

Содержание

Предисловие	11
Введение	13
1. Множество	13
2. Функция	14
3. Отношение	16
4. Отношение эквивалентности	17
5. Каноническое разложение функции.....	18
6. Мощность множества. Счетные и несчетные множества.....	19
7. Мощность континуума	20
8. Кардинальные числа. Сравнение мощностей.....	21
Часть I. МОДУЛЯРНАЯ АЛГЕБРА	25
Глава 1. Делимость	26
1.1. Позиционная система счисления	26
1.2. Простые числа	28
1.3. Факторизация целых чисел	29
1.4. Наибольший общий делитель.....	30
1.4.1. Алгоритм Евклида вычисления наибольшего общего делителя.....	31
1.4.2. Расширенный алгоритм Евклида вычисления наибольшего общего делителя	34
1.5. Наименьшее общее кратное.....	35
1.6. Непрерывные (цепные) и подходящие дроби.....	37
1.6.1. Вычисление подходящих дробей.....	38
1.6.2. Алгоритм вычисления подходящих дробей	39
Глава 2. Функции Мебиуса и Эйлера	41
2.1. Функции $\lfloor x \rfloor$, $ x $, $\{x\}$ для вещественного x	41
2.2. Мультипликативные функции	42
2.3. Функция и формула обращения Мебиуса	43
2.4. Функция Эйлера	47
Глава 3. Сравнения	49
3.1. Сравнение целых чисел.....	49
3.2. Свойства сравнений	49
3.3. Полная система вычетов.....	51

Операции над классами	51
3.4. Приведенная система вычетов.....	53
3.5. Теоремы Эйлера и Ферма.....	54
3.6. Классы целых чисел по модулю m , взаимно простых с модулем m	54
3.7. Модулярные арифметические операции	55
3.7.1. Алгоритм вычисления мультипликативно обратного элемента $a^{-1} \pmod{n}$ в \mathbb{Z}_n	56
3.7.2. Алгоритм вычисления модулярной степени в \mathbb{Z}_n	56
3.7.3. Алгоритм вычисления генератора мультипликативной циклической группы \mathbb{Z}_p^* при простом p (перебор).....	57
Глава 4. Сравнения с одной переменной.....	58
4.1. Решение сравнения с переменными	58
4.2. Сравнения первой степени	60
4.3. Система сравнений первой степени.....	61
4.3.1. Попарно взаимно простые модули	61
4.3.2. Алгоритм Гаусса для системы сравнений $x \equiv c_1 \pmod{m_1}, \dots,$ $x \equiv c_k \pmod{m_k}$ с попарно взаимно простыми модулями.....	62
4.3.3. Произвольные модули	63
4.4. Сравнения любой степени с простым модулем	64
4.5. Сравнения произвольной степени по составному модулю	65
Алгоритм решения сравнения $f(x) \equiv 0 \pmod{p^a}$	68
Глава 5. Сравнения второй степени	69
5.1. Квадратичные вычеты по простому модулю	69
5.2. Символ Лежандра	70
5.3. Символ Якоби.....	74
Алгоритм вычисления символа Якоби (и символа Лежандра) $JACOBI(a, n)$	76
5.4. Квадратичные вычеты по составному модулю	77
Глава 6. Примитивные корни и индексы.....	80
6.1. Экспонента, примитивные корни, индексы.....	80
6.1.1. Число классов вычетов данной экспоненты.....	82
6.1.2. Индексы (дискретные логарифмы).....	83
6.2. Примитивные корни по модулям p^a и $2p^a$	83
6.3. Вычисление примитивных корней по модулям p^a и $2p^a$	87
6.4. Индексы по модулям p^a и $2p^a$	88
6.5. Индексы и вычеты	88
6.6. Индексы по модулю 2^a	89
6.7. Индексы по любому составному модулю	91

Глава 7. Универсальные алгебры.....	93
7.1. Алгебры, подалгебры, гомоморфизм алгебр.....	93
7.2. Конгруэнции.....	96
Глава 8. Абстрактная алгебра.....	99
8.1. Полугруппы.....	99
8.2. Циклические полугруппы.....	101
8.3. Группы.....	103
8.3.1. Циклические группы.....	107
8.3.2. Смежные классы. Разложение группы по подгруппе.....	107
8.3.3. Конечные группы и теорема Лагранжа.....	109
8.3.4. Конечные циклические группы.....	109
8.3.5. Алгоритм вычисления всех подгрупп конечной циклической группы.....	111
8.4. Нормальные подгруппы, фактор-группы, теорема о гомоморфизме групп.....	111
8.5. Кольцо.....	114
8.6. Поле.....	117
8.7. Полиномиальные кольца.....	120
8.8. Идеал кольца.....	121
8.8.1. Главный идеал.....	122
8.8.2. Разностное кольцо (кольцо классов вычетов). Сравнения.....	122
8.9. Линейное векторное пространство.....	124
8.10. Булева алгебра.....	126
8.11. Решетка.....	126
Глава 9. Конечные поля.....	128
9.1. Представление конечного поля множеством классов вычетов по модулю неприводимого полинома.....	128
9.2. Поле разложения полинома $x^{p^m} - x$	130
9.3. Циклическость мультипликативной группы поля.....	130
9.4. Задание поля корнем неприводимого полинома.....	131
9.5. Строение конечных полей.....	133
9.5.1. Минимальный полином.....	136
9.5.2. Вычисление минимального полинома.....	137
9.5.3. Подполя конечного поля.....	139
9.5.4. Круговые полиномы.....	142
9.5.5. Алгоритм факторизации полинома $x^{p^m-1} - 1$ на круговые полиномы из $\text{GF}(q)$	144
9.6. Изоморфизм полей Галуа.....	145
9.7. Автоморфизмы поля Галуа.....	146

