

В. Б. Гисин

ДИСКРЕТНАЯ МАТЕМАТИКА

УЧЕБНИК И ПРАКТИКУМ ДЛЯ СПО

*Рекомендовано Учебно-методическим отделом среднего профессионального образования
в качестве учебника и практикума для студентов образовательных учреждений среднего
профессионального образования*

**Книга доступна в электронной библиотеке biblio-online.ru,
а также в мобильном приложении «Юрайт.Библиотека»**

Москва ■ Юрайт ■ 2019

УДК 51(075.32)
ББК 22.176я723
Г51

Автор:

Гисин Владимир Борисович — кандидат физико-математических наук, профессор, заведующий кафедрой «Математика» Департамента математики и информатики, член ученого совета факультета «Прикладная математика и информационные технологии», член ученого совета Финансового университета при Правительстве Российской Федерации.

Рецензенты:

Чечкин А. В. — доктор физико-математических наук, профессор кафедры «Математика» Департамента математики и информатики Финансового университета при Правительстве Российской Федерации;

Кудрявцев О. Е. — доктор физико-математических наук, доцент, профессор кафедры информатики и информационных таможенных технологий Ростовского филиала Российской таможенной академии.

Гисин, В. Б.

Г51 Дискретная математика : учебник и практикум для СПО / В. Б. Гисин. — М. : Издательство Юрайт, 2019. — 383 с. — (Серия : Профессиональное образование).

ISBN 978-5-534-11633-5

Математику традиционно делят на непрерывную и дискретную. К непрерывной математике относят то, что в той или иной форме опирается на идеи предела и непрерывности. Дискретная математика изучает те математические объекты, в которых дискретность, проявляющаяся в строении объекта и в динамике его изменения, является определяющей характеристикой.

В учебнике изложены традиционные разделы дискретной математики: множества и отношения, математическая логика, комбинаторика, графы, алгоритмы, кодирование. Первые четыре раздела составляют ядро стандартной подготовки по дискретной математике. Они могут быть дополнены главами из раздела V для тех, кто специализируется в социально-экономических дисциплинах, или главами из раздела VI для тех, кто обучается по направлениям, связанным с изучением информатики.

Соответствует актуальным требованиям Федерального государственного образовательного стандарта среднего профессионального образования и профессиональным требованиям.

Книга будет полезна студентам и практикующим специалистам.

УДК 51(075.32)

ББК 22.176я723



Все права защищены. Никакая часть данной книги не может быть воспроизведена в какой бы то ни было форме без письменного разрешения владельцев авторских прав. Правовую поддержку издательства обеспечивает юридическая компания «Дельфи».

ISBN 978-5-534-11633-5

© Гисин В. Б., 2016

© ООО «Издательство Юрайт», 2019

Оглавление

Предисловие	9
-------------------	---

Раздел I МНОЖЕСТВА И ОТНОШЕНИЯ

Глава 1. Множества.....	15
1.1. Понятие множества.....	15
1.2. Подмножества	17
1.3. Операции над множествами	18
1.4. Диаграммы Эйлера — Венна.....	20
1.5. Алгебра множеств	21
1.6. Прямое произведение множеств	22
1.7. Отображения и их свойства.....	23
1.7.1. Понятие отображения.....	23
1.7.2. Специальные виды отображений.....	24
1.7.3. Характеристические функции	25
1.7.4. Операции	26
Резюме	27
<i>Практикум</i>	<i>28</i>
<i>Задачи с решениями.....</i>	<i>28</i>
<i>Задания для самостоятельной работы.....</i>	<i>29</i>
Глава 2. Счетные множества	31
2.1. Мощность множества.....	31
2.2. Натуральный ряд	33
2.3. Метод математической индукции.....	35
2.4. Свойства счетных множеств	36
2.5. Диагональный метод Кантора.....	39
Резюме	40
<i>Практикум</i>	<i>41</i>
<i>Задачи с решениями.....</i>	<i>41</i>
<i>Задания для самостоятельной работы.....</i>	<i>45</i>
Глава 3. Отношения на множествах	47
3.1. Соответствия	47
3.2. Композиция соответствий.....	49
3.3. Бинарные отношения и их свойства.....	50
3.4. Отношения эквивалентности	52
Резюме	54
<i>Практикум</i>	<i>55</i>
<i>Задачи с решениями.....</i>	<i>55</i>
<i>Задания для самостоятельной работы.....</i>	<i>57</i>

Глава 4. Упорядоченные множества и решетки	59
4.1. Отношения порядка.....	59
4.2. Полурешетки и решетки	63
4.3. Булевы алгебры	65
Резюме	67
<i>Практикум</i>	<i>68</i>
<i>Задачи с решениями.....</i>	<i>68</i>
<i>Задания для самостоятельной работы.....</i>	<i>70</i>

Раздел II МАТЕМАТИЧЕСКАЯ ЛОГИКА

Глава 5. Логика высказываний.....	75
5.1. Высказывания и операции над ними.....	75
5.2. Формулы логики высказываний.....	76
5.3. Равносильность формул.....	78
5.4. Принцип двойственности	80
5.5. Тавтологически истинные формулы.....	81
5.6. Система натурального вывода	82
5.7. Метод резолюций.....	83
Резюме	85
<i>Практикум</i>	<i>85</i>
<i>Задачи с решениями.....</i>	<i>85</i>
<i>Задания для самостоятельной работы.....</i>	<i>87</i>
Глава 6. Логика предикатов	88
6.1. Понятие предиката.....	88
6.2. Логические операции над предикатами	90
6.3. Кванторы.....	91
6.4. Формулы логики предикатов и логические законы	93
6.5. Выполнимые формулы и проблема разрешения.....	95
6.6. Логика предикатов и математическая практика	96
Резюме	97
<i>Практикум</i>	<i>98</i>
<i>Задачи с решениями.....</i>	<i>98</i>
<i>Задания для самостоятельной работы.....</i>	<i>99</i>
Глава 7. Формальные теории	101
7.1. Формализация в математике.....	101
7.2. Логические исчисления	103
7.2.1. Исчисление высказываний.....	103
7.2.2. Исчисление предикатов	105
7.3. Теории первого порядка. Формальная арифметика.....	107
Резюме.....	110
<i>Практикум.....</i>	<i>111</i>
<i>Задачи с решениями</i>	<i>111</i>
<i>Задания для самостоятельной работы</i>	<i>111</i>
Глава 8. Булевы функции.....	113
8.1. Двоичные векторы	113
8.2. Понятие булевой функции.....	114
8.3. Булевы функции одной и двух переменных	115
8.4. Нормальные формы.....	117

8.5. Полные системы булевых функций.....	120
8.6. Важнейшие замкнутые классы булевых функций. Теорема Поста о полноте.....	121
8.7. Характеристические векторы подмножеств конечного множества	123
Резюме	125
<i>Практикум</i>	126
<i>Задачи с решениями</i>	126
<i>Задания для самостоятельной работы</i>	129

Раздел III КОМБИНАТОРИКА

Глава 9. Конечные множества и комбинаторика	135
9.1. Правило суммы и правило произведения	135
9.2. Принцип Дирихле	137
9.3. Размещения и перестановки.....	138
9.4. Сочетания.....	141
9.5. Свойства биномиальных коэффициентов.....	143
9.6. Принцип включения и исключения	145
Резюме	147
<i>Практикум</i>	147
<i>Задачи с решениями</i>	147
<i>Задания для самостоятельной работы</i>	149
Глава 10. Вероятность	151
10.1. Конечные вероятностные пространства	151
10.2. Пространство равновероятных исходов	153
10.3. Условная вероятность	155
10.4. Независимые события.....	157
10.5. Схема Бернулли.....	158
10.6. Случайные величины	160
10.7. Биномиальное распределение	162
10.8. Неравенство Чебышева. Закон больших чисел.....	163
Резюме	164
<i>Практикум</i>	165
<i>Задачи с решениями</i>	165
<i>Задания для самостоятельной работы</i>	167
Глава 11. Комбинаторный анализ	169
11.1. Степенные ряды.....	169
11.2. Биномиальный ряд.....	171
11.3. Производящие функции.....	174
11.4. Рекуррентные соотношения.....	177
11.5. Линейные рекуррентные соотношения.....	178
11.6. Производящие функции линейных рекуррентных последовательностей....	180
Резюме	184
<i>Практикум</i>	185
<i>Задачи с решениями</i>	185
<i>Задания для самостоятельной работы</i>	195
Глава 12. Числа Фибоначчи	197
12.1. Простейшие свойства	197
12.2. Формула Бине	198

12.3. Золотое сечение	201
12.4. Числа Фибоначчи и поиск экстремума.....	203
Резюме.....	210
<i>Практикум</i>	211
<i>Задачи с решениями</i>	211
<i>Задания для самостоятельной работы</i>	212

Раздел IV ГРАФЫ И ДЕРЕВЬЯ

Глава 13. Графы	215
13.1. Понятие графа.....	215
13.2. Маршруты, цепи и циклы	217
13.3. Эйлеровы цепи и циклы	219
13.4. Матрицы смежности и инцидентности.....	220
13.5. Бинарные отношения и графы	222
13.6. Порядковая функция графа	224
13.7. Внешняя и внутренняя устойчивость. Ядро	226
13.8. Планарные графы.....	231
Резюме.....	234
<i>Практикум</i>	235
<i>Задачи с решениями</i>	235
<i>Задания для самостоятельной работы</i>	240
Глава 14. Деревья.....	245
14.1. Понятие дерева.....	245
14.2. Остовное дерево связного графа	246
14.3. Ориентированные и упорядоченные деревья	248
14.4. Бинарные деревья	251
Резюме.....	253
<i>Практикум</i>	253
<i>Задачи с решениями</i>	253
<i>Задания для самостоятельной работы</i>	255

Раздел V МОДЕЛИ ДИСКРЕТНОЙ МАТЕМАТИКИ В ЭКОНОМИКЕ

Глава 15. Функции выбора.....	259
15.1. Понятие функции выбора.....	259
15.2. Примеры функций выбора	260
15.3. Логическое представление функций выбора	262
15.4. Основные свойства функций выбора	264
15.5. Логическое представление нормальных функций выбора	265
15.6. Логическое представление турнирных функций выбора.....	266
Резюме.....	268
<i>Практикум</i>	269
<i>Задачи с решениями</i>	269
<i>Задания для самостоятельной работы</i>	273
Глава 16. Дискретные модели принятия решений	276
16.1. Кооперативные игры.....	276
16.2. Решение Неймана — Моргенштерна.....	281
16.3. Устойчивые паросочетания.....	284
16.4. Отношения предпочтения.....	288

