mathbb{Q}^+ относительно f ? Замкнуто ли оно относительно g ?
- Пусть $f: \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ и $g: \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ определены формулами $f(X, Y) = X \cup Y$ и $g(X, Y) = X \cap Y$. Пусть $\mathcal{I} = \{X \in \mathcal{P}(\mathbb{N}) \mid X \text{ бесконечно}\}$. Замкнуто ли множество \mathcal{I} относительно f ? Замкнуто ли оно относительно g ?

Решения

- Если $x, y \in \mathbb{Q}^+$, то существуют натуральные числа p, q, r и s такие, что $x = p/q$ и $y = r/s$. Следовательно:

$$f(x, y) = \frac{x}{y} = \frac{p/q}{r/s} = \frac{p}{q} \cdot \frac{s}{r} = \frac{ps}{qr} \in \mathbb{Q}^+.$$

Это показывает, что \mathbb{Q}^+ замкнуто относительно f . Однако 2 и $1/2$ являются элементами \mathbb{Q}^+ и $g(2, 1/2) = 2^{1/2} = \sqrt{2} \notin \mathbb{Q}^+$ (см. теорему 6.4.5), поэтому \mathbb{Q}^+ не замкнуто относительно g .

- Если X и Y – бесконечные множества натуральных чисел, то $f(X, Y) = X \cup Y$ также бесконечно, поэтому \mathcal{I} замкнуто относительно f . С другой стороны, пусть E – множество четных натуральных чисел, а P – множество простых чисел. Тогда E и P оба бесконечны, но $g(E, P) = E \cap P = \{2\}$, что конечно. Поэтому \mathcal{I} не замкнуто относительно g .

Как и раньше, мы можем определить замыкание множества под функцией двух переменных как наименьшее замкнутое множество, содержащее его, и мы можем доказать, что такие замыкания всегда существуют.

Определение 5.4.8. Пусть $f: A \times A \rightarrow A$ и $B \subseteq A$. Тогда замыкание B относительно f – это наименьшее множество $C \subseteq A$ такое, что $B \subseteq C$ и C замкнуто относительно f , если существует такое наименьшее множество. Другими словами, множество $C \subseteq A$ является замыканием B относительно f , если оно обладает следующими свойствами:

1. $B \subseteq C$.
2. C замкнуто относительно f .
3. Для любого множества $D \subseteq A$ справедливо следующее: если $B \subseteq D$ и D замкнуто относительно f , то $C \subseteq D$.

Теорема 5.4.9. Предположим, что $f: A \times A \rightarrow A$ и $B \subseteq A$. Тогда B имеет замыкание относительно f .

Доказательство. См. упражнение 11.

Функцию от $A \times A$ к A можно рассматривать как операцию, которая может применяться к паре объектов $(x, y) \in A \times A$ для создания другого элемента A . Часто в математике операция, выполняемая над парой математических объектов (x, y) , представлена символом, который мы пишем между x и y . Например, если x и y – действительные числа, то $x + y$ обозначает другое число, а если x и y – множества, то $x \cup y$ – другое множество. По аналогии с этой нотацией, когда математики определяют функцию от $A \times A$ к A , они иногда представляют ее символом, а не буквой, и записывают результат применения функции к паре (x, y) , помещая символ между x и y , а не перед скобками (x, y) . Когда функция от $A \times A$ к A записывается таким образом, это обычно называется *бинарной операцией над A* .

Например, в части 2 примера 5.4.7 мы определили $g: \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ формулой $g(X, Y) = X \cap Y$. Вместо того чтобы вводить имя g для этой функции, мы могли бы говорить о \cap как о бинарной операции над $\mathcal{P}(\mathbb{N})$. В этом примере мы показали, что множество \mathcal{I} всех бесконечных подмножеств \mathbb{N} не замкнуто относительно g . Другими словами, \mathcal{I} не замкнуто относительно бинарной операции \cap . Что представляет из себя замыкание \mathcal{I} относительно n ? Ответ см. в упражнении 16.

Вот еще один пример. Мы могли бы определить бинарную операцию $*$ над \mathbb{Z} , сказав, что для любых целых чисел x и y справедливо равенство $x * y = x^2 - y^2$. Замкнуто ли множество $\{0, 1\}$ при бинарной операции $*$? Ответ отрицательный, потому что $0 * 1 = 0^2 - 1^2 = -1 \notin \{0, 1\}$. Таким образом, замыкание $\{0, 1\}$ относительно операции $*$ должно содержать -1 . Но, как вы можете легко проверить, множество $\{-1, 0, 1\}$ замкнуто относительно операции $*$. Следовательно, замыкание $\{0, 1\}$ относительно $*$ равно $\{-1, 0, 1\}$.

Упражнения

- *1. Пусть функция $f: \mathbb{R} \rightarrow \mathbb{R}$ определена формулой $f(x) = (x + 1)/2$. Замкнуты ли следующие множества относительно f ?
 - (a) \mathbb{Z} .
 - (b) \mathbb{Q} .
 - (c) $\{x \in \mathbb{R} \mid 0 \leq x < 4\}$.
 - (d) $\{x \in \mathbb{R} \mid 2 \leq x < 4\}$.
2. Пусть функция $f: \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ определена формулой $f(X) = X \cup \{17\}$. Замкнуты ли следующие множества относительно f ?

- (a) $\{X \subseteq \mathbb{N} \mid X \text{ бесконечно}\}.$
 (b) $\{X \subseteq \mathbb{N} \mid X \text{ конечно}\}.$
 (c) $\{X \subseteq \mathbb{N} \mid X \text{ содержит не более 100 элементов}\}.$
 (d) $\{X \subseteq \mathbb{N} \mid 16 \in X\}.$
- *3. Пусть функция $f: \mathbb{Z} \rightarrow \mathbb{Z}$ определена формулой $f(n) = n^2 - n$. Найдите замыкание $\{-1, 1\}$ относительно f .
4. Для любого множества A множество всех отношений на A есть $\mathcal{P}(A \times A)$.
 Пусть функция $f: \mathcal{P}(A \times A) \rightarrow \mathcal{P}(A \times A)$ определена формулой $f(R) = R^{-1}$.
 Замкнуто ли множество рефлексивных отношений на A относительно f ?
 А как насчет множества симметричных отношений и множества транзитивных отношений? (Подсказка: см. упражнение 12 в разделе 4.3.)
5. Пусть задана функция $f: A \rightarrow A$. Замкнуто ли \emptyset относительно f ?
6. Пусть задана функция $f: A \rightarrow A$.
- (a) Докажите, что если $\text{Ran}(f) \subseteq C \subseteq A$, то множество C замкнуто относительно f .
 - (b) Докажите, что для любого множества $B \subseteq A$ замыкание B относительно f является подмножеством $B \cup \text{Ran}(f)$.
- *7. Пусть задана функция $f: A \rightarrow A$ и она взаимно однозначна и сюръективна.
 Тогда по теореме 5.3.1 $f^{-1}: A \rightarrow A$. Докажите, что если $C \subseteq A$ и C замкнуты относительно f , то $A \setminus C$ замкнуто относительно f^{-1} .
8. Пусть задана функция $f: A \rightarrow A$ и $C \subseteq A$. Докажите, что C замкнуто относительно f тогда и только тогда, когда замыкание C относительно f равно C .
- *9. Пусть задана функция $f: A \rightarrow A$ и C_1 и C_2 – подмножества A , замкнутые относительно f .
- (a) Докажите, что $C_1 \cup C_2$ замкнуто относительно f .
 - (b) Должно ли $C_1 \cap C_2$ быть замкнутым относительно f ? Обоснуйте ответ.
 - (c) Должно ли $C_1 \setminus C_2$ быть замкнутым относительно f ? Обоснуйте ответ.
10. Пусть даны $f: A \rightarrow A$, $B_1 \subseteq A$ и $B_2 \subseteq A$. Пусть C_1 – замыкание B_1 относительно f , и пусть C_2 – замыкание B_2 .
- (a) Докажите, что если $B_1 \subseteq B_2$, то $C_1 \subseteq C_2$.
 - (b) Докажите, что замыкание $B_1 \cup B_2$ относительно f есть $C_1 \cup C_2$.
 - (c) Должно ли замыкание $B_1 \cap B_2$ представлять собой $C_1 \cap C_2$? Обоснуйте ответ.
 - (d) Должно ли замыкание $B_1 \setminus B_2$ представлять собой $C_1 \setminus C_2$? Обоснуйте ответ.
11. Докажите теорему 5.4.9.
- *12. Если \mathcal{F} – множество функций от A к A и $C \subseteq A$, то мы будем говорить, что C замкнуто относительно \mathcal{F} , если $\forall f \in \mathcal{F} \forall x \in C (f(x) \in C)$. Другими словами, C замкнуто относительно \mathcal{F} тогда и только тогда, когда для всех $f \in \mathcal{F}$ множество C замкнуто относительно f . Если $B \subseteq A$, то замыкание B относительно \mathcal{F} – это наименьшее множество $C \subseteq A$ такое, что $B \subseteq C$ и C

- замкнуто относительно \mathcal{F} . (В следующем упражнении вас просят доказать, что замыкание всегда существует.)
- Пусть f и g – функции от \mathbb{R} к \mathbb{R} , определенные формулами $f(x) = x + 1$ и $g(x) = x - 1$. Найдите замыкание $\{\emptyset\}$ относительно $\{f, g\}$.
 - Для каждого натурального числа n пусть функция $f_n: \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ определена формулой $f_n(X) = X \cup \{n\}$ и пусть $\mathcal{F} = \{f_n \mid n \in \mathbb{N}\}$. Найдите замыкание $\{\emptyset\}$ под \mathcal{F} .
13. Предположим, что \mathcal{F} – это множество функций от A к A и $B \subseteq A$. См. в предыдущем упражнении определение замыкания B относительно \mathcal{F} .
- Докажите, что B имеет замыкание относительно \mathcal{F} . Для каждого $f \in \mathcal{F}$ пусть C_f – замыкание B относительно f , а C – замыкание B относительно \mathcal{F} .
 - Докажите, что $\bigcup_{f \in \mathcal{F}} C_f \subseteq C$.
 - Должно ли $\bigcup_{f \in \mathcal{F}} C_f$ быть замкнуто относительно \mathcal{F} ? Обоснуйте свой ответ либо доказательством, либо контрпримером.
 - Должно ли выполняться $\bigcup_{f \in \mathcal{F}} C_f = C$? Обоснуйте свой ответ либо доказательством, либо контрпримером.
- *14. Пусть функция $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ определена формулой $f(x, y) = x - y$. Что означает замыкание \mathbb{N} относительно f ?
15. Пусть функция $f: \mathbb{R}^+ \times \mathbb{R}^+ \rightarrow \mathbb{R}^+$ определена формулой $f(x, y) = x/y$. Что означает замыкание \mathbb{Z}^+ относительно f ?
16. Как и в п. 2 примера 5.4.7, пусть $\mathcal{I} = \{X \in \mathcal{P}(\mathbb{N}) \mid X \text{ бесконечно}\}$.
- Докажите, что для любого множества $X \subseteq \mathbb{N}$ существуют множества $Y, Z \in \mathcal{I}$ такие, что $Y \cap Z = X$.
 - Что означает замыкание \mathcal{I} относительно бинарной операции \cap ?
- *17. Пусть $\mathcal{F} = \{f \mid f: \mathbb{R} \rightarrow \mathbb{R}\}$. Тогда для любых $f, g \in \mathcal{F}$ справедливо $f \circ g \in \mathcal{F}$, поэтому \circ – бинарная операция на \mathcal{F} . Замкнуты ли следующие множества относительно \circ ?
- $\{f \in \mathcal{F} \mid f \text{ взаимно однозначна}\}$. (Подсказка: см. теорему 5.2.5.)
 - $\{f \in \mathcal{F} \mid f \text{ сюръективна}\}$.
 - $\{f \in \mathcal{F} \mid f \text{ строго возрастает}\}$. (Функция $f: \mathbb{R} \rightarrow \mathbb{R}$ строго возрастает, если $\forall x \in \mathbb{R} \forall y \in \mathbb{R} (x < y \rightarrow f(x) < f(y))$.)
 - $\{f \in \mathcal{F} \mid f \text{ строго убывает}\}$. (Функция $f: \mathbb{R} \rightarrow \mathbb{R}$ строго убывает, если $\forall x \in \mathbb{R} \forall y \in \mathbb{R} (x < y \rightarrow f(x) > f(y))$.)
18. Пусть $\mathcal{F} = \{f \mid f: \mathbb{R} \rightarrow \mathbb{R}\}$. Если $f, g \in \mathcal{F}$, то определим функцию $f + g: \mathbb{R} \rightarrow \mathbb{R}$ по формуле $(f + g)(x) = f(x) + g(x)$. Обратите внимание, что «+» – это бинарная операция над \mathcal{F} . Замкнуты ли следующие множества относительно операции $+$?
- $\{f \in \mathcal{F} \mid f \text{ взаимно однозначна}\}$.
 - $\{f \in \mathcal{F} \mid f \text{ сюръективна}\}$.
 - $\{f \in \mathcal{F} \mid f \text{ строго возрастает}\}$. (См. определение строгого возрастания в предыдущем упражнении.)
 - $\{f \in \mathcal{F} \mid f \text{ строго убывает}\}$. (См. определение строгого убывания в предыдущем упражнении.)

19. Для любого множества A множество всех отношений на A есть $\mathcal{P}(A \times A)$, а \circ – бинарная операция над $\mathcal{P}(A \times A)$. Замкнуто ли множество рефлексивных отношений на A относительно \circ ? А что насчет множества симметричных отношений и множества транзитивных отношений?
- *20. Деление не является бинарной операцией над \mathbb{R} , потому что вы не можете делить на 0. Но мы можем решить эту проблему. Мы начинаем с добавления нового элемента в \mathbb{R} . Мы назовем этот новый элемент «NaN» (от «Not a Number» – не является числом). Примем $\bar{\mathbb{R}} = \mathbb{R} \cup \{\text{NaN}\}$ и определим функцию $f: \bar{\mathbb{R}} \times \bar{\mathbb{R}} \rightarrow \bar{\mathbb{R}}$ следующим образом:

$$f(x, y) = \begin{cases} x/y, & \text{если } x, y \in \mathbb{R} \text{ и } y \neq 0 \\ \text{NaN} & \text{в остальных случаях} \end{cases}.$$

Эта запись означает, что если $x, y \in \mathbb{R}$ и $y \neq 0$, то $f(x, y) = x/y$, в противном случае $f(x, y) = \text{NaN}$. Таким образом, например, $f(3, 7) = 3/7$, $f(3, 0) = \text{NaN}$ и $f(\text{NaN}, 7) = \text{NaN}$. Какие из следующих множеств замкнуты относительно f ?

- (a) \mathbb{R} .
- (b) \mathbb{R}^+ .
- (c) \mathbb{R}^- .
- (d) \mathbb{Q} .
- (e) $\mathbb{Q} \cup \{\text{NaN}\}$.

21. Если \mathcal{F} – множество функций от $A \times A$ к A и $C \subseteq A$, то мы будем говорить, что C замкнуто относительно \mathcal{F} , если $\forall f \in \mathcal{F} \forall x \in C \forall y \in C (f(x, y) \in C)$. Другими словами, C замкнуто относительно \mathcal{F} тогда и только тогда, когда для всех $f \in \mathcal{F}$ множество C замкнуто относительно f . Если $B \subseteq A$, то замыкание B относительно \mathcal{F} – это наименьшее множество $C \subseteq A$, такое что $B \subseteq C$ и C замкнуто относительно \mathcal{F} , если существует такое наименьшее множество. (Сравните эти определения с определениями в упражнении 12.)
- (a) Докажите, что замыкание B относительно \mathcal{F} существует.
 - (b) Пусть функции $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ и $g: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ определены формулами $f(x, y) = x + y$ и $g(x, y) = xy$. Каково замыкание $\mathbb{Q} \cup \{\sqrt[3]{2}\}$ относительно $\{f, g\}$?

5.5. ОБРАЗЫ И ПРООБРАЗЫ: ИССЛЕДОВАТЕЛЬСКИЙ ПРОЕКТ

Допустим, у нас есть функция $f: A \rightarrow B$. Мы уже показали, что f можно рассматривать как сопоставление каждого элемента A с ровно одним элементом B . В этом разделе мы увидим, что f можно также рассматривать как сопоставление подмножеств A с подмножествами B и наоборот.

Определение 5.5.1. Пусть задана функция $f: A \rightarrow B$ и $X \subseteq A$. Тогда *образ* X относительно f – это множество $f(X)$, определенное следующим образом:

$$f(X) = \{f(x) \mid x \in X\} = \{b \in B \mid \exists x \in X (f(x) = b)\}.$$

(Обратите внимание, что образ всей области значений A относительно f – это $\{f(a) \mid a \in A\}$, и, как мы видели в разделе 5.1, это то же самое, что и область определения f .)

Если $Y \subseteq B$, то *прообраз* Y относительно f – это множество $f^{-1}(Y)$, определенное следующим образом:

$$f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}.$$

Обратите внимание, что функция f в определении 5.5.1 может и не быть взаимно однозначной или сюръективной, и в результате f^{-1} может не быть функцией от B к A , и для $y \in B$ запись $f^{-1}(y)$ может не иметь смысла. Однако даже в этом случае определение 5.5.1 по-прежнему придает смысл записи $f^{-1}(Y)$ для $Y \subseteq B$.

Если вас это удивляет, посмотрите еще раз на определение $f^{-1}(Y)$ и обратите внимание, что оно не рассматривает f^{-1} как функцию. Определение относится только к результатам применения f к элементам A , но не к результатам применения f^{-1} к элементам B .

Например, пусть L будет функцией, определенной в п. 3 примера 5.1.2, которая ставит в соответствие каждому городу страну, в которой этот город расположен. Как и в примере 5.1.2, пусть C – множество всех городов, а N – множество всех стран. Если B – это множество всех городов с населением не менее одного миллиона, то B – это подмножество C , а образ B относительно L будет множеством

$$\begin{aligned} L(B) &= \{L(b) \mid b \in B\} \\ &= \{n \in N \mid \exists b \in B (L(b) = n)\} \\ &= (n \in N \mid \text{город с населением не менее одного миллиона человек,} \\ &\quad \text{расположенный в стране } n). \end{aligned}$$

Таким образом, $L(B)$ – это множество всех стран, в которых есть город с населением не менее одного миллиона человек. Пусть теперь A будет подмножеством N , состоящим из всех стран Африки. Тогда прообразом A относительно L будет множество

$$\begin{aligned} L^{-1}(A) &= \{c \in C \mid L(c) \in A\} \\ &= [c \in C \mid \text{страна, в которой расположен } c, \text{ находится в Африке}]. \end{aligned}$$

Таким образом, $L^{-1}(A)$ – это множество всех городов африканских стран.

Приведем еще один пример. Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ определяется формулой $f(x) = x^2$, и пусть $X = \{x \in \mathbb{R} \mid 0 \leq x < 2\}$. Отсюда

$$f(X) = \{f(x) \mid x \in X\} = \{x^2 \mid 0 \leq x < 2\}.$$

Следовательно, $f(X)$ – это множество всех квадратов действительных чисел от 0 до 2 (включая 0, но не 2). Немного подумав, вы должны прийти к выводу, что это множество $\{x \in \mathbb{R} \mid 0 \leq x < 4\}$. Введем обозначение $Y = \{x \in \mathbb{R} \mid 0 \leq x < 4\}$ и найдем $f^{-1}(Y)$. Согласно определению прообраза:

$$\begin{aligned}
 f^{-1}(Y) &= \{x \in \mathbb{R} \mid f(x) \in Y\} \\
 &= \{x \in \mathbb{R} \mid 0 \leq f(x) < 4\} \\
 &= \{x \in \mathbb{R} \mid 0 \leq x^2 < 4\} \\
 &= \{x \in \mathbb{R} \mid -2 < x < 2\}.
 \end{aligned}$$

К настоящему времени у вас сформировался достаточный опыт написания доказательств, и вы должны быть готовы применить свои навыки для ответа на математические вопросы. Поэтому значительная часть этого раздела будет посвящена исследовательскому проекту, в котором вы найдете для себя ответы на важные математические вопросы об образах и прообразах. Для начала мы ответим на первый вопрос.

Предположим, что задана функция $f: A \rightarrow B$, а W и X являются подмножествами A . Вы можете задать естественный вопрос: обязательно ли $f(W \cap X)$ совпадает с $f(W) \cap f(X)$? Утвердительный ответ выглядит вполне правдоподобным, поэтому давайте попробуем его доказать. Итак, наша цель – доказать, что $f(W \cap X) = f(W) \cap f(X)$. Поскольку это равенство между двумя множествами, мы берем произвольный элемент из одного множества и пытаемся доказать, что он является элементом другого.

Предположим сначала, что y – произвольный элемент из $f(W \cap X)$. По определению $f(W \cap X)$ это означает, что $y = f(x)$ для некоторого $x \in W \cap X$. Поскольку $x \in W \cap X$, то $x \in W$ и $x \in X$. Но теперь у нас есть $y = f(x)$ и $x \in W$, поэтому мы можем заключить, что $y \in f(W)$. Аналогично, поскольку $y = f(x)$ и $x \in X$, из этого следует, что $y \in f(X)$. Таким образом, $y \in f(W) \cap f(X)$. Этот вывод завершает первую половину доказательства.

Теперь пусть $y \in f(W) \cap f(X)$. Тогда $y \in f(W)$, так что существует некоторый элемент $w \in W$ такой, что $f(w) = y$, а также $y \in f(X)$, так что существует некоторый элемент $x \in X$ такой, что $y = f(x)$. Если бы мы только знали, что w и x равны, мы могли бы заключить, что $w = x \in W \cap X$, поэтому $y = f(x) \in f(W \cap X)$. Но лучшее, что мы можем сделать, – это сказать, что $f(w) = y = f(x)$. Это должно напомнить вам об определении взаимной однозначности. Если бы мы знали, что f взаимно однозначна, то на основании факта, что $f(w) = f(x)$, мы бы сделали вывод, что $w = x$, и доказательство было бы завершено. Но без этой уверенности мы, кажется, застряли.

Подведем итог тому, что мы обнаружили. Прежде всего первая половина доказательства сработала нормально, поэтому мы можем с уверенностью сказать, что в общем случае $f(W \cap X) \subseteq f(W) \cap f(X)$. Вторая половина сработала бы, если бы мы знали, что f взаимно однозначна, поэтому мы также можем сказать, что если f взаимно однозначна, то $f(W \cap X) = f(W) \cap f(X)$. Но что, если f не однозначна? Вдруг существует какой-то способ завершить доказательство, показав, что равенство $f(W \cap X) = f(W) \cap f(X)$ остается истинным, даже если f не является взаимно однозначной? Но к настоящему времени вы, вероятно, уже начали подозревать, что, возможно, $f(W \cap X)$ и $f(W) \cap f(X)$ не всегда равны, поэтому нам следует потратить некоторое время на то, чтобы попытаться показать, что предложенная теорема неверна. Другими словами, давайте посмотрим, сможем ли мы найти контрпример – такую функцию f и множества W и X , для которых $f(W \cap X) \neq f(W) \cap f(X)$.

К счастью, мы можем добиться большего, чем просто пробовать примеры наугад. Конечно, мы знаем, что лучше использовать функцию, которая не является взаимно однозначной, но, исследуя нашу попытку доказательства, мы можем сказать больше. Попытка доказать, что $f(W \cap X) = f(W) \cap f(X)$, столкнулась с проблемой только тогда, когда W и X содержали элементы w и x такие, что $w \neq x$, но $f(w) = f(x)$, поэтому нам следует выбрать пример, в котором это происходит. Другими словами, мы должны не только убедиться, что f не взаимно однозначна, мы также должны убедиться, что W и X содержат элементы, которые показывают, что f не взаимно однозначна.

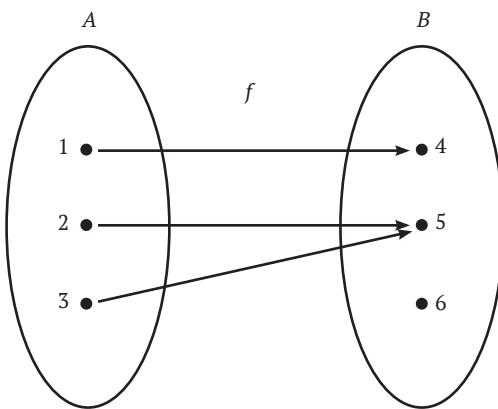


Рис. 5.6 ♦ Граф функции,
которая не является взаимно однозначной

Граф на рис. 5.6 представляет простую функцию, которая не является взаимно однозначной. Записывая его как множество упорядоченных пар, мы могли бы сказать, что $f = \{(1, 4), (2, 5), (3, 5)\}$ и $f: A \rightarrow B$, где $A = \{1, 2, 3\}$ и $B = \{4, 5, 6\}$. Два элемента A , которые показывают, что f не взаимно однозначна, – это 2 и 3, поэтому они должны быть элементами W и X соответственно. Почему бы просто не попробовать присвоить значения $W = \{2\}$ и $X = \{3\}$? При таком выборе мы получаем $f(W) = \{f(2)\} = \{5\}$ и $f(X) = \{f(3)\} = \{5\}$, поэтому $f(W \cap X) = \{5\} \cap \{5\} = \{5\}$. Но $f(W \cap X) = f(\emptyset) = \emptyset$, поэтому $f(W \cap X) \neq f(W) \cap f(X)$. (Если вы не поняли, почему $f(\emptyset) = \emptyset$, выясните это, используя определение 5.5.1!) Если вы хотите увидеть пример, в котором $W \cap X \neq \emptyset$, попробуйте значения $W = \{1, 2\}$ и $X = \{1, 3\}$.

Этот пример демонстрирует ошибочность теоремы о том, что $f(W \cap X)$ и $f(W) \cap f(X)$ всегда равны. Но наше доказательство подсказывает, что верна следующая теорема.

Теорема 5.5.2. Пусть $f: A \rightarrow B$ и W и X – подмножества A . Тогда $f(W \cap X) \subseteq f(W) \cap f(X)$. Кроме того, если f взаимно однозначна, то $f(W \cap X) = f(W) \cap f(X)$.

А теперь вам нужно попытаться ответить на несколько вопросов. В каждом случае постарайтесь дать как можно больше пояснений. Обоснуйте свои ответы доказательствами и контрпримерами.

1. Рассмотрим $f: A \rightarrow B$ и W и X – подмножества A .
 - (a) Всегда ли будет верно, что $f(W \cup X) = f(W) \cup f(X)$?
 - (b) Всегда ли будет верно, что $f(W \setminus X) = f(W) \setminus f(X)$?
 - (c) Всегда ли будет верно, что $W \subseteq X \Leftrightarrow f(W) \subseteq f(X)$?
2. Рассмотрим $f: A \rightarrow B$ и Y и Z – подмножества B .
 - (a) Всегда ли будет верно, что $f^{-1}(Y \cap Z) = f^{-1}(Y) \cap f^{-1}(Z)$?
 - (b) Всегда ли будет верно, что $f^{-1}(Y \cup Z) = f^{-1}(Y) \cup f^{-1}(Z)$?
 - (c) Всегда ли будет верно, что $f^{-1}(Y \setminus Z) = f^{-1}(Y) \setminus f^{-1}(Z)$?
 - (d) Всегда ли будет верно, что $Y \subseteq Z \Leftrightarrow f^{-1}(Y) \subseteq f^{-1}(Z)$?
3. Пусть $f: A \rightarrow B$ и $X \subseteq A$. Всегда ли будет верно, что $f^{-1}(f(X)) = X$?
4. Пусть $f: A \rightarrow B$ и $Y \subseteq B$. Всегда ли будет верно, что $f(f^{-1}(Y)) = Y$?
5. Пусть $f: A \rightarrow B$ и $C \subseteq A$. Докажите, что следующие утверждения эквивалентны:
 - (a) C замкнуто относительно f .
 - (b) $f(C) \subseteq C$.
 - (c) $C \subseteq f^{-1}(C)$.
6. Пусть $f: A \rightarrow B$ и $g: B \rightarrow C$. Можете ли вы доказать какие-нибудь интересные теоремы об образах и прообразах множеств относительно $g \circ f$?

Примечание: внимательный читатель, возможно, заметил двусмысличество в наших обозначениях образов и прообразов. Если $f: A \rightarrow B$ и $Y \subseteq B$, то мы использовали запись $f^{-1}(Y)$ для обозначения прообраза Y относительно f . Но если f взаимно однозначна и сюръективна, то, как мы видели в разделе 5.3, f^{-1} является функцией от B к A . Таким образом, $f^{-1}(Y)$ можно также интерпретировать как образ Y относительно функции f^{-1} . К счастью, эта двусмысличество безвредна, как показывает следующее задание.
7. Пусть функция $f: A \rightarrow B$ взаимно однозначна и сюръективна, и $Y \subseteq B$. Покажите, что прообраз Y относительно f и образ Y относительно f^{-1} равны. (Подсказка: сначала внимательно запишите определения этих двух множеств!)

Глава 6

Математическая индукция

6.1. ДОКАЗАТЕЛЬСТВО ПУТЕМ МАТЕМАТИЧЕСКОЙ ИНДУКЦИИ

В главе 3 мы изучали методы доказательства, которые можно использовать при рассуждении на любую математическую тему. В этой главе мы обсудим еще один метод доказательства, называемый *математической индукцией*, который предназначен для доказательства утверждений о, возможно, самой фундаментальной из всех математических структур – натуральных числах. Напомним, что множество всех натуральных чисел имеет вид $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Предположим, вы хотите доказать, что каждое натуральное число обладает некоторым свойством P . Другими словами, вы хотите показать, что числа 0, 1, 2, ... все имеют свойство P . Конечно, в этом списке бесконечно много чисел, поэтому вы не можете проверить их одно за другим, чтобы удостовериться, что все они имеют свойство P . Ключевая идея математической индукции состоит в следующем: чтобы перечислить все натуральные числа, вам достаточно начать с 0 и многократно добавлять 1. Таким образом, вы можете доказать, что каждое натуральное число имеет свойство P , показав, что 0 имеет свойство P и что всякий раз, когда вы добавляете 1 к числу, которое имеет свойство P , результирующее число также имеет свойство P . Это гарантирует, что когда вы перебираете список всех натуральных чисел, начиная с 0 и многократно добавляя 1, каждое полученное вами число будет иметь свойство P . Другими словами, все натуральные числа имеют свойство P . Итак, давайте подробнее рассмотрим, как работает метод математической индукции.

Чтобы доказать цель вида $\forall n \in \mathbb{N} P(n)$:

Сначала докажите $P(0)$, а затем $\forall n \in \mathbb{N}(P(n) \rightarrow P(n + 1))$. Первое из этих доказательств иногда называют *базовым (начальным) случаем*, а второе – *шагом индукции*.

Форма окончательного доказательства

Базовый случай: [Здесь приводится доказательство $P(0)$.]

Шаг индукции: [Здесь приводится доказательство $\forall n \in \mathbb{N}(P(n) \rightarrow P(n + 1))$.]

Позже мы приведем обоснование метода математической индукции, но сначала давайте рассмотрим пример доказательства, основанного на этом методе. Следующий перечень вычислений демонстрирует удивительную закономерность:

$$\begin{aligned} 2^0 &= 1 = 2^1 - 1 \\ 2^0 + 2^1 &= 1 + 2 = 3 = 2^2 - 1 \\ 2^0 + 2^1 + 2^2 &= 1 + 2 + 4 = 7 = 2^3 - 1 \\ 2^0 + 2^1 + 2^2 + 2^3 &= 1 + 2 + 4 + 8 = 15 = 2^4 - 1 \end{aligned}$$

Общая картина выглядит так:

$$2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1.$$

Работает ли эта закономерность для всех значений n ? Посмотрим, сможем ли мы это доказать.

Пример 6.1.1. Докажите, что для любого натурального числа n выполняется равенство $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$.

Стратегия доказательства

Наша цель – доказать утверждение $\forall n \in \mathbb{N}(P(n))$, где $P(n)$ – это утверждение $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$. Согласно нашей стратегии, мы можем сделать это, доказав два других утверждения, $P(0)$ и $\forall n \in \mathbb{N}(P(n) \rightarrow P(n + 1))$.

Подставляя 0 вместо n , мы видим, что $P(0)$ – это просто выражение $2^0 = 2^1 - 1$, первое выражение в нашем перечне вычислений. Доказать истинность этого утверждения несложно – просто выполните арифметические действия, чтобы убедиться, что обе части равны 1. Часто базовый случай доказательства индукцией очень прост, и единственная трудная работа при поиске доказательства – это выполнение шага индукции.

Для шага индукции мы должны доказать, что $\forall n \in \mathbb{N}(P(n) \rightarrow P(n + 1))$. Конечно, в доказательствах математической индукции применимы все методы, рассмотренные в главе 3, поэтому мы обозначим за n произвольное натуральное число, предположим, что $P(n)$ истинно, а затем докажем истинность $P(n + 1)$. Другими словами, пусть n – произвольное натуральное число. Предположим, что $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$, а затем докажем, что $2^0 + 2^1 + \dots + 2^{n+1} = 2^{n+2} - 1$. Из этого подхода вытекают следующие посылки и цель:

Посылки	Цель
$n \in \mathbb{N}$	$2^0 + 2^1 + \dots + 2^{n+1} = 2^{n+2} - 1$
$2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$	

Очевидно, что вторая посылка похожа на цель. Есть ли способ начать со второй посылки и вывести цель, используя алгебраические выкладки? Ключ

к доказательству скрывается в понимании того, что левая часть уравнения в цели точно такая же, как левая часть второй посылки, но с добавлением дополнительного члена 2^{n+1} . Итак, давайте попробуем добавить 2^{n+1} к обеим сторонам второй посылки. Это дает нам

$$(2^0 + 2^1 + \dots + 2^n) + 2^{n+1} = (2^{n+1} - 1) + 2^{n+1},$$

или, другими словами,

$$2^0 + 2^1 + \dots + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1.$$

Это и есть цель!

Решение

Теорема. Для любого натурального числа n справедливо равенство $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$.

Доказательство. Используем математическую индукцию.

Базовый случай: приняв $n = 0$, мы получим $2^0 = 1 = 2^1 - 1$, что и требовалось доказать.

Шаг индукции: пусть n – произвольное натуральное число; предположим, что $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$. Тогда

$$\begin{aligned} 2^0 + 2^1 + \dots + 2^{n+1} &= (2^0 + 2^1 + \dots + 2^n) + 2^{n+1} \\ &= (2^{n+1} - 1) + 2^{n+1} \\ &= 2 \cdot 2^{n+1} - 1 \\ &= 2^{n+2} - 1. \end{aligned}$$

Убеждает ли вас доказательство в примере 6.1.1, что равенство $2^0 + 2^1 + \dots + 2^n = 2^{n+1} - 1$, которое мы в наброске доказательства назвали $P(n)$, истинно для всех натуральных чисел n ? Что ж, конечно, $P(0)$ истинно, поскольку мы проверили это напрямую в базовом случае доказательства. На шаге индукции мы показали, что $\forall n \in \mathbb{N}(P(n) \rightarrow P(n + 1))$, поэтому мы знаем, что для любого натурального числа n $P(n) \rightarrow P(n + 1)$. Например, подставляя $n = 0$, мы можем заключить, что $P(0) \rightarrow P(1)$. Но теперь мы знаем, что и $P(0)$, и $P(0) \rightarrow P(1)$ истинны, поэтому, применяя *modus ponens*, мы можем заключить, что $P(1)$ также истинно. Аналогично, подставляя $n = 1$ на шаге индукции, мы получаем $P(1) \rightarrow P(2)$, поэтому, применяя *modus ponens* к операторам $P(1)$ и $P(1) \rightarrow P(2)$, мы можем заключить, что $P(2)$ истинно. Полагая $n = 2$ на шаге индукции, мы получаем $P(2) \rightarrow P(3)$, так что по *modus ponens* $P(3)$ тоже истинно. Продолжая таким образом, вы увидите, что, многократно применяя шаг индукции, можно показать, что $P(n)$ должно быть истинным для каждого натурального числа n . Другими словами, доказательство действительно показывает, что $\forall n \in \mathbb{N} P(n)$.

Как мы видели в последнем примере, самой сложной частью доказательства с помощью математической индукции обычно является шаг индукции, на котором вы должны доказать утверждение $\forall n \in \mathbb{N}(P(n) \rightarrow P(n + 1))$. Обычно лучше всего делать это, принимая за n произвольное натуральное число,

предполагая, что $P(n)$ истинно, а затем доказывая, что $P(n + 1)$ тоже истинно. Предположение, что $P(n)$ истинно, иногда называют *предположением индукции*, и ключ к доказательству обычно кроется в том, чтобы установить связь между предположением индукции $P(n)$ и целью $P(n + 1)$.

Вот еще один пример доказательства с помощью математической индукции.

Пример 6.1.2. Докажите, что $\forall n \in \mathbb{N} (\exists | (n^3 - n))$.

Стратегия доказательства

Как обычно, базовый вариант проверить несложно. Подробности приведены в следующем доказательстве. Для шага индукции пусть n – произвольное натуральное число, и предположим, что $3 | (n^3 - n)$, и мы должны доказать, что $3 | ((n + 1)^3 - (n + 1))$. Используя определение делимости, мы можем записать нашу ситуацию следующим образом:

Посылки	Цель
$n \in \mathbb{N}$	$\exists j \in \mathbb{Z} (3j = (n + 1)^3 - (n + 1))$
$\exists k \in \mathbb{Z} (3k = n^3 - n)$	

Вторая посылка – это предположение индукции, и нам нужно выяснить, как ее можно использовать для определения цели.

Согласно нашим методам работы с кванторами существования в доказательствах, лучше всего сначала использовать вторую посылку и обозначить за k конкретное целое число, такое что $3k = n^3 - n$. Чтобы завершить доказательство, нам нужно будет найти целое число j (вероятно, каким-то образом связанное с k) такое, что $3j = (n + 1)^3 - (n + 1)$. Мы развернем правую часть этого уравнения в поисках способа связать его с исходным уравнением $3k = n^3 - n$:

$$\begin{aligned} (n + 1)^3 - (n + 1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\ &= (n^3 - n) + 3n^2 + 3n \\ &= 3k + 3n^2 + 3n \\ &= 3(k + n^2 + n). \end{aligned}$$

Теперь должно быть ясно, что мы можем завершить доказательство, положив $j = k + n^2 + n$. Как и в аналогичных предыдущих доказательствах, мы не будем упоминать j в окончательном доказательстве.

Решение

Теорема. Для любого натурального числа n справедливо, что $3 | (n^3 - n)$.

Доказательство. Используем математическую индукцию.

Базовый случай: если $n = 0$, то $n^3 - n = 0 = 3 \cdot 0$, поэтому $3 | (n^3 - n)$.

Шаг индукции. Пусть n – произвольное натуральное число, и пусть $3 | (n^3 - n)$. Тогда мы можем выбрать такое целое число k , что $3k = n^3 - n$. Таким образом:

$$\begin{aligned}
 (n+1)^3 - (n+1) &= n^3 + 3n^2 + 3n + 1 - n - 1 \\
 &= (n^3 - n) + 3n^2 + 3n \\
 &= 3k + 3n^2 + 3n \\
 &= 3(k + n^2 + n).
 \end{aligned}$$

Поэтому $3 \mid ((n+1)^3 - (n+1))$, что и требовалось доказать.

Как только вы поймете принцип работы математической индукции, вы сможете понять доказательства, которые содержат некоторые вариации этого метода. Следующий пример иллюстрирует такую вариацию. В этом примере мы попытаемся выяснить, что больше: n^2 или 2^n . Давайте попробуем несколько значений n :

n	n^2	2^n	Что больше?
0	0	1	2^n
1	1	2	2^n
2	4	4	равны
3	9	8	n^2
4	16	16	равны
5	25	32	2^n
6	36	64	2^n

Поначалу это была гонка «нос в нос», но начиная с $n = 5$ похоже, что 2^n решительно опережает n^2 . Можем ли мы доказать, что n^2 всегда будет впереди при больших значениях n ?

Пример 6.1.3. Докажите, что $\forall n \geq 5 (2^n > n^2)$.

Стратегия доказательства

Нас интересует только доказательство неравенства $2^n > n^2$ для $n \geq 5$, поэтому базовым случаем нашего доказательства не может служить $n = 0$. Вместо этого в качестве базового случая следует использовать $n = 5$. После того как мы проверим выполнение неравенства при $n = 5$, шаг индукции покажет, что неравенство должно сохраняться, если, начиная с $n = 5$, многократно прибавлять 1 к n . Иными словами, неравенство должно выполняться для $n = 6, 7, 8, \dots$. После этого мы сможем заключить, что неравенство выполняется для всех $n \geq 5$.

Базовый случай $n = 5$ уже проверен в таблице. Для шага индукции пусть $n \geq 5$ произвольно, предположим, что $2^n > n^2$, и попытаемся доказать, что $2^{n+1} > (n+1)^2$. Как мы можем связать предположение индукции с целью? Возможно, самое простое соотношение включает левые части двух неравенств: $2^{n+1} = 2 \cdot 2^n$. Таким образом, умножая обе части предположения индукции $2^n > n^2$ на 2, мы можем заключить, что $2^{n+1} > 2n^2$. Теперь сравните это неравенство с целью $2^{n+1} > (n+1)^2$. Если бы мы могли доказать, что $2n^2 \geq (n+1)^2$, то достигли бы цели доказательства. Так что давайте пока забудем об исходной цели и посмотрим, сможем ли мы доказать, что $2n^2 \geq (n+1)^2$.

Возводя в квадрат правую часть новой цели, мы видим, что необходимо доказать истинность неравенства $2n^2 \geq n^2 + 2n + 1$, или, другими словами, $n^2 \geq 2n + 1$. Доказать это несложно: поскольку мы предположили, что $n \geq 5$, отсюда следует, что $n^2 \geq 5n = 2n + 3n > 2n + 1$.

Решение

Теорема. Для любого натурального числа $n \geq 5$ справедливо неравенство $2^n > n^2$.

Доказательство. Используем математическую индукцию.

Базовый случай: когда $n = 5$, мы имеем $2^5 = 32 > 25 = 5^2$.

Шаг индукции: возьмем произвольное число $n \geq 5$ и предположим, что $2^n > n^2$. Далее

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &> 2n^2 && \text{(предположение индукции)} \\ &= n^2 + n^2 \\ &\geq n^2 + 5n && \text{(поскольку } n \geq 5\text{)} \\ &= n^2 + 2n + 3n \\ &> n^2 + 2n + 1 = (n + 1)^2. \end{aligned}$$

Упражнения

- *1. Докажите, что для всех $n \in \mathbb{N}$ справедливо $0 + 1 + 2 + \dots + n = n(n + 1)/2$.
2. Докажите, что для всех $n \in \mathbb{N}$ справедливо $0^2 + 1^2 + 2^2 + \dots + n^2 = n(n + 1)(2n + 1)/6$.
- *3. Докажите, что для всех $n \in \mathbb{N}$ справедливо $0^3 + 1^3 + 2^3 + \dots + n^3 = [n(n + 1)/2]^2$.
4. Найдите формулу для $1 + 3 + 5 + \dots + (2n - 1)$, где $n \geq 1$, и докажите, что ваша формула верна. (Подсказка: сначала попробуйте несколько конкретных значений n и найдите закономерность.)
5. Докажите, что для всех $n \in \mathbb{N}$ справедливо $0 \cdot 1 + 1 \cdot 2 + 2 \cdot 3 + \dots + n(n + 1) = n(n + 1)(n + 2)/3$.
6. Найдите формулу для $0 \cdot 1 \cdot 2 + 1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \dots + n(n + 1)(n + 2)$ для $n \in \mathbb{N}$ и докажите, что ваша формула верна. (Подсказка: сравните это упражнение с упражнениями 1 и 5 и попытайтесь угадать формулу.)
- *7. Найдите формулу для $3^0 + 3^1 + 3^2 + \dots + 3^n$ для $n \geq 0$ и докажите, что ваша формула верна. (Подсказка: попробуйте угадать формулу, основываясь на примере 6.1.1. Затем попробуйте различные значения n и при необходимости скорректируйте свое предположение.)
8. Докажите, что для всех $n \geq 1$ справедливо равенство

$$1 - \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{2n-1} - \frac{1}{2n} = \frac{1}{n+1} + \frac{1}{n+2} + \frac{1}{n+3} + \dots + \frac{1}{2n}.$$

9. (а) Докажите, что для всех $n \in \mathbb{N}$ верно утверждение $2 | (n^2 + n)$.
 (б) Докажите, что для всех $n \in \mathbb{N}$ верно утверждение $6 | (n^3 - n)$.
10. Докажите, что для всех $n \in \mathbb{N}$ верно утверждение $64 | (9^n - 8n - 1)$.
11. Докажите, что для всех $n \in \mathbb{N}$ верно утверждение $9 | (4^n + 6n - 1)$.
12. (а) Докажите, что для всех $n \in \mathbb{N}$ значение $7^n - 5^n$ четно.
 (б) Докажите, что для всех $n \in \mathbb{N}$ верно утверждение $24 | (2 \cdot 7^n - 3 \cdot 5^n + 1)$.
13. Докажите, что для всех целых чисел a и b и всех $n \in \mathbb{N}$ верно утверждение $(a - b) | (a^n - b^n)$. (Подсказка: примите за a и b произвольные целые числа, а затем докажите по индукции, что $\forall n \in \mathbb{N} [(a - b) | (an - bn)]$. На шаге индукции вы должны связать $a^{n+1} - b^{n+1}$ с $a^n - b^n$. Возможно, вам будет полезно начать с решения следующего уравнения: $a^{n+1} - b^{n+1} = a(a^n - b^n) + ?$.)
14. Докажите, что для всех целых чисел a и b и всех $n \in \mathbb{N}$ верно утверждение $(a + b) | (a^{2n+1} + b^{2n+1})$.
15. Докажите, что для всех $n \geq 10$, $2^n > n^5$.
16. (а) Докажите, что для всех $n \in \mathbb{N}$ либо n четно, либо n нечетно, но не оба сразу.
 (б) Докажите, что, как утверждается в разделе 3.4, каждое целое число либо четное, либо нечетное, но не то и другое одновременно. (Подсказка: чтобы доказать, что отрицательное целое число n является четным или нечетным, но не тем и другим сразу, примените часть (а) к $-n$.)
17. Докажите, что для всех $n \geq 1$, $2 \cdot 2^1 + 3 \cdot 2^2 + 4 \cdot 2^3 + \dots + (n + 1)2^n = n2^{n+1}$.
18. (а) Где ошибка в следующем доказательстве того, что для каждого $n \in \mathbb{N}$ верно утверждение $1 \cdot 3^0 + 3 \cdot 3^1 + 5 \cdot 3^2 + \dots + (2n + 1)3^n = n3^{n+1}$?
Доказательство. Используем математическую индукцию. Пусть n – произвольное натуральное число, и предположим, что $1 \cdot 3^0 + 3 \cdot 3^1 + 5 \cdot 3^2 + \dots + (2n + 1)3^n = n3^{n+1}$.
 Далее
- $$\begin{aligned} 1 \cdot 3^0 + 3 \cdot 3^1 + 5 \cdot 3^2 + \dots + (2n + 1)3^n + (2n + 3)3^{n+1} \\ = n3^{n+1} + (2n + 3)3^{n+1} \\ = (3n + 3)3^{n+1} \\ = (n + 1)3^{n+2}, \end{aligned}$$
- что и требовалось доказать.
- (б) Найдите формулу для $1 \cdot 3^0 + 3 \cdot 3^1 + 5 \cdot 3^2 + \dots + (2n + 1)3^n$ и докажите, что ваша формула верна.
19. Предположим, что a – действительное число и $a < 0$. Докажите, что для всех $n \in \mathbb{N}$ если n четное, то $a^n > 0$, а если n нечетное, то $a^n < 0$.
20. Предположим, что a и b – действительные числа и $0 < a < b$.
 (а) Докажите, что для всех $n \geq 1$ справедливо неравенство $0 < a^n < b^n$. (Обратите внимание, что это обобщение примера 3.1.2.)

- (b) Докажите, что для всех $n \geq 2$ верно неравенство $0 < \sqrt[n]{a} < \sqrt[n]{b}$.
 (c) Докажите, что для всех $n \geq 1$ верно неравенство $ab^n + ba^n < a^{n+1} + b^{n+1}$.
 (d) Докажите, что для всех $n \geq 2$ верно неравенство

$$\left(\frac{a+b}{2}\right)^n < \frac{a^n + b^n}{2}.$$

6.2. ДОПОЛНИТЕЛЬНЫЕ ПРИМЕРЫ

Мы использовали математическую индукцию в последнем разделе как метод доказательства того, что все натуральные числа обладают некоторыми свойствами. Однако приложения математической индукции выходят далеко за рамки работы с натуральными числами. В этом разделе мы рассмотрим несколько примеров доказательств с помощью математической индукции, которые иллюстрируют широкий спектр ее применения.

Пример 6.2.1. Предположим, что R – частичный порядок на множестве A . Докажите, что каждое конечное непустое множество $B \subseteq A$ имеет R -минимальный элемент.

Стратегия доказательства

Сначала вы можете подумать, что математическая индукция не подходит для этого доказательства, потому что цель, похоже, не имеет формы $\forall n \in \mathbb{N} P(n)$. На самом деле в цели вообще не упоминаются натуральные числа! Но вы увидите, что натуральные числа имеют отношение к этой задаче, когда поймете, что поскольку множество B конечное и непустое, оно имеет n элементов для некоторого $n \in \mathbb{N}$, где $n \geq 1$. (Мы дадим более точное определение количества элементов в конечном множестве в главе 8. На данный момент достаточно интуитивного понимания этой концепции.) Следовательно, цель имеет вид $\forall n \geq 1 \forall B \subseteq A (B \text{ имеет } n \text{ элементов} \rightarrow B \text{ имеет минимальный элемент})$. Теперь мы можем использовать индукцию, чтобы доказать это утверждение.

В базовом случае у нас будет $n = 1$, поэтому мы должны доказать, что если множество B имеет один элемент, то оно имеет минимальный элемент. Легко убедиться, что в этом случае один элемент B должен быть минимальным.

Для шага индукции возьмем произвольный элемент $n \geq 1$, предположим, что $\forall B \subseteq A (B \text{ имеет } n \text{ элементов} \rightarrow B \text{ имеет минимальный элемент})$, и попытаемся доказать, что $\forall B \subseteq A (B \text{ имеет } n + 1 \text{ элемент} \rightarrow B \text{ имеет минимальный элемент})$. Руководствуясь формой цели, обозначим за B произвольное подмножество A , предположим, что B имеет $n + 1$ элемент, и попытаемся доказать, что B имеет минимальный элемент.

Как мы можем использовать предположение индукции для достижения нашей цели? Предположение говорит нам, что если бы у нас нашлось подмножество A , включающее n элементов, то оно имело бы минимальный элемент. Чтобы применить это знание, нам нужно найти подмножество A , включающее n элементов. Наше произвольное множество B является подмножеством A , и мы предположили, что оно имеет $n + 1$ элемент. Таким образом, самый

простой способ создать подмножество A , включающее n элементов, – это удалить один элемент из B . Пока не ясно, к чему приведет это рассуждение, но, по-видимому, это самый простой способ использовать предположение индукции. Давайте попробуем.

Пусть b – произвольный элемент из B , и пусть $B' = B \setminus \{b\}$. Тогда B' является подмножеством A , состоящего из n элементов, и поэтому согласно предположению индукции B' имеет минимальный элемент. Это экзистенциальное утверждение, поэтому мы немедленно вводим новую переменную, скажем c , для обозначения минимального элемента B' .

Наша цель – доказать, что B имеет минимальный элемент, что также является экзистенциальным утверждением, поэтому мы должны попытаться найти минимальный элемент B . В данный момент нам известны только два элемента, b и c , поэтому мы, вероятно, должны попытаться доказать, что один из них является минимальным элементом B . Но какой? Это зависит от того, будет ли один из элементов меньше другого в соответствии с частичным порядком R . Это говорит о том, что нам, скорее всего, придется использовать доказательство по случаям. В нашем доказательстве мы используем случаи bRc и $\neg bRc$. В первом случае мы доказываем, что b является минимальным элементом B , а во втором случае мы доказываем, что c является минимальным элементом B . Отметим, что заявление о том, что какой-то элемент является минимальным элементом B , является отрицательным утверждением, поэтому в обоих случаях мы используем доказательство от противного.

Решение

Теорема. Предположим, что R – частичный порядок на множестве A . Тогда каждое конечное непустое множество $B \subseteq A$ имеет R -минимальный элемент.

Доказательство. Мы покажем по индукции, что для любого натурального числа $n \geq 1$ каждое подмножество A , включающее n элементов, имеет минимальный элемент.

Базовый случай: $n = 1$. Предположим, что $B \subseteq A$ и B имеет один элемент. Тогда $B = \{b\}$ для некоторого $b \in A$. Очевидно $\neg \exists x \in B (x \neq b)$, поэтому, безусловно, $\neg \exists x \in B (xRb \wedge x \neq b)$. Таким образом, b минимально.

Шаг индукции: примем, что $n \geq 1$, и предположим, что каждое подмножество A , включающее n элементов, имеет минимальный элемент. Пусть теперь B – произвольное подмножество A , включающее $n + 1$ элементов. Пусть b – любой элемент B , и пусть $B' = B \setminus \{b\}$, подмножество A , включающее n элементов. Согласно предположению индукции мы можем выбрать минимальный элемент $c \in B'$.

Случай 1. bRc . Мы утверждаем, что b – минимальный элемент B . Чтобы понять, почему, давайте предположим, что это не так. Тогда мы можем выбрать некоторый $x \in B$ такой, что xRb и $x \neq b$. Поскольку $x \neq b$, то $x \in B'$. Кроме того, поскольку xRb и bRc , из транзитивности R следует, что xRc . Таким образом, поскольку c – минимальный элемент B' , мы должны иметь $x = c$. Но тогда, поскольку xRb , у нас есть cRb , а также bRc , из антисимметрии R следует, что $b = c$. Это явно невозможно, так как $c \in B' = B \setminus \{b\}$. Таким образом, b должен быть минимальным элементом B .

Случай 2. $\neg bRc$. В этом случае мы утверждаем, что c – минимальный элемент B . Чтобы понять, почему, давайте предположим, что это не так. Тогда мы можем выбрать некоторый $x \in B$ такой, что xRc и $x \neq c$. Поскольку c – минимальный элемент B' , не может быть $x \in B'$, поэтому остается лишь один возможный вариант – $x = b$. Но тогда, поскольку xRc , мы должны иметь bRc , что противоречит нашему предположению о $\neg bRc$. Таким образом, c – минимальный элемент множества B .

Обратите внимание, что бесконечное подмножество частично упорядоченного множества не обязательно должно иметь минимальный элемент, как мы видели в части 1 примера 4.4.5. Поэтому в нашей последней теореме понадобилось утверждение о конечности B . Эту теорему можно использовать для доказательства еще одного интересного факта о частичных порядках, опять же с помощью математической индукции.

Пример 6.2.2. Предположим, что A – конечное множество, а R – частичный порядок на A . Докажите, что R можно расширить до полного порядка на A . Другими словами, докажите, что существует полный порядок T на A такой, что $R \subseteq T$.

Стратегия доказательства

Мы рассмотрим лишь общую схему доказательства, оставив многие детали в качестве упражнений. Идея состоит в том, чтобы доказать по индукции, что $\forall n \in \mathbb{N} \forall A \forall R [(A \text{ имеет } n \text{ элементов и } R \text{ – частичный порядок на } A) \rightarrow \exists T (T \text{ – полный порядок на } A \text{ и } R \subseteq T)]$. Шаг индукции в этом доказательстве аналогичен таковому в последнем примере. Если R является частичным порядком на множестве A , включающем $n + 1$ элементов, то мы удаляем один элемент – допустим, a из множества A – и применяем предположение индукции к оставшемуся множеству $A' = A \setminus \{a\}$. Это даст нам общий порядок T' на A' , и для завершения доказательства мы должны каким-то образом превратить его в общий порядок T на A , такой, что $R \subseteq T$. Отношение T' уже говорит нам, как сравнивать любые два элемента множества A' , но не говорит, как сравнивать a с элементами A' . Мы должны найти ответ на этот вопрос, чтобы определить T , и основная трудность на этом этапе доказательства состоит в том, что мы должны принять это решение таким образом, чтобы в итоге получить $R \subseteq T$. Наше решение этой проблемы прежде всего опирается на тщательный выбор. Мы выбираем a как R -минимальный элемент A , а затем, когда определяем T , мы делаем элемент a меньшим в порядке T , чем каждый элемент A' . Мы используем теорему из последнего примера с условием $B = A$, чтобы гарантировать, что A имеет R -минимальный элемент.

Решение

Теорема. Пусть A – конечное множество и R – частичный порядок на A . Тогда существует полный порядок T на A такой, что $R \subseteq T$.

Доказательство. Мы покажем индукцией по n , что любой частичный порядок на множестве из n элементов может быть расширен до полного порядка. Ясно, что этого достаточно для доказательства теоремы.

Базовый случай: $n = 0$. Предположим, что R – частичный порядок на A и A имеет 0 элементов. Тогда ясно, что $A = R = \emptyset$. Легко проверить, что \emptyset – это полный порядок на A (пустота не противоречит никаким свойствам), так что мы преуспели с доказательством этой части.

Шаг индукции: пусть n – произвольное натуральное число. Предположим, что каждый частичный порядок на множестве из n элементов может быть расширен до полного порядка. Теперь предположим, что A имеет $n + 1$ элемент и R – частичный порядок на A . По теореме из последнего примера должен существовать некоторый $a \in A$ такой, что a является R -минимальным элементом A . Пусть $A' = A \setminus \{a\}$, и пусть $R' = R \cap (A' \times A')$. В упражнении 1 вас просят показать, что R' является частичным порядком на A' . По предположению индукции мы можем обозначить за T' полный порядок на A' такой, что $R' \subseteq T'$. Пусть теперь $T = T' \cup (\{a\} \times A)$. В упражнении 1 вас также просят показать, что T – это общий порядок на A и $R \subseteq T$, если требуется.

Теорема из последнего примера может быть распространена на частичные порядки на бесконечных множествах. Шаги в этом направлении см. в упражнении 19 в разделе 8.1.

Пример 6.2.3. Докажите, что для всех $n \geq 3$ если n различных точек на окружности соединены в последовательном порядке прямыми линиями, то внутренние углы полученного многоугольника в сумме составляют $(n - 2)180^\circ$.

Решение

На рис. 6.1 показан пример с $n = 4$. Мы не будем приводить стратегию отдельно для этого доказательства.

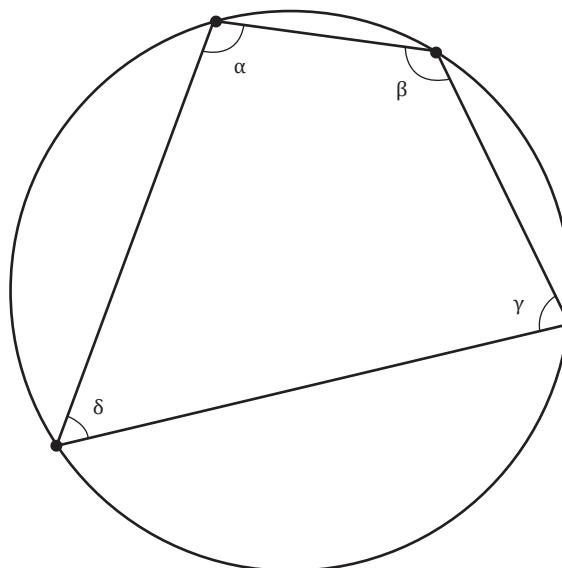


Рис. 6.1 ♦ $\alpha + \beta + \gamma + \delta = (4 - 2)180^\circ = 360^\circ$

Теорема. Для всех $n \geq 3$ если n различных точек на окружности соединены в последовательном порядке прямыми линиями, то внутренние углы полученного многоугольника в сумме составляют $(n - 2)180^\circ$.

Доказательство. Воспользуемся индукцией по n .

Базовый случай: предположим, что $n = 3$. Тогда многоугольник является треугольником, и хорошо известно, что внутренние углы треугольника в сумме составляют 180° .

Шаг индукции: пусть n – произвольное натуральное число, $n \geq 3$, и предположим, что утверждение истинно для n . Теперь рассмотрим многоугольник P , образованный соединением некоторых $n + 1$ различных точек A_1, A_2, \dots, A_{n+1} по кругу. Если мы пропустим последнюю точку A_{n+1} , то мы получим многоугольник P' только с n вершинами, и по предположению индукции внутренние углы этого многоугольника в сумме составляют $(n - 2)180^\circ$. Но теперь, как вы можете видеть на рис. 6.2, сумма внутренних углов P равна сумме внутренних углов P' плюс сумма внутренних углов треугольника $A_1A_nA_{n+1}$. Поскольку сумма внутренних углов треугольника равна 180° , мы можем сделать вывод, что сумма внутренних углов P равна

$$(n - 2)180^\circ + 180^\circ = ((n + 1) - 2)180^\circ,$$

что и требовалось доказать.

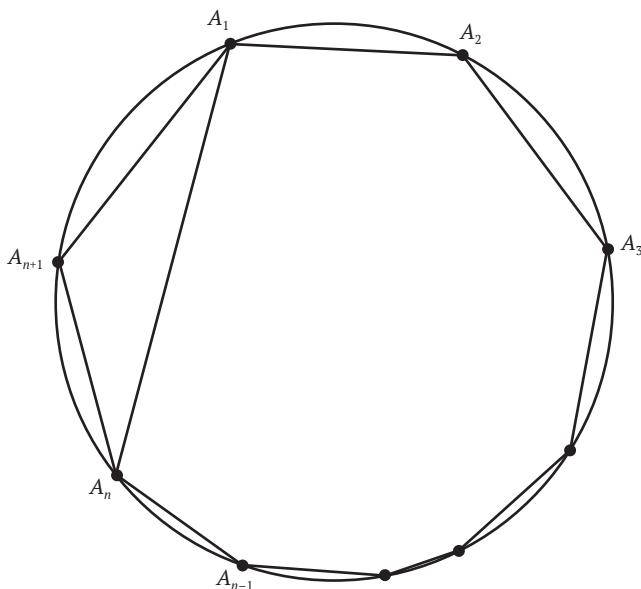
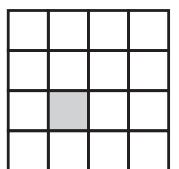


Рис. 6.2 ♦ Треугольник $A_1A_nA_{n+1}$ и многоугольник P

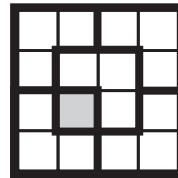
Пример 6.2.4. Докажите, что для любого положительного целого числа n квадратную сетку размером $2^n \times 2^n$, из которой удален один квадрат, можно покрыть L-образными плитками, которые выглядят следующим образом:

Стратегия доказательства

На рис. 6.3 показан пример для случая $n = 2$. В этом случае $2^n = 4$, поэтому у нас есть сетка 4×4 , а отсутствующий квадрат закрашен. Жирными линиями показано, как можно покрыть оставшиеся квадраты пятью плитками L-образной формы.



(a) Сетка 4×4 с одним
отсутствующим квадратом



(b) Сетка, покрытая
L-образными плитками

**Рис. 6.3 ♦ Покрытие сетки 4×4
с одним отсутствующим квадратом L-образными элементами**

Мы вновь будем применять в нашем доказательстве математическую индукцию, и поскольку нас интересуют только положительные значения n , базовым случаем будет $n = 1$. В этом случае у нас есть сетка 2×2 с одним отсутствующим квадратом, и ее, очевидно, можно покрыть одной L-образной плиткой. (Мысленно нарисуйте картинку.)

Для шага индукции мы принимаем за n произвольное положительное целое число и предполагаем, что сетку $2^n \times 2^n$ с любым отсутствующим квадратом можно покрыть L-образными плитками. Теперь предположим, что у нас есть сетка $2^{n+1} \times 2^{n+1}$ с одним отсутствующим квадратом. Чтобы использовать наше предположение индукции, мы должны каким-то образом связать ее с сеткой $2^n \times 2^n$. Поскольку $2^{n+1} = 2^n \cdot 2$, сетка $2^{n+1} \times 2^{n+1}$ вдвое шире и вдвое выше сетки $2^n \times 2^n$. Другими словами, разделив сетку $2^{n+1} \times 2^{n+1}$ пополам по горизонтали и вертикали, мы можем разделить ее на четыре «подсетки» $2^n \times 2^n$, как показано на рис. 6.4. Один удаленный квадрат будет расположен в одной из четырех подсеток; на рис. 6.4 он находится в правом верхнем углу.

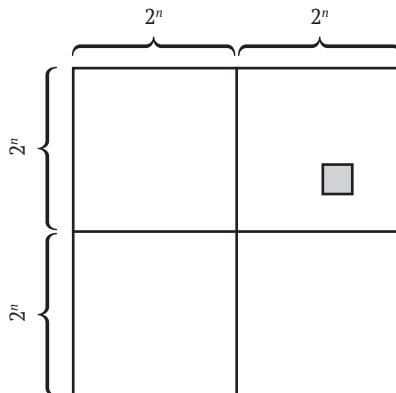


Рис. 6.4 ♦ Деление сетки $2^{n+1} \times 2^{n+1}$ на четыре подсетки $2^n \times 2^n$

Предположение индукции говорит нам, что можно покрыть верхнюю правую подсетку на рис. 6.4 L-образными плитками. Но как насчет трех остальных подсеток? Оказывается, есть хитрый способ разместить одну плитку на сетке, чтобы затем можно было использовать предположение индукции и показать, что остальные подсетки могут быть покрыты. Посмотрите, сможете ли вы придумать этот способ, прежде чем читать ответ в следующем доказательстве.

Решение

Теорема. Для любого положительного целого числа n квадратная сетка $2^n \times 2^n$ с одним отсутствующим квадратом может быть покрыта L-образными плитками.

Доказательство. Воспользуемся индукцией по n .

Базовый случай: предположим, что $n = 1$. Тогда мы имеем сетку 2×2 с одним отсутствующим квадратом, которую, очевидно, можно покрыть одной L-образной плиткой.

Шаг индукции: пусть n – произвольное положительное целое число, и предположим, что сетка $2^n \times 2^n$ с любым отсутствующим квадратом может быть покрыта L-образными плитками. Теперь рассмотрим сетку $2^{n+1} \times 2^{n+1}$ без одного квадрата. Разрежьте сетку пополам по вертикали и горизонтали, разделив ее на четыре подсетки размером $2^n \times 2^n$. Один удаленный квадрат относится к одной из этих подсеток, поэтому согласно предположению индукции остальная часть этой подсетки может быть покрыта L-образными плитками. Чтобы покрыть остальные три подсетки, сначала поместите одну L-образную плитку в центре так, чтобы она покрывала один квадрат из каждой из трех оставшихся подсеток, как показано на рис. 6.5. Оставшаяся покрытая область теперь содержит все квадраты, кроме одного в каждой подсетке, поэтому, применяя предположение индукции к каждой подсетке, мы видим, что эта область может быть покрыта плитками.

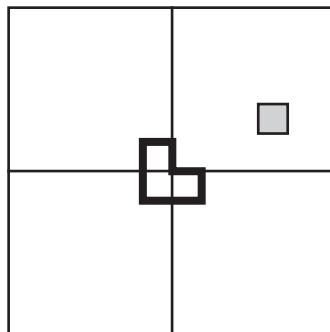


Рис. 6.5 ♦ Размещение L-образной плитки для последующего покрытия трех подсеток

Интересно отметить, что это доказательство можно использовать, чтобы выяснить, как размещать плитки на определенной сетке. Например, рассмотрим сетку 8×8 с одним отсутствующим квадратом, показанную на рис. 6.6.

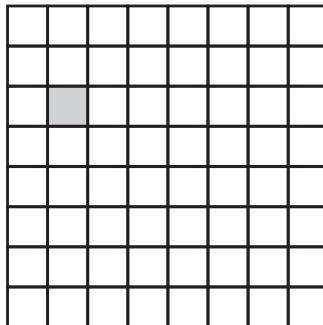


Рис. 6.6 ♦ Пример сетки 8×8
с одним отсутствующим квадратом

Согласно предыдущему доказательству, первым шагом в покрытии этой сетки плитками является ее разделение на четыре подсетки 4×4 и размещение одной плитки в центре, покрывая по одному квадрату от каждой подсетки, кроме верхнего левого угла. Это показано на рис. 6.7. Область, которую необходимо покрыть, теперь состоит из четырех подсеток 4×4 , в каждой из которых отсутствует один квадрат.

Как нам покрыть оставшиеся подсетки 4×4 ? Конечно, тем же методом! Например, давайте закроем подсетку в правом верхнем углу рис. 6.7. Нам нужно покрыть каждый квадрат этой подсетки, кроме левого нижнего угла, который уже был покрыт. Мы начинаем с того, что разрезаем ее на четыре подсетки 2×2 и кладем одну плитку в середину, как на рис. 6.8. Оставшаяся область, которую предстоит покрыть, состоит из четырех подсеток 2×2 , из каждой удален один квадрат. Каждую из них можно покрыть одной плиткой, завершив тем самым верхнюю правую подсетку на рис. 6.7.

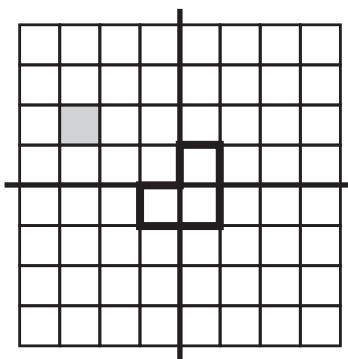


Рис. 6.7 ♦ Первый шаг
в покрытии оставшихся подсеток 4×4

Остальные три четверти рис. 6.7 заполняются аналогичной процедурой. Окончательное решение показано на рис. 6.9.

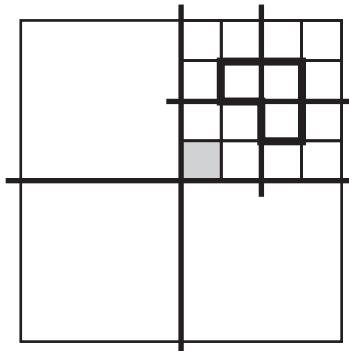
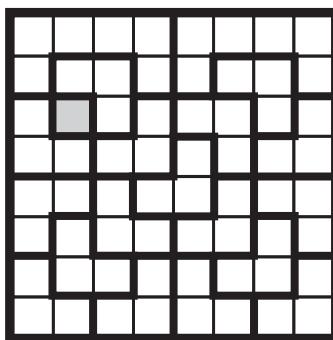
Рис. 6.8 ♦ Покрытие подсетки 2×2 

Рис. 6.9 ♦ Окончательное решение

Метод, который мы использовали при решении этой проблемы, является примером *рекурсивной* процедуры. Мы решили задачу для сетки 8×8 , разбив ее на четыре задачи с сеткой 4×4 . Чтобы решить каждую из них, мы разбили ее на четыре задачи 2×2 , каждую из которых было легко решить. Если бы мы начали с более крупной сетки, нам, возможно, пришлось бы повторить разделение много раз, прежде чем мы достигли бы простых задач 2×2 . Рекурсия и ее связь с математической индукцией являются предметом нашего следующего раздела.

Упражнения

- *1. Завершите доказательство в примере 6.2.2, выполнив следующие доказательства. (Здесь мы используем те же обозначения, что и в примере.)
 - (a) Докажите, что R' является частичным порядком на A' .
 - (b) Докажите, что T – полный порядок на A и $R \subseteq T$.
- 2. Предположим, что R – частичный порядок на множестве A , $B \subseteq A$ и B конечно. Докажите, что на A существует частичный порядок T такой, что $R \subseteq T$ и $\forall x \in B \forall y \in A (xTy \vee yTx)$. Отметим, что, в частности, если A конеч-

но, мы можем положить $B = A$, и тогда вывод означает, что T является полным порядком на A . Таким образом, это дает альтернативный подход к доказательству теоремы из примера 6.2.2. (Подсказка: используйте индукцию по количеству элементов в B . Для шага индукции предположим, что вывод верен для любого множества $B \subseteq A$, содержащего n элементов, и предположим, что B – подмножество A , включающее $n + 1$ элементов. Пусть b будет любой элемент из B , и пусть $B' = B \setminus \{b\}$, подмножество A , содержащее n элементов. Согласно предположению индукции, пусть T' – частичный порядок на A такой, что $R \subseteq T'$ и $\forall x \in B' \forall y \in A (xT'y \vee yT'x)$. Пусть теперь $A_1 = \{x \in A \mid (x, b) \in T'\}$ и $A_2 = A \setminus A_1$, и пусть $T = T' \cup (A_1 \times A_2)$. Докажите, что T обладает всеми необходимыми свойствами.)