9.8. Основные алгоритмы для конечных полей.....	147
9.8.1. Алгоритм Евклида для полиномов из $\mathbb{Z}_p[x]$	149
9.8.2. Расширенный алгоритм Евклида для полиномов из $\mathbb{Z}_p[x]$	150
9.8.3. Мультипликативный обратный элемент в \mathbb{F}_{p^m}	153
9.8.4. Модулярная степень в \mathbb{F}_{p^m}	153
9.8.5. Тестирование полинома из $\mathbb{Z}_p[x]$ на неприводимость	153
9.8.6. Порождение случайного неприводимого полинома над \mathbb{Z}_p	153
9.8.7. Тестирование неприводимого полинома на примитивность.....	154
9.8.8. Порождение случайного нормированного примитивного полинома над \mathbb{Z}_p	154
9.8.9. Вычисление порядка элемента конечной группы (метод Гаусса)	154
9.8.10. Вычисление генератора конечной циклической группы (метод Гаусса).....	154

Часть II. КРИПТОГРАФИЯ..... 156

Глава 10. Модулярная алгебра в криптографии..... 157

10.1. Криптография и ее цели	157
10.1.1. Хэш-функция.....	160
10.1.2. Алгоритм MASH-1	161
10.2. Проблема факторизации целых чисел.....	162
10.2.1. ρ -алгоритм Полларда факторизации целых чисел	162
10.2.2. $(p - 1)$ -алгоритм Полларда факторизации целых чисел	163
10.2.3. Алгоритм квадрат-решета факторизации целых чисел.....	164
10.3. Проблема RSA.....	165
10.4. Проблема квадратичного вычета.....	166
10.4.1. Алгоритм вычисления дискретного квадратного корня по простому модулю p	166
10.4.2. Алгоритм вычисления дискретного квадратного корня по простому модулю p , где $p \equiv 3 \pmod{4}$	167
10.4.3. Алгоритм вычисления дискретного квадратного корня по простому модулю p , где $p \equiv 5 \pmod{8}$	167
10.4.4. Алгоритм вычисления дискретного квадратного корня по простому модулю p при большом s	167
10.4.5. Алгоритм вычисления дискретного квадратного корня по модулю $n = p \cdot q$, где p и q есть простые числа.....	167
10.5. Проблема дискретного логарифма	168
10.5.1. Алгоритм «малый шаг – большой шаг» вычисления дискретного логарифма.....	168
10.5.2. ρ -алгоритм Полларда вычисления дискретного логарифма.....	169
10.5.3. Алгоритм Полига-Хеллмана вычисления дискретного логарифма	171

10.6. Проблема подмножества суммы	172
10.6.1. Наивный (переборный) алгоритм решения проблемы суммы.....	172
10.6.2. Алгоритм «встреча посередине» решения проблемы подмножества суммы	172
10.7. Проблема факторизации полиномов над конечным полем	173
10.7.1. Бесквадратная факторизация.....	173
10.7.2. Q-матричный алгоритм Берлекампа	174
10.8. Криптосистема RSA.....	175
10.8.1. Шифросистема RSA	175
10.8.2. Электронная цифровая подпись RSA с использованием хэш-функции	177
10.8.3. Электронная цифровая подпись RSA с извлечением сообщения.....	179
10.9. Криптосистема Эль-Гамала.....	180
10.9.1. Шифросистема Эль-Гамала над числовым полем Галуа $GF(p)$	180
10.9.2. Электронная цифровая подпись Эль-Гамала над числовым полем Галуа $GF(p)$	182
10.9.3. Шифросистема Эль-Гамала над полиномиальным полем Галуа $GF(p^m)$	184
10.9.4. Электронная цифровая подпись Эль-Гамала над полиномиальным полем Галуа $GF(p^m)$	187
10.10. Электронная цифровая подпись DSA.....	189
10.11. Криптографическая система Рабина	192
10.11.1. Шифросистема Рабина.....	192
10.11.2. Электронная цифровая подпись Рабина с извлечением сообщения.....	194
10.11.3. Модифицированная цифровая подпись Рабина с извлечением сообщения.....	195
10.12. Рюкзачная схема шифрования Меркле–Хеллмана.....	198
10.13. Рюкзачная схема шифрования Хора–Ривеста.....	199
10.14. Вероятностные схемы шифрования с открытым ключом.....	203
10.14.1. Вероятностная схема шифрования Голдвассер–Микали	204
10.14.2. Вероятностная схема шифрования Блюма–Голдвассер.....	206
10.15. Электронная цифровая подпись Фейге–Фиат–Шамира	208
10.16. Электронная цифровая подпись GQ.....	210
10.17. Электронная цифровая подпись Шнорра с хэш-функцией	211
10.18. Электронная цифровая подпись Ниберга–Рюппеля с извлечением сообщения.....	213

Глава 11. Криптография на эллиптических кривых над конечными полями	215
11.1. Эллиптические кривые.....	215

11.2. Эллиптические кривые над полем вещественных чисел	216
11.3. Эллиптические кривые в конечных полях.....	218
11.4. Сложение точек эллиптической кривой $E(F) y^2 = x^3 + ax + b$ над полем F характеристики $\text{char}(F) > 3$	219
11.5. Сложение точек эллиптической кривой $E(F) y^2 = x^3 + ax^2 + bx + c$ с над полем F характеристики $\text{char}(F) = 3$	220
11.6. Сложение точек суперсингулярной эллиптической кривой $E(F)$ $y^2 + cy = x^3 + ax + b$ над полем F характеристики $\text{char}(F) = 2$	222
11.7. Сложение точек несуперсингулярной эллиптической кривой $E(F)$ $y^2 + xy = x^3 + ax^2 + b$ над полем F характеристики $\text{char}(F) = 2$	224
11.8. Вычисление $k \cdot P$	226
11.9. Порядок группы точек эллиптической кривой	226
11.9.1. Алгоритм вычисления порядка элемента группы точек эллиптической кривой (метод Гаусса)	228
11.9.2. Алгоритм вычисления генератора циклической группы точек эллиптической кривой (метод Гаусса)	228
11.10. Криптосистемы на эллиптических кривых над числовым конечным полем	229
11.10.1. Шифросистема Эль-Гамала на эллиптических кривых над числовым конечным полем.....	229
11.10.2. Электронная цифровая подпись (ЭЦП) Эль-Гамала на эллиптических кривых над числовым конечным полем	232
Глава 12. Шифросистема NTRU на конечных полиномиальных кольцах.....	235
12.1. Проблема кратчайшего вектора в целочисленной решетке	235
12.2. Шифросистема NTRU	236
Глава 13. Блочные и потоковые шифры.....	241
13.1. Блочный шифр RC5-S.....	241
13.2. Потоковые шифры.....	245
13.2.1. Линейный регистр сдвига с обратной связью.....	245
13.2.2. Расшифровка линейного регистра сдвига	247
Часть III. КОДИРОВАНИЕ	250
Глава 14. Линейные коды	251
14.1. Линейные пространства над полями Галуа.....	251
14.2. Расстояние Хэмминга.....	252
14.3. Порождающая и проверочная матрицы.....	253
14.4. Декодирование в ближайшее кодовое слово.....	255

