

Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет компьютерных систем и сетей

Кафедра электронных вычислительных средств

М. И. Вашкевич, М. И. Порхун

ОСНОВЫ ДИСКРЕТНОЙ МАТЕМАТИКИ

*Рекомендовано УМО по образованию в области информатики
и радиоэлектроники в качестве учебно-методического пособия
для специальности 6-05-0611-05 «Компьютерная инженерия»*

Минск БГУИР 2025

УДК 519.854(076)
ББК 22.176я73
В23

Рецензенты:

кафедра математической кибернетики
Белорусского государственного университета
(протокол № 6 от 29.01.2024);

декан инженерно-педагогического факультета
Белорусского национального технического университета
кандидат технических наук, доцент А. А. Дробыш

Вашкевич, М. И.

В23

Основы дискретной математики : учеб.-метод. пособие /
М. И. Вашкевич, М. И. Порхун. – Минск : БГУИР, 2025. – 96 с. : ил.
ISBN 978-985-543-788-9.

Излагается материал базового курса дискретной математики для студентов, обучающихся по специальностям, связанным с информатикой и вычислительной техникой. Охватываются такие разделы, как теория множеств, теория отношений и функций, теория групп, колец и полей. В рамках теории колец излагаются основы теории чисел. Теоретический материал сопровождается рассмотрением множества практических примеров. В конце каждого раздела также приведены задачи, решая которые студенты могут более глубоко освоить теоретический материал. Ответы к задачам приведены в конце пособия.

УДК 519.854(076)
ББК 22.176я73

ISBN 978-985-543-788-9

© Вашкевич М. И., Порхун М. И., 2025
© УО «Белорусский государственный
университет информатики
и радиоэлектроники», 2025

Содержание

Введение.....	5
1 Основы теории множеств.....	6
1.1 Понятие множества.....	6
1.2 Запись множеств.....	7
1.3 Способы задания множеств	7
1.4 Подмножества.....	8
1.5 Булеан.....	8
1.6 Мощность множества	9
1.7 Изоморфизм множеств	10
1.8 Операции над множествами.....	11
1.9 Свойства операций над множествами.....	13
1.10 Круги Эйлера	13
1.11 Формулы выключений и исключений	15
1.12 Декартово произведение	16
1.13 Задачи	17
2 Теория отношений	20
2.1 Отношения. Базовые понятия	20
2.2 Способы задания отношений	22
2.3 Свойства отношений.....	23
2.4 Отношение эквивалентности	25
2.4.1 Эквивалентность	25
2.4.2 Разбиение	25
2.4.3 Классы эквивалентности	26
2.4.4 Классы вычетов по модулю	26
2.5 Отношение порядка	27
2.6 Оценка и визуализация качества ранжирования	28
2.7 Композиция отношений	30
2.7.1 Представление композиции отношений графами	31
2.7.2 Представление композиции отношений матрицами	32
2.8 Задачи	32
3 Функции (отображения).....	38
3.1 Функциональные отношения	38
3.2 Типы отображений (инъекция, сюръекция, биекция).....	38
3.3 Композиция функций.....	41

3.4 Подстановки	42
3.5 Рекурсивно-определенные функции	44
3.6 Задачи.....	45
4 Алгебраические структуры	50
4.1 Общее понятие алгебры.....	50
4.2 Таблица Кэли	50
4.3 Свойства операций	51
4.4 Алгебры с одной операцией	53
4.5 Группы	55
4.5.1 Определение группы	55
4.5.2 Циклическая группа	56
4.5.3 Диэдральная группа.....	58
4.5.4 Произведение групп	59
4.5.5 Подгруппы.....	59
4.5.6 Группа подстановок (симметрическая группа).....	60
4.5.7 Перестановочные матрицы.....	61
4.6 Гомоморфизм	62
4.7 Общее понятие о кольцах	63
4.8 Кольцо целых чисел	65
4.8.1 НОК и НОД чисел	66
4.8.2 Сравнения.....	67
4.8.3 Алгоритм Евклида (НОД).....	67
4.8.4 Делитель нуля и взаимно обратные элементы в кольце $\mathbb{Z}_n$	70
4.9 Китайская теорема об остатках (КТО)	71
4.10 Кольцо многочленов	72
4.11 Поля.....	75
4.12 Поля Галуа.....	76
4.13 Задачи.....	79
Приложение А. Ответы к задачам раздела 1	84
Приложение Б. Ответы к задачам раздела 2.....	87
Приложение В. Ответы к задачам раздела 3	92
Приложение Г. Ответы к задачам раздела 4.....	94
Список использованных источников	96

ВВЕДЕНИЕ

Дискретная математика является фундаментальной дисциплиной для подготовки инженера в области информатики и вычислительной техники. Это связано с тем, что информационные процессы носят принципиально дискретный характер, равно как и функционирование вычислительной техники описывается дискретными процессами. В основе дискретной математики лежит теория множеств. Язык теории множеств проник во все отрасли информатики, поэтому, не понимая этого языка, едва ли можно эффективно освоить более продвинутые разделы информатики, такие как кодирование данных, криптография и пр. Теория множеств тесно связана и с теорией вероятностей, на которую, в свою очередь, опирается и наиболее популярное в настоящее время научное направление – машинное обучение.