3. Предположим, что R – полный порядок на множестве A . Докажите, что каждое конечное непустое множество $B \subseteq A$ имеет R -наименьший элемент и R -наибольший элемент.
- *4. (a) Предположим, что R – отношение на $\forall x \in A \forall y \in A (xRy \vee yRx)$. (Заметим, что отсюда следует рефлексивность R .) Докажите, что для любого конечного непустого множества $B \subseteq A$ существует $x \in B$ такой, что $\forall y \in B ((x, y) \in R \circ R)$. (Подсказка: воспользуйтесь примером 6.2.1.)
(b) Рассмотрим турнир, в котором каждый участник играет с каждым другим участником ровно один раз и один из них выигрывает. Мы говорим, что участник x является *великолепным*, если для каждого другого участника y либо x превосходит y , либо есть третий участник z такой, что x превосходит z , а z превосходит y . Докажите, что существует хотя бы один великолепный участник.
5. Для каждого $n \in \mathbb{N}$ положим $F_n = 2^{(2^n)} + 1$. (Эти числа называются числами Ферма в честь французского математика Пьера де Ферма (1601–1665). Ферма показал, что F_0, F_1, F_2, F_3 и F_4 – простые числа, и предположил, что все остальные числа такого рода тоже простые. Однако более 100 лет спустя Эйлер показал, что F_5 не является простым числом. Неизвестно, существует ли какое-либо $n > 4$, для которого F_n простое.)
Докажите, что для всех $n \geq 1$ справедливо равенство $F_n = (F_0 \cdot F_1 \cdot F_2 \cdots F_{n-1}) + 2$.
6. Докажите, что если $n \geq 1$ и a_1, a_2, \dots, a_n – любые действительные числа, то $|a_1 + a_2 + \dots + a_n| \leq |a_1| + |a_2| + \dots + |a_n|$. (Обратите внимание, что это обобщение неравенства треугольника; см. упражнение 13(с) раздела 3.5.1.)
(a) Докажите, что если a и b – положительные действительные числа, то $a/b + b/a \geq 2$. (Подсказка: начните с того, что $(a - b)^2 \geq 0$.)
(b) Предположим, что a, b и c – действительные числа и $0 < a \leq b \leq c$. Докажите, что $b/c + c/a - b/a \geq 1$. (Подсказка: начните с того факта, что $(c - a)(c - b) \geq 0$.)
(c) Докажите, что если $n \geq 2$ и a_1, a_2, \dots, a_n – действительные числа такие, что $0 < a_1 \leq a_2 \leq \dots \leq a_n$, то справедливо неравенство $a_1/a_2 + a_2/a_3 + \dots + a_{n-1}/a_n + a_n/a_1 \geq n$.
- *8. Если $n \geq 2$ и a_1, a_2, \dots, a_n – список положительных действительных чисел, тогда число $(a_1 + a_2 + \dots + a_n)/n$ называется *средним арифметическим*

чисел a_1, a_2, \dots, a_n , а число $\sqrt[n]{a_1 a_2 \dots a_n}$ – *средним геометрическим*. В этом упражнении вы докажете *неравенство среднего арифметического и среднего геометрического*, согласно которому среднее арифметическое всегда не меньше среднего геометрического.

- Докажите, что неравенство среднего арифметического и среднего геометрического выполняется для списков чисел длины 2. Другими словами, докажите, что для всех положительных действительных чисел a и b справедливо неравенство $(a + b)/2 \geq \sqrt{ab}$.
- Докажите, что неравенство среднего арифметического и среднего геометрического выполняется для любого списка чисел, длина которого является степенью 2. Другими словами, докажите, что для всех $n \geq 1$ если a_1, a_2, \dots, a_{2^n} – список положительных действительных чисел, то

$$\frac{a_1 + a_2 + \dots + a_{2^n}}{2^n} \geq \sqrt[2^n]{a_1 a_2 \dots a_{2^n}}.$$

- Предположим, что $n_0 \geq 2$ и неравенство среднего арифметического и среднего геометрического не выполняется для некоторого списка длины n_0 . Другими словами, существуют положительные действительные числа a_1, a_2, \dots, a_{n_0} такие, что

$$\frac{a_1 + a_2 + \dots + a_{n_0}}{n_0} < \sqrt[n_0]{a_1 a_2 \dots a_{n_0}}.$$

Докажите, что для всех $n \geq n_0$ неравенство среднего арифметического и среднего геометрического не выполняется для некоторого списка длины n .

- Докажите, что неравенство среднего арифметического и среднего геометрического всегда выполняется.
- Докажите, что если $n \geq 2$ и a_1, a_2, \dots, a_n – список положительных действительных чисел, то выполняется неравенство

$$\frac{\frac{n}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_n}}}{n} \leq \sqrt[n]{a_1 a_2 \dots a_n}.$$

(Подсказка: воспользуйтесь решением уравнения 8. Число в левой части неравенства выше называется *гармоническим средним* для чисел a_1, a_2, \dots, a_n)

- Докажите, что если a_1, a_2, b_1 и b_2 – действительные числа, причем $a_1 \leq a_2$ и $b_1 \leq b_2$, то $a_1 b_2 + a_2 b_1 \leq a_1 b_1 + a_2 b_2$.
- Предположим, что n – натуральное число, a_1, a_2, \dots, a_n и b_1, b_2, \dots, b_n – действительные числа, $a_1 \leq a_2 \leq \dots \leq a_n, b_1 \leq b_2 \leq \dots \leq b_n$, и f – взаимно однозначная сюръективная функция от $\{1, 2, \dots, n\}$ к $\{1, 2, \dots, n\}$. Докажите, что $a_1 b_{f(1)} + a_2 b_{f(2)} + \dots + a_n b_{f(n)} \leq a_1 b_1 + a_2 b_2 + \dots + a_n b_n$. (Этот факт известен как *неравенство перестановки*.)

11. Докажите, что для любого множества A если A имеет n элементов, то $\mathcal{P}(A)$ имеет $2n$ элементов.
12. Если A – множество, пусть $\mathcal{P}_2(A)$ – множество всех подмножеств A , которые имеют ровно два элемента. Докажите, что для любого множества A если A имеет n элементов, то $\mathcal{P}_2(A)$ имеет $n(n - 1)/2$ элементов. (Подсказка: см. решение упражнения 11.)
13. Предположим, что n – натуральное число. Равносторонний треугольник разрезается на $4n$ конгруэнтных равносторонних треугольников равносторонними отрезками, параллельными сторонам треугольника, и удаляется один угол. (На рис. 6.10 показан пример для случая $n = 2$.) Покажите, что оставшуюся площадь можно покрыть трапециевидной плиткой, например $\Delta\Delta$.

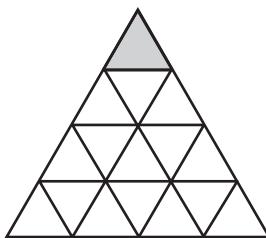


Рис. 6.10 ♦ Деление равностороннего треугольника на $4n$ конгруэнтных равносторонних треугольников (здесь $n = 2$)

14. Пусть n – натуральное число. Предположим, что n хорд нарисованы по кругу таким образом, что каждая хорда пересекается друг с другом, но никакие три не пересекаются в одной точке. Докажите, что хорды разрезают окружность на $(n^2 + n + 2)/2$ областей. (На рис. 6.11 показан пример для случая $n = 4$. Обратите внимание, что на этом рисунке есть $(4^2 + 4 + 2)/2 = 11$ регионов.)

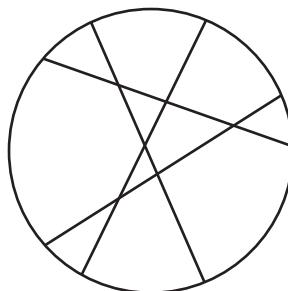


Рис. 6.11 ♦ Деление круга хордами, когда никакие три из них не пересекаются в одной точке (здесь $n = 4$)

15. Пусть n – положительное целое число, и предположим, что n хорд нарисованы по кругу произвольным образом, разрезая круг на несколько областей a . Докажите, что области можно раскрасить двумя цветами таким образом, что соседние области (то есть области, имеющие общую границу) имеют разные цвета. (На рис. 6.12 показан пример для случая $n = 4$.)

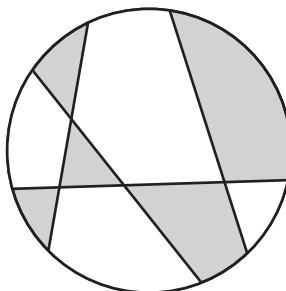


Рис. 6.12 ♦ Пример раскраски соседних областей для случая $n = 4$

16. Докажите, что для любого конечного множества A и любой функции $f: A \rightarrow A$ если f взаимно однозначна, то она сюръективна. (Подсказка: используйте индукцию по количеству элементов в A . Для шага индукции предположим, что вывод справедлив для любого множества A , содержащего n элементов, и предположим, что A имеет $n + 1$ элементов и $f: A \rightarrow A$. Предположим, что f является взаимно однозначной, но не сюръективной. Тогда существует некоторый элемент $a \in A$ такой, что $a \notin \text{Ran}(f)$. Пусть $A' = A \setminus \{a\}$ и $f' = f \cap (A' \times A')$. Покажите, что $f': A' \rightarrow A'$, f' взаимно однозначна и не сюръективна, что противоречит предположению индукции.)
17. Где ошибка в следующем доказательстве того, что если $A \subseteq \mathbb{N}$ и $0 \in A$, то $A = \mathbb{N}$?

Доказательство. Докажем по индукции, что $\forall n \in \mathbb{N} (n \in A)$.

Базовый случай: если $n = 0$, то по определению $n \in A$.

Шаг индукции: возьмем произвольный элемент $n \in \mathbb{N}$ и предположим, что $n \in A$. Поскольку n произвольно, отсюда следует, что каждое натуральное число является элементом A и, следовательно, в частности, $n + 1 \in A$.

18. Предположим, что $f: \mathbb{R} \rightarrow \mathbb{R}$. Где ошибка в следующем доказательстве того, что для любого конечного непустого множества $A \subseteq \mathbb{R}$ существует действительное число c такое, что $\forall x \in A (f(x) = c)$?

Доказательство. Мы докажем по индукции, что для любого $n > 1$ если A – любое подмножество \mathbb{R} с n элементами, то $\exists c \in \mathbb{R} \forall x \in A (f(x) = c)$.

Базовый случай: $n = 1$. Предположим, что $A \subseteq \mathbb{R}$ и A содержит один элемент. Тогда $A = \{a\}$ для некоторого $a \in \mathbb{R}$. Пусть $c = f(a)$. Тогда ясно, что $\forall x \in A (f(x) = c)$.

Шаг индукции: предположим, что $n > 1$, и для всех $A \subseteq \mathbb{R}$ если A содержит n элементов, то $\exists c \in \mathbb{R} \forall x \in A (f(x) = c)$. Теперь предположим, что $A \subseteq \mathbb{R}$ и A со-

держит $n + 1$ элементов. Пусть a_1 – любой элемент из A , и пусть $A_1 = A \setminus \{a_1\}$. Тогда в A_1 есть n элементов, поэтому по предположению индукции существует $c_1 \in \mathbb{R}$ такое, что $\forall x \in A_1 (f(x) = c_1)$. Если мы сможем показать, что $f(a_1) = c_1$, то успешно завершим доказательство, поскольку из этого следует, что $\forall x \in A (f(x) = c_1)$.

Пусть a_2 – элемент A , отличный от a_1 , и пусть $A_2 = A \setminus \{a_2\}$. Снова применяя предположение индукции, мы можем выбрать число $c_2 \in \mathbb{R}$ такое, что $\forall x \in A_2 (f(x) = c_2)$. Обратите внимание, что поскольку $a_1 \neq a_2$ и $a_1 \in A_2$, то $f(a_1) = c_2$. Теперь пусть a_3 будет элементом A , отличным от a_1 и a_2 . Тогда $a_3 \in A_1$ и $a_3 \in A_2$, поэтому $f(a_3) = c_1$ и $f(a_3) = c_2$. Следовательно, $c_1 = c_2$, поэтому $f(a_1) = c_1$, что нам и требовалось.

6.3. РЕКУРСИЯ

В главе 3 мы научились доказывать утверждения вида $\forall n P(n)$, присваивая n произвольное значение и доказывая $P(n)$. В этой главе мы изучили другой метод доказательства таких утверждений, когда n может охватывать все натуральные числа: доказать $P(0)$, а затем доказать, что для любого натурального числа n если $P(n)$ истинно, то и $P(n + 1)$ тоже истинно. После того как доказаны эти утверждения, можно пройти все натуральные числа по порядку и убедиться, что P должно быть истинным для каждого из них.

Воспользовавшись этой идеей, мы можем представить новый способ определения функций. В главе 5 мы обычно определяли функцию f , показывая, как вычислить $f(n)$ для любого n в области определения f . Если область определения f представляет собой множество всех натуральных чисел, альтернативным методом определения f было бы показать, что представляет из себя $f(0)$, а затем показать, как следует вычислять $f(n + 1)$, если мы уже знаем значение $f(n)$ для любого натурального числа n . Такое определение позволило бы нам перебрать все натуральные числа, чтобы вычислить отображение каждого из них относительно f .

Например, мы можем использовать следующие уравнения для описания функции f с областью определения \mathbb{N} :

$$f(0) = 1;$$

для любого $n \in \mathbb{N}$ справедливо равенство $f(n + 1) = (n + 1) \cdot f(n)$.

Второе уравнение говорит нам, как вычислить $f(n + 1)$, но только если мы уже знаем значение $f(n)$. Таким образом, хотя мы не можем использовать это уравнение, чтобы напрямую ответить, каково отображение любого числа относительно f , мы можем использовать его, чтобы перебрать все натуральные числа по порядку и вычислить их отображения.

Начнем с $f(0)$, которое, как мы знаем из первого уравнения, равно 1. Подставляя $n = 0$ во второе уравнение, мы видим, что $f(1) = 1 \cdot f(0) = 1 \cdot 1 = 1$, поэтому мы определили значение $f(1)$. Но теперь, когда мы знаем, что $f(1) = 1$, можем снова использовать второе уравнение для вычисления $f(2)$. Подставляя $n = 1$ во второе уравнение, мы находим, что $f(2) = 2 \cdot f(1) = 2 \cdot 1 = 2$. Анало-

гично, полагая $n = 2$ во втором уравнении, мы получаем $f(3) = 3 \cdot f(2) = 3 \cdot 2 = 6$. Продолжая действовать таким способом, мы можем вычислить $f(n)$ для любого натурального числа n . Таким образом, два уравнения действительно дают нам правило, которое определяет уникальное значение $f(n)$ для каждого натурального числа n , поэтому они определяют функцию f с областью определения \mathbb{N} . Определения такого типа называются *рекурсивными* определениями.

Иногда мы будем работать в обратном направлении, используя рекурсивное определение для нахождения функции. Например, предположим, что мы хотим вычислить $f(6)$, где f – это только что определенная функция. Согласно второму уравнению в определении функции, $f(6) = 6 \cdot f(5)$, поэтому для завершения вычисления мы должны вычислить $f(5)$. Снова используя второе уравнение, мы находим, что $f(5) = 5 \cdot f(4)$, поэтому должны вычислить $f(4)$. Продолжение этого способа дает нам следующую цепочку вычислений:

$$\begin{aligned}f(6) &= 6 \cdot f(5) \\&= 6 \cdot 5 \cdot f(4) \\&= 6 \cdot 5 \cdot 4 \cdot f(3) \\&= 6 \cdot 5 \cdot 4 \cdot 3 \cdot f(2) \\&= 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot f(1) \\&= 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot f(0) \\&= 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 \\&= 720.\end{aligned}$$

Возможно, теперь вы узнали функцию f . Для любого положительного целого числа n $f(n) = n \cdot (n - 1) \cdot (n - 2) \cdots 1$ и $f(0) = 1$. Число $f(n)$ называется *факториалом* от n и обозначается $n!$. (Напомним, что мы использовали это обозначение в доказательстве теоремы 3.7.3.) Например, $6! = 720$. Часто, если функция может быть записана в виде формулы с многоточием (...), то использования многоточия можно избежать, дав рекурсивное определение функции. С таким определением обычно легче работать.

Многие знакомые функции проще всего определить с помощью рекурсивных определений. Например, для любого числа a мы могли бы определить a^n посредством следующего рекурсивного определения:

$$\begin{aligned}a^0 &= 1; \\ \text{для любого } n \in \mathbb{N} \quad a^{n+1} &= a^n \cdot a.\end{aligned}$$

Используя это определение, мы бы вычислили a^4 следующим образом:

$$\begin{aligned}a^4 &= a^3 \cdot a \\&= a^2 \cdot a \cdot a \\&= a^1 \cdot a \cdot a \cdot a \\&= a^0 \cdot a \cdot a \cdot a \cdot a \\&= 1 \cdot a \cdot a \cdot a \cdot a.\end{aligned}$$

В качестве другого примера рассмотрим сумму $2^0 + 2^1 + 2^2 + \cdots + 2^n$, которая фигурирует в первом примере этой главы. Многоточие намекает, что мы могли бы использовать рекурсивное определение. Если мы примем $f(n) = 2^0 + 2^1 + 2^2 + \cdots + 2^n$, то заметим, что для каждого $n \in \mathbb{N}$ справедливо равенство

$f(n + 1) = 2^0 + 2^1 + 2^2 + \dots + 2^n + 2^{n+1} = f(n) + 2^{n+1}$. Таким образом, мы могли бы определить f рекурсивно следующим образом:

$$\begin{aligned}f(0) &= 2^0 = 1; \\ \text{для каждого } n \in \mathbb{N} \quad f(n + 1) &= f(n) + 2^{n+1}.\end{aligned}$$

Для проверки правильности этого определения давайте протестируем его на случае $n = 3$:

$$\begin{aligned}f(3) &= f(2) + 2^3 \\ &= f(1) + 2^2 + 2^3 \\ &= f(0) + 2^1 + 2^2 + 2^3 \\ &= 2^0 + 2^1 + 2^2 + 2^3 \\ &= 15.\end{aligned}$$

Суммы, подобные той, что приведена в последнем примере, встречаются достаточно часто, поэтому для них есть специальные обозначения. Если a_0, a_1, \dots, a_n – это список чисел, тогда сумма этих чисел записывается как $\sum_{i=0}^n a_i$. Эта запись читается как «сумма всех a_i при переборе значений i от 0 до n ». Например, мы можем использовать это обозначение для записи суммы в последнем примере:

$$\sum_{i=0}^n 2^i = 2^0 + 2^1 + 2^2 + \dots + 2^n.$$

В более общем случае если $n \geq m$, то

$$\sum_{i=m}^n a_i = a_m + a_{m+1} + a_{m+2} + \dots + a_n.$$

Например,

$$\sum_{i=3}^6 i^2 = 3^2 + 4^2 + 5^2 + 6^2 = 9 + 16 + 25 + 36 = 86.$$

Буква i в этих формулах является зависимой переменной и, следовательно, может быть заменена новой переменной без изменения смысла формулы.

А теперь давайте попробуем дать рекурсивное определение этой записи. Пусть m – произвольное целое число; проведем рекурсию по n . Так же, как базовый случай для доказательства индукции не обязательно должен быть $n = 0$, базой для рекурсивного определения также может быть число, отличное от 0. В этом случае нас интересуют только $n \geq m$, поэтому мы берем $n = m$ как базу для нашей рекурсии:

$$\sum_{i=m}^m a_i = a_m;$$

$$\text{для каждого } n \geq m \quad \sum_{i=m}^{n+1} a_i = \sum_{i=m}^n a_i + a_{n+1}.$$

Применив это определение к предыдущему примеру, мы получим

$$\begin{aligned}\sum_{i=3}^6 i^2 &= \sum_{i=3}^5 i^2 + 6^2 \\&= \sum_{i=3}^4 i^2 + 5^2 + 6^2 \\&= \sum_{i=3}^3 i^2 + 4^2 + 5^2 + 6^2 \\&= 3^2 + 4^2 + 5^2 + 6^2,\end{aligned}$$

чего мы и ожидали.

Очевидно, что индукция и рекурсия тесно связаны, поэтому неудивительно, что если понятие было определено рекурсией, то доказательства, связанные с этим понятием, часто лучше проводить с помощью индукции. Например, в разделе 6.1 мы рассмотрели некоторые доказательства по индукции, которые включали суммирование и возведение в степень, а теперь мы увидели, что суммирование и возведение в степень можно определить рекурсивно. Поскольку факториальную функцию также можно определить рекурсивно, доказательства с участием факториалов часто используют индукцию.

Пример 6.3.1. Докажите, что для любого $n \geq 4$ справедливо неравенство $n! > 2^n$.

Стратегия доказательства

Поскольку проблема включает факториал и возведение в степень, которые определены рекурсивно, индукция представляется хорошим методом для доказательства. Базовым случаем будет $n = 4$, и достаточно простой арифметики, чтобы проверить, что в этом случае неравенство истинно. Для шага индукции нашим предположением будет $n! > 2^n$, и мы должны доказать, что $(n+1)! > 2^{n+1}$. Конечно, очевидный способ связать предположение индукции с целью – это использовать рекурсивные определения факториала и возведения в степень, которые говорят нам, что $(n+1)! = (n+1) \cdot n!$ и $2^{n+1} = 2^n \cdot 2$. После того как мы подставим эти определения, все остальное становится довольно простым.

Решение

Теорема. Для каждого $n \geq 4$ $n! > 2^n$.

Доказательство. Применим математическую индукцию.

Базовый случай: когда $n = 4$, мы имеем $n! = 24 > 16 = 2^4$.

Шаг индукции: возьмем произвольное число $n \geq 4$ и предположим, что $n! > 2^n$. Далее

$$\begin{aligned}(n+1)! &= (n+1) \cdot n! \\&> (n+1) \cdot 2^n \quad (\text{предположение индукции}) \\&> 2 \cdot 2^n = 2^{n+1}.\end{aligned}$$

Пример 6.3.2. Докажите, что для любого действительного числа a и всех натуральных чисел m и n выполняется равенство $a^{m+n} = a^m \cdot a^n$.

Стратегия доказательства

Здесь есть три универсальных квантора, и мы будем рассматривать первые два иначе, чем третий. Пусть a и m произвольны; с помощью математической индукции докажем, что $\forall n \in \mathbb{N}(a^{m+n} = a^m \cdot a^n)$. Ключевым алгебраическим аспектом на этапе индукции будет формула $a^{n+1} = a^n \cdot a$ из рекурсивного определения возведения в степень.

Решение

Теорема. Для любого действительного числа a и всех натуральных чисел m и n выполняется равенство $a^{m+n} = a^m \cdot a^n$.

Доказательство. Пусть a – произвольное действительное число, а m – произвольное натуральное число. Переайдем теперь к индукции по n .

Базовый случай: когда $n = 0$, мы имеем $a^{m+0} = a^{m+0} = a^m = a^m \cdot 1 = a^m \cdot a^0 = a^m \cdot a^n$.

Индукционный шаг. Предположим, $a^{m+n} = a^m \cdot a^n$. Далее

$$\begin{aligned} a^{m+(n+1)} &= a^{(m+n)+1} \\ &= a^{m+n} \cdot a && \text{(определение возведения в степень)} \\ &= a^m \cdot a^n \cdot a && \text{(предположение индукции)} \\ &= a^m \cdot a^{n+1} && \text{(определение возведения в степень).} \end{aligned}$$

Пример 6.3.3. Последовательность чисел a_0, a_1, a_2, \dots рекурсивно определяется следующим образом:

$$a_0 = 0;$$

для каждого $n \in \mathbb{N}$ справедливо равенство $a_{n+1} = 2a_n + 1$.

Найдите формулу для a_n и докажите, что ваша формула верна.

Стратегия доказательства

Вероятно, неплохо было бы начать с вычисления первых нескольких членов последовательности. Мы уже знаем, что $a_0 = 0$, поэтому, подставляя $n = 0$ во второе уравнение, мы получаем $a_1 = 2a_0 + 1 = 0 + 1 = 1$. В свою очередь, подставляя $n = 1$, мы получаем $a_2 = 2a_1 + 1 = 2 + 1 = 3$. Продолжая таким образом, мы получаем следующую таблицу значений:

n	0	1	2	3	4	5	6	...
a_n	0	1	3	7	15	31	63	...

Прекрасно! Получаемые нами числа на единицу меньше степени 2. Пожалуй, что формула имеет вид $a_n = 2^n - 1$, но мы не можем быть уверены, что это так, пока не докажем это. К счастью, формулу довольно легко доказать по индукции.

Решение

Теорема. Если последовательность a_0, a_1, a_2, \dots определяется рекурсивным правилом, данным ранее, то для любого натурального числа n справедлива формула $a_n = 2^n - 1$.

Доказательство. Применим математическую индукцию.

Базовый случай: $a_0 = 0 = 2^0 - 1$.

Шаг индукции. Предположим, что $a_n = 2^n - 1$. Тогда

$$\begin{aligned} a_{n+1} &= 2a_n + 1 && (\text{определение } a_{n+1}) \\ &= 2(2^n - 1) + 1 && (\text{предположение индукции}) \\ &= 2^{n+1} - 2 + 1 = 2^{n+1} - 1. \end{aligned}$$

Закончим этот раздел довольно необычным примером. Мы докажем, что для любого действительного числа $x > -1$ и любого натурального числа n справедливо неравенство $(1+x)^n > nx$. Естественный способ продолжить – взять произвольный $x > -1$, а затем использовать индукцию по n . На этапе индукции мы предполагаем, что $(1+x)^n > nx$, а затем пытаемся доказать, что $(1+x)^{n+1} > (n+1)x$. Поскольку мы предположили, что $x > -1$, то получаем $1+x > 0$, поэтому можем умножить обе части предположения индукции $(1+x)^n > nx$ на $1+x$, чтобы получить

$$\begin{aligned} (1+x)^{n+1} &= (1+x)(1+x)^n \\ &> (1+x)nx \\ &= nx + nx^2. \end{aligned}$$

Но вывод, который нам нужен для шага индукции, следующий: $(1+x)^{n+1} > (n+1)x$, и пока не ясно, как сделать этот вывод из неравенства, которое мы вывели.

Нашим решением будет замена исходной задачи другой задачей, которая кажется более сложной, но на самом деле проще. Вместо прямого доказательства неравенства $(1+x)^n > nx$ мы докажем $(1+x)^n \geq 1+nx$, а затем заметим, что поскольку $1+nx > nx$, отсюда прямо следует, что $(1+x)^n > nx$. Вы можете подумать, что если у нас были трудности с доказательством $(1+x)^n > nx$, нам наверняка будет труднее доказать более сложное утверждение $(1+x)^n \geq 1+nx$. Но оказывается, что подход, который мы безуспешно пытались применить к исходной задаче, отлично работает с новой задачей!

Теорема 6.3.4. Для любого $x > -1$ и любого натурального числа n справедливо неравенство $(1+x)^n > nx$.

Доказательство. Возьмем произвольное значение $x > -1$ и докажем путем индукции, что для любого натурального числа n выполняется неравенство $(1+x)^n \geq 1+nx$, откуда прямо следует, что $(1+x)^n > nx$.

Базовый случай: если $n = 0$, то $(1+x)^0 = (1+x)^0 = 1 = 1+0 = 1+nx$.

Шаг индукции: предположим $(1+x)^n \geq 1+nx$. Далее

$$\begin{aligned}
 (1+x)^{n+1} &= (1+x)(1+x)^n \\
 &\geq (1+x)(1+nx) && \text{(предположение индукции)} \\
 &= 1+x+nx+nx^2 \\
 &\geq 1+(n+1)x && \text{(поскольку } nx^2 \geq 0\text{).}
 \end{aligned}$$

Упражнения

*1. Найдите формулу ряда, заданного суммой $\sum_{i=1}^n \frac{1}{i(i+1)}$, и докажите, что ваша формула верна.

2. Докажите, что для всех $n \geq 1$ выполняется равенство

$$\sum_{i=1}^n \frac{1}{i(i+1)(i+2)} = \frac{n^2 + 3n}{4(n+1)(n+2)}.$$

3. Докажите, что для всех $n \geq 2$ выполняется равенство

$$\sum_{i=2}^n \frac{1}{(i-1)(i+1)} = \frac{3n^2 - n - 2}{4n(n+1)}.$$

4. Докажите, что для всех $n \in \mathbb{N}$ выполняется равенство

$$\sum_{i=0}^n (2i+1)^2 = \frac{(n+1)(2n+1)(2n+3)}{3}.$$

5. Предположим, что r – действительное число и $r \neq 1$. Докажите, что для всех $n \in \mathbb{N}$ выполняется равенство

$$\sum_{i=0}^n r^i = \frac{r^{n+1} - 1}{r - 1}.$$

(Обратите внимание, что это упражнение обобщает пример 6.1.1 и упражнение 7 из раздела 6.1.)

*6. Докажите, что для всех $n \geq 1$ выполняется неравенство

$$\sum_{i=1}^n \frac{1}{i^2} \leq 2 - \frac{1}{n}.$$

7. (а) Предположим, что $a_0, a_1, a_2, \dots, a_n$ и $b_0, b_1, b_2, \dots, b_n$ – две последовательности действительных чисел. Докажите, что истинно равенство

$$\sum_{i=0}^n (a_i + b_i) = \sum_{i=0}^n a_i + \sum_{i=0}^n b_i.$$

- (b) Предположим, что c – действительное число и a_0, a_1, \dots, a_n – последовательность действительных чисел. Докажите, что истинно равенство

$$c \cdot \sum_{i=0}^n a_i = \sum_{i=0}^n (c \cdot a_i).$$

*8. Гармонические числа – это числа H_n , где $n \geq 1$, вычисляемые по формуле

$$H_n = \sum_{i=n}^n \frac{1}{i}.$$

- (a) Докажите, что для всех натуральных чисел n и m если $n \geq m \geq 1$, то $H_n - H_m \geq (n - m)/n$. (Подсказка: пусть m – произвольное натуральное число и $m \geq 1$. Проведите индукцию по n , приняв $n = m$ в качестве базового случая индукции.)
- (b) Докажите, что для всех $n \geq 0$ справедливо неравенство $H_{2^n} \geq 1 + n/2$.
- (c) (Для тех, кто изучал матанализ.) Покажите, что $\lim_{n \rightarrow \infty} H_n = \infty$, поэтому $\sum_{i=1}^{\infty} (1/i)$ расходится.
9. Пусть H_n определено, как в упражнении 8. Докажите, что для всех $n \geq 2$

$$\sum_{k=1}^{n-1} H_k = nH_n - n.$$

10. Найдите формулу для $\sum_{i=1}^n (i \cdot (i!))$ и докажите, что она верна.
11. Найдите формулу для $\sum_{i=0}^n (i/(i+1)!)$ и докажите, что она верна.
12. (a) Докажите, что для всех $n \in \mathbb{N}$ выполняется неравенство $2^n > n$.
- (b) Докажите, что для всех $n \geq 9$ выполняется неравенство $n! \geq (2^n)^2$.
- (c) Докажите, что для всех $n \in \mathbb{N}$ выполняется неравенство $n! \leq 2^{(n^2)}$.
13. Предположим, что k – натуральное число.
- (a) Докажите, что для всех $n \in \mathbb{N}$ выполняется неравенство $(k^2 + n)! \geq k^{2n}$.
- (b) Докажите, что для всех $n \geq 2k^2$ выполняется неравенство $n! \geq k^n$. (Подсказка: используйте индукцию, а для выбора базового случая используйте часть (a). Обратите внимание, что на языке упражнения 19 раздела 5.1 это означает, что если $f(n) = k^n$ и $g(n) = n!$, то $f \in O(g)$.)
14. Докажите, что для любого действительного числа a и всех натуральных чисел m и n выполняется равенство $(a^m)^n = a^{mn}$.
15. Последовательность a_0, a_1, a_2, \dots рекурсивно определяется следующим образом:

$$a_0 = 0;$$

для любого $n \in \mathbb{N}$ истинно равенство $a_{n+1} = 2a_n + n$.

Докажите, что для всех $n \in \mathbb{N}$ истинно равенство $a_n = 2^n - n - 1$.

16. Последовательность a_0, a_1, a_2, \dots рекурсивно определяется следующим образом:

$$a_0 = 2;$$

для любого $n \in \mathbb{N}$ истинно равенство $a_{n+1} = (a_n)^2$.

Найдите формулу для a_n и докажите, что она верна.

17. Последовательность a_1, a_2, a_3, \dots рекурсивно определяется следующим образом:

$$a_1 = 1;$$

для любого $n \geq 1$ истинно равенство $a_{n+1} = \frac{a_n}{a_n + 1}$.

Найдите формулу для a_n и докажите, что она верна.

18. Для $n \geq k \geq 0$ величина $\binom{n}{k}$ определяется следующим образом:

$$\binom{n}{k} = \frac{n!}{k! \cdot (n - k)!}.$$

- (a) Докажите, что для всех $n \in \mathbb{N}$ истинно равенство $\binom{n}{0} = \binom{n}{n} = 1$.

- (b) Докажите, что для всех натуральных чисел n и k если $n \geq k > 0$, то

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

- (c) Если A является множеством и $k \in \mathbb{N}$, пусть $\mathcal{P}_k(A)$ – множество всех подмножеств A , содержащих k элементов. Докажите, что если A имеет

ет n элементов и $n \geq k \geq 0$, то $\mathcal{P}_k(A)$ имеет $\binom{n}{k}$ элементов. (Подсказка: докажите методом индукции, что $\forall n \in \mathbb{N} \forall A [A \text{ – множество из } n \text{ элементов} \rightarrow \forall k (n \geq k \geq 0 \rightarrow \mathcal{P}_k(A) \text{ имеет } \binom{n}{k} \text{ элементов}]]$. Повторите упражнения 11 и 12 из раздела 6.2. Фактически это упражнение обобщает упражнение 12 из раздела 6.2. Это упражнение показывает,

что $\binom{n}{k}$ – это количество способов выбора k элементов из множества размера n , поэтому его иногда называют *n выбор k*.)

- (d) Докажите, что для всех действительных чисел x и y и любого натурального числа n справедливо равенство

$$(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k.$$

(Это равенство называется *биномиальной теоремой*, поэтому числа $\binom{n}{k}$ иногда называют *биномиальными коэффициентами*.)

Примечание. Анализ частей (а) и (б) показывает, что числа $\binom{n}{k}$ удобно вычислять, используя треугольный массив, как на рис. 6.13. Этот массив называется *треугольником Паскаля* в честь французского математика Блеза Паскаля (1623–1662). Каждая строка треугольника соответствует определенному значению n , и в нем перечислены значения $\binom{n}{k}$ для всех k от 0 до n . Из части (а) следует, что первое и последнее числа в каждой строке равны 1. Из части (б) следует, что каждое из остальных чисел является суммой двух чисел над ним. Например, линии на рис. 6.13 показывают, что $\binom{3}{2} = 3$ – это сумма $\binom{2}{1} + \binom{2}{2} = 2 + 1 = 3$.

$$\begin{array}{ll} n=0: & 1 \\ n=1: & 1 \quad 1 \\ n=2: & 1 \quad 2 \quad 1 \\ n=3: & 1 \quad 3 \quad 3 \quad 1 \\ n=4: & 1 \quad 4 \quad 6 \quad 4 \quad 1 \\ & \vdots \end{array}$$

Рис. 6.13 ♦ Треугольник Паскаля

19. Значение обозначений, используемых в этом упражнении, см. в упражнении 18.

(а) Докажите, что для всех $n \in \mathbb{N}$ истинно равенство $\sum_{k=0}^n \binom{n}{k} = 2^n$. (Подсказка: вы можете сделать это путем индукции, используя части (а) и (б) упражнения 18, или можете объединить часть (с) упражнения 18 с упражнением 11 из раздела 6.2, или можете подставить что-то вместо x и y в часть (д) упражнения 18.)

(б) Докажите, что для всех $\sum_{k=0}^n (-1)^k \binom{n}{k} = 0$.

20. Последовательность a_0, a_1, a_2, \dots рекурсивно определена следующим образом:

$$a_0 = 0;$$

для любого $n \in \mathbb{N}$ истинно равенство $a_{n+1} = (a_n)^2 + \frac{1}{4}$.

Докажите, что для всех $n \geq 1$ истинно неравенство $0 < a_n < 1$.

21. В этой задаче мы определим для каждого натурального числа n функцию $f_n: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$. Последовательность функций f_0, f_1, f_2, \dots рекурсивно определяется следующим образом:

для любого $x \in \mathbb{Z}^+$ истинно $f_0(x) = x$;

для любого $n \in \mathbb{N}$ и любого $x \in \mathbb{Z}^+$ истинно $f_{n+1}(x) = 2^{f_n(x)}$.

- (a) Первое равенство в этом рекурсивном определении дает формулу для $f_0(x)$, а именно $f_0(x) = x$. Найдите формулы для $f_1(x), f_2(x)$ и $f_3(x)$.
 - (b) Докажите, что для всех натуральных чисел n и всех положительных целых чисел x и y если $x < y$, то $f_n(x) < f_n(y)$.
 - (c) Докажите, что для всех натуральных чисел m и n и всех положительных целых чисел x если $m < n$, то $f_m(x) < f_n(x)$.
 - (d) Докажите, что для любого натурального числа n истинно $f_n \in O(f_{n+1})$, но $f_{n+1} \notin O(f_n)$. (Значение используемых здесь обозначений см. в упражнении 19 в разделе 5.1.)
Теперь определим $g: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ по формуле $g(x) = f_x(x)$.
 - (e) Вычислите $g(1), g(2)$ и $g(3)$. (Не пытайтесь вычислить $g(4)$; ответом будет число, состоящее более чем из 6×10^{19727} цифр.)
 - (f) Докажите, что для любого натурального числа n истинно $f_n \in O(g)$, но $g \notin O(f_n)$.
22. Объясните парадокс доказательства теоремы 6.3.4, в котором мы упростили доказательство, изменив цель на утверждение, которое выглядело так, как будто его будет труднее доказать.

6.4. СИЛЬНАЯ ИНДУКЦИЯ

Применяя метод математической индукции, на шаге индукции мы доказываем, что натуральное число обладает некоторым свойством, исходя из предположения, что предыдущее число обладает таким же свойством. В некоторых случаях это предположение звучит недостаточно убедительно, чтобы служить основанием доказательства, и нам нужно предположить, что все меньшие натуральные числа обладают этим свойством. Это идея варианта математической индукции, которую иногда называют *сильной индукцией*.

Чтобы доказать цель вида $\forall n \in \mathbb{N} P(n)$:

Докажите, что $\forall n[(\forall k < n P(k)) \rightarrow P(n)]$, где n и k в этом утверждении пробегают натуральные числа. Конечно, самый прямой способ доказать это – принять за n произвольное натуральное число, предположить, что $\forall k < n P(k)$, а затем доказать $P(n)$.

Заметим, что при доказательстве по методу сильной индукции базовый случай не требуется. Все, что нужно, – это модифицированная форма шага индукции, на котором мы доказываем, что если каждое натуральное число, меньшее n , обладает свойством P , то n тоже обладает свойством P . При доказательстве с помощью сильной индукции мы ссылаемся на предположение,

что каждое натуральное число, меньшее n , обладает свойством P , как на предположение (гипотезу) индукции.

Чтобы лучше понять, почему работает сильная индукция, мы сначала кратко рассмотрим, почему работает обычная индукция. Напомним, что доказательство с помощью обычной индукции предлагает нам пройти через все натуральные числа по порядку и убедиться, что каждое из них обладает некоторым свойством P . Базовый случай запускает процесс, а шаг индукции показывает, что процесс всегда можно продолжить, прибавив к текущему числу единицу и тем самым перейдя к следующему случаю. Но обратите внимание, что в этом процессе, когда мы проверяем, что некоторое натуральное число n обладает свойством P , мы уже убедились, что *все меньшие числа* обладают этим свойством. Другими словами, мы уже знаем, что $\forall k < n P(k)$. Идея сильной индукции заключается в том, что мы должны иметь возможность использовать эту информацию в нашем доказательстве $P(n)$.

Давайте более тщательно проработаем детали этой идеи. Предположим, что мы следовали стратегии доказательства сильной индукции и доказали утверждение $\forall n[(\forall k < n P(k)) \rightarrow P(n)]$. Затем, подставляя 0 вместо n , мы можем заключить, что $(\forall k < 0 P(k)) \rightarrow P(0)$. Но поскольку не существуют натуральные числа меньше 0, утверждение $\forall k < 0 P(k)$ истинно в силу своей пустоты. Следовательно, по *modus ponens* $P(0)$ истинно. (Это объясняет, почему в доказательстве с помощью сильной индукции базовый случай не нужно проверять отдельно; базовый случай $P(0)$ фактически следует из модифицированной формы шага индукции, используемого в сильной индукции.) Аналогично, подставляя 1 вместо n , можно заключить, что $(\forall k < 1 P(k)) \rightarrow P(1)$. Единственное натуральное число меньше 1 – это 0, и мы только что показали, что $P(0)$ истинно, поэтому утверждение $\forall k < 1 P(k)$ истинно. Следовательно, по *modus ponens* $P(1)$ также верно. Теперь подставим 2 вместо n , чтобы получить выражение $(\forall k < 2 P(k)) \rightarrow P(2)$. Поскольку $P(0)$ и $P(1)$ истинны, утверждение $\forall k < 2 P(k)$ истинно, и, следовательно, по *modus ponens* $P(2)$ истинно. Продолжая таким образом, мы можем показать, что $P(n)$ истинно для любого натурального числа n , что нам и требуется. Альтернативное обоснование метода сильной индукции см. в упражнении 1 к этому разделу.

В качестве первого примера метода сильной индукции мы доказываем важный факт теории чисел, известный как *алгоритм деления*¹.

Теорема 6.4.1. (Алгоритм деления.) Для всех натуральных чисел n и m если² $m > 0$, существуют такие натуральные числа q и r , что $n = qm + r$ и $r < m$. (Числа q и r называются частным и остатком при делении n на m .)

Стратегия доказательства

Пусть m – произвольное натуральное число; с помощью сильной индукции докажем, что $\forall n \exists q \exists r (n = qm + r \wedge r < m)$. Согласно определению сильной индукции это означает, что мы должны принять за n произвольное натураль-

¹ Терминология здесь несколько неудачна, поскольку то, что мы называем алгоритмом деления, на самом деле является теоремой, а не алгоритмом. Тем не менее это общепринятое название.

² В этой книге автор относит 0 к натуральным числам. – Прим. перев.

ное число, предположить, что $\forall k < n \exists q \exists r (k = qm + r \wedge r < m)$, и доказать, что $\exists q \exists r (n = qm + r \wedge r < m)$.

Наша цель – экзистенциальное утверждение, поэтому мы должны попытаться найти значения q и r с требуемыми свойствами. Если $n < m$, это не составит труда, потому что мы можем просто положить $q = 0$ и $r = n$. Но если $n \geq m$, то это не сработает, поскольку у нас должно быть $r < m$, значит, в этом случае мы должны сделать что-то другое. Как обычно в таких случаях, мы обращаемся к предположению индукции. Его формула начинается с $\forall k < n$, поэтому мы должны подставить в нее некоторое натуральное число, меньшее n , вместо k , но что мы должны подставить? Ссылка на деление в формулировке теоремы дает намек. Если мы tolкуем деление как повторяющееся вычитание, то деление n на m предполагает многократное вычитание m из n . Первым шагом в этом процессе будет вычисление $n - m$, которое является натуральным числом меньше n . Возможно, нам стоит вставить $n - m$ вместо k . Не совсем понятно, к чему это приведет, но попробовать стоит. Фактически вы увидите в доказательстве, что как только мы сделаем этот шаг, почти сразу последует желаемый вывод.

Обратите внимание: мы используем тот факт, что частное и остаток существуют для некоторого натурального числа, меньшего, чем n , чтобы доказать, что они существуют для n , но это меньшее число не $n - 1$, это $n - m$. Вот почему мы используем сильную индукцию, а не обычную индукцию для этого доказательства.

Доказательство. Пусть m – произвольное натуральное число. Выполним сильную индукцию по n .

Предположим, что n – натуральное число, и для любого $k < n$ существуют такие натуральные числа q и r , что $k = qm + r$ и $r < m$.

Случай 1. $n < m$. Пусть $q = 0$ и $r = n$. Тогда очевидно, что $n = qm + r$ и $r < m$.

Случай 2. $n \geq m$. Пусть $k = n - m < n$, и обратите внимание, что поскольку $n \geq m$, то k – натуральное число. По предположению индукции мы можем выбрать q' и r' так, чтобы $k = q'm + r'$ и $r' < m$. Тогда $n - m = q'm + r'$, поэтому $n = q'm + r' + m = (q' + 1)m + r'$. Таким образом, если мы положим $q = q' + 1$ и $r = r'$, то получим $n = qm + r$ и $r < m$, что и требовалось доказать.

Алгоритм деления также может быть расширен до отрицательных целых чисел n , и можно показать, что для любых m и n частное и остаток q и r уникальны. Подробнее об этом см. упражнение 14.

Наш следующий пример – еще одна важная теорема теории чисел. Мы использовали эту теорему в нашем доказательстве во введении, утверждая, что существует бесконечно много простых чисел. Подробнее об этой теореме мы поговорим в главе 7.

Теорема 6.4.2. Каждое целое число $n > 1$ является либо простым, либо произведением двух или более простых чисел.

Стратегия доказательства

Запишем цель в виде $\forall n \in \mathbb{N} [n > 1 \rightarrow (n \text{ простое} \vee n - \text{произведение простых чисел})]$, а затем воспользуемся сильной индукцией. Наше предположение ин-

дукции таково: $\forall k < n [k > 1 \rightarrow (k \text{ простое} \vee k - \text{произведение простых чисел})]$, и мы должны доказать, что $n > 1 \rightarrow (n - \text{простое число} \vee n - \text{произведение простых чисел})$. Конечно, мы начинаем с предположения, что $n > 1$, и в соответствии с нашими стратегиями доказательства дизъюнкций хороший способ завершить доказательство – это предположить, что n не является простым числом, и доказать, что оно должно быть произведением простых чисел. Поскольку предположение, что n не является простым, означает $\exists a \exists b (n = ab \wedge a < n \wedge b < n)$, мы немедленно используем экзистенциальное утверждение, чтобы ввести новые переменные a и b в доказательство. Применение предположения индукции к a и b теперь приводит к желаемому выводу.

Доказательство. Используем сильную индукцию. Предположим, что $n > 1$, и предположим, что для любого целого числа k если $1 < k < n$, то k либо простое, либо произведение простых чисел. Конечно, если n простое, то доказывать нечего, поэтому предположим, что n не простое. Следовательно, мы можем выбрать натуральные числа a и b такие, что $n = ab$, $a < n$ и $b < n$. Заметим, что поскольку $a < n = ab$, отсюда следует, что $b > 1$, и аналогично мы должны иметь $a > 1$. Таким образом, по предположению индукции каждое из a и b либо простое, либо произведение простых чисел. Но тогда, поскольку $n = ab$, n – произведение простых чисел.

Метод рекурсии, изученный в предыдущем разделе, также имеет строгую форму. В качестве примера рассмотрим следующее определение последовательности чисел, называемых *числами Фибоначчи*. Эти числа впервые были изучены итальянским математиком Леонардо Пизанским (около 1170–1250), более известным под прозвищем Фибоначчи.

$$\begin{aligned} F_0 &= 0; \\ F_1 &= 1; \\ \text{для любого } n \geq 2 \quad F_n &= F_{n-2} + F_{n-1}. \end{aligned}$$

Например, подставляя $n = 2$ в последнее уравнение, мы находим, что $F_2 = F_0 + F_1 = 0 + 1 = 1$. Аналогично, $F_3 = F_1 + F_2 = 1 + 1 = 2$ и $F_4 = F_2 + F_3 = 1 + 2 = 3$. Продолжение вычислений приводит к следующим значениям числового ряда:

n	0	1	2	3	4	5	6	7	8	...
F_n	0	1	1	2	3	5	8	13	21	...

Обратите внимание, что начиная с F_2 каждое число Фибоначчи вычисляется с использованием не только предыдущего числа в последовательности, но и числа перед ним. В этом смысле рекурсия является сильной. Поэтому неудивительно, что доказательства с использованием чисел Фибоначчи часто требуют сильной, а не обычной индукции.

Чтобы проиллюстрировать это, мы докажем следующую замечательную формулу для чисел Фибоначчи:

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

Поначалу трудно поверить, что эта формула верна. Ведь числа Фибоначчи – это целые числа, и вовсе не очевидно, даст ли эта формула целочисленное значение. К тому же какое отношение числа Фибоначчи имеют к $\sqrt{5}$? Тем не менее доказательство сильной индукцией показывает, что формула верна. (Про вывод этой формулы говорится в упражнении 9.)

Теорема 6.4.3. *Если F_n – это n -е число Фибоначчи, то*

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

Стратегия доказательства

Поскольку F_0 и F_1 определяются отдельно от F_n для $n \geq 2$, мы проверяем формулу для этих случаев отдельно. В случае $n \geq 2$ определение F_n подразумевает, что мы должны использовать предположение о том, что формула верна для F_{n-2} и F_{n-1} , чтобы доказать, что она верна для F_n . Поскольку нам нужно знать, что формула работает для двух предыдущих случаев, мы должны использовать сильную, а не обычную индукцию. Остальная часть доказательства проста, хотя вычисления становятся слегка запутанными.

Доказательство. Используем сильную индукцию. Пусть n – произвольное натуральное число, и предположим, что для всех $k < n$ справедлива формула

$$F_k = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^k - \left(\frac{1-\sqrt{5}}{2}\right)^k}{\sqrt{5}}.$$

Случай 1. $n = 0$. Тогда

$$\begin{aligned} \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}} &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^0 - \left(\frac{1-\sqrt{5}}{2}\right)^0}{\sqrt{5}} \\ &= \frac{1-1}{\sqrt{5}} = 0 = F_0. \end{aligned}$$

Случай 2. $n = 1$. Тогда

$$\begin{aligned} \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}} &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^1 - \left(\frac{1-\sqrt{5}}{2}\right)^1}{\sqrt{5}} \\ &= \frac{\sqrt{5}}{\sqrt{5}} = 1 = F_1. \end{aligned}$$

Случай 3. $n \geq 2$. Тогда, применяя предположение индукции к $n - 2$ и $n - 1$, получаем

$$\begin{aligned} F_n &= F_{n-2} + F_{n-1} \\ &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2}}{\sqrt{5}} + \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}}{\sqrt{5}} \\ &= \frac{\left[\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} + \left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\right] - \left[\left(\frac{1-\sqrt{5}}{2}\right)^{n-2} + \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right]}{\sqrt{5}} \\ &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} \left[1 + \frac{1+\sqrt{5}}{2}\right] - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2} \left[1 + \frac{1-\sqrt{5}}{2}\right]}{\sqrt{5}}. \end{aligned}$$

Теперь заметим, что

$$\left(\frac{1+\sqrt{5}}{2}\right)^2 = \frac{1+2\sqrt{5}+5}{4} = \frac{6+2\sqrt{5}}{4} = \frac{3+\sqrt{5}}{2} = 1 + \frac{1+\sqrt{5}}{2},$$

и аналогично

$$\left(\frac{1-\sqrt{5}}{2}\right)^2 = 1 + \frac{1-\sqrt{5}}{2}.$$

Подставляя в формулу значение F_n , мы получаем

$$\begin{aligned} F_n &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^{n-2} \left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^{n-2} \left(\frac{1-\sqrt{5}}{2}\right)^2}{\sqrt{5}} \\ &= \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}. \end{aligned}$$

Обратите внимание, что при доказательстве теоремы 6.4.3 нам пришлось рассматривать случаи $n = 0$ и $n = 1$ отдельно. Роль, которую эти случаи играют в доказательстве, аналогична роли, которую играет базовый случай в доказательстве с помощью обычной математической индукции. Хотя мы уже говорили, что для доказательств с помощью сильной индукции не требуются базовые случаи, в таких доказательствах нередко встречаются некоторые начальные случаи, рассматриваемые отдельно.

Важным свойством натуральных чисел, которое связано с математической индукцией, является тот факт, что каждое непустое множество натуральных чисел имеет наименьший элемент. Иногда это свойство называют *принципом полного упорядочивания* (или *вполне упорядочивания*), и мы можем доказать его, используя сильную индукцию.

Теорема 6.4.4. (Принцип полного упорядочивания.) *Каждое непустое множество натуральных чисел имеет наименьший элемент.*

Стратегия доказательства

Наша цель такова – $\forall S \subseteq \mathbb{N} (S \neq \emptyset \rightarrow S \text{ имеет наименьший элемент})$. Приняв за S произвольное подмножество \mathbb{N} , мы докажем контрапозицию условного утверждения. Другими словами, мы предположим, что S не имеет наименьшего элемента, и докажем, что в таком случае $S = \emptyset$. Способ индукции заключается в том, что для множества $S \subseteq \mathbb{N}$ сказать, что $S = \emptyset$, – то же самое, что сказать, что $\forall n \in \mathbb{N} (n \notin S)$. Мы докажем это последнее утверждение с помощью сильной индукции.

Доказательство. Предположим, что $S \subseteq \mathbb{N}$ и S не имеет наименьшего элемента. Мы докажем, что $\forall n \in \mathbb{N} (n \notin S)$, поэтому $S = \emptyset$. Таким образом, если $S \neq \emptyset$, то S должен иметь наименьший элемент.

Чтобы доказать истинность утверждения $\forall n \in \mathbb{N} (n \notin S)$, воспользуемся сильной индукцией. Предположим, что $n \in \mathbb{N}$ и $\forall k < n (k \notin S)$. Ясно, что если $n \in S$, то n будет наименьшим элементом S , а это противоречит предположению, что S не имеет наименьшего элемента. Следовательно, $n \notin S$.

Иногда доказательства, которые могут быть выполнены по индукции, записываются вместо этого как приложения принципа вполне упорядочивания. В качестве примера использования принципа вполне упорядочивания в доказательстве мы представляем доказательство иррациональности $\sqrt{2}$. В упражнении 2 представлен альтернативный подход к этому доказательству с использованием сильной индукции.

Теорема 6.4.5. Значение $\sqrt{2}$ иррационально.

Стратегия доказательства

Поскольку иррациональное означает «нерациональное», наша цель – отрицательное утверждение, и логично будет использовать доказательство от противного. Таким образом, мы предполагаем, что значение $\sqrt{2}$ рационально, и пытаемся прийти к противоречию. Предположение о рациональности $\sqrt{2}$ означает, что существуют целые числа p и q такие, что $p/q = \sqrt{2}$, и поскольку

значение $\sqrt{2}$ положительно, мы можем также ограничить область нашего внимания положительными p и q . Так как это эзистенциальное утверждение, наш следующий шаг, вероятно, должен состоять в том, чтобы принять за p и q положительные целые числа, такие, что $p/q = \sqrt{2}$. Как вы увидите в доказательстве, простые алгебраические манипуляции с уравнением $p/q = \sqrt{2}$ не приводят к каким-либо очевидным противоречиям, но они приводят к заключению, что p и q должны быть четными. Таким образом, мы можем сократить эту дробь на 2, получив новую дробь с меньшим числителем и знаменателем, равную $\sqrt{2}$.

Как можно вывести противоречие из этого вывода? Ключевая идея состоит в том, чтобы отметить, что наши рассуждения применимы к любой дроби, равной $\sqrt{2}$. Следовательно, мы можем последовательно сокращать такую дробь, и для нее не может быть наименьшего числителя и знаменателя. Но это нарушает принцип полного упорядочивания! Таким образом, мы получили противоречие.

Эта идея более подробно изложена в следующем доказательстве, в котором мы применили принцип полного упорядочивания к множеству всех возможных знаменателей дробей, равных $\sqrt{2}$. Мы решили поместить это применение принципа в начало доказательства, потому что оно дает самое короткое и наиболее прямое доказательство. Читатели доказательства могут быть сначала озадачены тем, почему мы используем принцип полного упорядочивания (если они не читали данную стратегию доказательства!), но после алгебраических преобразований уравнения $p/q = \sqrt{2}$ практически сразу возникает противоречие. Это хороший пример того, как умный, тщательно спланированный шаг в начале доказательства может привести к замечательной изюминке в окончании.

Доказательство. Предположим, что значение $\sqrt{2}$ рационально. Это означает, что $\exists q \in \mathbb{Z}^+ \exists p \in \mathbb{Z}^+ (p/q = \sqrt{2})$, так что множество $S = \{q \in \mathbb{Z}^+ \mid \exists p \in \mathbb{Z}^+ (p/q = \sqrt{2})\}$ не пусто.

В соответствии с принципом вполне упорядочивания мы можем обозначить за q наименьший элемент S . Так как $q \in S$, мы можем выбрать некоторый $p \in \mathbb{Z}^+$ такой, что $p/q = \sqrt{2}$. Следовательно, $p^2/q^2 = 2$, поэтому $p^2 = 2q^2$ и, следовательно, p^2 четно. Теперь применим теорему из примера 3.4.3, которая гласит, что любое целое x четно тогда и только тогда, когда x^2 четно. Поскольку p^2 четно, p должно быть четным, поэтому мы можем выбрать $\bar{p} \in \mathbb{Z}^+$ такое, что $p = 2\bar{p}$. Следовательно, $p^2 = 4\bar{p}^2$ и, подставляя это в уравнение $p^2 = 2q^2$, получаем $4\bar{p}^2 = 2q^2$; отсюда $2\bar{p}^2 = q^2$ и q^2 является четным числом. Теорема из примера 3.4.3 опять же говорит, что число q должно быть четным, поэтому мы можем выбрать некоторое число $\bar{q} \in \mathbb{Z}^+$ такое, что $q = 2\bar{q}$. Но тогда $\sqrt{2} = p/q = (2\bar{p})/(2\bar{q}) = \bar{p}/\bar{q}$, поэтому $\bar{q} \in S$. Ясно, что $\bar{q} < q$, и это противоречит тому факту, что q было выбрано наименьшим элементом S . Следовательно, $\sqrt{2}$ иррационален.

Упражнения

- *1. Это упражнение дает альтернативное обоснование метода сильной индукции. Все переменные в этом упражнении имеют диапазон значений \mathbb{N} . Предположим, что $P(n)$ – утверждение о натуральном числе n , и предположим, что, следуя стратегии сильной индукции, мы доказали, что $\forall n[(\forall k < n P(k)) \rightarrow P(n)]$. Пусть $Q(n)$ – утверждение $\forall k < n P(k)$.
- Докажите $\forall n Q(n) \leftrightarrow \forall n P(n)$, не используя индукцию.
 - Докажите $VnQ(n)$, используя *обычную* индукцию. Таким образом, из части (a) $\forall n P(n)$ истинно.
2. Перепишите доказательство теоремы 6.4.5 как доказательство сильной индукцией, что $\forall q \in \mathbb{N}[q > 0 \rightarrow \neg \exists p \in \mathbb{Z}^+(p/q = \sqrt{2})]$.
3. В этом упражнении вы дадите еще одно доказательство того, что $\sqrt{2}$ иррационален. Предположим, что $\sqrt{2}$ рационален. Как и в доказательстве теоремы 6.4.5, пусть $S = \{q \in \mathbb{Z}^+ \mid \exists p \in \mathbb{Z}^+(p/q = \sqrt{2})\} \neq \emptyset$, пусть q будет наименьшим элементом множества S и пусть p – натуральное число такое, что $p/q = \sqrt{2}$. Теперь получим противоречие, показав, что $p - q \in S$ и $p - q < q$.
- *4. (a) Докажите, что $\sqrt{6}$ иррационален.
(b) Докажите, что значение $\sqrt{2} + \sqrt{3}$ иррационально.
5. Марсианская денежная система использует цветные бусины вместо монет. Синяя бусина стоит 3 марсианских кредита, а красная бусина стоит 7 марсианских кредитов. Таким образом, три синие бусины стоят 9 кредитов, а синяя и красная бусина вместе – 10 кредитов, но никакая комбинация синих и красных бусин не стоит 11 кредитов. Докажите, что для всех $n \geq 12$ существует некоторая комбинация синих и красных бусин, которая стоит n кредитов.
6. Предположим, что x – действительное число, $x \neq 0$ и $x + 1/x$ – целое число. Докажите, что для всех $n \geq 1$ значение $x^n + 1/x^n$ является целым числом.
- *7. Пусть F_n будет n -м числом Фибоначчи. Все переменные в этом упражнении находятся в диапазоне \mathbb{N} .
- Докажите, что для всех n справедливо $\sum_{i=0}^n F_i = F_{n+2} - 1$.
 - Докажите, что для всех n справедливо $\sum_{i=0}^n (F_i)^2 = F_n F_{n+1}$.
 - Докажите, что для всех n справедливо $\sum_{i=0}^n F_{2i+1} = F_{2n+2}$.
 - Найдите формулу для $\sum_{i=0}^n F_{2i}$ и докажите, что ваша формула верна.
8. Пусть F_n будет n -м числом Фибоначчи. Все переменные в этом упражнении находятся в диапазоне \mathbb{N} .
- Докажите, что для всех $m \geq 1$ и всех n истинно $F_{m+n} = F_{m-1}F_n + F_m F_{n+1}$.
 - Докажите, что для всех $m \geq 1$ и всех $n \geq 1$ истинно $F_{m+n} = F_{m+1}F_{n+1} - F_{m-1}F_{n-1}$.

- (c) Докажите, что для всех n истинно $(F_n)^2 + (F_{n+1})^2 = F_{2n+1}$ и $(F_{n+2})^2 - (F_n)^2 = F_{2n+2}$.
- (d) Докажите, что для всех m и n если $m \mid n$, то $F_m \mid F_n$.
- (e) Обозначения, используемые в этом упражнении, приведены в упражнении 18 в разделе 6.3. Докажите, что для всех $n \geq 1$ выполняются равенства

$$\begin{aligned} F_{2n-1} &= \binom{2n-2}{0} + \binom{2n-3}{1} + \binom{2n-4}{2} + \cdots + \binom{n-1}{n-1} \\ &= \sum_{i=0}^{n-1} \binom{2n-i-2}{i} \end{aligned}$$

и

$$\begin{aligned} F_{2n} &= \binom{2n-1}{0} + \binom{2n-2}{1} + \binom{2n-3}{2} + \cdots + \binom{n}{n-1} \\ &= \sum_{i=0}^{n-1} \binom{2n-i-1}{i}. \end{aligned}$$

- *9. Последовательность чисел a_0, a_1, a_2, \dots называется *обобщенной последовательностью Фибоначчи* (generalized Fibonacci sequence), или для краткости *последовательностью Гибоначчи* (Gibonacci sequence), если для каждого $n \geq 2$ истинно $a_n = a_{n-2} + a_{n-1}$. Таким образом, последовательность Гибоначчи удовлетворяет тому же *рекуррентному соотношению*, что и числа Фибоначчи, но может начинаться иначе.

- (a) Предположим, что c – действительное число и $\forall n \in \mathbb{N} (a_n = c^n)$. Докажите, что a_0, a_1, a_2, \dots является последовательностью Гибоначчи тогда и только тогда, когда $c = (1 + \sqrt{5})/2$ или $c = (1 - \sqrt{5})/2$.
- (b) Предположим, что s и t – действительные числа, и для всех $n \in \mathbb{N}$ верна формула

$$a_n = s \left(\frac{1 + \sqrt{5}}{2} \right)^n + t \left(\frac{1 - \sqrt{5}}{2} \right)^n.$$

Докажите, что a_0, a_1, a_2, \dots является последовательностью Гибоначчи.

- (c) Предположим, что a_0, a_1, a_2, \dots является последовательностью Гибоначчи. Докажите, что существуют действительные числа s и t такие, что для всех $n \in \mathbb{N}$ верна формула

$$a_n = s \left(\frac{1 + \sqrt{5}}{2} \right)^n + t \left(\frac{1 - \sqrt{5}}{2} \right)^n.$$

(Подсказка: сначала покажите, что существуют действительные числа s и t , такие, что приведенная выше формула верна для a_0 и a_1 . Затем покажите, что при таком выборе s и t формула верна для всех n .)

10. Числа Лукаса (названные в честь французского математика Эдуарда Лукаса, 1842–1891) – это числа L_0, L_1, L_2, \dots , определенные следующим образом:

$$L_0 = 2;$$

$$L_1 = 1;$$

для всех $n \geq 2$ $L_n = L_{n-2} + L_{n-1}$.

Найдите формулу для L_n и докажите, что ваша формула верна. (Подсказка: обратитесь к упражнению 9.)

11. Последовательность a_0, a_1, a_2, \dots рекурсивно определена следующим образом:

$$a_0 = -1;$$

$$a_1 = 0;$$

для всех $n \geq 2$ $a_n = 5a_{n-1} - 6a_{n-2}$.

Найдите формулу для a_n и докажите, что ваша формула верна. (Подсказка: обратитесь к упражнению 9.)

12. Последовательность a_0, a_1, a_2, \dots рекурсивно определяется следующим образом:

$$a_0 = 0;$$

$$a_1 = 1;$$

$$a_2 = 1;$$

для всех $n \geq 3$ $a_n = \frac{1}{2}a_{n-3} + \frac{3}{2}a_{n-2} + \frac{1}{2}a_{n-1}$.

Докажите, что для всех $n \in \mathbb{N}$ $a_n = F_n$, n -е число Фибоначчи.

13. Для каждого натурального числа n положим $A_n = \{1, 2, \dots, n\}$, и пусть $P_n = \{X \in \mathcal{P}(A_n) \mid X \text{ не содержит двух последовательных целых чисел}\}$. Например, $P_3 = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 3\}\}$; P_3 не содержит множества $\{1, 2\}$, $\{2, 3\}$ и $\{1, 2, 3\}$, потому что каждое из них содержит по крайней мере одну пару последовательных целых чисел. Докажите, что для каждого n количество элементов в P_n равно F_{n+2} для $(n + 2)$ -го числа Фибоначчи. (Например, количество элементов в P_3 равно $5 = F_5$. Подсказка: какие элементы P_n содержат n ? Какие нет? Ответы на оба вопроса относятся к элементам P_m , для некоторых $m < n$.)

14. Предположим, что n и m – целые числа и $m > 0$.

- (a) Докажите, что существуют целые числа q и r такие, что $n = qm + r$ и $0 \leq r < m$. (Подсказка: если $n \geq 0$, то это следует из теоремы 6.4.1. Если $n < 0$, то начните с применения теоремы 6.4.1 к $-n$ и m . Другой подход – применить теорему 6.4.1 к $-n - 1$ и m .)
- (b) Докажите, что целые числа q и r в части (a) уникальны. Другими словами, покажите, что если q' и r' – целые числа такие, что $n = q'm + r'$ и $0 \leq r' < m$, то $q = q'$ и $r = r'$.

- (c) Докажите, что для любого целого числа n верно одно из следующих утверждений: $n \equiv 0(\text{mod } 3)$, $n \equiv 1(\text{mod } 3)$, $n \equiv 2(\text{mod } 3)$. (Напомним, что это обозначение было введено в определении 4.5.9.)
15. Предположим, что k – натуральное число. Докажите, что существует такое натуральное число a , что для всех $n > a$ справедливо $2^n \geq n^k$. (На языке упражнения 19 из раздела 5.1 это означает, что если $f(n) = n^k$ и $g(n) = 2^n$, то $f \in O(g)$. Подсказка: согласно алгоритму деления для любого натурального числа n существуют натуральные числа q и r такие, что $n = qk + r$ и $0 \leq r < k$. Следовательно, $2^n \geq 2^{qk} = (2^q)^k$. Чтобы выбрать a , выясните, насколько большим должно быть q , чтобы гарантировать, что $2^q \geq n$. Вам может пригодиться пример 6.1.3.)
16. (a) Предположим, что k – натуральное число, a_1, a_2, \dots, a_k – действительные числа, а f_1, f_2, \dots, f_k и g – все функции от \mathbb{Z}^+ к \mathbb{R} . Также предположим, что f_1, f_2, \dots, f_k – все элементы $O(g)$. (Значение используемых здесь обозначений см. в упражнении 19 к разделу 5.1.) Определим функцию $f: \mathbb{Z}^+ \rightarrow \mathbb{R}$ формулой $f(n) = a_1f_1(n) + a_2f_2(n) + \dots + a_kf_k(n)$. Докажите, что $f \in O(g)$. (Подсказка: используйте индукцию по k и упражнение 19(с) раздела 5.1.)
- (b) Пусть $g: \mathbb{Z}^+ \rightarrow \mathbb{R}$ определяется формулой $g(n) = 2^n$. Предположим, что $a_0, a_1, a_2, \dots, a_k$ – действительные числа, и определим $f: \mathbb{Z}^+ \rightarrow \mathbb{R}$ формулой $f(n) = a_0 + a_1n + a_2n^2 + \dots + a_kn^k$. (Такая функция называется полиномом.) Докажите, что $f \in O(g)$. (Подсказка: используйте упражнение 15 и часть (а) этого упражнения.)
17. Последовательность a_0, a_1, a_2, \dots рекурсивно определяется следующим образом:

$$a_0 = 1;$$

для всех $n \in \mathbb{N}$ верна формула $a_{n+1} = 1 + \sum_{i=0}^n a_i$.

Найдите формулу для a_n и докажите, что ваша формула верна.

18. Последовательность a_0, a_1, a_2, \dots рекурсивно определяется следующим образом:

$$a_0 = 1;$$

для всех $n \in \mathbb{N}$ верна формула $a_{n+1} = 1 + \frac{1}{a_n}$.

Найдите формулу для a_n и докажите, что ваша формула верна. (Подсказка: эти числа связаны с числами Фибоначчи.)

19. Докажите, что не существует таких натуральных чисел a, b, c и d , что

$$a^2 + 2b^2 = c^2 \text{ и } 2a^2 + b^2 = d^2. \tag{*}$$

- (a) Докажите, что для всех целых m и n если $3 \mid (m^2 + n^2)$, то $3 \mid m$ и $3 \mid n$. (Подсказка: в упражнении 14 (с) либо $m \equiv 0(\text{mod } 3)$, либо $m \equiv 1(\text{mod } 3)$,

либо $m \equiv 2(\text{mod } 3)$, а также либо $n \equiv 0(\text{mod } 3)$, либо $n \equiv 1(\text{mod } 3)$, либо $n \equiv 2(\text{mod } 3)$. Это дает девять возможностей. Определите, какие из этих возможностей совместимы с предположением, что $3 \mid (m^2 + n^2)$.) Теперь предположим, что есть натуральные числа, удовлетворяющие равенствам (*). Пусть

$$S = \{d \in \mathbb{Z}^+ \mid \exists a \in \mathbb{Z}^+ \exists b \in \mathbb{Z}^+ \exists c \in \mathbb{Z}^+ (a^2 + 2b^2 = c^2 \wedge 2a^2 + b^2 = d^2)\}.$$

Тогда $S \neq \emptyset$, поэтому по принципу полного упорядочения мы можем обозначить за d наименьший элемент S . Пусть a, b и c – положительные целые числа, удовлетворяющие (*).

- (b) Докажите, что $3 \mid c$ и $3 \mid d$. (Подсказка: добавьте два уравнения в (*), а затем примените часть (a).)
 - (c) Докажите, что $3 \mid a$ и $3 \mid b$. (Подсказка: добавьте два уравнения в (*), а затем примените часть (b).)
 - (d) Покажите, что в S существует элемент, меньший, чем d , что противоречит нашему выбору d . (Подсказка: соедините части (b) и (c).)
20. Число $(1 + \sqrt{5})/2$, которое фигурирует в формуле чисел Фибоначчи в теореме 6.4.3, называется *золотым сечением*. Обычно его обозначают φ , и оно постоянно встречается в математике, искусстве и мире природы. В этом упражнении вы исследуете несколько математических контекстов возникновения φ .
- (a) На рис. 6.14 $AEDF$ представляет собой квадрат. Покажите, что если отношение длины длинной стороны прямоугольника $BCFE$ к его короткой стороне такое же, как отношение длины длинной стороны прямоугольника $ABCD$ к его более короткой стороне, то это отношение равно φ .

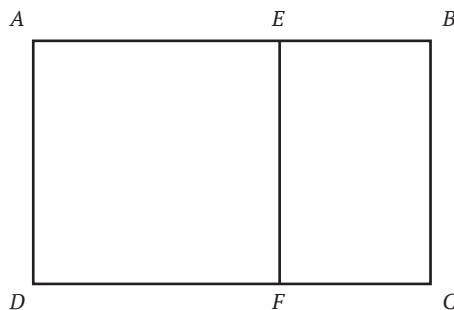


Рис. 6.14 ♦ Геометрическая интерпретация золотого сечения

- (b) Покажите, что $\cos(36^\circ) = \varphi/2$. (Подсказка: пусть $x = \cos(36^\circ)$. Сначала покажите, что $\cos(108^\circ) = -\cos(72^\circ)$. Затем используйте тригонометрические тождества, чтобы выразить $\cos(108^\circ)$ и $\cos(72^\circ)$ через x . Подставьте в уравнение $\cos(108^\circ) = -\cos(72^\circ)$, чтобы получить уравнение, содержащее x , а затем решите его.)

- (c) На рис. 6.15 $ABCDE$ – правильный пятиугольник с длиной стороны 1. Покажите, что длина диагонали AC равна φ . (Подсказка: сначала найдите углы в треугольнике ABC ; для этого вам может пригодиться пример 6.2.3. Затем используйте часть (b).)

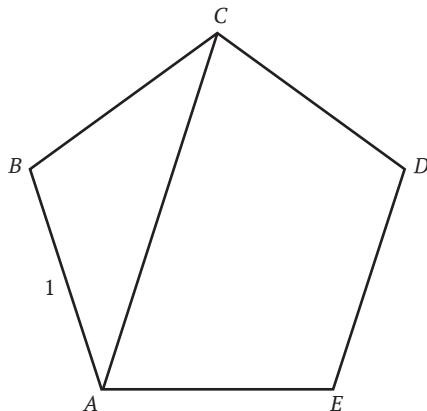


Рис. 6.15 ♦ Правильный пятиугольник
с длиной стороны 1

21. Коммутативный закон умножения гласит, что для любых чисел a и b истинно равенство $ab = ba$. Ассоциативный закон гласит, что для любых чисел a , b и c истинно равенство $(ab)c = a(bc)$. В этом упражнении вы покажете, что хотя эти законы сформулированы для произведений двух или трех чисел, на их основании можно переупорядочивать и перегруппировывать множители в произведении любого перечня чисел любым способом.

- (a) Используйте ассоциативный и коммутативный законы, чтобы показать, что для любых чисел a , b , c и d истинно равенство произведений $(ab)(cd) = c((ad)b)$.
- (b) Положим, что *сгруппированное слева произведение* списка чисел a_1, a_2, \dots, a_n – это произведение, в котором множители сгруппированы следующим образом:

$$\cdots(((a_1 a_2) a_3) a_4) \cdots a_{n-1}) a_n.$$

Более точно мы можем определить сгруппированное слева произведение рекурсивным образом: для списка, состоящего из одного числа a_1 , сгруппированным слева произведением будет 1. Если сгруппированное слева произведение a_1, a_2, \dots, a_n равно p , то сгруппированное слева произведение $a_1, a_2, \dots, a_n, a_{n+1}$ равно pa_{n+1} . Используйте ассоциативный закон, чтобы показать, что любое произведение, полученное из списка чисел a_1, a_2, \dots, a_n (с множителями в таком порядке, но с круглыми скобками, вставленными для группировки множителей любым способом), равно сгруппированному слева произведению.