14.5. Расстояние и корректирующая способность кода.....	256
14.6. Каноническая форма базисных матриц систематического кода.....	256
14.6.1. Каноническая проверочная матрица	256
14.6.2. Каноническая кодирующая матрица	257
14.6.3. Алгоритм систематизации несистематического линейного кода.....	260
14.7. Декодирование линейного кода (декодер).....	261
14.8. Бинарный код Хэмминга.....	263
Глава 15. Циклические коды	266
15.1. Порождающая и проверочная матрицы циклического кода	266
15.2. Канонические порождающая и проверочная матрицы циклического кода.....	268
15.3. Систематический кодер циклического кода.....	270
Глава 16. Коды Боуза–Чоудхури–Хоквингема (коды БЧХ)	271
16.1. Построение кодов БЧХ.....	271
16.2. Декoder Питерсона–Горенштейна–Цирлера	276
16.3. Алгоритм Питерсона–Горенштейна–Цирлера БЧХ-кода с исправлением t и менее ошибок	281
Глава 17. Коды сжатия информации	298
17.1. Алфавитное кодирование.....	298
17.2. Кодирование с минимальной избыточностью.....	299
17.3. Алгоритм Фано построения разделимой префиксной схемы алфавитного кодирования, близкого к оптимальному	300
17.4. Оптимальное кодирование.....	301
17.5. Алгоритм Хаффмана оптимальной разделимой префиксной схемы алфавитного кодирования	303
17.6. Кодер и декодер Прюфера для деревьев	309
Глава 18. Основы теории информации	311
18.1. Количество информации и энтропия	311
18.1.1. Равновероятность знаков алфавита.....	311
18.1.2. Разновероятность знаков алфавита. Формулы Шеннона	313
18.2. Свойства энтропии.....	313
18.3. Энтропия при непрерывном сообщении	316
18.4. Условная энтропия	319
18.5. Взаимная энтропия	326

Приложения	327
1. Множества, функции, отношения	327
2. Модулярная алгебра.....	334
3. Криптография.....	341
4. Кодирование.....	342
5. Информация и энтропия.....	345
Литература.....	347
Обозначения.....	349

Предисловие

Дискретная математика является фундаментом для всего компьютеринга, включая программную инженерию. Она столь же важна для компьютерных дисциплин, как и математический анализ для остальных инженерных специальностей.

Дискретная математика есть область науки, посвященная изучению дискретных объектов и структур. В широком смысле она включает в себя: теорию множеств, отношения и функции, теорию чисел, абстрактную алгебру, математическую логику, булеву алгебру, логику высказываний, цифровую логику, логику предикатов, методы доказательства, комбинаторный анализ, рекуррентные соотношения, теорию графов и сетей, основы алгоритмизации, теорию автоматов и формальных языков, теорию алгоритмов, вычислимость и вычислительную сложность, дискретную вероятность, целочисленную оптимизацию, криптографию, теорию информации и кодирования.

Дискретная математика стала важным звеном математического образования инженера.

Настоящая книга является первой в серии задуманных авторским коллективом книг по дискретной математике. Она предназначена студентам бакалавриата, изучающим академический курс «Дискретная математика» для формирования у студентов следующих компетенций:

- 1) способность к самоорганизации и самообразованию в области дискретных математических моделей;
- 2) готовность применить аппарат дискретной математики для решения поставленных практических задач;
- 3) способность применить соответствующую задаче математическую модель с проверкой ее адекватности;
- 4) способность провести анализ результатов моделирования для принятия решений на основе полученных результатов.

В предлагаемой книге авторы сосредоточились на изложении математических основ современной теории кодирования и криптографии, доступных для понимания студентов первых лет обучения.

Основные теоретические и практические положения, изложение и анализ практических алгоритмов, иллюстрируемые большим числом примеров, позволят сформировать прочную теоретическую базу, необходимую для дальнейшей работы практикующих программистов и ИТ-специалистов.

В приложении предлагаются задачи, которые могут быть использованы как для проведения практических занятий, так и для самостоятельной работы.

Авторы выражают глубокую благодарность рецензентам Калягину В. А., Ульянову М. В. и научному редактору книги Захарову В. А. за замечания, позволившие существенно улучшить качество книги. Мы также благодарны преподавателям

департамента программной инженерии НИУ ВШЭ Ахметсафиной Р. З., Гринкругу Е. М., Дворянскому Л. В., Дегтяреву К. Ю., Каленковой А. А., Ломазовой И. А., Подбельскому В. В., Шилову В. В., а также Амосову А. А., Дубинскому Ю. А., Фролову А. Б. из НИУ МЭИ за стимулирующие беседы. Авторы благодарят студентов Горденко М. К., Сапожкова Е. Д., Чиркову Е. Н. за активное участие в составлении и апробации задач и упражнений приложения.

Введение

1. Множество

Понятие множества неопределимо. Это простейшее исходное понятие человечество сформировало из опыта всего своего исторического развития. То же можно сказать о смысле простейшего отношения принадлежности: элемент a принадлежит множеству A (обозначение $a \in A$) – и о смысле отношения тождества (совпадения, равенства) двух элементов a и b из некоторого множества (обозначение $a = b$). Другими словами, предполагается, что читатель умеет распознавать совпадение или несовпадение двух элементов и устанавливать факт принадлежности или непринадлежности элемента множеству.

Пусть U есть некоторое множество. A есть подмножество множества U , если всякий элемент из множества A принадлежит множеству U . Множество U универсально (универсум), если все рассматриваемые множества есть подмножества множества U .