Дискретная математика охватывает обширный пласт знаний, и данное пособие включает лишь незначительную часть тех понятий, которые изучает дискретная математика. В частности, в нем излагаются основы теории множеств, отношений, функций, а также основы теории групп, колец и полей. Излагаемые материалы основаны на курсе лекций и практических занятий, проведенных авторами с 2019 по 2023 г. для студентов Белорусского государственного университета информатики и радиоэлектроники специальности «Электронные вычислительные средства».

1 ОСНОВЫ ТЕОРИИ МНОЖЕСТВ

Хотя теория множеств рассматривается как краеугольный камень современной математики, нет ничего нового в интуитивной идее множества. С самых ранних времен математики рассматривали множества объектов одного или другого вида. Однако, только начиная с работ Георга Кантора, множества заняли свое место как принципиальный объект математической теории.

Использование современной математики позволяет объединять и исследовать с единых позиций такие понятия и явления, которые ранее казались различными и далекими. При этом важно уметь применять к реальным явлениям те математические понятия и методы, которые наиболее близки к ним, и научиться за общими абстрактными понятиями видеть конкретные образы окружающего мира.

1.1 Понятие множества

Понятие множества принадлежит к числу фундаментальных понятий математики. Основатель теории множеств Георг Кантор определил в 1872 г. множество как *«объединение в одно целое объектов, хорошо различимых нашей интуицией или нашей мыслью»*. Те основы теории множеств, о которых мы будем говорить, в некотором смысле являются побочным продуктом работ Г. Кантора, поскольку его главной целью было рассмотрение актуально бесконечных множеств.

Вообще **множество** – это совокупность объектов (предметов или понятий), которая рассматривается как одно целое. Объекты, входящие в эту совокупность, называются **элементами** множества.

Утверждение «объект a принадлежит множеству A » сокращенно записывают в виде $a \in A$. Если элемент a не принадлежит множеству A , то пишут $a \notin A$. Символ $\in$ называется **знаком принадлежности**.

Два множества A и B называются **равными** ($A = B$), если A и B содержат одни и те же элементы.

Таким образом, множества A и B равны, если любой $x \in A$ тогда и только тогда, когда $x \in B$. В связи с этим доказательство равенства двух множеств обычно состоит из доказательств двух утверждений:

- 1) для любого x , если $x \in A$, то $x \in B$;
- 2) для любого x , если $x \in B$, то $x \in A$.

1.2 Запись множеств

Для записи множества обычно используют фигурные скобки. Например, $\{1, 2, 3, 4\}$ – есть множество, содержащее натуральные числа 1, 2, 3 и 4. Для обозначения множеств, как правило, используют прописные буквы $A = \{\text{Вера, Надежда, Любовь}\}$.

Часто при перечислении множества используется описание характеристического свойства элементов этого множества. Например, $C = \{1, 8, 27, \dots, k^3, \dots\}$ описывает множество кубов всех положительных чисел, а $S = \{1, 2, 4, \dots, n^2\}$ описывает множество квадратов всех положительных чисел, которые меньше или равны n .

Порядок перечисления элементов множества роли не играет. Каждый элемент может входить в множество не более одного раза. Например, множества $\{1, 2, 3\}$ и $\{3, 1, 2, 1\}$ равны, т. к. каждый элемент первого множества принадлежит второму множеству и наоборот.

Множество, не содержащее элементов, называется *пустым* ($\emptyset$).

То есть множество A называется пустым, если для любого x мы имеем $x \notin A$. Такое множество единственно.

Пустое множество является подмножеством любого множества.

Любые два пустых множества равны, потому что нет элементов, по которым их можно было бы различить (ведь содержимое двух пустых мешков одинаково).

Роль пустого множества аналогична роли числа нуль. Это понятие можно использовать для определения заведомо несуществующей совокупности элементов (например, множества зеленых слонов в этой комнате). Без понятия пустого множества во всех случаях, когда мы не знаем содержит ли множество хоть один элемент, приходилось бы добавлять оговорку «если оно существует».

1.3 Способы задания множеств

Чтобы задать множество, нужно указать, какие элементы ему принадлежат. Используют следующие основные три формы записи множеств:

- 1) перечисление элементов: $\{a, b, c, \dots, z\}$;
- 2) указание характеристического свойства $\{x | x \text{ обладает свойством } P\}$;
- 3) порождающая процедура $\{x | x := f\}$.

С заданием свойства P нужно быть предельно точным. При определении множества $C = \{x \mid x \text{ – парень из группы 701}\}$ выбрать элементы будет трудно, однако если условие будет другим, например, $C = \{x \mid x \text{ – парень из группы 701, ростом выше 175 см}\}$, то проблем не будет.

Пример задания множества при помощи характеристического свойства:

$$F = \{n \mid n \in \mathbb{N} \text{ и } x^n + y^n = z^n \text{ имеет решение в целых ненулевых числах}\}.$$

Пример задания множества при помощи порождающей процедуры:

$$S = \{a_n \mid a_n = a_{n-2} + a_{n-1}, \quad a_0 = 1, \quad a_1 = 2, \quad n \leq 10\}.$$

Итак, вместо того чтобы перечислять все элементы множества, указывается свойство, определяющее, какие элементы в это множество включены.

1.4 Подмножества

Множество A , все элементы которого принадлежат множеству B , называется **подмножеством** (частью) множества B . Это отношение между множествами называют **включением** и обозначают символом $\subset$, т. е. $A \subset B$.