- (c) Используйте ассоциативный и коммутативный законы, чтобы показать, что любые два произведения чисел a_1, a_2, \dots, a_n с множителями, расположенными в любом порядке и сгруппированными любым способом, равны.

6.5. Вновь про замыкания

В разделе 5.4 мы обещали использовать математическую индукцию, чтобы дать альтернативную трактовку замыканий множеств относительно функций. В этом разделе мы выполняем данное обещание.

Напомним, что если у нас есть функция $f: A \rightarrow A$ и множество $B \subseteq A$, то замыкание B относительно f – это наименьшее множество $C \subseteq A$ такое, что $B \subseteq C$ и C замкнуто относительно f . Далее мы найдем это множество C , начав с B , а затем добавив только те элементы A , которые должны быть добавлены, если мы хотим получить множество, замкнутое относительно f . Мы начнем с краткого описания того, как мы это сделаем, на основе примеров из раздела 5.4. Затем воспользуемся рекурсией и индукцией, чтобы уточнить эту схематичную идею и доказать, что она работает.

Как вы видели в примерах в разделе 5.4, если мы хотим найти такое множество $C \subseteq A$, что $B \subseteq C$ и C замкнуто относительно f , то для каждого $x \in B$ мы должны иметь $f(x) \in C$. Другими словами, $\{f(x) \mid x \in B\} \subseteq C$. Напомним из раздела 5.5, что $\{f(x) \mid x \in B\}$ называется образом B относительно f и обозначается $f(B)$. Таким образом, нам нужно, чтобы соблюдалась истинность $f(B) \subseteq C$. Но тогда аналогичные рассуждения подразумевают, что образ $f(B)$ относительно f также должен быть подмножеством C ; другими словами, $f(f(B)) \subseteq C$.

Движение по этому пути приводит к последовательности множеств, которые должны содержаться в C : $B, f(B), f(f(B))$ и т. д. Мы докажем, что если собрать все эти множества вместе и найти их объединение, это даст нам замыкание B относительно f . Другими словами, если мы положим $B_0 = B$, $B_1 = f(B)$, $B_2 = f(f(B))$, ..., то замыкание B относительно f есть $B_0 \cup B_1 \cup B_2 \cup \dots$. Использование многоточия в нашем описании этого процесса предполагает, что мы должны использовать индукцию и рекурсию. Мы сделаем это в формулировке и доказательстве нашей следующей теоремы.

Теорема 6.5.1. Пусть нам дана функция $f: A \rightarrow A$ и $B \subseteq A$. Пусть множества B_0, B_1, B_2, \dots определены рекурсивно следующим образом:

$$\begin{aligned} B_0 &= B; \\ \text{для всех } n \in \mathbb{N}, \quad B_{n+1} &= f(B_n). \end{aligned}$$

Тогда замыкание B относительно f – это множество $\bigcup_{n \in \mathbb{N}} B_n$.

Доказательство. Пусть $C = \bigcup_{n \in \mathbb{N}} B_n$. Поскольку $f: A \rightarrow A$, нетрудно заметить, что каждое множество B_n является подмножеством A , и, следовательно, $C \subseteq A$. Согласно определению замыкания, мы должны проверить два утверждения: что $B \subseteq C$, C замкнуто относительно f , и для любого множества $D \subseteq A$ если $B \subseteq D$ и D замкнуто относительно f , то $C \subseteq D$.

Первое из них справедливо, потому что $B = B_0 \subseteq \bigcup_{n \in \mathbb{N}} B_n = C$. Для второго предположим, что $x \in C$. Тогда по определению C мы можем выбрать некоторое число $m \in \mathbb{N}$ такое, что $x \in B_m$. Но тогда $f(x) \in f(B_m) = B_{m+1}$, поэтому $f(x) \in \bigcup_{n \in \mathbb{N}} B_n = C$. Поскольку за x мы приняли произвольный элемент C , это показывает, что C замкнуто относительно f .

Наконец, пусть $B \subseteq D \subseteq A$ и D замкнуто относительно f . Мы должны показать, что $C \subseteq D$, и по определению C достаточно доказать, что $\forall n \in \mathbb{N} (B_n \subseteq D)$. Докажем это индукцией по n .

Базовый случай выполняется, потому что по исходному предположению $B_0 = B \subseteq D$. Для шага индукции предположим, что $n \in \mathbb{N}$ и $B_n \subseteq D$. Теперь предположим, что $x \in B_{n+1}$. По определению B_{n+1} это означает, что $x \in f(B_n)$, поэтому существует некоторый элемент $b \in B_n$ такой, что $x = f(b)$. Но по предположению индукции $B_n \subseteq D$, поэтому $b \in D$, и поскольку D замкнуто относительно f , из этого следует, что $x = f(b) \in D$. Поскольку x был произвольным элементом B_{n+1} , это говорит, что $B_{n+1} \subseteq D$.

Комментарий. Поскольку доказательство должно ссылаться на множество $\bigcup_{n \in \mathbb{N}} B_n$, часто бывает удобно дать этому множеству имя C в самом начале доказательства. Согласно доказательству, нетрудно увидеть, что для любого $n \in \mathbb{N}$ справедливо $B_n \subseteq A$ и, следовательно, $C \subseteq A$. Как и прежде, если вы не понимаете, почему это так, вам следует проработать детали доказательства самостоятельно. (Вы можете попробовать доказать истинность $\forall n \in \mathbb{N} (B_n \subseteq A)$ по математической индукции.) Затем определение замыкания говорит нам, что мы должны доказать три утверждения: $B \subseteq C$, C замкнуто относительно f , и для всех $D \subseteq A$ если $B \subseteq D$ и D замкнуто относительно f , то $C \subseteq D$. Конечно, мы доказываем их по очереди.

Доказательство первого из этих утверждений, $B \subseteq C$, также не детализовано. Если у вас возникли проблемы с его выполнением, см. упражнение 8 в разделе 3.3. Второе утверждение, которое мы должны доказать, гласит, что C замкнуто относительно f , и доказательство основано на определении замкнутости: пусть x будет произвольным, предположим $x \in C$ и докажем, что $f(x) \in C$. В соответствии с определением C утверждение $x \in C$ означает $\exists n \in \mathbb{N} (x \in B_n)$, поэтому мы сразу же вводим переменную m для обозначения натурального числа, такого что $x \in B_m$. Цель $f(x) \in C$ также является эзистенциальным утверждением, поэтому для ее доказательства мы должны найти натуральное число k такое, что $f(x) \in B_k$. Доказательство показывает, что равенство $k = m + 1$ выполняется.

Наконец, чтобы доказать третье утверждение, мы используем естественную стратегию: пусть D будет произвольным множеством, предположим, что $B \subseteq D \subseteq A$ и D замкнуто относительно f , а затем доказываем, что $C \subseteq D$. И вновь, если вы не понимаете, почему из $\forall n \in \mathbb{N} (B_n \subseteq D)$ следует вывод $C \subseteq D$, как утверждается в доказательстве, вам следует проработать детали доказательства самостоятельно. Последнее утверждение доказывается индукцией, как и следовало ожидать, исходя из рекурсивной природы определения B_n . Для шага индукции пусть n – произвольное натуральное число, предположим, что $B_n \subseteq D$, и докажем, что $B_{n+1} \subseteq D$. Чтобы доказать, что $B_{n+1} \subseteq D$, возьмем произвольный элемент из B_{n+1} и докажем, что он должен быть элементом D . Запись рекурсивного определения B_{n+1} дает нам возможность использовать

предположение индукции, которое, как обычно, является ключом к завершению шага индукции.

В конце этой главы мы еще раз вернемся к одному из доказательств во введении. Напомним, что в нашем первом доказательстве во введении мы использовали формулу

$$(2^b - 1) \cdot (1 + 2^b + 2^{2b} + \dots + 2^{(a-1)b}) = 2^{ab} - 1.$$

Мы возвращались к этому доказательству в разделе 3.7 и обещали дать более тщательное доказательство этой формулы после знакомства с математической индукцией. Теперь мы готовы выполнить обещание. Конечно, теперь мы можем представить формулу более корректно, используя символьную запись суммы.

Теорема 6.5.2. Для всех натуральных чисел a и b справедлива формула

$$(2^b - 1) \cdot \sum_{k=0}^{a-1} 2^{kb} = 2^{ab} - 1.$$

Доказательство. Примем за b произвольное натуральное число, а затем проведем индукцию по a .

Базовый случай: когда $a = 1$, мы имеем

$$\begin{aligned} (2^b - 1) \cdot \sum_{k=0}^{a-1} 2^{kb} &= (2^b - 1) \cdot \sum_{k=0}^0 2^{kb} \\ &= (2^b - 1) \cdot 1 \\ &= 2^{ab} - 1. \end{aligned}$$

Шаг индукции: предположим, что $a \geq 1$ и $(2^b - 1) \cdot \sum_{k=0}^{a-1} 2^{kb} = 2^{ab} - 1$. Отсюда

$$\begin{aligned} (2^b - 1) \cdot \sum_{k=0}^a 2^{kb} &= (2^b - 1) \cdot \left(\sum_{k=0}^{a-1} 2^{kb} + 2^{ab} \right) \\ &= (2^b - 1) \cdot \sum_{k=0}^{a-1} 2^{kb} + 2^b \cdot 2^{ab} - 2^{ab} \\ &= 2^{ab} - 1 + 2^{b+ab} - 2^{ab} \\ &= 2^{(a+1)b} - 1. \end{aligned} \quad (\text{предположение индукции})$$

Упражнения

- *1. Пусть функция $f: \mathbb{R} \rightarrow \mathbb{R}$ определена формулой $f(x) = x + 1$, и пусть $B = \{0\}$. В п. 2 примера 5.4.4 мы видели, что замыкание B относительно f равно \mathbb{N} . Чем являются множества B_0, B_1, B_2, \dots , определенные в теореме 6.5.1?
- 2. Пусть функция $f: \mathbb{R} \rightarrow \mathbb{R}$ определена формулой $f(x) = x - 1$, и пусть $B = \mathbb{N}$. В примере 5.4.2 мы видели, что замыканием B относительно f является \mathbb{Z} . Чем являются множества B_0, B_1, B_2, \dots , определенные в теореме 6.5.1?

3. Предположим, что \mathcal{F} – это множество функций от A к A и $B \subseteq A$. В упражнении 12 раздела 5.4 мы определили замыкание B относительно \mathcal{F} как наименьшее множество $C \subseteq A$ такое, что $B \subseteq C$ и для каждого $f \in \mathcal{F}$ множество C замкнуто относительно f . Пусть множества B_0, B_1, B_2, \dots определены рекурсивно следующим образом:

$$B_0 = B; \\ \text{для всех } n \in \mathbb{N} \quad B_{n+1} = \bigcup_{f \in \mathcal{F}} f(B_n).$$

Докажите, что $\bigcup_{n \in \mathbb{N}} B_n$ является замыканием B относительно \mathcal{F} .

- *4. Пусть для каждого натурального числа n функция $f_n: \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$ определяется формулой $f_n(X) = X \cup \{n\}$, и пусть $\mathcal{F} = \{f_n \mid n \in \mathbb{N}\}$. Пусть $B = \{\emptyset\}$. В части (b) упражнения 12 из раздела 5.4 вы показали, что замыкание B относительно \mathcal{F} – это множество всех конечных подмножеств \mathbb{N} . Что представляют собой множества B_0, B_1, B_2, \dots , определенные в упражнении 3?
- *5. Пусть функция $f: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ определена формулой $f(x, y) = xy$. Пусть P – множество всех простых чисел. Что представляет собой замыкание P относительно f ?
6. Рассмотрим следующую ошибочную теорему.

Ошибочная теорема. Пусть дана функция $f: A \times A \rightarrow A$ и $B \subseteq A$. Пусть множества B_0, B_1, B_2, \dots определены рекурсивно следующим образом:

$$B_0 = B; \\ \text{для всех } n \in \mathbb{N} \quad B_{n+1} = f(B_n \times B_n).$$

Тогда замыканием B относительно f будет множество $\bigcup_{n \in \mathbb{N}} B_n$.

Где ошибка в следующем доказательстве теоремы?

Доказательство. Пусть $C = \bigcup_{n \in \mathbb{N}} B_n$. Достаточно очевидно, что каждое множество B_n является подмножеством A , поэтому $C \subseteq A$ и $B = B_0 \subseteq C$. Чтобы увидеть, что C замкнуто относительно f , предположим, что $x, y \in C$. Тогда по определению C существует некоторое число $m \in \mathbb{N}$ такое, что $x, y \in B_m$. Следовательно, $f(x, y) \in f(B_m \times B_m) = B_{m+1}$. Отсюда $f(x, y) \in \bigcup_{n \in \mathbb{N}} B_n = C$. Наконец, предположим, что $B \subseteq D \subseteq A$ и D замкнуто относительно f . Чтобы доказать, что $C \subseteq D$, достаточно доказать истинность $\forall n \in \mathbb{N} (B_n \subseteq D)$. Докажем это по индукции. Базовый случай выполняется, поскольку по предположению $B_0 = B \subseteq D$. Для шага индукции предположим, что $B_n \subseteq D$, и пусть произвольный элемент $x \in B_{n+1}$. По определению B_{n+1} это означает, что $x = f(a, b)$ для некоторых $a, b \in B_n$. По предположению индукции $B_n \subseteq D$, поэтому $a, b \in D$, и поскольку D замкнуто относительно f , из этого следует, что $x = f(a, b) \in D$. Следовательно, $B_{n+1} \subseteq D$.

- *7. Пусть $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ определяется формулой $f(x, y) = xy$, и пусть $B = \{x \in \mathbb{R} \mid -2 \leq x \leq 0\}$. Покажите, что f и B представляют собой контрпример к ошибочной теореме из упражнения 6.
- (a) Что представляют собой множества B_0, B_1, B_2, \dots , определенные в ошибочной теореме?

- (b) Покажите, что $\bigcup_{n \in \mathbb{N}} B_n$ не является замыканием B относительно f . Какое из трех условий в определении замыкания (определение 5.4.8) не выполняется?
- (c) Что представляет собой замыкание B относительно f ?
8. Предположим, что $f: A \times A \rightarrow A$ и $B \subseteq A$. Пусть множества B_0, B_1, B_2, \dots определены рекурсивно следующим образом:

$$B_0 = B; \\ \text{для всех } n \in \mathbb{N} \ B_{n+1} = B_n \cup f(B_n \times B_n).$$

- (a) Докажите, что для всех натуральных чисел m и n если $m \leq n$, то $B_m \subseteq B_n$. (Подсказка: присвойте m произвольное значение, а затем используйте индукцию по n .)
- (b) Докажите, что $\bigcup_{n \in \mathbb{N}} B_n$ – замыкание B относительно f .
9. Предположим, что $f: A \rightarrow A$ и f – постоянная функция; другими словами, существует некоторый $c \in A$ такой, что для всех $x \in A$ выполняется $f(x) = c$. Предположим, $B \subseteq A$. Что представляют собой множества B_0, B_1, B_2, \dots , определенные в теореме 6.5.1? Что представляет собой замыкание B относительно f ?
10. Во введении есть еще одно доказательство, которое можно было бы более строго записать с помощью индукции. Напомним, что при доказательстве теоремы 4 во введении мы использовали тот факт, что если n – целое положительное число, $x = (n+1)! + 2$ и $0 \leq i \leq n-1$, тогда $(i+2) \mid (x+i)$. Используйте индукцию, чтобы доказать это. (Мы использовали этот факт, чтобы показать, что $x+i$ не является простым.)
Остальные упражнения в этом разделе будут использовать следующее определение. Предположим, что $R \subseteq A \times A$. Пусть R^1, R^2, R^3, \dots определены рекурсивно следующим образом:

$$R^1 = R; \\ \text{для всех } n \in \mathbb{Z}^+ \text{ истинно } R^{n+1} = R^n \circ R.$$

- Ясно, что для любого натурального числа n R_n является отношением на A .
11. Предположим, что $R \subseteq A \times A$. Докажите, что для всех натуральных чисел m и n истинно утверждение $R^{m+n} = R^m \circ R^n$.
12. Предположим, что $f: A \rightarrow A$.
- (a) Докажите, что для любого натурального n $f^n: A \rightarrow A$.
 - (b) Предположим, что $B \in A$, и пусть множества B_0, B_1, B_2, \dots определены как в теореме 6.5.1. Докажите, что для любого натурального числа n истинно $f^n(B) = B_n$.
13. Предположим, что $f: A \rightarrow A$ и $a \in A$. Мы говорим, что a является *периодической точкой* для f , если существует некоторое натуральное число n такое, что $f^n(a) = a$.
- (a) Докажите, что если a – периодическая точка для f , то замыкание $\{a\}$ относительно f является конечным множеством.

- (b) Предположим, что замыкание $\{a\}$ относительно f – конечное множество. Должна ли a быть периодической точкой для f ?
14. Предположим, что $R \subseteq A \times A$, и пусть $T = \bigcup_{n \in \mathbb{Z}^+} R^n$. Докажите, что T – транзитивное замыкание R . (Определение транзитивного замыкания см. в упражнении 25 раздела 4.4.)
15. Предположим, что R и S – отношения на A и $R \subseteq S$. Докажите, что для любого натурального числа n истинно $R^n \subseteq S^n$.
16. Пусть R и S – отношения на A , а n – натуральное число.
- Какая связь между $R^n \cap S^n$ и $(R \cap S)^n$? Обоснуйте свои выводы доказательствами или контрпримерами.
 - Какая связь между $R^n \cup S^n$ и $(R \cup S)^n$? Обоснуйте свои выводы доказательствами или контрпримерами.
17. Предположим, что R – отношение на A , а T – транзитивное замыкание R . Если $(a, b) \in T$, то согласно упражнению 14 существует некоторое натуральное число n такое, что $(a, b) \in R^n$, и поэтому по принципу полного упорядочивания (теорема 6.4.4) такое n должно быть наименьшим. Мы определяем *расстояние от a до b* как наименьшее натуральное число n такое, что $(a, b) \in R^n$, и обозначаем это расстояние как $d(a, b)$.
- Предположим, что $(a, b) \in T$ и $(b, c) \in T$ (и, следовательно, $(a, c) \in T$, поскольку T транзитивно). Докажите, что $d(a, c) \leq d(a, b) + d(b, c)$.
 - Предположим, что $(a, c) \in T$ и $0 < m < d(a, c)$. Докажите, что существует некоторый элемент $b \in A$ такой, что $d(a, b) = m$ и $d(b, c) = d(a, c) - m$.
18. Предположим, что R – отношение на A . Для каждого натурального числа n пусть $J_n = \{0, 1, 2, \dots, n\}$. Если $a \in A$ и $b \in A$, мы будем говорить, что функция $f: J_n \rightarrow A$ является *R-путем от a к b длины n* , если $f(0) = a$, $f(n) = b$, и для всех $i < n$ истинно $(f(i), f(i+1)) \in R$.
- Докажите, что для всех $n \in \mathbb{Z}^+$ истинно $R^n = \{(a, b) \in A \times A \mid$ существует *R-путь от a до b длины n* $\}$.
 - Докажите, что транзитивное замыкание R есть $\{(a, b) \in A \times A \mid$ существует *R-путь от a до b (любой длины)* $\}$.
19. Предположим, что R является отношением на A . В этом упражнении мы находим взаимосвязь между расстоянием, как определено в упражнении 17, и *R-путями*, которые обсуждались в упражнении 18.
- Предположим, что $d(a, b) = n$ и $a \neq b$. Докажите, что если f – это *R-путь от a до b длины n* , то f взаимно однозначна.
 - Предположим, что $d(a, a) = n$. Докажите, что если f – это *R-путь от a до a длины n* , то $\forall i < n \forall j < n (f(i) = f(j) \rightarrow i = j)$. (Другими словами, f взаимно однозначна, за исключением того факта, что $f(0) = f(n) = a$.)
20. Предположим, что R – отношение на A , T – транзитивное замыкание R и A имеет m элементов. Докажите, что

$$T = R \cup R^2 \cup \dots \cup R^m = \bigcup \{R^n \mid 1 \leq n \leq m\}.$$

(Подсказка: используйте упражнение 19.)

Глава 7

Теория чисел

7.1. НАИБОЛЬШИЕ ОБЩИЕ ДЕЛИТЕЛИ

Эта глава содержит введение в теорию чисел – вы изучите натуральные числа 1, 2, 3, Может показаться, что эти числа настолько просты для понимания, что их исследование не приведет к каким-либо интересным открытиям. Но в этой главе вы увидите, что поиск ответов на простые вопросы о положительных целых числах может оказаться на удивление трудным, а ответы иногда раскрывают тонкие и неожиданные закономерности. Конечно, единственный способ убедиться в правильности ответов на наши вопросы – это дать доказательства, используя методы, которые вы освоили в предыдущих главах этой книги. К настоящему моменту вы должны уметь читать и записывать доказательства, поэтому мы меньше будем обсуждать стратегию доказательства и оставим больше доказательств в качестве упражнений.

Мы начнем с концепции, лежащей в основе всей теории чисел, – *наибольшего общего делителя* пары натуральных чисел.

Определение 7.1.1. Пусть a – натуральное число. *Делители* a – это натуральные числа, которые делят a . Обозначим множество делителей a через $D(a)$. Таким образом:

$$D(a) = \{d \in \mathbb{Z}^+ \mid d \text{ делит } a\} = \{d \in \mathbb{Z}^+ \mid \exists k \in \mathbb{Z} (a = kd)\}.$$

Если a и b – два натуральных числа, то $D(a) \cap D(b)$ – это множество натуральных чисел, которые делят как a , так и b – *общие делители* a и b . Самый большой элемент этого множества называется *наибольшим общим делителем* a и b (greatest common divisor) и обозначается $\gcd(a, b)$.

Например, $D(18) = \{1, 2, 3, 6, 9, 18\}$ и $D(12) = \{1, 2, 3, 4, 6, 12\}$, поэтому множество общих делителей 18 и 12 – это $D(18) \cap D(12) = \{1, 2, 3, 6\}$. Наибольший из этих общих делителей равен 6, поэтому $\gcd(18, 12) = 6$.

Обратите внимание, что 1 и a всегда являются элементами $D(a)$ и это конечное множество, поскольку $D(a) \subseteq \{1, 2, \dots, a\}$. Таким образом, для любых двух натуральных чисел a и b пересечение $D(a) \cap D(b)$ – конечное непустое множество (поскольку оно содержит 1), поэтому оно имеет наибольший эле-

мент (см. упражнение 3 в разделе 6.2). Другими словами, $\gcd(a, b)$ всегда определен.

Как мы можем вычислить $\gcd(a, b)$, имея два натуральных числа a и b ? Один из способов – начать с перечисления всех элементов $D(a)$ и $D(b)$, как мы это делали при вычислении $\gcd(18, 12)$. Но если a и b большие, это может быть непрактично. К счастью, есть способ получше.

Поскольку $D(a) \cap D(b) = D(b) \cap D(a)$, то очевидно, что $\gcd(a, b) = \gcd(b, a)$. Другими словами, в наших обозначениях наибольшего общего делителя двух натуральных чисел не имеет значения, какое целое число мы указываем первым. Часто бывает удобно сначала указать большее число; в частности, при вычислении $\gcd(a, b)$ мы будем предполагать, что $a \geq b$.

Одно полезное наблюдение состоит в том, что если $b | a$, то $\gcd(a, b) = b$. Это потому, что b – самый большой элемент $D(b)$. Если $b | a$, то b также является элементом $D(a)$, поэтому оно должно быть наибольшим элементом пересечения $D(a) \cap D(b)$. Это говорит о том, что для вычисления $\gcd(a, b)$, где $a \geq b$, мы могли бы начать с деления a на b . Согласно алгоритму деления (теорема 6.4.1), если мы разделим a на b , то найдем натуральные числа q и r (частное и остаток), такие что $a = qb + r$ и $r < b$. Если $r = 0$, то $a = qb$, поэтому $b | a$ и, следовательно, $\gcd(a, b) = b$.

Но что, если $r > 0$? Как мы можем вычислить $\gcd(a, b)$ в этом случае? Мы утверждаем, что в этом случае $D(a) \cap D(b) = D(b) \cap D(r)$. Докажем этот факт. Предположим сначала, что $d \in D(a) \cap D(b)$. Тогда $d | a$ и $d | b$, поэтому существуют целые числа j и k такие, что $a = jd$ и $b = kd$. Но тогда из уравнения $a = qb + r$ мы получаем $r = a - qb = jd - qkd = (j - qk)d$, поэтому $d | r$. Следовательно, $d \in D(r)$, и поскольку также $d \in D(b)$, то $d \in D(b) \cap D(r)$. Аналогичное рассуждение показывает, что если $d \in D(b) \cap D(r)$, то $d \in D(a) \cap D(b)$, поэтому $D(a) \cap D(b) = D(b) \cap D(r)$. Из определения наибольшего общего делителя следует, что $\gcd(a, b) = \gcd(b, r)$.

Подведем итог тому, что мы узнали с помощью теоремы.

Теорема 7.1.2. *Предположим, что a и b – натуральные числа, где $a \geq b$. Пусть r будет остатком от деления a на b . Если $r = 0$, то $\gcd(a, b) = b$, а если $r > 0$, то $\gcd(a, b) = \gcd(b, r)$.*

Итак, помогает ли эта теорема вычислить $\gcd(a, b)$, если $r > 0$? Одна из причин думать, что это возможно, заключается в том, что $b \leq a$ и $r < b$, поэтому, вероятно, легче вычислить $\gcd(b, r)$, чем $\gcd(a, b)$. Таким образом, теорема позволяет нам заменить нашу исходную задачу вычисления $\gcd(a, b)$ потенциально более простой задачей вычисления $\gcd(b, r)$.

Это должно напомнить вам об изучении рекурсии в главе 6. Рекурсивное определение функции f с областью определения \mathbb{Z}^+ дает нам метод нахождения $f(n)$ с использованием значений $f(k)$ для $k < n$. Повторно используя этот метод, мы можем вычислить $f(n)$ для любого n . Возможно, если мы повторно применим наш метод деления, то сможем вычислить $\gcd(a, b)$.

Прежде чем развивать эту идею в общем виде, давайте попробуем ее на примере. Предположим, мы хотим найти $\gcd(672, 161)$. Начнем с деления $a = 672$ на $b = 161$, что дает нам частное $q = 4$ и остаток $r = 28$:

$$672 = 4 \cdot 161 + 28.$$

По теореме 7.1.2 заключаем, что $\gcd(672, 161) = \gcd(a, b) = \gcd(b, r) = \gcd(161, 28)$. Итак, давайте попробуем вычислить $\gcd(161, 28)$, что кажется уже более простой задачей.

Как решить эту задачу? Конечно, тем же методом! Начнем с деления 161 на 28, чтобы получить частное 5 и остаток 21:

$$161 = 5 \cdot 28 + 21.$$

Снова применяя теорему 7.1.2, видим, что $\gcd(161, 28) = \gcd(28, 21)$. Чтобы вычислить $\gcd(28, 21)$, разделим 28 на 21:

$$28 = 1 \cdot 21 + 7.$$

Таким образом, $\gcd(28, 21) = \gcd(21, 7)$. Но $21 = 3 \cdot 7 + 0$, поэтому $7 \mid 21$ и, следовательно, $\gcd(21, 7) = 7$. Мы заключаем, что это ответ на нашу исходную задачу: $\gcd(672, 161) = 7$.

Мы можем резюмировать наши расчеты в виде списка следующих равенств:

$$\begin{aligned} 672 &= 4 \cdot 161 + 28, \\ 161 &= 5 \cdot 28 + 21, \\ 28 &= 1 \cdot 21 + 7, \\ 21 &= 3 \cdot 7 + 0. \end{aligned}$$

Эти вычисления образуют убывающий список натуральных чисел: 672, 161, 28, 21, 7, 0. Первые два числа являются нашими исходными натуральными числами a и b , после них каждое число является остатком от деления предыдущего числа на число перед ним. Наибольшие общие делители всех соседних пар натуральных чисел в списке одинаковы. Вычисление закончилось, когда мы получили остаток 0, а последнее ненулевое число в списке $7 = \gcd(21, 7) = \gcd(672, 161)$.

Теперь давайте сформулируем обобщение. Предположим, мы хотим найти $\gcd(a, b)$, где a и b – положительные целые числа и $a \geq b$. Определим последовательность натуральных чисел r_0, r_1, r_2, \dots рекурсивно следующим образом. Чтобы начать последовательность, положим $r_0 = a$ и $r_1 = b$; заметим, что $r_0 \geq r_1$. Тогда пусть q_2 и r_2 будут частным и остатком при делении r_0 на r_1 :

$$r_0 = q_2 \cdot r_1 + r_2, \quad 0 \leq r_2 < r_1.$$

Если $r_2 \neq 0$, то мы разделим r_1 на r_2 , чтобы получить частное q_3 и остаток r_3 . В общем, вычислив r_0, r_1, \dots, r_n , если $r_n \neq 0$, затем мы делим r_{n-1} на r_n , чтобы получить частное и остаток от q_{n+1} и r_{n+1} :

$$r_{n-1} = q_{n+1} \cdot r_n + r_{n+1}, \quad 0 \leq r_{n+1} < r_n.$$

Вычисление прекращается, когда мы достигаем остатка 0.

Уверены ли мы, что в конечном итоге у нас останется 0? Что ж, если этого не случится, то последовательность делений будет продолжаться вечно,

и в итоге мы получим бесконечную последовательность натуральных чисел r_0, r_1, r_2, \dots , где $r_0 \geq r_1 > r_2 > \dots$. Это невозможно, так как $\{r_0, r_1, r_2, \dots\}$ было бы непустым множеством натуральных чисел без наименьшего элемента, что противоречит принципу полного порядка (теорема 6.4.4). Таким образом, в конечном итоге мы должны получить остаток 0.

Предположим, что m – наибольший индекс, для которого $r_m \neq 0$. Тогда $r_{m+1} = 0$ и есть m делений, которые можно записать следующим образом:

$$\begin{aligned} r_0 &= q_2 \cdot r_1 + r_2, \\ r_1 &= q_3 \cdot r_2 + r_3, \\ &\dots \\ r_{m-1} &= q_{m+1} \cdot r_m + 0. \end{aligned}$$

Применяя теорему 7.1.2 к каждому делению, заключаем, что

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \dots = \gcd(r_{m-1}, r_m) = r_m.$$

Таким образом, $\gcd(a, b)$ – это последнее ненулевое значение в последовательности r_0, r_1, r_2, \dots .

Этот метод вычисления наибольшего общего делителя двух натуральных чисел называется *алгоритмом Евклида*. Он назван в честь Евклида, который описал его в книге VII своих «Элементов».

Пример 7.1.3. Найдите наибольший общий делитель 444 и 1392.

Решение

Мы применяем алгоритм Евклида к числам $a = 1392$ и $b = 444$. Расчеты показаны в табл. 7.1. Каждое уравнение в столбце «Деление» показывает вычисление деления, которое приводит к частному и остатку в следующей строке. Поскольку последний ненулевой остаток равен 12, мы заключаем, что $\gcd(1392, 444) = 12$.

Таблица 7.1. Расчет $\gcd(1392, 444)$ по алгоритму Евклида

n	q_n	r_n	Деление
0		1392	
1		444	$1392 = 3 \cdot 444 + 60$
2	3	60	$444 = 7 \cdot 60 + 24$
3	7	24	$60 = 2 \cdot 24 + 12$
4	2	12	$24 = 2 \cdot 12 + 0$
5	2	0	

Входными данными для алгоритма Евклида в последнем примере были $a = 1392$ и $b = 444$. Поучительно посмотреть, как вычисленные остатки связаны с этими входными данными. Переставив первое уравнение в столбце «Деление» в табл. 7.1, мы видим, что

$$r_2 = 60 = 1392 - 3 \cdot 444 = a - 3b.$$

Аналогичным образом из следующего уравнения получаем

$$r_3 = 24 = 444 - 7 \cdot 60 = b - 7r_2 = b - 7(a - 3b) = -7a + 22b,$$

а третье уравнение дает нам

$$r_4 = 12 = 60 - 2 \cdot 24 = r_2 - 2r_3 = (a - 3b) - 2(-7a + 22b) = 15a - 47b.$$

Мы видим, что каждый остаток можно записать в виде $sa + tb$ для некоторых целых чисел s и t . Мы говорим, что каждый остаток – это линейная комбинация a и b . Но последний ненулевой остаток является наибольшим общим делителем a и b , поэтому мы заключаем, что $\gcd(a, b)$ является линейной комбинацией a и b : $\gcd(a, b) = r_4 = 15a - 47b$. Обобщение этого рассуждения доказывает нашу следующую теорему.

Теорема 7.1.4. Для всех натуральных чисел a и b существуют такие целые числа s и t , что $\gcd(a, b) = sa + tb$.

Доказательство. Как обычно, будем считать, что $a \geq b$; если нет, мы можем просто поменять местами значения a и b . Пусть r_0, r_1, \dots, r_{m+1} – последовательность чисел, полученная с помощью алгоритма Евклида, где $r_m \neq 0$ и $r_{m+1} = 0$. Мы утверждаем, что для любого натурального числа $n \leq m$ r_n является линейной комбинацией a и b . Другими словами, для любого натурального числа n , если $n \leq m$, существуют целые числа s_n и t_n такие, что $r_n = s_n a + t_n b$. Докажем это утверждение с помощью сильной индукции.

Предположим, что n – натуральное число и $n \leq m$, и предположим также, что для всех $k < n$ r_k является линейной комбинацией a и b . Теперь рассмотрим три случая.

Случай 1: $n = 0$. Тогда $r_n = r_0 = a = s_0 a + t_0 b$, где $s_0 = 1$ и $t_0 = 0$.

Случай 2: $n = 1$. Тогда $r_n = r_1 = b = s_1 a + t_1 b$, где $s_1 = 0$ и $t_1 = 1$.

Случай 3: $n \geq 2$. Тогда r_n – это остаток от деления r_{n-2} на r_{n-1} :

$$r_{n-2} = q_n \cdot r_{n-1} + r_n.$$

По предположению индукции существуют целые числа $s_{n-1}, s_{n-2}, t_{n-1}$ и t_{n-2} такие, что

$$r_{n-1} = s_{n-1} a + t_{n-1} b.$$

Следовательно,

$$\begin{aligned} r_n &= r_{n-2} - q_n \cdot r_{n-1} = (s_{n-2} a + t_{n-2} b) - q_n (s_{n-1} a + t_{n-1} b) \\ &= (s_{n-2} - q_n s_{n-1}) a + (t_{n-2} - q_n t_{n-1}) b, \end{aligned}$$

поэтому $r_n = s_n a + t_n b$, где $s_n = s_{n-2} - q_n s_{n-1}$ и $t_n = t_{n-2} - q_n t_{n-1}$.

Этим утверждением мы завершаем индуктивное доказательство того, что для любого $n \leq m$ r_n является линейной комбинацией a и b . Применяя это утверждение к случаю $n = m$, мы заключаем, что $\gcd(a, b) = r_m$ является линейной комбинацией a и b .

Альтернативное доказательство теоремы 7.1.4 см. в упражнении 4. Одно из преимуществ приведенного доказательства состоит в том, что оно дает нам метод нахождения целых чисел s и t , таких что $\gcd(a, b) = sa + tb$. Следуя алгоритму Евклида, мы можем рекурсивно вычислять числа s_n и t_n , используя формулы:

$$\begin{aligned} s_0 &= 1, & t_0 &= 0, \\ s_1 &= 0, & t_1 &= 1, \\ \text{для } n \geq 2 \quad s_n &= s_{n-2} - q_n s_{n-1} & t_n &= t_{n-2} - q_n t_{n-1}. \end{aligned}$$

Если m – наибольший индекс, для которого $r_m \neq 0$, то $\gcd(a, b) = r_m = s_m a + t_m b$. Версия алгоритма Евклида, в которой мы используем эти дополнительные числа s_n и t_n , называется *расширенным алгоритмом Евклида*.

Пример 7.1.5. Используйте расширенный алгоритм Евклида, чтобы найти $\gcd(574, 168)$ и выразить его как линейную комбинацию 574 и 168.

Решение

Расчеты приведены в табл. 7.2. Получаем, что $\gcd(574, 168) = 14 = 5 \cdot 574 - 17 \cdot 168$.

Таблица 7.2. Расчет $\gcd(574, 168)$ по расширенному алгоритму Евклида

n	q_n	r_n	s_n	t_n	Деление
0		574	1	0	$574 = 3 \cdot 168 + 70$
1		168	0	1	$168 = 2 \cdot 70 + 28$
2	3	70	$1 - 3 \cdot 0 = 1$	$0 - 3 \cdot 1 = -3$	$70 = 2 \cdot 28 + 14$
3	2	28	$0 - 2 \cdot 1 = -2$	$1 - 2 \cdot (-3) = 7$	$28 = 2 \cdot 14 + 0$
4	2	14	$1 - 2 \cdot (-2) = 5$	$-3 - 2 \cdot 7 = -17$	
5	2	0			

Непосредственным следствием теоремы 7.1.4 является следующий удивительный факт.

Теорема 7.1.6. Для всех натуральных чисел a, b и d если $d | a$ и $d | b$, то $d | \gcd(a, b)$.

Доказательство. Пусть a, b и d – произвольные натуральные числа, и пусть $d | a$ и $d | b$. Тогда существуют целые числа j и k такие, что $a = jd$ и $b = kd$. Теперь по теореме 7.1.4 пусть s и t – такие целые числа, что $\gcd(a, b) = sa + tb$. Отсюда

$$\gcd(a, b) = sa + tb = sjd + tkd = (sj + tk)d,$$

следовательно, $d | \gcd(a, b)$.

Напомним из части 3 примера 4.4.3, что отношение делимости является частичным порядком на \mathbb{Z}^+ . Мы могли бы интерпретировать теорему 7.1.6 как утверждение, что $\gcd(a, b)$ является наибольшим элементом $D(a) \cap D(b)$ не только относительно обычного порядка натуральных чисел, но также и относительно частичного порядка делимости.

Упражнения

1. Пусть $a = 57$ и $b = 36$.
 - (а) Найдите $D(a)$, $D(b)$ и $D(a) \cap D(b)$.
 - (б) Используйте алгоритм Евклида, чтобы найти $\gcd(a, b)$.
- *2. Найдите $\gcd(a, b)$ и выразите его как линейную комбинацию a и b .
 - (а) $a = 775$, $b = 682$.
 - (б) $a = 562$, $b = 243$.
3. Найдите $\gcd(a, b)$ и выразите его как линейную комбинацию a и b .
 - (а) $a = 2790$, $b = 1206$.
 - (б) $a = 191$, $b = 156$.
4. Завершите следующее альтернативное доказательство теоремы 7.1.4. Предположим, что a и b – натуральные числа. Пусть $L = \{n \in \mathbb{Z}^+ \mid \exists s \in \mathbb{Z} \exists t \in \mathbb{Z} (n = sa + tb)\}$. Покажите, что L имеет наименьший элемент. Пусть d – наименьший элемент в L . Теперь покажите, что $d = \gcd(a, b)$. (Подсказка: покажите, что когда вы делите a или b на d , остаток не может быть положительным.)
- *5. Предположим, что a и b – натуральные числа, и пусть $d = \gcd(a, b)$. Докажите, что любое целое число n является линейной комбинацией a и b тогда и только тогда, когда $d \mid n$.
6. Докажите, что для всех натуральных чисел a, b и c выполняется равенство $\gcd(a, b) = \gcd(a + bc, b)$.
- *7. Предположим, что a, a', b и b' – натуральные числа.
 - (а) Если $a \leq a'$ и $b \leq b'$, должно ли быть так, что $\gcd(a, b) \leq \gcd(a', b')$? Обоснуйте свой ответ либо доказательством, либо контрпримером.
 - (б) Если $a \mid a'$ и $b \mid b'$, должно ли быть так, что $\gcd(a, b) \mid \gcd(a', b')$? Обоснуйте свой ответ либо доказательством, либо контрпримером.
8. Докажите, что для любого натурального числа a справедливо равенство $\gcd(5a + 2, 13a + 5) = 1$.
- *9. Докажите, что для всех натуральных чисел a и b справедливо равенство $\gcd(2a - 1, 2b - 1) = 2^{\gcd(a, b)} - 1$.
10. Докажите, что для всех натуральных чисел a, b и n справедливо равенство $\gcd(na, nb) = n \gcd(a, b)$.
11. Предположим, что a, b и c – натуральные числа.
 - (а) Докажите, что $D(\gcd(a, b)) = D(a) \cap D(b)$.
 - (б) Докажите, что $\gcd(\gcd(a, b), c)$ является наибольшим элементом $D(a) \cap D(b) \cap D(c)$.
12. (а) Используйте алгоритм Евклида, чтобы найти $\gcd(55, 34)$. Узнаете ли вы числа в последовательности r_0, r_1, \dots ? (Подсказка: вернитесь к разделу 6.4.) Сколько здесь шагов деления?

- (b) Предположим, что $n \geq 2$. Что такое $\gcd(F_{n+1}, F_n)$? Сколько шагов деления требуется при использовании алгоритма Евклида для поиска $\gcd(F_{n+1}, F_n)$? (F – это n -е число Фибоначчи.)
13. Предположим, что a и b – натуральные числа и $a \geq b$. Пусть r_0, r_1, \dots, r_{m+1} – последовательность чисел, полученная при использовании алгоритма Евклида для вычисления $\gcd(a, b)$, где $r_m \neq 0$ и $r_{m+1} = 0$. Обратите внимание, что это означает, что для алгоритма потребовалось m делений.
- Докажите, что $\forall k \in \mathbb{N}(k < m \rightarrow r_{m-k} \geq F_{k+2})$, где F_{k+2} – $(k + 2)$ -е число Фибоначчи.
 - Пусть $\varphi = (1 + \sqrt{5})/2$ (φ – так называемое золотое сечение, см. упражнение 20 в разделе 6.4). Докажите, что для каждого натурального k справедливо неравенство $F_k < \varphi^k/\sqrt{5} - 1$. (Подсказка: используйте теорему 6.4.3.)
 - Покажите, что

$$m < \frac{\log(b+1)}{\log \varphi} + \frac{\log 5}{2\log \varphi} - 1.$$

(В этой формуле можно использовать как логарифмы с основанием 10, так и натуральные логарифмы.)

- Покажите, что если b содержит не более 100 цифр, то количество делений при использовании алгоритма Евклида для вычисления $\gcd(a, b)$ будет не более 479.
14. (a) Докажите следующую альтернативную версию алгоритма деления: для любых натуральных чисел a и b существуют такие натуральные числа q и r , что $r \leq b/2$ и либо $a = qb + r$, либо $a = qb - r$.
- (b) Предположим, что a, b и r – натуральные числа, q – натуральное число и либо $a = qb + r$, либо $a = qb - r$. Докажите, что $\gcd(a, b) = \gcd(b, r)$.
- (c) Предположим, что a и b – натуральные числа и $a \geq b$. Определим последовательность r_0, r_1, \dots рекурсивно следующим образом: $r_0 = a$, $r_1 = b$, и для всех $n \geq 1$, если $r_n \neq 0$, мы используем часть (a), чтобы найти натуральные числа q_{n+1} и r_{n+1} , такие что $r_{n+1} < r_n \neq 2$, и либо $r_{n-1} = q_{n+1}r_n + r_{n+1}$, либо $r_{n-1} = q_{n+1}r_n - r_{n+1}$. Докажите, что существует m такое, что $r_m \neq 0$ и $r_{m+1} = 0$ и $\gcd(a, b) = r_m$. Это дает нам новый метод вычисления наибольших общих делителей; он называется *алгоритмом Евклида с наименьшим абсолютным остатком*.
- (d) Вычислите $\gcd(1515, 555)$ с помощью как обычного алгоритма Евклида, так и алгоритма Евклида с наименьшим абсолютным остатком. Какой алгоритм требует меньше шагов?

7.2. ПРОСТЫЕ МНОЖИТЕЛИ

В разделе 6.4 вы видели, что каждое целое число $n > 1$ либо простое, либо может быть записано как произведение простых чисел; во втором случае говорят, что n можно разложить в произведение *простых множителей*. Раз-

ложение числа в произведение простых множителей также называется *факторизацией*. В этом разделе мы покажем, что факторизация в определенном смысле уникальна. Одним из важных инструментов в этом исследовании будут наибольшие общие делители. В частности, нас будут интересовать пары натуральных чисел, наибольший общий делитель которых имеет наименьшее возможное значение, 1.

Определение 7.2.1. Если a и b – натуральные числа и $\gcd(a, b) = 1$, то мы говорим, что a и b *взаимно просты*.

Точно так же мы можем сказать, что a и b взаимно просты, если их единственный общий делитель равен 1. Например, $D(50) = \{1, 2, 5, 10, 25, 50\}$ и $D(63) = \{1, 3, 7, 9, 21, 63\}$, поэтому $D(50) \cap D(63) = \{1\}$. Следовательно, $\gcd(50, 63) = 1$, поэтому 50 и 63 взаимно просты.

Одна из причин, по которой взаимно простые целые числа важны, заключается в нашей следующей теореме. Ключом к доказательству теоремы является использование экзистенциального подтверждения, чтобы ввести обозначения для целых чисел, о существовании которых мы знаем.

Теорема 7.2.2. Для всех натуральных чисел a, b и c если $c \mid ab$ и $\gcd(a, c) = 1$, то $c \mid b$.

Доказательство. Предположим, что $c \mid ab$ и $\gcd(a, c) = 1$. Тогда существует некоторое целое число j такое, что $ab = jc$, а по теореме 7.1.4 существуют целые числа s и t такие, что $sa + tc = 1$. Следовательно:

$$b = b \cdot 1 = b \cdot (sa + tc) = sab + tbc = sjc + tbc = (sj + tb)c,$$

поэтому $c \mid b$.

Обратите внимание, что если p – простое число, то $D(p) = \{1, p\}$. Таким образом, для любого положительного целого числа a единственными возможными значениями $\gcd(a, p)$ являются 1 и p . Если $p \mid a$, то $\gcd(a, p) = p$, а если нет, то единственный общий делитель a и p равен 1, и поэтому a и p взаимно просты. Комбинируя это наблюдение с теоремой 7.2.2, мы получаем следующий важный факт о простых делителях.

Теорема 7.2.3. Для всех натуральных чисел a, b и p если p простое и $p \mid ab$, то либо $p \mid a$, либо $p \mid b$.

Доказательство. Предположим, что p – простое число и $p \mid ab$. Как мы заметили ранее, если $p \nmid a$, то a и p взаимно просты, и поэтому по теореме 7.2.2 $p \mid b$. Таким образом, либо $p \mid a$, либо $p \mid b$.

Комментарий. Обратите внимание, что для доказательства дизъюнкции $(p \mid a) \vee (p \mid b)$ мы использовали стратегию предположения $p \nmid a$, а затем доказательства $p \mid b$.

Используя математическую индукцию, мы можем распространить эту теорему на случай простого числа, делящего произведение списка натуральных чисел.

Теорема 7.2.4. Предположим, что p – простое число и a_1, a_2, \dots, a_k – натуральные числа. Если $p \mid (a_1 a_2 \cdots a_k)$, то для некоторого $i \in \{1, 2, \dots, k\}$, $p \mid a_i$.

Доказательство. Докажем эту теорему индукцией по k . Другими словами, мы будем использовать индукцию, чтобы доказать следующее утверждение: для любого $k \geq 1$ если p делит произведение любого списка из k натуральных чисел, то оно делит одно из целых чисел в списке.

Наш базовый случай – $k = 1$, и в этом случае утверждение явно верно: если $p \mid a_1$, то существует $i \in \{1\}$ такое, что $p \mid a_i$, а именно $i = 1$.

Теперь предположим, что утверждение верно для любого списка из k натуральных чисел, и пусть a_1, a_2, \dots, a_{k+1} – список натуральных чисел таких, что $p \mid (a_1 a_2 \cdots a_k a_{k+1})$. Поскольку $a_1 a_2 \cdots a_k a_{k+1} = (a_1 a_2 \cdots a_k) a_{k+1}$, по теореме 7.2.3 $p \mid (a_1 a_2 \cdots a_k)$ или $p \mid a_{k+1}$. В первом случае по предположению индукции $p \mid a_i$ для некоторого $i \in \{1, 2, \dots, k\}$, а во втором $p \mid a_{k+1}$, где $i = k + 1$.

Теперь мы готовы рассмотреть вопрос об уникальности факторизации. Рассмотрим, например, задачу записи 12 как произведения простых чисел. На самом деле существует три различных способа записать 12 как произведение простых чисел: $12 = 2 \cdot 2 \cdot 3 = 2 \cdot 3 \cdot 2 = 3 \cdot 2 \cdot 2$. Но, конечно, во всех трех случаях мы перемножаем одни и те же три простых числа, только в другом порядке. Чтобы не считать их тремя разными факторизациями числа 12, мы будем рассматривать только разложения, в которых простые числа перечислены от наименьшего к наибольшему. Этому дополнительному требованию удовлетворяет только одна факторизация числа 12: $12 = 2 \cdot 2 \cdot 3$.

В более общем плане нас будут интересовать выражения вида $p_1 p_2 \cdots p_k$, где p_1, p_2, \dots, p_k – простые числа и $p_1 \leq p_2 \leq \cdots \leq p_k$. Мы будем говорить, что такое выражение является произведением неубывающего списка простых чисел. Мы покажем, что каждое целое число больше 1 может быть записано как произведение неубывающего списка простых чисел уникальным способом.

Напомним: чтобы показать, что объект с некоторым свойством уникален, мы доказываем, что любые два объекта с этим свойством должны быть равны. Таким образом, ключом к доказательству единственности факторизаций будет следующий факт.

Теорема 7.2.5. Предположим, что p_1, p_2, \dots, p_k и q_1, q_2, \dots, q_m – простые числа, $p_1 \leq p_2 \leq \cdots \leq p_k$, $q_1 \leq q_2 \leq \cdots \leq q_m$ и $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$. Тогда $k = m$ и для всех $i \in \{1, \dots, k\}$, $p_i = q_i$.

Доказательство. Доказательство проведем индукцией по k . Другими словами, мы используем индукцию, чтобы доказать, что для всех $k \geq 1$ если произведение некоторого неубывающего списка k простых чисел равно произведению другого неубывающего списка простых чисел, то эти два списка должны быть одинаковыми.

Когда $k = 1$, имеем $p_1 = q_1 q_2 \cdots q_m$. Если $m > 1$, то это противоречит тому, что p_1 – простое число. Следовательно, $m = 1$ и $p_1 = q_1$.

Для шага индукции предположим, что утверждение верно для произведений неубывающих списков k простых чисел, и предположим, что p_1, p_2, \dots, p_{k+1} и q_1, q_2, \dots, q_m – простые числа, $p_1 \leq p_2 \leq \cdots \leq p_{k+1}$, $q_1 \leq q_2 \leq \cdots \leq q_m$, и $p_1 p_2 \cdots p_{k+1} = q_1 q_2 \cdots q_m$. Обратите внимание, что если $m = 1$, то это уравнение говорит, что

$p_1 p_2 \cdots p_{k+1} = q_1$, и, как и в базовом случае, это противоречит тому факту, что q_1 – простое число, поэтому $m > 1$.

Ясно, что $p_{k+1} \mid (p_1 p_2 \cdots p_{k+1})$, поэтому $p_{k+1} \mid (q_1, q_2, \dots, q_m)$, и по теореме 7.2.4 следует, что $p_{k+1} \mid q_i$ для некоторых i . Следовательно, $p_{k+1} \leq q_i \leq q_m$. Аналогичное рассуждение показывает, что $q_m \mid p_j$ для некоторого j , поэтому $q_m \leq p_j \leq p_{k+1}$. Мы заключаем, что $p_{k+1} = q_m$. Исключение этих множителей из уравнения $p_1 p_2 \cdots p_{k+1} = q_1 q_2 \cdots q_m$ дает нам $p_1 p_2 \cdots p_{k+1} = q_1 q_2 \cdots q_{m-1}$, а теперь индуктивное предположение говорит нам, что остальные множители в обеих частях уравнения совпадают, как и требовалось.

Теперь у нас есть все необходимое, чтобы заявить о существовании и единственности разложения числа на простые множители. Эта теорема настолько важна, что известна как *основная теорема арифметики*.

Теорема 7.2.6. (Основная теорема арифметики.) Для каждого целого числа $n > 1$ существуют *уникальные простые числа* p_1, p_2, \dots, p_k такие, что $p_1 \leq p_2 \leq \cdots \leq p_k$ и $n = p_1 p_2 \cdots p_k$.

Доказательство. По теореме 6.4.2 каждое целое число больше 1 либо простое, либо представляет собой произведение простых чисел. Перечисление простых чисел от наименьшего к наибольшему дает нам требуемое неубывающее разложение на простые числа. Единственность разложения следует из теоремы 7.2.5.

Если мы напишем произведение списка простых чисел p_1, p_2, \dots, p_k в виде $1 \cdot p_1 p_2 \cdots p_k$, то естественно ввести соглашение о том, что произведение пустого списка равно 1. С помощью этого соглашения мы можем расширить основную теорему арифметики, чтобы сказать, что каждое положительное целое число имеет *уникальную факторизацию*, где разложение числа 1 является произведением пустого списка простых чисел.

Пример 7.2.7. Найдите факторизацию для следующих целых чисел: 275, 276, 277.

Решение

Самый простой способ найти факторизацию натурального числа – это найти его наименьший простой делитель, вычленить его и повторять, пока все множители не станут простыми. Это дает следующие результаты. (Обратите внимание, что 277 – простое число, поэтому процесс факторизации 277 немедленно останавливается.)

$$275 = 5 \cdot 55 = 5 \cdot 5 \cdot 11,$$

$$276 = 2 \cdot 138 = 2 \cdot 2 \cdot 69 = 2 \cdot 2 \cdot 3 \cdot 23,$$

$$277 = 277.$$

Когда в факторизации целого числа повторяются простые числа, часто используют обозначение степени этих чисел. Например, факторизаций 275 и 276 в последнем примере можно записать в форме $275 = 5^2 \cdot 11$ и $276 = 2^2 \cdot 3 \cdot 23$. В более общем смысле: мы можем записать факторизацию натурального числа n в форме $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, где p_1, p_2, \dots, p_k – простые числа ряда

$p_1 < p_2 < \dots < p_k$, а также e_1, e_2, \dots, e_k – натуральные числа. Опять же, по основной теореме арифметики это представление числа n уникально.

Основная теорема арифметики может пролить свет на ряд концепций теории чисел. Например, предположим, что n и d – натуральные числа и $d \mid n$. Тогда существует такое натуральное число c , что $cd = n$. Пусть теперь разложения c и d на простые множители имеют вид $c = p_1 p_2 \cdots p_k$ и $d = q_1 q_2 \cdots q_m$. Тогда $n = cd = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_m$. Если мы переставим простые числа в этом произведении в неубывающий порядок, то это должно быть единственное разложение числа n на простые числа. Следовательно, d должно быть произведением некоторой коллекции простых чисел в факторизации n . Обратите внимание, что мы включаем сюда возможность того, что вложенная коллекция является пустой вложенной коллекцией (так что $d = 1$ и $c = n$) или что она включает все простые числа в факторизации n (так что $d = n$ и $c = 1$).

Перепишем этот вывод с использованием степенной записи и предположим, что разложение числа n на простые множители представлено рядом $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Тогда делители числа n в точности равны числам вида $p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, где для всех $i \in \{1, 2, \dots, k\}$ $0 \leq f_i \leq e_i$. Например, в примере 7.2.7 мы видели, что разложение на простые множители 276 равно $276 = 2^2 \cdot 3 \cdot 23$. Следовательно,

$$\begin{aligned} D(276) &= (1, 2, 2^2, 3, 2 \cdot 3, 2^2 \cdot 3, 23, 2 \cdot 23, 2^2 \cdot 23, 3 \cdot 23, 2 \cdot 3 \cdot 23, 2^2 \cdot 3 \cdot 23) \\ &= \{1, 2, 4, 3, 6, 12, 23, 46, 92, 69, 138, 276\}. \end{aligned}$$

Разложение на простые множители также поможет вам понять концепцию наибольшего общего делителя. Предположим, что a и b – натуральные числа. Пусть p_1, p_2, \dots, p_k – список всех простых чисел, которые встречаются при разложении на простые множители числа a или b . Тогда мы можем записать a и b в виде

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k},$$

где некоторые из показателей степени e_i и f_i могут быть равны 0, поскольку некоторые простые числа могут встречаться только в одной из факторизаций. Касательно обсуждения делимости и разложения на простые множители в предыдущем абзаце, общие делители a и b – это числа вида $p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k}$, где для каждого $i \in \{1, \dots, k\}$, $g_i \leq e_i$ и $g_i \leq f_i$. Наибольший общий делитель может быть найден, если каждому g_i присвоено максимально возможное значение, то есть $\min(e_i, f_i)$ = минимум e_i и f_i . Другими словами,

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \cdots p_k^{\min(e_k, f_k)}.$$

Например, в примере 7.1.3 мы использовали алгоритм Евклида, чтобы найти, что $\gcd(1392, 444) = 12$. Вместо этого мы могли бы разложить 1392 и 444 на простые числа:

$$\begin{aligned} 1392 &= 2^4 \cdot 3 \cdot 29 = 2^4 \cdot 3^1 \cdot 29^1 \cdot 37^0, \\ 444 &= 2^2 \cdot 3 \cdot 37 = 2^2 \cdot 31 \cdot 29^0 \cdot 37^1. \end{aligned}$$

Эти факторизации дают нам еще один способ найти наибольший общий делитель 1392 и 444:

$$\gcd(1392, 444) = 2^{\min(4,2)} \cdot 3^{\min(1,1)} \cdot 29^{\min(1,0)} \cdot 37^{\min(0,1)} = 2^2 \cdot 3^1 \cdot 29^0 \cdot 37^0 = 12.$$

Обычно алгоритм Евклида – более эффективный способ найти наибольший общий делитель двух натуральных чисел, чем разложение на простые множители. Но если вам известны факторизации двух натуральных чисел, вы можете очень легко вычислить их наибольший общий делитель.

Еще одно понятие, проясняемое факторизацией простых чисел, – это *наименьшее общее кратное*. Для любых натуральных чисел a и b наименьшее общее кратное чисел a и b , обозначенное $\text{lcm}(a, b)$, является наименьшим положительным целым числом m таким, что $a | m$ и $b | m$. Наименьшее общее кратное возникает, когда мы складываем дроби: чтобы сложить две дроби со знаменателями a и b , мы начинаем с переписывания их с общим знаменателем $\text{lcm}(a, b)$.

Пусть, как раньше,

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}.$$

Для каждого $i \in \{1, \dots, k\}$ любое общее кратное a и b должно включать множитель $p_i^{g_i}$ в свое разложение на простые множители, где $g_i \geq e_i$ и $g_i \geq f_i$. Наименьшее возможное значение g_i – это максимальное значение e_i и f_i , которое мы обозначим $\max(e_i, f_i)$, поэтому

$$\text{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \cdots p_k^{\max(e_k, f_k)}.$$

Нетрудно показать, что для любых чисел e и f $\min(e, f) + \max(e, f) = e + f$ (см. упражнение 4), поэтому

$$\begin{aligned} \gcd(a, b) \cdot \text{lcm}(a, b) &= (p_1^{\min(e_1, f_1)} \cdots p_k^{\min(e_k, f_k)}) \cdot (p_1^{\max(e_1, f_1)} \cdots p_k^{\max(e_k, f_k)}) \\ &= p_1^{\min(e_1, f_1) + \max(e_1, f_1)} \cdots p_k^{\min(e_k, f_k) + \max(e_k, f_k)} \\ &= p_1^{e_1 + f_1} \cdots p_k^{e_k + f_k} \\ &= (p_1^{e_1} \cdots p_k^{e_k}) \cdot (p_1^{f_1} \cdots p_k^{f_k}) = ab. \end{aligned}$$

Это дает нам еще один способ вычисления $\text{lcm}(a, b)$:

$$\text{lcm}(a, b) = \frac{ab}{\gcd(a, b)}.$$

Альтернативное доказательство истинности этой формулы см. в упражнении 8.

Итак, теперь у нас есть два способа вычислить $\text{lcm}(1392, 444)$:

$$\text{lcm}(1392, 444) = 2^{\max(4,2)} \cdot 3^{\max(1,1)} \cdot 29^{\max(1,0)} \cdot 37^{\max(0,1)} = 2^4 \cdot 3^1 \cdot 29^1 \cdot 37^1 = 51\,504$$

и

$$\text{lcm}(1392, 444) = \frac{1392 \cdot 444}{\text{gcd}(1392, 444)} = \frac{618\,048}{12} = 51\,504.$$

Отсюда следует, что если мы хотим сложить две дроби со знаменателями 1392 и 444, то должны использовать общий знаменатель 51 504.

Пример 7.2.8. Найдите наименьшее общее кратное чисел 1386 и 1029.

Решение

Начнем с использования алгоритма Евклида, чтобы найти $\text{gcd}(1386, 1029)$. Расчеты в табл. 7.3 показывают, что $\text{gcd}(1386, 1029) = 21$. Следовательно,

$$\text{lcm}(1386, 1029) = \frac{1386 \cdot 1029}{\text{gcd}(1386, 1029)} = \frac{1386 \cdot 1029}{21} = 67\,914.$$

Таблица 7.3. Расчет $\text{gcd}(1386, 1029)$ по алгоритму Евклида

n	q_n	r_n	Деление
0		1386	
1		1029	$1386 = 1 \cdot 1029 + 357$
2	1	357	$1029 = 2 \cdot 357 + 315$
3	2	315	$357 = 1 \cdot 315 + 42$
4	1	42	$315 = 7 \cdot 42 + 21$
5	7	21	$42 = 2 \cdot 21 + 0$
6	2	0	

В качестве альтернативы мы могли бы использовать разложение на простые множители: $1386 = 2 \cdot 3^2 \cdot 7 \cdot 11$ и $1029 = 3 \cdot 7^3$, поэтому $\text{lcm}(1386, 1029) = 2 \cdot 3^2 \cdot 7^3 \cdot 11 = 67\,914$.

Упражнения

- Найдите разложения на простые множители следующих натуральных чисел: 650, 756, 1067.
- *Найдите $\text{lcm}(1495, 650)$.
- Найдите $\text{lcm}(1953, 868)$.
- Докажите, что для любых чисел e и f $\min(e, f) + \max(e, f) = e + f$.
- *Предположим, что a и b – натуральные числа. Докажите, что a и b взаимно просты, если их факторизации не имеют общих простых чисел.
- Предположим, что a и b – натуральные числа. Докажите, что a и b взаимно просты, если существуют целые числа s и t такие, что $sa + tb = 1$.

7. Предположим, что a, b, a' и b' – натуральные числа, a и b взаимно просты, $a' \mid a$ и $b' \mid b$. Докажите, что a' и b' взаимно просты.
- *8. Предположим, что a и b – натуральные числа. В этом упражнении вы должны дать альтернативное доказательство формулы $\text{lcm}(a, b) = ab/\gcd(a, b)$. Пусть $m = \text{lcm}(a, b)$.
- Докажите, что $ab/\gcd(a, b)$ – целое число и что $a \mid (ab/\gcd(a, b))$ и $b \mid (ab/\gcd(a, b))$. Используйте это, чтобы заключить, что $m < ab/\gcd(a, b)$. Пусть q и r будут частным и остатком при делении ab на m . Таким образом, $ab = qm + r$ и $0 \leq r < m$.
 - Докажите, что $r = 0$.
 - По части (b) $ab = qm$. Докажите, что $q \mid a$ и $q \mid b$.
 - Используйте часть (c), чтобы сделать вывод, что $m \geq ab/\gcd(a, b)$. Вместе с частью (a) это показывает, что $m = ab/\gcd(a, b)$.
9. Предположим, что a и b – натуральные числа, и пусть $d = \gcd(a, b)$. Тогда $d \mid a$ и $d \mid b$, поэтому существуют натуральные числа j и k такие, что $a = jd$ и $b = kd$. Докажите, что j и k взаимно просты.
10. Докажите, что для всех натуральных чисел a, b и d если $d \mid ab$, то существуют натуральные числа d_1 и d_2 такие, что $d = d_1d_2$, $d_1 \mid a$ и $d_2 \mid b$.
11. Докажите, что для всех натуральных чисел a, b и m если $a \mid m$ и $b \mid m$, то $\text{lcm}(a, b) \mid m$.
12. Предположим, что a, b и c – натуральные числа. Пусть m – наименьшее натуральное число такое, что $a \mid m$, $b \mid m$ и $c \mid m$. Докажите, что $m = \text{lcm}(\text{lcm}(a, b), c)$.
13. Докажите, что для всех натуральных чисел a и b если $a^2 \mid b^2$, тогда $a \mid b$.
14. (a) Найдите все простые числа p такие, что $5p + 9 \in \{n^2 \mid n \in \mathbb{N}\}$.
 (b) Найдите все простые числа p такие, что $15p + 4 \in \{n^2 \mid n \in \mathbb{N}\}$.
 (c) Найдите все простые числа p такие, что $5p + 8 \in \{n^3 \mid n \in \mathbb{N}\}$.
15. Пусть $H = \{4n + 1 \mid n \in \mathbb{N}\} = \{1, 5, 9, 13, \dots\}$. Элементы множества H называются числами Гильберта (названы в честь Дэвида Гильберта (1862–1943)). Число Гильберта, которое больше 1 и не может быть записано как произведение двух меньших чисел Гильберта, называется *простым числом Гильберта*. Например, 9 – простое число Гильберта. (Конечно, 9 не простое число в обычном смысле, так как $9 = 3 \cdot 3$, но $3 \notin H$.)
- Покажите, что H замкнуто относительно умножения; то есть $\forall x \in H \quad \forall y \in H (xy \in H)$.
 - Докажите, что каждое число Гильберта, большее 1, является либо простым числом Гильберта, либо произведением двух или более простых чисел Гильберта.
 - Покажите, что 441 – это число Гильберта, которое можно записать как произведение неубывающего списка простых чисел Гильберта двумя разными способами. Следовательно, факторизация числа Гильберта не уникальна.

16. Предположим, что a и b – натуральные числа. Докажите, что существуют относительно простые натуральные числа c и d такие, что $c \mid a$, $d \mid b$ и $cd = \text{lcm}(a, b)$.
17. Предположим, что a , b и c – натуральные числа.
- Докажите, что $\gcd(a, bc) \mid (\gcd(a, b) \cdot \gcd(a, c))$.
 - Докажите, что $\text{lcm}(\gcd(a, b), \gcd(a, c)) \mid \gcd(a, bc)$. (Подсказка: используйте упражнение 11.)
 - Предположим, что b и c взаимно просты. Докажите, что $\gcd(a, bc) = \gcd(a, b) \cdot \gcd(a, c)$.
18. Вспомните упражнение 5 раздела 6.2, где сказано, что числа $F_n = 2^{(2n)} + 1$ называются числами Ферма. Ферма показал, что F_n – простое число при $0 \leq n \leq 4$, а Эйлер показал, что F_5 не является простым числом. Неизвестно, существует ли какое-либо $n > 4$, для которого F_n является простым. В этом упражнении вы увидите одну причину, по которой можно заинтересоваться простыми числами этой формы. Покажите, что если m – натуральное число, а $2m + 1$ – простое число, то m является степенью 2. (Подсказка: если m не является степенью 2, то m имеет нечетное простое число p в его разложении на простые множители. Следовательно, существует натуральное число r такое, что $m = pr$. Теперь примените решение упражнения 14 из раздела 6.1, чтобы заключить, что $(2^r + 1) \mid (2^m + 1)$.)

19. Пусть x – положительное рациональное число.

- Докажите, что существуют натуральные числа a и b такие, что $x = a/b$ и $\gcd(a, b) = 1$.
- Предположим, что a, b, c и d – натуральные числа, $x = a/b = c/d$ и $\gcd(a, b) = \gcd(c, d) = 1$. Докажите, что $a = c$ и $b = d$.
- Докажите, что существуют простые числа p_1, p_2, \dots, p_k и ненулевые целые числа e_1, e_2, \dots, e_k такие, что $p_1 < p_2 < \dots < p_k$ и

$$x = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}.$$

Обратите внимание, что некоторые из показателей e_i могут быть отрицательными.

- Докажите, что представление x в части (c) уникально. Другими словами, если p_1, p_2, \dots, p_k и q_1, q_2, \dots, q_m – простые числа, e_1, e_2, \dots, e_k и f_1, f_2, \dots, f_m – ненулевые целые числа, $p_1 < p_2 < \dots < p_k$, $q_1 < q_2 < \dots < q_m$ и

$$x = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m},$$

тогда $k = m$ и для всех $i \in \{1, 2, \dots, k\}$, $p_i = q_i$ и $e_i = f_i$.

20. Завершите следующее доказательство того, что $\sqrt{2}$ – иррациональное число. Предположим, что $a/b = \sqrt{2}$, где a и b – натуральные числа. Тогда $a^2 = 2b^2$. Далее получим противоречие, рассматривая показатель степени 2 в разложении на простые множители a и b .

7.3. Модульная арифметика

Предположим, что m – натуральное число. Напомним из определения 4.5.9, что для любых целых чисел a и b мы говорим, что a конгруэнтно b по модулю m , если $m \mid (a - b)$. Мы пишем $a \equiv b \pmod{m}$, или, что короче, $a \equiv_m b$, чтобы указать, что a конгруэнтно b по модулю m . В теореме 4.5.10 мы видели, что \equiv_m является отношением эквивалентности на \mathbb{Z} . Для любого целого числа a пусть $[a]_m$ – класс эквивалентности a относительно отношения эквивалентности \equiv_m . Множество всех этих классов эквивалентности обозначается \mathbb{Z}/\equiv_m . Таким образом:

$$[a]_m = \{b \in \mathbb{Z} \mid b \equiv a \pmod{m}\}, \quad \mathbb{Z}/\equiv_m = \{[a]_m \mid a \in \mathbb{Z}\}.$$

Как мы знаем из теоремы 4.5.4, \mathbb{Z}/\equiv_m является разбиением \mathbb{Z} .

Например, в случае $m = 3$ имеем:

$$\begin{aligned} [0]_3 &= \{b \in \mathbb{Z} \mid b \equiv 0 \pmod{3}\} = \{0, 3, 6, 9, \dots, -3, -6, -9, \dots\}, \\ [1]_3 &= \{b \in \mathbb{Z} \mid b \equiv 1 \pmod{3}\} = \{1, 4, 7, 10, \dots, -2, -5, -8, \dots\}, \\ [2]_3 &= \{b \in \mathbb{Z} \mid b \equiv 2 \pmod{3}\} = \{2, 5, 8, 11, \dots, -1, -4, -7, \dots\}. \end{aligned}$$

Обратите внимание, что каждое целое число является элементом ровно одного из этих классов эквивалентности. Отсюда следует, что каждое целое число конгруэнтно по модулю 3 ровно одному из чисел 0, 1 и 2. Это пример следующей общей теоремы.

Теорема 7.3.1. *Предположим, что m – натуральное число. Тогда для каждого целого числа a существует ровно одно целое число r такое, что $0 \leq r < m$ и $a \equiv r \pmod{m}$.*

Доказательство. Пусть a – произвольное целое число. Пусть q и r будут частным и остатком от деления a на m (см. упражнение 14 в разделе 6.4). Это означает, что $a = qm + r$ и $0 \leq r < m$. Тогда $a - r = qm$, поэтому $m \mid (a - r)$, поэтому $a \equiv r \pmod{m}$. Это доказывает существование искомого целого числа r .

Чтобы доказать единственность, предположим, что r_1 и r_2 – целые числа такие, что $0 \leq r_1 < m$, $0 \leq r_2 < m$, $a = r_1 \pmod{m}$ и $a = r_2 \pmod{m}$. Тогда из симметрии и транзитивности отношения эквивалентности \equiv_m следует $r_1 \equiv r_2 \pmod{m}$, поэтому существует некоторое целое число d такое, что $r_1 - r_2 = dm$. Но из $0 \leq r_1 < m$ и $0 \leq r_2 < m$ мы видим, что $-m < r_1 - r_2 < m$. Таким образом, $-m < dm < m$, что означает, что $-1 < d < 1$. Единственное целое число строго между -1 и 1 – это 0 , поэтому $d = 0$ и, следовательно, $r_1 - r_2 = dm = 0$. Другими словами, $r_1 = r_2$.

Комментарий. Конечно, существование и единственность числа r доказываются раздельно, и доказательство единственности использует обычную стратегию предположения, что r_1 и r_2 – два целых числа с требуемыми свойствами, а затем показывает, что $r_1 = r_2$.

Теорема 7.3.1 утверждает, что каждое целое число конгруэнтно по модулю m ровно с одним элементом множества $\{0, 1, \dots, m - 1\}$. Мы говорим, что это множество является *полной системой вычетов по модулю m* .

Отметим, что по лемме 4.5.5

$a \equiv r \pmod{m}$ тогда и только тогда, когда $a \in [r]_m$ тогда и только тогда, когда $[a]_m = [r]_m$.

Таким образом, теорема 7.3.1 показывает, что каждый класс эквивалентности в \mathbb{Z}/\equiv_m равен ровно одному из классов эквивалентности в списке $[0]_m, [1]_m, \dots, [m - 1]_m$. Таким образом, эти m классов эквивалентности различны и $\mathbb{Z}/\equiv_m = \{[0]_m, [1]_m, \dots, [m - 1]_m\}$.

Рассмотрим любые два класса эквивалентности X и Y в \mathbb{Z}/\equiv_m . Что-то удивительное происходит, если мы складываем или умножаем элементы X и Y . Оказывается, что все суммы вида $x + y$, где $x \in X$ и $y \in Y$, принадлежат одному классу эквивалентности, а также все произведения xy принадлежат одному и тому же классу эквивалентности. Другими словами, мы имеем следующую теорему.