Пусть A, B, C есть произвольные подмножества множества U ; a, b, c есть элементы множества U . Обозначим символом \emptyset пустое множество, то есть множество без элементов.

Основными неопределяемыми отношениями в теории множеств являются следующие отношения:

- $a = b$, элементы a и b равны (совпадают);
- $a \in A$, элемент a принадлежит множеству A .

Пусть знак \leftrightarrow означает «если и только если»; а знаки $\&$, \vee , \neg , \rightarrow , \forall , \exists есть логические знаки конъюнкции, дизъюнкции, отрицания, импликации, квантора общности и квантора существования. Используем их в общепринятом содержательном смысле. Знак $\exists!$ означает квантор существования единственного элемента.

Обозначим через $a \notin A$ отношение элемент a не принадлежит множеству A и через $a \neq b$ отношение элементы a и b не равны (не совпадают).

Введем далее следующие отношения:

- $A \subseteq B \leftrightarrow \forall a (a \in A \rightarrow a \in B)$, отношение включения множеств, при этом множество A называется подмножеством множества B , а множество B называется надмножеством множества A ;
- $A \supseteq B \leftrightarrow B \subseteq A$;
- $A = B \leftrightarrow A \subseteq B \ \& \ A \supseteq B$, отношение равенства множеств;
- $A \subset B \leftrightarrow A \subseteq B \ \& \ A \neq B$, отношение строгого включения множеств;
- $A \supset B \leftrightarrow B \subset A$.

Обозначим через $P(A)$ (или 2^A) множество всех подмножеств множества A . Введем следующие операции над множествами:

- $A \cup B = \{x \in U: x \in A \vee x \in B\}$, объединение множеств A и B ;
- $A \cap B = \{x \in U: x \in A \& x \in B\}$, пересечение множеств A и B ;
- $A - B = \{x \in U: x \in A \& x \notin B\}$, разность множеств A и B ;
- $\bar{A} = U - A$, дополнение к множеству A ;
- $A \div B = (A \cup B) - (A \cap B)$, симметрическая разность множеств A и B ;
- $A \times B = \{(a, b): a \in A \& b \in B\}$, декартово произведение множеств A и B .

Под натуральным числом понимаем количество элементов конечного множества. Количество элементов пустого множества есть 0.

Распространим декартово произведение на несколько сомножителей:

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n): a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n\}.$$

Определим декартову степень множества

$$A^n = A \times A \times \dots \times A \text{ (} n \text{ раз)}, A^0 = \emptyset.$$

Множества \emptyset и A называются несобственными (тривиальными) подмножествами множества A . Если $A \subset B$ & $A \neq \emptyset$, то A есть собственное подмножество множества B .

Иногда пишут $A \cdot B$ или AB вместо $A \cap B$.

Примем следующие обозначения.

Множество натуральных чисел $\mathbb{N} = \{0, 1, 2, \dots\}$.

Множество положительных натуральных чисел $\mathbb{N}_+ = \{1, 2, \dots\}$.

Множество целых чисел $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$.

Множество $\mathbb{Z}_n = E_n = \{0, 1, 2, \dots, n - 1\}$.

Множество рациональных чисел $\mathbb{Q} = \left\{ \frac{m}{n}: m \in \mathbb{Z}, n \in \mathbb{N}_+ \right\}$.

Множество вещественных чисел $\mathbb{R} = (-\infty, +\infty)$.

Множество неотрицательных вещественных чисел $\mathbb{R}_+ = [0, +\infty)$.

Множество комплексных чисел $\mathbb{C} = \{x + iy: x \in \mathbb{R}, y \in \mathbb{R}\}$, здесь $i^2 = -1$.

2. Функция

Определение. Пусть A и B есть два множества. *Функция* $f: A \rightarrow B$ есть отображение, которое каждому элементу x из A ставит в соответствие некоторый элемент y из B . Это обстоятельство записывается как $y = f(x)$.

Замечание. В этом определении функция f всюду определена. Частично определенная функция $f: A \rightarrow B$ есть отображение, которое каждому элементу из множества A сопоставляет не более одного элемента из множества B . Всюду определенная функция является частным случаем частично определенной функции.

Область определения функции $f: A \rightarrow B$ есть множество $D(f) = \{a \in A: \exists b \in B (f(a) = b)\}$.

Область значений функции $f: A \rightarrow B$ есть множество $R(f) = \{b \in B: \exists a \in A (f(a) = b)\}$.

Образ $Im(f) = \{f(x): x \in A\}$ *функции* $f: A \rightarrow B$ есть множество $f(A)$ всех значений функций f .

Заметим, что $Im f = R(f) = f(A)$.

Если $f(a) = b$, то элемент b есть образ элемента a , а элемент a есть прообраз элемента b .

Полный прообраз элемента $b \in B$ есть множество $f^{-1}(b) = \{a \in A: f(a) = b\}$.

Полный прообраз множества $C \subseteq B$ есть множество $f^{-1}(C) = \{a \in A: f(a) \in C\}$.

Сужение функции f , заданной на множестве A , на подмножество S множества A есть функция g – такая, что $\forall a \in S(g(a) = f(a))$.

Расширение функции f , заданной на множестве A , на надмножество T множества A есть функция h – такая, что $\forall a \in A(h(a) = f(a))$.

Функцию с конечной областью определения удобно задавать таблицей. Например, пусть множества $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 3, 4, 5\}$, функция $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & & 1 & 2 \end{pmatrix}$. Здесь $f(1) = 3$, $f(2)$ не определено, $f(3) = 1$, $f(4) = 2$. Порядок столбцов несуществен.

Область определения $D(f) = \{1, 3, 4\}$, область значений $R(f) = Im(f) = f(A) = \{1, 2, 3\}$.

Определение. Функция $f: A \rightarrow B$ есть взаимно-однозначное отображение (1–1-отображение) между множествами A и B , если

- 1) $\forall b \in B \exists a \in A (f(a) = b)$,
- 2) $\forall a \in A \forall b \in A (a \neq b \Rightarrow f(a) \neq f(b))$.