Согласно определению

$$A \subset B \leftrightarrow \forall x, x \in A \Rightarrow x \in B.$$

Обозначение $A \subset B$ означает нестрогое включение и допускает равенство множеств.

Пустое множество является подмножеством любого множества, т. е. $\emptyset \subset A$.

1.5 Булеан

Понятие подмножества используется для определения такого важного понятия, как булеан.

Множество, элементами которого являются все подмножества множества A , называют множеством всех подмножеств A , или **булеаном** множества A . Булеан обозначают как $\mathcal{P}(A)$.

Если A содержит n элементов, множество $\mathcal{P}(A)$ включает 2^n элементов.

Пример 1.1. Найти булеан множества $A = \{a, b\}$.

Решение. $\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$.

Универсальное множество U есть множество, обладающее таким свойством, что все рассматриваемые множества являются его подмножеством.

Содержание универсального множества определяется контекстом задачи.

Во многих переборных алгоритмах требуется последовательно рассмотреть все подмножества заданного множества $A = \{a_1, \dots, a_k\}$. В компьютере целые числа представляются кодами в двоичной системе счисления, причем число $2^k - 1$ представляется кодом, содержащим k единиц, а все числа, меньше $2^k - 1$, представляются кодами, имеющими не более k ненулевых разрядов. Можно установить взаимно однозначную связь между двоичным k -разрядным числом и подмножеством A . Причем наличие 1 в n -й позиции числа будет соответствовать наличию элемента a_n в соответствующем подмножестве. Таким образом, код числа 0 является представлением пустого множества $\emptyset$, код числа 1 является представлением подмножества $\{a_1\}$ и т. д. Код числа $2^k - 1$ является представлением всего множества $\{a_1, \dots, a_k\}$. Учитывая это, можно составить простой алгоритм генерации всех подмножеств универсума.

Алгоритм. Генерация всех подмножеств n -элементного множества

Вход: число $k > 0$ – мощность множества.

Выход: последовательность кодов подмножеств.

```
for i from 0 to  $2^k - 1$  do
  yield dec2bin(i) // код очередного подмножества
end for
```

Эта процедура применяется, например, в машинном обучении при подборе оптимального подмножества информативных признаков в задаче классификации.

1.6 Мощность множества

Если A – конечное множество, то **мощность** множества A равна числу элементов этого множества и обозначается как $|A|$.

Пример 1.2. Определить мощности следующих множеств:

а) $A = \{a, b\}$;

б) $B = \{\{a, b\}\}$;

в) $C = \{2, 3, 3\}$;

г) $D = \{17, 18, 19, \dots, 5325, 5326\}$.

Решение

а) $|A| = 2$;

б) $|B| = 1$;

в) множество C состоит всего из двух элементов 2 и 3. Напомним, что $\{2, 3, 3\} = \{2, 3\}$;

г) количество последовательных целых чисел в интервале от m до n включительно равно $n - m + 1$. Для множества D мы имеем $5326 - 17 + 1 = 5310$.

Почему же мы используем термин «мощность»? Ведь могли бы мы использовать, например, термин «размер множества»? Дело в том, что понятие мощности также распространяется и на бесконечные множества.

Ниже приведены примеры некоторых бесконечных множеств:

1) $\mathbb{N}$ – множество натуральных чисел $\{1, 2, 3, \dots\}$;

2) $\mathbb{Z}$ – множество целых чисел;

3) $\mathbb{R}$ – множество вещественных чисел.

Вопрос о том, чем конечное отличается от бесконечного, может поставить в тупик. С античных времен известен принцип «часть меньше целого». Оказывается, этот принцип можно использовать в качестве характеристического свойства конечных множеств. Для бесконечных множеств он не имеет места.

Бесконечные множества бывают **счетными** (которые можно перенумеровать и которые равномощны множеству натуральных чисел) и **несчетными**, которые не могут быть сведены к множеству натуральных чисел.

1.7 Изоморфизм множеств

Если между A и B установлено *взаимно однозначное соответствие* (т. е. каждому элементу одного множества соответствует только один элемент другого множества), то говорят, что A и B **изоморфны**: $A \sim B$. Для конкретных элементов $a \in A$ и $b \in B$, которые соответствуют друг другу, пишут $a \mapsto b$.

Если между двумя множествами A и B может быть установлено взаимно однозначное соответствие, то множества имеют одинаковую мощность:

$$|A| = |B| \triangleq A \sim B.$$

Например, взаимно однозначное соответствие $n \mapsto 2n$ устанавливает связь между множеством натуральных чисел $\mathbb{N}$ и множеством четных натуральных чисел $2\mathbb{N}$, т. е. $\mathbb{N} \sim 2\mathbb{N}$ (множество $\mathbb{N}$ изоморфно множеству четных чисел).

Таким образом, для бесконечных множеств не соблюдается принцип «часть меньше, чем целое».

1.8 Операции над множествами

Над множествами можно производить ряд операций. При рассмотрении операций над множествами будем в качестве примера использовать следующие множества:

$$A = \{1, 2, 3\}, B = \{2, 3, 5, 4\}, U = \{1, 2, 3, \dots, 9\}.$$

Пересечением множеств A и B называется множество, состоящее из тех и только тех элементов, которые принадлежат и A и B .

$$A \cap B = \{x: x \in A \wedge x \in B\}$$

В общем случае пересечение совокупности множеств определяется следующим образом: если $I \in \{1, 2, 3, \dots, k\}$, то

$$\bigcap_{i \in I} A_i = A_1 \cap A_2 \cap \dots \cap A_k = \{x: x \in A_i \text{ для всех } i \in I\}.$$

Множество I называется **индексным множеством**.