16.5. Теорема Эрроу.....	291
Резюме	296
<i>Практикум</i>	297
<i>Задачи с решениями</i>	297
<i>Задания для самостоятельной работы</i>	299
Глава 17. Биномиальная модель ценообразования.....	301
17.1. Биномиальная решетка	301
17.2. Опционы. Основные понятия.....	303
17.2.1. Однопериодная модель ценообразования опционов	304
17.2.2. Двух- и трехпериодные модели ценообразования опционов.....	306
17.3. Многопериодная модель.....	309
17.4. Случайное блуждание. Числа Каталана	312
Резюме	315
<i>Практикум</i>	316
<i>Задачи с решениями</i>	316
<i>Задания для самостоятельной работы</i>	317
Раздел VI	
МОДЕЛИ ДИСКРЕТНОЙ МАТЕМАТИКИ В ИНФОРМАТИКЕ	
Глава 18. Алгоритмы и вычислимость	321
18.1. Уточнение понятия алгоритма.....	321
18.2. Рекурсивные функции	322
18.3. Вычислимость и разрешимость	325
Резюме	326
<i>Практикум</i>	327
<i>Задачи с решениями</i>	327
<i>Задания для самостоятельной работы</i>	328
Глава 19. Элементы теории кодирования.....	330
19.1. Двоичное кодирование	330
19.2. Векторное пространство $\{0, 1\}^n$	331
19.3. Отображения из $\{0, 1\}^n$ в $\{0, 1\}^m$	332
19.4. Блочные двоичные коды.....	334
19.5. Коды Хемминга.....	336
19.6. Линейные коды и матричная алгебра	338
Резюме	339
<i>Практикум</i>	340
<i>Задачи с решениями</i>	340
<i>Задания для самостоятельной работы</i>	342
Глава 20. Арифметика целых чисел и основы криптографии	343
20.1. Основы теории делимости.....	343
20.2. Кольцо вычетов.....	345
20.3. Функция Эйлера	347
20.4. Система шифрования <i>RSA</i>	348
20.5. Сложность вычислений и односторонние функции	350
20.6. Односторонние функции и схемы криптографических протоколов	354
20.7. Протокол электронной подписи.....	357
Резюме	359
<i>Практикум</i>	360
<i>Задачи с решениями</i>	360
<i>Задания для самостоятельной работы</i>	363

Глава 21. Модели реляционных баз данных	364
21.1. Алгебра многоместных отношений	364
21.2. Математическая модель реляционной базы данных.....	367
21.3. Функциональные зависимости	368
21.4. Нормальные формы	369
Резюме.....	373
<i>Практикум</i>	374
<i>Задачи с решениями</i>	374
<i>Задания для самостоятельной работы</i>	376
Рекомендуемая литература	378
Предметный указатель	379

Предисловие

Математику традиционно делят на непрерывную и дискретную. К непрерывной математике относят то, что в той или иной форме опирается на идеи предела и непрерывности, все остальное относят к дискретной математике в широком смысле. Содержание дискретной математики как одной из математических дисциплин существенно уже. Дискретная математика изучает те математические объекты, в которых дискретность, проявляющаяся в строении объекта и в динамике его изменения, является определяющей характеристикой.

Учебные курсы дискретной математики обычно содержат те разделы дискретной математики в широком смысле, которые не попали в другие математические курсы, но необходимы для полноценной подготовки специалистов соответствующего профиля, а также разделы, традиционно относимые к дискретной математике (булевы функции, дискретное представление информации, комбинаторика, графы).

В предлагаемом курсе можно выделить три главные линии. Во-первых, в курсе изучаются так называемые основания математики (теория множеств и математическая логика), без которых немислима серьезная и профессиональная математическая подготовка; во-вторых — теоретические основы современной информатики (теория алгоритмов и вычислимых функций, теория кодирования, алгебра логики, теория баз данных); в третьих — те факты, методы и конструкции дискретной математики, которые применяются в экономико-математических моделях. Эти линии переплетаются и расходятся, но явно прослеживаются почти в любой теме курса.

В главе 1, посвященной теории множеств, приводятся сведения из теории множеств, с которыми читатели частично могли познакомиться еще в школе. По сравнению со школьным материалом заметно расширен и систематизирован. Понятия, которые вводятся в этой главе, не являются специфическими для дискретной математики. Они составляют основу современного математического языка, общеупотребительны и используются во всех математических курсах и в других главах книги.

При изучении каждой темы мы стараемся познакомить читателя с основными идеями и фундаментальными фактами и довести изложение до нетривиальных результатов. Объем, цели и задачи курса заставляют сводить к минимуму технически сложные и громоздкие построения (их в курсе, похоже, и нет). Приводимые доказательства, как правило, содержат некоторую важную идею (иногда, может быть, более важную, чем доказываемый факт). В ряде случаев мы не приводим доказательств. Это делается тогда, когда доказательства слишком сложны и объемны (такие теоремы отмече-

ны «звездочкой» — символом «*») или не добавляют ничего нового к пониманию существа дела. Иногда мы ограничиваемся проведением доказательства для частных случаев. Это делается тогда, когда доказательство в общем случае, не давая ничего нового в смысле идей, связано со значительными техническими усложнениями.

Некоторые понятия вводятся в специально выделенных определениях, некоторые даются менее формально. Это различие обусловлено значимостью соответствующих понятий и терминологической устойчивостью. Все новые понятия и термины выделяются в тексте полужирным шрифтом.

Все главы снабжены задачами и заданиями для самостоятельной работы. Решение задач является обязательным компонентом изучения математических дисциплин. Задачи с решениями иллюстрируют и дополняют материал главы, а иногда содержат доказательства теорем. Задания для самостоятельного решения, как правило, имеют аналоги среди разобранных примеров и задач с решениями. Впрочем, имеется некоторое количество задач, в которых читателю придется искать решение совершенно самостоятельно.

Представленный учебник рассчитан на изучение дискретной математики в течение одного семестра и не предполагает знания высшей математики. Изучение материала может быть построено в зависимости от направления подготовки. Первые четыре раздела составляют ядро стандартной подготовки по дискретной математике. Эти четыре раздела могут быть дополнены главами из раздела V для тех, кто специализируется в социально-экономических дисциплинах, или главами из раздела VI для тех, кто обучается по направлениям, связанным с изучением информатики.

В результате изучения учебника студент должен освоить:

трудовые действия

- по изучению математического аппарата, необходимого для освоения фундаментальных и прикладных математических дисциплин и информатики: теории множеств, математической логики, булевых функций, теории алгоритмов, теории кодирования, теории выбора и принятия решений;
- по применению методов построения и анализа дискретных моделей;
- по самостоятельной работе с учебной литературой по дискретной математике;

необходимые умения

- построения обоснованных выводов, анализа логической обоснованности утверждений;
- изложения результатов расчетов, исследований и анализов; представления и обоснования выводов;
- применения математического аппарата для построения и анализа кодов, баз данных, алгоритмов;
- анализа моделей, связанных с выбором и принятием решений;
- решения задач по установленным правилам;

необходимые знания

- основ теории множеств и математической логики, концепций доказуемости и вычислимости;

- основ комбинаторики и комбинаторного анализа;
- основ теории графов и методологические принципы применения теории графов для решения практических задач;
- понятийного аппарата, используемого в теории принятия решений;
- понятийного аппарата, используемого в информатике.

Мы не приводим сколько-нибудь полного списка литературы, ограничиваясь указанием на несколько книг, которые, как нам кажется, наиболее близко связаны по тематике с настоящей книгой и являются просто очень хорошо написанными книгами.

Автор благодарен профессорам О. Е. Кудрявцеву и А. В. Чечкину за рецензирование рукописи и сделанные замечания. Автор благодарен своим близким за терпение и поддержку.

Раздел I

МНОЖЕСТВА И ОТНОШЕНИЯ



Глава 1

МНОЖЕСТВА

В результате освоения материала данной главы студент должен:

знать

- способы задания множеств;
- определения основных операций над множествами и свойства операций;
- определения основных типов отображений;

уметь

- находить объединение, пересечение, разность и симметрическую разность двух множеств, дополнение множества;
- представлять графически операции над множествами и интерпретировать на диаграммах свойства операций;

владеть

- приемами представления математических задач на языке теории множеств;
 - навыками выполнения преобразований в алгебре множеств.
-

1.1. Понятие множества

Понятие множества является одним из наиболее общих математических понятий. Его определение не удастся свести к другим понятиям. Поэтому для понятия множества дается описательное определение, содержание и смысл которого раскрываются при изучении теории множеств. **Множество** — это набор, совокупность каких-либо объектов, называемых его **элементами**, обладающих некоторым общим для них характеристическим свойством. В качестве примеров можно привести множество действительных чисел, множество решений заданного алгебраического уравнения, множество прямых, проходящих через заданную точку. В принципе никаких ограничений на природу элементов, их количество и свойства не налагается, так что допустимо рассмотрение таких множеств, как множество налогоплательщиков, множество процентных ставок и т.п.

Элементы, составляющие множество, обычно обозначаются малыми латинскими буквами, а само множество — большой латинской буквой. Знак \in используется для обозначения принадлежности элемента множеству. Запись $a \in A$ означает, что элемент a принадлежит множеству A . Если некоторый объект x не является элементом множества A , пишут $x \notin A$. Например, если A — это множество четных чисел, то $2 \in A$, а $1 \notin A$. Множества A и B считаются **равными** (пишут $A = B$), если они состоят из одних и тех же элементов.

Если множество содержит конечное число элементов, его называют **конечным**; в противном случае множество называется **бесконечным**.

Если множество A конечно, символом $|A|$ будет обозначаться число его элементов. Множество, не содержащее ни одного элемента, называется **пустым** и обозначается символом \emptyset . Очевидно, что $|\emptyset| = 0$.

Пример 1.1. Пусть A — множество действительных решений квадратного уравнения $x^2 + px + q = 0$. Множество A конечно, $|A| \leq 2$. Если дискриминант $D = p^2 - 4q$ отрицательный, множество A пусто. Множество действительных решений квадратичного неравенства $x^2 + px + q \leq 0$ конечно, если $D \leq 0$, и бесконечно, если $D > 0$.

Конечное множество может быть задано перечислением всех его элементов. Если множество A состоит из элементов x, y, z, \dots , пишут $A = \{x, y, z, \dots\}$. Например:

$A = \{0, 2, 4, 6, 8\}$ — множество четных десятичных цифр;

$B = \{2, 3\}$ — множество решений уравнения $x^2 - 5x + 6 = 0$;

$C = \{0, 1, 2, 3, 4, 5, 6\}$ — множество остатков при делении целых чисел на 7.

Иногда перечислением элементов задают и бесконечное множество. Это делают в тех случаях, когда ясен алгоритм последовательного порождения элементов. Например, $A = \{0, 1, 4, 9, 16, \dots\}$ — множество квадратов целых чисел.