Замечание. Последнее условие можно заменить на условие

- 2) $\forall a \in A \forall b \in A (f(a) = f(b) \Rightarrow a = b)$.

Функции $f: A \rightarrow B$ и $g: C \rightarrow D$ равны, если $A = C$, $B = D$, $\forall x \in A (f(x) = g(x))$.

Функция $I_A: A \rightarrow A$, для которой $\forall x \in A (I(x) = x)$, называется тождественной функцией.

Функция $f: A \rightarrow B$ есть отображение *в* (инъективная функция, или инъекция), если $\forall a \in A \forall b \in A$ условие $a \neq b$ влечет $f(a) \neq f(b)$.

Инъективная функция различные элементы из области определения переводит в различные элементы из области значений.

Функция $f: A \rightarrow B$ есть отображение *на* (сюръективная функция, или сюръекция), если область значений B совпадает с образом $f(A)$, то есть если $f(A) = B$.

Функция $f: A \rightarrow B$ есть взаимно-однозначная функция (или биекция), если f является отображением *в* и отображением *на*, то есть является одновременно инъективной и сюръективной функцией: 1) $a \neq b \rightarrow f(a) \neq f(b)$, 2) $Im(f) = B$.

Определение. Композиция $g \circ f$ функций $f: A \rightarrow B$ и $g: B \rightarrow C$ есть функция $g \circ f: A \rightarrow C$, для которой $\forall x \in A ((g \circ f)(x) = g(f(x)))$.

Замечание. Символ композиции \circ иногда опускается.

Утверждение. $(h \circ g) \circ f = h \circ (g \circ f)$.

Доказательство. Пусть $f: A \rightarrow B$, $g: B \rightarrow C$, $h: C \rightarrow D$. Тогда $((h \circ g) \circ f)(x) = ((hg)f)(x) = (h \circ g)f(x) = h(g(f(x))) = h((g \circ f)(x)) = (h \circ (g \circ f))(x)$.

Замечание. Для тождественной функции $f \circ I_A = I_B \circ f = f$.

Определение. Функция $f^{-1}: B \rightarrow A$ называется обратной к функции $f: A \rightarrow B$, если $f \circ f^{-1} = I_B$ и $f^{-1} \circ f = I_A$.

Замечание. 1. g обратна к $f \leftrightarrow f$ обратна к g .

2. Функция $f: A \rightarrow B$ имеет обратную функцию, \Leftrightarrow функция f есть взаимно-однозначное отображение.

Утверждение. Если обратная функция для функции f существует, то она единственна.

Доказательство. Пусть функции f^{-1} и g обратны к функции $f: A \rightarrow B$. Тогда $f^{-1} \circ I_B = f^{-1} \circ (f \circ g) = (f^{-1} \circ f) \circ g = I_A \circ g = g$.

Следствие. Пусть для функций f и g существуют обратные функции f^{-1} и g^{-1} . Тогда справедливы утверждения:

1. $(f^{-1})^{-1} = f$.
2. $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Доказательство. 1. Так как f^{-1} обратна к f , то f обратна к f^{-1} , то есть $f = (f^{-1})^{-1}$.

2. $(f \circ g) \circ (g^{-1} \circ f^{-1}) = f \circ (g \circ g^{-1}) \circ f^{-1} = f \circ I_B \circ f^{-1} = f \circ f^{-1} = I_A$.

Аналогично $(g^{-1} \circ f^{-1}) \circ (f \circ g) = I_B$. Тогда функция $g^{-1} \circ f^{-1}$ обратна к $f \circ g$, то есть $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

Теорема. Функция $f: A \rightarrow B$ имеет обратную функцию тогда и только тогда, когда отображение f взаимно-однозначно.

Доказательство. Пусть функция f имеет обратную функцию f^{-1} . Покажем, что отображение f взаимно-однозначно, то есть что $a \neq b \rightarrow f(a) \neq f(b)$ и $B = \text{Im}(f)$. В самом деле, пусть $f(a) = f(b)$. Тогда $a = I_A(a) = f^{-1}(f(a)) = f^{-1}(f(b)) = I_A(b) = b$, то есть $f(a) = f(b) \rightarrow a = b$, откуда $a \neq b \rightarrow f(a) \neq f(b)$.

Пусть $b \in B$. Тогда $b = I_B(b) = (f \circ f^{-1})(b) = f(f^{-1}(b))$, то есть всякий b есть образ некоторого $a = f^{-1}(b) \in A$. Поэтому $B = \text{Im}(f)$.

Пусть теперь f есть взаимно-однозначное отображение. Покажем, что функция f имеет обратную функцию. В самом деле, так как $B = \text{Im}(f)$, то каждый элемент b из B есть образ в точности одного элемента a из A : $f(a) = b$. Пусть $g(b) = a$. Для соответствия $g: B \rightarrow A$ имеем:

$$\begin{aligned} (g \circ f)(a) &= g(f(a)) = g(b) = a = I_A, \\ (f \circ g)(b) &= f(g(b)) = f(a) = b = I_B. \end{aligned}$$

Следовательно, g есть обратная функция для f . Теорема доказана.

3. Отношение

Пусть A_1, A_2, \dots, A_n есть произвольные множества, вообще говоря, разнородные.

Определение. n -арное отношение p^n на множествах A_1, A_2, \dots, A_n есть подмножество p^n декартова произведения $A_1 \times A_2 \times \dots \times A_n$.

Замечание. n -арное отношение p^n на множестве A есть подмножество p^n натуральной степени множества A^n , $n > 0$. Индекс n -арности (местности) отношения p иногда опускается.

Возможна множественная (суффиксная) $(x_1, \dots, x_n) \in p$ и предикатная (префиксная) $p(x_1, \dots, x_n)$ формы записи отношений. В последнем случае отношение p называют также предикатом. Для бинарного отношения используется инфиксная запись $x \text{ р } y$. Унарное отношение $p \subseteq E$ есть подмножество множества E . Предикат $p(x)$, соответствующий унарному отношению, называется свойством.

Набор $a = (a_1, a_2, \dots, a_n) \in \rho$ (допустима запись $\rho(a_1, a_2, \dots, a_n)$) называется элементом отношения.

Определение. Отношение *конечно*, если оно состоит из конечного числа элементов.