Теорема 7.3.2. Предположим, что m – натуральное число, а X и Y – элементы \mathbb{Z}/\equiv_m . Тогда

1. Существует единственное $S \in \mathbb{Z}/\equiv_m$ такое, что $\forall x \in X \forall y \in Y (x + y \in S)$.
2. Существует единственное $P \in \mathbb{Z}/\equiv_m$ такое, что $\forall x \in X \forall y \in Y (xy \in P)$.

Мы вскоре докажем эту теорему, но сначала воспользуемся ею, чтобы ввести определения двух бинарных операций над \mathbb{Z}/\equiv_m .

Определение 7.3.3. Предположим, что X и Y – элементы \mathbb{Z}/\equiv_m . Для них мы определяем сумму и произведение X и Y , обозначая их $X + Y$ и $X \cdot Y$, следующим образом:

$X + Y =$ единственное $S \in \mathbb{Z}/\equiv_m$ такое, что $\forall x \in X \forall y \in Y (x + y \in S)$,
 $X \cdot Y =$ единственное $P \in \mathbb{Z}/\equiv_m$ такое, что $\forall x \in X \forall y \in Y (xy \in P)$.

Ключом к нашему доказательству теоремы 7.3.2 будет следующая лемма.

Лемма 7.3.4. Предположим, что m – натуральное число. Тогда для всех целых чисел a, a', b и b' если $a' \equiv a \pmod{m}$ и $b' \equiv b \pmod{m}$, то $a' + b' \equiv a + b \pmod{m}$ и $a'b' \equiv ab \pmod{m}$.

Доказательство. Предположим, что $a' \equiv a \pmod{m}$ и $b' \equiv b \pmod{m}$. Тогда $m | (a' - a)$ и $m | (b' - b)$, поэтому мы можем выбрать целые числа c и d такие, что $a' - a = cm$ и $b' - b = dm$, или, другими словами, $a' = a + cm$ и $b' = b + dm$. Следовательно, $(a' + b') - (a + b) = (a + cm + b + dm) - (a + b) = cm + dm = (c + d)m$, поэтому $m | ((a' + b') - (a + b))$, что означает $a' + b' \equiv a + b \pmod{m}$. Аналогично, $a'b' - ab = (a + cm)(b + dm) - ab = adm + bcm + cdm^2 = (ad + bc + cdm)m$, поэтому $m | (a'b' - ab)$, и, следовательно, $a'b' \equiv ab \pmod{m}$.

Доказательство теоремы 7.3.2. Поскольку X и Y являются элементами \mathbb{Z}/\equiv_m , мы можем обозначить как a и b целые числа, такие что $X = [a]_m$ и $Y = [b]_m$. Для

доказательства части 1 теоремы примем $S = [a + b]_m$. Теперь возьмем произвольные элементы $x \in X$ и $y \in Y$. Тогда $x \in [a]_m$ и $y \in [b]_m$, поэтому $x = a(\text{mod } m)$ и $y = b(\text{mod } m)$. По лемме 7.3.4 следует, что $x + y \equiv a + b(\text{mod } m)$, поэтому $x + y \in [a + b]_m = S$. Поскольку x и y произвольны, мы заключаем, что $\forall x \in X \forall y \in Y (x + y \in S)$.

Чтобы доказать единственность S , предположим, что S' – другой класс эквивалентности – такой, что $\forall x \in X \forall y \in Y (x + y \in S')$. Поскольку $a \in X$ и $b \in Y$, то $a + b \in S$ и $a + b \in S'$. Следовательно, S и S' не пересекаются, и поскольку \mathbb{Z}/\equiv_m попарно не пересекается, отсюда следует, что $S = S'$.

Доказательство части 2 аналогично с использованием $P = [ab]_m$; см. упражнение 2.

Доказательство теоремы 7.3.2 говорит о том, что если $X = [a]_m$ и $Y = [b]_m$, то сумма X и Y является классом эквивалентности $S = [a + b]_m$, а произведение $P = [ab]_m$. Отсюда вытекает следующая теорема.

Теорема 7.3.5. Для любого натурального числа m и любых целых чисел a и b выполняются равенства

$$[a]_m + [b]_m = [a + b]_m \quad \text{и} \quad [a]_m \cdot [b]_m = [ab]_m.$$

Давайте попробуем эти идеи. Рассмотрим случай $m = 5$. Мы знаем, что каждый элемент \mathbb{Z}/\equiv_5 равен либо $[0]_5$, $[1]_5$, $[2]_5$, $[3]_5$, либо $[4]_5$, и мы будем часто записывать классы эквивалентности в одной из этих форм. Например, $[2]_5 + [4]_5 = [6]_5$, но также $6 \equiv 1(\text{mod } 5)$, поэтому $[6]_5 = [1]_5$. Таким образом, можно сказать, что $[2]_5 + [4]_5 = [1]_5$. Аналогично $[2]_5 \cdot [4]_5 = [8]_5 = [3]_5$. В табл. 7.4 приведен полный перечень значений операций сложения и умножения для \mathbb{Z}/\equiv_5 .

Таблица 7.4. Результаты сложения и умножения для \mathbb{Z}/\equiv_5

+	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

•	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

Как сложение и умножение в \mathbb{Z}/\equiv_m соотносятся со сложением и умножением в \mathbb{Z} ? Многие свойства сложения и умножения в \mathbb{Z} легко переносятся в \mathbb{Z}/\equiv_m .

Теорема 7.3.6. Предположим, что m – натуральное число. Тогда для всех классов эквивалентности X , Y и Z в \mathbb{Z}/\equiv_m :

1. $X + Y = Y + X$. (Сложение коммутативно.)
2. $(X + Y) + Z = X + (Y + Z)$. (Сложение ассоциативно.)
3. $X + [0]_m = X$. ($[0]_m$ – элемент тождественности для сложения.)
4. Существует такой $X' \in \mathbb{Z}/\equiv_m$, что $X + X' = [0]_m$. (X имеет аддитивную инверсию.)

5. $X \cdot Y = Y \cdot X$. (Умножение коммутативно.)
6. $(X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)$. (Умножение ассоциативно.)
7. $X \cdot [1]_m = X$. ($[1]_m$ – единичный элемент для умножения.)
8. $X \cdot [0]_m = [0]_m$.
9. $X \cdot (Y + Z) = (X \cdot Y) + (X \cdot Z)$. (Умножение распространяется на слагаемые.)

Доказательство. Поскольку $X, Y, Z \in \mathbb{Z}/\equiv_m$, существуют целые числа a, b и c такие, что $X = [a]_m$, $Y = [b]_m$ и $Z = [c]_m$. В части 1 мы используем коммутативность сложения по \mathbb{Z} :

$$X + Y = [a]_m + [b]_m = [a + b]_m = [b + a]_m = [b]_m + [a]_m = Y + X.$$

Доказательство части 2 построено аналогично. Для доказательства части 3 вычислим

$$X + [0]_m = [a]_m + [0]_m = [a + 0]_m = [a]_m = X.$$

Для части 4 пусть $X' = [-a]_m$. Далее

$$X + X' = [a]_m + [-a]_m = [a + (-a)]_m = [0]_m.$$

Доказательства остальных частей аналогичны (см. упражнение 3).

В упражнении 4 вам нужно показать, что элементы тождественности и обратные элементы в теореме 7.3.6 уникальны. Таким образом, в части 3 теоремы мы можем сказать, что $[0]_m$ – это не просто элемент тождественности, но и вполне уникальный элемент тождественности для сложения, и аналогично $[1]_m$ является элементом тождественности для умножения. В части 4 мы можем сказать, что X' является уникальным противоположным элементом X ; мы будем обозначать противоположный элемент X как $-X$. Например, согласно табл. 7.4 для \mathbb{Z}/\equiv_5 $[4]_5 + [1]_5 = [0]_5$, поэтому $-[4]_5 = [1]_5$.

А как насчет обратимости относительно умножения? Если $X \in \mathbb{Z}/\equiv_m$, $X' \in \mathbb{Z}/\equiv_m$ и $X \cdot X' = [1]_m$, то мы говорим, что X' является обратной величиной относительно умножения (мультипликативной инверсией) X . Например, согласно табл. 7.4 для \mathbb{Z}/\equiv_5 : $[3]_5 \cdot [2]_5 = [1]_5$, поэтому $[2]_5$ является мультипликативной инверсией $[3]_5$. Фактически в \mathbb{Z}/\equiv_5 каждому элементу, кроме $[0]_5$, сопоставлена мультипликативная инверсия. Мультипликативные инверсии, если они существуют, также уникальны (см. упражнение 4). В общем, если $X \in \mathbb{Z}/\equiv_m$, то мультипликативная инверсия X , если она существует, обозначается X^{-1} . Таким образом, $[3]_5^{-1} = [2]_5$.

Небольшой эксперимент показывает, что мультипликативных инверсий часто не существует. Например, вы можете самостоятельно убедиться, что в \mathbb{Z}/\equiv_6 только $[1]_6$ и $[5]_6$ имеют мультипликативные инверсии (см. упражнение 1). Когда у класса эквивалентности есть мультипликативная инверсия? Ответ дает наша следующая теорема.

Теорема 7.3.7. Пусть a и m – натуральные числа. Тогда $[a]_m$ имеет мультипликативную инверсию, если и только если a и m взаимно просты.

Доказательство. Предположим сначала, что $[a]_m$ имеет мультипликативную инверсию; скажем, $[a]_m^{-1} = [a']_m$. Тогда $[a]_m \cdot [a']_m = [aa']_m = [1]_m$, и, следовательно, $aa' \equiv 1 \pmod{m}$. Это означает, что $m \mid (aa' - 1)$, поэтому мы можем выбрать такое целое число c , что $aa' - 1 = cm$, или, что то же самое, $cm + a'a = 1$. Таким образом, 1 является линейной комбинацией m и a , и согласно упражнению 6 в из предыдущего раздела следует, что m и a взаимно просты.

Для доказательства в обратном направлении предположим, что m и a взаимно просты. Тогда по теореме 7.1.4 существуют натуральные числа s и t такие, что $sm + ta = 1$. Следовательно, $ta - 1 = -sm$, поэтому $ta \equiv 1 \pmod{m}$. Мы заключаем, что $[a]_m \cdot [t]_m = [ta]_m = [1]_m$, поэтому $[t]_m$ является мультипликативной инверсией $[a]_m$.

Комментарий. Обратите внимание, что заключение теоремы является биусловным утверждением, и в доказательстве используется обычная стратегия доказательства обоих направлений биусловия по отдельности.

Доказательство теоремы 7.3.7 показывает, что для любых натуральных чисел m и a мы можем использовать расширенный алгоритм Евклида, чтобы найти $[a]_m^{-1}$. Если алгоритм показывает, что $\gcd(m, a) \neq 1$, то $[a]_m^{-1}$ не существует, но если мы обнаружим, что $\gcd(m, a) = 1 = sm + ta$, то $[a]_m^{-1} = [t]_m$.

Пример 7.3.8. Найдите, если возможно, мультипликативные инверсии $[34]_{847}$ и $[35]_{847}$ для \mathbb{Z}/\equiv_{847} .

Решение

В табл. 7.5 показано вычисление $\gcd(847, 34)$ по расширенному алгоритму Евклида. Мы заключаем, что $\gcd(847, 34) = 1 = 11 \cdot 847 - 274 \cdot 34$, и, следовательно, $[34]_{847}^{-1} = [-274]_{847} = [573]_{847}$. Как вы легко можете проверить, $34 \cdot 573 = 19\,482 = 1 \pmod{847}$, поэтому $[34]_{847} \cdot [573]_{847} = [19\,482]_{847} = [1]_{847}$.

Таблица 7.5. Расчет $\gcd(847, 34)$ по расширенному алгоритму Евклида

n	q_n	r_n	s_n	t_n	Деление
0		847	1	0	
1		34	0	1	$847 = 24 \cdot 34 + 31$
2	24	31	1	-24	$34 = 1 \cdot 31 + 3$
3	1	3	-1	25	$31 = 10 \cdot 3 + 1$
4	10	1	11	-274	$3 = 3 \cdot 1 + 0$
5	3	0			

Самостоятельно убедитесь, что $\gcd(847, 35) = 7$. Следовательно, $[35]_{847}$ не имеет мультипликативной инверсии.

Пример 7.3.9. В классе 25 учеников. На Пасху учитель купил несколько коробок яиц, по дюжине яиц в каждой, а затем раздал их ученикам, чтобы они украсили их. После того как каждому ученику раздали равное количество яиц, у него осталось 7 яиц. Какое наименьшее количество коробок с яйцами он мог бы купить?

Решение

Пусть x будет количеством коробок яиц, купленных учителем. Итак, у него было $12x$ яиц, и осталось 7 яиц, после того как яйца были разделены поровну между 25 учениками. Поэтому $25 \mid (12x - 7)$, то есть $12x \equiv 7 \pmod{25}$. Мы должны найти наименьшее натуральное число x , удовлетворяющее этой конгруэнтности.

Если бы мы решали уравнение $12x = 7$ для действительного числа x , мы бы знали, что делать. Если $12x = 7$, то, умножая обе части уравнения на $1/12$, мы заключаем, что $x = 7/12$. Фактически это рассуждение можно перевернуть: если $x = 7/12$, то, умножая на 12, мы получаем $12x = 7$. Таким образом, уравнения $12x = 7$ и $x = 7/12$ эквивалентны, откуда следует, что $x = 7/12$ – единственное решение уравнения $12x = 7$.

К сожалению, мы работаем с конгруэнтностью $12x \equiv 7 \pmod{25}$, которая не является уравнением. Но мы можем превратить ее в уравнение, работая с классами эквивалентности. Наша конгруэнтность эквивалентна уравнению $[12]_{25} \cdot [x]_{25} = [7]_{25}$, и мы можем решить это уравнение, повторяя наше решение уравнения $12x = 7$. Начнем с нахождения мультипликативной инверсии $[12]_{25}$. Применяя расширенный алгоритм Евклида, мы находим, что $\gcd(25, 12) = 1 = 1 \cdot 25 - 2 \cdot 12$, поэтому $[12]_{25}^{-1} = [-2]_{25} = [23]_{25}$.

Чтобы решить уравнение $[12]_{25} \cdot [x]_{25} = [7]_{25}$, умножим обе части на $[12]_{25}^{-1} = [23]_{25}$. Я подробно распишу все шаги, чтобы было понятно, как используются свойства из теоремы 7.3.6:

$$\begin{aligned}[12]_{25} \cdot [x]_{25} &= [7]_{25}, \\ [12]_{25}^{-1} \cdot ([12]_{25} \cdot [x]_{25}) &= [12]_{25}^{-1} \cdot [7]_{25}, \\ ([12]_{25}^{-1} \cdot [12]_{25}) \cdot [x]_{25} &= [23]_{25} \cdot [7]_{25}, \\ [1]_{25} \cdot [x]_{25} &= [161]_{25} = [11]_{25}, \\ [x]_{25} &= [11]_{25}.\end{aligned}$$

Как и раньше, эти шаги можно поменять местами: умножение обеих частей уравнения $[x]_{25} = [11]_{25}$ на $[12]_{25}$ дает нам $[12]_{25} \cdot [x]_{25} = [7]_{25}$. Следовательно:

$$\begin{aligned}12x \equiv 7 \pmod{25} \text{ тогда и только тогда, когда } [12]_{25} \cdot [x]_{25} &= [7]_{25} \\ \text{тогда и только тогда, когда } [x]_{25} &= [11]_{25} \\ \text{тогда и только тогда, когда } x &\in [11]_{25}.\end{aligned}$$

Другими словами, решения конгруэнтности $12x \equiv 7 \pmod{25}$ – это в точности элементы класса эквивалентности $[11]_{25}$, а наименьшее положительное решение $-x = 11$. Если учитель купил 11 коробок яиц, то у него было 132 яйца, и после того, как он раздал по 5 каждому ученику, у него осталось еще 7.

В этом примере нам повезло, что 25 и 12 были взаимно простыми числами, так что $[12]_{25}$ имеет мультипликативную инверсию. Она сыграла решающую роль в нашем решении конгруэнтности $12x \equiv 7 \pmod{25}$. Как мы можем решить конгруэнтность вида $ax \equiv b \pmod{m}$, если m и a не являются взаимно простыми? Мы не будем подробно анализировать такие конгруэнтности, но рассмотрим несколько примеров, иллюстрирующих, как они могут быть решены с помощью следующих двух теорем.

Теорема 7.3.10. Пусть m и a – натуральные числа, и пусть $d = \gcd(m, a)$. Тогда для каждого целого числа b если $d \nmid b$, то не существует такого целого числа x , что $ax \equiv b \pmod{m}$.

Доказательство. См. упражнение 7.

Теорема 7.3.11. Предположим, что n и m – натуральные числа. Тогда для всех целых чисел a и b

$na \equiv nb \pmod{nm}$ тогда и только тогда, когда $a \equiv b \pmod{m}$.

Доказательство. См. упражнение 8.

Пример 7.3.12. Решите следующие конгруэнтности:

$$77x \equiv 120 \pmod{374}, \quad 77x \equiv 121 \pmod{374}.$$

Решение

Начнем с вычисления $\gcd(374, 77) = 11$. Поскольку $11 \nmid 120$, теорема 7.3.10 говорит нам, что первая конгруэнтность, $77x = 120 \pmod{374}$, не имеет решений. Чтобы решить вторую конгруэнтность, мы сначала запишем ее как $11 \cdot 7x \equiv 11 \cdot 11 \pmod{11 \cdot 34}$, а затем заметим, что по теореме 7.3.11 это эквивалентно $7x = 11 \pmod{34}$. Чтобы решить это сравнение, мы вычисляем, что $\gcd(34, 7) = 1 = -1 \cdot 34 + 5 \cdot 7$, поэтому $[7]_{34}^{-1} = [5]_{34}$. Следовательно:

$$\begin{aligned} 7x \equiv 11 \pmod{34}, \text{ тогда и только тогда, когда } [7]_{34} \cdot [x]_{34} \equiv [11]_{34} \\ \text{тогда и только тогда, когда } [x]_{34} = [7]_{34}^{-1} \cdot [11]_{34} = [5]_{34} \cdot [11]_{34} = [55]_{34} = [21]_{34} \\ \text{тогда и только тогда, когда } x \in [21]_{34}. \end{aligned}$$

Таким образом, решения второй конгруэнтности являются элементами $[21]_{34}$.

Упражнения

1. Составьте таблицы сложения и умножения для \mathbb{Z}/\equiv_6 .
2. Завершите доказательство теоремы 7.3.2.
3. Докажите п. 5–9 теоремы 7.3.6.
- *4. Пусть m – натуральное число.
 - (a) Предположим, что Z_1 и Z_2 являются аддитивными элементами идентичности для \mathbb{Z}/\equiv_m ; другими словами, для всех $X \in \mathbb{Z}/\equiv_m$ $X + Z_1 = X$ и $X + Z_2 = X$. Докажите, что $Z_1 = Z_2$. Это равенство говорит о том, что аддитивный единичный элемент в \mathbb{Z}/\equiv_m единственен. (Подсказка: вычислите $Z_1 + Z_2$ двумя разными способами.)
 - (b) Предположим, что $X \in \mathbb{Z}/\equiv_m$ и X'_1 и X'_2 оба аддитивно инверсны для X ; другими словами, $X + X'_1 = X + X'_2 = [0]_m$. Докажите, что $X'_1 = X'_2 = [0]_m$. Это равенство говорит о том, что аддитивная инверсия X уникальна. (Подсказка: вычислите $X'_1 + X + X'_2$. Двумя разными способами.)

- (c) Докажите, что мультиликативный единичный элемент в \mathbb{Z}/\equiv_m уникален.
- (d) Докажите, что если класс эквивалентности $X \in \mathbb{Z}/\equiv_m$ имеет мультиликативную инверсию, то эта инверсия уникальна.
5. Докажите, что если p – простое число, то каждый элемент \mathbb{Z}/\equiv_p , кроме $[0]_p$, имеет мультиликативную инверсию.
6. Если $ab = 0(\text{mod } m)$, обязательно ли, что $a = 0(\text{mod } m)$ или $b = 0(\text{mod } m)$? Обоснуйте свой ответ либо доказательством, либо контрпримером.
7. Докажите теорему 7.3.10.
- *8. Докажите теорему 7.3.11.
9. В классе 26 учеников. Учитель купил несколько наборов закладок, каждый из которых содержал по 20 закладок. Когда он раздал закладки ученикам, то обнаружил, что ему нужно добавить 2 дополнительные закладки со своего стола, чтобы иметь возможность раздать каждому студенту одинаковое количество закладок. Если каждый ученик получил от 10 до 20 закладок, сколько наборов купил учитель?
- *10. Решите следующие конгруэнтности.
- $40x \equiv 8(\text{mod } 237)$.
 - $40x \equiv 8(\text{mod } 236)$.
11. Решите следующие конгруэнтности.
- $31x \equiv 24(\text{mod } 384)$.
 - $32x \equiv 24(\text{mod } 384)$.
12. Предположим, что стул без подлокотников стоит 35 долларов, а стул с подлокотниками стоит 50 долларов. Если Алиса потратила 720 долларов на стулья, сколько стульев каждого вида она купила?
- Покажите, что если x – количество стульев без подлокотников, которые она купила, то $35x \equiv 20(\text{mod } 50)$.
 - Решите конгруэнтность в части (a).
 - Не каждое решение конгруэнтности в части (a) приводит к ответу на задание. Какие именно решения подходят? (Примечание: существует несколько возможных ответов на задание.)
13. Пусть m и n – взаимно простые положительные целые числа. Докажите, что для всех целых чисел a и b $a \equiv b(\text{mod } m)$ тогда и только тогда, когда $na \equiv nb(\text{mod } m)$.
14. Пусть m_1 и m_2 – натуральные числа. Докажите, что для всех целых чисел a и b если $a \equiv b(\text{mod } m_1)$ и $a \equiv b(\text{mod } m_2)$, то $a \equiv b(\text{mod lcm}(m_1, m_2))$. (Подсказка: используйте упражнение 11 из раздела 7.2.)
15. Докажите, что для всех натуральных чисел m , a и b если $a \equiv b(\text{mod } m)$, то $\gcd(m, a) = \gcd(m, b)$.
16. Пусть $a \equiv b(\text{mod } m)$. Докажите, что для любого натурального числа n $a^n \equiv b^n(\text{mod } m)$.

В упражнениях 17–19 используются следующие обозначения. Если $d_0, d_1, \dots, d_k \in \{0, 1, \dots, 9\}$, то $(d_k \cdots d_1 d_0)_{10}$ – число, представление которого в десятичной системе счисления равно $dk \cdots d_1 d_0$. Другими словами:

$$(d_k \cdots d_1 d_0)_{10} = d_0 + 10d_1 + \cdots + 10^k d_k.$$

17. Предположим, что $n = (d \cdots dd)_{10}$.
- (a) Докажите, что $n \equiv (d_0 + d_1 + \cdots + d_k) \pmod{3}$.
 - (b) Покажите, что $3 \mid n$ тогда и только тогда, когда $3 \mid (d_0 + d_1 + \cdots + d_k)$. (Это дает удобный способ проверить натуральное число на делимость на 3: сложить цифры и проверить, делится ли сумма цифр на 3.)
18. Пусть $n = (dk \cdots d_1 d_0)_{10}$.
- (a) Докажите, что $n \equiv (d_0 - d_1 + d_2 - d_3 + \cdots + (-1)^k d_k) \pmod{11}$.
 - (b) Покажите, что $11 \mid n$, если и только если $11 \mid (d_0 - d_1 + \cdots + (-1)^k d_k)$.
 - (c) Делится ли 535 172 на 11?
19. Определим функцию f с областью определения $\{n \in \mathbb{Z} \mid n \geq 10\}$ следующим образом: если $n = (d_k \cdots d_1 d_0)_{10}$, то $f(n) = (d_k \cdots d_1)_{10} + 5d_0$. Например, $f(1743) = 174 + 5 \cdot 3 = 189$.
- (a) Покажите, что для всех $n \geq 10$ $f(n) \equiv 5n \pmod{7}$ и $n \equiv 3f(n) \pmod{7}$.
 - (b) Покажите, что для всех $n \geq 10$ утверждение $7 \mid n$ истинно, если и только если $7 \mid f(n)$. (Это дает удобный способ проверить большое целое число n на делимость на 7: многократно применяйте f , пока не получите число, делимость которого на 7 легко определить.)
 - (c) Проверьте, делится ли 627 334 на 7.
20. (a) Найдите пример натуральных чисел m, a, a', b и b' таких, что $a' \equiv a \pmod{m}$ и $b' \equiv b \pmod{m}$, но $(a')^{b'} \not\equiv a^b \pmod{m}$.
- (b) Покажите, что невозможно определить операцию возведения в степень через классы эквивалентности таким образом, чтобы для всех натуральных чисел m, a и b было истинно утверждение $(a')^{b'} \not\equiv a^b \pmod{m}$.
21. Предположим, что m – натуральное число. Определим $f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}/\equiv_m$ формулой $f(a, b) = [a + b]_m$ и определим $h: (\mathbb{Z}/\equiv_m) \times (\mathbb{Z}/\equiv_m) \rightarrow \mathbb{Z}/\equiv_m$ по формуле $h(X, Y) = X + Y$. Сравните это упражнение с упражнением 21 в разделе 5.1.
- (a) Покажите, что для всех целых чисел x_1, x_2, y_1 и y_2 если $x_1 \equiv_m y_1$ и $x_2 \equiv_m y_2$, то $f(x_1, x_2) = f(y_1, y_2)$. (Расширяя терминологию упражнения 21 в разделе 5.1, мы могли бы сказать, что f совместима с \equiv_m)
 - (b) Покажите, что для всех целых чисел x_1 и x_2 , $h([x_1]_m, [x_2]_m) = f(x_1, x_2)$.

7.4. ТЕОРЕМА ЭЙЛЕРА

В предыдущем разделе вы увидели, что некоторые элементы \mathbb{Z}/\equiv_m имеют мультипликативные обратные значения, а некоторые нет. В этом разделе мы сосредоточимся на тех, у которых обратные значения есть. Обозначим через $(\mathbb{Z}/\equiv_m)^*$ множество элементов \mathbb{Z}/\equiv_m , у которых есть мультипликативные обратные значения. Другими словами:

$$(\mathbb{Z}/\equiv_m)^* = \{X \in \mathbb{Z}/\equiv_m \mid \text{для некоторого } X' \in \mathbb{Z}/\equiv_m, X \cdot X' = [1]_m\}.$$

Число элементов $(\mathbb{Z}/\equiv_m)^*$ обозначается $\varphi(m)$. Функция φ называется *функцией Эйлера*, или *тотальной функцией Эйлера* (также известна под названием *тотиент*, или *функция сумм*); она была предложена Эйлером в 1763 году. Для любого натурального числа m справедливо $(\mathbb{Z}/\equiv_m)^* \subseteq \mathbb{Z}/\equiv_m$ и \mathbb{Z}/\equiv_m имеет m элементов, поэтому $\varphi(m) \leq m$. И $[1]_m \cdot [1]_m = [1]_m$, поэтому $[1]_m \in (\mathbb{Z}/\equiv_m)^*$ и, следовательно, $\varphi(m) \geq 1$. Например,

$$(\mathbb{Z}/\equiv_{10})^* = \{[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}\}.$$

поэтому $\varphi(10) = 4$.

Для наших целей наиболее важными свойствами множества $(\mathbb{Z}/\equiv_m)^*$ является то, что оно замкнуто относительно обращения и умножения. То есть можно сформулировать следующую теорему.

Теорема 7.4.1. Пусть m – натуральное число.

1. Для любого $X \in (\mathbb{Z}/\equiv_m)^*$ справедливо $X^{-1} \in (\mathbb{Z}/\equiv_m)^*$.
2. Для любых X и $Y \in (\mathbb{Z}/\equiv_m)^*$ справедливо $X \cdot Y \in (\mathbb{Z}/\equiv_m)^*$.

Доказательство

1. Предположим, что $X \in (\mathbb{Z}/\equiv_m)^*$. Тогда X имеет мультипликативное обратное X^{-1} , и $X \cdot X^{-1} = [1]_m$. Но это уравнение также говорит нам, что X является мультипликативным обратным для X^{-1} ; другими словами, $(X^{-1})^{-1} = X$. Следовательно, $X^{-1} \in (\mathbb{Z}/\equiv_m)^*$.
2. Предположим, что $X \in (\mathbb{Z}/\equiv_m)^*$ и $Y \in (\mathbb{Z}/\equiv_m)^*$. Тогда X и Y имеют мульти-
пликативные обратные X^{-1} и Y^{-1} . Следовательно:

$$(X \cdot Y) \cdot (X^{-1} \cdot Y^{-1}) = (X \cdot X^{-1}) \cdot (Y \cdot Y^{-1}) = [1]_m \cdot [1]_m = [1]_m.$$

Это означает, что $X^{-1} \cdot Y^{-1}$ является мультипликативным обратным $X \cdot Y$, поэтому $(X \cdot Y)^{-1} = X^{-1} \cdot Y^{-1}$ и $X \cdot Y \in (\mathbb{Z}/\equiv_m)^*$.

Предположим, что $X \in (\mathbb{Z}/\equiv_m)^*$. По теореме 7.4.1 для любого $Y \in (\mathbb{Z}/\equiv_m)^*$ спра-
ведливо $X \cdot Y \in (\mathbb{Z}/\equiv_m)^*$, поэтому мы можем определить функцию $f_X: (\mathbb{Z}/\equiv_m)^* \rightarrow (\mathbb{Z}/\equiv_m)^*$ по формуле $f_X(Y) = X \cdot Y$. Исследуем свойства этой функции.

Прежде всего f_X взаимно однозначна. Чтобы понять, почему это так, пред-
положим, что $Y_1 \in (\mathbb{Z}/\equiv_m)^*$, $Y_2 \in (\mathbb{Z}/\equiv_m)^*$ и $f_X(Y_1) = f_X(Y_2)$. Тогда $X \cdot Y_1 = X \cdot Y_2$, и поэтому

$$Y_1 = [1]_m \cdot Y_1 = X^{-1} \cdot X \cdot Y_1 = X^{-1} \cdot X \cdot Y_2 = [1]_m \cdot Y_2 = Y_2.$$

Это доказывает, что функция f_X взаимно однозначна. Далее мы покажем, что f_X сюръективна. Чтобы доказать это, предположим, что $Y \in (\mathbb{Z}/\equiv_m)^*$. Тогда, поскольку $(\mathbb{Z}/\equiv_m)^*$ замкнуто относительно обращения и умножения, $X^{-1} \cdot Y \in (\mathbb{Z}/\equiv_m)^*$ и

$$f_X(X^{-1} \cdot Y) = X \cdot X^{-1} \cdot Y = [1]_m \cdot Y = Y.$$

Таким образом, f_X сюръективна.

Например, снова рассмотрим случай $m = 10$, и пусть $X = [3]_{10}$. Применение f_X к четырем элементам $(\mathbb{Z}/\equiv_{10})^*$ дает значения, показанные в табл. 7.6. Обратите внимание, что, поскольку f_X взаимно однозначна и сюръективна, каждый из четырех элементов $(\mathbb{Z}/\equiv_{10})^*$ появляется ровно один раз в столбце $f_X(Y)$; каждый элемент появляется хотя бы один раз, потому что f_X сюръективна, и он появляется только один раз, потому что f_X взаимно однозначна. Поэтому записи во втором столбце табл. 7.6 в точности такие же, как записи в первом столбце, но перечислены в другом порядке.

Таблица 7.6. Значения f_X при $X = [3]_{10}$

Y	$f_X(Y)$
$[1]_{10}$	$[3]_{10} \cdot [1]_{10} = [3]_{10}$
$[3]_{10}$	$[3]_{10} \cdot [3]_{10} = [9]_{10}$
$[7]_{10}$	$[3]_{10} \cdot [7]_{10} = [1]_{10}$
$[9]_{10}$	$[3]_{10} \cdot [9]_{10} = [7]_{10}$

В более общем смысле предположим, что m – натуральное число и $X \in (\mathbb{Z}/\equiv_m)^*$. По определению фи-функции Эйлера в $(\mathbb{Z}/\equiv_m)^*$ есть $\varphi(m)$ элементов. Пусть $Y_1, Y_2, \dots, Y_{\varphi(m)}$ – список этих элементов. Тогда, поскольку f_X взаимно однозначна и сюръективна, каждый из этих элементов встречается ровно один раз в списке $f_X(Y_1), f_X(Y_2), \dots, f_X(Y_{\varphi(m)})$. Другими словами, два списка $Y_1, Y_2, \dots, Y_{\varphi(m)}$ и $f_X(Y_1), f_X(Y_2), \dots, f_X(Y_{\varphi(m)})$ содержат совершенно одинаковые записи, только перечисленные в разном порядке, – точно так же, как два столбца в табл. 7.6. Из коммутативных и ассоциативных законов умножения следует, что если мы перемножим все записи в каждом из двух списков, произведения будут одинаковыми (см. упражнение 21 в разделе 6.4):

$$\begin{aligned} Y_1, Y_2, \dots, Y_{\varphi(m)} &= f_X(Y_1), f_X(Y_2), \dots, f_X(Y_{\varphi(m)}) \\ &= (X \cdot Y_1) \cdot (X \cdot Y_2) \cdots (X \cdot Y_{\varphi(m)}) \\ &= X^{\varphi(m)} \cdot (Y_1 \cdot Y_2 \cdots Y_{\varphi(m)}), \end{aligned}$$

где, конечно, под $X^{\varphi(m)}$ мы подразумеваем X , умноженное на себя $\varphi(m)$ раз. Чтобы упростить это уравнение, пусть $Z = Y_1 \cdot Y_2 \cdots Y_{\varphi(m)}$. Тогда уравнение гласит: $Z = X^{\varphi(m)} \cdot Z$. Поскольку $(\mathbb{Z}/\equiv_m)^*$ замкнуто относительно умножения, $Z \in (\mathbb{Z}/\equiv_m)^*$, поэтому оно имеет обратное значение. Умножая обе части уравнения $Z = X^{\varphi(m)} \cdot Z$ на Z^{-1} , получаем

$$[1]_m = Z \cdot Z^{-1} = X^{\varphi(m)} \cdot Z \cdot Z^{-1} = X^{\varphi(m)} \cdot [1]_m = X^{\varphi(m)}.$$

Таким образом, мы доказали следующую теорему.

Теорема 7.4.2. Если m – натуральное число и $X \in (\mathbb{Z}/\equiv_m)^*$, то $X^{\varphi(m)} = [1]_m$.

Чтобы понять значение этой теоремы, можно перефразировать ее в терминах чисел.

Теорема 7.4.3. (Теорема Эйлера.) Пусть m – натуральное число. Тогда для любого положительного целого числа a если $\gcd(m, a) = 1$, то $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Доказательство. Предположим, что a – натуральное число и $\gcd(m, a) = 1$. Тогда по теореме 7.3.7 $[a]_m \in (\mathbb{Z}/\equiv_m)^*$, поэтому по теореме 7.4.2 $[a]_m^{\varphi(m)} = [1]_m$, где $[a]_m^{\varphi(m)}$ обозначает $[a]_m$, умноженное на себя $\varphi(m)$ раз. Но

$$[a]_m^{\varphi(m)} = \underbrace{[a]_m \cdot [a]_m \cdots [a]_m}_{\varphi(m) \text{ множителей}} = \underbrace{[a \cdot a \cdots a]_m}_{\varphi(m) \text{ множителей}} = [a^{\varphi(m)}]_m.$$

(Более подробное доказательство этого уравнения см. в упражнении 5.) Таким образом, $[a^{\varphi(m)}]_m = [a]_m^{\varphi(m)} = [1]_m$ и, следовательно, $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Например, 10 и 7 взаимно прости, поэтому, согласно теореме Эйлера, $7^{\varphi(10)}$ должно быть конгруэнтно 1 по модулю 10. Чтобы проверить это, мы вычисляем

$$7^{\varphi(10)} = 7^4 = 2401 \equiv 1 \pmod{10}.$$

Чтобы применить теорему Эйлера, нам нужно уметь вычислить $\varphi(m)$. Конечно, мы можем проверить все элементы \mathbb{Z}/\equiv_m один за другим и посчитать, сколько из них имеют мультипликативные обратные, как мы сделали в случае $m = 10$, но для больших m это будет непрактично. Остальную часть этого раздела мы посвящаем поиску более эффективного способа вычисления $\varphi(m)$.

Начнем с перефразирования определения $\varphi(m)$. Мы знаем, что $\{0, 1, \dots, m - 1\}$ является полной системой вычетов по модулю m , но поскольку $0 \equiv m \pmod{m}$, мы также можем сказать, что $\{1, 2, \dots, m\}$ – полная система вычетов. Таким образом, $\mathbb{Z}/\equiv_m = \{[1]_m, [2]_m, \dots, [m - 1]_m, [m]_m\} = \{[a]_m \mid 1 \leq a \leq m\}$, где каждый элемент \mathbb{Z}/\equiv_m появляется в этом списке элементов ровно один раз. Чтобы определить, какие из этих элементов входят в $(\mathbb{Z}/\equiv_m)^*$, мы используем теорему 7.3.7, которая говорит нам, что для любого положительного целого числа a значение $[a]_m$ имеет мультипликативное обратное тогда и только тогда, когда m и a взаимно прости. Таким образом:

$$(\mathbb{Z}/\equiv_m)^* = \{[a]_m \mid 1 \leq a \leq m \text{ и } \gcd(m, a) = 1\}.$$

Это дает нам еще одно толкование фи-функции Эйлера:

$$\varphi(m) = \text{количество элементов в множестве } \{a \mid 1 \leq a \leq m \text{ и } \gcd(m, a) = 1\}.$$

Используя эту характеристику фи-функции, легко вычислить $\varphi(p)$, когда p простое: если $1 \leq a \leq p - 1$, то $p \nmid a$, и, следовательно, $\gcd(p, a) = 1$, но $\gcd(p, p) = p > 1$. Таким образом,

$$\{a \mid 1 \leq a \leq p \text{ и } \gcd(p, a) = 1\} = \{1, 2, \dots, p - 1\},$$

так что $\varphi(p) = p - 1$. Фактически почти так же легко вычислить $\varphi(p^k)$ для любого натурального k . Если a – натуральное число и $p \mid a$, то $\gcd(p^k, a) \geq p > 1$, но если $p \nmid a$, то единственный общий делитель p^k и a равен 1, поэтому $\gcd(p^k, a) = 1$. Таким образом, элементы множества $\{a \mid 1 \leq a \leq p^k\}$, которые

не являются взаимно простыми с p^k , – это в точности те элементы, которые делятся на p , и этими элементами являются $p, 2p, 3p, \dots, p^k = p^{k-1}p$. Другими словами,

$$\{a \mid 1 \leq a \leq p^k \text{ и } \gcd(p^k, a) = 1\} = \{1, 2, \dots, p^k\} \setminus \{p, 2p, \dots, p^{k-1}p\},$$

и количество элементов в этом множестве равно $p^k - p^{k-1} = p^{k-1}(p - 1)$. Таким образом, $\varphi(p^k) = p^{k-1}(p - 1)$.

Чтобы вычислить $\varphi(m)$ для других значений m , мы используем следующую теорему, которую докажем позже в этом разделе.

Теорема 7.4.4. *Предположим, что m и n – взаимно простые положительные целые числа. Тогда $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.*

Функция f от положительных целых чисел к действительным числам называется *мультипликативной функцией*, если она обладает тем свойством, что для всех относительно простых положительных целых чисел m и n $f(mn) = f(m) \cdot f(n)$. Таким образом, теорема 7.4.4 утверждает, что функция Эйлера является мультипликативной. Ряд других важных функций в теории чисел также мультипликативны, но φ – единственная подобная функция, которую мы будем изучать в этой книге. (Еще два примера см. в упражнениях 16 и 17.)

Теорема 7.4.4 позволяет нам использовать факторизацию любого натурального числа m для нахождения $\varphi(m)$. Предположим, что факторизация m равна $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, где p_1, p_2, \dots, p_k – простые числа и $p_1 < p_2 < \cdots < p_k$. Тогда $p_1^{e_1}$ и $p_2^{e_2} \cdots p_k^{e_k}$ взаимно прости, потому что у них нет общих простых множителей (см. упражнение 5 в разделе 7.2), следовательно, $\varphi(m) = \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2} \cdots p_k^{e_k})$.

Повторяя это рассуждение, мы заключаем, что

$$\begin{aligned}\varphi(m) &= \varphi(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \varphi(p_1^{e_1}) \cdot \varphi(p_2^{e_2}) \cdots \varphi(p_k^{e_k}) \\ &= p_1^{e_1-1}(p_1 - 1) \cdot p_2^{e_2-1}(p_2 - 1) \cdots p_k^{e_k-1}(p_k - 1).\end{aligned}$$

Например, $600 = 2^3 \cdot 3 \cdot 5^2$, поэтому

$$\varphi(600) = \varphi(2^3 \cdot 3 \cdot 5^2) = 2^2(2 - 1) \cdot 3^0(3 - 1) \cdot 5^1(5 - 1) = 160.$$

Это было намного проще, чем явно перечислить 160 элементов $(\mathbb{Z}/\equiv_{600})^*$!
Наше доказательство теоремы 7.4.4 будет зависеть от трех лемм.

Лемма 7.4.5. *Предположим, что m и n – взаимно простые натуральные числа. Тогда для всех целых чисел a и b $a \equiv b \pmod{mn}$ тогда и только тогда, когда $a \equiv b \pmod{m}$ и $a \equiv b \pmod{n}$.*

Доказательство. См. упражнение 6.

Лемма 7.4.6. *Для всех натуральных чисел a, b и c $\gcd(ab, c) = 1$ тогда и только тогда, когда $\gcd(a, c) = 1$ и $\gcd(b, c) = 1$.*

Доказательство. См. упражнение 7.

Лемма 7.4.7. Предположим, что m и n – взаимно простые натуральные числа. Тогда для всех целых чисел a и b существует некоторое целое число r такое, что $1 \leq r \leq mn$, $r \equiv a \pmod{m}$ и $r \equiv b \pmod{n}$.

Доказательство. Пусть a и b – произвольные целые числа. Поскольку m и n взаимно просты, существуют целые числа s и t такие, что $sm + tn = 1$. Следовательно, $tn - 1 = -sm$ и $sm - 1 = -tn$. Пусть $x = tna + smb$. Тогда

$$x - a = (tn - 1)a + smb = -sma + smb = sm(b - a),$$

значит, $m \mid (x - a)$, поэтому $x \equiv a \pmod{m}$. Также

$$x - b = tna + (sm - 1)b = tna - tnb = tn(a - b),$$

значит, $n \mid (x - b)$ и $x \equiv b \pmod{n}$.

Поскольку $\{1, 2, \dots, mn\}$ – полная система вычетов по модулю mn , мы можем найти такое целое число r , что $r \equiv x \pmod{mn}$ и $1 \leq r \leq mn$. По лемме 7.4.5 $r \equiv x \pmod{m}$ и $r \equiv x \pmod{n}$, а из транзитивности \equiv_m и \equiv_n следует, что $r \equiv a \pmod{m}$ и $r \equiv b \pmod{n}$.

Комментарий. После введения произвольных целых чисел a и b целью является экистенциальное утверждение. Как это часто бывает при доказательстве экистенциальных утверждений, доказательство вводит число x , никак не объясняя выбор x . Оказывается, число x имеет множество свойств, которые нам нужны, но, возможно, не все из них, поскольку оно может и не лежать между 1 и mn . Поэтому нам нужен дополнительный шаг, чтобы найти число r , обладающее всеми необходимыми свойствами.

Для доказательства теоремы 7.4.4 нам понадобится еще одна идея. Предположим, что A – это множество из p элементов, а B – это множество из q элементов; скажем, $A = \{a_1, a_2, \dots, a_p\}$ и $B = \{b_1, b_2, \dots, b_q\}$. Тогда $A \times B$ имеет pq элементов. Чтобы понять, почему, представьте, что элементы $A \times B$ располагаются в таблице с упорядоченной парой (a_i, b_j) в строке i , столбце j таблицы. Поскольку таблица будет иметь p строк и q столбцов, $A \times B$ должно иметь pq элементов. Более детальное доказательство этого факта см. в упражнении 22 в разделе 8.1.

Теперь мы готовы доказать, что φ – мультиплекативная функция.

Доказательство теоремы 7.4.4. Пусть $R = \{a \mid 1 \leq a \leq mn \text{ и } \gcd(mn, a) = 1\}$. По лемме 7.4.6 если $a \in R$, то $\gcd(m, a) = 1$ и $\gcd(n, a) = 1$, поэтому $[a]_m \in (\mathbb{Z}/\equiv_m)^*$ и $[a]_n \in (\mathbb{Z}/\equiv_n)^*$. Таким образом, мы можем определить функцию $f: R \rightarrow (\mathbb{Z}/\equiv_m)^* \times (\mathbb{Z}/\equiv_n)^*$ по формуле $f(a) = ([a]_m, [a]_n)$. Наш план состоит в том, чтобы показать, что f взаимно однозначна и сюръективна, что означает, что множества R и $(\mathbb{Z}/\equiv_m)^* \times (\mathbb{Z}/\equiv_n)^*$ имеют одинаковое количество элементов. Но R имеет $\varphi(mn)$ элементов, а $(\mathbb{Z}/\equiv_m)^* \times (\mathbb{Z}/\equiv_n)^*$ имеет $\varphi(m) \cdot \varphi(n)$ элементов, откуда следует, что $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Чтобы показать, что f взаимно однозначна, предположим, что $a_1 \in R$, $a_2 \in R$ и $f(a_1) = f(a_2)$. Это означает, что $([a_1]_m, [a_1]_n) = ([a_2]_m, [a_2]_n)$, поэтому $[a_1]_m = [a_2]_m$ и $[a_1]_n = [a_2]_n$, и поэтому $a_1 = a_2 \pmod{m}$ и $a_1 = a_2 \pmod{n}$. По лемме 7.4.5 следует, что $a_1 = a_2 \pmod{mn}$. Но поскольку $\{a \mid 1 \leq a \leq mn\}$ – полная система

вычетов по модулю mn , никакие два различных элемента R не конгруэнтны по модулю mn , поэтому $a_1 = a_2$. Это завершает доказательство того, что f взаимно однозначно.

Наконец, чтобы показать, что f сюръективна, пусть $([a]_m, [b]_n)$ будет произвольным элементом $(\mathbb{Z}/\equiv_m)^* \times (\mathbb{Z}/\equiv_n)^*$. По лемме 7.4.7 существует такое целое число r , что $1 \leq r \leq mn$, $r \equiv a \pmod{m}$ и $r \equiv b \pmod{n}$. Следовательно, $[r]_m = [a]_m \in (\mathbb{Z}/\equiv_m)^*$ и $[r]_n = [b]_n \in (\mathbb{Z}/\equiv_n)^*$, поэтому по теореме 7.3.7 $\gcd(m, r) = \gcd(n, r) = 1$. Применяя лемму 7.4.6, приходим к выводу, что $\gcd(mn, r) = 1$. Следовательно, $r \in R$ и $f(r) = ([r]_m, [r]_n) = ([a]_m, [b]_n)$, что показывает, что f сюръективна.

Упражнения

1. Перечислите элементы $(\mathbb{Z}/\equiv_m)^*$.
- *2. Найдите $\varphi(m)$:
 - (a) $m = 539$.
 - (b) $m = 540$.
 - (c) $m = 541$.
3. Проверьте эти примеры теоремы Эйлера, вычислив $a^{\varphi(m)}$ и убедившись, что $a^{\varphi(m)} \equiv 1 \pmod{m}$.
 - (a) $m = 18, a = 5$.
 - (b) $m = 19, a = 2$.
 - (c) $m = 20, a = 3$.
4. Проверьте эти примеры леммы 7.4.7, найдя целое число r такое, что $1 \leq r \leq mn$, $r \equiv a \pmod{m}$ и $r \equiv b \pmod{n}$.
 - (a) $m = 5, n = 8, a = 4, b = 1$.
 - (b) $m = 7, n = 10, a = 6, b = 4$.
5. Предположим, что m и a – натуральные числа. Используйте математическую индукцию, чтобы доказать, что для любого натурального числа n $[a]^n_m = [a^n]_m$.
- *6. Докажите лемму 7.4.5.
7. Докажите лемму 7.4.6.
- *8. Покажите, что если в лемме 7.4.5 мы откажемся от предположения о том, что m и n взаимно просты, то одно направление утверждения «тогда и только тогда» будет правильным, а другое – нет. Обоснуйте свой ответ, приведя доказательство в пользу одного направления и контрпример для другого.
9. Если мы откажемся от гипотезы о взаимной простоте m и n из леммы 7.4.7, верна ли лемма? Обоснуйте свой ответ, приведя доказательство или контрпример.
10. Докажите малую теорему Ферма, которая гласит, что если p – простое число, то для любого натурального числа a выполняется $a^p \equiv a \pmod{p}$.

11. Докажите, что если m и a – взаимно простые положительные целые числа, то $[a]_m^{-1} = [a^{\varphi(m)-1}]_m$.
12. Докажите, что для всех натуральных чисел m, a, p и q справедливо утверждение: если m и a взаимно просты и $p \equiv q \pmod{\varphi(m)}$, то $a^p \equiv a^q \pmod{m}$.
13. Докажите, что если a, b_1, b_2, \dots, b_k – натуральные числа и $\gcd(a, b_1) = \gcd(a, b_2) = \dots = \gcd(a, b_k) = 1$, то $\gcd(a, b_1 b_2 \cdots b_k) = 1$.
14. Предположим, что m_1, m_2, \dots, m_k – попарно взаимно простые натуральные числа; т. е. для всех $i, j \in \{1, 2, \dots, k\}$ если $i \neq j$, то $\gcd(m_i, m_j) = 1$. Пусть $M = m_1 m_2 \cdots m_k$. Докажите, что для всех целых чисел a и b $a \equiv b \pmod{M}$ тогда и только тогда, когда для каждого $i \in \{1, 2, \dots, k\}$, $a \equiv b \pmod{m_i}$.
15. Докажите китайскую теорему об остатках. (Теорема была впервые сформулирована китайским математиком Сунь Цзы в III в.)
 - (a) Предположим, что m_1, m_2, \dots, m_k – попарно взаимно простые натуральные числа; т. е. для всех $i, j \in \{1, 2, \dots, k\}$, если $i \neq j$, то $\gcd(m_i, m_j) = 1$. Пусть $M = m_1 m_2 \cdots m_k$. Докажите, что для всех целых чисел a_1, a_2, \dots, a_k существует целое число r такое, что $1 \leq r \leq M$ и для всех $i \in \{1, 2, \dots, k\}$ $r \equiv a_i \pmod{m_i}$. (Подсказка: используйте индукцию по k . На шаге индукции используйте лемму 7.4.7. Вы также найдете полезными упражнения 13 и 14.)
 - (b) Докажите, что целое число r в части (a) уникально.
16. Для каждого натурального числа n пусть $\tau(n)$ = количество элементов $D(n)$. Например, $D(6) = \{1, 2, 3, 6\}$, поэтому $\tau(6) = 4$. Докажите, что τ – мультипликативная функция. Предположим, что m и n – взаимно простые положительные целые числа.
 - (a) Докажите, что если $a \in D(m)$ и $b \in D(n)$, то $ab \in D(mn)$.
 - (b) Согласно части (a), мы можем определить функцию $f: D(m) \times D(n) \rightarrow D(mn)$ по формуле $f(a, b) = ab$. Докажите, что f взаимно однозначна и сюръективна.
 - (c) Докажите, что $\tau(mn) = \tau(m) \cdot \tau(n)$, что указывает на мультипликативность τ .
17. Для каждого натурального числа n пусть $\sigma(n)$ = сумма всех элементов $D(n)$. Например, $D(6) = \{1, 2, 3, 6\}$, поэтому $\sigma(6) = 1 + 2 + 3 + 6 = 12$. Докажите, что σ – мультипликативная функция. (Подсказка: используйте функцию f из части (b) упражнения 16.)
18. Докажите теорему Евклида о совершенных числах. Напомним, что натуральное число n называется *совершенным*, если n равно сумме всех делителей числа n , меньших n . Можно сказать иначе: n совершенно, если $\sigma(n) = 2n$, где σ – функция, определенная в упражнении 17. Докажите, что если p – натуральное число, а $2^p - 1$ – простое число, то $2^{p-1}(2^p - 1)$ совершенно. (Подсказка: вам пригодятся упражнение 17 и пример 6.1.1.)
19. Докажите теорему Эйлера о совершенных числах. Предположим, что n – четное совершенное число. (Как и в упражнении 18, сказать, что n совершенно, означает, что $\sigma(n) = 2n$, где σ – функция, определенная в упражнении 17.)

- (a) Докажите, что существуют натуральные числа k и m такие, что $n = 2^k m$ и m нечетно.
- (b) Докажите, что $2^{k+1}m = (2^{k+1} - 1)\sigma(m)$.
- (c) Докажите, что $2^{k+1} \mid \sigma(m)$. Таким образом, существует натуральное число d такое, что $\sigma(m) = 2^{k+1}d$.
- (d) Докажите, что $m = (2k + 1 - 1)d$.
- (e) Докажите, что $d = 1$. (Подсказка: предположим, что $d > 1$. Тогда $1, d$ и m являются различными делителями m , поэтому $\sigma(m) \geq 1 + d + m$. Получили противоречие.)
- (f) Пусть $p = k + 1$. Тогда из пунктов (a), (d) и (e) следует, что $n = 2^{p-1}(2p - 1)$. Докажите, что $2p - 1$ – простое число и, соответственно, n – совершенное число, рассмотренное в упражнении 18.

7.5. КРИПТОГРАФИЯ С ОТКРЫТЫМ КЛЮЧОМ

Предположим, вы хотите совершить покупку в интернете. Вы переходите на сайт продавца и размещаете заказ. Затем веб-сайт просит вас ввести номер вашей кредитной карты. Вы вводите номер карты на своем компьютере, и он должен передать номер через интернет на компьютер продавца.

В интернете любые данные обычно проходят через несколько компьютеров на пути от отправителя к получателю. В результате существует вероятность того, что кто-то, имеющий доступ к одному из этих промежуточных компьютеров, может подслушивать, когда ваш компьютер отправляет продавцу номер вашей кредитной карты. Чтобы такой перехватчик не украл номер вашей кредитной карты, ваш компьютер шифрует (кодирует) номер перед его отправкой. Затем компьютер продавца расшифровывает (декодирует) номер и списывает средства с вашей кредитной карты.

Например, предположим, что номер вашей кредитной карты представляет собой 16-значную последовательность $m = m_1 m_2 \dots m_{16}$. Каждая m_i – это одна из цифр $0, 1, 2, \dots, 9$, но мы будем думать об этом как о представлении класса эквивалентности $[m_i]_{10} \in \mathbb{Z}/\equiv_{10}$. Если ваш компьютер и компьютер продавца могут согласовать случайную последовательность цифр $k = k_1 k_2 \dots k_{16}$, тогда они могут действовать следующим образом, выполняя все вычисления в \mathbb{Z}/\equiv_{10} . Ваш компьютер может заменить i -ю цифру m_i номера вашей кредитной карты на цифру c_i , так что $[c_i]_{10} = [m_i]_{10} + [k_i]_{10}$. Ваш компьютер отправит 16-значную последовательность $c = c_1 c_2 \dots c_{16}$ на компьютер продавца, который затем восстановит исходную последовательность m по формуле $[m_i]_{10} = [c_i]_{10} + (-[k_i]_{10})$. Последовательность k – это *ключ*, который ваш компьютер использует для шифрования номера кредитной карты, а компьютер продавца – для его расшифровки. Злоумышленник, не знающий ключа k , не сможет расшифровать зашифрованное сообщение c и узнать номер вашей кредитной карты m .

Но как ваш компьютер и компьютер продавца могут согласовать ключ k ? Если один компьютер выбирает ключ и отправляет его другому, то перехватчик может узнать ключ и затем расшифровать зашифрованное сообщение.

Безопасная отправка ключа так же сложна, как отправка номера кредитной карты, поэтому, похоже, мы не добились каких-либо успехов.

Проблема с этой схемой заключается в том, что она использует *симметричную криптографию*, в которой один и тот же ключ используется как для шифрования, так и для дешифрования. Решением проблемы является использование *криптографии с открытым ключом*, в которой ключи шифрования и дешифрования разные. Компьютер продавца создает два ключа: один для шифрования и один для дешифрования. Он отправляет ключ шифрования на ваш компьютер. Ваш компьютер использует ключ шифрования для шифрования номера вашей кредитной карты, а затем отправляет зашифрованный номер на компьютер продавца, который использует свой ключ дешифрования для восстановления номера кредитной карты. Злоумышленник может узнать ключ шифрования, поэтому этот ключ считается открытым. Но это никак не поможет злодею, потому что для дешифрования требуется другой ключ, который никогда никому не передается и остается секретным.

Вас может удивить, что можно иметь разные ключи для шифрования и дешифрования, но это возможно. В этом разделе мы обсудим одну хорошо известную систему шифрования с открытым ключом под названием RSA. Она названа в честь Рона Ривеста (Ron Rivest, род. 1947), Ади Шамира (Adi Shamir, род. 1952) и Леонарда Адлемана (Leonard Adleman, род. 1945), которые разработали систему в 1977 году. Аналогичная система была разработана в 1973 году Клиффордом Коксом (1950–), математиком, который работал на британскую разведку, но она была засекречена до 1997 года. Как вы увидите, система RSA основана на теореме Эйлера.

Мы представили идею криптографии с открытым ключом в контексте покупок в интернете, но ее можно использовать в любой ситуации, когда один человек хочет отправить сообщение другому, не давая злоумышленнику возможности прочитать его. Предположим, Алиса хочет безопасно отправить сообщение Бобу. Чтобы использовать систему открытых ключей RSA, они должны поступить следующим образом. Сначала Боб выбирает два различных простых числа p и q . Он вычисляет $n = pq$ и $\varphi(n) = (p - 1)(q - 1)$. Затем он выбирает положительное целое число e такое, что e и $\varphi(n)$ взаимно просты и $e < \varphi(n)$. По теореме 7.3.7 $[e]_{\varphi(n)}$ имеет мультипликативное обратное в $\mathbb{Z}/\equiv_{\varphi(n)}$, которое может быть вычислено с помощью расширенного алгоритма Евклида. Таким образом, Боб может вычислить положительное целое число d такое, что $d < \varphi(n)$ и $[e]_{\varphi(n)} \cdot [d]_{\varphi(n)} = [1]_{\varphi(n)}$, что означает, что $ed \equiv 1 \pmod{\varphi(n)}$. Боб отправляет Алисе пару чисел (n, e) ; это ключ шифрования, который Алиса будет использовать для шифрования своего сообщения. Боб держит в секрете числа p , q и d ; он будет использовать d для расшифровки сообщений Алисы.

Предположим, что сообщение, которое Алиса хочет отправить, является натуральным числом $m < n$. Конечно, ее сообщение может быть отрывком текста, а не числом, но отрывок текста может быть закодирован как натуральное число. Если текст длинный, возможно, потребуется закодировать его как последовательность натуральных чисел, каждое из которых меньше n , и тогда каждое из этих натуральных чисел придется зашифровать отдельно. Но для простоты обсуждения мы предположим, что сообщение Алисы представляет собой одно натуральное число $m < n$.

Как и раньше, мы рассматриваем сообщение m как представление класса эквивалентности $[m]_n \in \mathbb{Z}/\equiv_n$, и Алиса и Боб будут выполнять все свои вычисления, используя арифметику в \mathbb{Z}/\equiv_n . Чтобы зашифровать свое сообщение, Алиса вычисляет $[m]^e_n$; другими словами, она вычисляет уникальное натуральное число $c < n$ такое, что $[m]^e_n = [c]_n$. Число c – это зашифрованное сообщение, которое она отправляет Бобу.

Чтобы расшифровать сообщение, Боб вычисляет $[c]^d_n$. Что заставляет систему RSA работать, так это удивительный факт, что $[c]^d_n = [m]_n$, как мы докажем ниже.

Таким образом, вычисляя $[c]^d_n$, Боб может восстановить исходное сообщение m . Обратите внимание, что и шифрование, и дешифрование включают возвведение в степень, но показатель шифрования e и показатель расшифровки d различаются. Таким образом, не имеет значения, узнает ли перехватчик e ; пока Боб хранит d в секрете, перехватчик не будет знать, какой показатель степени использовать для расшифровки зашифрованного сообщения.

Чтобы показать, что RSA работает, нам нужно доказать следующую теорему.

Теорема 7.5.1. Предположим, что p и q – разные простые числа, $n = pq$, e и d – такие натуральные числа, что $ed \equiv 1 \pmod{\phi(n)}$, а m и c – такие натуральные числа, что $[m]^e_n = [c]_n$. Тогда справедлива эквивалентность $[c]^d_n = [m]_n$.

Доказательство. Если $e = d = 1$, то $[m]_n = [c]_n$, и истинность вывода очевидна. Если это условие не выполняется, то $ed > 1$, поэтому, поскольку $ed \equiv 1 \pmod{\phi(n)}$, существует некоторое положительное целое число k такое, что $ed - 1 = k\phi(n)$, и, следовательно, $ed = k\phi(n) + 1 = k(p - 1)(q - 1) + 1$. А поскольку $[m]^d_n = [c]_n$, мы имеем $m^e \equiv c \pmod{n}$, поэтому $n \mid (m^e - c)$.

Хотя в конечном итоге мы хотим сделать вывод об арифметике в \mathbb{Z}/\equiv_n , мы сочтем полезным сначала выполнить некоторые вычисления в \mathbb{Z}/\equiv_p и \mathbb{Z}/\equiv_q . Поскольку $p \mid n$ и $n \mid (m^e - c)$, то в силу транзитивности отношения делимости $p \mid (m^e - c)$. Следовательно, $m^e \equiv c \pmod{p}$, или, что эквивалентно: $[m]^d_p = [c]_p$.

Обратите внимание, что обычные правила возвведения в степень применимы и для возвведения в степень в \mathbb{Z}/\equiv_p . В частности, для любого $X \in \mathbb{Z}/\equiv_p$ и любых натуральных чисел a и b имеем:

$$X^a \cdot X^b = \underbrace{X \cdots X}_{a \text{ множителей}} \cdot \underbrace{X \cdots X}_{b \text{ множителей}} = \underbrace{X \cdots X}_{a+b \text{ множителей}} = X^{a+b}$$

И

$$(X^a)^b = \underbrace{X \cdots X}_{a \text{ множителей}} \cdot \underbrace{\underbrace{X \cdots X}_{a \text{ множителей}} \cdots \underbrace{X \cdots X}_{a \text{ множителей}}}_{b \text{ групп множителей}} = \underbrace{X \cdots X}_{ab \text{ множителей}} = X^{ab}.$$

(Более подробные доказательства этих уравнений см. в упражнении 8.) Применяя эти правила, мы видим, что

$$c_p^d = ([m]_p^e)^d = [m]_p^{ed} = [m]_p^{k(p-1)(q-1)+1} = ([m]_p^{p-1})^{k(q-1)} \cdot [m]_p.$$

Далее мы утверждаем, что $[c]_p^d = [m]_p$. Чтобы доказать истинность данного утверждения, рассмотрим два случая.

Случай 1. $p \nmid m$. Тогда p и m взаимно просты, поэтому по теореме Эйлера $[m]_p^{p-1} = [1]_p$. Следовательно:

$$[c]_p^d = ([m]_p^{p-1})^{k(q-1)} \cdot [m]_p = [1]_p^{k(q-1)} \cdot [m]_p = [1]_p \cdot [m]_p = [m]_p.$$

Случай 2. $p \mid m$. Тогда $[m]_p = [0]_p$, поэтому

$$[c]_p^d = [m]_p^{ed} = [0]_p^{ed} = [0]_p = [m]_p.$$

В обоих случаях мы пришли к искомому выводу, что $[c]_p^d = [m]_p$. Следовательно, $c^d \equiv m \pmod{p}$. Аналогичные рассуждения показывают, что $c^d \equiv m \pmod{q}$, а поскольку $pq = n$, по лемме 7.4.5 следует, что $c^d \equiv m \pmod{n}$. Другими словами, $[c]_n^d = [m]_n$, что и требовалось доказать.

Давайте попробуем это на простом примере. Предположим, Боб выбирает простые числа $p = 3$ и $q = 11$, поэтому $n = pq = 33$ и $\varphi(n) = (p-1)(q-1) = 20$. Он также выбирает $e = 7$, а затем вычисляет $[e]_{\varphi(n)}^{-1} = [7]_{20}^{-1} = [3]_{20}$, откуда $d = 3$. (Проверяя работу Боба, обратите внимание: $[7]_{20} \cdot [3]_{20} = [21]_{20} = [1]_{20}$.) Боб отправляет числа $n = 33$ и $e = 7$ Алисе.

Предположим, Алиса хочет отправить Бобу сообщение $m = 5$. Она вычисляет

$$[m]_n^e = [5]_{33}^7 = [78\ 125]_{33} = [14]_{33},$$

следовательно, ее зашифрованное сообщение $c = 14$. Она отправляет это число Бобу. Чтобы расшифровать сообщение, Боб вычисляет

$$[c]_n^d = [14]_{33}^3 = [2744]_{33} = [5]_{33}.$$

Таким образом, Боб успешно восстанавливает исходное сообщение $m = 5$.

Безопасно ли общение Алисы и Боба? Предположим, что злоумышленник перехватывает как сообщение Боба Алисе, так и сообщение Алисы Бобу, таким образом узнавая числа $n = 33$, $e = 7$ и $c = 14$. Найдя разложение на простые множители $n = 33 = 3 \cdot 11$, злоумышленник может узнать, что $p = 3$ и $q = 11$ (или наоборот), и поэтому $\varphi(n) = (p-1)(q-1) = 20$. Но тогда злоумышленник может вычислить, как это сделал Боб, что $[e]_{\varphi(n)}^{-1} = [7]_{20}^{-1} = [3]_{20}$, таким образом узнав показатель степени дешифрования $d = 3$. Теперь перехватчик может расшифровать сообщение Алисы точно так же, как это сделал Боб. Связь не защищена!

Что пошло не так? Проблема в том, что в этом простом примере мы использовали маленькие числа. Первым шагом злоумышленника будет поиск разложения $n = 33$ на простые множители, которыми являются два простых числа. Небольшое число n можно легко разложить на множители просто делением n на все меньшие простые числа до тех пор, пока не будет найден простой множитель, но если n велико, эта процедура займет слишком много времени, чтобы быть практически полезной. Особенно сложно разложить на множители числа, которые являются произведением двух больших

простых чисел. По состоянию на 2019 год самое большое такое число, которое когда-либо раскладывали на простые множители, представляет собой произведение двух 116-значных простых чисел. Разложение было найдено в 2009 году после двух лет вычислений на многих сотнях компьютеров, работающих одновременно, что эквивалентно почти 2000 лет вычислений на одном компьютере. Разложение на множители произведения простых чисел, значительно больших, чем это, с нынешними вычислительными технологиями считается практически невозможным. Сегодня большинство людей, использующих RSA, выбирают простые числа, состоящие из нескольких сотен цифр. Если злоумышленник узнает числа n и e , то в принципе у него достаточно информации, чтобы найти расшифровочный показатель степени d , но единственный известный способ сделать это – разложить n на простые множители. Безопасность RSA зависит от того факта, что на практике используемые числа настолько велики, что факторизация n за разумное время невозможна.

Но постойте! А как насчет вычислений, которые Алиса и Боб должны делать с этими чрезвычайно большими числами? Будут ли они также вычислительно невыполнимы? Если так, то система бесполезна. К счастью, существуют эффективные способы выполнения вычислений, требуемых от Алисы и Боба. Хотя подробное обсуждение того, как выполняются эти вычисления, выходит за рамки данной книги, мы можем кратко прокомментировать основные моменты.

Самые сложные вычисления, которые предстоит выполнить Алисе и Бобу:

- Боб должен найти два больших простых числа p и q ;
- Боб должен найти $[e]_{\phi(n)}^{-1}$;
- Алиса должна вычислить $[m]_n^e$, а Боб – $[c]_n^d$.

Чтобы найти простые числа p и q , Боб может просто случайным образом выбирать достаточно большие числа и проверять их на простоту, пока не найдет два простых числа. Проблема проверки большого числа на простоту широко изучена. В 2019 году, используя самые известные методы, компьютер мог определить, является ли 1000-значное число простым, за несколько минут. Но это недостаточно быстро для использования RSA, поскольку Бобу, возможно, придется проверить простоту сотен чисел, прежде чем он найдет простое число. Поэтому большинство реализаций RSA используют вероятностные тесты на простоту. Эти тесты занимают доли секунды, но их точность не гарантируется; в частности, если число не простое, есть вероятность, что тест не обнаружит этого и сообщит, что число простое. Но если повторить тест несколько раз, вероятность ошибки можно сделать сколь угодно малой. Подробнее о вероятностном тестировании говорится в упражнениях 10–14.

Мы уже знаем метод, который Боб может использовать для вычисления $[e]_{\phi(n)}^{-1}$ – это расширенный алгоритм Евклида. Этот алгоритм очень быстро работает даже с огромными числами. Подробнее об этом см. в упражнении 13 в разделе 7.1.

Наконец, чтобы зашифровать и расшифровать сообщения, Алиса и Боб должны возвести элементы \mathbb{Z}/\equiv_n в большую степень. Предположим, что $X \in \mathbb{Z}/\equiv_n$ и a – натуральное число. Самый простой способ вычислить X^a – умножить X на себя несколько раз, но это невозможно, если a большое. Есть более

удачный способ использовать рекурсию. Если $a = 1$, то, конечно, $X^a = X$. Для больших значений a мы используем следующие формулы:

$$\begin{aligned} X^{2k} &= X^k \cdot X^k; \\ X^{2k+1} &= X^k \cdot X^k \cdot X. \end{aligned}$$

Пример 7.5.2. Найдите $[347]_{582}^{172}$.

Решение

Пусть $X = [347]_{582} \in \mathbb{Z}/\equiv_{582}$; мы должны найти X^{172} . Поскольку 172 – четное число, мы начинаем с вычисления

$$X^{172} = X^{2 \cdot 86} = X^{86} \cdot X^{86}.$$

Если мы сможем найти X^{86} , нам просто нужно будет умножить его на себя, чтобы найти X^{172} . Чтобы найти X^{86} , мы используем тот же метод:

$$X^{86} = X^{2 \cdot 43} = X^{43} \cdot X^{43}.$$

Теперь нам нужно найти X^{43} , и поскольку 43 нечетно, воспользуемся формулой

$$X^{43} = X^{2 \cdot 21 + 1} = X^{21} \cdot X^{21} \cdot X.$$

Продолжая таким образом, мы получаем следующий список формул:

$$\begin{aligned} X^{172} &= X^{86} \cdot X^{86}, \\ X^{86} &= X^{43} \cdot X^{43}, \\ X^{43} &= X^{21} \cdot X^{21} \cdot X, \\ X^{21} &= X^{10} \cdot X^{10} \cdot X, \\ X^{10} &= X^5 \cdot X^5, \\ X^5 &= X^2 \cdot X^2 \cdot X, \\ X^2 &= X^1 \cdot X^1 = X \cdot X. \end{aligned}$$

Теперь мы можем работать с этим списком в обратном порядке и вычислять каждую формулу:

$$\begin{aligned} X^2 &= X \cdot X = [347]_{582} \cdot [347]_{582} = [120409]_{582} = [517]_{582}, \\ X^5 &= X^2 \cdot X^2 \cdot X = [517]_{582} \cdot [517]_{582} \cdot [347]_{582} = [92749283]_{582} = [17]_{582}, \\ X^{10} &= X^5 \cdot X^5 = [17]_{582} \cdot [17]_{582} = [289]_{582}, \\ X^{21} &= X^{10} \cdot X^{10} \cdot X = [289]_{582} \cdot [289]_{582} \cdot [347]_{582} = [28981787]_{582} = [515]_{582}, \\ X^{43} &= X^{21} \cdot X^{21} \cdot X = [515]_{582} \cdot [515]_{582} \cdot [347]_{582} = [92033075]_{582} = [251]_{582}, \\ X^{86} &= X^{43} \cdot X^{43} = [251]_{582} \cdot [251]_{582} = [63001]_{582} = [145]_{582}, \\ X^{172} &= X^{86} \cdot X^{86} = [145]_{582} \cdot [145]_{582} = [21025]_{582} = [73]_{582}. \end{aligned}$$

Мы заключаем, что $[347]_{582}^{172} = [73]_{582}$. Если вы посчитаете, то обнаружите, что мы выполнили только 10 умножений – намного меньше, чем 171, которые потребовались бы, если бы мы просто взялись перемножать 172 числа X . Поглубже о количестве умножений, необходимых для вычисления X^a в целом, см. упражнение 9.

Мы заканчиваем этот раздел еще одним примером использования RSA. На этот раз мы будем использовать числа, которые достаточно велики, чтобы заставить нас использовать эффективные методы вычислений, хотя они все еще не такие большие, как те, которые используются в реальном приложении RSA.

Пример 7.5.3. Предположим, Боб выбирает простые числа $p = 48611$ и $q = 37813$. Он вычисляет $n = pq = 1\ 838\ 127\ 743$ и $\varphi(n) = (p-1)(q-1) = 1\ 838\ 041\ 320$. Затем он выбирает показатель степени шифрования $e = 184\ 270\ 657$.

1. Найдите показатель степени дешифрования d .
2. Предположим, Алиса хочет отправить сообщение $m = 357\ 249\ 732$. Найдите зашифрованное сообщение c и убедитесь, что Боб может его расшифровать.

Решения

1. Для вычисления d Боб использует расширенный алгоритм Евклида, чтобы найти $[e]_{\varphi(n)}^{-1} = [184\ 270\ 657]_{1\ 838\ 041\ 320}^{-1}$. Вычислительные шаги показаны в табл. 7.7. Боб заключает, что $d = 88\ 235\ 833$.