В общем случае множества можно задавать по так называемой **схеме свертывания**. Пусть заданы характеристическое свойство F и класс элементов K . Тогда по схеме свертывания можно определить множество A , которое содержит все элементы из K , обладающие свойством F . Для определения по схеме свертывания используется следующая запись:

$$A = \{x \mid x \text{ обладает свойством } F\}.$$

Применяя сокращение $F(x)$ для обозначения того, что элемент x обладает свойством F , будем писать

$$A = \{x \mid F(x)\}.$$

Класс K может быть указан явно; в этом случае используется запись

$$A = \{x \in K \mid F(x)\}.$$

Например, множество четных чисел P можно определить как

$$P = \{x \mid x \text{ — четное целое число}\},$$

или как

$$P = \{x \in \mathbb{Z} \mid x \text{ четно}\},$$

где через \mathbb{Z} обозначено множество целых чисел.

Неограниченное применение схемы свертывания может приводить к противоречиям. Например, можно получить «множество всех множеств»:

$$M = \{x \mid x \text{ — множество}\}.$$

Если считать M множеством, то получаем $M \in M$. Подобное построение лежит в основе следующего парадокса.

Парадокс Рассела. Назовем множество правильным, если оно не является своим элементом, и неправильным в противном случае. Определим R как множество всех правильных множеств. Более формально, по схеме свертывания

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

В соответствии с определением для любого множества A справедливо утверждение:

$$A \in R \text{ тогда и только тогда, когда } A \notin A.$$

В частности, если считать R множеством, его само можно взять в качестве A . Получаем противоречие:

$$R \in R \text{ тогда и только тогда, когда } R \notin R.$$

Рассуждая более подробно, если R — правильное множество, т.е. не является своим элементом, оно должно находиться в R , т.е. быть своим элементом, и значит, неправильным множеством. Если же R — неправильное множество, оно является своим элементом, т.е. содержится в R . Но R содержит только правильные множества. Таким образом, R не может быть ни правильным, ни неправильным.

Введем используемое в дальнейшем понятие **индексированного семейства множеств**. Пусть I — некоторое множество, каждому элементу которого i сопоставлено однозначно определенное множество A_i . Элементы множества I называют индексами, а совокупность множеств A_i называют индексированным семейством множеств и обозначают через $(A_i)_{i \in I}$.

1.2. Подмножества

Определение 1.1. Множество B называется **подмножеством**, или частью, множества A , если всякий элемент множества B является элементом множества A .

Если множество B является подмножеством множества A , пишут $B \subseteq A$ или $A \supseteq B$. Если $B \subseteq A$ и множество A содержит хотя бы один элемент, не содержащийся в множестве B , пишут $B \subset A$ или $A \supset B$.

Например, множество натуральных чисел \mathbb{N} является подмножеством множества целых чисел \mathbb{Z} , а последнее в свою очередь является подмножеством множества рациональных чисел \mathbb{Q} , т.е. $\mathbb{N} \subset \mathbb{Z}$ и $\mathbb{Z} \subset \mathbb{Q}$, или, короче, $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.

Легко видеть, что если $B \subseteq A$ и $A \subseteq B$, то множества A и B состоят из одних и тех же элементов и, значит, $A = B$.

Подмножество множества A может быть задано определяющим свойством. Например, свойство быть четным числом определяет в множестве целых чисел подмножество четных чисел.

Каково бы ни было множество A , пустое множество и само множество A являются его подмножествами: $\emptyset \subseteq A$ и $A \subseteq A$. Пустое множество может быть задано свойством, которым не обладает ни один элемент множества A , например $x \neq x$. Свойство быть корнем уравнения $x^2 + 1 = 0$ задает пустое подмножество множества действительных чисел. Множество A может быть задано как свое подмножество каким-нибудь свойством, которым обладают все элементы множества A , например $x = x$.

Определение 1.2. Подмножества множества A , отличные от пустого множества \emptyset и самого множества A , называются **собственными подмножествами**.

Для заданного множества A через 2^A будет обозначаться множество всех его подмножеств.

Пример 1.2. Пусть $A = \{a, b, c\}$. Тогда множество 2^A состоит из следующих элементов: $\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}$.

Далее будет показано, что если множество A конечно и содержит n элементов, то множество 2^A имеет 2^n подмножеств, т.е. $|2^A| = 2^{|A|}$.

1.3. Операции над множествами

Определение 1.3. Пересечение множеств A и B , обозначаемое $A \cap B$, — это множество, состоящее из всех тех элементов, которые принадлежат обоим множествам A и B .

Например, если $A = \{1, 2, 3\}$ и $B = \{2, 3, 4\}$, то $A \cap B = \{2, 3\}$.

В соответствии с определением $A \cap B \subseteq A$ и $A \cap B \subseteq B$, причем $A \cap B$ является в определенном смысле наибольшим множеством, обладающим этими свойствами:

$$\text{если } C \subseteq A \text{ и } C \subseteq B, \text{ то } C \subseteq A \cap B.$$

Далее, $A \cap B = B$ тогда и только тогда, когда $B \subseteq A$.

Если множества A и B не имеют общих элементов, их пересечение пусто: $A \cap B = \emptyset$; в этом случае говорят, что множества A и B **не пересекаются**.

Определение 1.4. Объединение множеств A и B , обозначаемое $A \cup B$, — это множество, состоящее из всех тех элементов, которые принадлежат хотя бы одному из множеств A и B .

Например, если $A = \{1, 2, 3\}$ и $B = \{2, 3, 4\}$, то $A \cup B = \{1, 2, 3, 4\}$.

В соответствии с определением $A \subseteq A \cup B$ и $B \subseteq A \cup B$, причем $A \cup B$ является наименьшим множеством, обладающим этими свойствами:

$$\text{если } A \subseteq C \text{ и } B \subseteq C, \text{ то } A \cup B \subseteq C.$$

Далее, $A \cup B = B$ тогда и только тогда, когда $A \subseteq B$.

Операции пересечения и объединения можно обобщить на случай произвольного индексированного семейства множеств. **Пересечением семейства множеств** $(A_i)_{i \in I}$ называется множество A , состоящее из всех тех элементов, которые принадлежат каждому из множеств A_i . Пишут

$$A = \bigcap_{i \in I} A_i.$$

Если множество индексов состоит из натуральных чисел, используются и другие обозначения, например:

$$A_1 \cap A_2 \cap A_3, \text{ если } I = \{1, 2, 3\};$$

$$A_1 \cap A_2 \cap \dots \cap A_n \text{ или } \bigcap_{i=1}^n A_i, \text{ если } I = \{1, 2, \dots, n\};$$

$$\bigcap_{i=1}^{\infty} A_i \text{ если } I \text{ — это множество всех натуральных чисел, и т.п.}$$

Аналогично, **объединением семейства множеств** $(A_i)_{i \in I}$ называется множество A , состоящее из всех тех элементов, которые принадлежат хотя бы одному из множеств A_i . Для объединения используют обозначение

$$A = \bigcup_{i \in I} A_i$$

и другие, подобные тем, которые используются для пересечения.

Пример 1.3. Пусть $A_n = \left[0; \frac{n}{n+1}\right]$, где $n = 1, 2, \dots$ пробегает множество натуральных чисел. Тогда, очевидно,

$$\bigcap_{n=1}^{\infty} A_n = \left[0; \frac{1}{2}\right],$$

поскольку $A_1 \subseteq A_2 \subseteq \dots$.

Покажем, что

$$\bigcup_{n=1}^{\infty} A_n = [0; 1).$$

В самом деле, если $x \in (0; 1)$, то $x \in A_n$, когда $x > 1/n$, т.е. при $n > 1/x$. Если же $x < 0$ или $x \geq 1$, то x не попадает ни в одно из множеств A_n , а значит, не попадает и в их объединение.

Определение 1.5. Разность множеств A и B , обозначаемая $A \setminus B$, — это множество, состоящее из всех тех элементов, которые принадлежат множеству A , но не принадлежат множеству B .

Например, если $A = \{1, 2, 3\}$ и $B = \{2, 3, 4\}$, то $A \setminus B = \{1\}$.

В соответствии с определением $A \setminus B \subseteq A$ и $(A \setminus B) \cap B = \emptyset$, причем $A \setminus B$ является в определенном смысле наибольшим множеством, обладающим этими свойствами:

если $C \subseteq A$ и $C \cap B = \emptyset$, то $C \subseteq A \setminus B$.

Далее, $A \setminus B = A$ тогда и только тогда, когда $A \cap B = \emptyset$, и $A \setminus B = \emptyset$ тогда и только тогда, когда $A \subseteq B$.

Если $B \subseteq A$, то разность $A \setminus B$ называют также **дополнением** (или **относительным дополнением**) множества B в множестве A . Иногда относительное дополнение будет обозначаться через \overline{B}_A . Любое собственное подмножество B множества A вместе со своим относительным дополнением образует разбиение множества A на два непересекающихся непустых множества:

$$B \cap \overline{B}_A = \emptyset, B \cup \overline{B}_A = A.$$

Часто в теоретико-множественных конструкциях используется **универсальное** множество U . Считается, что все рассматриваемые множества являются его подмножествами.

Определение 1.6. Относительное дополнение множества A до универсального множества называется **дополнением** (без прилагательного «относительное») и обозначается через \overline{A} .

Очевидно, что $\overline{\overline{U}} = \emptyset$ и $\overline{\emptyset} = U$.

Определение 1.7. Симметрическая разность множеств A и B , обозначаемая $A \Delta B$, — это множество, состоящее из всех тех элементов, которые принадлежат одному из множеств A и B , но не принадлежат другому.

Более формально,

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

Например, если $A = \{1, 2, 3\}$ и $B = \{2, 3, 4\}$, то $A \Delta B = \{1, 4\}$.

1.4. Диаграммы Эйлера — Венна

Для наглядного представления операций над множествами используются диаграммы Эйлера — Венна. На таких диаграммах фон рисунка, обычно ограниченный прямоугольником, соответствует универсальному множеству. Каждое «основное» множество изображается внутренней частью соответствующего круга. Возникающие на рисунке области изображают множества, получающиеся в результате операций.

Например, на рис. 1.1 круги изображают множества A и B . Объединение двух кругов соответствует объединению $A \cup B$; область 3 соответствует пересечению $A \cap B$; область 1 — множеству $A \setminus B$; область 2 — множеству $B \setminus A$; область 4 — множеству $\overline{A \cup B}$; объединение областей 1 и 2 соответствует симметрической разности $A \Delta B$. Легко видеть, что имеет место следующее соотношение:

$$A \Delta B = (A \cup B) \setminus (A \cap B).$$

Если $B \subset A$, то круг, соответствующий множеству B , располагают внутри круга, соответствующего множеству A (рис. 1.2).

Множества, не имеющие общих элементов, изображаются непересекающимися кругами (рис. 1.3).