4. Отношение эквивалентности

Пусть A есть произвольное множество.

Определение. Бинарное отношение $\sigma \subseteq A \times A$ есть *отношение эквивалентности* (обозначение $a \sim b$), если оно удовлетворяет следующим аксиомам:

- 1) $a \sim a$, рефлексивность;
- 2) $a \sim b \rightarrow b \sim a$, симметричность;
- 3) $a \sim b \ \& \ b \sim c \rightarrow a \sim c$, транзитивность.

Обозначение. $a \sim b$, $\sigma(a, b)$, $(a, b) \in \sigma$, $a \sigma b$.

Определение. *Разбиение* *множества* A есть семейство попарно непересекающихся непустых подмножеств множества A , таких, что: $A = \bigcup_{i \in I} A_i, \forall i \neq j (A_i \cap A_j = \emptyset)$.

Подмножества A_i называются *смежными классами* разбиения I .

Пример. $A = \{0, 1, 2, 3, 4, 5\} = \{0, 1, 5\} \cup \{2\} \cup \{3, 4\}$.

Теорема. 1. Каждому отношению эквивалентности, определенному на множестве A , соответствует некоторое разбиение множества A .

2. Каждому разбиению множества A соответствует некоторое отношение эквивалентности, определенное на множестве A .

Коротко: между классом всех определенных на множестве A эквивалентностей и классом всех разбиений множества A существует взаимно-однозначное соответствие.

Доказательство. 1. Пусть σ есть отношение эквивалентности, определенное на множестве A и $a \in A$. Построим множество $K_a = \{x \in A: x \sim a\}$ всех элементов x , эквивалентных a . Оно обозначается также через $[a]_\sigma$. Множества K_a называются *смежными классами* A по σ , или классами эквивалентности.

Заметим, что если $b \in K_a$, то $b \sim a$. Покажем, что $a \sim b \leftrightarrow K_a = K_b$. В самом деле, пусть $a \sim b$. Пусть произвольный элемент $c \in K_a$. Тогда $c \sim a, a \sim b, c \sim b, c \in K_b$, и потому $K_a \subseteq K_b$. Аналогично показываем, что $K_b \subseteq K_a$. Тогда $K_a = K_b$. Пусть теперь $K_a = K_b$. Тогда $a \in K_b$ и $a \sim b$. Утверждение доказано.

Если два класса K_a и K_b имеют общий элемент c , то они совпадают. В самом деле, если $c \in K_a, c \in K_b$, то $b \sim c, c \sim a$ и $b \sim a$, откуда $K_a = K_b$. Поэтому всякие два класса эквивалентности либо не пересекаются, либо (в случае непустого пересечения) совпадают. Всякий элемент c попадает в класс эквивалентности K_c . Поэтому система смежных классов есть разбиение множества A .

2. Пусть задано некоторое разбиение множества A . Определим на A отношение \sim , положив $a \sim b \leftrightarrow$ элементы a и b принадлежат одному и тому же классу разбиения. Отношение \sim удовлетворяет аксиомам 1) $a \sim a$, 2) $a \sim b \rightarrow b \sim a$, 3) $a \sim b \ \& \ b \sim c$, и потому оно есть отношение эквивалентности.

Замечание. 1. Разбиение множества A на одноэлементные подмножества $A = \bigcup_{a \in A} \{a\}$ и разбиение A , состоящее из одного только множества A , называются тривиальными (несобственными) разбиениями.

2. Разбиение A на одноэлементные подмножества соответствует отношению эквивалентности, которое есть равенство.

3. Разбиение множества A , состоящее из одного только множества A , соответствует отношению эквивалентности, содержащему все множество $A \times A$.

$$4. a \sigma b \leftrightarrow [a]_{\sigma} = [b]_{\sigma}.$$

Определение. Совокупность классов эквивалентности множества A называется *фактор-множеством* A/σ множества A по эквивалентности σ .

Определение. Отображение $p: A \rightarrow A/\sigma$, при котором $p(a) = [a]_{\sigma}$, называется *каноническим* (естественным).

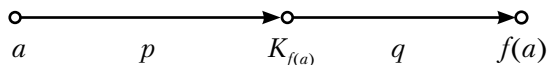
5. Каноническое разложение функции

Пусть $f: A \rightarrow B$ есть некоторая функция. Определим на A отношение $\sigma \in A \times A$, положив $a \sim b \leftrightarrow a \in A \leftrightarrow b \in A$ ($a \sim b \leftrightarrow f(a) = f(b)$). Отношение σ есть отношение эквивалентности, так как выполняются следующие свойства:

- 1) $a \sim a$, ибо $f(a) = f(a)$;
- 2) $a \sim b \rightarrow b \sim a$, ибо $f(a) = f(b) \rightarrow f(b) = f(a)$;
- 3) $a \sim b$ & $b \sim c \rightarrow a \sim c$, ибо $f(a) = f(b)$ & $f(b) = f(c) \rightarrow f(a) = f(c)$.

Введенное отношение σ называется *ядерной эквивалентностью* для отображения f . Классы эквивалентности A/σ есть полные прообразы элементов множества B при отображении f , то есть $A_b = f^{-1}(b)$.

Отображение f можно разложить в композицию двух отображений, согласно следующему рисунку:



Имеет место равенство $f = q \circ p$, то есть $f(a) = q(p(a))$.

Представление $f = q \circ p$ называется *каноническим разложением* (представлением) функции f .