Таблица 7.7. Вычисление показателя степени дешифрования d

n	q_n	r_n	s_n	t_n
0		1 838 041 320	1	0
1		184 270 657	0	1
2	9	179 605 407	1	-9
3	1	4 665 250	-1	10
4	38	2 325 907	39	-389
5	2	13 436	-79	788
6	173	1479	13 706	-136 713
7	9	125	-123 433	1 231 205
8	11	104	1 371 469	-1 3679 968
9	1	21	-1 494 902	14 911 173
10	4	20	7 351 077	-73 324 660
11	1	1	-8 845 979	88 235 833
12	20	0		

В качестве проверки Боб может вычислить, что

$$ed - 1 = 16\ 259\ 274\ 917\ 852\ 280 = 8\ 845\ 979\varphi(n),$$

так что $ed \equiv 1 \pmod{\varphi(n)}$.

2. Пусть $X = [m]_n = [357\ 249\ 732]_{1\ 838\ 127\ 743}$. Чтобы зашифровать свое сообщение, Алиса должна вычислить $X^e = X^{184\ 270\ 657}$. Вычислительные шаги показаны в табл. 7.8. Конечно, Алиса планирует свои вычисления, начиная с конца этой таблицы, но выполняет вычисления с самого начала. Она отправляет зашифрованное сообщение $c = 1\ 357\ 673\ 396$.

Таблица 7.8. Вычисление зашифрованного сообщения с

k	X^k	k	X^k
2	$[413\ 387\ 288]_n$	44 987	$[418\ 397\ 817]_n$
5	$[1\ 105\ 456\ 936]_n$	89 975	$[1\ 597\ 035\ 021]_n$
10	$[1\ 522\ 283\ 045]_n$	179 951	$[1\ 491\ 451\ 285]_n$
21	$[1\ 773\ 257\ 888]_n$	359 903	$[954\ 701\ 208]_n$
43	$[638\ 596\ 171]_n$	719 807	$[1\ 817\ 497\ 177]_n$
87	$[664\ 005\ 337]_n$	1 439 614	$[1\ 774\ 588\ 706]_n$
175	$[661\ 296\ 271]_n$	2 879 229	$[1\ 061\ 291\ 500]_n$
351	$[993\ 223\ 048]_n$	5 758 458	$[21\ 397\ 340]_n$
702	$[1\ 294\ 276\ 724]_n$	11 516 916	$[1\ 624\ 593\ 674]_n$
1405	$[1\ 088\ 781\ 967]_n$	23 033 832	$[1\ 474\ 914\ 774]_n$
2811	$[1\ 010\ 306\ 117]_n$	46 067 664	$[1\ 189\ 097\ 151]_n$
5623	$[1\ 064\ 784\ 897]_n$	92 135 328	$[46\ 825\ 442]_n$
11246	$[1\ 739\ 950\ 485]_n$	184 270 657	$[1\ 357\ 673\ 396]_n$
22493	$[799\ 178\ 524]_n$		

Чтобы расшифровать сообщение, Боб присваивает значение $Y = [c]_n$ и вычисляет $Y^d = Y^{88235833}$, как показано в табл. 7.9. Как и ожидалось, он получает $m = 357\ 249\ 732$.

Таблица 7.9. Расшифровка сообщения

k	Y^k	k	Y^k
2	$[42\ 593\ 275]_n$	21 541	$[120\ 530\ 669]_n$
5	$[1\ 698\ 473\ 378]_n$	43 083	$[189\ 879\ 402]_n$
10	$[1\ 210\ 371\ 791]_n$	86 167	$[781\ 925\ 623]_n$
21	$[1\ 085\ 519\ 751]_n$	172 335	$[1\ 276\ 315\ 424]_n$
42	$[1\ 335\ 983\ 514]_n$	344 671	$[1\ 511\ 938\ 429]_n$
84	$[1\ 212\ 154\ 100]_n$	689 342	$[1\ 116\ 941\ 725]_n$
168	$[638\ 363\ 154]_n$	1 378 684	$[748\ 516\ 067]_n$
336	$[1\ 695\ 419\ 879]_n$	2 757 369	$[590\ 443\ 992]_n$
673	$[250\ 463\ 254]_n$	5 514 739	$[1\ 169\ 450\ 853]_n$
1346	$[1\ 092\ 090\ 842]_n$	11 029 479	$[83\ 459\ 512]_n$
2692	$[149\ 835\ 148]_n$	22 058 958	$[643\ 822\ 280]_n$
5385	$[1\ 009\ 240\ 318]_n$	44 117 916	$[1\ 032\ 113\ 647]_n$
10 770	$[1\ 219\ 871\ 219]_n$	88 235 833	$[357\ 249\ 732]_n$

Упражнения

1. Предположим, Боб выбирает $p = 5$, $q = 11$ и $e = 7$.
 - (а) Найдите n , $\varphi(n)$ и d .
 - (б) Предположим, Алиса хочет отправить сообщение $m = 9$. Найдите зашифрованное сообщение c и убедитесь, что Боб может его расшифровать.
- *2. Предположим, Боб выбирает $p = 71$, $q = 83$ и $e = 1369$.
 - (а) Найдите n , $\varphi(n)$ и d .
 - (б) Предположим, Алиса хочет отправить сообщение $m = 1001$. Найдите зашифрованное сообщение c и убедитесь, что Боб может его расшифровать.
3. Предположим, Боб выбирает $p = 71$ и $q = 83$. Почему $e = 1368$ – плохой выбор?
4. Предположим, Боб выбирает $p = 17\ 389$, $q = 14947$ и $e = 35\ 824\ 631$.
 - (а) Найдите n , $\varphi(n)$ и d .
 - (б) Предположим, Алиса хочет отправить сообщение $m = 123\ 456\ 789$. Найдите зашифрованное сообщение c и убедитесь, что Боб может его расшифровать.
- *5. Вы подслушиваете Алису и Боба. Вы перехватываете сообщение $(n, e) = (493, 129)$, отправленное Алисе Бобом, а затем сообщение $c = 149$, отправленное Бобу Алисой.
 - (а) Разложите n на простые множители.
 - (б) Найдите расшифровочный показатель степени d .
 - (с) Расшифруйте сообщение.
6. Предположим, Алиса и Боб используют RSA. Как обычно, Боб генерировал числа n , e и d и отправил n и e Алисе, но сохранил d в секрете. У Алисы есть сообщение m , представляющее собой контракт, который она хочет отправить на подписание Бобу. Контракт не секретный – она готова отправить его Бобу без шифрования. Но она хочет, чтобы Боб подписал контракт цифровой подписью. Как и обычная подпись, это должно быть сообщение, которое не может подделать посторонний, чтобы Алиса знала, что подпись поставил Боб, а не какой-то самозванец, и Боб не смог позже отрицать, что он подписал контракт. Чтобы создать свою подпись, Боб вычисляет уникальное целое число s такое, что $0 \leq s < n$ и $[m]_n^d = [s]_n$, и отправляет s Алисе.
 - (а) Докажите, что $[s]_n^e = [m]_n$ и если s' – любое целое число такое, что $0 \leq s' < n$ и $s' \neq s$, то $[s']_n^e \neq [m]_n$. Таким образом, Алиса может подтвердить подпись, вычислив $[s]_n^e$ и убедившись, что оно равно $[m]_n$.
 - (б) Почему самозванец не может подделать подпись Боба?
- *7. В этом упражнении вы увидите, почему важно, чтобы p и q были простыми. Предположим, Боб выбирает $p = 9$, $q = 35$ и $e = 95$, не замечая, что 9 и 35 не простые числа. Он вычисляет $n = pq = 315$ и отправляет $(n, e) = (315, 95)$ Алисе.

- (a) Предположим, Алиса хочет отправить сообщение $m = 123$. Какое зашифрованное сообщение с она отправит?
- (b) Боб вычисляет $\varphi = (p - 1)(q - 1) = 272$; он думает, что это $\varphi(n)$, но он ошибается. Чтобы найти показатель степени расшифровки d , он затем вычисляет $[e]_{\varphi}^{-1} = [d]_{\varphi}$. Какое значение d он получит?
- (c) Что получает Боб, когда пытается расшифровать сообщение Алисы, используя расшифровочный показатель степени d из части (b)?
- (d) Каково правильное значение $\varphi(n)$? Какой расшифровочный показатель степени d получил бы Боб, если бы он использовал правильное значение для $\varphi(n)$ и вычислил $[e]_{\varphi(n)}^{-1} = [d]_{\varphi(n)}$? Что получил бы Боб, попытавшись расшифровать сообщение Алисы с этим показателем степени?
8. Предположим, что m – натуральное число и $X \in \mathbb{Z}/\equiv_m$.
- (a) Дайте рекурсивное определение X^a для положительных целых чисел a .
- (b) Используйте математическую индукцию, чтобы доказать, что для всех натуральных чисел a и b справедливо равенство $X^a \cdot X^b = X^{a+b}$.
- (c) Используйте математическую индукцию, чтобы доказать, что для всех натуральных чисел a и b справедливо равенство $(X^a)^b = X^{ab}$.
- *9. Предположим, что $X \in \mathbb{Z}/\equiv_n$. Докажите, что для каждого натурального числа a рекурсивный метод вычисления X^a , проиллюстрированный в примере 7.5.2, использует не более $2\log_2 a$ умножений.

Упражнения 10–14 посвящены вероятностному тестированию на простоту. В этих заданиях мы ищем вычислительный тест, который можно выполнить с натуральным числом n таким образом, что если n простое, то n проходит тест, а если n не простое, то тест провален. Вы убедитесь, что существуют тесты, которые правильно работают во многих случаях (но не во всех).

10. Согласно теореме Эйлера, если n простое и $2 \leq a \leq n - 1$, то $a^{n-1} \equiv 1 \pmod{n}$. Отсюда можно вывести следующий тест на простоту: чтобы проверить, является ли целое число $n > 2$ простым, выберите случайное число $a \in \{2, 3, \dots, n - 1\}$ и проверьте, выполняется ли равенство $a^{n-1} \equiv 1 \pmod{n}$. Если да, то n проходит тест, а если нет, то не проходит. Этот тест называется *тестом Ферма на простоту*, потому что частный случай теоремы Эйлера, на которой он основан, тесно связан с малой теоремой Ферма; см. упражнение 10 в разделе 7.4. Если n простое, то по теореме Эйлера оно гарантированно проходит проверку. К сожалению, составные числа также иногда проходят проверку. Если $2 \leq a \leq n - 1$ и $a^{n-1} \equiv 1 \pmod{n}$, но n не является простым числом, то мы говорим, что n является псевдопростым числом Ферма для основания a ; он проходит тест на простоту Ферма с использованием основания a , даже если он не является простым. Если $2 \leq a \leq n - 1$ и $a^{n-1} \not\equiv 1 \pmod{n}$, то мы говорим, что a является *свидетелем Ферма* для n . Если для n существует свидетель Ферма, то по теореме Эйлера n не является простым числом.
- (a) Покажите, что 15 – псевдопростое число Ферма для основания 4, а 3 – свидетель Ферма для 15.

- (b) Покажите, что если n – псевдопростое число Ферма для основания a , то n и a взаимно просты.
11. Вспомните из упражнения 5 в разделе 6.2, что числа $F_n = 2^{(2^n)} + 1$ называются числами Ферма. Ферма показал, что F_n – простое при $0 \leq n \leq 4$, а Эйлер показал, что F_5 не является простым. Неизвестно, существует ли какое-либо $n > 4$, для которого F_n является простым. В этом упражнении вы покажете, что для каждого натурального числа n справедливо $2^{F_n-1} \equiv 1 \pmod{F_n}$. Таким образом, если F_n не простое, то согласно терминологии упражнения 10 это псевдопростое число Ферма по основанию 2. Другими словами, тест на простоту Ферма в случае $a = 2$ бесполезен для проверки того, является ли F_n простым.
- (a) Покажите, что $2^{(2^n)} \equiv -1 \pmod{F_n}$.
 - (b) Покажите, что $2^{(2^n+1)} \equiv 1 \pmod{F_n}$.
 - (c) Покажите, что $2^{n+1} \mid (F_n - 1)$. (Подсказка: используйте упражнение 12 (а) в разделе 6.3.)
 - (d) Покажите, что $2^{F_n-1} \equiv 1 \pmod{F_n}$. (Подсказка: используйте части (b) и (c) и упражнение 16 в разделе 7.3.)
12. Предположим, что n – целое число больше 2, и пусть $R = \{2, 3, \dots, n - 1\}$. Пусть
- $$R_1 = \{a \in R \mid a^{n-1} \equiv 1 \pmod{n}\},$$
- $$R_2 = R \setminus R_1 = \{a \in R \mid a^{n-1} \not\equiv 1 \pmod{n}\}.$$
- Предположим, что $a \in R_2$ и $\gcd(n, a) = 1$. Тогда a является свидетелем Ферма для n , поэтому n не является простым. (Значение терминов, используемых в этом упражнении, см. в упражнении 10.)
- (a) Покажите, что для каждого $x \in R_1$ существует единственный $y \in R_2$ такой, что $ax \equiv y \pmod{n}$.
 - (b) Согласно части (a), мы можем определить функцию $f: R_1 \rightarrow R_2$ по формуле
- $$f(x) = \text{уникальный } y \in R_2 \text{ такой, что } ax \equiv y \pmod{n}.$$
- Докажите, что функция f взаимно однозначна.
- (c) Используйте часть (b), чтобы сделать вывод, что по крайней мере половина элементов R являются свидетелями Ферма для n . (Это показывает, что с вероятностью не менее $1/2$ n не пройдет тест на простоту Ферма. Если повторить тест с другими значениями a , вероятность неверного результата может быть сколь угодно малой.)
13. Упражнение 12 показывает, что если есть хотя бы один свидетель Ферма для n , который является взаимно простым с n , то тест на простоту Ферма имеет хорошие шансы обнаружить, что n не является простым. К сожалению, существуют составные числа n , для которых такого свидетельства нет. Целое число $n > 2$ называется *числом Кармайкла*, если оно не является простым, но при этом является псевдопростым числом Ферма по основанию a для любого целого числа $a \in \{2, 3, \dots, n - 1\}$ таких, что

a и *n* взаимно просты. Они названы в честь Роберта Дэниела Кармайкла (1879–1967), который их первым изучил. Если *n* – число Кармайкла, то, хотя *n* не является простым, тест на простоту Ферма вряд ли обнаружит этот факт. В 1994 году Уильям Алфорд (1937–2003), Эндрю Грэнвилл (род. 1962) и Карл Померанс (род. 1944) доказали, что чисел Кармайкла бесконечно много. В этом задании вы должны показать, что 561 – это число Кармайкла. (Фактически это наименьшее число Кармайкла.) Мы представляем проверить, что $561 = 3 \cdot 11 \cdot 17$, поэтому 561 не является простым числом. Предположим, что $2 \leq a \leq n - 1$ и $\gcd(561, a) = 1$.

- (a) Покажите, что $a^{560} \equiv 1 \pmod{3}$.
 - (b) Покажите, что $a^{560} \equiv 1 \pmod{11}$.
 - (c) Покажите, что $a^{560} \equiv 1 \pmod{17}$.
 - (d) Покажите, что $a^{560} \equiv 1 \pmod{561}$. (Подсказка: используйте упражнение 14 из раздела 7.4.)
14. Исследуйте математические основы *теста Миллера–Рабина* – широко используемого вероятностного теста на простоту. Он назван в честь Гэри Л. Миллера (род. 1946) и Майкла О. Рабина (род. 1931). Предположим, что *n* – нечетное целое число и *n* > 1.
- (a) Докажите, что существуют натуральные числа *s* и *d* такие, что $n - 1 = 2^s d$ и *d* нечетно.
 - (b) Докажите, что если *n* – простое число, а *b* – такое натуральное число, что $b^2 \equiv 1 \pmod{n}$, то либо $b \equiv 1 \pmod{n}$, либо $b \equiv -1 \pmod{n}$.
Пусть *s* и *d* такие же, как в части (a). Если $2 \leq a \leq n - 1$, $a^d \not\equiv 1 \pmod{n}$ и для всех натуральных чисел $i < s$ справедливо $a^{2^i d} \not\equiv -1$, то *a* называется *свидетелем Миллера–Рабина* по *n*.
 - (c) Докажите, что если существует свидетель Миллера–Рабина по *n*, то *n* не является простым числом. (Подсказка: предположим, что *a* – свидетель Миллера–Рабина по *n*, а *n* простое. Тогда по теореме Эйлера $a^{2^s d} = a^{n-1} \equiv 1 \pmod{n}$. Поэтому мы можем принять за *k* наименьшее натуральное число такое, что $a^{2^k d} \equiv 1 \pmod{n}$. Теперь используйте часть (b), чтобы получить противоречие.)
Тест Миллера–Рабина работает следующим образом: чтобы проверить, является ли нечетное целое число *n* > 1 простым, выберите случайное число $a \in \{2, 3, \dots, n - 1\}$ и проверьте, является ли *a* свидетелем Миллера–Рабина для *n*. Если да, то *n* не проходит тест. Если нет, то *n* проходит тест. Согласно части (c), если *n* простое, то свидетелей Миллера–Рабина нет, поэтому *n* гарантированно пройдет проверку. Можно доказать, что если *n* не простое, то не менее $3/4$ чисел $a \in \{2, 3, \dots, n - 1\}$ являются свидетелями Миллера–Рабина для *n*, поэтому *n* не пройдет проверку с вероятностью не менее $3/4$. Как и в упражнении 12, вероятность неверного результата может быть уменьшена при желании путем повторения теста с разными вариантами выбора *a*.
 - (d) Покажите, что число 13 не является свидетелем Миллера–Рабина для 85, а 14 является таковым.

Глава 8

Бесконечные множества

8.1. Равномощные множества

В этой главе мы обсудим метод сравнения размеров бесконечных множеств. Удивительно, но оказывается, что в определенном смысле бесконечность бывает разных размеров!

Для конечных множеств мы определяем размер множества путем подсчета. Что значит подсчитать количество элементов в множестве? Когда вы подсчитываете элементы в множестве A , вы по очереди указываете на элементы A , произнося слова «один», «два» и т. д. Мы можем толковать процесс подсчета как определение функции f от множества $\{1, 2, \dots, n\}$ к A для некоторого натурального числа n . Для каждого $i \in \{1, 2, \dots, n\}$ мы принимаем за $f(i)$ элемент A , на который вы указываете, когда говорите « i ». Поскольку каждый элемент A указывается ровно один раз, функция f взаимно однозначна и сюръективна. Таким образом, подсчет элементов A – это просто метод установления взаимно однозначного соответствия между множеством $\{1, 2, \dots, n\}$ и A для некоторого натурального числа n . Однозначное соответствие – ключевая идея измерения размеров множеств, а форма $\{1, 2, \dots, n\}$ – это стандарт, по которому мы измеряем размеры конечных множеств. Это наводит нас на следующее определение.

Определение 8.1.1. Пусть A и B – некоторые множества. Мы говорим, что A *равномощно* B , если существует функция $f: A \rightarrow B$, которая взаимно однозначна и сюръективна. Мы будем писать $A \sim B$, чтобы указать, что A равнозначно B . Для каждого натурального числа n пусть $I_n = \{i \in \mathbb{Z}^+ \mid i \leq n\}$. Множество A называется *конечным*, если существует натуральное число n такое, что $I_n \sim A$. В противном случае A *бесконечно*.

В упражнении 6 вы докажете, что если A конечно, то существует ровно одно число n такое, что $I_n \sim A$. Таким образом, имеет смысл определить *количество элементов* конечного множества A как уникальное n такое, что $I_n \sim A$. Это

число также иногда называют *мощностью* A и обозначают $|A|$. Обратите внимание, что согласно этому определению \emptyset конечно и $|\emptyset| = 0$.

Определение равномощности также может применяться к бесконечным множествам, с результатами, которые иногда удивляют. Например, вы можете подумать, что \mathbb{Z}^+ не может быть равномощным \mathbb{Z} , потому что \mathbb{Z} включает не только все положительные целые числа, но также все отрицательные целые числа и ноль. Но рассмотрим функцию $f: \mathbb{Z}^+ \rightarrow \mathbb{Z}$, определенную следующим образом:

$$f(n) = \begin{cases} n/2, & \text{если } n \text{ четное} \\ (1-n)/2, & \text{если } n \text{ нечетное} \end{cases}.$$

Эта запись означает, что для любого положительного целого числа n если n четно, то $f(n) = n/2$, а если n нечетно, то $f(n) = (1-n)/2$. Значения f в табл. 8.1 показывают закономерность, на основании которой можно предположить, что f может быть взаимно однозначной и сюръективной.

Таблица 8.1. Пример значений функции $f(n)$

n	1	2	3	4	5	6	7	...
$f(n)$	0	1	-1	2	-2	3	-3	...

Чтобы проверить это более тщательно, сначала обратите внимание, что для каждого положительного целого числа n если n четно, то $f(n) = n/2 > 0$, а если n нечетно, то $f(n) = (1-n)/2 \leq 0$. Теперь предположим, что n_1 и n_2 – натуральные числа и $f(n_1) = f(n_2)$. Если $f(n_1) = f(n_2) > 0$, то n_1 и n_2 должны быть четными, поэтому уравнение $f(n_1) = f(n_2)$ означает $n_1/2 = n_2/2$, и, следовательно, $n_1 = n_2$. Аналогично, если $f(n_1) = f(n_2) \leq 0$, то n_1 и n_2 оба нечетны, поэтому мы получаем $(1 - n_1)/2 = (1 - n_2)/2$, откуда еще раз следует, что $n_1 = n_2$. Таким образом, f взаимно однозначна.

Чтобы убедиться, что f сюръективна, пусть m будет произвольным целым числом. Если $m > 0$, то пусть $n = 2m$, т. е. четное положительное целое число, а если $m \leq 0$, то пусть $n = 1 - 2m$, т. е. нечетное положительное целое число. В обоих случаях легко проверить, что $f(n) = m$. Таким образом, f является как взаимно однозначной, так и сюръективной, поэтому согласно определению 8.1.1 $\mathbb{Z}^+ \sim \mathbb{Z}$.

Обратите внимание, что функцию f пришлось выбирать очень осторожно. Есть много других функций от \mathbb{Z}^+ к \mathbb{Z} , которые взаимно однозначны, но не сюръективны, или сюръективны, но не взаимно однозначны, или ни то, ни другое, но это не противоречит нашему утверждению, что $\mathbb{Z}^+ \sim \mathbb{Z}$. Согласно определению 8.1.1, чтобы показать, что $\mathbb{Z}^+ \sim \mathbb{Z}$, нам нужно только показать, что существует по крайней мере одна функция от \mathbb{Z}^+ к \mathbb{Z} , которая взаимно однозначна и сюръективна, и, конечно, чтобы доказать это, достаточно привести пример такой функции.

Возможно, еще более удивительным примером является соответствие $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+$. Чтобы продемонстрировать это, мы должны придумать взаимно однозначную и сюръективную функцию $f: \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$. Элементом области

определения этой функции может быть упорядоченная пара (i, j) , где i и j – натуральные числа. В упражнении 12 вы должны показать, что следующая формула определяет функцию от $\mathbb{Z}^+ \times \mathbb{Z}^+$ к \mathbb{Z}^+ , которая взаимно однозначна и сюръективна:

$$f(i, j) = \frac{(i + j - 2)(i + j - 1)}{2} + i.$$

Таблица 8.2 поможет вам понять этот пример.

Таблица 8.2. Пример значений взаимно однозначной сюръективной функции $f(i, j)$

		j				
		1	2	3	4	5
i	1	1	2	4	7	11
	2	3	5	8	12	
	3	6	9	13		
	4	10	14		⋮	
	5	15				

Теорема 8.1.2. Предположим, что $A \sim B$ и $C \sim D$. Тогда:

1. $A \times C \sim B \times D$.
2. Если A и C не пересекаются и B и D не пересекаются, то $A \cup C \sim B \cup D$.

Доказательство. Поскольку $A \sim B$ и $C \sim D$, мы можем выбрать функции $f: A \rightarrow B$ и $g: C \rightarrow D$, которые взаимно однозначны и сюръективны.

1. Определим $h: A \times C \rightarrow B \times D$ формулой $h(a, c) = (f(a), g(c))$.

Чтобы убедиться, что h взаимно однозначна, предположим, что $h(a_1, c_1) = h(a_2, c_2)$. Это означает, что $(f(a_1), g(c_1)) = (f(a_2), g(c_2))$, поэтому $f(a_1) = f(a_2)$ и $g(c_1) = g(c_2)$. Поскольку f и g взаимно однозначны, отсюда следует, что $a_1 = a_2$ и $c_1 = c_2$, поэтому $(a_1, c_1) = (a_2, c_2)$.

Чтобы убедиться, что h сюръективна, предположим, что $(b, d) \in B \times D$. Тогда, поскольку f и g обе сюръективны, мы можем выбрать $a \in A$ и $c \in C$ такие, что $f(a) = b$ и $g(c) = d$. Следовательно, $h(a, c) = (f(a), g(c)) = (b, d)$, что и требовалось доказать. Таким образом, h взаимно однозначна и сюръективна, поэтому $A \times C \sim B \times D$.

2. Предположим, что A и C не пересекаются и B и D тоже не пересекаются. В упражнении 14 вы докажете, что $f \cup g$ является взаимно однозначной и сюръективной функцией от $A \cup C$ к $B \cup D$, поэтому $A \cup C \sim B \cup D$.

Нетрудно показать, что отношение \sim рефлексивно, симметрично и транзитивно. Другими словами, можно предположить следующую теорему.

Теорема 8.1.3. Для любых множеств A , B и C :

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

1. Функция тождественности i_A взаимно однозначна и сюръективна для функции от A к A .
2. Предположим, что $A \sim B$. Тогда мы можем выбрать некоторую функцию $f: A \rightarrow B$, которая взаимно однозначна и сюръективна. По теореме 5.3.4 f^{-1} является функцией от B к A . Но теперь заметим, что $(f^{-1})^{-1} = f$, которая является функцией от A к B , поэтому снова по теореме 5.3.4 f^{-1} также взаимно однозначна. Следовательно, $B \sim A$.
3. Предположим, что $A \sim B$ и $B \sim C$. Тогда мы можем выбрать взаимно однозначные сюръективные функции $f: A \rightarrow B$ и $g: B \rightarrow C$. По теореме 5.2.5 $g \circ f: A \rightarrow C$ взаимно однозначна и сюръективна, поэтому $A \sim C$.

Теоремы 8.1.2 и 8.1.3 часто помогают показать, что множества равнomoщны. Например, ранее мы показали, что $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+$ и $\mathbb{Z}^+ \sim \mathbb{Z}$, поэтому из части 3 теоремы 8.1.3 следует, что $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}$. Часть 2 говорит нам, что не нужно различать утверждения « A равнomoщно B » и « B равнomoщно A », потому что они эквивалентны. Например, мы уже знаем, что $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+$, поэтому также можем написать $\mathbb{Z}^+ \sim \mathbb{Z}^+ \times \mathbb{Z}^+$. Согласно части 1 теоремы 8.1.2 $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z} \times \mathbb{Z}$, поэтому мы также имеем $\mathbb{Z}^+ \sim \mathbb{Z} \times \mathbb{Z}$.

Теперь мы нашли три множества \mathbb{Z} , $\mathbb{Z}^+ \times \mathbb{Z}^+$ и $\mathbb{Z} \times \mathbb{Z}$, равнomoщных множеству \mathbb{Z}^+ . Такие множества особенно важны и имеют особое название.

Определение 8.1.4. Множество A называется *исчислимым*, если $\mathbb{Z}^+ \sim A$. Оно называется *счетным*, если оно либо конечно, либо исчислимо. В противном случае это *несчетное* множество.

Мы можем называть счетными такие множества, элементы которых можно подсчитать, перебирая все из них один за другим и называя положительные целые числа по порядку. Если процесс счета заканчивается в какой-то момент, то множество *конечно*; а если подсчет никогда не заканчивается, то множество *исчислимо*. Следующая теорема предлагает еще два способа определить счетное множество.

Теорема 8.1.5. Пусть A – множество. Следующие утверждения эквивалентны:

1. A счетно.
2. Либо $A = \emptyset$, либо есть сюръективная функция $f: \mathbb{Z}^+ \rightarrow A$.
3. Существует взаимно однозначная функция $f: A \rightarrow \mathbb{Z}^+$.

Доказательство. 1 \rightarrow 2. Предположим, что множество A счетно. Если A исчислимо, то существует взаимно однозначная и сюръективная функция $f: \mathbb{Z}^+ \rightarrow A$, поэтому ясно, что утверждение 2 верно. Теперь предположим, что A конечно. Если $A = \emptyset$, то доказывать больше нечего, поэтому предположим, что $A \neq \emptyset$. Тогда мы можем выбрать некоторый элемент $a_0 \in A$. Пусть $g: I_n \rightarrow A$ – взаимно однозначная функция, где n – количество элементов A . Теперь определим $f: \mathbb{Z}^+ \rightarrow A$ следующим образом:

$$f(i) = \begin{cases} g(i), & \text{если } i \leq n \\ a_0, & \text{если } i > n \end{cases}$$

Теперь легко убедиться, что f сюръективна, как и требовалось.

$2 \rightarrow 3$. Предположим, что либо $A = \emptyset$, либо существует сюръективная функция от \mathbb{Z}^+ к A . Рассмотрим эти две возможности по очереди. Если $A = \emptyset$, то пустое множество является взаимно однозначной функцией от A к \mathbb{Z}^+ . Теперь предположим, что $g: \mathbb{Z}^+ \rightarrow A$ и g сюръективна. Тогда для каждого $a \in A$ множество $\{n \in \mathbb{Z}^+ \mid g(n) = a\}$ не пусто, поэтому по принципу полного упорядочения оно должно иметь наименьший элемент. Следовательно, мы можем определить функцию $f: A \rightarrow \mathbb{Z}^+$ формулой

$$f(a) = \text{наименьшее } n \in \mathbb{Z}^+ \text{ такое, что } g(n) = a.$$

Заметим, что для каждого $a \in A$ справедливо $g(f(a)) = a$, поэтому $g \circ f = i_A$. Но тогда по теореме 5.3.3 следует, что f взаимно однозначна, что и подразумевалось.

$3 \rightarrow 1$. Предположим, что $g: A \rightarrow \mathbb{Z}^+$ и g взаимно однозначна. Пусть $B = \text{Ran}(g) \subseteq \mathbb{Z}^+$. Тогда g отображается на B . Это означает, что если мы рассматриваем g как функцию от A к B , то она взаимно однозначна и сюръективна, поэтому $A \sim B$. Таким образом, достаточно показать, что B счетно, поскольку по теореме 8.1.3 отсюда следует, что A также счетно.

Предположим, что B не конечно. Мы должны показать, что B исчислимо, что мы можем сделать, задав взаимно однозначное определение для функции $f: \mathbb{Z}^+ \rightarrow B$. Идея в основе определения состоит в том, чтобы просто принять за $f(n)$ n -й элемент B для каждого $n \in \mathbb{Z}^+$. (Напомним, что $B \subseteq \mathbb{Z}^+$, поэтому мы можем использовать порядок положительных целых чисел, чтобы понять идею n -го элемента B .) Более точное определение f и доказательство того, что f взаимно однозначна и сюръективна, дано в упражнении 15.

Если A счетно и $A \neq \emptyset$, то по теореме 8.1.5 существует функция $f: \mathbb{Z}^+ \rightarrow A$, которая сюръективна. Если для каждого $n \in \mathbb{Z}^+$ мы положим $a_n = f(n)$, то тот факт, что f сюръективна, означает, что каждый элемент A появляется хотя бы один раз в списке a_1, a_2, a_3, \dots . Другими словами, $A = \{a_1, a_2, a_3, \dots\}$. Счетность множества A часто используется для того, чтобы записывать элементы A в список, индексированный натуральными числами. Фактически вы можете толковать счетность непустых множеств как их *списочность*. Конечно, если множество A счетно, то функцию f можно считать взаимно однозначной, а это означает, что каждый элемент A появится только один раз в списке a_1, a_2, a_3, \dots . Пример применения счетности, когда элементы счетного множества записаны в виде списка, см. в упражнении 19.

Теорема 8.1.5 также иногда полезна для доказательства исчислимости множества, как показывает доказательство нашей следующей теоремы.

Теорема 8.1.6. *Множество \mathbb{Q} исчислимо.*

Доказательство. Пусть $f: \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Q}$ определяется следующим образом:

$$f(p, q) = p/q.$$

Ясно, что f сюръективна, поскольку по определению все рациональные числа могут быть записаны как дроби, но обратите внимание, что f не является взаимно однозначной. Например, $f(1, 2) = f(2, 4) = 1/2$. Поскольку $\mathbb{Z}^+ \sim \mathbb{Z}$, по

теореме 8.1.2 мы имеем $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z} \times \mathbb{Z}^+$, и поскольку мы уже знаем, что $\mathbb{Z}^+ \times \mathbb{Z}^+$ исчислимо, отсюда следует, что $\mathbb{Z} \times \mathbb{Z}^+$ также исчислимо. Таким образом, мы можем выбрать взаимно однозначную сюръективную функцию $g: \mathbb{Z}^+ \rightarrow \mathbb{Z} \times \mathbb{Z}^+$. По теореме 5.2.5 $f \circ g: \mathbb{Z}^+ \rightarrow \mathbb{Q}$ сюръективна, поэтому по теореме 8.1.5 \mathbb{Q} счетно. Ясно, что \mathbb{Q} не конечно, поэтому оно должно быть исчислимым.

Хотя наша глава посвящена бесконечным множествам, методы этого раздела можно использовать для доказательства теорем, полезных для вычисления мощности конечных множеств. Мы заканчиваем этот раздел одним примером такой теоремы и приводим несколько других примеров в упражнениях (см. упражнения 20–30).

Теорема 8.1.7. Предположим, что A и B – непересекающиеся конечные множества. Тогда $A \cup B$ конечно и $|A \cup B| = |A| + |B|$.

Доказательство. Пусть $n = |A|$ и $m = |B|$. Пусть $A \sim I_n$ и $B \sim I_m$. Обратите внимание, что если $x \in I_m$, то $1 \leq x \leq m$, и, следовательно, $n + 1 \leq x + n \leq n + m$, поэтому $x + n \in I_{n+m} \setminus I_n$. Таким образом, мы можем определить функцию $f: I_m \rightarrow I_{n+m} \setminus I_n$ по формуле $f(x) = x + n$. Легко проверить, что f взаимно однозначна и сюръективна, поэтому $I_m \sim I_{n+m} \setminus I_n$. Поскольку $B \sim I_m$, то $B \sim I_{n+m} \setminus I_n$. Применяя часть 2 теоремы 8.1.2, можно заключить, что $A \cup B \sim I_n \cup (I_{n+m} \setminus I_n) = I_{n+m}$. Следовательно, $A \cup B$ конечно и $|A \cup B| = n + m = |A| + |B|$.

Упражнения

- *1. Покажите, что следующие множества исчислимы.
 - (a) \mathbb{N} .
 - (b) Множество всех четных целых чисел.
- 2. Покажите, что следующие множества счетны:
 - (a) $\mathbb{Q} \times \mathbb{Q}$.
 - (b) $\mathbb{Q}(\sqrt{2})$. (См. упражнение 21(b) раздела 5.4, чтобы узнать значение используемых здесь обозначений.)
- 3. В этом задании мы будем использовать следующие обозначения интервалов действительных чисел. Если a и b – действительные числа и $a < b$, то

$$\begin{aligned}[a, b] &= \{x \in \mathbb{R} \mid a \leq x \leq b\}, \\ (a, b) &= \{x \in \mathbb{R} \mid a < x < b\}, \\ (a, b] &= \{x \in \mathbb{R} \mid a < x \leq b\}, \\ [a, b) &= \{x \in \mathbb{R} \mid a \leq x < b\}.\end{aligned}$$

- (a) Докажите, что $[0, 1] \sim [0, 2]$.
- (b) Покажите, что $(-\pi/2, \pi/2) \sim \mathbb{R}$. (Подсказка: используйте тригонометрическую функцию.)
- (c) Покажите, что $(0, 1) \sim \mathbb{R}$.
- (d) Покажите, что $(0, 1] \sim (0, 1)$.

- *4. Обоснуйте свой ответ на каждый вопрос либо доказательством, либо контрпримером.
- Предположим, что $A \sim B$ и $A \times C \sim B \times D$. Должно ли быть так, что $C \sim D$?
 - Предположим, что $A \sim B$, A и C не пересекаются, B и D не пересекаются и $A \cup C \sim B \cup D$. Должно ли быть так, что $C \sim D$?
5. Докажите, что если $A \sim B$, то $\mathcal{P}(A) = \mathcal{P}(B)$.
- *6. (a) Докажите, что для всех натуральных чисел n и m если $I_n \sim I_m$, то $n = m$.
(Подсказка: используйте индукцию по n .)
- (b) Докажите, что если A конечно, то существует ровно одно натуральное число n такое, что $I_n \sim A$.
7. Предположим, что A и B – множества, а A конечно. Докажите, что $A \sim B$ тогда и только тогда, когда B также конечно и $|A| = |B|$.
- *8. (a) Докажите, что если $n \in \mathbb{N}$ и $A \subseteq I_n$, то A конечно и $|A| \leq n$. Кроме того, если $A \neq I_n$, то $|A| < n$.
- (b) Докажите, что если A конечно и $B \subseteq A$, то B также конечно и $|B| \leq |A|$. Кроме того, если $B \neq A$, то $|B| < |A|$.
9. Предположим, что $B \subseteq A$, $B \neq A$ и $B \sim A$. Докажите, что A бесконечно.
10. Докажите, что если $n \in \mathbb{N}$, $f: I_n \rightarrow B$ и f сюръективна, то B конечно и $|B| \leq n$.
11. Предположим, что A и B – конечные множества и $f: A \rightarrow B$.
- Докажите, что если $|A| < |B|$, то f не сюръективна.
 - Докажите, что если $|A| > |B|$, то f не является взаимно однозначной.
(Иногда это правило называют *принципом Дирихле* или *принципом картотеки*, потому что это неравенство означает, что если n карточек помещены в m ящиков, где $n > m$, то в каком-то ящике должно быть больше одной карточки.)
 - Докажите, что если $|A| = |B|$, то f взаимно однозначна тогда и только тогда, когда f сюръективна.
12. Покажите, что функция $f: \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$, определенная формулой
- $$f(i, j) = \frac{(i + j - 2)(i + j - 1)}{2} + i,$$
- взаимно однозначна и сюръективна.
13. Приведите еще одно доказательство того, что $\mathbb{Z}^+ \times \mathbb{Z}^+ \sim \mathbb{Z}^+$. Пусть $f: \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ определяется формулой
- $$f(m, n) = 2^{m-1}(2n - 1).$$
- Докажите, что f взаимно однозначна и сюръективна.
14. Завершите доказательство части 2 теоремы 8.1.2, показав, что если $f: A \rightarrow B$ и $g: C \rightarrow D$ – взаимно однозначные сюръективные функции, A и C не пересекаются и B и D тоже не пересекаются, то $f \cup g$ представляет собой взаимно однозначную сюръективную функцию от $A \cup C$ к $B \cup D$.

15. Завершите доказательство $3 \rightarrow 1$ теоремы 8.1.5. Предположим, что $B \subseteq \mathbb{Z}^+$ и B бесконечно. Теперь определим функцию $f: \mathbb{Z}^+ \rightarrow B$ рекурсией следующим образом:

для всех $n \in \mathbb{Z}^+$

$$f(n) = \text{наименьший элемент } B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < n\}.$$

Конечно, определение рекурсивно, потому что определение $f(n)$ ссылается на $f(m)$ для всех $m < n$.

- (a) Предположим, что $n \in \mathbb{Z}^+$. Определение $f(n)$ имеет смысл, только если мы можем быть уверены, что $B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < n\} \neq \emptyset$, и в этом случае принцип полного упорядочения гарантирует, что оно имеет наименьший элемент. Докажите, что $B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < n\} \neq \emptyset$. (Подсказка: см. упражнения 8 и 10.)
- (b) Докажите, что для всех $n \in \mathbb{Z}^+$ справедливо отношение $f(n) \geq n$.
- (c) Докажите, что f взаимно однозначна и сюръективна.

16. Приведите альтернативное доказательство теоремы 8.1.6.

- (a) Найдите функцию $f: \mathbb{Z}^+ \rightarrow \mathbb{Z} \setminus \{0\}$, которая взаимно однозначна и сюръективна.
- (b) Пусть функция $g: \mathbb{Z}^+ \rightarrow \mathbb{Q}^+$ определяется следующим образом. Предположим, что $n \in \mathbb{Z}^+$ и разложение n на простые множители равно $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, где p_1, p_2, \dots, p_k – простые числа, $p_1 < p_2 < \cdots < p_k$ и e_1, e_2, \dots, e_k – натуральные числа. Далее пусть

$$g(n) = g(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = p_1^{f(e_1)} p_2^{f(e_2)} \cdots p_k^{f(e_k)},$$

где f – функция из части (a). (Как и в разделе 7.2, мы считаем, что пустое произведение равно 1, так что $g(1) = 1$.) Докажите, что g взаимно однозначна и сюръективна. (Подсказка: вам пригодится упражнение 19 в разделе 7.2.)

- (c) Используйте g для определения взаимно однозначной сюръективной функции $h: \mathbb{Z} \rightarrow \mathbb{Q}$ и сделайте вывод, что \mathbb{Q} исчислимо.

17. Докажите, что если $B \subseteq A$ и A счетно, то B счетно.

18. Докажите, что если $B \subseteq A$, A бесконечно и B конечно, то $A \setminus B$ бесконечно.

19. Предположим, что A исчислимо и R – частичный порядок на A . Докажите, что R можно расширить до полного порядка на A . Другими словами, докажите, что существует полный порядок T на A такой, что $R \subseteq T$. Отметим, что мы доказали аналогичную теорему для конечного A в примере 6.2.2. (Подсказка: поскольку A исчислимо, мы можем записать элементы A в список: $A = \{a_1, a_2, a_3, \dots\}$. Теперь, используя упражнение 2 раздела 6.2, рекурсивно определим частичные порядки R_n для $n \in \mathbb{N}$, так что $R = R_0 \subseteq R_1 \subseteq R_2 \subseteq \dots$ и $\forall i \in I_n \forall j \in \mathbb{Z}^+ ((a_i, a_j) \in R_n \vee (a_j, a_i) \in R_n)$. Примем $T = \bigcup_{n \in \mathbb{N}} R_n$.

20. Предположим, что A конечно и $B \subseteq A$. Согласно упражнению 8, множества B и $A \setminus B$ конечны. Докажите, что $|A \setminus B| = |A| - |B|$. (В частности, если $a \in A$, то $|A \setminus \{a\}| = |A| - 1$. Мы использовали этот факт в нескольких доказательствах в главе 6; например, мы использовали его в примерах 6.2.1 и 6.2.2.)

21. Предположим, что n – натуральное число и для каждого $i \in I_n$ имеется конечное множество A_i . Также предположим, что $\forall i \in I_n \forall j \in I_n (i \neq j \rightarrow A_i \cap A_j = \emptyset)$. Докажите, что $\bigcup_{i \in I_n} A_i$ конечно и $|\bigcup_{i \in I_n} A_i| = \sum_{i=1}^n |A_i|$.
- *22. (a) Докажите, что если A и B – конечные множества, то $A \times B$ конечно и $|A \times B| = |A| \cdot |B|$. (Подсказка: используйте индукцию по $|B|$. Другими словами, докажите по индукции следующее утверждение: $\forall n \in \mathbb{N} \forall A \forall B$ (если A и B конечны и $|B| = n$, то $A \times B$ конечно и $|A \times B| = |A| \cdot n$). Вам может пригодиться теорема 4.1.3.)
(b) Блюда в ресторане Алисы состоят из основного блюда и десерта. Основным блюдом может быть стейк, курица, свиные отбивные, креветки или спагетти, а на десерт может быть мороженое, торт или пирог. Сколько разных блюд вы можете заказать в ресторане Алисы?
23. Для любых множеств A и B множество всех функций от A к B обозначается ${}^A B$.
(a) Докажите, что если $A \sim B$ и $C \sim D$, то ${}^A C \sim {}^B D$.
(b) Докажите, что если A , B и C – множества и $A \cap B = \emptyset$, то ${}^{A \cup B} C \sim {}^A C \times {}^B C$.
(c) Докажите, что если A и B – конечные множества, то ${}^A B$ конечно и $|{}^A B| = |B|^{|A|}$. (Подсказка: используйте индукцию по $|A|$.)
(d) У профессора в группе 20 студентов, и он должен поставить каждому студенту оценку A , B , C , D или F . Сколько вариантов расстановки оценок доступно профессору?
24. Пусть $|A| = n$ и $F = \{f \mid f$ является взаимно однозначной и сюръективной функцией от I_n к $A\}$.
(a) Докажите, что F конечно и $|F| = n!$. (Подсказка: используйте индукцию по n .)
(b) Пусть $L = \{R \mid R$ – полный порядок на $A\}$. Докажите, что $F \sim L$, а значит, $|L| = n!$.
(c) Пять человек должны сидеть в ряду из пяти мест. Сколько вариантов их размещения существует?
25. Предположим, что A – конечное множество, а R – отношение эквивалентности на A . Предположим также, что существует некоторое натуральное число n такое, что $\forall x \in A (|[x]R| = n)$. Докажите, что A/R конечно и $|A/R| = |A|/n$. (Подсказка: используйте упражнение 21.)
26. (a) Предположим, что A и B – конечные множества. Докажите, что $A \cup B$ конечно и $|A \cup B| = |A| + |B| - |A \cap B|$.
(b) Предположим, что A , B и C – конечные множества. Докажите, что $A \cup B \cup C$ конечно и
- $$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$
27. Докажите *принцип включения-исключения*, который обобщает формулы из упражнения 26. Предположим, A_1, A_2, \dots, A_n – конечные множества. Пусть $P = \mathcal{P}(I_n) \setminus \{\emptyset\}$, и для каждого $S \in P$ пусть $A_S = \bigcap_{i \in S} A_i$.

Докажите, что $\bigcup_{i \in I_n} A_i$ конечно и

$$\left| \bigcup_{i \in I_n} A_i \right| = \sum_{S \in P} (-1)^{|S|+1} |A_S|.$$

(Обозначение в правой части этого уравнения дает результат прохождения всех множеств $S \in P$, вычисления числа $(-1)^{|S|+1} |A_S|$ для каждого S , а затем сложения этих чисел. Совет: используйте индукцию по n .)

28. Докажите, что если A и B – конечные множества и $|A| = |B|$, то $|A \Delta B|$ четно.
29. Каждый клиент в неком банке имеет ПИН-код, который представляет собой последовательность из четырех цифр. Покажите, что если у банка более 10 000 клиентов, то у некоторых двух клиентов должен быть одинаковый ПИН-код. (Подсказка: см. упражнение 11.)
30. Алиса открыла свою зачетку и воскликнула: «Не могу поверить, что завалила теорию вероятностей у профессора Джонсона». «Ты посещала этот курс? – спросил Боб, – забавно, я тоже его посещал и не помню, чтобы когда-нибудь видел тебя там». «Что ж, – смущенно призналась Алиса, – похоже, я действительно часто прогуливала лекции». «Да, я тоже», – сказал Боб. Докажите, что Алиса или Боб пропустили как минимум половину занятий.

8.2. СЧЕТНЫЕ И НЕСЧЕТНЫЕ МНОЖЕСТВА

Часто, когда мы выполняем некоторую операцию со счетными множествами, результатом снова является счетное множество.

Теорема 8.2.1. Предположим, что A и B – счетные множества. Тогда:

1. $A \times B$ счетно.
2. $A \cup B$ счетно.

Доказательство. Поскольку A и B счетны, по теореме 8.1.5 мы можем выбрать взаимно однозначные функции $f: A \rightarrow \mathbb{Z}^+$ и $g: B \rightarrow \mathbb{Z}^+$.

1. Определим функцию $h: A \times B \rightarrow \mathbb{Z}^+ \times \mathbb{Z}^+$ по формуле $h(a, b) = (f(a), g(b))$. Как и в доказательстве части 1 теоремы 8.1.2, нетрудно показать, что h взаимно однозначна. Поскольку $\mathbb{Z}^+ \times \mathbb{Z}^+$ исчислимо, мы можем объявить взаимно однозначную сюръективную функцию $j: \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$. Тогда по теореме 5.2.5 комбинация $j \circ h: A \times B \rightarrow \mathbb{Z}^+$ взаимно однозначна, поэтому по теореме 8.1.5 $A \times B$ счетно.
2. Определим функцию $h: A \cup B \rightarrow \mathbb{Z}$ следующим образом:

$$h(x) = \begin{cases} f(x), & \text{если } x \in A \\ -g(x), & \text{если } x \notin A \end{cases}$$

Далее мы исходим из того, что h взаимно однозначна. Чтобы убедиться в этом, предположим, что $h(x_1) = h(x_2)$ для некоторых x_1 и x_2 в $A \cup B$.

Если $h(x_1) = h(x_2) > 0$, то согласно определению h мы должны иметь $x_1 \in A$, $x_2 \in A$ и $f(x_1) = h(x_1) = h(x_2) = f(x_2)$. Но тогда, поскольку f взаимно однозначна, $x_1 = x_2$. Аналогично, если $h(x_1) = h(x_2) \leq 0$, то должно существовать $g(x_1) = -h(x_1) = -h(x_2) = g(x_2)$, и тогда, поскольку g взаимно однозначна, $x_1 = x_2$. Таким образом, h взаимно однозначна.

Поскольку \mathbb{Z} исчислимо, мы можем объявить взаимно однозначную сюръективную функцию $j: \mathbb{Z} \rightarrow \mathbb{Z}^+$. Затем, как и в части 1, мы находим, что комбинация $j \circ h: A \cup B \rightarrow \mathbb{Z}^+$ взаимно однозначна, поэтому $A \cup B$ счетно.

Как показывает наша следующая теорема, часть 2 теоремы 8.2.1 может быть расширена на объединение более чем двух множеств.

Теорема 8.2.2. *Объединение счетного числа счетных множеств счетно. Другими словами, если \mathcal{F} – семейство множеств и \mathcal{F} счетно, а также каждый элемент \mathcal{F} является счетным, то $\bigcup \mathcal{F}$ является счетным.*

Доказательство. Предположим сначала, что $\emptyset \notin \mathcal{F}$. В конце доказательства обсудим случай $\emptyset \in \mathcal{F}$.

Если $\mathcal{F} = \emptyset$, то очевидно, что $\bigcup \mathcal{F}$ счетно. Теперь предположим, что $\mathcal{F} \neq \emptyset$. Далее, как описано после доказательства теоремы 8.1.5, поскольку \mathcal{F} счетно и непусто, мы можем записать элементы \mathcal{F} в список, индексированный положительными целыми числами. Другими словами, мы можем сказать, что $\mathcal{F} = \{A_1, A_2, A_3, \dots\}$. Аналогично, каждый элемент \mathcal{F} счетный и непустой (так как $\emptyset \notin \mathcal{F}$), поэтому для каждого положительного целого числа i элементы A_i могут быть представлены в виде списка. Таким образом, мы можем написать

$$\begin{aligned} A_1 &= \{a_1^1, a_2^1, a_3^1, \dots\}, \\ A_2 &= \{a_1^2, a_2^2, a_3^2, \dots\}, \end{aligned}$$

и в общем

$$A_i = \{a_1^i, a_2^i, a_3^i, \dots\}.$$

Обратите внимание, что по определению объединения $\bigcup \mathcal{F} = \{a_j^i \mid i \in \mathbb{Z}^+, j \in \mathbb{Z}^+\}$.

Теперь определим функцию $f: \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \bigcup \mathcal{F}$ формулой $f(i, j) = a_j^i$.

Ясно, что f сюръективна. Поскольку $\mathbb{Z}^+ \times \mathbb{Z}^+$ исчислимо, мы можем объявить взаимно однозначную сюръективную функцию $g: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+ \times \mathbb{Z}^+$. Отсюда $f \circ g: \mathbb{Z}^+ \rightarrow \bigcup \mathcal{F}$ сюръективна, поэтому $\bigcup \mathcal{F}$ счетно.

Наконец, предположим, что $\emptyset \in \mathcal{F}$. Пусть $\mathcal{F}' = \mathcal{F} \setminus \{\emptyset\}$. Тогда \mathcal{F}' также является счетным семейством счетных множеств и $\emptyset \notin \mathcal{F}'$, так что согласно предыдущим рассуждениям счетно. Но ясно, что $\bigcup \mathcal{F} = \bigcup \mathcal{F}'$, поэтому $\bigcup \mathcal{F}$ тоже счетно.

Еще одна операция, сохраняющая счетность, – это формирование конечных последовательностей. Предположим, что A – множество и a_1, a_2, \dots, a_n – список элементов A .

Мы могли бы определить множители в этом списке с помощью функции $f: I_n \rightarrow A$, где для каждого i $f(i) = a_i$ – i -й член в списке. Такая функция называется *конечной последовательностью* элементов A .

Определение 8.2.3. Предположим, что A – множество. Функция $f: I_n \rightarrow A$, где n – натуральное число, называется *конечной последовательностью* элементов A , и n называется *длиной последовательности*.

Теорема 8.2.4. Предположим, что A – счетное множество. Тогда множество всех конечных последовательностей элементов A также счетно.

Доказательство. Для каждого $n \in \mathbb{N}$ пусть S_n – множество всех последовательностей длины n элементов A . Сначала покажем, что для любого $n \in \mathbb{N}$ множество S_n счетно, а затем продолжим индукцией по n .

В базовом случае мы предполагаем $n = 0$. Обратите внимание, что $I_0 = \emptyset$, поэтому последовательность длины 0 является функцией $f: \emptyset \rightarrow A$, и единственной такой функцией является \emptyset . Таким образом, $S_0 = \{\emptyset\}$, что очевидно представляет собой счетное множество.

Для шага индукции предположим, что n – натуральное число, а S_n счетно. Мы должны показать, что S_{n+1} счетно. Рассмотрим функцию $F: S_n \times A \rightarrow S_{n+1}$, определенную следующим образом:

$$F(f, a) = f \cup \{(n + 1, a)\}.$$

Другими словами, для любой последовательности $f \in S_n$ и любого элемента $a \in A$ функция $F(f, a)$ – это последовательность, которую вы получаете, начиная с f , которая представляет собой последовательность длины n , а затем добавляя a в качестве члена с номером $n + 1$. В упражнении 2 вы докажете, что F взаимно однозначна. Следовательно, $S_n \times A \sim S_{n+1}$. Но S_n и A счетны, поэтому по теореме 8.2.1 $S_n \times A$ счетно, а значит, S_{n+1} счетно.

Этот вывод завершает индуктивное доказательство того, что для любого $n \in \mathbb{N}$ множество S_n счетно. Наконец, заметим, что множество всех конечных последовательностей элементов A равно $\bigcup_{n \in \mathbb{N}} S_n$ и оно счетно по теореме 8.2.2.

В качестве примера использования теоремы 8.2.4 вы должны суметь показать, что множество всех грамматических предложений вашего языка является счетным множеством. (См. упражнение 17.)

К этому моменту у вас мог возникнуть вопрос: а вдруг все множества являются счетными? Существуют ли в теории множеств какие-либо операции, которые можно использовать для создания несчетных множеств? Наша следующая теорема говорит о том, что ответ положительный, и это операция степенного множества (множество всех подмножеств данного множества). Этот факт был открыт немецким математиком Георгом Кантором (1845–1918) с помощью известного и гениального доказательства. Фактически именно Кантор первым пришел к идеи сравнения размеров бесконечных множеств. Доказательство Кантора несколько сложнее, чем предыдущие доказательства в этой главе, поэтому мы обсудим стратегию, лежащую в основе доказательства, прежде чем представлять само доказательство.

Теорема 8.2.5. (Теорема Кантора.) $\mathcal{P}(\mathbb{Z}^+)$ несчетно.

Стратегия доказательства

Доказательство основано на утверждении 2 теоремы 8.1.5. Мы покажем, что не существует функции $f: \mathbb{Z}^+ \rightarrow \mathcal{P}(\mathbb{Z}^+)$, которая сюръективна. Ясно, что $\mathcal{P}(\mathbb{Z}^+) \neq \emptyset$, так что из теоремы 8.1.5 следует, что $\mathcal{P}(\mathbb{Z}^+)$ несчетно.

Наша стратегия будет заключаться в том, что мы возьмем произвольную функцию $f: \mathbb{Z}^+ \rightarrow \mathcal{P}(\mathbb{Z}^+)$ и докажем, что она не сюръективна. Переформулируя эту отрицательную цель как положительное утверждение, мы должны показать, что $\exists D [D \in \mathcal{P}(\mathbb{Z}^+) \wedge \forall n \in \mathbb{Z}^+ (D \neq f(n))]$. Это наводит на мысль, что мы должны попытаться найти конкретное множество D , для которого можем доказать как утверждение $D \in \mathcal{P}(\mathbb{Z}^+)$, так и $\forall n \in \mathbb{Z}^+ (D \neq f(n))$. Это самый сложный шаг в поиске доказательства. Действительно, существует множество D , благодаря которому доказательство сработает, но чтобы его найти, потребуется определенная сообразительность.

Нам нужно убедиться, что $D \in \mathcal{P}(\mathbb{Z}^+)$, или, другими словами, $D \subseteq \mathbb{Z}^+$, поэтому мы знаем, что нам нужно учитывать только натуральные числа при принятии решения, какими должны быть элементы D . Но это по-прежнему оставляет нам бесконечно много решений: для каждого натурального числа n мы должны решить, хотим ли мы, чтобы это число было элементом D . Нам также необходимо убедиться, что $\forall n \in \mathbb{Z}^+ (D \neq f(n))$. Это накладывает бесконечно много ограничений на наш выбор D : для каждого натурального числа n мы должны убедиться, что $D \neq f(n)$. Почему бы не принимать каждое из наших бесконечно многих решений таким образом, чтобы гарантировать выполнение соответствующего ограничения? Другими словами, для каждого натурального числа n мы принимаем решение о том, является ли n элементом D таким образом, чтобы гарантировать, что $D \neq f(n)$. Это несложно. Мы можем считать n элементом D , если $n \notin f(n)$, и оставить n вне D , если $n \in f(n)$. Это гарантирует, что $D \neq f(n)$, потому что только одно из этих множеств будет содержать конкретное число n как элемент, а другое – нет. Это говорит о том, что мы должны использовать следующее определение: $D = \{n \in \mathbb{Z}^+ \mid n \notin f(n)\}$.

Таблица 8.3 поможет вам понять определение множества D . Для каждого $m \in \mathbb{Z}^+$ функция $f(m)$ является подмножеством \mathbb{Z}^+ , которое можно определить, ответив для каждого натурального числа n , истинно ли утверждение $n \in f(m)$. Ответы на эти вопросы можно расположить, как показано в табл. 8.3. Каждая строка этой таблицы дает ответы, необходимые для определения множества $f(m)$ для конкретного значения m . Множество D также можно определить с помощью ряда ответов «да» и «нет», как показано в нижней части табл. 8.3. Для каждого $n \in \mathbb{Z}^+$ мы должны решить, действительно ли $n \in D$, задав вопрос, действительно ли $n \in f(n)$, и ответы на эти вопросы заключены в рамки в табл. 8.3. Поскольку $n \in D$, если и только если $n \notin f(n)$, ряд ответов «да» и «нет», который задает D , можно найти, прочитав ответы в рамке по диагонали в табл. 8.3 и инвертировав все ответы. Эти ответы гарантированно будут отличаться от каждой строки табл. 8.3, потому что для каждого $n \in \mathbb{Z}^+$ ответ отличается от строки n в n -й позиции.

Если вам трудно уследить за ходом мысли в этом рассуждении, не беспокойтесь об этом. Помните, что рассуждения, использованные при выборе множества D , в любом случае не будут частью доказательства! Прочитав доказательство, вы можете вернуться и перечитать два последних абзаца.

Таблица 8.3. Иллюстрация определения множества D

$n \in f(m)?$	n				
	1	2	3	4	5
1	да	нет	нет	да	да
2	да	да	нет	нет	да
m	нет	нет	нет	да	нет
	да	да	нет	да	нет
	нет	да	да	нет	нет
	...				
$n \in D?$	нет	нет	да	нет	да
					...

Должно быть ясно, что выбранное нами множество D является подмножеством \mathbb{Z}^+ , поэтому $D \in \mathcal{P}(\mathbb{Z}^+)$. Другая наша цель – доказать, что $\forall n \in \mathbb{Z}^+ (D \neq f(n))$, поэтому пусть n – произвольное натуральное число; докажем, что $D \neq f(n)$. Теперь напомним, что мы тщательно выбрали D , чтобы иметь возможность доказать $D \neq f(n)$, и этот выбор опирался на то, истинно ли утверждение $n \in f(n)$. Возможно, самый простой способ написать доказательство – это рассмотреть два случая $n \in f(n)$ и $n \notin f(n)$ по отдельности. В любом случае применение определения D легко приводит к заключению, что $D \neq f(n)$.

Доказательство. Пусть задана функция $f: \mathbb{Z}^+ \rightarrow \mathcal{P}(\mathbb{Z}^+)$. Мы покажем, что f не может быть сюръективной, найдя такое множество $D \in \mathcal{P}(\mathbb{Z}^+)$, что $D \notin \text{Ran}(f)$. Пусть $D = \{n \in \mathbb{Z}^+ \mid n \notin f(n)\}$. Ясно, что $D \subseteq \mathbb{Z}^+$, поэтому $D \in \mathcal{P}(\mathbb{Z}^+)$. Пусть теперь n – произвольное натуральное число. Рассмотрим два случая.

Случай 1. $n \in f(n)$. Поскольку $D = \{n \in \mathbb{Z}^+ \mid n \notin f(n)\}$, мы можем заключить, что $n \notin D$. Но тогда, поскольку $n \in f(n)$ и $n \notin D$, следует, что $D \neq f(n)$.

Случай 2. $n \notin f(n)$. Тогда по определению $D \in f(n) \in D$. Поскольку $n \in D$ и $n \notin f(n)$, $D \neq f(n)$.

Так как эти случаи являются исчерпывающими, из них следует, что $\forall n \in \mathbb{Z}^+ (D \neq f(n))$, поэтому $D \notin \text{Ran}(f)$. Поскольку f была произвольной, это показывает, что не существует сюръективной функции $f: \mathbb{Z}^+ \rightarrow \mathcal{P}(\mathbb{Z}^+)$. Ясно, что $\mathcal{P}(\mathbb{Z}^+) \neq \emptyset$, поэтому по теореме 8.1.5 $\mathcal{P}(\mathbb{Z}^+)$ несчетно.

Метод, использованный в доказательстве теоремы 8.2.5, называется *диагонализацией* из-за диагонального расположения ответов в рамке в табл. 8.3. Диагонализация – это мощный метод, который можно использовать для доказательства многих теорем, включая нашу следующую теорему. Однако вместо того, чтобы привести еще одно рассуждение о диагонализации, мы просто применим теорему 8.2.5 для доказательства следующей теоремы.

Теорема 8.2.6. Множество \mathbb{R} несчетно.

Доказательство. Мы определим функцию $f: \mathcal{P}(\mathbb{Z}^+) \rightarrow \mathbb{R}$ и покажем, что f взаимно однозначна. Если бы \mathbb{R} было счетным, тогда существовала бы взаимно однозначная функция $g: \mathbb{R} \rightarrow \mathbb{Z}^+$. Но тогда $g \circ f$ будет взаимно однозначной функцией от $\mathcal{P}(\mathbb{Z}^+)$ к \mathbb{Z}^+ и, следовательно, $\mathcal{P}(\mathbb{Z}^+)$ будет счетным, что противоречит теореме Кантора. Значит, это покажет, что \mathbb{R} несчетно.

Чтобы определить f , предположим, что $A \in \mathcal{P}(\mathbb{Z}^+)$. Тогда $f(A)$ будет действительным числом от 0 до 1, которое мы укажем в десятичном разложении. Для каждого натурального числа n n -я цифра $f(A)$ будет числом d_n , определенным следующим образом:

$$d_n = \begin{cases} 3, & \text{если } n \notin A \\ 7, & \text{если } n \in A \end{cases}.$$

Другими словами, в десятичной записи мы имеем $f(A) = 0.d_1d_2d_3\dots$

Например, если E – это множество всех положительных четных целых чисел, тогда $f(E) = 0,37373737\dots$. Если P – множество всех простых чисел, то $f(P) = 0,37737373337\dots$.

Чтобы убедиться, что f взаимно однозначна, предположим, что $A \in \mathcal{P}(\mathbb{Z}^+)$, $B \in \mathcal{P}(\mathbb{Z}^+)$ и $A \neq B$. Тогда существует некоторое $n \in \mathbb{Z}^+$ такое, что либо $n \in A$ и $n \notin B$, либо $n \in B$ и $n \notin A$. Но тогда $f(A)$ и $f(B)$ не могут быть равными, так как их десятичные разложения различаются n -й цифрой¹. Таким образом, f взаимно однозначна.

Упражнения

- *1. (a) Докажите, что множество всех иррациональных чисел $\mathbb{R} \setminus \mathbb{Q}$ несчетно.
 (б) Докажите, что $\mathbb{R} \setminus \mathbb{Q} \sim \mathbb{R}$.
- 2. Пусть $F: S_n \times A \rightarrow S_{n+1}$ – функция, определенная в доказательстве теоремы 8.2.4. Покажите, что F взаимно однозначна и сюръективна.
- 3. Приведите альтернативное доказательство теоремы 8.2.4. Пусть A – счетное множество, и пусть S – множество всех конечных последовательностей элементов A . Поскольку A счетно, существует взаимно однозначная функция $g: A \rightarrow \mathbb{Z}^+$. Для каждого натурального числа n пусть p_n будет n -м простым числом; то есть $p_1 = 2, p_2 = 3$ и т.д. Определим функцию $F: S \rightarrow \mathbb{Z}^+$ следующим образом: предположим, что $f \in S$ и длина f равна n . Отсюда

$$F(f) = p_1^{g(f(1))} p_2^{g(f(2))} \cdots p_n^{g(f(n))}.$$

Докажите, что функция F взаимно однозначна, а значит, множество S счетно.

- 4. Пусть $P = \{X \in \mathcal{P}(\mathbb{Z}^+) \mid X \text{ конечно}\}$. Докажите, что P исчислимо.
- *5. Докажите следующую более общую форму теоремы Кантора: для любого множества A справедливо утверждение $A \sim \mathcal{P}(A)$. (Подсказка: используйте доказательство теоремы 8.2.5.)

¹ Здесь следует быть немного осторожнее. На самом деле два разных десятичных разложения могут представлять одно и то же число. Например, на лекциях по математическому анализу вы могли узнать удивительный факт, что $0,999\dots = 1,000\dots$ Однако это происходит только с десятичными разложениями, которые заканчиваются либо бесконечной последовательностью девяток, либо бесконечной последовательностью нулей. Для десятичных разложений, состоящих из 3 и 7, разные десятичные разложения всегда представляют разные числа.

6. Определение обозначений, используемых в этом упражнении, см. в упражнении 23 раздела 8.1.
- Докажите, что для любых множеств A, B и C ${}^A(B \times C) \sim {}^A B \times {}^A C$.
 - Докажите, что для любых множеств A, B и ${}^{(A \times B)}C \sim {}^A({}^B C)$.
 - Докажите, что для любого множества A $\mathcal{P}(A) \sim {}^A\{\text{да, нет}\}$. (Обратите внимание, что если A конечно и $|A| = n$, то из упражнения 23(с) раздела 8.1 следует, что $|\mathcal{P}(A)| = |\{\text{да, нет}\}|^{|A|} = 2^n$. Конечно, вы уже доказали это другим способом в упражнении 11 раздела 6.2.)
 - Докажите, что ${}^{\mathbb{Z}^+}\mathcal{P}(\mathbb{Z}^+) \sim \mathcal{P}(\mathbb{Z}^+)$.
7. Предположим, что A исчислимо. Докажите, что существует такое разбиение P множества A , что P исчислимо и для любого $X \in P$ X тоже исчислимо.
- *8. Докажите, что если A и B – непересекающиеся множества, то $\mathcal{P}(A \cup B) \sim \mathcal{P}(A) \times \mathcal{P}(B)$.
9. (а) Предположим, что $A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots$ и $\bigcup_{n \in \mathbb{Z}^+} A_n = \mathbb{R}$. Докажите, что для каждого несчетного множества $B \subseteq R$ существует некоторое натуральное число n такое, что $B \cap A_n$ несчетно.
- (б) Предположим, что $A_1 \subseteq A_2 \subseteq A_3 \subseteq \dots$ и $\bigcup_{n \in \mathbb{Z}^+} A_n = \mathbb{R}$. Предположим также, что для любого бесконечного множества $B \subseteq \mathbb{Z}^+$ существует некоторое натуральное число n такое, что $B \cap A_n$ бесконечно. Докажите, что для некоторого n $A = \mathbb{Z}^+$.
10. Предположим, что $A \subseteq \mathbb{R}^+$, $b \in \mathbb{R}^+$, и для каждого списка a_1, a_2, \dots, a_k конечного числа различных элементов A , $a_1 + a_2 + \dots + a_k \leq b$. Докажите, что A счетно. (Подсказка: для каждого положительного целого числа n пусть $A_n = \{x \in A \mid x \geq 1/n\}$. Что вы можете сказать о количестве элементов в A_n ?)
11. Предположим, что E – отношение эквивалентности на \mathbb{R} и для всех действительных чисел x и y $[x]_E \sim [y]_E$. Докажите, что либо \mathbb{R}/E несчетно, либо для любого $x \in \mathbb{R}$ $[x]_E$ несчетно.
12. Действительное число x называется *алгебраическим*, если существует натуральное число n и целые числа a_0, a_1, \dots, a_n такие, что $a_0 + a_1x + a_2x^2 + \dots + a_nx^n = 0$ и $a_n \neq 0$. Пусть A – множество всех алгебраических чисел.
- Докажите, что $\mathbb{Q} \subseteq A$.
 - Докажите, что $\sqrt{2} \in A$.
 - Докажите, что A счетно. Примечание: вы можете использовать тот факт, что если n – натуральное число, a_0, a_1, \dots, a_n – целые числа, $a_n \neq 0$, то $\{x \in \mathbb{R} \mid a_0 + a_1x + a_2x^2 + \dots + a_nx^n = 0\}$ конечно.
13. Предположим, что $\mathcal{F} \subseteq \{f \mid f: \mathbb{Z}^+ \rightarrow \mathbb{R}\}$ и \mathcal{F} счетно. Докажите, что существует функция $g: \mathbb{Z}^+ \rightarrow \mathbb{R}$ такая, что $\mathcal{F} \subseteq O(g)$. (Значение используемых здесь обозначений см. в упражнении 19 раздела 5.1.)
14. Предположим, что $\mathcal{F} \subseteq \mathcal{P}(\mathbb{Z}^+)$ и \mathcal{F} попарно не пересекается. Докажите, что \mathcal{F} счетно.
- *15. Если A и B – бесконечные множества, мы говорим, что A и B *почти не пересекаются*, если пересечение $A \cap B$ конечно. Если \mathcal{F} – семейство бес-

конечных множеств, то мы говорим, что \mathcal{F} попарно почти не пересекается, если для всех A и B в \mathcal{F} справедливо, что если $A \neq B$, то A и B почти не пересекаются. Докажите, что существует такое семейство множеств $\mathcal{F} \subseteq \mathcal{P}(\mathbb{Z}^+)$, что все элементы \mathcal{F} бесконечны, \mathcal{F} попарно почти не пересекается и \mathcal{F} несчетно. (Сравните это с предыдущим упражнением.)

Пусть $P = \{X \in \mathcal{P}(\mathbb{Z}^+) \mid X \text{ конечно}\}$ и $Q = \{X \in \mathcal{P}(\mathbb{Z}^+) \mid X \text{ бесконечно}\}$. В соответствии с упражнением 4 множество P счетно, поэтому мы можем выбрать взаимно однозначную сюръективную функцию $g: P \rightarrow \mathbb{Z}^+$.

- (a) Докажите, что Q несчетно. Для каждого $A \in Q$ пусть $S_A = \{A \cap I_n \mid n \in \mathbb{Z}^+\}$. Например, если A – это множество всех простых чисел, тогда $S_A = \{0, \{2\}, \{2, 3\}, \{2, 3, 5\}, \dots\}$. (Мы могли бы описать S_A как множество всех начальных сегментов A .)
 - (b) Докажите, что если $A \in Q$, то $S_A \subseteq P$ и S_A бесконечно.
 - (c) Докажите, что если $A, B \in Q$ и $A \neq B$, то $S_A \cap S_B$ конечно.
 - (d) Пусть $\mathcal{F} = \{g(S_A) \mid A \in Q\}$. Докажите, что $\mathcal{F} \subseteq \mathcal{P}(\mathbb{Z}^+)$, каждый элемент \mathcal{F} бесконечен, \mathcal{F} попарно почти не пересекается и \mathcal{F} несчетно.
16. Докажите, что существует функция $f: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ такая, что для всех натуральных чисел a, b и c существует некоторое натуральное число n такое, что $f(an + b) = c$.
17. Докажите, что множество всех грамматических предложений английского языка счетно. (Подсказка: каждое грамматическое предложение английского языка – это конечная последовательность английских слов. Сначала покажите, что множество всех грамматических предложений счетно, а затем покажите, что оно бесконечно.)
18. Некоторые действительные числа можно определить с помощью фразы на обычном разговорном языке. Например, фраза «отношение длины окружности к ее диаметру» определяет число π .
- (a) Докажите, что множество чисел, которые можно определить с помощью английской фразы, счетно. (Подсказка: см. упражнение 17.)
 - (b) Докажите, что существуют действительные числа, которые нельзя определить с помощью английских фраз.

8.3. ТЕОРЕМА КАНТОРА–ШРЕДЕРА–БЕРНШТЕЙНА

Предположим, что A и B – множества, а f – взаимно однозначная функция от A к B . Тогда f показывает, что $A \sim \text{Ran}(f) \subseteq B$, поэтому естественно думать, что B имеет размер не менее A . Это предполагает следующие обозначения.