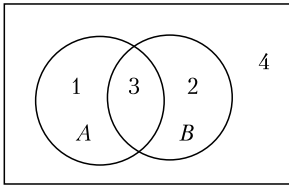


Рис. 1.1. Операции над множествами

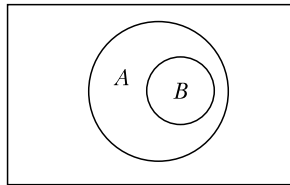


Рис. 1.2. Случай $B \subset A$

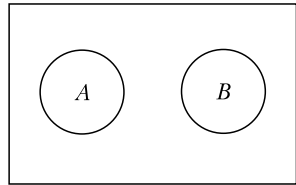


Рис. 1.3. Непересекающиеся множества A и B

Равные множества изображаются равными кругами, т.е. по сути дела одним и тем же кругом.

Диаграммы Эйлера — Венна удобно использовать для проверки соотношений между множествами.

Пример 1.4. Рассмотрим такое рассуждение: если некоторые элементы множества A являются элементами множества B и при этом ни один элемент множества B не является элементом множества C , то некоторые элементы множества C не являются элементами множества A . Это рассуждение неверно. Достаточно рассмотреть диаграмму на рис. 1.4.

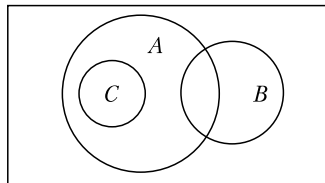


Рис. 1.4. К примеру 1.4: $A \cap B \neq \emptyset$, $B \subseteq \overline{C}$, $C \subseteq A$

Несложно проверить, что имеется пять различных вариантов расположения двух кругов (кроме тех трех, которые изображены на рис. 1.1—1.3, расположения, соответствующие соотношениям $A \subset B$ и $A = B$).

Для трех основных множеств A, B, C число различных вариантов расположения кругов существенно возрастает (см. рис. 1.4). С увеличением числа основных множеств прямое применение диаграмм Эйлера — Венна становится менее удобным, и применяются различные их модификации.

1.5. Алгебра множеств

Приведем основные тождества так называемой алгебры множеств (будем предполагать, что используемые в тождествах множества A, B, C являются подмножествами универсального множества U).

Коммутативность:

$$1. A \cap B = B \cap A; 1'. A \cup B = B \cup A.$$

Ассоциативность:

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

Дистрибутивность:

$$3. (A \cup B) \cap C = (A \cap C) \cup (B \cap C); 3'. (A \cap B) \cup C = (A \cup C) \cap (B \cup C).$$

Идемпотентность:

$$4. A \cap A = A; 4'. A \cup A = A.$$

Законы поглощения:

$$5. A \cap (A \cup B) = A; 5'. A \cup (A \cap B) = A.$$

Законы нуля и единицы:

$$6. A \cap U = A; 6'. A \cup U = U.$$

$$7. A \cap \emptyset = \emptyset; 7'. A \cup \emptyset = A.$$

$$8. A \cap \bar{A} = \emptyset; 8'. A \cup \bar{A} = U.$$

$$9. \bar{\emptyset} = U; 9'. \bar{U} = \emptyset.$$

Инволютивность дополнения:

$$10. \bar{\bar{A}} = A.$$

Законы де Моргана:

$$11. \overline{A \cap B} = \bar{A} \cup \bar{B}; 11'. \overline{A \cup B} = \bar{A} \cap \bar{B}.$$

Каждому соотношению (кроме соотношения 10) соответствует так называемое **двойственное** соотношение, которое получается заменой операций пересечения операциями объединения и операций объединения операциями пересечения. Соотношение 10 совпадает со своим двойственным.

То, что операции над множествами обладают перечисленными свойствами, означает, что подмножества универсального множества образуют **булеву алгебру**.

Убедиться в справедливости перечисленных свойств можно путем несложной непосредственной проверки или используя диаграммы Эйлера — Венна.

Пример 1.5. Проверим первый из законов де Моргана. Покажем сначала, что $A \cap B \subseteq \overline{A \cup B}$. Предположим, что $x \in A \cap B$. Тогда $x \notin A \cup B$, так что x не принадлежит хотя бы одному из множеств A и B . Таким образом, $x \notin A$ или $x \notin B$, т.е. $x \in \bar{A}$ или $x \in \bar{B}$. Это означает, что $x \in \bar{A} \cup \bar{B}$. Мы показали, что произвольный элемент множества $A \cap B$ является элементом множества $\bar{A} \cup \bar{B}$. Следовательно, $A \cap B \subseteq \bar{A} \cup \bar{B}$. Обратное включение $A \cap B \supseteq \bar{A} \cup \bar{B}$ доказывается аналогично. Достаточно повторить все шаги предыдущего рассуждения в обратном порядке.

1.6. Прямое произведение множеств

Из любой пары элементов a и b (необязательно различных) можно составить новый элемент — **упорядоченную пару** (a, b) . Упорядоченные пары (a, b) и (c, d) считают равными и пишут $(a, b) = (c, d)$, если $a = c$ и $b = d$. В частности, $(a, b) = (b, a)$ лишь в том случае, когда $a = b$. Элементы a и b называют **координатами** упорядоченной пары (a, b) (соответственно первой и второй).

Определение 1.8. **Прямым (декартовым) произведением** множеств A и B называется множество всех упорядоченных пар (a, b) , где $a \in A$ и $b \in B$.

Прямое произведение множеств A и B обозначается через $A \times B$. В соответствии с определением имеем

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

Если множества A и B конечны, справедливо соотношение

$$|A \times B| = |A| \times |B|.$$

Пример 1.6. Пусть $A = \{1, 2, 3\}$ и $B = \{2, 3, 4\}$. Тогда множество $A \times B$ состоит из следующих девяти элементов: $(1, 4)$, $(2, 4)$, $(3, 4)$, $(1, 3)$, $(2, 3)$, $(3, 3)$, $(1, 2)$, $(2, 2)$, $(3, 2)$. Графически элементы произведения множеств $A \times B$ удобно помещать на «координатной плоскости», или в клетках прямоугольной таблицы:

$$\begin{array}{ccc} (1, 4) & (2, 4) & (3, 4) \\ (1, 3) & (2, 3) & (3, 3) \\ (1, 2) & (2, 2) & (3, 2) \end{array}$$

Подобно парам, можно рассматривать упорядоченные тройки, четверки и, вообще, упорядоченные наборы элементов произвольной длины. Упорядоченный набор элементов длины n обозначается через (a_1, a_2, \dots, a_n) . Для таких наборов используется также название **кортеж** длины n . Допускаются в том числе и кортежи длины 1 — это просто одноэлементные множества. Кортежи (a_1, a_2, \dots, a_n) и (b_1, b_2, \dots, b_n) считаются равными, если $a_1 = b_1$, $a_2 = b_2$, ..., $a_n = b_n$.

Определение 1.9. **Прямое произведение** множеств A_1, A_2, \dots, A_n — это множество всех кортежей (a_1, a_2, \dots, a_n) , таких что $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$.

Обозначается прямое произведение через $A_1 \times A_2 \times \dots \times A_n$.

Понятие прямого произведения может быть обобщено на случай произвольного семейства множеств $(A_i)_{i \in I}$. Назовем I -кортежем набор элементов $(a_i)_{i \in I}$, такой что $a_i \in A_i$ для каждого $i \in I$. Прямое произведение семейства множеств $(A_i)_{i \in I}$ — это множество, состоящее из всех I -кортежей. Для обозначения этого множества используются символ

$$\prod_{i \in I} A_i$$

и его разновидности, подобные тем, которые применяются для обозначения пересечения и объединения семейства множеств.

В случае когда множество A умножается само на себя, произведение называют (декартовой) **степенью** и используют экспоненциальные обозначения. Так, в соответствии с определением

$$A \times A = A^2, A \times A \times A = A^3$$

и т.д. Считается, что $A^1 = A$ и $A^0 = \emptyset$.

Непосредственно из определений следует справедливость следующих соотношений:

$$\begin{aligned}(A \cup B) \times C &= (A \times C) \cup (B \times C); \\ (A \cap B) \times C &= (A \times C) \cap (B \times C); \\ (A \setminus B) \times C &= (A \times C) \setminus (B \times C).\end{aligned}$$

1.7. Отображения и их свойства

1.7.1. Понятие отображения

Отображение f множества X в множество Y считается заданным, если каждому элементу x из X сопоставлен ровно один элемент y из Y , обозначаемый $f(x)$. Множество X называется **областью определения** отображения f , а множество Y — **областью значений**.

Множество упорядоченных пар

$$\Gamma_f = \{(x, y) \mid x \in X, y \in Y, y = f(x)\}$$

называют **графиком** отображения f . Непосредственно из определения вытекает, что график отображения f является подмножеством декартова произведения $X \times Y$: $\Gamma_f \subseteq X \times Y$.

Приведем теперь формальное определение понятия отображения на языке теории множеств.

Определение 1.10. Отображение — это тройка множеств (X, Y, G) , такая что $G \subseteq X \times Y$, и каждый элемент x из X является первым элементом ровно одной пары (x, y) из G .

Пусть в обозначениях определения 1.10 $x \in X$. Полагая $y = f(x)$, где $(x, y) \in G$, получаем отображение f множества X в множество Y . При этом, очевидно, $G = \Gamma_f$.

Если $y = f(x)$, мы будем писать также $f: x \rightarrow y$ и говорить, что элемент x переходит или отображается в элемент y ; элемент $f(x)$ называется **образом элемента x** относительно отображения f , а элемент x — **прообразом элемента $y = f(x)$** . Для обозначения отображений мы будем использовать записи вида $f: X \rightarrow Y$. Часто отображения задают равенством вида $y = f(x)$, где x и y — переменные; значениями переменной x , называемой аргументом, служат элементы множества X ; переменная y принимает свои значения в множестве Y . В этом случае отображения называют также функциями.

Пример 1.7. 1. Пусть $X = Y$ — множество действительных чисел. Формула $y = 2x$ задает отображение множества X в множество Y .

2. Пусть X — множество всех треугольников на плоскости, а Y — множество действительных чисел. Сопоставляя треугольнику его площадь, получаем отображение первого множества во второе.

3. Пусть $X = \{1, 2, 3\}$, $Y = \{2, 3, 4\}$. Множество пар $G = \{(1, 2), (2, 2), (3, 3)\}$ задает отображение f , при котором $f(1) = f(2) = 2$, $f(3) = 3$. Множество G является графиком отображения f .

Отображение f конечного множества $X = \{a, b, \dots, c\}$ часто бывает удобно задать с помощью таблицы (матрицы), состоящей из двух строк. В первой

строке располагаются элементы множества X , а под ними, во второй строке — их образы:

$$\begin{pmatrix} a & b & \dots & c \\ f(a) & f(b) & \dots & f(c) \end{pmatrix}.$$

Например, таблица

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 2 & 3 \end{pmatrix}$$

задает отображение из примера 1.7 (п. 3); таблица

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

задает отображение множества четвертей координатной плоскости в себя при повороте плоскости на 90° против часовой стрелки вокруг начала координат (естественно, вместо самих четвертей мы используем их номера).