Пример 1.3. Найти пересечение множеств A и B .

Решение. $A \cap B = \{2, 3\}$.

Объединением множеств A и B называют множество, состоящее из всех элементов, которые принадлежат хотя бы одному из множеств A или B :

$$A \cup B = \{x: x \in A \vee x \in B\}.$$

Например, если $A = \{1, 2, 6, 7\}$, а $B = \{2, 3, 5, 6\}$, то $A \cup B = \{1, 2, 3, 5, 6, 7\}$.

В общем случае объединение задается так.

$$\bigcup_{i \in I} A_i = A_1 \cup A_2 \cup \dots \cup A_k = \{x \mid \exists i \in I, \text{ что } x \in A_i\}.$$

Пример 1.4. Найти объединение множеств A и B .

Решение. $A \cup B = \{1, 2, 3, 4, 5\}$.

Разность множеств A и B называется множество всех тех и только тех элементов A , которые не содержатся в B .

$$A \setminus B = \{x | x \in A \wedge x \notin B\}.$$

Пример 1.5. Найти разности множеств A и B .

Решение. $A \setminus B = \{1\}$, $B \setminus A = \{4, 5\}$.

Симметрической разностью множеств A и B называется множество таких элементов, которые есть или только в A , или только в B . Аналог «исключающего ИЛИ».

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

Пример 1.6. Найти симметрическую разность множеств A и B .

Решение. $A \triangle B = \{1, 4, 5\}$.

Дополнением множества A называется множество всех элементов универсального множества U , которые не входят в множество A .

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

Например, если $U = \mathbb{N}$, а A – множество всех четных чисел, то $\bar{A}$ – множество всех нечетных чисел.

Пример 1.7. Найти дополнение множества B .

Решение. $\bar{B} = \{1, 7, 8, 9\}$.

Для произвольных множеств A и B справедливо равенство

$$A \setminus B = A \cap \bar{B}.$$

Для доказательства равенства двух множеств нужно показать, что каждое из множеств является подмножеством другого. Это можно осуществить, выбирая произвольный элемент одного множества и доказывая, что он принадлежит другому множеству:

$$\begin{aligned} a \in A \setminus B &\Leftrightarrow (a \in A) \wedge (a \notin B) \Leftrightarrow \\ &\Leftrightarrow (a \in A) \wedge (a \in \bar{B}) \Leftrightarrow \\ &\Leftrightarrow (a \in A \cap \bar{B}). \end{aligned}$$

определение разности $A \setminus B$
определение дополнения
определение пересечения.

1.9 Свойства операций над множествами

Основные свойства операций над множествами и примеры этих свойств приведены в таблице 1.1.

Таблица 1.1 – Свойства операций над множествами

Свойство	Примеры
Коммутативность	$A \cup B = B \cup A$ (относительно объединения). $A \cap B = B \cap A$ (относительно пересечения). $A \Delta B = B \Delta A$ (относительно симметрической разности)
Ассоциативность	$A \cup (B \cup C) = (A \cup B) \cup C$ (относительно объединения). $(A \cap B) \cap C = A \cap (B \cap C)$ (относительно пересечения)
Дистрибутивность	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (объединения относительно пересечения). $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (пересечения относительно объединения)
Идемпотентность	$A \cap A = A$ (относительно пересечения). $A \cup A = A$ (относительно объединения)
Законы де Моргана	$\overline{A \cup B} = \bar{A} \cap \bar{B}$. $\overline{A \cap B} = \bar{A} \cup \bar{B}$
Законы операций с константами	$A \cup \emptyset = A$. $A \cap \emptyset = \emptyset$. $A \cup U = U$. $A \cap U = A$. $A \cup \bar{A} = U$. $A \cap \bar{A} = \emptyset$
Закон двойного отрицания	$\bar{\bar{A}} = A$

1.10 Круги Эйлера

Круги Эйлера – удобный инструмент, позволяющий изображать множества и иллюстрировать операции над ними.

Примеры использования кругов Эйлера для иллюстрации основных операций над множествами приведены на рисунке 1.1.

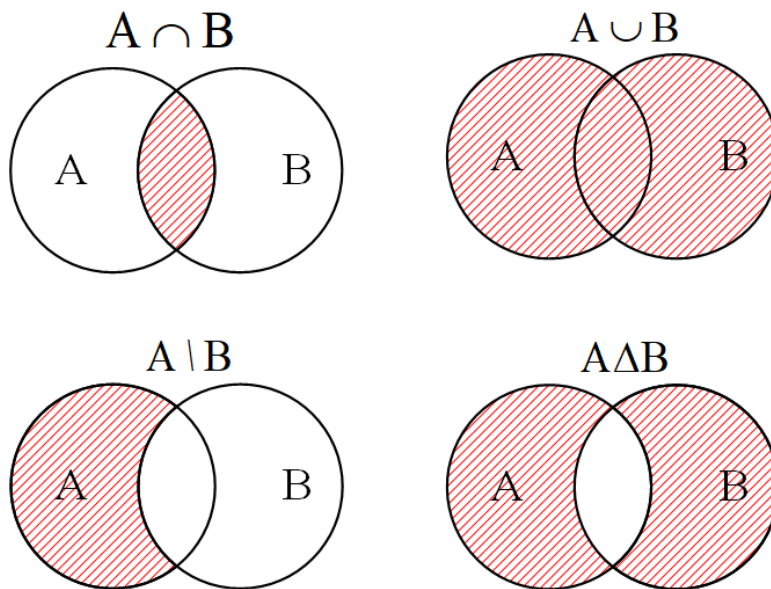


Рисунок 1.1 – Примеры использования кругов Эйлера

Круги Эйлера можно использовать для доказательства теоретико-множественных соотношений.