Пример. Получить каноническое разложение функции

$$f: E_{10} \rightarrow E_{10}, f = 0112105533 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 1 & 1 & 2 & 1 & 0 & 5 & 5 & 3 & 3 \end{pmatrix}.$$

Область определения $D(f) = E_{10}$. Область значений $Im(f) = \{0, 1, 2, 3, 5\}$. Классы эквивалентности:

$$\begin{aligned} K_0 &= [0]_{\sigma} = f^{-1}(0) = \{0, 5\}, q(K_0) = 0; \\ K_1 &= [1]_{\sigma} = f^{-1}(1) = \{1, 2, 4\}, q(K_1) = 1; \\ K_2 &= [2]_{\sigma} = f^{-1}(2) = \{3\}, q(K_2) = 2; \\ K_3 &= [3]_{\sigma} = f^{-1}(3) = \{8, 9\}, q(K_3) = 3; \\ K_5 &= [5]_{\sigma} = f^{-1}(5) = \{6, 7\}, q(K_5) = 5. \end{aligned}$$

Функции p и q задаются следующим образом:

$$p(a) = K_{f(a)} = \left(\begin{array}{cccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ K_0 & K_1 & K_1 & K_2 & K_1 & K_0 & K_5 & K_5 & K_3 & K_3 \end{array} \right)$$

$$D(p) = E_{10}, \text{Im}(p) = \{K_0, K_1, K_2, K_3, K_5\}; q(K_a) = a = \left(\begin{array}{ccccc} K_0 & K_1 & K_2 & K_3 & K_5 \\ 0 & 1 & 2 & 3 & 5 \end{array} \right),$$

$$D(q) = \{K_0, K_1, K_2, K_3, K_5\}, \text{Im}(q) = \{0, 1, 2, 3, 5\}; f(a) = q(p(a)).$$

Б. Мощности множеств. Счетные и несчетные множества

Определение. Множества A и B эквивалентны ($A \sim B$), если между их элементами можно установить взаимно-однозначное соответствие.

Отношение эквивалентности множеств обладает следующими свойствами:

1. $A \sim A$, рефлексивность;
2. $A \sim B \rightarrow B \sim A$, симметричность;
3. $A \sim B \ \& \ B \sim C \rightarrow A \sim C$, транзитивность.

Определение. Мощности множества A (обозначение $|A|$) есть класс эквивалентных ему множеств. Мощности конечного множества есть число его элементов.

Замечание. Эквивалентные множества A и B равномощны, то есть $A \sim B \leftrightarrow |A| = |B|$.

Определение. Множество A счетно, если A эквивалентно множеству \mathbb{N} натуральных чисел. В противном случае множество A несчетно.

Утверждение. Из всякого бесконечного множества можно выделить счетное подмножество.

Доказательство. Пусть A есть бесконечное множество. Выделим в A произвольный элемент a_0 . Множество $A - \{a_0\}$ бесконечно. Выделим в нем элемент a_1 . Множество $A - \{a_0, a_1\}$ бесконечно. Выделим в нем элемент a_2 . И так далее. В бесконечном множестве A выделено счетное подмножество $B = \{a_0, a_1, a_2, \dots\}$.

Утверждение. Множество \mathbb{Q}_+ положительных рациональных чисел счетно.

Доказательство. Расположим элементы из \mathbb{Q}_+ в следующей таблице:

1	1/2	1/3	1/4	1/5	...
2	2/2	2/3	2/4	2/5	...
3	3/2	3/3	3/4	3/5	...
4	4/2	4/3	4/4	4/5	...
...					

Выписываем элементы из \mathbb{Q}_+ по диагонали сверху вниз, выпуская ранее встречавшиеся числа: 1, 1/2, 2, 1/3, 3, 2/3, ... Следовательно, множество \mathbb{Q}_+ счетно.

Утверждение. Объединение конечного или счетного множества счетных множеств счетно.

Доказательство. Расположим элементы множеств A_1, A_2, A_3, \dots (их число может

быть и конечным) в следующей таблице:

$$\begin{array}{l} A_1: a_{11}, a_{12}, a_{13}, a_{14}, \dots \\ A_2: a_{21}, a_{22}, a_{23}, a_{24}, \dots \\ A_3: a_{31}, a_{32}, a_{33}, a_{34}, \dots \\ A_4: a_{41}, a_{42}, a_{43}, a_{44}, \dots \\ \dots \end{array}$$

Выписываем элементы из $A_1 \cup A_2 \cup A_3 \cup \dots$ по диагонали сверху вниз, выпуская ранее встречавшиеся элементы: $a_{11}, a_{12}, a_{21}, a_{13}, a_{22}, a_{31}, \dots$. Следовательно, множество $A_1 \cup A_2 \cup \dots$ счетно.

Замечание. Объединение конечного множества и счетного множества счетно. Множество рациональных чисел счетно, ибо $\mathbb{Q} = \mathbb{Q}_- \cup \mathbb{Q}_+ \cup \{0\}$, где \mathbb{Q}_- есть множество отрицательных рациональных чисел.

7. Мощност континуума

Утверждение. Множество C всех бесконечных последовательностей из 0 и 1 не счетно.

Доказательство. Допустим противное: существует пересчет всех бесконечных последовательностей A_1, A_2, A_3, \dots из 0 и 1:

$$\begin{array}{l} A_1: a_{11}, a_{12}, a_{13}, a_{14}, \dots \\ A_2: a_{21}, a_{22}, a_{23}, a_{24}, \dots \\ A_3: a_{31}, a_{32}, a_{33}, a_{34}, \dots \\ A_4: a_{41}, a_{42}, a_{43}, a_{44}, \dots \\ \dots \end{array}$$

Построим последовательность $B: b_1, b_2, b_3, \dots$, где

$$b_i = \begin{cases} 1, & \text{если } a_{ii} = 0, \\ 0, & \text{если } a_{ii} = 1, \end{cases} \quad i = 1, 2, 3, \dots$$

Последовательность B лежит вне указанного пересчета. B отличается от A_1 элементом $b_1 \neq a_{11}$, от A_2 – элементом $b_2 \neq a_{22}$, от A_3 – элементом $b_3 \neq a_{33}$ и т. д. Следовательно, исходное множество C не счетно.

Определение. Множество A имеет *мощность континуума* c , если A эквивалентно множеству всех бесконечных последовательностей из 0 и 1.

Следствие. Множество C всех бесконечных последовательностей из 0 и 1 имеет мощность континуума: $|C| = c$ (в силу рефлексивности).

Утверждение. Множество $P(\mathbb{N})$ всех подмножеств множества натуральных чисел имеет мощность континуума.

Доказательство. Всякую бесконечную последовательность из 0 и 1 можно рассматривать как характеристическую функцию некоторого подмножества мно-

жества натуральных чисел. Следовательно, множество $P(\mathbb{N})$ имеет мощность континуума: $|P(\mathbb{N})| = c$.