Теорема 1.1. Если множества X и Y конечны, то число отображений из X в Y равно $|X|^{|Y|}$.

Пусть $f: X \rightarrow Y$ — отображение множества X в множество Y , а A и B — подмножества множеств X и Y соответственно. Множество

$$f(A) = \{y \mid y = f(x) \text{ для некоторого } x \in A\}$$

называется **образом множества A** . Множество

$$f^{-1}(B) = \{x \mid f(x) \in B\}$$

называется **прообразом множества B** . Отображение $f: A \rightarrow Y$, при котором x переходит в $f(x)$ для всех $x \in A$, называется **сужением** отображения f на множество A ; сужение будет обозначаться через $f|_A$.

Отображение вида $f: X \times Y \rightarrow Z$ называют функцией двух переменных и пишут $z = f(x, y)$. Аналогично определяются функции большего числа переменных.

Определение 1.11. Пусть имеются отображения $f: X \rightarrow Y$ и $g: Y \rightarrow Z$. Отображение $X \rightarrow Z$, при котором x переходит в $g(f(x))$, называется **композицией отображений f и g** и обозначается через $f \cdot g$ или просто fg .

В соответствии с определением $(fg)(x) = g(f(x))$.

Например, если отображения f, g множества действительных чисел в себя заданы формулами $f(x) = x + 1$, $g(x) = 2x$, то

$$(fg)(x) = g(f(x)) = g(x + 1) = 2(x + 1);$$

$$(gf)(x) = f(g(x)) = f(2x) = 2x + 1.$$

1.7.2. Специальные виды отображений

Отображение множества X в X , при котором каждый элемент переходит сам в себя, $x \rightarrow x$, называется **тождественным** и обозначается через id_X .

Для произвольного отображения $f: X \rightarrow Y$ имеем

$$id_X \times f = f \times id_Y.$$

Определение 1.12. Отображение $f: X \rightarrow Y$ называется:

- **инъективным**, если образы различных элементов также различны, т.е. $f(x) \rightarrow f(y)$ при $x \rightarrow y$;
- **сюръективным** (говорят также, что f — отображение X на Y), если всякий элемент y из Y является образом некоторого элемента x из X , т.е. $f(X) = Y$;
- **биективным**, если оно одновременно инъективно и сюръективно.

Биективное отображение $f: X \rightarrow Y$ **обратимо**. Это означает, что существует отображение $g: Y \rightarrow X$, называемое обратным к отображению f , такое что $g(f(x)) = x$ и $f(g(y)) = y$ для любых $x \in X, y \in Y$. Ясно, что при этом отображение f является обратным к отображению g . Отображение, обратное к отображению f , обозначается через f^{-1} . В соответствии с определением

$$ff^{-1} = id_X, f^{-1}f = id_Y, (f^{-1})^{-1} = f.$$

Нетрудно видеть, что отображение биективно тогда и только тогда, когда оно обратимо. Говорят, что обратимое отображение $f: X \rightarrow Y$ устанавливает взаимно однозначное соответствие между элементами множеств X и Y , или, короче, между множествами X и Y . Инъективное отображение $f: X \rightarrow Y$ устанавливает взаимно однозначное соответствие между множеством X и множеством $f(X)$.

Пример 1.8. 1. Функция $f: \mathbb{R} \rightarrow \mathbb{R}_{>0}, f(x) = e^x$, устанавливает взаимно однозначное соответствие множества всех действительных чисел \mathbb{R} с множеством положительных действительных чисел $\mathbb{R}_{>0}$. Обратным к отображению f является отображение $g: \mathbb{R}_{>0} \rightarrow \mathbb{R}, g(x) = \ln x$.

2. Отображение $f: \mathbb{R} \rightarrow \mathbb{R}_{>0}, f(x) = x^2$, множества всех действительных \mathbb{R} на множество неотрицательных чисел $\mathbb{R}_{\geq 0}$ сюръективно, но не инъективно, и поэтому не является биективным.

Теорема 1.2. (а) Композиция инъективных отображений инъективна. (б) Композиция сюръективных отображений сюръективна. (в) Композиция биективных отображений биективна.

► **Доказательство.** Пусть заданы отображения $f: X \rightarrow Y$ и $g: Y \rightarrow Z$.

(а) Предположим, что f и g инъективны. Если x_1 и x_2 — несовпадающие элементы множества X , то $f(x_1) \neq f(x_2)$, поскольку отображение f инъективно. Но тогда и $g(f(x_1)) \neq g(f(x_2))$, поскольку отображение g инъективно. Это означает, что композиция $fg: X \rightarrow Z$ инъективна.

(б) Предположим, что f и g сюръективны. Это означает, что $f(X) = Y$ и $g(Y) = Z$. Но тогда $g(f(X)) = g(Y) = Z$, т.е. $(fg)(X) = Z$, и, следовательно, композиция $fg: X \rightarrow Z$ сюръективна.

(в) Композиция биективных отображений инъективна в силу (а) и сюръективна в силу (б) и, следовательно, биективна. ◀

1.7.3. Характеристические функции

Пусть X — некоторое множество и A — его подмножество. Определим отображение χ_A множества X в двухэлементное множество $\{0, 1\}$ следующим образом: $\chi_A(x) = 1$, если $x \in A$, и $\chi_A(x) = 0$, если $x \notin A$. Функция χ_A называется **характеристической функцией** подмножества A .

Очевидно, $A \subseteq B$ тогда и только тогда, когда $\chi_A(x) \leq \chi_B(x)$ для всех x .

Имеется простая связь между операциями над подмножествами множества X и операциями над их характеристическими функциями:

$$\begin{aligned}\chi_{A \cap B}(x) &= \min(\chi_A(x), \chi_B(x)) = \chi_A(x) \times \chi_B(x); \\ \chi_{A \cup B}(x) &= \max(\chi_A(x), \chi_B(x)) = \chi_A(x) + \chi_B(x) - \chi_A(x) \times \chi_B(x); \\ \chi_{A \setminus B}(x) &= \max(\chi_A(x) - \chi_B(x), 0) = \chi_A(x) \times (1 - \chi_B(x)); \\ \chi_X(x) &\equiv 1; \chi_\emptyset(x) \equiv 0.\end{aligned}$$

1.7.4. Операции

Бинарной операцией на множестве X называется отображение $f: X \times X \rightarrow X$. Результат применения бинарной операции к паре (x, y) принято записывать в виде $x * y$, где $*$ — символ операции. Таким образом, $f: (x, y) \rightarrow x * y$.

Пример 1.9. Отображение $f: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$, $f(x, y) = x + y$, — это операция сложения на множестве действительных чисел; $f: 2^X \times 2^X \rightarrow 2^X$, $f(A, B) = A \cap B$ — операция пересечения на множестве подмножеств множества X .

Бинарная операция $*$ на множестве X называется:

- коммутативной, если $x * y = y * x$ для всех x, y из X ;
- ассоциативной, если $(x * y) * z = x * (y * z)$ для всех x, y, z из X .

При записи повторенной несколько раз ассоциативной бинарной операции скобки можно опускать — результат от порядка выполнения операций не зависит. Например:

$$((x * y) * z) * t = (x * (y * z)) * t = x * ((y * z) * t) = x * (y * (z * t)).$$

Операции сложения и умножения на множестве действительных чисел коммутативны и ассоциативны; операции объединения и пересечения подмножеств универсального множества также коммутативны и ассоциативны. Рассмотрим не столь очевидный пример.

Пример 1.10. Зададим бинарную на отрезке $[0; 1]$ формулой

$$x * y = x + y - xy.$$

Очевидно, так определенная операция коммутативна. Покажем, что она и ассоциативна. Имеем

$$\begin{aligned}(x * y) * z &= (x + y - xy) * z = x + y - xy + z - (x + y - xy)z = \\ &= x + y + z - xy - xz - yz + xyz; \\ x * (y * z) &= x * (y + z - yz) = x + y + z - yz - x(y + z - yz) = \\ &= x + y + z - xy - xz - yz + xyz,\end{aligned}$$

откуда

$$(x * y) * z = x * (y * z).$$

Бинарная операция на конечном множестве может быть задана с помощью таблицы.

Пример 1.11. Зададим на множестве $X = \{0, 1, 2, 3, 4\}$ операцию «умножение по модулю 5» (остаток при делении произведения на 5):

—	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Верхняя строка и левый столбец содержат элементы множества X , которые служат метками соответствующих столбцов и строк. На пересечении строки с меткой x и столбца с меткой y находится произведение xy по модулю 5. Например, произведение 2 на 3 по модулю 5 равно 1.

Резюме

Теория множеств лежит в основе современной математики, и в частности дискретной математики. В дальнейшем от читателя потребуются свободное владение языком теории множеств, знание основных операций и умение выполнять преобразования в алгебре множеств. В курсе дискретной математики мы будем иметь дело, как правило, с конечными множествами. Вычисления, связанные с конечными множествами, будут систематически рассматриваться в разделе, посвященном комбинаторике. Некоторые простейшие факты приведены в настоящей главе. Последний параграф посвящен отображениям. Здесь приведены общие сведения об отображениях, определены специальные классы отображений. Все это необходимо при изучении любой математической дисциплины.

Фактического материала, фиксируемого теоремами, в этой главе сравнительно немного. Главное — овладеть системой понятий и освоить обозначения.

Основные обозначения, используемые в главе, приведены в табл. 1.1.

Таблица 1.1

Теоретико-множественные обозначения

Обозначение	Краткое описание
$x \in A$	Элемент x является элементом множества A
$x \notin A$	Элемент x не является элементом множества A
$\{x \mid P(x)\}$	Множество всех элементов, обладающих свойством P
$\{x \in A \mid P(x)\}$	Множество всех элементов множества A , обладающих свойством P
$ A $	Число элементов (конечного) множества A
\emptyset	Пустое множество
U	Универсальное множество
$A = B$	Множества A и B состоят из одних и тех же элементов
$B \subseteq A$	Множество B является подмножеством множества A
$B \subset A$	Множество B является подмножеством множества A , при этом в A есть элементы, не входящие в B
2^A	Множество всех подмножеств множества A
$A \cap B$	Пересечение множеств A и B
$A \cup B$	Объединение множеств A и B

Обозначение	Краткое описание
$A \setminus B$	Разность множеств A и B (относительное дополнение множества B в множестве A)
$A \Delta B$	Симметрическая разность множеств A и B
$A \times B$	Прямое (декартово) произведение множеств A и B
id_X	Тождественное отображение множества A в себя
χ_A	Характеристическая функция подмножества A
f^{-1}	Обратное отображение отображения f
$f \times g$	Композиция отображений f и g

Практикум

Задачи с решениями

1.1. Пусть универсальное множество U — множество всех сотрудников некоторой организации; A — множество всех сотрудников старше 35 лет; B — множество сотрудников, имеющих стаж работы более 10 лет; C — множество менеджеров фирмы. Определим, каковы характеристические свойства элементов следующих множеств: а) \overline{B} ; б) $\overline{A} \cap B \cap C$; в) $A \cup (B \cap \overline{C})$; г) $B \setminus C$; д) $C \setminus B$.