Пример 1.8. Доказать свойство $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Решение. Это можно сделать, построив области, соответствующие левой и правой части этого выражения, и выяснить, совпадают они или нет (рисунок 1.2).

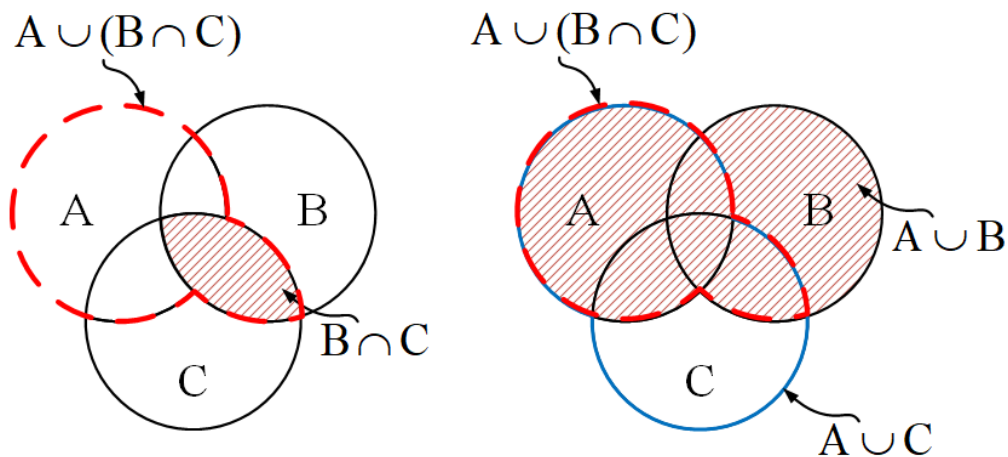


Рисунок 1.2 – Круги Эйлера для примера 1.8

Круги Эйлера также часто используют для графического выполнения тождественных преобразований.

Пример 1.9. Упростить выражение $(A \cap B \cap C) \cup (\bar{A} \cap C) \cup (\bar{B} \cap C)$.

Решение. Это выражение можно представить, как показано на рисунке 1.3.

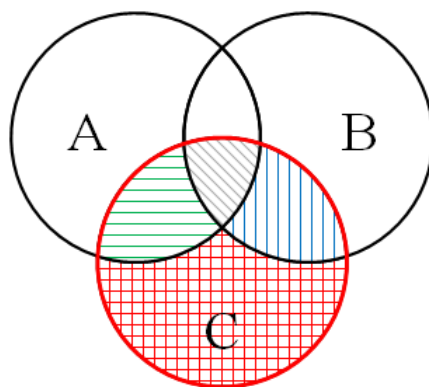


Рисунок 1.3 – Круги Эйлера для примера 1.9

Наклонная штриховка соответствует $(A \cap B \cap C)$, вертикальная – $(\bar{A} \cap C)$, а горизонтальная – $(\bar{B} \cap C)$. Объединение этих областей, как и следовало ожидать, совпадает с C .

1.11 Формулы выключений и исключений

Если множества A и B конечны, то из определений нетрудно видеть, что

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

То есть если мы хотим найти число элементов в объединении $A \cup B$, мы должны сложить число элементов в A с числом элементов в B и вычесть (исключить) $|A \cap B|$, поскольку эти элементы были посчитаны два раза.

Можно показать, что для разности множеств применимо следующее выражение:

$$|A \setminus B| = |A| - |A \cap B|.$$

Для симметрической разности верно, что

$$|A \Delta B| = |A| + |B| - 2|A \cap B|.$$

Пример 1.10. Пусть A – список из 30 учащихся, посещающих кружок математики, и B – список из 35, посещающих кружок литературы. Известно, что 20 учащихся находятся и в одном, и в другом списке. Найдите число школьников, которые:

- а) находятся только в списке A ;
- б) находятся только в списке B ;

в) находятся либо в A , либо в B , либо сразу в двух списках;

г) только в одном из списков.

Решение. Запишем на языке множеств наше условие: $|A| = 30$, $|B| = 35$, $|A \cap B| = 20$.

а) $|A \setminus B| = |A| - |A \cap B| = 30 - 20 = 10$;

б) $|B \setminus A| = |B| - |A \cap B| = 35 - 20 = 15$;

в) требуется найти $|A \cup B|$. Воспользуемся правилом включений – исключений:

$$|A \cup B| = |A| + |B| - |A \cap B| = 30 + 35 - 20 = 45.$$

Другими словами, мы складываем два листа и затем вычеркиваем 20 имен, которые попали туда дважды;

г) используя пункты «а» и «б», можно получить $10 + 15 = 20$. На языке теории множеств это множество описывается выражением $A \Delta B = (A \setminus B) \cup (B \setminus A)$.