Определение 8.3.1. Если A и B – множества, то мы будем говорить, что B доминирует A , и писать $A \preceq B$, если существует взаимно однозначная функция $f: A \rightarrow B$. Если $A \preceq B$ и $A \not\sim B$, то мы говорим, что B строго доминирует A , и пишем $A \prec B$.

Например, при доказательстве теоремы 8.2.6 мы задали взаимно однозначную функцию $f: \mathcal{P}(\mathbb{Z}^+) \rightarrow \mathbb{R}$, поэтому $\mathcal{P}(\mathbb{Z}^+) \lesssim \mathbb{R}$. Конечно, для любых множеств A и B если $A \sim B$, тогда также $A \lesssim B$. Также должно быть очевидно, что если $A \subseteq B$, то $A \lesssim B$. Например, $\mathbb{Z}^+ \lesssim \mathbb{R}$. Фактически из теоремы 8.2.6 мы также знаем, что $\mathbb{Z}^+ \not\sim \mathbb{R}$, поэтому можем сказать, что $\mathbb{Z}^+ \prec \mathbb{R}$.

Вы можете подумать, что отношение \lesssim будет частичным порядком, но, оказывается, это не так. В упражнении 1 вы убедитесь, что \lesssim рефлексивно и транзитивно, но не антисимметрично. (В терминологии упражнения 25 раздела 4.5 \lesssim является предварительным порядком.) Например, $\mathbb{Z}^+ \sim \mathbb{Q}$, поэтому $\mathbb{Z}^+ \lesssim \mathbb{Q}$ и $\mathbb{Q} \lesssim \mathbb{Z}^+$, но, разумеется, $\mathbb{Z}^+ \neq \mathbb{Q}$. Однако это наводит на интересный вопрос: если $A \lesssim B$ и $B \lesssim A$, тогда A и B могут не быть равными, но должны ли они быть равномощными?

Оказывается, да, как мы докажем в нашей следующей теореме. Обычно с этой теоремой связывают имена нескольких математиков. Кантор был первым, кто сформулировал теорему и дал частичное доказательство. Позже Эрнст Шредер (1841–1902) и Феликс Бернштейн (1878–1956) независимо друг от друга нашли полные доказательства.

Теорема 8.3.2. (Теорема Кантора–Шредера–Бернштейна.) *Пусть A и B – множества. Если $A \lesssim B$ и $B \lesssim A$, то $A \sim B$.*

Стратегия доказательства

Мы начнем с предположения, что $A \lesssim B$ и $B \lesssim A$, что означает, что мы можем выбрать взаимно однозначные функции $f: A \rightarrow B$ и $g: B \rightarrow A$. Чтобы доказать, что $A \sim B$, нам нужно найти взаимно однозначную сюръективную функцию $h: A \rightarrow B$.

На данный момент мы мало что знаем об A и B . Единственные инструменты, которые у нас есть, чтобы сопоставить элементы A и B , – это функции f и g . Если f сюръективна, то, конечно, мы можем положить $h = f$; и если g сюръективна, то мы можем положить $h = g^{-1}$. Но может оказаться, что ни f , ни g не сюръективны. Как в этом случае найти нужную функцию h ?

Нашим решением будет объединить части f и g^{-1} , чтобы получить h . Для этого мы разделим A на две части X и Y , а B – на две части W и Z , таким образом, чтобы X и W можно было сопоставить с помощью f , а Y и Z можно было сопоставить с помощью g . Точнее, $W = f(X) = \{f(x) \mid x \in X\}$ и $Y = g(Z) = \{g(z) \mid z \in Z\}$. Подход проиллюстрирован на рис. 8.4. Получив это разделение, мы сможем определить h , полагая $h(a) = f(a)$ для $a \in X$ и $h(a) = g^{-1}(a)$ для $a \in Y$.

Как мы можем выбрать множества X , Y , W и Z ? Прежде всего обратите внимание, что каждый элемент Y должен быть в $\text{Ran}(g)$, поэтому любой элемент A , который не находится в $\text{Ran}(g)$, должен быть в X . Другими словами, если мы положим $A_1 = A \setminus \text{Ran}(g)$, то мы должны иметь $A_1 \subseteq X$. Но теперь рассмотрим любой $a \in A_1$. Мы знаем, что у нас должен быть $a \in X$, и, следовательно, $f(a) \in W$. Но теперь заметим, что поскольку g взаимно однозначна, $g(f(a))$ будет отличаться от $g(z)$ для любого $z \in Z$, поэтому $g(f(a)) \notin g(Z) = Y$. Таким образом, мы должны иметь $g(f(a)) \in X$. Поскольку a был произвольным элементом из A_1 , это говорит о том, что если мы положим $A_2 = g(f(A_1)) = \{g(f(a)) \mid a \in A_1\}$, то

мы должны иметь $A_2 \subseteq X$. Аналогично, если мы положим $A_3 = g(f(A_2))$, то окажется, что у нас должно быть $A_3 \subseteq X$. Продолжая таким образом, мы можем определить множества A_n для каждого натурального числа n , и для каждого n мы должны иметь $A_n \subseteq X$. Как вы увидите, допущение $X = \bigcup_{n \in \mathbb{Z}^+} A_n$ работает. В следующем доказательстве мы фактически не упоминаем множества W и Z .

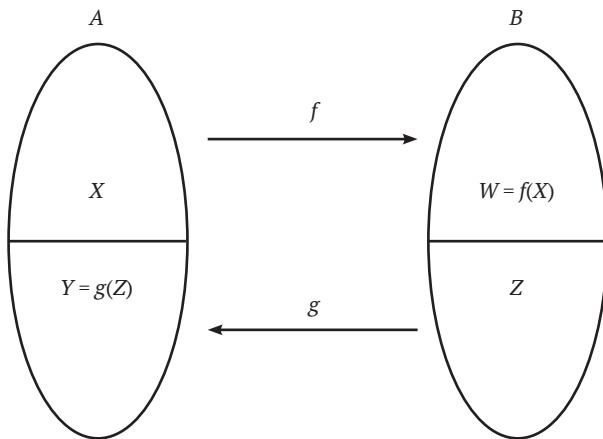


Рис. 8.4 ♦ Разделение множеств A и B на части с сопоставлениями

Доказательство. Предположим, что $A \lesssim B$ и $B \lesssim A$. Тогда мы можем выбрать взаимно однозначные функции $f: A \rightarrow B$ и $g: B \rightarrow A$. Пусть $R = \text{Ran}(g) \subseteq A$. Тогда g отображается на R , поэтому по теореме 5.3.4 $g^{-1}: R \rightarrow B$.

Теперь определим последовательность множеств A_1, A_2, A_3, \dots с помощью рекурсии следующим образом:

$$\begin{aligned} A_1 &= A \setminus R; \\ A_{n+1} &= g(f(A_n)) = \{g(f(a)) \mid a \in A_n\} \text{ для любого } n \in \mathbb{Z}^+. \end{aligned}$$

Пусть $X = \bigcup_{n \in \mathbb{Z}^+} A_n$ и $Y = A \setminus X$. Конечно, каждый элемент a находится в любом из множеств X или Y , но не в обоих одновременно. Теперь определим функцию $h: A \rightarrow B$ следующим образом:

$$h(a) = \begin{cases} f(a), & \text{если } a \in Y \\ g^{-1}(a), & \text{если } a \in Y \end{cases}$$

Обратите внимание, что для любого $a \in A$ если $a \notin R$, то $a \in A_1 \subseteq X$. Таким образом, если $a \in Y$, то $a \in R$, поэтому $g(a)$ определена. Следовательно, это определение имеет смысл.

Мы покажем, что h взаимно однозначна и сюръективна, откуда следует, что $A \sim B$. Чтобы показать, что h взаимно однозначна, предположим, что $a_1 \in A$, $a_2 \in A$ и $h(a_1) = h(a_2)$.

Случай 1. $a_1 \in X$. Предположим, что $a_2 \in Y$. Тогда, согласно определению h , $h(a_1) = f(a_1)$ и $h(a_2) = g^{-1}(a_2)$. Таким образом, уравнение $h(a_1) = h(a_2)$ означает

$f(a_1) = g^{-1}(a_2)$, поэтому $g(f(a_1)) = g(g^{-1}(a_2)) = a_2$. Поскольку $a_1 \in X = \bigcup_{n \in \mathbb{Z}^+} A_n$, мы можем выбрать такое число $n \in \mathbb{Z}^+$, что $a_1 \in A_n$. Но тогда $a_2 = g(f(a_1)) \in g(f(A_n)) = A_{n+1}$, поэтому $a_2 \in X$, что противоречит нашему предположению, что $a_2 \in Y$.

Таким образом, $a_2 \notin Y$, значит, $a_2 \in X$. Это означает, что $h(a_2) = f(a_2)$, поэтому из уравнения $h(a_1) = h(a_2)$ мы получаем $f(a_1) = f(a_2)$. Но f взаимно однозначна, поэтому $a_1 = a_2$.

Случай 2. $a_1 \in Y$. Как и в случае 1, если $a_2 \in X$, то мы получаем противоречие, значит, $a_2 \in Y$. Таким образом, уравнение $h(a_1) = h(a_2)$ означает $g^{-1}(a_1) = g^{-1}(a_2)$. Следовательно, $a_1 = g(g^{-1}(a_1)) = g(g^{-1}(a_2)) = a_2$.

В обоих случаях $a_1 = a_2$, поэтому h взаимно однозначно.

Чтобы показать, что h сюръективна, предположим, что $b \in B$. Тогда $g(b) \in A$, так что либо $g(b) \in X$, либо $g(b) \in Y$.

Случай 1. $g(b) \in X$. Выберем n такое, что $g(b) \in A_n$. Обратите внимание, что $g(b) \in \text{Ran}(g) = R$ и $A_1 = A \setminus R$, поэтому $g(b) \notin A_1$. Поскольку $n > 1$, значит, $A_n = g(f(A_{n-1}))$, и поэтому мы можем выбрать такое $a \in A_{n-1}$, что $g(f(a)) = g(b)$. Но тогда, поскольку g взаимно однозначно, $f(a) = b$. Так как $a \in A_{n-1}$, $a \in X$, поэтому $h(a) = f(a) = b$. Таким образом, $b \in \text{Ran}(h)$.

Случай 2. $g(b) \in Y$. Тогда $h(g(b)) = g^{-1}(g(b)) = b$, поэтому $b \in \text{Ran}(h)$.

В обоих случаях $b \in \text{Ran}(h)$, значит, h сюръективна.

Теорема Кантора–Шредера–Бернштейна часто бывает полезной для демонстрации того, что множества равномощны. Например, в упражнении 3 раздела 8.1 я просил вас показать, что $(0, 1] \sim (0, 1)$, где

$$(0, 1] = \{x \in \mathbb{R} \mid 0 < x \leq 1\}$$

и

$$(0, 1) = \{x \in \mathbb{R} \mid 0 < x < 1\}.$$

На удивление сложно найти взаимно однозначное соответствие между этими двумя множествами, но легко показать, что они равномощны, используя теорему Кантора–Шредера–Бернштейна. Бессспорно, $(0, 1) \subseteq (0, 1]$, так что очевидно $(0, 1) \precsim (0, 1]$. Для другого направления определите $f: (0, 1] \rightarrow (0, 1)$ по формуле $f(x) = x/2$. Легко проверить, что эта функция взаимно однозначна (хотя и не сюръективна), поэтому $(0, 1] \precsim (0, 1)$. Таким образом, по теореме Кантора–Шредера–Бернштейна $(0, 1] \sim (0, 1)$. Подробнее об этом примере см. упражнение 9.

Наша следующая теорема демонстрирует более удивительное следствие теоремы Кантора–Шредера–Бернштейна.

Теорема 8.3.3. $\mathbb{R} \sim \mathcal{P}(\mathbb{Z}^+)$.

Непосредственно доказать данную теорему на примере определения взаимно однозначной функции от \mathbb{R} к $\mathcal{P}(\mathbb{Z}^+)$ довольно сложно. В нашем доказательстве мы будем использовать теорему Кантора–Шредера–Бернштейна и следующую лемму.

Лемма 8.3.4. Предположим, что x и y – действительные числа и $x < y$. Тогда существует такое рациональное число q , что $x < q < y$.

Доказательство. Пусть k – натуральное число, большее, чем $1/(y-x)$. Тогда $1/k < y-x$. Мы покажем, что существует дробь со знаменателем k , которая находится между x и y .

Пусть m и n – целые числа такие, что $m < x < n$, и пусть $S = \{j \in \mathbb{N} \mid m + j/k > x\}$. Обратите внимание, что $m + k(n-m)/k = n > x$, и, следовательно, $k(n-m) \in S$. Таким образом, $S \neq \emptyset$, поэтому по принципу полного упорядочения оно имеет наименьший элемент. Пусть j будет наименьшим элементом S . Отметим также, что $m + 0/k = m < x$, поэтому $0 \notin S$ и, следовательно, $j > 0$. Таким образом, $j-1$ является натуральным числом, но поскольку j – наименьший элемент множества S , то $j-1 \notin S$. Отсюда следует, что $m + (j-1)/k \leq x$.

Пусть $q = m + j/k$. Ясно, что q – рациональное число, и поскольку $j \in S$, то $q = m + j/k > x$. Кроме того, объединяя выводы, что $m + (j-1)/k \leq x$ и $1/k < y-x$, мы имеем

$$q = m + \frac{j}{k} = m + \frac{j-1}{k} + \frac{1}{k} < x + (y-x) = y.$$

Таким образом, мы получили неравенство $x < q < y$, что и требовалось доказать.

Доказательство теоремы 8.3.3. Как мы отмечали ранее, мы уже знаем, что $\mathcal{P}(\mathbb{Z}^+) \lesssim \mathbb{R}$. Теперь рассмотрим функцию $f: \mathbb{R} \rightarrow \mathcal{P}(\mathbb{Q})$, определенную следующим образом:

$$f(x) = \{q \in \mathbb{Q} \mid q < x\}.$$

Мы утверждаем, что f взаимно однозначна. Чтобы показать, что это так, предположим, что $x \in \mathbb{R}$, $y \in \mathbb{R}$ и $x \neq y$. Тогда либо $x < y$, либо $y < x$. Предположим сначала, что $x < y$. По лемме 8.3.4 мы можем выбрать такое рациональное число q , что $x < q < y$. Но тогда $q \in f(y)$ и $q \notin f(x)$, поэтому $f(x) \neq f(y)$. Аналогичное рассуждение показывает, что если $y < x$, то $f(x) \neq f(y)$, поэтому f взаимно однозначна.

Поскольку f взаимно однозначна, мы тем самым показали, что $\mathbb{R} \lesssim \mathcal{P}(\mathbb{Q})$. Но мы также знаем, что $\mathbb{Q} \sim \mathbb{Z}^+$, поэтому из упражнения 5 раздела 8.1 следует, что $\mathcal{P}(\mathbb{Q}) \sim \mathcal{P}(\mathbb{Z}^+)$. Таким образом, $\mathbb{R} \lesssim \mathcal{P}(\mathbb{Q}) \lesssim \mathcal{P}(\mathbb{Z}^+)$, поэтому в силу транзитивности отношения \lesssim (см. упражнение 1) мы имеем $\mathbb{R} \lesssim \mathcal{P}(\mathbb{Z}^+)$. Комбинируя это с тем фактом, что $\mathcal{P}(\mathbb{Z}^+) \lesssim \mathbb{R}$, и применяя теорему Кантора–Шредера–Бернштейна, мы заключаем, что $\mathbb{R} \sim \mathcal{P}(\mathbb{Z}^+)$.

В начале этой главы я обещал показать, что бесконечность бывает разных размеров. Но пока что мы нашли только два размера бесконечности. Один размер представлен исчислимыми множествами, которые равномощны друг другу. Единственными примерами неисчислимых бесконечных множеств, которые мы привели до сих пор, являются $\mathcal{P}(\mathbb{Z}^+)$ и \mathbb{R} , которые, как мы теперь знаем, равномощны. На самом деле размеров бесконечности гораздо больше. Например, $\mathcal{P}(\mathbb{R})$ – бесконечное множество, которое не является ни исчислимым, ни равномощным \mathbb{R} . Следовательно, оно представляет собой третий размер бесконечности. Подробнее об этом см. в упражнении 8.

Поскольку $\mathbb{Z}^+ \prec \mathbb{R}$, было бы естественно трактовать множество действительных чисел как *большее*, чем множество положительных целых чисел. В 1878 году Кантор спросил, умещается ли еще какой-то размер бесконечности между этими двумя размерами. Точнее, существует ли такое множество X , что $\mathbb{Z}^+ \prec X \prec \mathbb{R}$? Кантор предположил, что ответ отрицательный, но не смог это доказать. Его гипотеза известна как *гипотеза континуума*. На Втором Международном конгрессе математиков в 1900 году Дэвид Гильберт (1862–1943) прочитал знаменитую лекцию, в которой перечислил, по его мнению, самые важные нерешенные математические проблемы того времени, упомянув задачу доказательства или опровержения гипотезы континуума, которая стояла на первом месте в его списке.

Статус гипотезы континуума был замечательным образом определен в работах Курта Гёделя (1906–1978) в 1939 году и Пола Коэна (1934–2007) в 1963 году. Оказывается, ответ на вопрос Кантора требует углубленного изучения даже более основополагающих понятий, чем изложенные в этой книге стратегии доказательства и основные предположения, лежащие в основе теории множеств. После проведения таких исследований можно доказать фундаментальные теоремы о том, что вообще поддается доказательству, а что – нет. Гёдель и Коэн показали, что, используя методы доказательной математики и допущения теории множеств, принятые сегодня большинством математиков, невозможно доказать гипотезу континуума, но также невозможно ее опровергнуть!

Упражнения

- *1. Докажите, что отношение \lesssim рефлексивно и транзитивно. Другими словами:
 - (а) Для любого множества A выполняется отношение $A \lesssim A$.
 - (б) Для любых множеств A, B и C если $A \lesssim B$ и $B \lesssim C$, то $A \lesssim C$.
- 2. Докажите, что \prec нерефлексивно и транзитивно. Другими словами:
 - (а) Для любого множества A справедливо утверждение $A \not\prec A$.
 - (б) Для любых множеств A, B и C если $A \prec B$ и $B \prec C$, то $A \prec C$.
- 3. Предположим, что $A \subseteq B \subseteq C$ и $A \sim C$. Докажите, что $B \sim C$.
- 4. Предположим, что $A \lesssim B$ и $C \lesssim D$.
 - (а) Докажите, что $A \times C \lesssim B \times D$.
 - (б) Докажите, что если множества A и C не пересекаются и B и D тоже не пересекаются, то $A \cup C \lesssim B \cup D$.
 - (с) Докажите, что $\mathcal{P}(A) \lesssim \mathcal{P}(B)$.
- *5. Определение обозначений, используемых в этом упражнении, см. в упражнении 23 раздела 8.1. Предположим, что $A \lesssim B$ и $C \lesssim D$.
 - (а) Докажите, что если $A \neq \emptyset$, то ${}^AC \lesssim {}^BD$.
 - (б) Действительно ли в части (а) требуется предположение, что $A \neq \emptyset$?

6. (a) Докажите, что если $A \lesssim B$ и B конечно, то A конечно и $|A| \leq |B|$.
 (b) Докажите, что если $A < B$ и B конечно, то A конечно и $|A| < |B|$.
7. Докажите, что для любого множества A существует отношение $A < \mathcal{P}(A)$.
 (Подсказка: см. упражнение 5 раздела 8.2. Обратите внимание, что, в частности, если A конечно и $|A| = n$, то, как вы показали в упражнении 11 раздела 6.2 и снова в упражнении 6 (c) раздела 8.2, $|\mathcal{P}(A)| = 2^n$. Из упражнения 6(b) следует, что $2^n > n$. Конечно, вы уже доказали это другим способом в упражнении 12(a) раздела 6.3.)
- *8. Пусть $A_1 = \mathbb{Z}^+$, и для всех $n \in \mathbb{Z}^+$ пусть $A_{n+1} = \mathcal{P}(A_n)$.
 (a) Докажите, что для всех $n \in \mathbb{Z}^+$ и $m \in \mathbb{Z}^+$ если $n < m$, то $A < A$.
 (b) Множества A_n для $n \in \mathbb{Z}^+$ представляют бесконечно много размёров бесконечности. Есть ли еще размёры бесконечности? Другими словами, можете ли вы представить себе бесконечное множество, не равное множеству A_n для любого $n \in \mathbb{Z}^+$?
9. Доказательство теоремы Кантора–Шредера–Бернштейна дает метод построения взаимно однозначной и сюръективной функции $h: A \rightarrow B$ из взаимно однозначных функций $f: A \rightarrow B$ и $g: B \rightarrow A$. Используйте этот метод, чтобы найти взаимно однозначную сюръективную функцию $h: (0, 1] \rightarrow (0, 1)$. Начните с функций $f: (0, 1] \rightarrow (0, 1)$ и $g: (0, 1) \rightarrow (0, 1]$, определенных формулами:

$$f(x) = \frac{x}{2}, \quad g(x) = x.$$

10. Пусть $\mathcal{E} = \{R \mid R - \text{отношение эквивалентности на } \mathbb{Z}^+\}.$
 (a) Докажите, что $\mathcal{E} \lesssim \mathcal{P}(\mathbb{Z}^+)$.
 (b) Пусть $A = \mathbb{Z}^+ \setminus \{1, 2\}$ и \wp – множество всех разбиений \mathbb{Z}^+ . Определим $f: \mathcal{P}(A) \rightarrow \wp$ по формуле $f(X) = \{X \cup \{1\}, (A \setminus X) \cup \{2\}\}$. Докажите, что f взаимно однозначна.
 (c) Докажите, что $\mathcal{E} \sim \mathcal{P}(\mathbb{Z}^+)$.
11. Пусть $\mathcal{T} = \{R \mid R - \text{это полный порядок на } \mathbb{Z}^+\}$. Докажите, что $\mathcal{T} \sim \mathcal{P}(\mathbb{Z}^+)$.
 (Подсказка: используйте решение упражнения 10.)
12. (a) Докажите, что если A имеет хотя бы два элемента и $A \times A \sim A$, то $\mathcal{P}(A) \times \mathcal{P}(A) \sim \mathcal{P}(A)$.
 (b) Докажите, что $\mathbb{R} \times \mathbb{R} \sim \mathbb{R}$.
13. *Интервал* – это множество $I \subseteq \mathbb{R}$ с таким свойством, что для всех действительных чисел x, y и z если $x \in I, z \in I$ и $x < y < z$, то $y \in I$. Интервал *невырожден*, если он содержит как минимум два разных действительных числа. Предположим, что \mathcal{F} – множество невырожденных интервалов и \mathcal{F} попарно не пересекается.
 Докажите, что \mathcal{F} счетно. (Подсказка: по лемме 8.3.4 каждый невырожденный интервал содержит рациональное число.)

14. Определение обозначений, используемых в этом упражнении, см. в упражнении 23 раздела 8.1.
- (a) Докажите, что ${}^{\mathbb{R}}\mathbb{R} \sim \mathcal{P}(\mathbb{R})$.
 - (b) Докажите, что ${}^{\mathbb{Q}}\mathbb{R} \sim \mathbb{R}$.
 - (c) (Для читателей, изучавших матанализ.) Пусть $\mathcal{C} = \{f \in {}^{\mathbb{R}}\mathbb{R} \mid f \text{ непрерывна}\}$. Докажите, что $\mathcal{C} \sim \mathbb{R}$. (Подсказка: покажите, что если f и g – непрерывные функции и $\forall x \in \mathbb{Q}(f(x) = g(x))$, то $f = g$.)

Приложение

Решения некоторых упражнений

Решения заданий во введении

1. (a) Один из возможных ответов: $32\ 767 = 31 \cdot 1057$.
(b) Один из возможных ответов: $x = 2^{31} - 1 = 2\ 147\ 483\ 647$.
3. (a) Метод дает простое число 211.
(b) Метод дает два простых числа: 3 и 37.

Решения к главе 1

Раздел 1.1

1. (a) $(R \vee H) \wedge \neg(H \wedge T)$, где R означает утверждение «У нас будет задание для самостоятельного чтения», H означает «У нас будет домашняя работа», а T означает «Мы будем проходить тест».
(b) $\neg G \vee (G \wedge \neg S)$, где \in означает «Вы пойдете на лыжах», а S означает «Будет снег».
(c) $\neg[(\sqrt{7} < 2) \vee (\sqrt{7} = 2)]$.
6. (a) Я не куплю брюки без рубашки.
(b) Я не куплю брюки и не куплю рубашку.
(c) Либо я не куплю брюки, либо не куплю рубашку.

Раздел 1.2

1. (a)

P	Q	$\neg P \vee Q$
F	F	T
F	T	T
T	F	F
T	T	T

5. (b)

S	G	$(S \vee G) \wedge (\neg S \vee \neg G)$
F	F	F
F	T	T
T	F	T
T	T	F

5. (a)

P	Q	$P \downarrow Q$
F	F	T
F	T	F
T	F	F
T	T	F

(b) $\neg(P \vee Q)$.(c) $\neg P$ эквивалентно $P \downarrow P$, $P \vee Q$ эквивалентно $(P \downarrow Q) \downarrow (P \downarrow Q)$,
и $P \wedge Q$ эквивалентно $(P \downarrow P) \downarrow (Q \downarrow Q)$.

7. (a) и (c) истинны; (b) и (d) ложны.

9. (a) не является ни противоречием, ни тавтологией; (b) – контрадикция;
(c) и (d) – тавтологии.11. (a) $P \vee Q$.(b) P .(c) $\neg P \vee Q$.14. Мы дважды используем ассоциативный закон для \wedge :
$$[P \wedge (Q \wedge R)] \wedge S \text{ эквивалентно } [(P \wedge Q) \wedge R] \wedge S$$

что эквивалентно $(P \wedge Q) \wedge (R \wedge S)$.

16. $P \vee \neg Q$.

Раздел 1.3

- (a) $D(6) \wedge D(9) \wedge D(15)$, где $D(x)$ означает « x делится на 3».
 (b) $D(x, 2) \wedge D(x, 3) \wedge \neg D(x, 4)$, где $D(x, y)$ означает « x делится на y ».
 (c) $N(x) \wedge N(y) \wedge [(P(x) \wedge \neg P(y)) \vee (P(y) \wedge \neg P(x))]$, где $N(x)$ означает « x – натуральное число», а $P(x)$ означает « x – простое число».
- (a) $\{x \mid x \text{ – это планета}\}.$
 (b) $\{x \mid x \text{ – университет Лиги плюща}\}.$
 (c) $\{x \mid x \text{ – штат в США}\}.$
 (d) $\{x \mid x \text{ – провинция или территория в Канаде}\}.$
- (a) $(-3 \in R) \wedge (13 - 2(-3) > 1)$. Связанные переменные: x ; свободных переменных нет. Это утверждение истинно.
 (b) $(4 \in R) \wedge (4 < 0) \wedge (13 - 2(4) > 1)$. Связанные переменные: x ; свободных переменных нет. Это утверждение ложно.

- (c) $\neg[(5 \in R) \wedge (13 - 2(5) > c)]$. Связанные переменные: x ; свободные переменные: c .
8. (a) $\{x \mid \text{Элизабет Тейлор когда-то была замужем за } x\} = \{\text{Конрад Хилтон-младший, Майкл Уилдинг, Майкл Тодд, Эдди Фишер, Ричард Бертон, Джон Уорнер, Ларри Фортенски}\}$.
- (b) $\{x \mid x - \text{логическая связка, изучаемая в разделе 1.1}\} = \{\wedge, \vee, \neg\}$.
- (c) $\{x \mid x \text{ является автором этой книги}\} = \{\text{Дэниел Дж. Веллеман}\}$.

Раздел 1.4

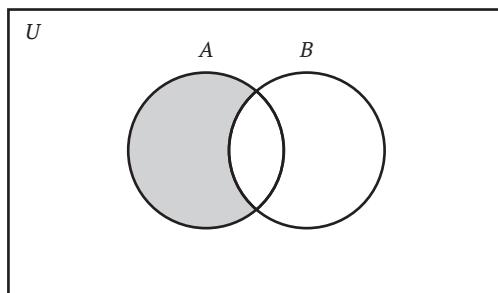
1. (a) $\{3, 12\}$.

(b) $\{1, 12, 20, 35\}$.

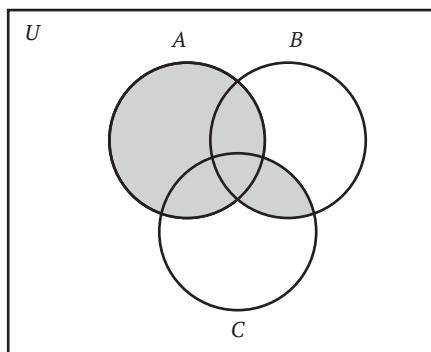
(c) $\{1, 3, 12, 20, 35\}$.

Множества в частях (a) и (b) являются подмножествами множества в части (c).

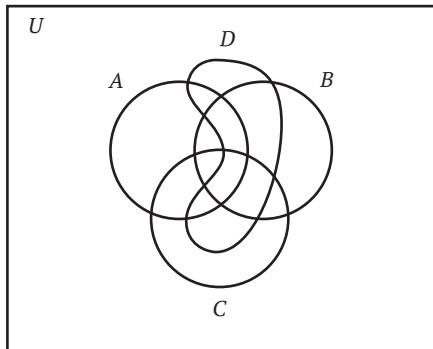
4. (a) Обе диаграммы Венна выглядят следующим образом:



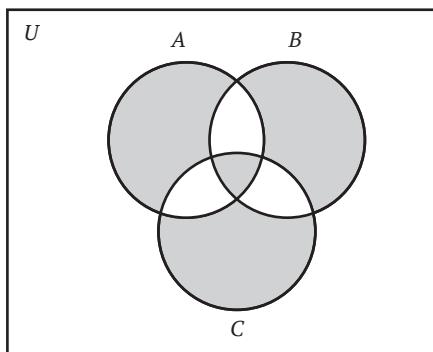
- (b) Обе диаграммы Венна выглядят следующим образом:



9. Множества (a), (d) и (e) равны между собой; множества (b) и (c) равны между собой.
12. (a) Нет области, соответствующей множеству $(A \cap D) \setminus (B \cup C)$, но в этом множестве могут быть элементы.
- (b) Вот один возможный вариант:



14. Диаграммы Венна для обоих множеств выглядят следующим образом:



Раздел 1.5

1. (a) $(S \vee \neg E) \rightarrow \neg H$, где S означает «Этот газ имеет неприятный запах», E означает «Этот газ взрывоопасен», а H означает «Этот газ является водородом».
- (b) $(F \wedge H) \rightarrow D$, где F означает «У Джорджа жар», H означает «У Джорджа болит голова», а D означает «Джордж пойдет к врачу».
- (c) $(F \rightarrow D) \wedge (H \rightarrow D)$, где буквы имеют то же значение, что и в части (b).
- (d) $(x \neq 2) \rightarrow (P(x) \rightarrow O(x))$, где $P(x)$ означает « x простое» и $O(x)$ означает « x нечетно».

4. (а) и (б) действительны, но (с) недействительны.
7. (а) Составьте таблицу истинности или рассмотрите следующую логическую цепочку:
- $(P \rightarrow R) \wedge (Q \rightarrow R)$ эквивалентно $(\neg P \vee R) \wedge (\neg Q \vee R)$,
 что эквивалентно $(\neg P \wedge \neg Q) \vee R$,
 что эквивалентно $\neg(P \vee Q) \vee R$,
 что эквивалентно $(P \vee Q) \rightarrow R$.
- (б) $(P \rightarrow R) \vee (Q \rightarrow R)$ эквивалентно $(P \wedge Q) \rightarrow R$.
9. $\neg(P \rightarrow \neg Q)$.

Решения к главе 2

Раздел 2.1

1. (а) $\forall x[\exists yF(x, y) \rightarrow S(x)]$, где $F(x, y)$ означает « x простил y », а $S(x)$ означает « x – святой».
- (б) $\neg\exists x[C(x) \wedge \forall y(D(y) \rightarrow S(x, y))]$, где $C(x)$ означает « x входит в группу математика», $D(y)$ означает « y входит в группу дискретной математики», а $S(x, y)$ означает « x умнее y ».
- (с) $\forall x(\neg(x = m) \rightarrow L(x, m))$, где $L(x, y)$ означает « x нравится y », а m означает Мэри.
- (д) $\exists x(P(x) \wedge S(j, x)) \wedge \exists y(P(y) \wedge S(r, y))$, где $P(x)$ означает « x является офицером полиции», $S(x, y)$ означает « x видел y », j означает Джейн, а r означает Роджер.
- (е) $\exists x(P(x) \wedge S(j, x) \wedge S(r, x))$, где буквы имеют то же значение, что и в части (д).
4. а) Все неженатые мужчины несчастны.
 (б) y – сестра одного из родителей x ; т. е. y – кровная тётя x .
8. (а), (д) и (е) истинны; (б), (с) и (ф) ложны.

Раздел 2.2

1. (а) $\exists x[M(x) \wedge \forall y(F(x, y) \rightarrow \neg H(y))]$, где $M(x)$ означает « x изучает математику», $F(x, y)$ означает « x и y – друзья», а $H(y)$ означает « y нуждается в помощи с домашним заданием». На разговорном языке это звучит так: существует студент-математик, все друзья которого не нуждаются в помощи с домашними заданиями.
- (б) $\exists x\forall y(R(x, y) \rightarrow \exists zL(y, z))$, где $R(x, y)$ означает « x и y – соседи по комнате», а $L(y, z)$ означает « y нравится z ». На разговорном языке это звучит так: существует кто-то такой, что всем его соседям по комнате нравится хотя бы один человек.
- (с) $\exists x[(x \in A \vee x \in B) \wedge (x \notin C \vee x \in D)]$.
- (д) $\forall x\exists y[y > x \wedge \forall z(z^2 + 5z \neq y)]$.

4. Подсказка: начните с замены $P(x)$ на $\neg P(x)$ в первом законе отрицания квантора, чтобы прийти к факту, что $\neg \exists x \neg P(x)$ эквивалентно $\forall x \neg \neg P(x)$.
6. Подсказка: начните с доказательства того, что $\exists x(P(x) \vee Q(x))$ эквивалентно $\neg \forall x \neg(P(x) \vee Q(x))$.
8. $(\forall x \in A P(x)) \wedge (\forall x \in B P(x))$
 эквивалентно $\forall x(x \in A \rightarrow P(x)) \wedge \forall x(x \in B \rightarrow P(x))$,
 что эквивалентно $\forall x[(x \in A \rightarrow P(x)) \wedge (x \in B \rightarrow P(x))]$,
 что эквивалентно $\forall x[(x \notin A \vee P(x)) \wedge (x \notin B \vee P(x))]$,
 что эквивалентно $\forall x[(x \notin A \wedge x \notin B) \vee P(x)]$,
 что эквивалентно $\forall x[\neg(x \in A \vee x \in B) \vee P(x)]$,
 что эквивалентно $\forall x[x \notin (A \cup B) \vee P(x)]$,
 что эквивалентно $\forall x[x \in (A \cup B) \rightarrow P(x)]$,
 что эквивалентно $\forall x \in (A \cup B) P(x)$.
11. $A \setminus B = \emptyset$ эквивалентно $\neg \exists x(x \in A \wedge x \notin B)$
 что эквивалентно $\forall x \neg(x \in A \wedge x \notin B)$,
 что эквивалентно $\forall x(x \notin A \vee x \in B)$,
 что эквивалентно $\forall x(x \in A \rightarrow x \in B)$,
 что эквивалентно $A \subseteq B$.
14. $A \cap B = \emptyset$ эквивалентно $\neg \exists x(x \in A \wedge x \in B)$
 что эквивалентно $\forall x \neg(x \in A \wedge x \in B)$,
 что эквивалентно $\forall x(x \notin A \vee x \notin B)$,
 что эквивалентно $\forall x(x \in A \rightarrow x \notin B)$,
 что эквивалентно $\forall x(x \notin B \wedge x \in A) \leftrightarrow x \in A$,
 (см. раздел 1.5.1, упражнение 11(b))
 что эквивалентно $\forall x(x \in A \setminus B \leftrightarrow x \in A)$,
 что эквивалентно $A \setminus B = A$.

Раздел 2.3

1. (a) $\forall x(x \in \mathcal{F} \rightarrow \forall y(y \in x \rightarrow y \in A))$.
 (b) $\forall x(x \in A \rightarrow \exists n \in \mathbb{N}(x = 2n + 1))$.
 (c) $\forall n \in \mathbb{N} \exists m \in \mathbb{N}(n^2 + n + 1 = 2m + 1)$.
 (d) $\exists x(\forall y(y \in x \rightarrow \exists i \in I(y \in A_i)) \wedge \forall i \in I \exists y(y \in x \wedge y \notin A_i))$.
4. $\bigcap \mathcal{F} = \{\text{красный, синий}\}$ и $\bigcup \mathcal{F} = \{\text{красный, зеленый, синий, оранжевый, фиолетовый}\}$.
8. (a) $A_2 = \{2, 4\}, A_3 = \{3, 6\}, B_2 = \{2, 3\}, B_3 = \{3, 4\}$.
 (b) $\bigcap_{i \in I}(A_i \cup B_i) = \{3, 4\}$ и $(\bigcap_{i \in I} A_i) \cup (\bigcap_{i \in I} B_i) = \{3\}$.
 (c) Они не эквивалентны.
12. Один из примеров: $A = \{1, 2\}$ и $B = \{2, 3\}$.
14. (a) $B_3 = \{1, 2, 3, 4, 5\}$ и $B_4 = \{1, 2, 4, 5, 6\}$.
 (b) $\bigcap_{j \in J} B_j = \{1, 2, 4, 5\}$.
 (c) $\bigcap_{i \in I}(\bigcap_{j \in J} A_{i,j}) = \{1, 2, 4\}$. Это не эквивалентно множеству в части (b).
 (d) $x \in \bigcap_{j \in J}(\bigcup_{i \in I} A_{i,j})$ означает $\forall j \in J \exists i \in I (x \in A_{i,j})$, а $x \in \bigcup_{j \in J}(\bigcap_{i \in I} A_{i,j})$ означает $\exists i \in I \forall j \in J (x \in A_{i,j})$. Они не эквивалентны.

Решения к главе 3

Раздел 3.1

1. (a) Гипотезы: n является целым числом больше 1 и n не является простым. Вывод: $2^n - 1$ не является простым числом. Гипотезы верны, когда $n = 6$, поэтому теорема говорит нам, что $2^6 - 1$ не является простым числом. Это верно, поскольку $2^6 - 1 = 63 = 9 \cdot 7$.
 (b) Мы можем заключить, что 32 767 не является простым числом. Это правильно, поскольку $32\,767 = 151 \cdot 217$.
 (c) Теорема ничего нам не говорит; 11 – простое число, поэтому гипотезы не выполняются.
4. Предположим, что $0 < a < b$. Тогда $b - a > 0$. Умножая обе части на положительное число $b + a$, получаем $(b + a) \cdot (b - a) > (b + a) \cdot 0$, или, другими словами, $b^2 - a^2 > 0$. Поскольку $b^2 - a^2 > 0$, то $a^2 < b^2$. Следовательно, если $0 < a < b$, то $a^2 < b^2$.
8. Докажем обратное. Предположим, что $x \notin B$. Тогда, поскольку $x \in A$, следует, что $x \in A \setminus B$. Но мы также знаем, что $A \setminus B \subseteq C \cap D$, поэтому мы можем заключить, что $x \in C \cap D$, и, следовательно, $x \in D$. Таким образом, если $x \notin D$, то $x \in B$.
10. Подсказка: прибавьте b к обеим сторонам неравенства $a < b$.
12. Докажем обратное. Предположим, что $c \leq d$. Умножая обе части этого неравенства на положительное число a , получаем $ac \leq ad$. Кроме того, умножение обеих частей данного неравенства $a < b$ на положительное число d дает нам $ad < bd$. Комбинируя $ac \leq ad$ и $ad < bd$, мы можем заключить, что $ac < bd$. Таким образом, если $ac \geq bd$, то $c > d$.
15. Поскольку $x > 3 > 0$, по теореме из примера 3.2.1 $x^2 > 9$. Кроме того, умножая обе части данного неравенства $y < 2$ на -2 (и меняя направление неравенства на противоположное по правилу умножения на отрицательное число), получаем $-2y > -4$. Наконец, сложение неравенств $x^2 > 9$ и $-2y > -4$ дает нам $x^2 - 2y > 5$.

Раздел 3.2

1. (a) Предположим P . Так как $P \rightarrow Q$, то отсюда следует Q . Но тогда, поскольку $Q \rightarrow R$, мы можем заключить R . Таким образом, $P \rightarrow R$.
 (b) Предположим P . Чтобы доказать, что $Q \rightarrow R$, мы докажем обратное, поэтому предположим $\neg R$. Так как $\neg R \rightarrow (P \rightarrow \neg Q)$, то $P \rightarrow \neg Q$, и поскольку мы знаем P , то можем заключить $\neg Q$. Таким образом, $Q \rightarrow R$, поэтому $P \rightarrow (Q \rightarrow R)$.
5. Предположим, что $x \in A \setminus B$ и $x \in B \setminus C$. Поскольку $x \in A \setminus B$, $x \in A$ и $x \notin B$ и поскольку $x \in B \setminus C$, то $x \in B$ и $x \notin C$. Но теперь у нас есть $x \in B$ и $x \notin B$ – противоречие. Следовательно, не может быть, чтобы $x \in A \setminus B$ и $x \in B \setminus C$.

6. Предположим, что $a \in A \setminus B$. Это означает, что $a \in A$ и $a \notin B$. Поскольку $a \in A$ и $a \in C$, то $a \in A \cap C$. Но тогда, поскольку $A \cap C \subseteq B$, следует, что $a \in B$, а это противоречит тому факту, что $a \notin B$. Таким образом, $a \notin A \setminus B$.
9. Подсказка: предположим, что $a < 1/a < b < 1/b$. Теперь докажите, что $a < 1$, затем используйте этот факт, чтобы доказать, что $a < 0$, и далее используйте этот факт, чтобы доказать, что $a < -1$.
12. (a) Предложение «Тогда $x = 3$ и $y = 8$ » некорректно. (Почему?)
 (b) Один контрпример: $x = 3, y = 7$.

15.

P	Q	R	$P \rightarrow (Q \rightarrow R)$	$\neg R \rightarrow (P \rightarrow \neg Q)$
F	F	F	T	T
F	F	T	T	T
F	T	F	T	T
F	T	T	T	T
T	F	F	T	T
T	F	T	T	T
T	T	F	F	F
T	T	T	T	T

Раздел 3.3

1. Предположим, что $\exists x(P(x) \rightarrow Q(x))$. Тогда мы можем выбрать x_0 такое, что $P(x_0) \rightarrow Q(x_0)$. Теперь предположим, что $\forall x P(x)$. Тогда, в частности, истинно $P(x_0)$, и поскольку $P(x_0) \rightarrow Q(x_0)$, то истинно $Q(x_0)$. Поскольку мы нашли конкретное значение x , для которого выполняется $Q(x)$, мы можем заключить, что $\exists x Q(x)$. Таким образом, $\forall x P(x) \rightarrow \exists x Q(x)$.
3. Предположим, что $A \subseteq B \setminus C$, но A и C не пересекаются. Тогда мы можем выбрать некоторый элемент x такой, что $x \in A$ и $x \in C$. Поскольку $x \in A$ и $A \subseteq B \setminus C$, из этого следует, что $x \in B \setminus C$, значит, $x \in B$ и $x \notin C$. Но теперь у нас есть одновременно $x \in C$ и $x \notin C$ – противоречие. Таким образом, если $A \subseteq B \setminus C$, то A и C не пересекаются.
7. Предположим, что $x > 2$. Пусть $y = (x + \sqrt{x^2 - 4})/2$; равенство определено, поскольку $x^2 - 4 > 0$. Тогда

$$y + \frac{1}{y} = \frac{x + \sqrt{x^2 - 4}}{2} + \frac{2}{x + \sqrt{x^2 - 4}} = \frac{2x^2 + 2x\sqrt{x^2 - 4}}{2(x + \sqrt{x^2 - 4})} = x.$$

9. Предположим, что \mathcal{F} – семейство множеств и $A \in \mathcal{F}$. Предположим, что $x \in \bigcap \mathcal{F}$. Тогда из определения $\bigcap \mathcal{F}$, поскольку $x \in \bigcap \mathcal{F}$ и $A \in \mathcal{F}$, следует $x \in A$. Но x был произвольным элементом $\bigcap \mathcal{F}$, следовательно, $\bigcap \mathcal{F} \subseteq A$.
12. Подсказка: предположим, что $\mathcal{F} \subseteq \mathcal{G}$, и пусть x – произвольный элемент из $\bigcup \mathcal{F}$. Вы должны доказать, что $x \in \bigcup \mathcal{G}$, что означает $\exists A \in \mathcal{G}(x \in A)$, по-

этому вы должны попытаться найти некоторое множество $A \in \mathcal{G}$ такое, что $x \in A$. Для этого запишите исходные посылки в логической форме. Вы обнаружите, что одна из них представляет собой общее утверждение, а другая – экзистенциальное. Примените экзистенциальное подтверждение к экзистенциальной исходной посылке.

14. Допустим, $x \in \bigcup_{i \in I} \mathcal{P}(A_i)$. Тогда мы можем выбрать такое $i \in I$, что $x \in \mathcal{P}(A_i)$, или, другими словами, $x \subseteq A_i$. Пусть теперь a – произвольный элемент из x . Тогда $a \in A_i$, и, следовательно, $a \in \bigcup_{i \in I} A_i$. Поскольку a – произвольный элемент x , отсюда следует, что $x \subseteq \bigcup_{i \in I} A_i$, что, в свою очередь, значит $x \in \mathcal{P}(\bigcup_{i \in I} A_i)$. Таким образом, $\bigcup_{i \in I} \mathcal{P}(A_i) \subseteq \mathcal{P}(\bigcup_{i \in I} A_i)$.
17. Подсказка: последняя гипотеза означает $\forall A \in \mathcal{F} \forall B \in \mathcal{G}(A \subseteq B)$, поэтому если в ходе доказательства вы столкнетесь с множествами $A \in \mathcal{F}$ и $B \in \mathcal{G}$, вы можете заключить, что $A \subseteq B$. Начните доказательство с того, что примите за x произвольный элемент и предположите, что $x \in \bigcap \mathcal{F}$, а затем докажите, что $x \in \bigcap \mathcal{G}$. Чтобы увидеть, куда двигаться дальше, запишите эти утверждения логическими символами.
20. Предложение «Тогда для любого действительного числа x справедливо неравенство $x^2 < 0$ » неверно. (Почему?)
22. Исходя из логической формы доказываемого утверждения, доказательство должно иметь следующую схему:

Пусть $x = \dots$

Пусть y – произвольное действительное число.

[Здесь идет доказательство, что $xy^2 = y - x$.]

Поскольку число y произвольно, $\forall y \in \mathbb{R}(xy^2 = y - x)$.

Таким образом, $\exists x \in \mathbb{R} \forall y \in \mathbb{R}(xy^2 = y - x)$.

Эта схема наводит на мысль, что у следует вводить в доказательство после x . Следовательно, x не может быть определен в терминах y , потому что y еще не был введен в доказательство к моменту, когда мы определяем x . Но в данном доказательстве x определяется через y в первом же предложении. (Ошибка была замаскирована тем фактом, что предложение «Пусть y – произвольное действительное число» было исключено из доказательства. Если вы попытаетесь добавить это предложение к доказательству, то обнаружите, что нет такого места, где его можно было бы добавить, чтобы получить корректное доказательство ошибочной теоремы.)

25. Вот начало доказательства: пусть x – произвольное действительное число. Пусть $y = 2x$. Пусть теперь z – произвольное действительное число. Затем

Раздел 3.4

1. (\rightarrow) Предположим, что $\forall x(P(x) \wedge Q(x))$. Возьмем произвольный y . Тогда поскольку $\forall x(P(x) \wedge Q(x))$, то истинно $P(y) \wedge Q(y)$ и, в частности, $P(y)$. По-

скольку y взят произвольно, это доказывает, что $\forall x P(x)$. Аналогичное рассуждение доказывает $\forall x Q(x)$: для произвольного y справедливо $P(y) \wedge Q(y)$ и, следовательно, $Q(y)$. Таким образом, $\forall x P(x) \wedge \forall x Q(x)$.

(\leftarrow) Предположим, что $\forall x P(x) \wedge \forall x Q(x)$. Возьмем произвольный y . Тогда поскольку $\forall x P(x)$, то $P(y)$, и аналогично, поскольку $\forall x Q(x)$, то $Q(y)$. Таким образом, $P(y) \wedge Q(y)$, и поскольку y взят произвольно, отсюда следует, что $\forall x (P(x) \wedge Q(x))$.

4. Предположим, что $A \subseteq B$ и $A \not\subseteq C$. Поскольку $A \not\subseteq C$, мы можем выбрать некоторый элемент $a \in A$ такой, что $a \notin C$. Поскольку $a \in A$ и $A \subseteq B$, то $a \in B$. Поскольку $a \in B$ и $a \notin C$, то $B \not\subseteq C$.
7. Пусть A и B – произвольные множества. Пусть x произвольно, и пусть $x \in \mathcal{P}(A \cap B)$. Тогда $x \subseteq A \cap B$. Пусть теперь y – произвольный элемент x . Тогда поскольку $x \subseteq A \cap B$, то $y \in A \cap B$ и, следовательно, $y \in A$. Поскольку y взят произвольно, это показывает, что $x \subseteq A$, поэтому $x \in \mathcal{P}(A)$. Аналогичное рассуждение показывает, что $x \subseteq B$ и, следовательно, $x \in \mathcal{P}(B)$. Таким образом, $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$.

Теперь предположим, что $x \in \mathcal{P}(A) \cap \mathcal{P}(B)$. Тогда $x \in \mathcal{P}(A)$ и $x \in \mathcal{P}(B)$, поэтому $x \subseteq A$ и $x \subseteq B$. Предположим, что $y \in x$. Тогда из отношений $x \subseteq A$ и $x \subseteq B$ следует $y \in A$ и $y \in B$, поэтому $y \in A \cap B$. Таким образом, $x \subseteq A \cap B$, поэтому $x \in \mathcal{P}(A \cap B)$.

- 9.
- 13.
- 16.
- 18.

(a) Предположим, что $x \in (\bigcup \mathcal{F} \cap \bigcap \mathcal{G})$. Тогда мы можем выбрать некоторый $A \in \mathcal{F}$ такой, что $x \in \bigcup \mathcal{F}$ и $x \in \bigcap \mathcal{G}$. Поскольку $x \in \bigcup \mathcal{F}$, мы можем выбрать некоторый $A \in \mathcal{F}$ такой, что $x \in A$. Так как дано, что каждый элемент \mathcal{F} не пересекается с некоторым элементом \mathcal{G} , должно существовать некоторое множество $B \in \mathcal{G}$ такое, что $A \cap B = \emptyset$. Поскольку $x \in A$, отсюда следует, что $x \notin B$. Но мы также имеем $x \in \bigcap \mathcal{G}$ и $B \in \mathcal{G}$, откуда следует, что $x \in B$ – противоречие. Таким образом, $\bigcup \mathcal{F} \cap \bigcap \mathcal{G}$ должны быть непересекающимися.

(b) Предложение «Таким образом, мы можем выбрать множество A такое, что $A \in \mathcal{F}, A \in \mathcal{G}$ и $x \in A$ » некорректно. (Почему?)

(c) Одним из примеров является семейство $\mathcal{F} = \{\{1\}, \{2\}\}$, $\mathcal{G} = \{\{1\}, \{1, 2\}\}$.

22. Предположим, что $\bigcup \mathcal{F} \not\subseteq \bigcup \mathcal{G}$. Тогда существует некоторый такой, что $x \notin \bigcup \mathcal{G}$. Так как $x \in \bigcup \mathcal{F}$, мы можем выбрать множество $A \in \mathcal{F}$ такое, что $x \in A$. Возьмем теперь произвольное множество $B \in \mathcal{G}$. Если $A \subseteq B$, то поскольку $x \in A$, то $x \in B$. Но тогда поскольку $x \in B$ и $B \in \mathcal{G}$, то $x \in \bigcup \mathcal{G}$, что, как мы уже знаем, ложно. Следовательно, $A \not\subseteq B$. Поскольку B было произвольным, это показывает, что для всех $B \in \mathcal{G}$ справедливо $A \not\subseteq B$. Таким образом, мы показали, что существует некоторое множество $A \in \mathcal{F}$ такое, что для всех $B \in \mathcal{G}$ справедливо утверждение $A \not\subseteq B$.
24. (a) Предположим, что $x \in \bigcup_{i \in I} (A_i \setminus B_i)$. Затем мы можем выбрать число $i \in I$ такое, что $x \in A_i \setminus B_i$, что означает $x \in A_i$ и $x \notin B_i$. Поскольку $x \in A_i$, то $x \in \bigcup_{i \in I} A_i$, и поскольку $x \notin B_i$, то $x \notin \bigcap_{i \in I} B_i$. Таким образом, $x \in (\bigcup_{i \in I} A_i) \setminus (\bigcap_{i \in I} B_i)$.
- (b) Один из возможных примеров: $I = \{1, 2\}$, $A_1 = B_1 = \{1\}$, $A_2 = B_2 = \{2\}$.

Раздел 3.5

1. Предположим, что $x \in A \cap (B \cup C)$. Тогда $x \in A$ и либо $x \in B$, либо $x \in C$.
- Случай 1. $x \in B$. Тогда поскольку $x \in A$, то $x \in A \cap B$, поэтому $x \in (A \cap B) \cup C$.
- Случай 2. $x \in C$. Тогда очевидно, что $x \in (A \cap B) \cup C$.
- Поскольку элемент x был взят произвольно, мы можем заключить, что $A \cap (B \cup C) \subseteq (A \cap B) \cup C$.
5. Предположим, что $x \in A$. Теперь рассмотрим два случая:
- Случай 1. $x \in C$. Тогда $x \in A \cap C$, поэтому поскольку $A \cap C \subseteq B \cap C$, то $x \in B \cap C$ и, следовательно, $x \in B$.
- Случай 2. $x \notin C$. Так как $x \in A$, то $x \in A \cup C$, и, значит, поскольку $A \cup C \subseteq B \cup C$, то $x \in B \cup C$. Но $x \notin C$, значит, должно быть $x \in B$.
- Таким образом, $x \in B$, а поскольку x взят произвольно, то $A \subseteq B$.
8. Подсказка: предположим, что $x \in \mathcal{P}(A) \cup \mathcal{P}(B)$, что означает, что либо $x \in \mathcal{P}(A)$, либо $x \in \mathcal{P}(B)$. Рассматривайте это как два отдельных случая.
- В случае 1 предположим, что $x \in \mathcal{P}(A)$, что означает $x \subseteq A$, и докажем, что $x \in \mathcal{P}(A \cup B)$, что означает $x \subseteq A \cup B$. Случай 2 аналогичен.
12. Пусть x – произвольное действительное число.
- (\leftarrow) Предположим, $|x - 4| > 2$.
- Случай 1. $x - 4 \geq 0$. Тогда $|x - 4| = x - 4$, поэтому мы имеем $x - 4 > 2$, и, следовательно, $x > 6$. Добавление x к обеим сторонам дает нам $2x > 6 + x$, поэтому $2x - 6 > x$. Поскольку $x > 6$, это означает, что $2x - 6$ положительно, значит, $|2x - 6| = 2x - 6 > x$.
- Случай 2. $x - 4 < 0$. Тогда $|x - 4| = 4 - x$, поэтому мы имеем $4 - x > 2$, и, следовательно, $x < 2$. Поэтому $3x < 6$ и, вычитая $2x$ с обеих сторон неравенства, получаем $x < 6 - 2x$. Кроме того, из $x < 2$ мы получаем $2x < 4$, поэтому $2x - 6 < -2$. Следовательно, $2x - 6$ отрицательно, поэтому $|2x - 6| = 6 - 2x > x$.
- (\rightarrow) Подсказка: повторите направление « \leftarrow », используя случаи $2x - 6 \geq 0$ и $2x - 6 < 0$.

16. (a) Предположим, что $x \in \bigcup(\mathcal{F} \cup \mathcal{G})$. Тогда мы можем выбрать множество $A \in \mathcal{F} \cup \mathcal{G}$ такое, что $x \in A$. Поскольку $A \in \mathcal{F} \cup \mathcal{G}$, либо $A \in \mathcal{F}$, либо $A \in \mathcal{G}$.
- Случай 1. $A \in \mathcal{F}$. Поскольку $x \in A$ и $A \in \mathcal{F}$, то $x \in \bigcup \mathcal{F}$. Следовательно, $x \in (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$.
- Случай 2. $A \in \mathcal{G}$. Поскольку $x \in A$ и $A \in \mathcal{G}$, то $x \in \bigcup \mathcal{G}$. Следовательно, $x \in (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$.
- Таким образом, $x \in (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$.
- Теперь предположим, что $x \in (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G})$. Тогда либо $x \in \bigcup \mathcal{F}$, либо $x \in \bigcup \mathcal{G}$.
- Случай 1. $x \in \bigcup \mathcal{F}$. Тогда мы можем выбрать некоторое множество $A \in \mathcal{F}$ такое, что $x \in A$. Поскольку $A \in \mathcal{F}$, то $A \in \mathcal{F} \cup \mathcal{G}$, поэтому из $x \in A$ следует, что $x \in \bigcup(\mathcal{F} \cup \mathcal{G})$.
- Случай 2. $x \in \bigcup \mathcal{G}$. Аналогичные рассуждения показывают, что $x \in \bigcup(\mathcal{F} \cup \mathcal{G})$.
- Таким образом, $x \in \bigcup(\mathcal{F} \cup \mathcal{G})$.
- (b) Теорема такова: $\bigcap(\mathcal{F} \cup \mathcal{G}) = (\bigcap \mathcal{F}) \cap (\bigcap \mathcal{G})$.
20. (\rightarrow) Предположим, что $A \Delta B$ и C не пересекаются. Пусть x – произвольный элемент из $A \cap C$. Тогда $x \in A$ и $x \in C$. Если $x \notin B$, то, поскольку $x \in A$, справедливо утверждение $x \in A \setminus B$ и, следовательно, $x \in A \Delta B$. Но при этом $x \in C$, что противоречит нашему предположению, что $A \Delta B$ и C не пересекаются. Следовательно, $x \in B$. Поскольку мы также знаем, что $x \in C$, мы имеем $x \in B \cap C$. Поскольку x представляет собой произвольный элемент из $A \cap C$, это означает, что $A \cap C \subseteq B \cap C$. Аналогичное рассуждение показывает, что $B \cap C \subseteq A \cap C$.
- (\leftarrow) Предположим, что $A \cap C = B \cap C$. Предположим, что $A \Delta B$ и C пересекаются. Тогда мы можем выбрать некоторый элемент x такой, что $x \in A \Delta B$ и $x \in C$. Поскольку $x \in A \Delta B$, то либо $x \in A \setminus B$, либо $x \in B \setminus A$.
- Случай 1. $x \in A \setminus B$. Тогда $x \in A$ и $x \notin B$. Поскольку мы также знаем, что $x \in C$, мы можем заключить, что $x \in A \cap C$, но $x \notin B \cap C$. Это противоречит тому факту, что $A \cap C = B \cap C$.
- Случай 2. $x \in B \setminus A$. Аналогичные рассуждения также приводят к противоречию.
- Таким образом, мы можем заключить, что $A \Delta B$ и C не пересекаются.
23. (a) Подсказка: предположите, что $x \in A \setminus C$, а затем разбейте доказательство на случаи $x \in B$ и $x \notin B$. (b) Подсказка: примените часть (a).
24. (a) Предположим, что $x \in (A \cup B) \Delta C$. Тогда либо $x \in (A \cup B) \setminus C$, либо $x \in C \setminus (A \cup B)$.
- Случай 1. $x \in (A \cup B) \setminus C$. Тогда либо $x \in A$, либо $x \in B$ и $x \notin C$. Теперь мы разбиваем случай 1 на два подслучаи, в зависимости от того, $x \in A$ или $x \in B$.
- Случай 1а. $x \in A$. Тогда $x \in A \setminus C$, поэтому $x \in A \Delta C$, поэтому $x \in (A \Delta C) \cup (B \Delta C)$.
- Случай 1б. $x \in B$. Аналогично, $x \in B \Delta C$, поэтому $x \in (A \Delta C) \cup (B \Delta C)$.
- Случай 2. $x \in C \setminus (A \cup B)$. Тогда $x \in C$, $x \notin A$ и $x \notin B$. Отсюда следует, что $x \in A \Delta C$ и $x \in B \Delta C$, поэтому, безусловно, $x \in (A \Delta C) \cup (B \Delta C)$.

- (b) Вот один из возможных примеров: $A = \{1\}$, $B = \{2\}$, $C = \{1, 2\}$.
27. Доказательство ошибочно, потому что оно только устанавливает, что либо $0 < x$, либо $x < 6$, хотя необходимо доказать, что $0 < x$ и $x < 6$. Однако это можно исправить.
29. Доказательство верно.
31. Подсказка: вот контрпример к теореме: $A = \{1, 2\}$, $B = \{1\}$, $C = \{2\}$.

Раздел 3.6

1. Пусть x – произвольное действительное число. Пусть $y = x/(x^2 + 1)$. Тогда
- $$x - y = x - \frac{x}{x^2 + 1} = \frac{x^3 + x}{x^2 + 1} - \frac{x}{x^2 + 1} = \frac{x^3}{x^2 + 1} = x^2 \cdot \frac{x}{x^2 + 1} = x^2 y.$$
- Чтобы убедиться в уникальности y , предположим, что $x^2 z = x - z$. Тогда $z(x^2 + 1) = x$, и поскольку $x^2 + 1 \neq 0$, мы можем разделить обе стороны на $x^2 + 1$, чтобы заключить, что $z = x/(x^2 + 1) = y$.
4. Предположим, что $x \neq 0$. Пусть $y = 1/x$. Теперь пусть z – произвольное действительное число. Тогда $zy = z(1/x) = z/x$, что и требовалось доказать. Чтобы убедиться, что y уникально, предположим, что y' – число со свойством $\forall z \in \mathbb{R} (zy' = z/x)$. Тогда, в частности, взяв $z = 1$, имеем $y' = 1/x$, поэтому $y' = y$.
6. (a) Пусть $A = \emptyset \in \mathcal{P}(U)$. Тогда ясно, что для любого $B \in \mathcal{P}(U)$ $A \cup B = 0 \cup B = B$.
- Чтобы убедиться, что множество A единственno, предположим, что $A' \in \mathcal{P}(U)$ и для всех $B \in \mathcal{P}(U)$ справедливо $A' \cup B = B$. Тогда, в частности, приняв $B = \emptyset$, мы можем заключить, что $A' \cup \emptyset = \emptyset$. Но ясно, что $A' \cup \emptyset = A'$, поэтому $A' = \emptyset = A$.

- (b) Подсказка: пусть $A = U$.
11. Существование: нам дано, что для каждого $\mathcal{G} \subseteq \mathcal{F}$ справедливо $\bigcup \mathcal{G} \in \mathcal{F}$, поэтому, в частности, из $\mathcal{F} \subseteq \mathcal{F}$ следует $\bigcup \mathcal{F} \in \mathcal{F}$. Пусть $A = \bigcup \mathcal{F}$. Теперь предположим, что $B \in \mathcal{F}$. Далее из упражнения 8 раздела 3.3.1 следует, что $B \subseteq \bigcup \mathcal{F} = A$, что и ожидалось.
- Единственность: предположим, что $A_1 \in \mathcal{F}$, $A_2 \in \mathcal{F}$, $\forall B \in \mathcal{F} (B \subseteq A_1)$ и $\forall B \in \mathcal{F} (B \subseteq A_2)$. Применяя этот последний факт к $B = A_1$, мы можем заключить, что $A_1 \subseteq A_2$, и аналогично предыдущий факт влечет, что $A_2 \subseteq A_1$. Таким образом, $A_1 = A_2$.

Раздел 3.7

1. Совет: сравнение части (b) с упражнением 16 из раздела 3.3.1 может дать вам представление о том, что использовать в качестве A .
5. Пусть $\mathcal{P}(\bigcup_{i \in I} A_i) \subseteq \bigcup_{i \in I} \mathcal{P}(A_i)$. Очевидно, что $\bigcup_{i \in I} A_i \subseteq \bigcup_{i \in I} A_i$, поэтому $\bigcup_{i \in I} A_i \in \mathcal{P}(\bigcup_{i \in I} A_i)$, и отсюда следует, что $\bigcup_{i \in I} A_i \in \bigcup_{i \in I} \mathcal{P}(A_i)$. Из определения объ-

единения семьи следует, что существует некоторое число $i \in I$ такое, что $\bigcup_{i \in I} A_i \subseteq A_i$. Возьмем теперь произвольное число $j \in I$. Из упражнения 8 в разделе 3.3.1 следует, что $A_j \subseteq \bigcup_{i \in I} A_i$, так что $A_j \subseteq A_i$.

8. Предположим, что $\lim_{x \rightarrow c} f(x) = L > 0$. Пусть $\epsilon = L$. Тогда по определению предела мы можем выбрать некоторое число $\delta > 0$ такое, что для всех x если $0 < |x - c| < \delta$, то $|f(x) - L| < \epsilon = L$. Пусть теперь x – произвольное действительное число, и пусть $0 < |x - c| < \delta$. Тогда $|f(x) - L| < L$, поэтому $-L < f(x) - L < L$ и, следовательно, $0 < f(x) < 2L$. Следовательно, для любого действительного числа x если $0 < |x - c| < \delta$, то $f(x) > 0$.
10. Доказательство корректно.

Решения к главе 4

Раздел 4.1

1. (a) $\{(x, y) \in P \times P \mid x \text{ является родителем } y\} = \{(Билл Клинтон, Челси Клинтон), (Голди Хоун, Кейт Хадсон), \dots\}$.
(b) $\{(x, y) \in C \times U \mid \text{есть кто-то, кто живет в } x \text{ и посещает } y\}$. Если вы студент университета, пусть x будет городом, в котором вы живете, а y – университетом, который вы посещаете; тогда (x, y) будет элементом этого множества истинности.
4. $A \times (B \cap C) = (A \times B) \cap (A \times C) = \{(1, 4), (2, 4), (3, 4)\}$,
 $A \times (B \cup C) = (A \times B) \cup (A \times C)$
 $= \{(1, 1), (2, 1), (3, 1), (1, 3), (2, 3), (3, 3), (1, 4), (2, 4), (3, 4)\}$.
 $(A \times B) \cap (C \times D) = (A \cap C) \times (B \cap D) = \emptyset$,
 $(A \times B) \cup (C \times D) = \{(1, 1), (2, 1), (3, 1), (1, 4), (2, 4), (3, 4), (3, 5), (4, 5)\}$,
 $(A \cup C) \times (B \cup D) = \{(1, 1), (2, 1), (3, 1), (4, 1), (1, 4), (2, 4), (3, 4), (4, 4), (1, 5), (2, 5), (3, 5), (4, 5)\}$.
6. Случаи не являются исчерпывающими.
8. Да, это истинно.
10. Предположим, что $(x, y) \in (A \setminus C) \times (B \setminus D)$. Тогда $x \in A \setminus C$ и $y \in B \setminus D$, что означает $x \in A$, $x \notin C$, $y \in B$ и $y \notin D$. Поскольку $x \in A$ и $y \in B$, то $(x, y) \in A \times B$. И поскольку $x \notin C$, то $(x, y) \notin C \times D$. Следовательно, $(x, y) \in (A \times B) \setminus (C \times D)$.
15. Теорема неверна. Контрпример: $A = \{1\}$, $B = C = D = \emptyset$.
Обратите внимание, что $A \not\subseteq C$. Где ошибка в доказательстве того, что $A \subseteq C$?

Раздел 4.2

1. (a) Область определения = $\{p \in P \mid p \text{ имеет ныне живущего ребенка}\}$;
Область значений = $\{p \in P \mid p \text{ имеет ныне живущего родителя}\}$.
(b) Область определения = \mathbb{R} ; область значений = \mathbb{R}^+ .

5. (a) $\{(1, 4), (1, 5), (1, 6), (2, 4), (3, 6)\}$.
 (b) $\{(4, 4), (5, 5), (5, 6), (6, 5), (6, 6)\}$.
 8. $E \circ E \subseteq F$.

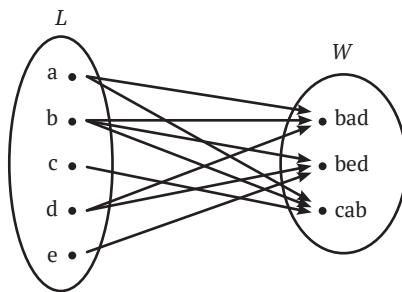
11. Докажем обратное для обоих направлений.

(\rightarrow) Предположим, что $\text{Ran}(R)$ и $\text{Dom}(S)$ не пересекаются. Тогда мы можем выбрать некоторый элемент $b \in \text{Ran}(R) \cap \text{Dom}(S)$. Поскольку $b \in \text{Ran}(R)$, мы можем выбрать некоторый элемент $a \in A$ такой, что $(a, b) \in R$. Аналогично, поскольку $b \in \text{Dom}(S)$, мы можем выбрать некоторый элемент $c \in C$ такой, что $(b, c) \in S$. Но тогда $(a, c) \in S \circ R$, поэтому $S \circ R \neq \emptyset$.

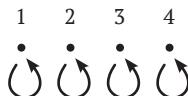
(\leftarrow) Предположим, что $S \circ R \neq \emptyset$. Тогда мы можем выбрать некоторый элемент $(a, c) \in S \circ R$. По определению $S \circ R$ это означает, что мы можем выбрать некоторый элемент $b \in B$ такой, что $(a, b) \in R$ и $(b, c) \in S$. Но тогда $b \in \text{Ran}(R)$ и $b \in \text{Dom}(S)$, поэтому $\text{Ran}(R)$ и $\text{Dom}(S)$ не пересекаются.

Раздел 4.3

1.



3.



5. $S \circ R = \{(a, y), (a, z), (b, x), (c, y), (c, z)\}$.
7. (\rightarrow) Предположим, что R рефлексивно. Пусть (x, y) – произвольный элемент i_A . Тогда из определения i_A следует $x = y \in A$. Поскольку R рефлексивно, $(x, y) = (x, x) \in R$. Так как (x, y) произвольно, это показывает, что $i_A \subseteq R$.
 (\leftarrow) Пусть $i_A \subseteq R$. Возьмем произвольный элемент $x \in A$. Тогда $(x, x) \in i_A$, поскольку $i_A \subseteq R$, $(x, x) \in R$. Так как x был произвольным, это показывает, что R рефлексивно.
10. Предположим, что $(x, y) \in i_D$. Тогда $x = y \in D = \text{Dom}(S)$, значит, существует элемент $z \in A$ такой, что $(x, z) \in S$. Следовательно $(z, x) \in S^{-1}$, поэтому $(x, y) = (x, x) \in S^{-1} \circ S$. Таким образом, $i_D \subseteq S^{-1} \circ S$. Доказательство другого утверждения аналогично.

13. (a) Да. Чтобы доказать это, предположим, что R_1 и R_2 рефлексивны, и предположим, что $a \in A$. Поскольку R_1 рефлексивно, $(a, a) \in R_1$, поэтому $(a, a) \in R_1 \cup R_2$.
- (b) Да. Чтобы доказать это, предположим, что R_1 и R_2 симметричны, и пусть $(x, y) \in R_1 \cup R_2$. Тогда либо $(x, y) \in R_1$, либо $(x, y) \in R_2$. Если $(x, y) \in R_1$, то, поскольку R_1 симметрично, $(y, x) \in R_1$, поэтому $(y, x) \in R_1 \cup R_2$. Аналогичные рассуждения показывают, что если $(x, y) \in R_2$, то $(y, x) \in R_1 \cup R_2$.
- (c) Нет. Контрпример: $A = \{1, 2, 3\}$, $R_1 = \{(1, 2)\}$, $R_2 = \{(2, 3)\}$.
17. Прежде всего отметим, что согласно части 2 теоремы 4.3.4, поскольку R и S симметричны, $R = R^{-1}$ и $S = S^{-1}$. Следовательно:

$R \circ S$ симметрично,

если и только если $R \circ S = (R \circ S)^{-1}$ (теорема 4.3.4, часть 2)),
 если и только если $R \circ S = R^{-1} \circ S^{-1}$,
 если и только если $R \circ S = S \circ R$.

20. Предположим, что R транзитивно, и предположим, что $(X, Y) \in S$ и $(Y, Z) \in S$. Чтобы доказать, что $(X, Z) \in S$, мы должны показать, что $\forall x \in X \forall z \in Z (xRz)$, поэтому возьмем произвольные $x \in X$ и $z \in Z$. Поскольку $Y \in B$, $Y \neq \emptyset$, поэтому мы можем выбрать $y \in Y$. Так как $(X, Y) \in S$ и $(Y, Z) \in S$, по определению S имеем xRy и yRz . Но тогда, поскольку R транзитивно, xRz , что и требовалось доказать. Пустое множество нужно было исключить из B , чтобы мы могли найти $y \in Y$ в этом доказательстве. (Можете ли вы найти контрпример, если не исключить пустое множество?)
23. Подсказка: предположим, что aRb и bRc . Чтобы доказать aRc , предположим, что $X \subseteq A \setminus \{a, c\}$ и $X \cup \{a\} \in \mathcal{F}$; вы должны доказать, что $X \cup \{c\} \in \mathcal{F}$. Для этого вам может быть полезно рассмотреть два случая: $b \notin X$ и $b \in X$. Во втором случае попробуйте работать с множествами $X' = (X \cup \{a\}) \setminus \{b\}$ и $X'' = (X \cup \{c\}) \setminus \{b\}$.