Следствие. Множество всех подмножеств множества натуральных чисел несчетно.

Утверждение. Если к бесконечному множеству добавить конечное или счетное множество элементов, то его мощность не изменится.

Доказательство. Пусть A есть бесконечное множество, а B есть конечное или счетное множество, причем $A \cap B = \emptyset$. Покажем, что $A \sim A \cup B$. Выделим из множества A счетное подмножество A_1 . Тогда $A = C \cup A_1$, где $C = A - A_1$, и $A \cup B = (C \cup A_1) \cup B = C \cup (A_1 \cup B)$. Так как $A_1 \cup B \sim A_1$, то $A \cup B = C \cup (A_1 \cup B)$, $C \cup (A_1 \cup B) \sim C \cup A_1$ в силу транзитивности и с учетом того, что $A = C \cup A_1$, получаем $A \cup B \sim A$.

Утверждение. Если A есть несчетное множество, а B есть конечное или счетное его подмножество, то $A - B \sim A$.

Доказательство. Пусть $C = A - B$. Тогда $A = C \cup B$. Множество C несчетно, ибо в противном случае C конечно или счетно, и тогда $A = C \cup B$ конечно или счетно. Множество $C \cup B \sim C$, или $A \sim C$, то есть $A \sim A - B$.

Теорема. Множество $U = [0, 1]$ имеет мощность континуума c .

Доказательство. Множество U эквивалентно множеству всех последовательностей из 0 и 1.

Замечание. 1. $|[0, 1]| = |(0, 1)| = |(0, 1]| = |[0, 1)| = c$.

2. Если $a < b$, то $|[a, b]| = c$, ибо функция $y = a + x(b - a)$ отображает $[0, 1]$ на $[a, b]$ взаимно-однозначно.

3. $|[a, b]| = |(a, b)| = |(a, b]| = |[a, b)| = c$.

4. $|(-\infty, \infty)| = |\mathbb{R}| = c$, ибо функция $y = \operatorname{tg}(x)$ отображает интервал $(a, b) = (-\pi/2, \pi/2)$ на всю числовую ось \mathbb{R} взаимно-однозначно.

8. Кардинальные числа. Сравнение мощностей

Определение. *Мощность множества* есть класс эквивалентных между собой множеств. *Кардинальное число*, или кардинал, есть знак (символ), приписываемый мощности как классу эквивалентных между собой множеств. Мощности конечных множеств называются *финитными кардиналами*. Мощности бесконечных множеств называются *трансфинитными кардиналами*.

Пример. Счетной мощности (мощность множества натуральных чисел) присваивается кардинальное число \aleph_0 (алеф-нуль). Мощности множества вещественных чисел присваивается кардинальное число c .

Замечание. Мощность множества A обозначается через $|A|$, а также через $\operatorname{card}(A)$ или $s(A)$. Мощность конечного множества есть число его элементов.

Пусть A, B есть произвольные множества и $|A|, |B|$ есть их мощности.

Априори возможны четыре случая.

1. Множество A эквивалентно некоторому подмножеству множества B , а множество B эквивалентно некоторому подмножеству множества A .

2. Множество A эквивалентно некоторому подмножеству множества B , а множество B не эквивалентно никакому подмножеству множества A .

3. Множество B эквивалентно некоторому подмножеству множества A , а множество A не эквивалентно никакому подмножеству множества B .

4. Множество A не эквивалентно никакому подмножеству множества B , а множество B не эквивалентно никакому подмножеству множества A .

Определение.

$$|A| = |B|, \text{ если } A \sim B.$$

$$|A| \leq |B|, \text{ если } A \text{ эквивалентно некоторому подмножеству в } B.$$

$|A| < |B|$, если A эквивалентно некоторому подмножеству в B , а множество B не эквивалентно никакому подмножеству множества A .

$$|A| \geq |B|, \text{ если } |B| \leq |A|.$$

$$|A| > |B|, \text{ если } |B| < |A|.$$

Замечание. Случай, когда множество A не эквивалентно никакому подмножеству множества B , а множество B не эквивалентно никакому подмножеству множества A , невозможен.

Теорема (Кантор–Бернштейн). Если множество A эквивалентно некоторому подмножеству B_1 множества B , а множество B эквивалентно некоторому подмножеству A_1 множества A , то множества A и B эквивалентны (то есть имеют равную мощность). Коротко: $|A| \leq |B| \ \& \ |B| \leq |A| \rightarrow |A| = |B|$.

Доказательство. Случаи $B_1 = B$ и $A_1 = A$ можно исключить, ибо если $B_1 = B$, то условие теоремы утверждает, что $A \sim B$, из чего, естественно, следует $A \sim B$. Случай $A_1 = A$ аналогичен.

Итак, пусть $A_1 \subset A$, $B_1 \subset B$. Пусть функции $f: A \rightarrow B_1$, $g: B \rightarrow A_1$ устанавливают взаимно-однозначное соответствие между A и B_1 и между B и A_1 , то есть $A \sim_f B_1$, $B \sim_g A_1$. С помощью функций f и g расслоим множества A и B на «кольца» следующим образом. Имеем:

$$A \sim_f B_1 \subset B, B \sim_g A_1 \subset A,$$

$$A_1 \sim_f B_2 \subset B_1, B_1 \sim_g A_2 \subset A_1,$$

$$A_2 \sim_f B_3 \subset B_2, B_2 \sim_g A_3 \subset A_2,$$

...

Сформируем множества («кольца»):

$$K_0^A = A - A_1, K_0^B = B - B_1,$$

$$K_1^A = A_1 - A_2, K_1^B = B_1 - B_2,$$

$$K_2^A = A_2 - A_3, K_2^B = B_2 - B_3,$$

...

Функции f и g устанавливают следующие взаимно-однозначные соответствия:

$$K_0^A \sim_f K_1^B, K_0^B \sim_g K_1^A,$$

$$K_1^A \sim_f K_2^B, K_1^B \sim_g K_2^A,$$

...

Конец ознакомительного фрагмента.

Приобрести книгу можно

в интернет-магазине

«Электронный универс»

e-Univers.ru