Проверка:

$$|A \Delta B| = |A| + |B| - 2|A \cap B| = 30 + 35 - 2 \cdot 20 = 25.$$

1.12 Декартово произведение

Декартово произведение множеств A и B , обозначаемое $A \times B$, есть множество $\{(a, b): a \in A \text{ и } b \in B\}$. Объект (a, b) называют **упорядоченной парой** с первой компонентой a и второй компонентой b . Декартово произведение иногда называют прямым произведением множеств.

Порядок компонент в паре существенен! По аналогии, как в декартовой системе координат, мы знаем, что точка $(1, 2)$ не совпадает с точкой $(2, 1)$.

Аналогично упорядоченным парам можно рассматривать упорядоченные тройки, четверки и т. д., в таком случае их называют **наборами**, или **кортежами**.

Пример 1.11. Пусть $A = \{a_1, a_2, a_3\}$, а $B = \{b_1, b_2\}$. Найти декартово произведение $A \times B$.

Решение. $A \times B = \{(a_1, b_1), (a_1, b_2), (a_2, b_1), (a_2, b_2), (a_3, b_1), (a_3, b_2)\}$.

Поскольку порядок элементов в паре существенен, то $A \times B \neq B \times A$.

Если $|A| = n$, $|B| = m$, то $|A \times B| = n \cdot m$.

Обратим внимание, что произведение множеств не стоит в одном ряду с ранее введенными операциями над множествами. Элементы произведения множеств

существенно отличаются от элементов сомножителей и представляют собой объекты другой категории.

Пусть, например, $\mathbb{N}$ – множество натуральных чисел, тогда $\mathbb{N} \times \mathbb{N}$ будет множеством пар натуральных чисел (p, q) . Такие пары могут определять самые различные объекты, например: дроби p/q , номера домов и квартир. Именно поэтому $(p, q) \neq (q, p)$. Если бы это правило не соблюдалось, то числитель мог бы стать знаменателем, а номер дома превратиться в номер квартиры.

1.13 Задачи

1 Перечислите элементы следующих множеств:

а) $S = \{x \mid x - \text{целое положительное число и } x^2 < 100\}$;

б) $C = \{x \mid x - \text{целое положительное число и } x^3 < 100\}$;

в) $Q = \{x \mid x - \text{целое положительное число и } x^4 < 100\}$.

Какое из следующих утверждений истинно:

а) $S \subset C$;

в) $Q \subset S$;

б) $C \subset S$;

г) $S \subset Q$?

2 Найдите все элементы множества $P = \{x \mid x - \text{простое число, } x < 70\}$.

3 Опишите следующие множества при помощи характеристического свойства:

а) $A = \{10, 2, -6, -14, \dots\}$;

в) $C = \left\{\frac{2}{3}, \frac{8}{9}, \frac{26}{27}, \frac{80}{81}, \dots\right\}$;

б) $B = \{\pm 3, \pm 9, \pm 27, \pm 81, \dots\}$;

г) $D = \{3, 6, 9, 12, 15, 18, 21, \dots\}$.

4 Пусть $A = \{2, 3\}$, $B = \{1, \{2, 3\}\}$. Определите, какие из утверждений верны, а какие нет. Дайте обоснование ответа.

а) $\{1\} \subset A$;

в) $\emptyset \subset B$;

б) $\{1\} \in A$;

г) $\emptyset \in B$.

5 Пусть $A = \{\emptyset, a, \{b, c\}\}$, $B = \{b, c\}$. Определите, какие из утверждений верны, а какие – нет. Дайте обоснование ответа.

а) $\{a\} \subset A$;

в) $B \in A$;

б) $\{a\} \in A$;

г) $B \subset A$.

6 Перечислите подмножества множества $A = \{a, b, c\}$.

7 Установите вид отношения между множествами A и B (равенство, включение):

а) A – множество всех равносторонних треугольников; B – множество всех равнобедренных треугольников, имеющих один угол величиной 60° градусов;

б) $A = \{x : x = 2y \text{ и } y \in \mathbb{N}\}, B = \{x : x = 6y \text{ и } y \in \mathbb{N}\}$.

8 Найдите булеан множества $A = \{1, 2, 3, 4\}$ и определить его мощность.

9 Множество $A \in \{1, 2, 5, 7, 8\}, B \in \{2, 6, 9\}$. Найдите объединение, пересечение и разности множеств. Запишите универсальное множество для данной задачи.

10 Множество $A \in \{1, 2, \dots, 7\}, B \in \{4, 5, \dots, 9\}$. Найдите:

а) $(A \cap B)'$;

в) $A \Delta B$;

б) $A \setminus B$;

г) $B \setminus A$.

11 Множество $A \in \{a, b, c, d, e\}, B \in \{p, q, r, s\}$. Найдите объединение, пересечение и разность множеств. Запишите универсальное множество для данной задачи.

12 Определите, верно ли равенство $A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus C)$.

13 Пусть A – множество всех точек плоскости, у которых ордината (y) положительна, B – множество всех точек плоскости, у которых абсцисса (x) положительна. Опишите следующие множества:

а) $A \cap B$;

г) $\bar{A}$;

б) $A \cup B$;

д) $\overline{A \cap B}$;

в) $A \setminus B$;

е) $\overline{A \cup B}$.