Раздел 4.4

1. (a) Частичный, но не полный порядок. (b) Это не частичный порядок.
 (c) Частичный, но не полный порядок.
4. (\rightarrow) Предположим, что R одновременно антисимметрично и симметрично. Предположим, что $(x, y) \in R$. Тогда поскольку R симметрично, $(y, x) \in R$ и поскольку R является антисимметричным, то $x = y$. Следовательно $(x, y) \in i_A$. Поскольку (x, y) выбраны произвольно, это показывает, что $R \subseteq i_A$.
 (\leftarrow) Предположим, что $R \subseteq i_A$. Предположим, что $(x, y) \in R$. Тогда $(x, y) \in i_A$, поэтому $x = y$ и, следовательно, $(y, x) = (x, y) \in R$. Это показывает, что R симметрично. Чтобы убедиться, что R антисимметрично, предположим, что $(x, y) \in R$ и $(y, x) \in R$. Тогда $(x, y) \in i_A$, поэтому $x = y$.
8. Чтобы показать, что T рефлексивно, возьмем произвольную пару $(a, b) \in A \times B$. Поскольку R и S оба рефлексивны, мы имеем aRa и bSb . По опре-

делению T следует, что $(a, b)T(a, b)$. Чтобы убедиться, что T антисимметрично, предположим, что $(a, b)T(a', b')$ и $(a', b')T(a, b)$. Тогда aRa' , и $a'Ra$, так как R антисимметрично, $a = a'$. Аналогично, bSb' и $b'Sb$, поэтому, поскольку S антисимметрично, мы также имеем $b = b'$. Таким образом, $(a, b) = (a', b')$, что и требовалось доказать. Наконец, чтобы показать, что T транзитивно, предположим, что $(a, b)T(a', b')$ и $(a', b')T(a'', b'')$. Тогда aRa' и $a'Ra'$, и так как R транзитивно, aRa'' . Аналогично, bSb' и $b'Sb''$, поэтому bSb'' , и, следовательно, $(a, b)T(a'', b'')$.

Даже если и R , и S являются полными порядками, T не обязательно должен быть полным порядком.

11. Минимальные элементы B – простые числа. B не имеет наименьшего элемента.
14. (a) b является R -наибольшим элементом B
тогда и только тогда, когда $b \in B$ и $\forall x \in B (xRb)$
тогда и только тогда, когда $b \in B$ и $\forall x \in B (bR^{-1}x)$
тогда и только тогда, когда b является R^{-1} -наименьшим элементом B .
(b) b является R -максимальным элементом B
тогда и только тогда, когда $b \in B$ и $\neg \exists x \in B (bRx \wedge b \neq x)$
тогда и только тогда, когда $b \in B$ и $\neg \exists x \in B (xR^{-1}b \wedge x \neq b)$
тогда и только тогда, когда b является R^{-1} -минимальным элементом B .
17. Нет. Пусть $A = \mathbb{R} \times \mathbb{R}$, и пусть $R = \{((x, y), (x', y)) \in A \times A \mid x \leq x' \text{ и } y \leq y'\}$. (Вы можете сравнить это с упражнением 8.) Пусть $B = \{(0, 0)\} \cup (\{1\} \times \mathbb{R})$. Самостоятельно убедитесь, что R является частичным порядком на A и что $(0, 0)$ – единственный минимальный элемент B , но это не наименьший элемент.
21. (a) Пусть $x \in U$ и xRy . Чтобы доказать, что $y \in U$, мы должны показать, что y является верхней гранью для B , поэтому предположим, что $b \in B$. Поскольку $x \in U$, x является верхней гранью для B , поэтому bRx . Но у нас также есть xRy , поэтому из транзитивности R мы можем заключить, что bRy . Поскольку b был произвольным элементом, это показывает, что y является верхней гранью B .
(b) Предположим, что $b \in B$. Чтобы доказать, что b – это нижняя граница для U , пусть x – произвольный элемент U . Тогда, по определению U , x является верхней границей для B , поэтому bRx . Поскольку x было произвольным элементом, это показывает, что b является нижней границей для U .
(c) Подсказка: предположим, что x – точная нижняя грань U . Сначала используйте часть (b), чтобы показать, что x является верхней гранью для B и, следовательно, $x \in U$. Затем используйте тот факт, что x является нижней гранью для U , чтобы показать, что x является наименьшим элементом U , другими словами, это наименьшая верхняя грань B .
24. (a) Предположим, что $(x, y) \in S$. Тогда либо $(x, y) \in R$, либо $(x, y) \in R^{-1}$. Если $(x, y) \in R$, то $(y, x) \in R^{-1}$, поэтому $(y, x) \in S$. Если $(x, y) \in R^{-1}$, то $(y, x) \in R$, поэтому $(y, x) \in S$. Следовательно, S симметрично. Поскольку $S = R \cup R^{-1}$, ясно, что $R \subseteq S$.

- (b) Предположим, что T – симметричное отношение на A и $R \subseteq T$. Чтобы показать, что $S \subseteq T$, пусть (x, y) – произвольный элемент из S . Тогда либо $(x, y) \in R$, либо $(x, y) \in R^{-1}$. Если $(x, y) \in R$, то, поскольку $R \subseteq T$, $(x, y) \in T$. Если $(x, y) \in R^{-1}$, то $(y, x) \in R$, и поэтому, с учетом $R \subseteq T$, $(y, x) \in T$. Но T симметрично, поэтому $(x, y) \in T$.
27. (a) Во-первых, обратите внимание, что $R_1 \subseteq R$ и $R_2 \subseteq R$. Из упражнения 26 следует, что $S_1 \subseteq S$ и $S_2 \subseteq S$, поэтому $S_1 \cup S_2 \subseteq S$. Для другого направления обратите внимание, что $R = R_1 \cup R_2 \subseteq S_1 \cup S_2$ и, согласно упражнению 13(b) раздела 4.3.1, $S_1 \cup S_2$ симметрично. Следовательно, согласно упражнению 24 (b), $S \subseteq S_1 \cup S_2$.
- (b) Повторяя первую половину доказательства в части (a), мы можем использовать упражнение 26, чтобы показать, что $T_1 \cup T_2 \subseteq T$. Однако ответ на упражнение 13(c) раздела 4.3.1 был отрицательным, поэтому мы не можем скопировать вторую половину доказательства. Фактически пример, приведенный в решении упражнения 13(c), работает как пример, для которого $T_1 \cup T_2 \neq T$.

Раздел 4.5

1. Вот список всех разбиений:

$\{\{1, 2, 3\}\}$
 $\{\{1, 2\}, \{3\}\}$
 $\{\{1, 3\}, \{2\}\}$
 $\{\{2, 3\}, \{1\}\}$
 $\{\{1\}, \{2\}, \{3\}\}$

3. (a) R является отношением эквивалентности. Всего существует 26 классов эквивалентности – по одному на каждую букву английского алфавита. Классы эквивалентности таковы: множество всех слов, начинающихся с «*a*», множество всех слов, начинающихся с «*b*», ..., множество всех слов, начинающихся с «*z*».
- (b) S не является отношением эквивалентности, потому что оно не транзитивно.
- (c) T является отношением эквивалентности. Классы эквивалентности таковы: множество всех однобуквенных слов, множество всех двухбуквенных слов и т. д. Для любого натурального числа n если существует хотя бы одно английское слово длины n , то множество всех слов длины n является классом эквивалентности.
6. Необходимо предположить, что для каждого дня d кто-то родился в этот день. Что может пойти не так, если, скажем, случайно 23 апреля никто не родился? Где в доказательстве используется это предположение?
10. Поскольку S – отношение эквивалентности, определяемое \mathcal{F} , доказательство теоремы 4.5.6 показывает, что $A/S = \mathcal{F} = A/R$. Искомый вывод следует теперь из упражнения 9.
13. См. лемму 7.3.4.

16. В соответствии с упражнением 16 (а) раздела 3.5 $\bigcup(\mathcal{F} \cup \mathcal{G}) = (\bigcup \mathcal{F}) \cup (\bigcup \mathcal{G}) = A \cup B$; мы видим, что $\mathcal{F} \cup \mathcal{G}$ попарно не пересекается. Предположим, что $X \in \mathcal{F} \cup \mathcal{G}$, $Y \in \mathcal{F} \cup \mathcal{G}$ и $X \cap Y \neq \emptyset$. Если $X \in \mathcal{F}$ и $Y \in \mathcal{G}$, то $X \subseteq A$ и $Y \subseteq B$, и поскольку A и B не пересекаются, то X и Y не пересекаются – получилось противоречие. Следовательно, не может быть такого, чтобы $X \in \mathcal{F}$ и $Y \in \mathcal{G}$, и аналогичный аргумент может использоваться для исключения возможности того, что $X \in \mathcal{G}$ и $Y \in \mathcal{F}$. Таким образом, X и Y оба являются либо элементами \mathcal{F} , либо элементами \mathcal{G} . Если они оба находятся в \mathcal{F} , то, поскольку \mathcal{F} попарно не пересекается, $X = Y$. Аналогичное рассуждение применимо, если они оба находятся в \mathcal{G} . Наконец, мы имеем $\forall X \in \mathcal{F}(X \neq \emptyset)$ и $\forall X \in \mathcal{G}(X \neq \emptyset)$, и из упражнения 8 раздела 2.2 следует, что $\forall X \in \mathcal{F} \cup \mathcal{G}(X \neq \emptyset)$.
20. (a) Вот доказательство транзитивности: предположим, что $(x, y) \in T$ и $(y, z) \in T$. Тогда, поскольку $T = R \cap S$, $(x, y) \in R$ и $(y, z) \in R$, так как R транзитивно, $(x, z) \in R$. Аналогично, $(x, z) \in S$, поэтому $(x, z) \in R \cap S = T$.
- (b) Предположим, что $x \in A$. Тогда для всех $y \in A$
- $$\begin{aligned} y \in [x]_T &\text{ тогда и только тогда, когда } (y, x) \in T \\ &\text{ тогда и только тогда, когда } (y, x) \in R \wedge (y, x) \in S \\ &\text{ тогда и только тогда, когда } y \in [x]_R \wedge y \in [x]_S \\ &\text{ тогда и только тогда, когда } y \in [x]_R \cap [x]_S. \end{aligned}$$
- (c) Предположим, что $X \in A/T$. Тогда, поскольку A/T является разбиением, $X \neq \emptyset$. Кроме того, для некоторого $x \in A$ $X = [x]_T = [x]_R \cap [x]_S$, так как $[x]_R \in A/R$ и $[x]_S \in A/S$, $X \in (A/R) \cdot (A/S)$. Теперь предположим, что $X \in (A/R) \cdot (A/S)$. Тогда для некоторых y и z из A справедливо $X = [y]_R \cap [z]_S$. Кроме того, $X \neq \emptyset$, поэтому мы можем выбрать некоторый $x \in X$. Следовательно, $x \in [y]_R$ и $x \in [z]_S$, и по части 2 леммы 4.5.5 следует, что $[x]_R = [y]_R$ и $[x]_S = [z]_S$. Следовательно, $X = [x]_R \cap [x]_S = [x]_T \in A/T$.
22. $\mathcal{F} \otimes \mathcal{F} = \{ \mathbb{R}^+ \times \mathbb{R}^+, \mathbb{R}^- \times \mathbb{R}^+, \mathbb{R}^- \times \mathbb{R}^-, \mathbb{R}^+ \times \mathbb{R}^-, \mathbb{R}^+ \times \{0\}, \mathbb{R}^- \times \{0\}, \{0\} \times \mathbb{R}^+, \{0\} \times \mathbb{R}^-, \{0, 0\} \}$. С геометрической точки зрения это четыре квадранта плоскости, положительная и отрицательная оси x , положительная и отрицательная оси y и начало координат.
24. (a) Подсказка: пусть $T = \{(X, Y) \in A/S \times A/S \mid \exists x \in X \exists y \in Y(xRy)\}$.
- (b) Предположим, что $x, y, x', y' \in A$, xSy' , и ySy' . Тогда $[x]_S = [x']_S$ и $[y]_S = [y']_S$, поэтому xRy , если и только если $[x]_S T [y]_S$, если и только если $[x']_S T [y']_S$, если $x'Ry'$.

Решения к главе 5

Раздел 5.1

1. (a) Да.
(b) Нет.
(c) Да.

3. (a) $f(a) = b, f(b) = b, f(c) = a$.
 (b) $f(2) = 0$.
 (c) $f(\pi) = 3$ и $f(-\pi) = -4$.
5. $L \circ H: N \rightarrow N$, и для любого $n \in N$ справедливо $(L \circ H)(n) = n$. Следовательно, $L \circ H = i_N$, $H \circ L: C \rightarrow C$, и для любого $c \in C$ выполняется $(H \circ L)(c) =$ столица страны, в которой находится c .
7. (a) Предположим, что $c \in C$. Мы должны доказать, что существует единственный элемент $b \in B$ такой, что $(c, b) \in f \upharpoonright C$.
 Существование: пусть $b = f(c) \in B$. Тогда $(c, b) \in f$ и $(c, b) \in C \times B$, и, следовательно, $(c, b) \in f \cap (C \times B) = f \upharpoonright C$.
 Единственность: предположим, что $(c, b_1) \in f \upharpoonright C$ и $(c, b_2) \in f \upharpoonright C$. Тогда $(c, b_1) \in f$ и $(c, b_2) \in f$, поэтому, поскольку f – функция, $b_1 = b_2$.
 Это доказывает, что $f \upharpoonright C$ является функцией от C до B . Наконец, чтобы вывести формулу для $(f \upharpoonright C)(c)$, предположим, что $c \in C$, и пусть $b = f(c)$. В части доказательства, относящегося к существованию, мы показали, что $(c, b) \in f \upharpoonright C$. Отсюда следует, что $f(c) = b = (f \upharpoonright C)(c)$.
 (b) (\rightarrow) Предположим, что $g = f \upharpoonright C$. Тогда $g = f \cap (C \times B)$, поэтому очевидно, что $g \subseteq f$.
 (\leftarrow) Предположим, что $g \subseteq f$. Предположим, что $c \in C$, и пусть $b = g(c)$. Тогда $(c, b) \in g$, поэтому $(c, b) \in f$, и, следовательно, $f(c) = b$. Но тогда согласно части (a) $(f \upharpoonright C)(c) = f(c) = b = g(c)$. Поскольку c произвольно, из теоремы 5.1.4 следует, что $g = f \upharpoonright C$.
 (c) $h \upharpoonright Z = h \cap (\mathbb{Z} \times \mathbb{R}) = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y = 2x + 3\} \cap (\mathbb{Z} \times \mathbb{R}) = \{(x, y) \in \mathbb{Z} \times \mathbb{R} \mid y = 2x + 3\} = g$.
10. Поскольку $f \neq g$, согласно теореме 5.1.4 мы можем выбрать такой элемент $a \in A$, что $f(a) \neq g(a)$. Следовательно, $(a, f(a)) \in f$ и $(a, f(a)) \notin g$, поэтому по определению симметричной разности $(a, f(a)) \in f \Delta g$, и аналогично $(a, g(a)) \in f \Delta g$. Поскольку $f(a) \neq g(a)$, $f \Delta g$ не является функцией.
13. (a) Пусть $b \in B$. Поскольку $\text{Dom}(S) = B$, мы знаем, что существует некоторый элемент $c \in C$ такой, что $(b, c) \in S$. Чтобы убедиться в его единственности, предположим, что $c' \in C$ и $(b, c') \in S$. Так как $\text{Ran}(R) = B$, мы можем выбрать такой элемент $a \in A$, что $(a, b) \in R$. Но тогда $(a, c) \in S \circ R$ и $(a, c') \in S \circ R$, и поскольку $S \circ R$ – функция, то $c = c'$.
 (b) $A = \{1\}, B = \{2, 3\}, C = \{4\}, R = \{(1, 2), (1, 3)\}, S = \{(2, 4), (3, 4)\}$.
15. (a) Нет. Пример: $A = \{1\}, B = \{2, 3\}, f = \{(1, 2)\}, R = \{(1, 1)\}$.
 (b) Да. Предположим, что R симметрично. Пусть $(x, y) \in S$. Тогда мы можем выбрать некоторые элементы u и v в множестве A такие, что $f(u) = x, f(v) = y$ и $(u, v) \in R$. Так как R симметрично, $(v, u) \in R$ и, следовательно, $(y, x) \in S$.
 (c) Нет. Пример: $A = \{1, 2, 3, 4\}, B = \{5, 6, 7\}, f = \{(1, 5), (2, 6), (3, 6), (4, 7)\}, R = \{(1, 2), (3, 4)\}$.
19. (a) Пусть $a = 3$ и $c = 8$. Тогда для любого $x > a = 3$, $|f(x)| = |7x + 3| = 7x + 3 < 7x + x = 8x < 8x^2 = c|g(x)|$.
 Это показывает, что $f \in O(g)$.

Предположим теперь, что $g \in O(f)$. Тогда мы можем выбрать $a \in \mathbb{Z}^+$ и $c \in \mathbb{R}^+$ так, что $\forall x > a (|g(x)| \leq c|f(x)|)$, или, другими словами, $\forall x > a (x^2 \leq c(7x + 3))$. Пусть x будет любым натуральным числом, большим, чем a и $10c$. Умножая обе части неравенства $x > 10c$ на x , можно заключить, что $x^2 > 10cx$. Но поскольку $x > a$, мы также имеем $x^2 \leq c(7x + 3) \leq c(7x + 3x) = 10cx$, поэтому мы пришли к противоречию. Следовательно, $g \notin O(f)$.

- (b) Ясно, что для любой функции $f \in \mathcal{F}$ выполняется $\forall x \in \mathbb{Z}^+ (|f(x)| \leq 1 \cdot |f(x)|)$, поэтому $f \in O(f)$ и, следовательно, $(f, f) \in S$. Таким образом, S рефлексивно. Чтобы увидеть, что оно также транзитивно, предположим, что $(f, g) \in S$ и $(g, h) \in S$. Тогда существуют натуральные числа a_1 и a_2 и положительные действительные числа c_1 и c_2 такие, что $\forall x > a_1 (|f(x)| \leq c_1 |g(x)|)$ и $\forall x > a_2 (|g(x)| \leq c_2 |h(x)|)$. Пусть a – максимум из a_1 и a_2 , и пусть $c = c_1 c_2$. Тогда для всех $x > a$ выполняется

$$|f(x)| \leq c_1 |g(x)| \leq c_1 c_2 |h(x)| = c |h(x)|.$$

Таким образом, $(f, h) \in S$, значит, S транзитивно. Наконец, чтобы убедиться, что S не является частичным порядком, мы покажем, что оно не антисимметрично. Пусть f и g – функции от \mathbb{Z}^+ до \mathbb{R} , определенные формулами $f(x) = x$ и $g(x) = 2x$. Тогда для всех $x \in \mathbb{Z}^+ |f(x)| \leq |g(x)|$ и $|g(x)| \leq 2|f(x)|$, поэтому $f \in O(g)$, а также $g \in O(f)$. Следовательно, $(f, g) \in S$ и $(g, f) \in S$, но $f \neq g$.

- (c) Поскольку $f_1 \in O(g)$, мы можем выбрать $a_1 \in \mathbb{Z}^+$ и $c_1 \in \mathbb{R}^+$ так, что $\forall x > a_1 (|f_1(x)| \leq c_1 |g(x)|)$. Аналогично, поскольку $f_2 \in O(g)$, мы можем выбрать $a_2 \in \mathbb{Z}^+$ и $c_2 \in \mathbb{R}^+$ так, чтобы $\forall x > a_2 (|f_2(x)| \leq c_2 |g(x)|)$. Пусть a будет максимумом из a_1 и a_2 , и пусть $c = |s|c_1 + |t|c_2 + 1$. (Мы добавили 1 здесь, просто чтобы убедиться, что c положительно, как требуется в определении O .) Тогда для всех $x > a$

$$\begin{aligned} |f(x)| &= |sf_1(x) + tf_2(x)| \leq |s||f_1(x)| + |t||f_2(x)| \leq |s|c_1 |g(x)| + |t|c_2 |g(x)| \\ &= (|s|c_1 + |t|c_2) |g(x)| \leq c |g(x)|. \end{aligned}$$

Следовательно, $f \in O(g)$.

21. (a) Подсказка: пусть $h = \{(X, y) \in A/R \times B \mid \exists x \in X (f(x) = y)\}$.
(b) Подсказка: используйте тот факт, что для всех x и y в A если xRy , то $[x]_R = [y]_R$.

Раздел 5.2

2. (a) f не является функцией.
(b) f не является функцией. g – это функция, которая сюръективна, но не взаимно однозначна.
(c) R взаимно однозначна и сюръективна.
5. (a) Предположим, что $x_1 \in A$, $x_2 \in A$ и $f(x_1) = f(x_2)$. Затем мы можем выполнить следующие алгебраические шаги:

$$\begin{aligned}\frac{x_1 + 1}{x_1 - 1} &= \frac{x_2 + 1}{x_2 - 1}, \\ (x_1 + 1)(x_2 - 1) &= (x_2 + 1)(x_1 - 1), \\ x_1 x_2 - x_1 + x_2 - 1 &= x_1 x_2 - x_2 + x_1 - 1, \\ 2x_2 &= 2x_1, \\ x_2 &= x_1.\end{aligned}$$

Эти выкладки показывают, что f взаимно однозначна.

Чтобы показать, что f сюръективна, предположим, что $y \in A$. Пусть

$$x = \frac{y+1}{y-1}.$$

Обратите внимание, что эта дробь определена, поскольку $y \neq 1$, а также, очевидно, $x \neq 1$, поэтому $x \in A$. Тогда

$$f(x) = \frac{x+1}{x-1} = \frac{\frac{y+1}{y-1} + 1}{\frac{y+1}{y-1} - 1} = \frac{\frac{2y}{y-1}}{\frac{2}{y-1}} = y.$$

(b) Для любого $x \in A$

$$(f \circ f)(x) = \frac{\frac{x+1}{x-1} + 1}{\frac{x+1}{x-1} - 1} = \frac{\frac{2x}{x-1}}{\frac{2}{x-1}} = x = i_A(x).$$

9. (a) $\{1, 2, 3, 4\}$.
 (b) f сюръективна, но не взаимно однозначна.
13. (a) Предположим, что f взаимно однозначна. Предположим, что $c_1 \in C$, $c_2 \in C$ и $(f \upharpoonright C)(c_1) = (f \upharpoonright C)(c_2)$. Из упражнения 7(а) раздела 5.1 следует, что $f(c_1) = f(c_2)$, поэтому, поскольку f взаимно однозначна, $c_1 = c_2$.
 (b) Пусть $f \upharpoonright C$ сюръективна. Пусть $b \in B$. Тогда, поскольку $f \upharpoonright C$ сюръективна, мы можем выбрать некоторый элемент $c \in C$ такой, что $(f \upharpoonright C)(c) = b$. Но тогда $c \in A$, и согласно упражнению 7(а) раздела 5.1.1 $f(c) = b$.
 (c) Пусть $A = B = \mathbb{R}$ и $C = \mathbb{R}^+$. Для (a) используйте $f(x) = |x|$, а для (b) используйте $f(x) = x$.
17. (a) Предположим, что R рефлексивно, а функция f сюръективна. Пусть $x \in B$ произвольно. Поскольку f сюръективна, мы можем выбрать некоторый элемент $u \in A$ такой, что $f(u) = x$.
 Так как R рефлексивно, то $(u, u) \in R$. Следовательно, $(x, x) \in S$.
 (b) Предположим, что R транзитивно, а f взаимно однозначна. Предположим, что $(x, y) \in S$ и $(y, z) \in S$. Поскольку $(x, y) \in S$, мы можем выбрать

некоторые u и v в A такие, что $f(u) = x$, $f(v) = y$ и $(u, v) \in R$. Аналогично, поскольку $(y, z) \in S$, мы можем выбрать p и q в A так, что $f(p) = y$, $f(q) = z$ и $(p, q) \in R$. Поскольку $f(v) = y = f(p)$ и f взаимно однозначна, то $v = p$. Следовательно, $(v, q) = (p, q) \in R$. Так как у нас также есть $(u, v) \in R$, из транзитивности R следует, что $(u, q) \in R$, поэтому $(x, z) \in S$.

20. (a) Возьмем произвольный элемент $b \in B$. Поскольку f сюръективна, мы можем выбрать некоторый элемент $a \in A$ такой, что $f(a) = b$. Следовательно, $g(b) = (g \circ f)(a) = (h \circ f)(a) = h(b)$. Поскольку элемент b был произвольным, это показывает, что $\forall b \in B(g(b) = h(b))$, поэтому $g = h$.
- (b) Пусть c_1 и c_2 – два различных элемента C . Пусть $b \in B$. Пусть g и h – функции от B к C такие, что $\forall x \in B(g(x) = c_1)$, $\forall x \in B \setminus \{b\}(h(x) = c_1)$ и $h(b) = c_2$. (Формально $g = B \times \{c_1\}$ и $h = [(B \setminus \{b\}) \times \{c_1\}] \cup \{(b, c_2)\}$.) Тогда $g \neq h$, поэтому по предположению $g \circ f \neq h \circ f$, поэтому мы можем выбрать $a \in A$ такой, что $g(f(a)) \neq h(f(a))$. Но, кстати, g и h были определены, единственный $x \in B$, для которого $g(x) \neq h(x)$ – это $x = b$, откуда следует, что $f(a) = b$. Поскольку b было произвольным, это показывает, что f сюръективна.

Раздел 5.3

1. $R^{-1}(p) = \text{человек, сидящий сразу справа от } p$.
3. Пусть $g(x) = (3x - 5)/2$. Тогда для любого $x \in \mathbb{R}$

$$f(g(x)) = \frac{\frac{2(3x - 5)}{3} + 5}{3} = \frac{3x - 5 + 5}{3} = \frac{3x}{3} = x$$

и

$$g(f(x)) = \frac{\frac{3(2x + 5)}{2} - 5}{2} = \frac{2x + 5 - 5}{2} = \frac{2x}{2} = x.$$

Следовательно, $f \circ g = i_{\mathbb{R}}$ и $g \circ f = i_{\mathbb{R}}$, и по теоремам 5.3.4 и 5.3.5 из этого следует, что f взаимно однозначна и сюръективна и $f^{-1} = g$.

5. $f^{-1}(x) = 2 - \log x$.
9. Предположим, что $f: A \rightarrow B$, $g: B \rightarrow A$ и $f \circ g = i_B$. Пусть b – произвольный элемент B . Пусть $a = g(b) \in A$. Тогда $f(a) = f(g(b)) = (f \circ g)(b) = i_B(b) = b$. Поскольку b было произвольным, это означает, что f сюръективна.
11. (a) Предположим, что функция f взаимно однозначна и $f \circ g = i_B$. Согласно части 2 теоремы 5.3.3, f также сюръективна, поэтому $f^{-1}: B \rightarrow A$ и $f^{-1} \circ f = i_A$. Это дает нам достаточно информации, чтобы повторить рассуждения в доказательстве теоремы 5.3.5:

$$g = i_A \circ g = (f^{-1} \circ f) \circ g = f^{-1} \circ (f \circ g) = f^{-1} \circ i_B = f^{-1}.$$

- (b) Подсказка: повторите решение части (а).
 (c) Совет: используйте части (а) и (b) вместе с теоремой 5.3.3.
14. (a) Предположим, что $x \in A' = \text{Ran}(g)$. Тогда мы можем выбрать некоторый $b \in B$ такой, что $g(b) = x$. Следовательно, $(g \circ f)(x) = g(f(g(b))) = g((f \circ g)(b)) = g(i_B(b)) = g(b) = x$.
- (b) Согласно данной информации $(f \upharpoonright A') \circ g = i_B$, а согласно части (а), $g \circ (f \upharpoonright A') = i_{A'}$. Следовательно, по теореме 5.3.4 $f \upharpoonright A'$ является взаимно однозначной сюръективной функцией от A' к B , а по теореме 5.3.5 $g = (f \upharpoonright A')^{-1}$.
16. Подсказка: предположим, что $x \in \mathbb{R}$. Чтобы определить, правда ли $x \in \text{Ran}(f)$, посмотрите, сможете ли вы найти действительное число y такое, что $f(y) = x$. Другими словами, вы должны попытаться решить уравнение $4y - y^2 = x$ относительно y через x . Обратите внимание, что это похоже на метод, который мы использовали в части 1 примера 5.3.6. Однако в этом случае вы обнаружите, что для некоторых значений x нет решения для y , а для некоторых значений x существует более одного решения для y .
18. Поскольку функция g взаимно однозначна и сюръективна, $g^{-1}: C \rightarrow B$. Пусть $h = g^{-1} \circ f$. Тогда $h: A \rightarrow B$ и

$$\begin{aligned} g \circ h &= g \circ (g^{-1} \circ f) \\ &= (g \circ g^{-1}) \circ f && (\text{теорема 4.2.5}) \\ &= i_C \circ f && (\text{теорема 5.3.2}) \\ &= f && (\text{упражнение 9 из раздела 4.3.1}). \end{aligned}$$

Раздел 5.4

1. (a) Нет.
 (b) Да.
 (c) Да.
 (d) Нет.
3. $\{-1, 0, 1, 2\}$.
7. Предположим, что $C \subseteq A$ и C замкнуто относительно f . Предположим, что $x \in A \setminus C$, поэтому $x \in A$ и $x \notin C$. Тогда $f^{-1}(x) \in A$. Предположим, что $f^{-1}(x) \in C$. Тогда, поскольку C замкнуто относительно f , $x = f(f^{-1}(x)) \in C$; получили противоречие. Следовательно, $f^{-1}(x) \notin C$, поэтому $f^{-1}(x) \in A \setminus C$. Так как x был произвольным элементом из $A \setminus C$, это показывает, что $A \setminus C$ замкнуто относительно f^{-1} .
9. (a) Предположим, что $x \in C_1 \cup C_2$. Тогда либо $x \in C_1$, либо $x \in C_2$.
 Случай 1. $x \in C_1$. Тогда поскольку C_1 замкнуто относительно f , то $f(x) \in C_1$, поэтому $f(x) \in C_1 \cup C_2$.
 Случай 2. $x \in C_2$. Тогда поскольку C_2 замкнуто относительно f , то $f(x) \in C_2$, поэтому $f(x) \in C_1 \cup C_2$.
 Следовательно, $f(x) \in C_1 \cup C_2$. Поскольку x было произвольным, мы можем заключить, что $C_1 \cup C_2$ замкнуто относительно f .

- (b) Да. Доказательство. Предположим, что $x \in C_1 \cap C_2$. Тогда $x \in C_1$ и $x \in C_2$. Поскольку $x \in C_1$ и C_1 замкнуто относительно f , то $f(x) \in C_1$. Аналогично $f(x) \in C_2$. Следовательно, $f(x) \in C_1 \cap C_2$, так что, поскольку x произвольно, $C_1 \cap C_2$ замкнуто относительно f .
- (c) Нет. Вот контрпример: $A = \{1, 2\}$, $f = \{(1, 2), (2, 2)\}$, $C_1 = \{1, 2\}$, $C_2 = \{2\}$.
12. (a) \mathbb{Z} .
(b) $\{X \subseteq \mathbb{N} \mid X$ конечно $\}$.
14. \mathbb{Z} .
17. (a) Да.
(b) Да.
(c) Да.
(d) Нет. (Композиция двух строго убывающих функций строго возрастает.)
20. (b) и (e) замкнуты относительно f .

Решения к главе 6

Раздел 6.1

1. Базовый случай: когда $n = 0$, обе части уравнения равны 0.

Шаг индукции: предположим, что $n \in \mathbb{N}$ и $0 + 1 + 2 + \dots + n = n(n + 1)/2$. Отсюда

$$\begin{aligned} 0 + 1 + 2 + \dots + (n + 1) &= (0 + 1 + 2 + \dots + n) + (n + 1) \\ &= \frac{n(n + 1)}{2} + (n + 1) \\ &= (n + 1) \left(\frac{n}{2} + 1 \right) = \frac{(n + 1)(n + 2)}{2}, \end{aligned}$$

что и требовалось доказать.

3. Базовый случай: когда $n = 0$, обе части уравнения равны 0.

Шаг индукции: предположим, что $n \in \mathbb{N}$ и $0^3 + 1^3 + 2^3 + \dots + n^3 = [n(n + 1)/2]^2$. Отсюда

$$\begin{aligned} 0^3 + 1^3 + 2^3 + \dots + (n + 1)^3 &= (0^3 + 1^3 + 2^3 + \dots + n^3) + (n + 1)^3 \\ &= \left[\frac{n(n + 1)}{2} \right]^2 + (n + 1)^3 \\ &= (n + 1)^2 \left[\frac{n^2}{4} + n + 1 \right] \\ &= (n + 1)^2 \cdot \frac{n^2 + 4n + 4}{4} \\ &= \left[\frac{(n + 1)(n + 2)}{2} \right]^2. \end{aligned}$$

7. Подсказка: формула $(3^{n+1} - 1)/2$.
10. Базовый случай: когда $n = 0$, $9^n - 8n - 1 = 0 = 64 \cdot 0$, поэтому $64 | (9^n - 8n - 1)$.

Шаг индукции. Предположим, что $n \in \mathbb{N}$ и $64 | (9^n - 8n - 1)$. Тогда существует такое целое число k , что $9^n - 8n - 1 = 64k$. Следовательно:

$$\begin{aligned} 9^{n+1} - 8(n+1) - 1 &= 9^{n+1} - 8n - 9 \\ &= 9^{n+1} - 72n - 9 + 64n \\ &= 9(9^n - 8n - 1) + 64n \\ &= 9(64k) + 64n \\ &= 64(9k + n), \end{aligned}$$

поэтому $64 | (9^{n+1} - 8(n+1) - 1)$.

12. (a) Базовый случай: когда $n = 0$, $7^n - 5^n = 0 = 2 \cdot 0$, поэтому $7^n - 5^n$ четно.
- Шаг индукции: предположим, что $n \in \mathbb{N}$ и $7^n - 5^n$ четно. Тогда существует такое целое число k , что $7^n - 5^n = 2k$. Следовательно:

$$\begin{aligned} 7^{n+1} - 5^{n+1} &= 7 \cdot 7^n - 5 \cdot 5^n = 2 \cdot 7^n + 5 \cdot (7^n - 5^n) \\ &= 2 \cdot 7^n + 5 \cdot 2k = 2(7^n + 5k), \end{aligned}$$

поэтому $7^{n+1} - 5^{n+1}$ четно.

- (b) Для шага индукции вам может оказаться полезным заполнить следующее уравнение: $2 \cdot 7^{n+1} - 3 \cdot 5^{n+1} + 1 = 2 \cdot 7^n - 3 \cdot 5^n + 1 + ?$.
15. Базовый случай: когда $n = 10$, $2^n = 1024 > 1000 = n^3$.

Шаг индукции: предположим, что $n \geq 10$ и $2^n > n^3$. Далее

$$\begin{aligned} 2^{n+1} &= 2 \cdot 2^n \\ &> 2n^3 && \text{(предположение индукции)} \\ &= n^3 + n^3 \\ &\geq n^3 + 10n^2 && \text{(поскольку } n \geq 10\text{)} \\ &= n^3 + 3n^2 + 7n^2 \\ &\geq n^3 + 3n^2 + 70n && \text{(поскольку } n \geq 10\text{)} \\ &= n^3 + 3n^2 + 3n + 67n \\ &> n^3 + 3n^2 + 3n + 1 = (n+1)^3. \end{aligned}$$

20. (a) Базовый случай: когда $n = 1$, доказываемое утверждение: $0 < a < b$, как и было дано.

Шаг индукции: предположим, что $n \geq 1$ и $0 < a^n < b^n$. Умножая это неравенство на положительное число a , получаем $0 < a^{n+1} < ab^n$, а умножение неравенства $a < b$ на положительное число b^n дает $ab^n < b^{n+1}$. Комбинируя эти неравенства, можно заключить, что $0 < a^{n+1} < b^{n+1}$.

- (b) Подсказка: сначала обратите внимание, что $\sqrt[n]{a}$ и $\sqrt[n]{b}$ положительны. (Для нечетных n это следует из упражнения 19. Для четных n каждый из a и b имеет два корня n -й степени, один положительный и один отрицательный, но $\sqrt[n]{a}$ и $\sqrt[n]{b}$ – по определению положительные корни.) Теперь воспользуйтесь доказательством от противного и примените часть (a).

- (c) Подсказка: доказываемое неравенство можно переформулировать так: $a^{n+1} - ab^n - ba^n + b^{n+1} > 0$. Теперь разложите на множители левую часть этого неравенства.
- (d) Совет: используйте математическую индукцию. Для базового случая используйте случай $n = 1$ из части (c). Для шага индукции умножьте обе части предположения индукции на $(a + b)/2$, а затем примените часть (c).

Раздел 6.2

1. (a) Мы должны доказать, что R' рефлексивно (на A'), транзитивно и антисимметрично. Для первого предположим, что $x \in A'$. Поскольку R рефлексивно (на A) и $x \in A$, то $(x, x) \in R$, следовательно, $(x, x) \in R \cap (A' \times A') = R'$. Это доказывает, что R' рефлексивно.
- Далее предположим, что $(x, y) \in R'$ и $(y, z) \in R'$. Тогда $(x, y) \in R$, $(y, z) \in R$ и $x, y, z \in A'$. Поскольку R транзитивно, $(x, z) \in R$, поэтому $(x, z) \in R \cap (A' \times A') = R'$. Следовательно, R' транзитивно.
- Наконец, предположим, что $(x, y) \in R'$ и $(y, x) \in R'$. Тогда $(x, y) \in R$ и $(y, x) \in R$, и так как R антисимметрично, $x = y$. Таким образом, R' антисимметрично.
- (b) Чтобы убедиться, что T рефлексивно, предположим, что $x \in A$. Если $x = a$, то $(x, x) = (a, a) \in \{a\} \times A \subseteq T$. Если $x \neq a$, то $x \in A'$ и, поскольку R' рефлексивно, $(x, x) \in R' \subseteq T' \subseteq T$.
- Для транзитивности предположим, что $(x, y) \in T$ и $(y, z) \in T$. Если $x = a$, то $(x, z) = (a, z) \in \{a\} \times A \subseteq T$. Теперь предположим, что $x \neq a$. Тогда $(x, y) \notin \{a\} \times A$, поэтому, поскольку $(x, y) \in T = T' \cup (\{a\} \times A)$, мы должны иметь $(x, y) \in T'$. Но $T' \subseteq A' \times A'$, поэтому $y \in A'$ и, следовательно, $y \neq a$. Аналогичные рассуждения теперь показывают, что $(y, z) \in T$. Поскольку T' транзитивно, то $(x, z) \in T' \subseteq T$.
- Чтобы показать, что T антисимметрично, предположим, что $(x, y) \in T$ и $(y, x) \in T$. Если $x = a$, то $(y, x) \notin T'$, поэтому $(y, x) \in \{a\} \times A$ и поэтому $y = a = x$. Аналогично, если $y = a$, то $x = y$. Теперь предположим, что $x \neq a$ и $y \neq a$. Тогда, как и в доказательстве транзитивности, следует, что $(x, y) \in T'$ и $(y, x) \in T$, поэтому в силу антисимметрии $T' x = y$.
- Теперь мы знаем, что T – частичный порядок. Чтобы убедиться, что он полный, предположим, что $x \in A$ и $y \in A$. Если $x = a$, то $(x, y) \in \{a\} \times A \subseteq T$. Аналогично, если $y = a$, то $(y, x) \in T$. Теперь предположим, что $x \neq a$ и $y \neq a$. Тогда $x \in A'$ и $y \in A'$, поэтому, поскольку T' является полным порядком, либо $(x, y) \in T' \subseteq T$, либо $(y, x) \in T' \subseteq T$.
- Наконец, чтобы убедиться, что $R \subseteq T$, предположим, что $(x, y) \in R$. Если $x = a$, то $(x, y) \in \{a\} \times A \subseteq T$. Теперь предположим, что $x \neq a$. Если $y = a$, то тот факт, что $(x, y) \in R$, противоречил бы R -минимальности a . Следовательно, $y \neq a$. Но тогда $(x, y) \in R \cap (A' \times A') = R' \subseteq T' \subseteq T$.
4. (a) Докажем утверждение: $\forall n \geq 1 \forall B \subseteq A [B \text{ имеет } n \text{ элементов} \rightarrow \exists x \in B \forall y \in B ((x, y) \in R \circ R)]$. Продолжим индукцией по n .

Базовый случай: предположим, что $n = 1$. Если $B \subseteq A$ и B имеет один элемент, то для некоторого $x \in B$ справедливо $B = \{x\}$. Поскольку R рефлексивно, $(x, x) \in R$ и, следовательно, $(x, x) \in R \circ R$. Но x – единственный элемент в B , поэтому $\forall y \in B ((x, y) \in R \circ R)$, что и требовалось доказать.

Шаг индукции: предположим, что $n \geq 1$ и для любого $B \subseteq A$, и если B имеет n элементов, то $\exists x \in B \forall y \in B ((x, y) \in R \circ R)$. Теперь предположим, что $B \subseteq A$ и B имеет $n + 1$ элементов. Выберем некоторый элемент $b \in B$, и пусть $B' = B \setminus \{b\}$. Тогда $B' \subseteq A$ и B' имеет n элементов, поэтому по предположению индукции существует некоторый $x \in B'$ такой, что $\forall y \in B' ((x, y) \in R \circ R)$. Теперь рассмотрим два случая.

Случай 1: $(x, b) \in R \circ R$. Тогда $\forall y \in B ((x, y) \in R \circ R)$, и доказательство завершено.

Случай 2: $(x, b) \notin R \circ R$. В этом случае мы докажем, что $\forall y \in B ((b, y) \in R \circ R)$. Для этого возьмем произвольный элемент $y \in B$. Если $y = b$, то, поскольку R рефлексивно, $(b, b) \in R$ и, следовательно, $(b, y) = (b, b) \in R \circ R$. Теперь предположим, что $y \neq b$. Тогда $y \in B'$, поэтому, исходя из выбора x , мы знаем, что $(x, y) \in R \circ R$. Это означает, что для некоторого $z \in A$ истинно $(x, z) \in R$ и $(z, y) \in R$. Мы имеем $(x, z) \in R$, поэтому если $(z, b) \in R$, то $(x, b) \in R \circ R$ вопреки предположению для этого случая. Следовательно, $(z, b) \notin R$, поэтому, согласно предположению о R , $(b, z) \in R$. Но тогда, поскольку $(b, z) \in R$ и $(z, y) \in R$, имеем $(b, y) \in R \circ R$, что и требовалось доказать.

- (b) Подсказка: пусть $A = B$ = множество участников, и пусть $R = \{(x, y) \in A \times A \mid x \text{ побеждает } y\} \cup i_A$. Теперь примените часть (a).
- 8. (a) Пусть $m = (a + b)/2$, среднее арифметическое значений a и b , и пусть $d = (a - b)/2$. Тогда легко проверить, что $m + d = a$ и $m - d = b$, поэтому

$$\sqrt{ab} = \sqrt{(m+d)(m-d)} = \sqrt{m^2 - d^2} \leq \sqrt{m^2} = m = \frac{a+b}{2}.$$

- (b) Воспользуемся индукцией по n .

Базовый случай: $n = 1$. Этот случай рассматривается в части (a).

Шаг индукции: предположим, что $n \geq 1$, и неравенство среднего арифметического и среднего геометрического выполняется для списков длины 2^n . Пусть теперь $a_1, a_2, \dots, a_{2^{n+1}}$ – список из $2n + 1$ положительных действительных чисел. Примем:

$$m_1 = \frac{a_1 + a_2 + \dots + a_{2^n}}{2^n}, \quad m_2 = \frac{a_{2^n+1} + a_{2^n+2} + \dots + a_{2^{n+1}}}{2^n}.$$

Обратите внимание, что $a_1 + a_2 + \dots + a_{2^n} = m_1 2^n$, и аналогично $a_{2^n+1} + a_{2^n+2} + \dots + a_{2^{n+1}} = m_2 2^n$. Кроме того, по индуктивному предположению мы знаем, что $m_1 \geq \sqrt[2^n]{a_1 a_2 \dots a_{2^n}}$ и $m_2 \geq \sqrt[2^n]{a_{2^n+1} a_{2^n+2} \dots a_{2^{n+1}}}$. Следовательно:

$$\begin{aligned}\frac{a_1 + a_2 + \dots + a_{2^{n+1}}}{2^{n+1}} &= \frac{m_1 2^n + m_2 2^n}{2^{n+1}} = \frac{m_1 + m_2}{2} \geq \sqrt{m_1 m_2} \\ &\geq \sqrt[2^n]{a_1 a_2 \cdots a_{2^n}} \sqrt[2^n]{a_{2^n+1} a_{2^n+2} \cdots a_{2^{n+1}}} \\ &= \sqrt[2^{n+1}]{a_1 a_2 \cdots a_{2^{n+1}}}.\end{aligned}$$

(c) Воспользуемся индукцией по n .

Базовый случай: если $n = n_0$, то по предположению неравенство среднего арифметического и среднего геометрического не выполняется для некоторого списка длины n .

Шаг индукции: предположим, что $n \geq n_0$, и существуют положительные действительные числа a_1, a_2, \dots, a_n такие, что

$$\frac{a_1 + a_2 + \dots + a_n}{n} < \sqrt[n]{a_1 a_2 \cdots a_n}.$$

Пусть $m = (a_1 + a_2 + \dots + a_n)/n$, и пусть $a_{n+1} = m$. Тогда имеем $m < \sqrt[n]{a_1 a_2 \cdots a_n}$, поэтому $m^n < a_1 a_2 \cdots a_n$. Умножение обеих частей этого неравенства на m дает $m^{n+1} < a_1 a_2 \cdots a_n m = a_1 a_2 \cdots a_{n+1}$, поэтому $m < \sqrt[n+1]{a_1 a_2 \cdots a_{n+1}}$. Но обратите внимание, что у нас также есть $mn = a_1 + a_2 + \dots + a_n$, так что

$$\frac{a_1 + \dots + a_{n+1}}{n+1} = \frac{mn + m}{n+1} = \frac{m(n+1)}{n+1} = m < \sqrt[n+1]{a_1 a_2 \cdots a_{n+1}}.$$

Таким образом, у нас есть список длины $n+1$, для которого не выполняется неравенство среднего арифметического и среднего геометрического.

(d) Предположим, что неравенство среднего арифметического и среднего геометрического не выполняется для некоторого списка положительных действительных чисел. Пусть n_0 будет длиной этого списка. Выберите целое число $n \geq 1$ такое, что $n_0 \leq 2^n$. (Фактически мы могли бы просто принять $n = n_0$, как вы покажете в упражнении 12(a) в разделе 6.3.1.) Тогда, согласно части (b), неравенство среднего арифметического и среднего геометрического выполняется для всех списков длины 2^n , но по части (c) оно не должно выполняться для некоторого списка длиной 2^n . Это противоречие, поэтому неравенство должно выполняться всегда.

10. (a) Подсказка: покажите, что $(a_1 b_1 + a_2 b_2) - (a_1 b_2 + a_2 b_1) \geq 0$.
- (b) Используйте индукцию по n . Для шага индукции предположим, что результат верен для последовательностей длины n , и предположим, что $a_1 \leq a_2 \leq \dots \leq a_n \leq a_{n+1}$, $b_1 \leq b_2 \leq \dots \leq b_n \leq b_{n+1}$ и f является взаимно однозначной сюръективной функцией от $\{1, 2, \dots, n+1\}$ на себя. Теперь рассмотрим два случая. Для случая 1 предположим, что $f(n+1) = n+1$, и воспользуемся предположением индукции, чтобы завершить доказательство. Для случая 2 предположим, что $f(n+1) <$

$n + 1$. Найдем взаимно однозначную сюръективную функцию g от $\{1, 2, \dots, n + 1\}$ на себя такую, что g почти то же самое, что и f , но $g(n + 1) = n + 1$, и покажем, что

$$a_1 b_{f(1)} + \dots + a_{n+1} b_{f(n+1)} \leq a_1 b_{g(1)} + \dots + a_{n+1} b_{g(n+1)} \leq a_1 b_1 + \dots + a_{n+1} b_{n+1}.$$

11. Выполним индукцию по n .

Базовый случай: $n = 0$. Если A имеет 0 элементов, то $A = \emptyset$, поэтому $\mathcal{P}(A) = \{\emptyset\}$, которое имеет $1 = 2^0$ элементов.

Шаг индукции: предположим, что для каждого множества A с n элементами $\mathcal{P}(A)$ имеет 2^n элементов. Теперь предположим, что A имеет $n + 1$ элементов. Пусть a – произвольный элемент из A , и пусть $A' = A \setminus \{a\}$. Тогда A' имеет n элементов, поэтому по предположению индукции $\mathcal{P}(A')$ имеет 2^n элементов. Есть два типа подмножеств A : те, которые содержат a в качестве элемента, и те, которые не содержат. Подмножества, которые не содержат a , являются просто подмножествами A' , а их 2^n . Те, которые действительно содержат a , – это множества вида $X \cup \{a\}$, где $X \in \mathcal{P}(A')$, и их также 2^n , так как существует 2^n возможных вариантов для X . Таким образом, общее количество элементов $\mathcal{P}(A)$ равно $2^n + 2^n = 2^{n+1}$.

14. Базовый случай: $n = 1$. Одна хорда разрезает круг на две области, и $(n^2 + n + 2)/2 = 2$.

Шаг индукции: предположим, что, когда нарисовано n хорд, круг разрезан на $(n^2 + n + 2)/2$ областей. Когда рисуется новая хорда, она пересекает каждую из предыдущих n хорд ровно один раз. Следовательно, она пройдет через $n + 1$ областей, разрезая каждую из этих областей на две части. (Каждый раз, когда она пересекает одну из первых n хорд, она переходит из одной области в другую.) Следовательно, количество областей после прорисовки следующей хорды равно

$$\frac{n^2 + n + 2}{2} + (n + 1) = \frac{n^2 + 3n + 4}{2} = \frac{(n + 1)^2 + (n + 1) + 2}{2},$$

что и требовалось найти.

Раздел 6.3

1. Подсказка: формула имеет вид:

$$\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}.$$

6. Базовый случай: $n = 1$. Тогда

$$\sum_{i=1}^n \frac{1}{i^2} = 1 \leq 1 = 2 - \frac{1}{n}.$$

Шаг индукции: предположим, что

$$\sum_{i=1}^n \frac{1}{i^2} \leq 2 - \frac{1}{n}.$$

Тогда

$$\begin{aligned}\sum_{i=1}^{n+1} \frac{1}{i^2} &= \sum_{i=1}^n \frac{1}{i^2} + \frac{1}{(n+1)^2} \leq 2 - \frac{1}{n} + \frac{1}{(n+1)^2} \\ &= 2 - \frac{n^2 + n + 1}{n(n+1)^2} < 2 - \frac{n^2 + n}{n(n+1)^2} = 2 - \frac{1}{n+1}.\end{aligned}$$

8. (a) Пусть m произвольно, а затем по индукции докажем, что для всех $n \geq m$ выполняется неравенство $H_n - H_m \geq (n - m)/n$.

Базовый случай: $n = m$. Тогда $H_n - H_m = 0 \geq 0 = (n - m)/n$.

Шаг индукции: предположим, что $n \geq m$ и $H_n - H_m = 0 \geq 0 = (n - m)/n$. Тогда

$$\begin{aligned}H_{n+1} - H_m &= H_n + \frac{1}{n+1} - H_m \geq \frac{n-m}{n} + \frac{1}{n+1} \\ &\geq \frac{n-m}{n+1} + \frac{1}{n+1} = \frac{n+1-m}{n+1}.\end{aligned}$$

- (b) Базовый случай: если $n = 0$, то $H_{2^n} = H_1 = 1 \geq 1 = 1 + n/2$.

Шаг индукции: предположим, что $n \geq 0$ и $H_{2^n} \geq 1 + n/2$. По части (a):

$$H_{2^{n+1}} - H_{2^n} \geq \frac{2^{n+1} - 2^n}{2^{n+1}} = \frac{1}{2}.$$

Следовательно:

$$H_{2^{n+1}} \geq H_{2^n} + \frac{1}{2} \geq 1 + \frac{n}{2} + \frac{1}{2} = 1 + \frac{n+1}{2}.$$

- (c) Поскольку $\lim_{n \rightarrow \infty} (1 + n/2) = \infty$, согласно части (b) $\lim_{n \rightarrow \infty} H_{2^n} = \infty$. Ясно, что H_n образуют возрастающую последовательность, поэтому $\lim_{n \rightarrow \infty} H_n = \infty$.

12. (a) Подсказка: попробуйте доказать, что $2^n \geq n + 1$, из чего следует желаемый вывод.

- (b) Базовый случай: $n = 9$. Тогда $n! = 362\,880 \geq 262\,144 = (2^n)^2$.

Шаг индукции: предположим, что $n \geq 9$ и $n! \geq (2^n)^2$. Тогда

$$(n+1)! = (n+1) \cdot n! \geq (n+1) \cdot (2^n)^2 \geq 10 \cdot 2^{2n} \geq 2^2 \cdot 2^{2n} = 2^{2n+2} = (2^{n+1})^2.$$

- (c) Базовый случай: $n = 0$. Тогда $n! = 1 \leq 1 = 2^{(n^2)}$.

Шаг индукции: предположим, что $n! \leq 2^{(n^2)}$. Тогда

$$\begin{aligned}2^{((n+1)^2)} &= 2^{n^2+2n+1} = 2^{(n^2)} \cdot 2^{2n+1} \geq 2^{(n^2)} \cdot 2^{n+1} \\ &> n! \cdot (n+1) \quad (\text{согласно предположению индукции и части (a)}) \\ &= (n+1)!\end{aligned}$$

15. Базовый случай: $n = 0$. Тогда $a_n = a_0 = 0 = 2^0 - 0 - 1 = 2^n - n - 1$.

Шаг индукции: предположим, что $n \in \mathbb{N}$ и $a_n = 2n - n - 1$. Тогда

$$\begin{aligned} a_{n+1} &= 2a_n + n = 2(2^n - n - 1) + n = 2^{n+1} - 2n - 2 + n \\ &= 2^{n+1} - n - 2 = 2^{n+1} - (n + 1) - 1. \end{aligned}$$

18. (a) $\binom{n}{0} = \frac{n!}{0!n!} = 1$ и $\binom{n}{n} = \frac{n!}{n!0!} = 1$.

$$\begin{aligned} \text{(b)} \quad \binom{n}{k} + \binom{n}{k-1} &= \frac{n!}{k!(n-k)!} + \frac{n!}{(k-1)!(n-k+1)!} \\ &= \frac{n!(n-k+1)}{k!(n-k+1)!} + \frac{n!k}{k!(n-k+1)!} \\ &= \frac{n!(n+1)}{k!(n+1-k)!} = \binom{n+1}{k}. \end{aligned}$$

(c) Воспользуемся подсказкой.

Базовый случай: $n = 0$. Предположим, что A – это множество из 0 элементов. Тогда $A = \emptyset$, единственное значение k , о котором мы должны беспокоиться, – это $k = 0$, $\mathcal{P}_0(A) = \{\emptyset\}$, который имеет 1 элемент,

и $\binom{0}{0} = 1$.

Шаг индукции: предположим, что желаемый вывод верен для множеств из n элементов и A – это множество из $n + 1$ элементов. Пусть a – элемент A , и пусть $A' = A \setminus \{a\}$, которое представляет собой множество из n элементов. Теперь предположим, что $0 \leq k \leq n + 1$. Рассмотрим три случая.

Случай 1: $k = 0$. Тогда $\mathcal{P}_k(A) = \{\emptyset\}$, имеющий 1 элемент, и $\binom{n+1}{k} = 1$.

Случай 2: $k = n + 1$. Тогда $\mathcal{P}_k(A) = \{A\}$, который имеет 1 элемент, и $\binom{n+1}{k} = 1$.

Случай 3: $0 < k \leq n$. Есть два типа k -элементных подмножеств A : те, которые содержат a как элемент, и те, которые не содержат. Подмножества из k элементов, которые не содержат a , являются просто подмножествами из k элементов в A' , и по предположению индукции существует $\binom{n}{k}$ из них. Те, которые действительно содержат a , – это множества вида $X \cup \{a\}$, где $X \in \mathcal{P}_{k-1}(A')$, и по предположению индукции их $\binom{n}{k-1}$, так как это количество возможностей для X . Следовательно, согласно части (b), общее количество k -элементных подмножеств A равно

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

- (d) Пусть x и y произвольны; докажем уравнение индукцией по n .

Базовый случай: $n = 0$. Тогда обе части уравнения равны 1.

Шаг индукции: мы будем использовать части (a) и (b). Предположим, что

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k.$$

Тогда

$$\begin{aligned} (x+y)^{n+1} &= (x+y)(x+y)^n \\ &= (x+y) \sum_{k=0}^n \binom{n}{k} x^{n-k} y^k && \text{(предположение индукции)} \\ &= (x+y) \left[\binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \cdots + \binom{n}{n} y^n \right] \\ &= \binom{n}{0} x^{n+1} + \binom{n}{0} x^n y + \binom{n}{1} x^n y + \binom{n}{1} x^{n-1} y^2 \\ &\quad + \cdots + \binom{n}{n} x y^n + \binom{n}{n} y^{n+1} \\ &= x^{n+1} + \left[\binom{n}{0} + \binom{n}{1} \right] x^n y + \left[\binom{n}{1} + \binom{n}{2} \right] x^{n-1} y^2 \\ &\quad + \cdots + \left[\binom{n}{n-1} + \binom{n}{n} \right] x y^n + y^{n+1} \\ &= \binom{n+1}{0} x^{n+1} + \binom{n+1}{1} x^n y + \binom{n+1}{2} x^{n-1} y^2 \\ &\quad + \cdots + \binom{n+1}{n} x y^n + \binom{n+1}{n+1} y^{n+1} \\ &= \sum_{k=0}^{n+1} \binom{n+1}{k} x^{n+1-k} y^k. \end{aligned}$$

20. Подсказка: на удивление легче доказать, что для всех $n \geq 1$ выполняется неравенство $0 < a_n < 1/2$.

Раздел 6.4

1. (a) (\rightarrow) Предположим, что $\forall n Q(n)$. Пусть n произвольно. Тогда $Q(n+1)$ истинно, что означает $\forall k < n+1 P(k)$. В частности, поскольку $n < n+1$, $P(n)$ истинно. Так как n было произвольным, это доказывает, что $\forall n P(n)$.

(\leftarrow) Предположим, что $\forall n P(n)$. Тогда для любого n очевидно, что $\forall k < n P(k)$, что означает, что $Q(n)$ истинно.

- (b) Базовый случай: $n = 0$. Тогда $Q(n)$ – это утверждение $\forall k < 0 P(k)$, которое истинно в силу пустоты.

Шаг индукции: предположим, что $Q(n)$ истинно. Это означает, что $\forall k < n P(k)$ истинно, поэтому по предположению следует, что $P(n)$ истинно. Следовательно, $\forall k < n + 1 P(k)$ истинно, отсюда следует, что $Q(n + 1)$ истинно.

4. (a) Предположим, что $\sqrt{6}$ рационален. Пусть $S = \{q \in \mathbb{Z}^+ \mid \exists p \in \mathbb{Z}^+ (p/q = \sqrt{6})\}$. Тогда $S \neq \emptyset$, так что мы можем принять за q наименьший элемент S и можем выбрать положительное целое число p такое, что $p/q = \sqrt{6}$. Следовательно, $p^2 = 6q^2$, значит, p^2 четно и p тоже четно. Это означает, что $p = 2\bar{p}$ для некоторого целого числа \bar{p} . Таким образом, $4\bar{p}^2 = 6q^2$, значит, $2\bar{p}^2 = 3q^2$ и, следовательно, $3q^2$ четно. Легко убедиться, что если q нечетное, то $3q^2$ нечетное, поэтому q должно быть четным, что означает, что $q = 2\bar{q}$ для некоторого целого \bar{q} . Но тогда $\sqrt{6} = \bar{p}/\bar{q}$ и $\bar{q} < q$, что противоречит тому факту, что q – наименьший элемент S .
- (b) Предположим, что $\sqrt{2} + \sqrt{3} = p/q$. Возведение обеих сторон в квадрат дает $5 + 2\sqrt{6} = p^2/q^2$, откуда $\sqrt{6} = (p^2 - 5q^2)/(2q^2)$, что противоречит части (a).

7. (a) Воспользуемся обычной индукцией по n .

Базовый случай: $n = 0$. Обе части уравнения равны 0.

Шаг индукции: предположим, что $\sum_{i=0}^n F_i = F_{n+2} - 1$. Тогда

$$\sum_{i=0}^{n+1} F_i = \sum_{i=0}^n F_i + F_{n+1} = (F_{n+2} - 1) + F_{n+1} = F_{n+3} - 1.$$

- (b) Используем обычную индукцию по n .

Базовый случай: $n = 0$. Обе части уравнения равны 0.

Шаг индукции. Предположим, что $\sum_{i=0}^n (F_i)^2 = F_n F_{n+1}$. Тогда

$$\sum_{i=0}^{n+1} (F_i)^2 = \sum_{i=0}^n (F_i)^2 + (F_{n+1})^2 = F_n F_{n+1} + (F_{n+1})^2 = F_{n+1}(F_n + F_{n+1}) = F_{n+1} F_{n+2}.$$

- (c) Используем обычную индукцию по n .

Базовый случай: $n = 0$. Обе части уравнения равны 1.

Шаг индукции: предположим, что $\sum_{i=0}^n F_{2i+1} = F_{2n+2}$. Тогда

$$\sum_{i=0}^{n+1} F_{2i+1} = \sum_{i=0}^n F_{2i+1} + F_{2n+3} = F_{2n+2} + F_{2n+3} = F_{2n+4} = F_{2(n+1)+2}.$$

- (d) Формула имеет вид: $\sum_{i=0}^n F_{2i} = F_{2n+1} - 1$.

9. (a) (\rightarrow) Пусть a_0, a_1, a_2, \dots представляет собой последовательность Гибонacci. Пусть, в частности, $a_2 = a_0 + a_1$, что означает $c^2 = 1 + c$. Реше-

ние этого квадратного уравнения по формуле корней квадратного уравнения приводит к заключению $c = (1 \pm \sqrt{5})/2$.

(\leftarrow) Предположим, что $c = (1 + \sqrt{5})/2$ или $c = (1 - \sqrt{5})/2$. Тогда $c^2 = 1 + c$, и поэтому для любого $n \geq 2$ $a_n = c^n = c^{n-2}c^2 = c^{n-2}(1 + c) = c^{n-2} + c^{n-1} = a^{n-2} + a^{n-1}$.

- (b) Будет удобно ввести обозначения $c_1 = (1 + \sqrt{5})/2$ и $c_2 = (1 - \sqrt{5})/2$. Тогда для любого $n \geq 2$ выполняется равенство $a_n = sc_1^n + tc_2^n = sc_1^{n-2}c_1^2 + tc_2^{n-2}c_2^2 = sc_1^{n-2}(1 + c_1) + tc_2^{n-2}(1 + c_2) = (sc_1^{n-2} + tc_2^{n-2}) + c_1^{n-1} + tc_2^{n-1}) = a_{n-2} + a_{n-1}$.

(c) Подсказка: пусть $s = (5a_0 + (2a_1 - a_0)\sqrt{5})/10$ и $t = (5a_0 + (2a_1 - a_0)\sqrt{5})/10$.

11. Подсказка: формула имеет вид $a_n = 2 \cdot 3^n - 3 \cdot 2^n$.

15. Пусть a больше $5k$ и $k(k+1)$. Теперь предположим, что $n > a$, и с помощью алгоритма деления выберем q и r так, что $n = qk + r$ и $0 \leq r < k$. Заметим, что если $q \leq 4$, то $n = qk + r \leq 4k + r < 5k \leq a$; получается противоречие. Следовательно, $q > 4$, значит, $q \geq 5$, и из примера 6.1.3 следует, что $2^q \geq q^2$. Аналогичные рассуждения показывают, что $q \geq k+1$, поэтому $q^2 \geq q(k+1) = qk + q > qk + k > qk + r = n$. Следовательно, $2^n \geq 2^{qk} = (2^q)^k \geq (q^2)^k \geq n^k$.

18. Подсказка: формула $a_n = F_{n+2}/F_{n+1}$.

21. (a) Для любых чисел a, b, c и d :

$$\begin{aligned} (ab)(cd) &= (cd)(ab) && \text{(коммутативный закон)} \\ &= c(d(ab)) && \text{(ассоциативный закон)} \\ &= c((da)b) && \text{(ассоциативный закон)} \\ &= c((ad)b) && \text{(коммутативный закон).} \end{aligned}$$

- (b) Для упрощения обозначений мы будем предполагать, что любое произведение является сгруппированным слева, если скобки не используются для обозначения обратного. Воспользуемся сильной индукцией по n . Предположим, что утверждение истинно для произведений, содержащих менее n элементов, и рассмотрим любое произведение a_1, a_2, \dots, a_n . Если $n = 1$, то единственным произведением является произведение, сгруппированное слева, поэтому доказывать нечего. Теперь предположим, что $n > 1$. Тогда наше произведение имеет вид pq , где p – произведение a_1, \dots, a_{k-1} и q является произведением a_k, \dots, a_n для некоторого k , соответствующего неравенству $2 \leq k \leq n$. По предположению индукции $p = a_1 \cdots a_{k-1}$ и $q = a_k \cdots a_n$ (где по нашему соглашению эти два произведения сгруппированы слева). Таким образом, достаточно доказать равенство $(a_1 \cdots a_{k-1})(a_k \cdots a_n) = a_1 \cdots a_n$. Если $k = n$, то левая часть этого равенства уже сгруппирована слева, поэтому доказывать нечего. Если $k < n$, то

$$\begin{aligned} (a_1 \cdots a_{k-1})(a_k \cdots a_n) &= (a_1 \cdots a_{k-1}) ((a_k \cdots a_{n-1}) a_n) && \text{(определение группировки слева)} \\ &= ((a_1 \cdots a_{k-1}) (a_k \cdots a_{n-1})) a_n && \text{(ассоциативный закон)} \end{aligned}$$

$$\begin{aligned}
 &= (a_1 \cdots a_{n-1})a_n && \text{(предположение индукции)} \\
 &= a_1 \cdots a_n && \text{(определение группировки слева).}
 \end{aligned}$$

- (c) Согласно части (b), мы можем предположить, что два произведения сгруппированы слева. Таким образом, мы должны доказать, что если b_1, b_2, \dots, b_n – это перестановка a_1, a_2, \dots, a_n , тогда $a_1 \cdots a_n = b_1 \cdots b_n$, где, как и в части (b), мы предполагаем, что произведения сгруппированы слева, если скобки не указывают иное. Воспользуемся индукцией по n . Если $n = 1$, то произведения явно равны, потому что $b_1 = a_1$. Теперь предположим, что утверждение верно для произведений длины n , и предположим, что b_1, \dots, b_{n+1} – перестановка ряда a_1, \dots, a_{n+1} . Тогда b_{n+1} – один из элементов ряда a_1, \dots, a_{n+1} . Если $b_{n+1} = a_{n+1}$, то

$$\begin{aligned}
 b_1 \cdots b_{n+1} &= (b_1 \cdots b_n)a_{n+1} && \text{(определение группировки слева)} \\
 &= (a_1 \cdots a_n)a_{n+1} && \text{(предположение индукции)} \\
 &= a_1 \cdots a_{n+1} && \text{(определение группировки слева).}
 \end{aligned}$$

Теперь предположим, что $b_{n+1} = a_k$ для некоторого $k \leq n$. Запишем выражение $a_1 \cdots \widehat{a}_k \cdots a_n$ для (сгруппированного слева) произведения чисел a_1, \dots, a_n , исключив множитель a_k . Тогда

$$\begin{aligned}
 b_1 \cdots b_{n+1} &= (b_1 \cdots b_n)a_k && \text{(определение группировки слева)} \\
 &= (a_1 \cdots \widehat{a}_k \cdots a_{n+1})a_k && \text{(предположение индукции)} \\
 &= ((a_1 \cdots \widehat{a}_k \cdots a_n)a_{n+1})a_k && \text{(определение группировки слева)} \\
 &= (a_1 \cdots \widehat{a}_k \cdots a_n)(a_{n+1}a_k) && \text{(ассоциативный закон)} \\
 &= (a_1 \cdots \widehat{a}_k \cdots a_n)(a_ka_{n+1}) && \text{(коммутативный закон)} \\
 &= ((a_1 \cdots \widehat{a}_k \cdots a_n)a_k)a_{n+1} && \text{(ассоциативный закон)} \\
 &= (a_1 \cdots a_n)a_{n+1} && \text{(предположение индукции)} \\
 &= a_1 \cdots a_{n+1} && \text{(определение группировки слева).}
 \end{aligned}$$

Раздел 6.5

1. $B_n = \{n\}$.
4. $B_0 = \{\emptyset\}, B_1 = \{X \in \mathcal{P}(\mathbb{N}) \mid X \text{ имеет ровно один элемент}\}, B_2 = \{X \in \mathcal{P}(\mathbb{N}) \mid X \text{ имеет один или два элемента}\}$. В общем случае для каждого натурального числа n справедливо определение $B_n = \{X \in \mathcal{P}(\mathbb{N}) \mid X \neq \emptyset \text{ и } X \text{ имеет не более } n \text{ элементов}\}$.
5. $\{n \in \mathbb{Z} \mid n \geq 2\}$.
7. (a) $B_0 = \{x \in \mathbb{R} \mid -2 \leq x \leq 0\}, B_1 = \{x \in \mathbb{R} \mid 0 \leq x \leq 4\}, B_2 = \{x \in \mathbb{R} \mid 0 \leq x \leq 16\}$, В общем случае для любого натурального числа n справедливо определение $B_n = \{x \in \mathbb{R} \mid 0 \leq x \leq 2^{(2^n)}\}$.
- (b) $\bigcup_{n \in \mathbb{N}} B_n = \{x \in \mathbb{R} \mid x \geq -2\}$. Следовательно, $-1, 3 \in \bigcup_{n \in \mathbb{N}} B_n$, но $f(-1, 3) = -3 \notin \bigcup_{n \in \mathbb{N}} B_n$, поэтому $\bigcup_{n \in \mathbb{N}} B_n$ не замкнуто относительно f . Другими словами, свойство 2 в определении 5.4.8 не выполняется.
- (c) \mathbb{R} .
10. Воспользуемся индукцией по n .

Базовый случай: $n = 1$. Тогда $x = 2! + 2 = 4$. Единственное значение i , о котором мы должны беспокоиться, – это $i = 0$, и для этого значения i мы имеем $i + 2 = 2$ и $x + i = 4$. Поскольку $2 \mid 4$, имеем $(i + 2) \mid (x + i)$.

Шаг индукции: предположим, что n – натуральное число и для любого целого i если $0 \leq i \leq n - 1$, то $(i + 2) \mid ((n + 1)! + 2 + i)$. Пусть теперь $x = (n + 2)! + 2$, и предположим, что $0 \leq i \leq n$. Если $i = n$, то имеем

$$x + i = (n + 2)! + 2 + i = (i + 2)! + (i + 2) = (i + 2)((i + 1)! + 1),$$

поэтому $(i + 2) \mid (x + i)$. Теперь предположим, что $0 \leq i \leq n - 1$. По предположению индукции мы знаем, что $(i + 2) \mid ((n + 1)! + 2 + i)$, поэтому можем выбрать некоторое целое k такое, что $(n + 1)! + 2 + i = k(i + 2)$, а значит, $(n + 1)! = (k - 1)(i + 2)$. Следовательно:

$$\begin{aligned} x + i &= (n + 2)! + 2 + i = (n + 2)(n + 1)! + (i + 2) \\ &= (n + 2)(k - 1)(i + 2) + (i + 2) = (i + 2)((n + 2)(k - 1) + 1), \end{aligned}$$

поэтому $(i + 2) \mid (x + i)$.

14. Ясно, что T – отношение на A и $R = R^1 \subseteq T$. Чтобы показать, что T транзитивно, предположим, что $(x, y) \in T$ и $(y, z) \in T$. Тогда по определению T мы можем выбрать натуральные числа n и m такие, что $(x, y) \in R^n$ и $(y, z) \in R^m$. Таким образом, согласно упражнению 11 $(x, z) \in R^m \circ R^n = R^{m+n}$, поэтому $(x, z) \in \bigcup_{n \in \mathbb{Z}^+} R^n = T$. Следовательно, отношение T транзитивно.

Наконец, предположим, что $R \subseteq S \subseteq A \times A$ и отношение S транзитивно. Мы должны показать, что $T \subseteq S$, и, очевидно, по определению T достаточно показать, что $\forall n \in \mathbb{Z}^+ (R^n \subseteq S)$. Докажем это индукцией по n . Мы предположили, что $R \subseteq S$, поэтому, когда $n = 1$, мы имеем $R^n = R^1 = R \subseteq S$. Для шага индукции предположим, что n – натуральное число и $R^n \subseteq S$. Теперь предположим, что $(x, y) \in R^{n+1}$. Тогда по определению R^{n+1} мы можем выбрать $z \in A$ такой, что $(x, z) \in R$ и $(z, y) \in R^n$. По умолчанию $R \subseteq S$ и по предположению индукции $R^n \subseteq S$. Следовательно, $(x, z) \in S$ и $(z, y) \in S$, и, поскольку S транзитивно, $(x, y) \in S$. Так как пара (x, y) была произвольным элементом из R^{n+1} , это показывает, что $R^{n+1} \subseteq S$.

16. (a) $R \cap S \subseteq R$ и $R \cap S \subseteq S$. Следовательно, согласно упражнению 15 для любого натурального числа n , $(R \cap S)^n \subseteq R^n$ и $(R \cap S)^n \subseteq S^n$, поэтому $(R \cap S)^n \subseteq R^n \cap S^n$. Однако эти два отношения не обязательно должны быть равны. Например, если $A = \{1, 2, 3, 4\}$, $R = \{(1, 2), (2, 4)\}$ и $S = \{(1, 3), (3, 4)\}$, то $(R \cap S)^2 = \emptyset$, но $R^2 \cap S^2 = \{(1, 4)\}$.
(b) $R^n \cup S^n \subseteq (R \cup S)^n$, но они не обязательно должны быть равны. (Вы должны суметь доказать первое утверждение и найти контрпример, подтверждающий второе.)