Решение. а) \overline{B} — множество сотрудников организации, стаж работы которых не превышает 10 лет.

б) $\overline{A} \cap B \cap C$ — множество менеджеров фирмы не старше 35 лет, имеющих стаж работы более 10 лет.

в) $A \cup (B \cap \overline{C})$ — множество всех сотрудников фирмы старше 35 лет, а также сотрудников, не являющихся менеджерами, стаж работы которых более 10 лет.

г) $B \setminus C$ — множество сотрудников организации со стажем работы более 10 лет, не работающих менеджерами.

д) $C \setminus B$ — множество менеджеров со стажем работы не более 10 лет.

1.2. Пусть $U = \{1, 2, 3, 4\}$, $A = \{1, 3, 4\}$, $B = \{2, 3\}$, $C = \{2, 4\}$. Найдем: а) $\overline{A} \cup \overline{B}$; б) $\overline{A} \cap \overline{B}$; в) $A \cap \overline{B}$; г) $(B \setminus A) \cup \overline{C}$; д) $A \Delta (B \cup C)$.

Решение. а) $\overline{A} \cup \overline{B} = (U \setminus A) \cup (U \setminus B) = \{2\} \cup \{1, 4\} = \{1, 2, 4\}$.

б) $\overline{A} \cap \overline{B} = U \setminus (A \cap B) = \{1, 2, 3, 4\} \setminus \{3\} = \{1, 2, 4\}$.

в) $A \cap \overline{B} = A \cap (U \setminus B) = \{1, 3, 4\} \cap \{1, 4\} = \{1, 4\}$.

г) $(B \setminus A) \cup \overline{C} = \{2\} \cup \{1, 3\} = \{1, 2, 3\}$.

д) $A \Delta (B \cup C) = \{1, 3, 4\} \Delta \{2, 3, 4\} = \{1, 2\}$.

1.3. Докажем справедливость тождества

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$

Решение. Множества X и Y равны, если $X \subseteq Y$ и $Y \subseteq X$.

Покажем сначала, что $(A \cup B) \cap C \subseteq (A \cap C) \cup (B \cap C)$, т.е. любой элемент x из множества, заданного левой частью, принадлежит и множеству, заданному правой частью.

Пусть $x \in (A \cup B) \cap C$. Тогда x принадлежит одновременно $A \cup B$ и C , т.е. x принадлежит одному из множеств A или B и множеству C . Следовательно, справедливо по крайней мере одно из двух утверждений: x принадлежит A и C или B и C . Это означает, что x принадлежит пересечению $A \cap C$ или пересечению $B \cap C$. Значит, x принадлежит объединению $(A \cap C) \cup (B \cap C)$.

Обратное включение доказывается аналогично.

1.4. Пусть $X = \{0, 1\}$, $Y = \{a, b\}$. Найдем $X \times Y$, $Y \times X$, X^2 , $X \times Y \times X$.

Решение. Имеем:

$$X \times Y = \{(0, a), (0, b), (1, a), (1, b)\};$$

$$Y \times X = \{(a, 0), (a, 1), (b, 0), (b, 1)\};$$

$$X^2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\};$$

$$X \times Y \times X = \{(0, a, 0), (0, b, 0), (1, a, 0), (1, b, 0), (0, a, 1), (0, b, 1), (1, a, 1), (1, b, 1)\}.$$

1.5. Относительно каждого из приведенных ниже отображений установим, является ли оно инъективным, сюръективным, биективным:

а) $f: \mathbb{N} \rightarrow 2\mathbb{N}$ — отображение множества натуральных чисел в множество четных натуральных чисел, заданное формулой $f(x) = 2x$;

б) $f: \mathbb{R} \rightarrow \mathbb{Z}$ — отображение множества действительных чисел в множество целых чисел, ставящее в соответствие каждому числу x его целую часть, $f(x) = [x]$;

в) $f: \mathbb{Q} \setminus \{0\} \rightarrow \mathbb{Z} \times \mathbb{N}$ — отображение, ставящее в соответствие рациональному числу, отличному от нуля, пару (p, q) , где $p \in \mathbb{Z}$ — числитель, а q — знаменатель представляющей это число несократимой дроби;

г) $f: \{1, 2, 3, 4\} \rightarrow \{1, 2, 3, 4\}$ — отображение, которое ставит в соответствие числу x остаток от деления числа $3x$ на 5.

Решение. а) Данное отображение инъективно: если $x \neq y$, то $2x \neq 2y$. Оно также сюръективно, так как у каждого четного числа $2x$ есть прообраз x . В соответствии с определением отображение f биективно.

б) Это отображение сюръективно, поскольку у каждого целого x есть прообразы (например, само число x); не инъективно, поскольку, например, $[2, 4] = [2, 6] = 2$, и, следовательно, не биективно.

в) Отображение f инъективно, так как представление рационального числа в виде несократимой дроби единственно. Отображение f не сюръективно, так как, например, у пары $(2, 4)$ нет прообраза, дробь $2/4$ сократима.

г) Запишем данное отображение в явном виде: $f(1) = 3, f(2) = 1, f(3) = 4, f(4) = 2$. Мы видим, что это отображение биективно.

Задания для самостоятельной работы

1.6. Пусть универсальное множество U — множество всех студентов университета; A — множество всех студентов первого курса; B — множество студентов, получающих стипендию; C — множество студентов, не имеющих академических задолженностей. Укажите характеристические свойства элементов следующих множеств: а) $\overline{A \cap B}$; б) $A \cup (B \cap \overline{C})$. Изобразите множества A, B, C на диаграмме Эйлера — Венна.

1.7. Пусть $A = \{1, 2\}, B = \{2, 3\}, C = \{1, 3\}$. Найдите: а) $A \cup B \cup C$; б) $A \cap B \cap C$; в) $A \setminus (B \cup C)$; г) $(A \setminus B) \cup C$; д) $A \Delta (B \cup C)$.

1.8. Пусть $U = \{1, 2, 3, 4, 5, 6\}, A = \{1, 2, 3\}, B = \{1, 3, 5, 6\}, C = \{2, 5, 6\}$. Найдите: а) $A \setminus C$; б) $B \Delta C$; в) $C \setminus B$; г) $\overline{A \cup B}$; д) $A \cap \overline{C}$; е) $(C \cup A) \setminus B$.

1.9. Пусть $U = \mathbb{R}$ — универсальное множество, A — множество решений неравенства $x^2 - 5x + 4 \leq 0$, B — множество решений неравенства $x^2 > 2$. Найдите: а) $A \cap B$; б) $A \cap \overline{B}$; в) $\overline{A \cap \overline{B}}$; г) $A \Delta B$; д) $\overline{A \Delta B}$.

1.10. а) Даны два непересекающихся множества A и B . Что представляют собой множества $A \setminus B$ и $A \Delta B$?

б) Пусть A и B — такие множества, что $A \cap \overline{B} = \emptyset$. Что представляют собой множества $A \cap B$ и $A \cup B$?

1.11. Докажите справедливость следующих тождеств:

а) $(A \cap B) \cup (A \cap \overline{B}) = A$; б) $(\overline{A \Delta B}) \Delta C = A \Delta (B \Delta C)$;

в) $A \setminus (A \setminus B) = A \cap B$; г) $A \cup (\overline{A \cap B}) = A \cup B$.

1.12. Пусть $X = \{a, b\}, Y = \{b, c, d\}$. Найдите $X \times Y, Y \times X, Y^2, X \times Y \times X$.

1.13. Относительно каждого из приведенных ниже отображений установите, является ли оно инъективным, сюръективным, биективным:

а) $f: \mathbb{R} \rightarrow \mathbb{R}$ — отображение множества действительных чисел в себя, заданное формулой $f(x) = 3x$;

- б) $f: \mathbb{R} \rightarrow [0; 1)$ — отображение множества действительных чисел в полуинтервал $[0; 1)$, ставящее в соответствие каждому числу x его дробную часть, $f(x) = \{x\}$;
в) $f: \{1, 2, 3, 4, 5, 6\} \rightarrow \{1, 2, 3, 4, 5, 6\}$ — отображение, которое ставит в соответствие числу x остаток от деления числа $2x$ на 7;
е) $f: \{0, 1, 2, 3, 4, 5\} \rightarrow \{0, 1, 2, 3, 4, 5\}$ — отображение, которое ставит в соответствие числу x остаток от деления числа $4x$ на 6.

1.14. Пусть $f: X \rightarrow Y$ и $g: Y \rightarrow Z$ — некоторые отображения, а $h = fg: X \rightarrow Z$. Докажите, что справедливы следующие утверждения:

- а) если композиция $fg: X \rightarrow Z$ инъективна, отображение $f: X \rightarrow Y$ также инъективно;
б) если композиция $fg: X \rightarrow Z$ сюръективна, отображение $g: Y \rightarrow Z$ также сюръективно.

Глава 2

СЧЕТНЫЕ МНОЖЕСТВА

В результате освоения материала данной главы студент должен:

знать

- теоретические основы сравнения бесконечных множеств по мощности;
- основные свойства счетных множеств;
- принцип математической индукции;
- определяющие свойства натурального ряда;

уметь

- классифицировать множества по их мощности;
- устанавливать счетность множеств, используя основные свойства счетных множеств;

• проводить доказательства методом математической индукции;

владеть

- методами сравнения мощности бесконечных множеств;
 - навыками построения индуктивных доказательств.
-

2.1. Мощность множества

Напомним, что для конечного множества A мы обозначаем через $|A|$ число его элементов. Будем называть число элементов конечного множества его **мощностью**. Мощности конечных множеств A и B совпадают в том и только том случае, когда между элементами этих множеств можно установить взаимно однозначное соответствие.

Если $f: A \rightarrow B$ — отображение множеств, то $|f(A)| \leq |A|$ (некоторые элементы множества A могут «склеиться»). Отображение f инъективно тогда и только тогда, когда $|f(A)| = |A|$ («склеек» не происходит). Для конечных множеств отображение f сюръективно тогда и только тогда, когда $|f(A)| = |B|$.

Пусть A и B — конечные множества одинаковой мощности, $|A| = |B|$, а $f: A \rightarrow B$ — некоторое отображение. Тогда следующие условия равносильны:

- f инъективно;
- f сюръективно;
- f биективно (является взаимно однозначным соответствием).

В случае бесконечных множеств ситуация оказывается более сложной. Например, формулой $f(n) = 2n$ определяется отображение f множества натуральных чисел в себя, которое инъективно, но не сюръективно.