14 Укажите верные и неверные утверждения:

а) $(A \cap B \subset \emptyset) \Rightarrow (A = \emptyset) \text{ и } (B = \emptyset)$;

б) $(A \cup B \subset \emptyset) \Rightarrow (A = \emptyset) \text{ и } (B = \emptyset)$;

в) $(A \setminus B = A) \Rightarrow (B = \emptyset)$;

г) $(A \setminus B = \emptyset) \Rightarrow (A \subset B)$;

д) $(A \cap B = A \cup B) \Rightarrow (A = \emptyset) \text{ и } (B = \emptyset)$;

е) $(A \cap B = A \cup B) \Rightarrow (A = B)$.

15 Укажите верные и неверные утверждения:

а) $\emptyset \subset A$;

б) $A \subset \emptyset \Leftrightarrow A = \emptyset$;

в) $(A \neq B) \text{ и } (B \neq C) \Rightarrow (A \neq C)$.

16 Докажите или опровергните: $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

17 Докажите или опровергните: $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$.

18 Упростите выражение $\overline{A \cup (A \setminus \bar{B}) \cup (A \setminus \bar{B})}$.

19 Упростите выражение $(A \cap B \cap C) \cup (\bar{A} \cap C) \cup (\bar{B} \cap C)$.

20 Упростите выражение $(M \setminus N) \cap (N \setminus M)$.

21 В группе 35 студентов, из них 21 знают английский (множество A), 15 знают немецкий (множество B), 8 знают и английский, и немецкий. Покажите физический смысл объединения, пересечения и симметрической разности множеств A и B . Сколько студентов не знают ни одного языка?

22 Из 100 студентов, сдавших сессию, 37 сдали логику (множество A), 48 человек сдали экономику (множество B), 42 – математику (множество C). По экономике или математике сдали экзамен 76 человек, по экономике или логике тоже 76, а по математике или логике – 66 человек. Сколько человек сдали хотя бы один предмет, если все три предмета сдали 5 человек? Сколько человек не сдали ни одного предмета? Сколько человек сдали только один экзамен по логике?

23 Представьте диаграммой Эйлера следующие множества:

а) $(A \setminus B) \Delta (B \setminus C)$;

б) $(A \cap B \cap C) \setminus (C \cup B)$;

в) $(A \Delta B) \cap C$;

г) $(A \setminus C) \Delta (A \setminus B)$;

д) $(A \cap B) \cup (A \cap C)$.

2 ТЕОРИЯ ОТНОШЕНИЙ

2.1 Отношения. Базовые понятия

Понятие «отношение», широко распространенное в обычной речи, имеет вполне точное математическое значение. Формально отношения являются множествами. Однако это понятие играет весьма важную роль в дискретной математике и на его основе вводят целый ряд понятий и обозначений. Поэтому понятие «отношение» правомерно поставить в один ряд с понятием «множество».

Многие задачи математики, техники и других областей человеческой деятельности получают удобную интерпретацию на языке теории отношений. Все арифметические операции – это, по существу, некоторые отношения между числовыми множествами. Разнообразные отношения складываются между людьми: родители и дети, начальники и подчиненные, учителя и ученики.

Бинарное отношение устанавливает связь элементов одного множества A с элементами другого множества B .

Ясно, что такое отношение может быть задано совокупностью упорядоченных пар (x, y) , которые являются элементами множества $A \times B$. Часто отношение задается некоторым свойством, выраженным в словесной или символической форме.

Более кратко говорят, что бинарное отношение задается тройкой $\langle A, B, R \rangle$, где $R \subset A \times B$.

Для краткости отношения обозначают тем же символом, что и график отношения, а вместо слов «бинарное отношение» говорят просто «отношение».

Множество A называют **областью отправления**, а множество B – **областью прибытия** (рисунок 2.1).

Например, между множествами $A = \{a, b, c\}$ и $B = \{1, 2\}$ можно задать следующее отношение: $R = \{(a, 1), (b, 1), (b, 2)\}$.

Для понятия отношения порядок множеств имеет значение. Отношение между A и B совсем не то же самое, что отношение между B и A .

Область определения ($\text{Dom } R$) отношения R – множество всех $x \in A$, таких, что $(x, y) \in R$ для некоторых $y \in B$. **Область значения** ($\text{Im } R$) отношения R – множество всех $y \in B$, таких, что $(x, y) \in R$ для некоторых $x \in A$.

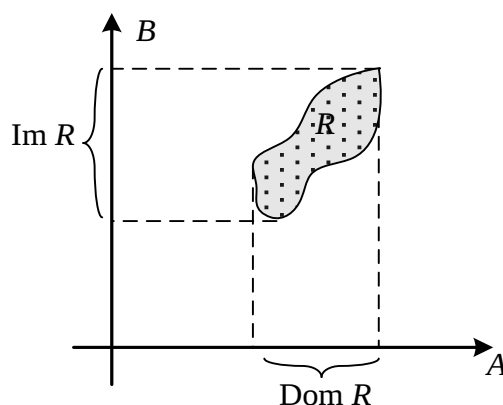


Рисунок 2.1 – Графическое представление отношения

На любом множестве можно определить **тождественное** отношение:

$$I = \{(a, a): a \in A\} \subset A^2.$$

Тождественное отношение играет роль «единичного» элемента.