18. (a) Воспользуемся индукцией.

Базовый случай: $n = 1$. Пусть $(a, b) \in R^1 = R$. Пусть $f = \{(0, a), (1, b)\}$. Тогда f – это R -путь от a до b длины 1. Для другого направления предположим, что f является R -путем от a до b длины 1. По определению R -пути это означает, что $f(0) = a$, $f(1) = b$, и $(f(0), f(1)) \in R$. Следовательно, $(a, b) \in R = R^1$.

Шаг индукции: предположим, что n – натуральное число и $R^n = \{(a, b) \in A \times A \mid$ существует R -путь от a до b длины $n\}$. Теперь предположим, что $(a, b) \in R^{n+1} = R^1 \circ R^n$ согласно упражнению 11. Тогда существует некоторый элемент с такой, что $(a, c) \in R^n$ и $(c, b) \in R$. По предположению индукции существует R -путь f от a до c длины n . Тогда $f \cup \{(n+1, b)\}$ – это R -путь от a до b длины $n+1$. Для другого направления предположим, что f является R -путем от a до b длины $n+1$. Пусть $c = f(n)$. Тогда $f \cup \{(n+1, b)\}$ – это R -путь от a до c длины n , поэтому по индуктивному предположению $(a, c) \in R^n$. Но также $(c, b) = (f(n), f(n+1)) \in R$, поэтому $(a, b) \in R^1 \circ R^n = R^{n+1}$.

- (b) Это следует из части (a) и упражнения 14.

Решения к главе 7

Раздел 7.1

2. (a) $\gcd(775, 682) = 31 = -7 \cdot 775 + 8 \cdot 682$.
 (b) $\gcd(562, 243) = 1 = 16 \cdot 562 - 37 \cdot 243$.
5. Пусть n – произвольное целое число.
 (\rightarrow) Предположим, что n – линейная комбинация a и b . Тогда существуют целые числа s и t такие, что $n = sa + tb$. Поскольку $d = \gcd(a, b)$, $d \mid a$ и $d \mid b$, поэтому существуют целые числа j и k такие, что $a = jd$ и $b = kd$. Следовательно, $n = sa + tb = sjd + tkd = (sj + tk)d$, поэтому $d \mid n$.
 (\leftarrow) Предположим, что $d \mid n$. Тогда существует такое целое число k , что $n = kd$. По теореме 7.1.4 существуют целые числа s и t такие, что $d = sa + tb$. Следовательно, $n = kd = k(sa + tb) = ksa + ktb$, поэтому n является линейной комбинацией a и b .
7. (a) Нет. Контрпример: $a = b = 2$, $a' = 3$, $b' = 4$.
 (b) Да. Предположим, что $a \mid a'$ и $b \mid b'$. Пусть $d = \gcd(a, b)$. Тогда $d \mid a$ и $d \mid b$. Поскольку $d \mid a$ и $a \mid a'$ по теореме 3.3.7, $d \mid a'$. Аналогично $d \mid b'$. Следовательно, по теореме 7.1.6 $d \mid \gcd(a', b')$.
9. Используем сильную индукцию по максимуму a и b . Другими словами, с помощью сильной индукции докажем следующее утверждение:

$$\forall k \in \mathbb{Z}^+ [\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ (\max(a, b) = k \rightarrow \gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a, b)} - 1)],$$

где $\max(a, b)$ обозначает максимум a и b .

Возьмем произвольное число $k \in \mathbb{Z}^+$ и предположим, что для любого натурального числа $k' < k$

$$\forall a \in \mathbb{Z}^+ \forall b \in \mathbb{Z}^+ (\max(a, b) = k' \rightarrow \gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a, b)} - 1).$$

Пусть теперь a и b – произвольные натуральные числа, и предположим, что $\max(a, b) = k$. Мы можем предположить, что $a \geq b$, в противном случае можем поменять местами значения a и b . Рассмотрим два случая.

Случай 1. $a = b$. Тогда

$$\gcd(2^a - 1, 2^b - 1) = \gcd(2^a - 1, 2^a - 1) = 2^a - 1 = 2^{\gcd(a,a)} - 1 = 2^{\gcd(a,b)} - 1.$$

Случай 2. $a > b$. Пусть $c = a - b > 0$, так что $a = c + b$. Пусть $k' = \max(c, b)$. Поскольку $b < a$ и $c < a$, $k' < a = \max(a, b) = k$. Следовательно:

$$\begin{aligned} \gcd(2^a - 1, 2^b - 1) &= \gcd(2^c - 1 + 2^a - 2^c, 2^b - 1) \\ &= \gcd(2^c - 1 + 2^c(2^b - 1), 2^b - 1) \\ &= \gcd(2^c - 1, 2^b - 1) && \text{(упражнение 6)} \\ &= 2^{\gcd(c,b)} - 1 && \text{(индуктивная гипотеза)} \\ &= 2^{\gcd(c+b,b)} - 1 && \text{(упражнение 6)} \\ &= 2^{\gcd(c,b)} - 1. \end{aligned}$$

12. (a) $\gcd(55, 34) = 1$. Числа r_i – это числа Фибоначчи. Всего 8 шагов деления.
 (b) $\gcd(F_{n+1}, F_n) = 1$. Всего $n - 1$ шагов деления.

Раздел 7.2

2. 14 950.
5. Предположим, что некоторое простое число p присутствует в разложениях на простые множители как a , так и b . Тогда $p \mid a$ и $p \mid b$, поэтому $\gcd(a, b) \geq p > 1$, и поэтому a и b не являются взаимно простыми.
- Теперь предположим, что a и b не взаимно просты. Пусть $d = \gcd(a, b) > 1$. Пусть p – любое простое число из факторизации d . Тогда, поскольку $d \mid a$ и $d \mid b$, число p должно входить в разложения на простые множители как a , так и b .
8. Пусть $d = \gcd(a, b)$ и $x = ab/\gcd(a, b) = ab/d$.
- (a) Поскольку $d = \gcd(a, b)$ и $d \mid b$, то существует такое целое число k , что $b = kd$. Следовательно, $x = akd/d = ak$, поэтому x – целое число и $a \mid x$. Аналогичное рассуждение показывает, что $b \mid x$, поэтому x является общим кратным a и b . Поскольку m – наименьшее общее кратное, $m \leq x$.
 - (b) Предположим, что $r > 0$. Поскольку $a \mid m$, существует такое целое число t , что $m = ta$. Следовательно, $r = ab - qm = ab - qta = (b - qt)a$, поэтому $a \mid r$. Аналогично $b \mid p$. Но $r < m$, поэтому это противоречит определению m как наименьшего положительного целого числа, которое делится как на a , так и на b . Следовательно, $r = 0$.
 - (c) При t , определенном как в части (b), $ab = qm = qta$. Разделив обе части на a , мы получим $b = qt$, поэтому $q \mid b$. Доказательство того, что $q \mid a$, аналогично.
 - (d) Поскольку $q \mid a$ и $q \mid b$, $q \leq \gcd(a, b)$. Следовательно, $ab = qm \leq \gcd(a, b)m$, поэтому $m \geq ab/\gcd(a, b)$.
11. Подсказка: один из подходов состоит в том, чтобы принять за q и r частное и остаток от деления m на $\text{lcm}(a, b)$ и доказать, что $r = 0$.

13. Пусть факторизация b имеет вид $b = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Тогда факторизация b^2 выглядит так: $b^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k}$. Поскольку $a^2 \mid b^2$, каждое простое число из факторизации a должно входить в ряд p_1, p_2, \dots, p_k , поэтому $a = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$ для некоторых натуральных чисел f_1, f_2, \dots, f_k . Следовательно, $a^2 = p_1^{2f_1} p_2^{2f_2} \cdots p_k^{2f_k}$. Поскольку $a^2 \mid b^2$, для каждого i должно быть $2f_i \leq 2e_i$, а значит, $f_i \leq e_i$. Следовательно, $a \mid b$.
16. Пусть p_1, p_2, \dots, p_k – список всех простых чисел, которые встречаются при разложении на простые множители a или b , так что

$$a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \quad b = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

для некоторых натуральных чисел e_1, e_2, \dots, e_k и f_1, f_2, \dots, f_k . Для $i = 1, 2, \dots, k$ пусть

$$g_i = \begin{cases} e_i, & \text{если } e_i \geq f_i \\ 0, & \text{если } e_i < f_i \end{cases}, \quad h_i = \begin{cases} 0, & \text{если } e_i \geq f_i \\ f_i, & \text{если } e_i < f_i \end{cases}.$$

Пусть

$$c = p_1^{g_1} p_2^{g_2} \cdots p_k^{g_k}, \quad d = p_1^{h_1} p_2^{h_2} \cdots p_k^{h_k}.$$

Тогда для всех i выполняются неравенства $g_i \leq e_i$ и $h_i \leq f_i$, следовательно, $c \mid a$ и $d \mid b$. Кроме того, c и d не имеют общих простых множителей, поэтому в упражнении 5 c и d взаимно просты. И наконец:

$$cd = p_1^{g_1+h_1} \cdots p_k^{g_k+h_k} = p_1^{\max(e_1, f_1)} \cdots p_k^{\max(e_k, f_k)} = \text{lcm}(a, b).$$

19. (a) Поскольку x – положительное рациональное число, существуют натуральные числа m и n такие, что $x = m/n$. Пусть $d = \gcd(m, n)$. Исходя из упражнения 9 мы можем обозначить за a и b натуральные числа такие, что $m = da$, $n = db$ и $\gcd(a, b) = 1$. Тогда

$$x = \frac{m}{n} = \frac{da}{db} = \frac{a}{b}.$$

- (b) Поскольку $a/b = c/d$, $ad = bc$. Следовательно, $a \mid bc$. Так как $\gcd(a, b) = 1$, по теореме 7.2.2 $a \mid c$. Аналогичные рассуждения показывают, что $c \mid a$, поэтому $a = c$. Следовательно, $ad = bc = ba$, и, разделив обе части на a , мы заключаем, что $b = d$.
- (c) Из части (a) имеем $x = a/b$, где a и b – взаимно простые натуральные числа. Пусть факторизации a и b представлены следующим образом:

$$a = r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j}, \quad b = s_1^{h_1} s_2^{h_2} \cdots s_l^{h_l}.$$

Отметим, что согласно упражнению 5 эти факторизации в общем случае не имеют общих простых чисел. Тогда

$$x = \frac{r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j}}{s_1^{h_1} s_2^{h_2} \cdots s_l^{h_l}} = r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j} s_1^{-h_1} s_2^{-h_2} \cdots s_l^{-h_l}.$$

Перестановка простых чисел $r_1, \dots, r_j, s_1, \dots, s_l$ в порядке возрастания дает искомое произведение $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$.

- (d) Начнем с обращения последовательности этапов части (c). Пусть r_1, r_2, \dots, r – те простые числа в произведении $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, чьи показатели положительны, перечисленные в порядке возрастания, а s_1, s_2, \dots, s_l – те, у которых показатели отрицательны. Переписывая каждое простое число, возведенное в отрицательную степень, как простое число в положительной степени в знаменателе, мы получаем дробь

$$x = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = \frac{r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j}}{s_1^{h_1} s_2^{h_2} \cdots s_l^{h_l}},$$

где все показатели g_i и h_i являются натуральными числами. У числителя и знаменателя нет общих простых множителей, поэтому они взаимно просты. Аналогичным образом произведение $q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m}$ можно переписать в виде дроби со всеми положительными показателями:

$$x = q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m} = \frac{v_1^{y_1} v_2^{y_2} \cdots v_t^{y_t}}{w_1^{z_1} w_2^{z_2} \cdots w_u^{z_u}}.$$

Согласно части (b), $r_1^{g_1} r_2^{g_2} \cdots r_j^{g_j} = v_1^{y_1} v_2^{y_2} \cdots v_t^{y_t}$ и $s_1^{h_1} s_2^{h_2} \cdots s_l^{h_l} = w_1^{z_1} w_2^{z_2} \cdots w_u^{z_u}$. Исходя из уникальности факторизаций в простых числах, $j = t$ и для всех $i \in \{1, \dots, j\}$ выполняются равенства $r_i = v_t$ и $g_i = y_i$, а также $l = u$ и для всех $i \in \{1, \dots, l\}$, $s_i = w_i$ и $h_i = z_i$. Переписывая простые числа в знаменателе как простые числа в отрицательной степени, мы обнаруживаем, что исходные два произведения $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ и $q_1^{f_1} q_2^{f_2} \cdots q_m^{f_m}$ одинаковые.

Раздел 7.3

4. (a) Поскольку Z_1 – аддитивный единичный элемент, $Z_1 + Z_2 = Z_2$. А поскольку Z_2 – аддитивный единичный элемент, $Z_1 + Z_2 = Z_1$. Следовательно, $Z_1 = Z_1 + Z_2 = Z_2$.
- (b) Поскольку X'_1 является аддитивным обратным для X , то $X'_1 + X + X'_2 = [0]_m + X'_2 = X'_2$. Аналогично, поскольку X'_2 является аддитивным обратным для X , то $X'_1 + X + X'_2 = X'_1 + [0]_m = X'_1$. Поэтому $X'_1 = X'_2$.
- (c) Предположим, что O_1 и O_2 – мультипликативные единичные элементы. Тогда $O_1 = O_1 \cdot O_2 = O_2$.
- (d) Предположим, что X'_1 и X'_2 – мультипликативные обратные к X . Тогда $X'_1 = X'_1 \cdot [1]_m = X'_1 \cdot X \cdot X'_2 = [1]_m \cdot X'_2 = X'_2$.

8. Пусть a и b – произвольные целые числа. Тогда

$na \equiv nb \pmod{nm}$ тогда и только тогда, когда $\exists k \in \mathbb{Z} (nb - na = knm)$
 тогда и только тогда, когда $\exists k \in \mathbb{Z} (b - a = km)$
 тогда и только тогда, когда $a \equiv b \pmod{m}$.

10. (a) $x \in [95]_{237}$.
 (b) $x \in [12]_{59}$.
13. Пусть a и b – произвольные целые числа. Предположим сначала, что $a \equiv b \pmod{m}$. Тогда $[a]_m = [b]_m$, поэтому $[na]_m = [n]_m \cdot [a]_m = [n]_m \cdot [b]_m = [nb]_m$, и поэтому $na \equiv nb \pmod{m}$.
 Теперь предположим, что $na \equiv nb \pmod{m}$, поэтому $[n]_m \cdot [a]_m = [na]_m = [nb]_m = [n]_m \cdot [b]_m$. Поскольку m и n взаимно просты, $[n]_m$ имеет мультипликативное обратное. Умножая обе части уравнения $[n]_m \cdot [a]_m = [n]_m$ на $[n]_m^{-1}$, мы получаем $[a]_m = [b]_m$, поэтому $a \equiv b \pmod{m}$.
15. Подсказка: докажите, что если $a \equiv b \pmod{m}$, то $D(m) \cap D(a) = D(m) \cap D(b)$.
17. (a) Сначала отметим, что $10 \equiv 1 \pmod{3}$, поэтому $[10]_3 = [1]_3$. Следовательно, $[10^2]_3 = [10]_3 \cdot [10]_3 = [1]_3 \cdot [1]_3 = [1]_3$, $[10^3]_3 = [10^2]_3 \cdot [10]_3 = [1]_3 \cdot [1]_3 = [1]_3$, и, в общем случае, для любого $i \in \mathbb{N}$ $[10^i]_3 = [1]_3$. (Более строгое доказательство можно провести по индукции.) Таким образом,

$$\begin{aligned}[n]_3 &= [d_0 + 10d_1 + \dots + 10^k d_k]_3 \\ &= [d_0]_3 + [10]_3 \cdot [d_1]_3 + \dots + [10^k]_3 \cdot [d_k]_3 \\ &= [d_0]_3 + [1]_3 \cdot [d_1]_3 + \dots + [1]_3 \cdot [d_k]_3 \\ &= [d_0 + d_1 + \dots + d_k]_3.\end{aligned}$$

Другими словами, $n \equiv (d_0 + d_1 + \dots + d_k) \pmod{3}$.

- (b) $3 \mid n$ тогда и только тогда, когда $[n]_3 = [0]_3$ тогда и только тогда, когда $[d_0 + \dots + d_k]_3 = [0]_3$ тогда и только тогда, когда $3 \mid (d_0 + \dots + d_k)$.
19. (a) Предположим, что $n \geq 10$. Сначала заметим, что

$$10f(n) = (d_k \dots d_1 d_0)_{10} + 50d_0 = (d_k \dots d_1 d_0)_{10} + 49d_0 = n + 49d_0.$$

Следовательно, $3f(n) - n = 49d_0 - 7f(n) = 7(7d_0 - f(n))$, поэтому $n \equiv 3f(n) \pmod{7}$, или, что эквивалентно, $[n]_7 = [3]_7 \cdot [f(n)]_7$. Поскольку $[3]_7^{-1} = [5]_7$, отсюда следует, что $[f(n)]_7 = [5]_7 \cdot [n]_7$, поэтому $f(n) \equiv 5n \pmod{7}$.

- (b) Предположим, что $n \geq 10$. Если $7 \mid n$, то $[n]_7 = [0]_7$, поэтому $[f(n)]_7 = [5n]_7 = [5]_7 \cdot [0]_7 = [0]_7$, и, следовательно, $7 \mid f(n)$. Аналогично, если $7 \mid f(n)$, тогда $[f(n)]_7 = [0]_7$, поэтому $[n]_7 = [3f(n)]_7 = [3]_7 \cdot [0]_7 = [0]_7$ и $7 \mid n$.
- (c) $f(627\ 334) = 62\ 733 + 5 \cdot 4 = 62\ 753$;
 $f(62\ 753) = 6275 + 5 \cdot 3 = 6290$;
 $f(6290) = 629 + 5 \cdot 0 = 629$;
 $f(629) = 62 + 5 \cdot 9 = 107$;
 $f(107) = 10 + 5 \cdot 7 = 45$;
 $f(45) = 4 + 5 \cdot 5 = 29$. Так как $7 \nmid 29$, $7 \nmid 62\ 7334$.

Раздел 7.4

2. (a) $\varphi(539) = 420$.
 (b) $\varphi(540) = 144$.
 (c) $\varphi(541) = 540$.
6. Предположим, что $a \equiv b \pmod{mn}$. Тогда $mn \mid (b - a)$, поэтому для некоторого целого k выполняется равенство $b - a = ktmn$. Следовательно, $m \mid (b - a)$ и $n \mid (b - a)$, поэтому $a \equiv b \pmod{m}$ и $a \equiv b \pmod{n}$.

Теперь предположим, что $a \equiv b \pmod{m}$ и $a \equiv b \pmod{n}$. Поскольку $a \equiv b \pmod{n}$, то $n \mid (b - a)$, поэтому существует некоторое целое j такое, что $b - a = jn$. Поскольку $a \equiv b \pmod{m}$, то $m \mid (b - a)$, поэтому $m \mid jn$. Но $\gcd(m, n) = 1$, поэтому по теореме 7.2.2 следует, что $m \mid j$. Пусть k – такое целое число, что $j = km$. Тогда $b - a = jn = ktmn$. Следовательно, $mn \mid (b - a)$, поэтому $a \equiv b \pmod{mn}$.

8. Первая половина решения упражнения 6 не использует гипотезу о том, что m и n взаимно прости, поэтому направление «тогда и только тогда» слева направо верно, даже если эта гипотеза опровергнута. Вот контрпример для другого направления: $a = 0, b = 12, m = 4, n = 6$.
10. Предположим, что p – простое число и a – натуральное число. Рассмотрим два случая.

Случай 1. $p \nmid a$. Тогда p и a взаимно прости, поэтому по теореме 7.4.2 $[a]_p^{p-1} = [1]_p$. Следовательно, $[a^p]_p = [a]_p^{p-1} \cdot [a]_p = [1]_p \cdot [a]_p = [a]_p$, так что $a^p \equiv a \pmod{p}$.

Случай 2. $p \mid a$. Тогда $[a]_p = [0]_p$, поэтому $[a^p]_p = [0]_p^p \cdot [0]_p = [a]_p$ и, следовательно, $a^p \equiv a \pmod{p}$.

13. Совет: используйте лемму 7.4.6 и индукцию по k .

15. (a) Используем индукцию по k .

Базовый случай: когда $k = 1$, утверждение, которое необходимо доказать, состоит в том, что для каждого положительного целого числа m_1 и каждого целого числа a_1 существует целое число r такое, что $1 \leq r \leq m_1$ и $r \equiv a_1 \pmod{m_1}$. Это верно, потому что $\{1, 2, \dots, m_1\}$ – полная система вычетов по модулю m_1 .

Шаг индукции: предположим, что утверждение верно для списков из k попарно взаимно простых натуральных чисел, и пусть m_1, m_2, \dots, m_{k+1} – список $k + 1$ попарно взаимно простых натуральных чисел. Пусть $M' = m_1 m_2 \cdots m_k$ и $M = m_1 m_2 \cdots m_{k+1} = M' m_{k+1}$. Пусть a_1, a_2, \dots, a_{k+1} – произвольные целые числа. По предположению индукции существует целое число r' такое, что для всех $i \in \{1, 2, \dots, k\}$, $r' \equiv a_i \pmod{m_i}$. Из упражнения 13 $\gcd(M', m_{k+1}) = 1$, поэтому по лемме 7.4.7 существует такое целое число r , что $1 \leq r \leq M$, $r \equiv r' \pmod{M'}$ и $r \equiv a_{k+1} \pmod{m_{k+1}}$. По упражнению 14 для каждого $i \in \{1, 2, \dots, k\}$, $r \equiv r' \pmod{m_i}$, и, следовательно, $r \equiv a_i \pmod{m_i}$.

(b) Предположим, что $1 \leq r_1, r_2 \leq M$ и для всех $i \in \{1, 2, \dots, k\}$, $r_1 \equiv a_i \pmod{m_i}$ и $r_2 \equiv a_i \pmod{m_i}$. Тогда для всех $i \in \{1, 2, \dots, k\}$ выполняется равенство

$r_1 \equiv r_2 \pmod{mi}$, поэтому в упражнении 14 $r_1 \equiv r_2 \pmod{M}$. Следовательно, $r_1 = r_2$.

17. Предположим, что m и n взаимно просты. Пусть элементы $D(m)$ равны a_1, a_2, \dots, a_s , и пусть элементы $D(n)$ равны b_1, b_2, \dots, b_t . Тогда $\sigma(m) = a_1 + a_2 + \dots + a_s$ и $\sigma(n) = b_1 + b_2 + \dots + b_t$. Используя функцию f из части (б) упражнения 16, мы видим, что все элементы $D(mn)$ являются произведениями вида $a_i b_j$, где $1 \leq i \leq s$ и $1 \leq j \leq t$. Таким образом, мы можем расположить элементы $D(mn)$ в таблице, состоящей из s строк и t столбцов, где запись в строке i , столбце j таблицы – это $a_i b_j$; каждый элемент $D(mn)$ встречается в этой таблице ровно один раз. Чтобы вычислить $\sigma(mn)$, мы должны сложить все записи в этой таблице. Мы сделаем это, сначала найдя сумму каждой строки таблицы, а затем сложив эти суммы.

Для $1 \leq i \leq s$ пусть r_i будет суммой строки i таблицы. Тогда

$$r_i = a_i b_1 + a_i b_2 + \dots + a_i b_t = a_i(b_1 + b_2 + \dots + b_t) = a_i \sigma(n).$$

Следовательно:

$$\begin{aligned} \sigma(mn) &= r_1 + r_2 + \dots + r_s = a_1 \sigma(n) + a_2 \sigma(n) + \dots + a_s \sigma(n) \\ &= (a_1 + a_2 + \dots + a_s) \sigma(n) = \sigma(m) \sigma(n). \end{aligned}$$

Раздел 7.5

2. (а) $n = 5893$, $\varphi(n) = 5740$, $d = 2109$.
 (б) $c = 3421$.
5. (а) $n = 17 \cdot 29$.
 (б) $d = 257$.
 (с) $m = 183$.
7. (а) $c = 72$.
 (б) $d = 63$.
 (с) 288.
 (д) $\varphi(n) = 144$, $d = 47, 18$.
9. Используем сильную индукцию. Предположим, что a – натуральное число, и для каждого положительного целого числа $k < a$ при вычислении X^k требуется не более $2\log_2 k$ умножений.

Случай 1. $a = 1$. Тогда $X^a = X^1 = X$, поэтому умножения не требуется, и $2\log_2 a = 2\log_2 1 = 0$.

Случай 2. a – четное число. Тогда $a = 2k$ для некоторого натурального числа $k < a$, и для вычисления X^a мы используем формулу $X^a = X^k \cdot X^k$. Пусть m будет числом умножений, используемых для вычисления X^k . По предположению индукции $m \leq 2\log_2 k$. Для вычисления X^a мы используем одно дополнительное умножение (для умножения X^k на себя), поэтому количество умножений равно

$$m + 1 \leq 2\log_2 k + 1 < 2(\log_2 k + 1) = 2\log_2(2k) = 2\log_2 a.$$

Случай 3. $a > 1$, и a нечетное. Тогда $a = 2k + 1$ для некоторого положительного целого числа $k < a$, и для вычисления X^a мы используем формулу $X^a = X^k \cdot X^k \cdot X$. Как и в случае 2, если мы допустим, что m – количество умножений, используемых для вычисления X^k , то мы имеем $m \leq 2\log_2 k$. Для вычисления X^a мы используем два дополнительных умножения, так что количество умножений равно

$$m + 2 \leq 2\log_2 k + 2 = 2(\log_2 k + 1) = 2\log_2(2k) < 2\log_2(2k + 1) = 2\log_2 a.$$

12. Так как $a \in R_2$, то $[a]_n^{n-1} \neq [1]_n$. А поскольку $\gcd(n, a) = 1$, $[a]_n$ имеет мультиPLICATIVНЫЙ обратный.

- (a) Предположим, что $x \in R_1$. Тогда $2 \leq x \leq n - 1$ и $[x]_n^{n-1} = [1]_n$. Поскольку $\{0, 1, \dots, n - 1\}$ – полная система вычетов по модулю n , существует единственный y такой, что $0 \leq y \leq n - 1$ и $ax \equiv y \pmod{n}$, поэтому $[a]_n \cdot [x]_n = [y]_n$. Мы должны доказать, что $y \in R_2$. Если $y = 0$, то $[x]_n = [a]_n^{-1} \cdot [1]_n = [a]_n^{-1} \neq [1]_n$, что противоречит тому, что $2 \leq x \leq n - 1$. Следовательно, $1 \leq y \leq n - 1$ и $[y]_n^{n-1} = [a]_n^{n-1} \cdot [x]_n^{n-1} = [a]_n^{n-1} \cdot [1]_n = [a]_n^{n-1} \neq [1]_n$. Значит, $y^{n-1} \not\equiv 1 \pmod{n}$. Отсюда следует, что $y \neq 1$, поэтому $2 \leq y \leq n - 1$.
- (b) Предположим, что $f(x_1) = f(x_2) = y$. Тогда $[a]_n \cdot [x_1]_n = [y]_n = [a]_n \cdot [x_2]_n$, поэтому $[x_1]_n = [a]_n^{-1} \cdot [y]_n = [x_2]_n$, и, следовательно, $x_1 = x_2$.
- (c) Согласно части (b), R_1 имеет то же количество элементов, что и $\text{Ran}(f)$. Так как $\text{Ran}(f) \subseteq R_2$, то R_2 имеет не менее того же количества элементов, что и R_1 . Таким образом, не менее половины элементов R лежат в R_2 .

Решения к главе 8

Раздел 8.1

1. (a) Определите $f: \mathbb{Z}^+ \rightarrow \mathbb{N}$ по формуле $f(n) = n - 1$. Легко проверить, что f взаимно однозначна и сюръективна.
- (b) Пусть $E = \{n \in \mathbb{Z} \mid n \text{ четно}\}$; определим $f: \mathbb{Z} \rightarrow E$ по формуле $f(n) = 2n$. Легко проверить, что f взаимно однозначна и сюръективна, поэтому $\mathbb{Z} \sim E$. Но мы уже знаем, что $\mathbb{Z}^+ \sim \mathbb{Z}$, поэтому по теореме 8.1.3 $\mathbb{Z}^+ \sim E$, а значит, E исчислимо.
4. (a) Нет. Контрпример: пусть $A = B = C = \mathbb{Z}^+$ и $D = \{1\}$.
- (b) Нет. Контрпример: пусть $A = B = N$, $C = \mathbb{Z}^-$ и $D = \emptyset$.
6. (a) Докажем, что $\forall n \in \mathbb{N} \forall m \in \mathbb{N} (I_n \sim I_m \rightarrow n = m)$ при помощи индукции по n .

Базовый случай: $n = 0$. Предположим, что $m \in \mathbb{N}$ и существует взаимно однозначная сюръективная функция $f: I_n \rightarrow I_m$. Поскольку $n = 0$, $I_n = \emptyset$. Но тогда, поскольку f сюръективна, мы также должны иметь $I_m = \emptyset$, поэтому $m = 0 = n$.

Шаг индукции: предположим, что $n \in \mathbb{N}$, и для всех $m \in \mathbb{N}$ если $I_n \sim I_m$, то $n = m$. Теперь предположим, что $m \in \mathbb{N}$ и $I_{n+1} \sim I_m$. Пусть $f: I_{n+1} \rightarrow$

I_m – взаимно однозначная сюръективная функция. Пусть $k = f(n + 1)$, и обратите внимание, что $1 \leq k \leq m$, поэтому значение m положительно. Учитывая тот факт, что f сюръективна, выберем некоторое число $j \leq n + 1$ такое, что $f(j) = m$.

Теперь определим функцию $g: I_n \rightarrow I_{m-1}$ следующим образом:

$$g(i) = \begin{cases} f(i), & \text{если } i \neq j \\ k, & \text{если } i = j \end{cases}.$$

Самостоятельно убедитесь, что g взаимно однозначна и сюръективна. Из предположения индукции следует, что $n = m - 1$, поэтому $n + 1 = m$.

- (b) Предположим, что множество A конечно. Тогда из определения конечности мы знаем, что существует хотя бы одно число $n \in \mathbb{N}$ такое, что $I_n \sim A$. Чтобы убедиться в его уникальности, предположим, что n и m – натуральные числа, $I_n \sim A$ и $I_m \sim A$. Тогда по теореме 8.1.3 $I_n \sim I_m$, поэтому согласно части (a) $n = m$.
8. (a) Воспользуемся индукцией по n .
- Базовый случай: $n = 0$. Предположим, что $A \subseteq I_0 = \emptyset$. Тогда $A = \emptyset$, поэтому $|A| = 0$.
- Шаг индукции. Предположим, что $n \in \mathbb{N}$ и для всех $A \subseteq I_n$ множество A конечно, $|A| \leq n$, и если $A \neq I_n$, то $|A| < n$. Теперь предположим, что $A \subseteq I_{n+1}$. Если $A = I_{n+1}$, то, очевидно, $A \sim I_{n+1}$, поэтому A конечно и $|A| = n + 1$. Теперь предположим, что $A \neq I_{n+1}$. Если $n + 1 \notin A$, то $A \subseteq I_n$, поэтому по предположению индукции множество A конечно и $|A| \leq n$. Если $n + 1 \in A$, то должно быть некоторое $k \in I_n$ такое, что $k \notin A$. Пусть $A' = (A \cup \{k\}) \setminus \{n + 1\}$. Тогда, сопоставив k с $n + 1$, легко показать, что $A' \sim A$. Кроме того, $A' \subseteq I_n$, поэтому по предположению индукции A' конечно и $|A'| \leq n$. Следовательно, согласно упражнению 7 множество A конечно и $|A| \leq n$.
- (b) Предположим, что множество A конечно и $B \subseteq A$. Пусть $n = |A|$ и функция $f: A \rightarrow I_n$ взаимно однозначна и сюръективна. Тогда $f(B) \subseteq I_n$, поэтому согласно части (a) $f(B)$ конечно, $|f(B)| \leq n$, и если $B \neq A$, то $f(B) \neq I_n$, поэтому $|f(B)| < n$. Поскольку $B \sim f(B)$, отсюда следует искомый вывод.

10. Подсказка: определите функцию $g: B \rightarrow I_n$ по формуле

$$g(x) = \text{наименьшее } i \in I_n \text{ такое, что } f(i) = x,$$

и покажите, что g взаимно однозначна.

12. Сначала обратите внимание, что либо $i + j - 2$, либо $i + j - 1$ четно, поэтому $f(i, j)$ является натуральным числом, и, следовательно, f является функцией от $\mathbb{Z}^+ \times \mathbb{Z}^+$ к \mathbb{Z}^+ , как заявлено. Будет полезно проверить два факта о функции f . Оба приведенных ниже факта можно проверить с помощью простых алгебраических выкладок.

- (a) Для всех $j \in \mathbb{Z}^+$, $f(1, j + 1) - f(1, j) = j$.

- (b) Для всех $i \in \mathbb{Z}^+$ и $j \in \mathbb{Z}^+$, $f(1, i + j - 1) \leq f(i, j) < f(1, i + j)$. Отсюда следует, что $i + j$ – наименьшее $k \in \mathbb{Z}^+$ такое, что $f(i, j) < f(1, k)$. Чтобы убедиться, что f взаимно однозначна, предположим, что $f(i_1, j_1) = f(i_2, j_2)$. Тогда в соответствии с приведенным выше фактом (b):

$$\begin{aligned} i_1 + j_1 &= \text{наименьшее } k \in \mathbb{Z}^+ \text{ такое, что } f(i_1, j_1) < f(1, k) \\ &= \text{наименьшее } k \in \mathbb{Z}^+ \text{ такое, что } f(i_2, j_2) < f(1, k) \\ &= i_2 + j_2. \end{aligned}$$

Из определения f следует, что

$$\begin{aligned} i_1 &= f(i_1, j_1) - \frac{(i_1 + j_1 - 2)(i_1 + j_1 - 1)}{2} \\ &= f(i_2, j_2) - \frac{(i_2 + j_2 - 2)(i_2 + j_2 - 1)}{2} \\ &= i_2. \end{aligned}$$

Но тогда, поскольку $i_1 = i_2$ и $i_1 + j_1 = i_2 + j_2$, должно выполняться равенство $j_1 = j_2$, поэтому $(i_1, j_1) = (i_2, j_2)$. Это доказывает, что f взаимно однозначна.

Чтобы доказать, что f сюръективна, предположим, что $n \in \mathbb{Z}^+$. Легко проверить, что $f(1, n + 1) > n$, поэтому мы можем принять за k наименьшее натуральное число такое, что $f(1, k) > n$. Обратите внимание, что $f(1, 1) = 1 \leq n$, поэтому $k \geq 2$. Поскольку k наименьшее, $f(1, k - 1) \leq n$, и поэтому из факта (a) следует, что

$$0 \leq n - f(1, k - 1) < f(1, k) - f(1, k - 1) = k - 1.$$

Добавляя 1 ко всем членам неравенства, получаем

$$1 \leq n - f(1, k - 1) + 1 < k.$$

Таким образом, если мы примем $i = n - f(1, k - 1) + 1$, то $1 \leq i < k$. Пусть $j = k - i$, и заметим, что $i \in \mathbb{Z}^+$ и $j \in \mathbb{Z}^+$. При таких значениях i и j мы имеем:

$$\begin{aligned} f(i, j) &= \frac{(i + j - 2)(i + j - 1)}{2} + i \\ &= \frac{(k - 2)(k - 1)}{2} + n - f(1, k - 1) + 1 \\ &= \frac{(k - 2)(k - 1)}{2} + n - \left[\frac{(k - 2)(k - 1)}{2} + 1 \right] + 1 = n. \end{aligned}$$

15. (a) Если $B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < n\} = \emptyset$, то $B \subseteq \{f(m) \mid m \in \mathbb{Z}^+, m < n\}$, поэтому согласно упражнениям 8 и 10 множество B конечно. Но мы предполагали, что B бесконечно, следовательно, это невозможно.
- (b) Используем сильную индукцию. Предположим, что $\forall m < n, f(m) \geq m$. Теперь предположим, что $f(n) < n$. Пусть $m = f(n)$. Тогда по пред-

положению индукции $f(m) \geq m$. Кроме того, по определению $f(n)$ $m = f(n) \in B \setminus \{f(k) \mid k \in \mathbb{Z}^+, k < n\} \subseteq B \setminus \{f(k) \mid k \in \mathbb{Z}^+, k < m\}$. Но поскольку $f(m)$ – наименьший элемент этого последнего множества, отсюда следует, что $f(m) \leq m$. Поскольку мы имеем одновременно $f(m) \geq m$ и $f(m) \leq m$, мы можем заключить, что $f(m) = m$. Но тогда $m \notin B \setminus \{f(k) \mid k \in \mathbb{Z}^+, k < n\}$, – получаем противоречие.

- (c) Предположим, что $i \in \mathbb{Z}^+, j \in \mathbb{Z}^+$ и $i \neq j$. Тогда либо $i < j$, либо $j < i$. Предположим сначала, что $i < j$. Тогда согласно определению $f(j)$ справедлива формула $f(j) \in B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < j\}$, и, очевидно, $f(i) \in \{f(m) \mid m \in \mathbb{Z}^+, m < j\}$. Отсюда следует, что $f(i) \neq f(j)$. Аналогичное рассуждение показывает, что если $j < i$, то $f(i) \neq f(j)$. Это доказывает, что f взаимно однозначна.

Чтобы доказать, что f сюръективна, предположим, что $n \in B$. Согласно части (b), $f(n+1) \geq n+1 > n$. Но, согласно определению f , $f(n+1)$ – наименьший элемент $B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < n+1\}$. Отсюда следует, что $n \notin B \setminus \{f(m) \mid m \in \mathbb{Z}^+, m < n+1\}$. Но $n \in B$, поэтому должно быть истинно утверждение $n \in \{f(m) \mid m \in \mathbb{Z}^+, m < n+1\}$. Другими словами, для некоторого положительного целого числа $m < n+1$ справедливо равенство $f(m) = n$.

17. Предположим, что $B \subseteq A$ и A счетно. Тогда по теореме 8.1.5 существует взаимно однозначная функция $f: A \rightarrow \mathbb{Z}^+$. Согласно упражнению 13 раздела 5.2, $f \upharpoonright B$ – это взаимно однозначная функция от B к \mathbb{Z}^+ , поэтому B счетно. (См. определение используемых здесь обозначений в упражнении 7 раздела 5.1.)
19. Следуя подсказке, мы рекурсивно определяем частичные порядки R_n для $n \in \mathbb{N}$, так что $R = R_0 \subseteq R_1 \subseteq R_2 \subseteq \dots$ и

$$\forall i \in I_n \quad \forall j \in \mathbb{Z}^+ ((a_i, a_j) \in R_n \vee (a_j, a_i) \in R_n). \quad (*)$$

Пусть $R_0 = R$. Нам дано R_n , для определения R_{n+1} применим упражнение 2 раздела 6.2, где $B = \{a_i \mid i \in I_{n+1}\}$. Наконец, пусть $T = \bigcup_{n \in \mathbb{N}} R_n$. Очевидно, что T рефлексивно, потому что рефлексивен каждый R_n . Чтобы доказать, что T транзитивно, предположим, что $(a, b) \in T$ и $(b, c) \in T$. Тогда для некоторых натуральных чисел m и n $(a, b) \in R_m$ и $(b, c) \in R_n$. Если $m \leq n$, то $R_m \subseteq R_n$, поэтому $(a, b) \in R_n$ и $(b, c) \in R_n$. Так как R_n транзитивно, то $(a, c) \in R_n \subseteq T$. Аналогичное рассуждение показывает, что если $n < m$, то $(a, c) \in T$, значит, T транзитивно. Доказательство антисимметричности T проводится аналогично. Наконец, чтобы доказать, что T является полным порядком, предположим, что $x \in A$ и $y \in A$. Поскольку мы пронумеровали элементы A , мы знаем, что для некоторых натуральных чисел m и n выполняются равенства $x = a_m$ и $y = a_n$. Но тогда по формуле (*) мы знаем, что или (a_m, a_n) , или (a_n, a_m) является элементом R_n и, следовательно, также элементом T .

22. (a) Воспользуемся подсказкой в задании.

Базовый случай: $n = 0$. Предположим, что A и B – конечные множества и $|B| = 0$. Тогда $B = \emptyset$, поэтому $A \times B = \emptyset$ и $|A \times B| = 0 = |A| \cdot 0$.

Шаг индукции: пусть n – произвольное натуральное число, и предположим, что для всех конечных множеств A и B если $|B| = n$, то $A \times B$ конечно и $|A \times B| = |A| \cdot n$. Теперь предположим, что A и B – конечные множества и $|B| = n + 1$. Выберите элемент $b \in B$, и пусть $B' = B \setminus \{b\}$, множество из n элементов. Тогда $A \times B = A \times (B' \cup \{b\}) = (A \times B') \cup (A \times \{b\})$, и поскольку $b \notin B'$, то $A \times B'$ и $A \times \{b\}$ не пересекаются. По предположению индукции $A \times B'$ конечно и $|A \times B'| = |A| \cdot n$. Кроме того, нетрудно увидеть, что $A \sim A \times \{b\}$ – просто сопоставив каждый элемент $x \in A$ с $(x, b) \in A \times \{b\}$ – так что $A \times \{b\}$ конечно и $|A \times \{b\}| = |A|$. По теореме 8.1.7 следует, что $A \times B$ конечно и $|A \times B| = |A \times B'| + |A \times \{b\}| = |A| \cdot n + |A| = |A| \cdot (n + 1)$.

- (b) Чтобы заказать еду, вы называете элемент $A \times B$, где $A = \{\text{стейк, курица, свиные отбивные, креветки, спагетти}\}$ и $B = \{\text{мороженое, торт, пирог}\}$. Итак, количество сочетаний блюд $|A \times B| = |A| \cdot |B| = 5 \cdot 3 = 15$.
24. (a) Базовый случай: $n = 0$. Если $|A| = 0$, то $A = \emptyset$, поэтому $F = \{\emptyset\}$ и $|F| = 1 = 0!$.

Шаг индукции: предположим, что n – натуральное число, и искомый вывод верен для n . Пусть теперь A – множество из $n + 1$ элементов, и пусть $F = \{f \mid f$ взаимно однозначная сюръективная функция от I_{n+1} до $A\}$. Пусть $g: I_{n+1} \rightarrow A$ – взаимно однозначная сюръективная функция. Для каждого $i \in I_{n+1}$ пусть $A_i = A \setminus \{g(i)\}$, множество из n элементов, и пусть $F'_i = \{f \mid f$ является взаимно однозначной сюръективной функцией от I_n до $A_i\}$. По предположению индукции F_i конечно и $|F_i| = n!$. Теперь пусть $F'_i = \{f \in F \mid f(n + 1) = g(i)\}$. Определим функцию $h: F_i \rightarrow F'_i$ по формуле $h(f) = f \cup \{(n + 1, g(i))\}$. Можно легко показать, что h взаимно однозначна и сюръективна, поэтому F'_i конечно и $|F'_i| = |F_i| = n!$. Наконец, заметим, что $F = \bigcup_{i \in I_{n+1}} F'_i$ и $\forall i \in I_{n+1} \forall j \in I_{n+1} (i \neq j \rightarrow F'_i \cap F'_j = \emptyset)$. Из упражнения 21 следует, что F конечно и $|F| = \sum_{i=1}^{n+1} |F'_i| = (n + 1) \cdot n! = (n + 1)!$.

- (b) Подсказка: определите функцию $h: F \rightarrow L$ формулой $h(f) = \{(a, b) \in A \times A \mid f^{-1}(a) \leq f^{-1}(b)\}$. (Вы должны убедиться, что это множество является полным порядком на A .) Чтобы доказать, что h взаимно однозначна, предположим, что $f \in F, g \in F$ и $f \neq g$. Пусть i будет наименьшим элементом I_n , для которого $f(i) \neq g(i)$. Теперь покажем, что $(f(i), g(i)) \in h(f)$, но $(f(i), g(i)) \notin h(g)$, поэтому $h(f) \neq h(g)$. Чтобы доказать, что h сюръективна, предположим, что R – полный порядок на A . Определим функцию $g: A \rightarrow I_n$ формулой $g(a) = |\{x \in A \mid xRa\}|$. Затем покажите, что $\forall a \in A \forall b \in A (aRb \leftrightarrow g(a) \leq g(b))$, и используйте этот факт, чтобы показать, что $g^{-1} \in F$ и $h(g^{-1}) = R$.

- (c) $5! = 120$.
27. Базовый случай: $n = 1$. Тогда $I_n = \{1\}$, $P = \{\{1\}\}$ и $A_{\{1\}} = A_1$. Следовательно, $\left| \bigcup_{i \in I_n} A_i \right| = |A_1|$ и $\sum_{S \in P} (-1)^{|S|+1} |A_S| = (-1)^2 |A_{\{1\}}| = |A_1|$.

Шаг индукции: предположим, что принцип включения-исключения выполняется для n множеств, и предположим, что A_1, A_2, \dots, A_{n+1} – конечные

множества. Пусть $P_n = \mathcal{P}(I_n) \setminus \{\emptyset\}$ и $P_{n+1} = \mathcal{P}(I_{n+1}) \setminus \{\emptyset\}$. Используя упражнение 26(а), упражнение 23(а) раздела 3.4 и индуктивную гипотезу:

$$\begin{aligned} \left| \bigcup_{i \in I_{n+1}} A_i \right| &= \left| \left(\bigcup_{i \in I_n} A_i \right) \cup A_{n+1} \right| \\ &= \left| \bigcup_{i \in I_n} A_i \right| + |A_{n+1}| - \left| \left(\bigcup_{i \in I_n} A_i \right) \cap A_{n+1} \right| \\ &= \sum_{S \in P_n} (-1)^{|S|+1} |A_S| + |A_{n+1}| - \left| \bigcup_{i \in I_n} (A_i \cap A_{n+1}) \right|. \end{aligned}$$

Теперь заметьте, что для каждого $S \in P_n$:

$$\bigcup_{i \in S} (A_i \cap A_{n+1}) = \left(\bigcup_{i \in S} A_i \right) \cap A_{n+1} = A_{S \cup \{n+1\}}.$$

Следовательно, используя другое применение индуктивной гипотезы:

$$\left| \bigcup_{i \in I_n} (A_i \cap A_{n+1}) \right| = \sum_{S \in P_n} (-1)^{|S|+1} |A_{S \cup \{n+1\}}|.$$

Таким образом:

$$\begin{aligned} \left| \bigcup_{i \in I_{n+1}} A_i \right| &= \sum_{S \in P_n} (-1)^{|S|+1} |A_S| + |A_{\{n+1\}}| - \sum_{S \in P_n} (-1)^{|S|+1} |A_{S \cup \{n+1\}}| \\ &= \sum_{S \in P_n} (-1)^{|S|+1} |A_S| + (-1)^2 |A_{\{n+1\}}| + \sum_{S \in P_n} (-1)^{|S \cup \{n+1\}|+1} |A_{S \cup \{n+1\}}|. \end{aligned}$$

Наконец, обратите внимание, что есть три типа элементов P_{n+1} : те, которые являются элементами P_n , множества $\{n+1\}$ и множества вида $S \cup \{n+1\}$. Отсюда следует, что последняя формула выше – это просто $\sum_{S \in P_n} (-1)^{|S|+1} |A_S|$, к чему мы и стремились.

Раздел 8.2

1. (a) По теореме 8.1.6 \mathbb{Q} счетно. Если бы $\mathbb{R} \setminus \mathbb{Q}$ было счетным, то по теореме 8.2.1 $\mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q}) = \mathbb{R}$ было бы счетным, что противоречит теореме 8.2.6. Таким образом, $\mathbb{R} \setminus \mathbb{Q}$ должно быть несчетным.
(b) Пусть $A = \{\sqrt{2} + n \mid n \in \mathbb{Z}^+\}$. Нетрудно увидеть, что A и \mathbb{Q} не пересекаются, поскольку $\sqrt{2}$ иррационален, а множество A счетно. Теперь примените теоремы 8.1.6 и 8.2.1, чтобы доказать, что $A \cup \mathbb{Q}$ исчислимо и, следовательно, $A \cup \mathbb{Q} \sim A$. Наконец, заметим, что $\mathbb{R} = (\mathbb{R} \setminus (A \cup \mathbb{Q})) \cup (A \cup \mathbb{Q})$ и $\mathbb{R} \setminus \mathbb{Q} = (\mathbb{R} \setminus (A \cup \mathbb{Q})) \cup A$, и применим часть 2 теоремы 8.1.2.
5. Предположим, что $A \sim \mathcal{P}(A)$. Тогда существует функция $f: A \rightarrow \mathcal{P}(A)$, которая взаимно однозначна и сюръективна. Пусть $X = \{a \in A \mid a \notin f(a)\} \in \mathcal{P}(A)$. Поскольку f сюръективна, должен существовать некий элемент $a \in A$

такой, что $f(a) = X$. Но тогда согласно определению X : $a \in X$ тогда и только тогда, когда $a \notin f(a)$, поэтому $X \neq f(a)$ – получили противоречие.

8. Подсказка: определите функцию $f: \mathcal{P}(A) \times \mathcal{P}(B) \rightarrow \mathcal{P}(A \cup B)$ формулой $f(X, Y) = X \cup Y$ и докажите, что f взаимно однозначна и сюръективна.
 10. Для каждого натурального числа n пусть $A_n = \{x \in A \mid x \geq 1/n\}$. Очевидно, что $\bigcup_{n \in \mathbb{Z}^+} A_n \subseteq A$. Теперь возьмем элемент $x \in A$. Тогда $x \in \mathbb{R}^+$, так что $x > 0$. Пусть n – натуральное число, достаточно большое, чтобы $n \geq 1/x$. Тогда $x \geq 1/n$, поэтому $x \in A_n$. Мы приходим к выводу, что $A \subseteq \bigcup_{n \in \mathbb{Z}^+} A_n$, и поэтому $\bigcup_{n \in \mathbb{Z}^+} A_n = A$.
- Предположим, что a_1, a_2, \dots, a_k – различные элементы A_n . Тогда
- $$b \geq a_1 + a_2 + \dots + a_k \geq \frac{1}{n} + \frac{1}{n} + \dots + \frac{1}{n} = \frac{k}{n},$$
- так что $k \leq bn$. Следовательно, A_n конечно, и фактически $|A_n| \leq bn$. По теореме 8.2.2 отсюда следует, что множество $A = \bigcup_{n \in \mathbb{Z}^+} A_n$ счетно.
13. Подсказка: сначала обратите внимание, что если $\mathcal{F} = \emptyset$, то g может быть любой функцией. Если $\mathcal{F} \neq \emptyset$, то, поскольку \mathcal{F} счетно, мы можем записать его элементы в виде списка $\mathcal{F} = \{f_1, f_2, \dots\}$. Теперь определим функцию $g: \mathbb{Z}^+ \rightarrow \mathbb{R}$ формулой $g(n) = \max\{|f_1(n)|, |f_2(n)|, \dots, |f_n(n)|\}$.
 15. (a) Если Q счетно, то согласно части 2 теоремы 8.2.1 $P \cup Q$ счетно. Но $P \cup Q = \mathcal{P}(\mathbb{Z}^+)$, что неисчислимо по теореме Кантора. Следовательно, Q неисчислимо.
 - (b) Предположим, что $A \in Q$. Для любого $n \in \mathbb{Z}^+$ действительна формула $A \cap I_n \subseteq I_n$, поэтому согласно упражнению 8 (а) в разделе 8.1 $A \cap I_n$ конечно. Следовательно, $S_A \subseteq P$. Предположим, что S_A конечно. Тогда существует некоторое натуральное число n такое, что $S_A = \{A \cap I_1, A \cap I_2, \dots, A \cap I_n\}$. Теперь мы утверждаем, что $A \subseteq I_n$; это завершит доказательство, поскольку из этого утверждения следует, что A конечно. Это противоречит нашему предположению, что $A \in Q$. Чтобы доказать это утверждение, предположим, что $m \in A$. Тогда $A \cap I_m \in S_A$, так что существует некоторое число $k \leq n$ такое, что $A \cap I_m = A \cap I_k \subseteq I_k \subseteq I_n$. Но $m \in A \cap I_m$, поэтому заключаем, что $m \in I_n$, как и требовалось.
 - (c) Предположим, что $A \in Q, B \in Q$ и $A \neq B$. Тогда существует некоторое натуральное число n такое, что или $n \in A$ и $n \notin B$, или $n \in B$ и $n \notin A$. Предположим, что $n \in A$ и $n \notin B$; доказательство для другого случая аналогично. Далее мы утверждаем, что $S_A \cap S_B \subseteq \{A \cap I_1, A \cap I_2, \dots, A \cap I_{n-1}\}$; это утверждение завершает доказательство, поскольку из него следует конечность $S_A \cap S_B$. Для доказательства утверждения предположим, что $X \in S_A \cap S_B$. Тогда существуют натуральные числа n_A и n_B такие, что $X = A \cap I_{n_A}$ и $X = B \cap I_{n_B}$. Если $n_A \geq n$, то

$$n \in A \cap I_{n_A} = X = B \cap I_{n_B} \subseteq B,$$

что является противоречием. Следовательно, $n_A < n$, поэтому $X = A \cap I_{n_A} \in \{A \cap I_1, \dots, A \cap I_{n-1}\}$, как и требовалось.

- (d) Если $A \in Q$, то $S_A \subseteq P$, и поскольку $g: P \rightarrow \mathbb{Z}^+$, то $g(S_A) \subseteq \mathbb{Z}^+$. Кроме того, поскольку S_A бесконечно, а g взаимно однозначна, $g(S_A)$ также бесконечна. Это доказывает, что $\mathcal{F} \subseteq \mathcal{P}(\mathbb{Z}^+)$ и каждый элемент \mathcal{F} бесконечен. Чтобы показать, что \mathcal{F} попарно почти не пересекается, предположим, что $X, Y \in \mathcal{F}$ и $X \neq Y$. Тогда существуют множества $A, B \in Q$ такие, что $X = g(S_A)$ и $Y = g(S_B)$. Поскольку $X \neq Y$, $A \neq B$, то согласно части (c) данного упражнения $S_A \cap S_B$ конечно, а значит, $g(S_A \cap S_B)$ конечно. По теореме 5.5.2 $g(S_A \cap S_B) = g(S_A) \cap g(S_B) = X \cap Y$, поэтому множества X и Y почти не пересекаются. Наконец, определим функцию $h: Q \rightarrow \mathcal{F}$ формулой $h(A) = g(S_A)$. Легко проверить, что h взаимно однозначна и сюръективна, поэтому $\mathcal{F} \sim Q$ и, следовательно, согласно части (a), \mathcal{F} неисчислимо.

Раздел 8.3

1. (a) Функция $i_A: A \rightarrow A$ взаимно однозначна.
 (b) Предположим, что $A \lesssim B$ и $B \lesssim C$. Тогда существуют взаимно однозначные функции $f: A \rightarrow B$ и $g: B \rightarrow C$. Согласно пункту 1 теоремы 5.2.5 $g \circ f: A \rightarrow C$ взаимно однозначна, поэтому $A \lesssim C$.
5. Пусть $g: A \rightarrow B$ и $h: C \rightarrow D$ – взаимно однозначные функции.
 (a) Так как $A \neq \emptyset$, мы можем выбрать некоторый элемент $a_0 \in A$. Заметим, что $g^{-1}: \text{Ran}(g) \rightarrow A$. Определим $j: B \rightarrow A$ следующим образом:

$$j(b) = \begin{cases} g^{-1}(b), & \text{если } b \in \text{Ran}(g) \\ a_0 & \text{в остальных случаях} \end{cases}.$$

Самостоятельно убедитесь, что функция j сюръективна.

Теперь определим $F: {}^AC \rightarrow {}^BD$ по формуле $F(f) = h \circ f \circ j$. Чтобы убедиться, что F взаимно однозначна, предположим, что $f_1 \in AC$, $f_2 \in AC$ и $F(f_1) = F(f_2)$, то есть $h \circ f_1 \circ j = h \circ f_2 \circ j$. Возьмем произвольный элемент $a \in A$. Поскольку j сюръективна, существует некоторый элемент $b \in B$ такой, что $j(b) = a$. Следовательно, $h(f_1(a)) = (h \circ f_1 \circ j)(b) = (h \circ f_2 \circ j)(b) = h(f_2(a))$, и поскольку h взаимно однозначна, из этого следует, что $f_1(a) = f_2(a)$. Поскольку элемент a был выбран произвольно, это показывает, что $f_1 = f_2$.

- (b) Да. (Самостоятельно обоснуйте этот ответ контрпримером.)
8. (a) Возьмем произвольное число n , затем проведем индукцию по m . Базовый случай – $m = n + 1$, и он рассмотрен в упражнении 7. Для шага индукции примените упражнение 2(b).
 (b) $\bigcup_{n \in \mathbb{Z}} A_n$ – бесконечное множество, не равномощное множеству A_n для любого $n \in \mathbb{Z}^+$. Фактически для любого положительного целого числа n справедливо $A_n \prec \bigcup_{n \in \mathbb{Z}^+} A_n$. Можете ли вы найти еще большие бесконечные множества?
10. (a) Заметьте, что $\mathcal{E} \subseteq \mathcal{P}(\mathbb{Z}^+ \times \mathbb{Z}^+)$. Из упражнения 5 раздела 8.1 следует, что $\mathcal{E} \lesssim \mathcal{P}(\mathbb{Z}^+ \times \mathbb{Z}^+) \sim \mathcal{P}(\mathbb{Z}^+)$.

- (b) Предположим, что $f(X) = f(Y)$. Тогда $X \cup \{1\} \in f(X) = f(Y) = \{Y \cup \{1\}, (A \setminus Y) \cup \{2\}\}$, поэтому либо $X \cup \{1\} = Y \cup \{1\}$, либо $X \cup \{1\} = (A \setminus Y) \cup \{2\}$. Но очевидно, что $2 \notin X \cup \{1\}$, так что вторую возможность можно исключить. Следовательно, $X \cup \{1\} = Y \cup \{1\}$. Поскольку ни X , ни Y не включают 1, отсюда следует, что $X = Y$.
- (c) Ясно, что A исчислимо, и в конце раздела 5.3 мы показали, что $\wp \sim \mathcal{E}$. Отсюда следует, что $\mathcal{P}(\mathbb{Z}^+) \sim \mathcal{P}(A) \precsim \wp \sim \mathcal{E}$. Объединяя это с частью (a) и применяя теорему Кантора–Шредера–Бернштейна, получаем желаемый вывод.
14. (a) Согласно определению функции $\mathbb{R}\mathbb{R} \subseteq \mathcal{P}(\mathbb{R} \times \mathbb{R})$, и, следовательно, исходя из упражнения 12 (b) и упражнения 5 раздела 8.1, $\mathbb{R}\mathbb{R} \precsim \mathcal{P}(\mathbb{R} \times \mathbb{R}) \sim \mathcal{P}(\mathbb{R})$.
 Ясно, что $\{\text{да, нет}\} \precsim \mathbb{R}$, поэтому в упражнении 6 (c) раздела 8.2 и упражнении $\mathcal{P}(\mathbb{R}) \sim \mathbb{R}\{\text{да, нет}\} \precsim \mathbb{R}\mathbb{R}$. Поскольку у нас как $\mathbb{R}\mathbb{R} \precsim \mathcal{P}(\mathbb{R})$, так и $\mathcal{P}(\mathbb{R}) \precsim \mathbb{R}\mathbb{R}$, по теореме Кантора–Шредера–Бернштейна $\mathbb{R}\mathbb{R} \sim \mathcal{P}(\mathbb{R})$.
- (b) Согласно теоремам 8.1.6 и 8.3.3, упражнению 23(a) раздела 8.1 и упражнению 6(d) раздела 8.2, $\mathbb{Q}\mathbb{R} \sim \mathbb{Z}^+ \mathcal{P}(\mathbb{Z}^+) \sim \mathcal{P}(\mathbb{Z}^+) \sim \mathbb{R}$.
- (c) Определим $F: \mathcal{C} \rightarrow \mathbb{Q}\mathbb{R}$ формулой $F(f) = f \upharpoonright \mathbb{Q}$. (Определения используемых здесь обозначений даны в упражнении 7 раздела 5.1.1.) Предположим, что $f \in \mathcal{C}$, $g \in \mathcal{C}$ и $F(f) = F(g)$. Тогда $f \upharpoonright \mathbb{Q} = g \upharpoonright \mathbb{Q}$, что означает, что для всех $x \in \mathbb{Q}$ $f(x) = g(x)$. Пусть теперь x – произвольное действительное число. Воспользуйтесь леммой 8.3.4, чтобы построить последовательность x_1, x_2, \dots рациональных чисел таких, что $\lim_{n \rightarrow \infty} x_n = x$. Тогда, поскольку f и g непрерывны, $f(x) = \lim_{n \rightarrow \infty} f(x_n) = \lim_{n \rightarrow \infty} g(x_n) = g(x)$. Поскольку x взят произвольно, это показывает, что $f = g$. Следовательно, F взаимно однозначна, поэтому $\mathcal{C} \precsim \mathbb{Q}\mathbb{R}$. Комбинируя этот вывод с частью (b), мы можем заключить, что $\mathcal{C} \precsim \mathbb{R}$.
 Теперь определим $G: \mathbb{R} \rightarrow \mathcal{C}$ формулой $G(x) = \mathbb{R} \times \{x\}$. Другими словами, $G(x)$ – это постоянная функция, значение которой для каждого действительного числа равно x . Ясно, что G взаимно однозначна, так что $\mathbb{R} \precsim \mathcal{C}$. По теореме Кантора–Шредера–Бернштейна следует, что $\mathcal{C} \sim \mathbb{R}$.

Дополнительные материалы

1. Barker-Plummer, D., Barwise, J., and Etchemendy, J., *Language, Proof and Logic*, 2nd edition. Stanford: CSLI Publications, 2011.
2. Burton, D., *Elementary Number Theory*, 7th edition. Boston: McGraw-Hill, 2011.
3. Eccles, P., *An Introduction to Mathematical Reasoning: Numbers, Sets and Functions*. Cambridge: Cambridge University Press, 1997.
4. Enderton, H., *A Mathematical Introduction to Logic*, 2nd edition. San Diego: Harcourt/Academic Press, 2001.
5. Enderton, H., *Elements of Set Theory*. San Diego: Academic Press, 1977.
6. Epp, S., *Discrete Mathematics: An Introduction to Mathematical Reasoning*. Boston: Brooks/Cole Cengage Learning, 2011.
7. Halmos, P., *Naive Set Theory*. Mineola, New York: Dover Publications, 2017.
8. Hamilton, A., *Logic for Mathematicians*, revised edition. Cambridge: Cambridge University Press, 1988.
9. Hamilton, A., *Numbers, Sets and Axioms: The Apparatus of Mathematics*. Cambridge: Cambridge University Press, 1982.
10. Leary, C. and Kristiansen, L., *A Friendly Introduction to Mathematical Logic*, Geneseo, New York: Milne Library, 2015.
11. Mendelson, E., *Introduction to Mathematical Logic*, 6th edition. Boca Raton, Florida: CRC Press, 2015.
12. Polya, G., *How to Solve It: A New Aspect of Mathematical Method*, 2nd edition. Princeton: Princeton University Press, 2014.
13. Rosen, K., *Discrete Mathematics and Its Applications*, 7th edition. New York: McGraw-Hill, 2012.
14. Rosen, K., *Elementary Number Theory and its Applications*, 6th edition. Boston: Pearson, 2010.
15. Silverman, J., *A Friendly Introduction to Number Theory*, 4th edition. Boston: Pearson, 2012.
16. van Dalen, D., Doets, H., and deSwart, H., *Sets: Naive, Axiomatic, and Applied*, Oxford: Pergamon Press, 1978.

Краткое изложение методов доказательства

Чтобы доказать цель следующего вида:

1. $\neg P$:
 - (a) повторно выразите утверждение как положительное;
 - (b) используйте доказательство от противного; то есть предположите, что P истинно, и попытайтесь прийти к противоречию.
2. $P \rightarrow Q$:
 - (a) предположите, что P истинно, и докажите Q ;
 - (b) докажите контрапозицию; то есть предположите, что Q ложно, и докажите, что P ложно.
3. $P \wedge Q$:
докажите по отдельности P и Q . Другими словами, рассматривайте их как две отдельные цели P и Q .
4. $P \vee Q$:
 - (a) предположите, что P ложно, и докажите Q , или предположите, что Q ложно, и докажите P ;
 - (b) используйте раздельное доказательство по случаям. В каждом случае либо докажите P , либо докажите Q .
5. $P \leftrightarrow Q$:
докажите $P \rightarrow Q$ и $Q \rightarrow P$, используя методы, перечисленные в п. 2.
6. $\forall x P(x)$:
обозначьте за x произвольный объект и докажите $P(x)$. (Если буква x уже обозначает что-то в доказательстве, вам придется использовать другую букву для обозначения произвольного объекта.)
7. $\exists x P(x)$:
найдите значение x , которое делает $P(x)$ истинным. Докажите $P(x)$ для этого значения x .
8. $\exists! x P(x)$:
 - (a) докажите $\exists x P(x)$ (существование) и $\forall y \forall z ((P(y) \wedge P(z)) \rightarrow y = z)$ (единственность);
 - (b) докажите эквивалентное утверждение $\exists x (P(x) \wedge \forall y (P(y) \rightarrow y = x))$.
9. $\forall n \in \mathbb{N} P(n)$:
 - (a) математическая индукция: докажите $P(0)$ (базовый случай) и $\forall n \in \mathbb{N} (P(n) \rightarrow P(n + 1))$ (шаг индукции);
 - (b) сильная индукция. Докажите, что $\forall n \in \mathbb{N} [(\forall k < n P(k)) \rightarrow P(n)]$.

Чтобы использовать исходные посылки следующего вида:

1. $\neg P$:

- (a) повторно выразите цель как положительное утверждение;
- (b) при доказательстве от противного вы можете прийти к противоречию, доказав P .

2. $P \rightarrow Q$:

- (a) если вам также дано P или вы можете доказать, что P истинно, вы можете сделать вывод, что Q истинно;
- (b) используйте контрапозицию: если вам дано (или вы можете доказать), что Q ложно, тогда вы можете сделать вывод, что P ложно.

3. $P \wedge Q$:

считайте это двумя исходными посылками P и Q .

4. $P \vee Q$:

- (a) используйте доказательство по случаям. В случае 1 предположите, что P истинно, а в случае 2 предположите, что Q истинно;
- (b) если вам также дано, что P ложно, или вы можете доказать, что P ложно, то вы можете заключить, что Q истинно. Точно так же, если вы знаете, что Q ложно, вы можете заключить, что P истинно.

5. $P \leftrightarrow Q$:

считайте это двумя исходными посылками: $P \rightarrow Q$ и $Q \rightarrow P$.

6. $\forall x P(x)$:

вы можете подставить вместо x произвольное значение, например a , и сделать вывод, что $P(a)$ истинно.

7. $\exists x P(x)$:

введите в доказательство новую переменную, скажем x_0 , чтобы обозначать конкретный объект, для которого истинно утверждение $P(x_0)$.

8. $\exists! x P(x)$:

введите в доказательство новую переменную, скажем x_0 , чтобы обозначать конкретный объект, для которого истинно утверждение $P(x_0)$. Вы также можете предположить, что $\forall y (P(y) \rightarrow y = x_0)$.

Приемы, которые можно использовать в любом доказательстве:

1. Доказательство от противного: предположите, что цель ложна, и придите к противоречию.
2. Доказательство по случаям. Рассмотрите несколько случаев, которые являются исчерпывающими, то есть включают все возможности. Докажите цель в каждом конкретном случае.

Предметный указатель

А

Алгоритм
деления, 298
Евклида, 320
расширенный, 322
с наименьшим остатком, 324

Антецедент, 53

Б

Биекция, 242

В

Вершина, 191
Возможность, 18

Г

Гипотеза, 12, 94
континуума, 382

Граница
верхняя, 207
наименьшая, 207
нижняя, 207
наибольшая, 168, 207
точная, 207

Д

Дедуктивное мышление, 11
Декартово произведение, 175
Делители, 317
общие, 317
наибольшие, 317

Диагонализация, 374

Диаграмма Венна, 44

Дизъюнкция, 19

Длина последовательности, 372

Доказательство, 11

Допущение, 17

З

Заключение, 17

Золотое сечение, 309

И

Индекс, 83

Индукция
математическая, 267
базовый случай, 267
предположение (гипотеза), 270
шаг, 267
сильная, 297

К

Квантор, 65
существования, 65
универсальный, 65

Класс эквивалентности, 214

Композиция, 183

Конечная последовательность, 372

Контрапозиция, 59

Контрпример, 12

Конъюнкция, 19

Криптография
симметричная, 350
с открытым ключом, 350

Л

Лемма, 217

Линейная комбинация чисел, 321

М

Множество, 35
бесконечное, 361
замкнутое, 254
замыкание, 255
значений, 183
индексное, 83
интервал, 383
истинности, 38, 179
исчислимое, 364
конечное, 361

- м**
- мощность, 362
 - несчетное, 364
 - нулевое, 41
 - образ, 262
 - объединение, 43
 - пересечение, 43
 - прообраз, 263
 - пустое, 41
 - равномощное, 361
 - разность, 43
 - семейство множеств, 84
 - симметричная разность, 45
 - соответствие множеств, 182
 - степенное, 85
 - счетное, 364
 - элемент
 - максимальный, 207
 - минимальный, 202
 - наибольший, 207
 - наименьший, 201
- Н**
- Наименьшее общее кратное, 329
- О**
- Область определения, 183
 - Обратное соответствие, 183
 - Обращение, 59
 - Ограничение, 233
 - Ориентированный граф, 193
 - Отношение
 - антисимметричное, 199
 - бинарное, 192
 - замыкание
 - симметричное, 212
 - транзитивное, 212
 - петля, 193
 - полный порядок, 199
 - предпорядок, 225
 - рефлексивное, 193
 - симметричное, 194
 - тождества, 193
 - транзитивное, 194
 - частичный порядок, 199
 - эквивалентности, 213
 - Отрицание, 19
- П**
- Парадокс Рассела, 92
 - Переменная
 - свободная, 37
 - связанная (фиксивная), 37
 - Подмножество, 49
 - Подтверждение
 - универсальное, 123
 - экзистенциальное, 123
 - Порядок
 - строгий
 - полный, 213
 - частичный, 213
 - Последовательность
 - Гибонауччи, 306
 - Фибонауччи, обобщенная, 306
 - Посылка. См. Допущение
 - Правила вывода, 111
 - modus ponens, 111
 - modus tollens, 111
 - Правило вывода
 - дизьюктивный силлогизм, 151
 - Принцип
 - включения-исключения, 369
 - Дирихле, 367
 - карточки. См. Принцип Дирихле
 - полного упорядочивания, 303
 - Простые множители.
 - См. Факторизация
 - Противопоставление.
 - См. Контрапозиция
- Р**
- Равносильность. См. Утверждение
 - биусловное
 - Разбиение, 214
 - Расстояние, 316
 - Ребро, 191
- С**
- Связка, 19
 - Семейство индексированное, 83
 - Система вычетов полная, 334
 - Следствие, 53
 - Соединительный символ. См. Связка
 - Соответствие взаимно однозначное, 242

-
- С**
- Среднее
 - арифметическое, 283
 - гармоническое, 284
 - геометрическое, 284
- Т**
- Теорема, 13, 94
 - арифметики, основная, 327
 - биномиальная, 296
 - доказательство, 94
 - исходные посылки, 97
 - Кантора–Шредера–Бернштейна, 378
 - контрпример, 94
 - цель, 97
 - Тест
 - Миллера–Рабина, 360
 - Ферма на простоту, 358
 - Тотиент. См. Функция Эйлера
 - Треугольник Паскаля, 296
- У**
- Универсум, 39
 - Упорядоченная пара, 174
 - Условие, 53
 - Утверждение
 - биусловное, 61, 134
 - пустое истинное, 79
- Ф**
- Факториал, 15, 288
 - Факторизация, 325
 - Функция, 226
 - взаимно однозначная, 236
 - двух переменных, 258
 - инъекция, 236
 - мультипликативная, 345
 - периодическая точка, 315
 - постоянная, 235
 - рекурсивное определение, 288
 - совместная, 235
 - строго возрастающая, 261
 - строго убывающая, 261
 - сюръекция, 236
 - тождества, 227
 - фиксированная точка, 254
 - Эйлера, 342
- Ц**
- Цифровая подпись, 357
- Ч**
- Число
 - алгебраическое, 376
 - биномиальный коэффициент, 296
 - взаимно простое, 325
 - гармоническое, 294
 - Гильберта, 331
 - простое, 331
 - дружественное, 16
 - Кармайкла, 359
 - Лукаса, 307
 - нечетное, 134
 - простое, 11
 - близнецы, 16
 - Мерсенна, 14
 - свидетели
 - Миллера–Рабина, 360
 - Ферма, 358
 - совершенное, 14
 - составное, 11
 - Фибоначчи, 300
 - четное, 134

Книги издательства «ДМК ПРЕСС»
можно купить оптом и в розницу
в книготорговой компании «Галактика»
(представляет интересы издательств
«ДМК ПРЕСС», «СОЛОН ПРЕСС», «КТК Галактика»).
Адрес: г. Москва, пр. Андропова, 38;
тел.: (499) 782-38-89, электронная почта: books@aliens-kniga.ru.
При оформлении заказа следует указать адрес (полностью),
по которому должны быть высланы книги;
фамилию, имя и отчество получателя.
Желательно также указать свой телефон и электронный адрес.
Эти книги вы можете заказать и в интернет-магазине: www.a-planeta.ru.

Дэниэл Веллеман

Искусство доказательства в математике

Главный редактор *Мовчан Д. А.*
dmkpress@gmail.com

Зам. главного редактора *Сенченкова Е. А.*
Перевод *Яценков В. С.*
Корректор *Синяева Г. И.*
Верстка *Чаннова А. А.*
Дизайн обложки *Мовчан А. Г.*

Гарнитура PT Serif. Печать цифровая.
Усл. печ. л. 36,08. Тираж 200 экз.

Веб-сайт издательства: www.dmkpress.com