В общем случае говорят, что множества A и B **равномощны**, и пишут $|A| = |B|$, если между элементами этих множеств можно установить взаимно однозначное соответствие. Если существует инъективное отображение множества A в множество B , то говорят, что мощность A не превосходит мощности B , и пишут $|A| \leq |B|$.

Теорема 2.1 (Кантора — Бернштейна). Если существуют инъективные отображения $f: A \rightarrow B$ и $g: B \rightarrow A$, то множества A и B равномощны. Иными словами: если $|A| \leq |B|$ и $|B| \leq |A|$, то $|A| = |B|$.

► **Доказательство.** Положим $A_0 = A$ и $A_1 = g(B)$. Поскольку g устанавливает взаимно однозначное соответствие между элементами множеств B и $A_1 = g(B)$, достаточно показать, что имеется взаимно однозначное соответствие между элементами множеств A и A_1 .

Рассмотрим отображение $h: A \rightarrow A$, равное композиции отображений f и g . Как композиция инъективных отображений, оно инъективно. Определим индуктивно последовательность множеств A_0, A_1, \dots , полагая $A_0 = A$; $A_1 = g(B)$; $A_{i+2} = h(A_i)$, $i = 0, 1, 2, \dots$.

Очевидно, $A_0 \supseteq A_1$. Далее, $A_1 = g(B) \supseteq g(f(A)) = A_2$. Поэтому

$$A_2 = h(A_0) \supseteq h(A_1) = A_3, A_3 = h(A_1) \supseteq h(A_2) = A_4, \dots$$

Таким образом,

$$A_0 \supseteq A_1 \supseteq A_2 \supseteq \dots \supseteq A_i \supseteq A_{i+1} \supseteq \dots$$

Положим

$$C_i = A_i \setminus A_{i+1}, i = 0, 1, \dots; C = \bigcap_{i=0}^{\infty} A_i.$$

Отображение h устанавливает взаимно однозначное соответствие между элементами множеств C_i и C_{i+2} для всех $i = 0, 1, 2, \dots$.

Множества $C, C_i, i = 0, 1, 2, \dots$, образуют разбиение множества A , т.е. они попарно не пересекаются, а их объединение составляет все множество A :

$$A = C \cup C_0 \cup C_1 \cup C_2 \cup C_3 \cup \dots$$

Точно так же множества $C, C_i, i = 1, 2, \dots$, образуют разбиение множества A_1 :

$$A_1 = C \cup C_1 \cup C_2 \cup C_3 \cup \dots$$

Перепишем эти разложения в следующем виде:

$$A = (C \cup C_1 \cup C_3 \cup \dots) \cup (C_0 \cup C_2 \cup C_4 \cup \dots);$$

$$A_1 = (C \cup C_1 \cup C_3 \cup \dots) \cup (C_2 \cup C_4 \cup \dots).$$

Отображение $\varphi: A \rightarrow A_1$, при котором

$$\varphi(x) = x, \text{ если } x \in C \cup C_1 \cup C_3 \cup \dots;$$

$$\varphi(x) = h(x), \text{ если } x \in C_0 \cup C_2 \cup C_4 \cup \dots,$$

устанавливает взаимно однозначное соответствие между элементами множеств A и A_1 . ◀

Следующие две теоремы приведем без доказательства.

Теорема 2.2 (Цермело). Для любых множеств A и B выполняется одно из трех условий: $|A| < |B|$, $|B| < |A|$, $|A| = |B|$.

Теорема 2.3. Если существует сюръективное отображение множества A на множество B , то $|A| \geq |B|$.

Замечание 2.1. Утверждение теоремы 2.3 в определенном смысле равносильно так называемой **аксиоме выбора**. Согласно аксиоме выбора если задано семейство множеств, то можно выбрать по элементу из каждого мно-

жества, входящего в это семейство, и составить из этих элементов новое множество. В аксиоматической теории множеств была установлена независимость аксиомы выбора от остальных аксиом теории множеств.

Приведенные три теоремы практически очевидны для конечных множеств. Их утверждения верны также и для бесконечных множеств и показывают, что сравнение по мощности бесконечных множеств обладает рядом «привычных» свойств сравнения по мощности конечных множеств.

В заключение покажем, что существуют множества сколь угодно больших мощностей.

Теорема 2.4 (Кантора). *Каково бы ни было множество A , множество всех его подмножеств 2^A имеет мощность строго большую, чем само множество A , т.е. $|A| < |2^A|$.*

► **Доказательство.** Соответствие $x \rightarrow \{x\}$, при котором каждому элементу x множества A сопоставлено одноэлементное подмножество $\{x\}$, задает инъективное отображение множества A в множество 2^A . Следовательно, $|A| \leq |2^A|$. Покажем теперь, что $|A| \neq |2^A|$. Предположим противное, т.е. что существует биективное отображение $f: A \rightarrow 2^A$.

Положим $D = \{x \in A \mid x \notin f(x)\}$. Тогда $x \in D$ в том и только том случае, если $x \notin f(x)$. Поскольку f биективно, существует такой элемент $d \in A$, что $f(d) = D$. Это приводит к противоречию: $d \in D$ тогда и только тогда, когда $d \notin D$. ◀

2.2. Натуральный ряд

Одно из наиболее просто устроенных бесконечных множеств — **ряд натуральных чисел**.

Неформально под натуральным рядом понимают последовательность чисел

$$0, 1, 2, 3, \dots$$

(мы включаем в натуральный ряд число 0, что делает более удобным изучение ряда вопросов дискретной математики).

В современной математике существование натурального ряда является одним из базовых постулатов. В соответствии с ним существует множество \mathbb{N} , удовлетворяющее определенным условиям — **аксиомам натурального ряда**.

Определение 2.1. Натуральный ряд — это множество \mathbb{N} вместе с отображением непосредственного следования $s: \mathbb{N} \rightarrow \mathbb{N}$, $s(x) = x'$, удовлетворяющие следующим условиям (аксиомам).

1. Множество \mathbb{N} содержит элемент, обозначаемый через 0, который не следует ни за каким элементом: $0 \in \mathbb{N}$ и $0 \neq s(x)$, каков бы ни был элемент $x \in \mathbb{N}$.

2. Отображение непосредственного следования инъективно: если $s(x) = s(y)$, то $x = y$.

3. Аксиома индукции: единственное подмножество множества \mathbb{N} , которое, во-первых, содержит 0 и, во-вторых, вместе с каждым элементом x содержит непосредственно следующий за ним элемент $s(x)$, — это само множество \mathbb{N} .

Из первых двух условий следует, что последовательность

$$0, s(0), s(s(0)), s(s(s(0))), \dots$$

не содержит повторяющихся элементов. В самом деле, если, например, $s(s(0)) = s(s(s(s(0))))$, то по аксиоме 2 $s(0) = s(s(s(0)))$ и $0 = s(s(0))$, что противоречит аксиоме 1. Аксиома индукции говорит о том, что элементами этой последовательности исчерпывается все множество \mathbb{N} . Таким образом, повторяя отображение s , можно, начав с 0 , добраться до произвольного $x \in \mathbb{N}$ за конечное число шагов.

Для каждого натурального числа x , кроме числа 0 , имеется однозначно определенное непосредственно предшествующее ему число, т.е. такое число y , что $s(y) = x$. Это несложно доказать, используя определение натурального ряда. Сначала заметим, что непосредственно предшествующее число определено однозначно: если $s(y) = x$ и $s(z) = x$, то $y = z$, поскольку отображение непосредственного следования инъективно. Далее, пусть A — множество, содержащее число 0 и все натуральные числа, для которых имеется непосредственно предшествующее число. Если $x \in A$, то $s(x) \in A$, так как x является числом, непосредственно предшествующим $s(x)$. В соответствии с аксиомой индукции множество A совпадает с натуральным рядом \mathbb{N} .

Используя привычные обозначения $s(0) = 1, s(s(0)) = 2, s(s(s(0))) = 3, \dots$, получаем $\mathbb{N} = \{0, 1, 2, 3, \dots\}$.

Элементы натурального ряда называют **натуральными числами**. Иногда натуральный ряд начинают не с нуля, а с единицы. Основываясь на принципе математической индукции, для натурального ряда можно определить операции сложения и умножения и отношение порядка. Начнем с операции сложения.

Пусть $a \in \mathbb{N}$. Рассмотрим подмножество G в $\mathbb{N} \times \mathbb{N}$, удовлетворяющее следующим условиям:

- $(0, z) \in G$ тогда и только тогда, когда $z = a$;
- если $(x, y) \in G$, то $(s(x), z) \in G$ тогда и только тогда, когда $z = s(y)$.

Обозначим через A подмножество множества натуральных чисел, удовлетворяющее следующему условию: $x \in A$ тогда и только тогда, когда имеется единственный элемент y , для которого $(x, y) \in G$. Из определения множества G следует, что $0 \in A$ и если $x \in A$, то $s(x) \in A$. По аксиоме индукции $A = \mathbb{N}$. Таким образом, множество G является графиком некоторой функции $f: \mathbb{N} \rightarrow \mathbb{N}$, удовлетворяющей следующим условиям:

$$f(0) = a; f(s(x)) = s(f(x)).$$

Полагая $f(x) = a + x$, эти условия можно записать в более привычных обозначениях:

$$a + 0 = a; a + s(x) = s(a + x). \quad (2.1)$$

Формулы (2.1) служат **рекурсивным определением** функции $f(x) = a + x$ и доставляют пример **определения по индукции**.

Полагая в формулах (2.1) $x = 0$, получаем $a + s(0) = s(a + 0)$, т.е. $s(a) = a + 1$. С учетом этих обозначений формулы (2.1) переписутся следующим образом:

$$a + 0 = a; a + (x + 1) = (a + x) + 1. \quad (2.2)$$

В соответствии с определением получаем теперь, например,

$$3 + 2 = 3 + (1 + 1) = (3 + 1) + 1 = 4 + 1 = 5.$$

В качестве еще одного примера определения по индукции приведем определение операции умножения.

Пусть $a \in \mathbb{N}$. Зададим функцию $f(x) = a \times x$ условиями

$$a \times 0 = 0; \quad a \times (x + 1) = a \times x + x. \quad (2.3)$$

Аксиома индукции равносильна следующему **принципу полного упорядочения**: каждое непустое подмножество множества натуральных чисел содержит наименьший элемент (т.е. элемент, который не следует ни за одним элементом этого множества).

2.3. Метод математической индукции

Многие математические доказательства основываются на аксиоме индукции, которую можно переформулировать следующим образом.

Принцип полной индукции. Пусть P — утверждение относительно натуральных чисел n , такое что:

- 1) P верно для $n = 0$;
 - 2) из справедливости P для $n = k$ следует справедливость P для $n = k + 1$.
- Тогда P верно для всех натуральных чисел.

Замечание 2.2. Чтобы показать, что эта формулировка следует из аксиомы индукции, достаточно рассмотреть множество $A = \{x \in \mathbb{N} \mid P \text{ верно для } x\}$.

Для доказательства в обратную сторону множеству $A \subseteq \mathbb{N}$ можно сопоставить свойство P «быть элементом множества A ».

О доказательствах, основанных на аксиоме индукции, говорят, что они проведены **методом математической индукции**. Такие доказательства имеют следующую структуру:

- устанавливается справедливость P для $n = 0$ (*база индукции*);
- предполагается, что P справедливо для некоторого произвольного, но фиксированного $n = k$ (*индуктивное предположение*);
- доказывается, что из индуктивного предположения следует: P верно для $n = k + 1$ (*индуктивный шаг*).

В качестве примеров проведем два доказательства методом математической индукции.

Пример 2.1. Докажем, что сумма первых натуральных чисел от 0 до n включительно равна $1/2n(n + 1)$: $0 + 1 + \dots + n = [n(n + 1)]/2$.

Решение. Утверждение верно при $n = 0$: имеем $0 = 1/2 \cdot 0 \cdot (0 + 1)$ (база индукции).

Предположим, что доказываемое утверждение верно для $n = k$ (индуктивное предположение), т.е.

$$0 + 1 + \dots + k = k(k + 1)/2.$$

Покажем, что тогда оно верно и для $n = k + 1$, т.е.

$$0 + 1 + \dots + k + (k + 1) = [(k + 1)(k + 2)]/2$$

(индуктивный шаг).

Сумма во втором равенстве отличается от суммы из первого равенства слагаемым $k + 1$. Поэтому в силу индуктивного предположения получаем

$$0 + 1 + \dots + k + (k + 1) = k(k + 1)/2 + k + 1 = [(k + 1)(k + 2)]/2,$$

что и требовалось доказать.

В соответствии с принципом математической индукции доказываемое утверждение верно для всех n .

Пример 2.2. Докажем, что число подмножеств множества, содержащего n элементов, равно 2^n .

Решение. Утверждение верно при $n = 0$: пустое множество \emptyset (единственное множество, содержащее 0 элементов) имеет ровно одно подмножество \emptyset .

Предположим теперь, что всякое множество с $n = k$ элементами имеет 2^k подмножеств, и покажем, что множество с $n = k + 1$ элементами имеет 2^{k+1} подмножеств. Пусть A — произвольное множество, содержащее $n = k + 1$ элементов. Так как $k + 1 > 0$, то A содержит хотя бы один элемент. Пусть $a \in A$. Разобьем совокупность всех подмножеств множества A на два класса. В класс P входят все подмножества, содержащие a , в класс Q входят все подмножества, не содержащие a :

$$P = \{X \subseteq A \mid a \in X\}; \quad Q = \{Y \subseteq A \mid a \notin Y\}.$$

Положим $A' = A \setminus \{a\}$. Множество A' содержит k элементов, так что по индуктивному предположению число его подмножеств равно 2^k . Но подмножества множества A' — это в точности подмножества множества A , не содержащие a . Следовательно, по индуктивному предположению $|Q| = 2^k$. Пара взаимно обратных отображений $P \rightarrow Q$, $X \mapsto X \setminus \{a\}$, и $Q \rightarrow P$, $Y \mapsto Y \cup \{a\}$ устанавливает между P и Q взаимно однозначное соответствие, так что $|P| = |Q| = 2^k$. Поэтому общее число подмножеств множества A составляет

$$|U| + |V| = 2^k + 2^k = 2^{k+1},$$

что и требовалось доказать.

Иногда принцип полной индукции применяется в следующей форме.

Пусть P — утверждение относительно натуральных чисел n , такое что:

1) P верно для $n = n_0$;

2) из справедливости P для $n = n_0, n_0 + 1, \dots, n_0 + k$ следует справедливость P для $n = n_0 + k + 1$.

Тогда P верно для всех $n \geq n_0$.

Принцип полной индукции в этой форме может быть сведен к предыдущей формулировке заменой утверждения P утверждением P' : утверждение P имеет место для всех t , таких что $n_0 \leq t \leq n$.

Пример 2.3. Докажем методом математической индукции, что каждое натуральное число $n \geq 2$ может быть представлено в виде произведения простых чисел.

Решение. Утверждение верно для $n = 2$: число 2 является простым, и произведение состоит из одного множителя. Предположим теперь, что любое натуральное число, не превосходящее натурального числа k , $k \geq 2$, может быть представлено в виде произведения простых чисел. Докажем, что тогда и число $k + 1$ может быть представлено в виде произведения простых чисел. Если число $k + 1$ простое, подходящее произведение состоит из одного множителя $k + 1$. Если число $k + 1$ составное, его можно представить в виде произведения $k + 1 = ab$, где a и b — натуральные числа, такие что $2 \leq a, b \leq k$. По предположению числа a и b представимы в виде произведения простых чисел. Следовательно, то же верно и для их произведения, равного числу $k + 1$.

2.4. Свойства счетных множеств

Начальный отрезок натурального ряда $[0; n] = \{1, 2, \dots, n\}$ конечен и содержит $n + 1$ элемент. Сам же натуральный ряд $\mathbb{N} = \{0, 1, 2, \dots\}$ бесконечен. Не может быть инъективным никакое отображение \mathbb{N} в $[0; n]$. Следова-

но, $|N| > n$, т.е. мощность натурального ряда превосходит любое натуральное число.

Определение 2.2. Множества, равномощные натуральному ряду, называются **счетными**.

Для обозначения мощности счетных множеств используется символ \aleph_0 (читается «алеф нуль»). Если множество A конечно или счетно, его элементы могут быть занумерованы, т.е. расположены в виде списка (конечного или бесконечного)

$$a_0, a_1, a_2, a_3, \dots$$

так, что всякий элемент множества A рано или поздно встретится в этом списке. Если множество A конечно, то и список конечен; в противном случае список оказывается бесконечным. Ясно, что при таких обозначениях отображение $i \rightarrow a_i$ — это и есть та самая биекция начального отрезка или всего натурального ряда на множество A , которая устанавливает конечность или счетность множества A .

Пример 2.4. Множество четных чисел счетно. Четные числа можно представить списком $0, 2, 4, 6, \dots$. Соответствие очевидно: $n \leftrightarrow 2n$. Точно так же счетно и множество нечетных чисел $1, 3, 5, \dots$. Здесь соответствие можно задать так: $n \leftrightarrow 2n + 1$.

Пример 2.5. Множество рациональных чисел счетно. Напомним, что всякое рациональное число, отличное от нуля, однозначно записывается в виде несократимой дроби p/q , где p и q — взаимно простые целые числа и $q > 0$. Будем считать, что число 0 представляется дробью $0/1$. Составим список, содержащий все рациональные числа, в порядке возрастания величины $|p| + q$:

$$0/1; -1/1; 1/1; -2/1; -1/2; 1/2; 2/1; \dots$$

Ясно, что любое рациональное число появится в этом списке через конечное число шагов и получит свой номер.

Укажем некоторые свойства счетных множеств.

Теорема 2.5. *Всякое подмножество счетного множества конечно или счетно.*

► **Доказательство.** Достаточно доказать справедливость утверждения для множества натуральных чисел: всякое подмножество A множества натуральных чисел конечно или счетно. Составим список элементов множества A в порядке их возрастания. Если этот список конечен — множество A конечно; если бесконечен — счетно. ◀

Из предыдущего утверждения вытекает, что счетные множества являются наименьшими по мощности бесконечными множествами: если $|A| \leq \aleph_0$, то A конечно или счетно.

Теорема 2.6. *Образ счетного множества относительно произвольного отображения является конечным или счетным множеством.*

► **Доказательство.** Пусть множество B является образом счетного множества A относительно некоторого отображения. Тогда $|B| \leq |A|$ по теореме 2.3 и, значит, B конечно или счетно.

Если элементы множества A представлены списком с повторениями

$$a_0, a_1, a_2, a_3, \dots,$$

т.е. списком, в котором некоторые элементы могут появляться многократно, это означает, что отображение $i \rightarrow a_i$ сюръективно (но, возможно, не инъективно). Таким образом, множество A является образом натурального ряда, и потому конечно или счетно. ◀

Теорема 2.7. *Всякое бесконечное множество содержит счетное подмножество.*

► **Доказательство.** Пусть A — бесконечное множество. Тогда $|A| \geq \aleph_0$. Но это неравенство означает, что существует инъективное отображение множества натуральных чисел в A . Образ этого отображения — счетное подмножество множества A . ◀

Теорема 2.8. *Объединение любого конечного (непустого) или счетного семейства счетных множеств счетно.*

► **Доказательство.** Пусть счетные множества A_0, A_1, \dots представлены списками своих элементов:

$$A_0 = \{a_{00}, a_{01}, a_{02}, a_{03}, \dots\};$$

$$A_1 = \{a_{10}, a_{11}, a_{12}, a_{13}, \dots\};$$

$$A_2 = \{a_{20}, a_{21}, a_{22}, a_{23}, \dots\};$$

$$A_3 = \{a_{30}, a_{31}, a_{32}, a_{33}, \dots\};$$

$$\dots\dots\dots$$

Составим список объединения этих множеств A , располагая элементы объединения в порядке возрастания суммы индексов:

$$A = \{a_{00}, a_{01}, a_{10}, a_{02}, a_{11}, a_{20}, a_{03}, \dots\}$$

(если некоторые из множеств имеют общие элементы, в этом списке возможны повторения). Множество A бесконечно и, значит, счетно. ◀

Из предыдущего утверждения вытекает, что объединение счетного числа конечных множеств конечно или счетно.

Теорема 2.9. *Декартово произведение конечного числа счетных множеств счетно.*

► **Доказательство.** Пусть $A = \{a_0, a_1, a_2, a_3, \dots\}$, $B = \{b_0, b_1, b_2, b_3, \dots\}$ — счетные множества. Покажем, что счетно декартово произведение $A \times B$. Составим список его элементов, подобно тому как составлялся список рациональных чисел:

$$(a_0, b_0), (a_0, b_1), (a_1, b_0), (a_0, b_2), (a_1, b_1), (a_2, b_0), \dots$$

Если счетны множества A, B, C , то счетно $A \times B$, а вместе с ним и $A \times B \times C = (A \times B) \times C$ как произведение двух счетных множеств. Аналогично устанавливается счетность любого конечного семейства счетных множеств. ◀

Теорема 2.10. *Пусть $L = \{a, b, \dots\}$ — счетный алфавит. Тогда множество слов над алфавитом L (т.е. конечных упорядоченных наборов символов алфавита) счетно.*

► **Доказательство.** Множество буквенных слов можно естественным образом отождествить с L^n , счетность которого следует из теоремы 2.9. Теперь достаточно сослаться на теорему 2.8: множество всех слов представляет собой объединение счетного семейства счетных множеств: слов из одной буквы; слов из двух букв и т.д. ◀