Введем следующие понятия:

1) **обратное** отношение: $R^{-1} = \{(b, a): (a, b) \in R\} \subset B \times A$;

2) **дополнение** отношения: $\bar{R} = \{(a, b): (a, b) \notin R\} \subset A \times B$.

Для бинарных отношений обычно используется **инфиксная форма записи**:

$$aRb = (a, b) \in R \subset A \times B,$$

читается, как a находится в отношении R к b . Эта форма позволяет более коротко формулировать утверждения об отношениях.

Пример 2.1. Пусть задано отношение $R = \{(a, b), (c, d), (e, f)\}$. Найти обратное отношение R^{-1} .

Решение. $R^{-1} = \{(b, a), (d, c), (f, e)\}$.

Рассмотрим еще один пример.

Пример 2.2. Пусть заданы множества $A = \{a, b, c\}$ и $B = \{1, 2\}$, а также отношение $R = \{(a, 1), (b, 1), (b, 2)\}$. Найти дополнение отношения $\bar{R}$.

Решение. $\bar{R} = \{(a, 2), (c, 1), (c, 2)\}$.

2.2 Способы задания отношений

Выделяют два способа задания отношений: при помощи матрицы и при помощи графа. Матричный способ задания отношения основан на представлении соответствующей ему прямоугольной матрицей M_R :

$$M_R(i, j) = a_j R b_i.$$

То есть ее столбцы соответствуют первым координатам (т. е. области отправления), а строки – вторым координатам, т. е. области прибытия. На пересечении i -й строки и j -го столбца ставится единица, если имеет место отношение $a_j R b_i$, и нуль, если это отношение не выполняется (нулевые клетки удобнее оставлять пустыми). Такая матрица содержит всю информацию об отношении R .

Пример 2.3. Пусть заданы множества $A = \{a, b, c\}$ и $B = \{1, 2\}$, а также отношение $R = \{(a, 1), (b, 1), (b, 2)\}$. Изобразите матрицу отношения R .

Решение. Матрица отношения R имеет следующий вид (рисунок 2.2).

R	a	b	c
1	1	1	
2		1	

Рисунок 2.2 – Матрица отношения R для примера 2.3

Рассмотрим теперь способ задания отношения при помощи графа. Ориентированный граф G обозначается как $G(V, E)$, состоит из множества V вершин и отношения $E \subset V \times V$ (множество ориентированных дуг или ребер). Если $(a, b) \in E$, тогда a называют начальной вершиной (a, b) , а b – его конечной вершиной.

На рисунке 2.3 показан пример использования графа для задания отношения $E = \{(a, a), (a, b), (b, c), (c, b), (c, a)\}$ на множестве $V = \{a, b, c\}$, т. е. области отправления и прибытия совпадают.

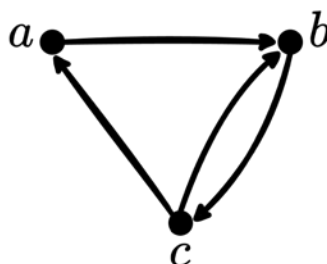


Рисунок 2.3 – Пример использования графа для задания отношения

Каждое бинарное отношение на конечном множестве можно представить ориентированным графом. С другой стороны, каждый ориентированный граф представляет бинарное отношение на множестве его вершин.

2.3 Свойства отношений

Пусть $R \subset A \times A$, тогда отношение R называется:

- **рефлексивным**, если для $\forall a \in A; (a, a) \in R$ (т. е. оно всегда выполняется между объектом и им самим, например, равенство, самообслуживание);
- **антирефлексивным**, если для $\forall a \in A; (a, a) \notin R$, т. е. отношение может выполняться только для несовпадающих объектов (например, строгое неравенство, «быть старше»);
- **симметричным**, если $\forall a, b \in A, (aRb \Rightarrow bRa)$. Другими словами: из $(a, b) \in R$ следует, что $(b, a) \in R$. Например, расстояние между двумя точками, «быть братом»;
- **асимметричным**, если невозможно одновременное выполнение двух соотношений aRb и bRa . По меньшей мере одно не выполняется (строгое включение, «быть отцом»); асимметричное отношение антисимметрично и антирефлексивно;
- **антисимметричным**, если $\forall a, b \in A$ из принадлежности (a, b) и (b, a) отношению R следует, что $a = b$. Более коротко: $(aRb \wedge bRa \Rightarrow a = b)$. То есть оба соотношения aRb и bRa выполняются одновременно только тогда, когда $a = b$ (строгое неравенство, включение);
- **транзитивным**, если $\forall a, b, c \in A (aRb \wedge bRc \Rightarrow aRc)$. Другими словами: из $(a, b) \in R$ и $(b, c) \in R$ следует, что $(a, c) \in R$, например, «быть делителем» или «быть родственником»;
- **полным**, если $\forall a, b \in A$, имеет место либо aRb , либо bRa .

Если R является полным отношением, то для любых двух различных элементов a и b либо пара (a, b) , либо пара (b, a) принадлежит отношению R .

Теоремы:

- 1) R рефлексивно $\Leftrightarrow I \subset R$;
- 2) R антирефлексивно $\Leftrightarrow R \cap I = \emptyset$;
- 3) R симметрично $\Leftrightarrow R = R^{-1}$;
- 4) R асимметрично $\Leftrightarrow R \cap R^{-1} = \emptyset$;
- 5) R антисимметрично $\Leftrightarrow R \cap R^{-1} \subset I$;
- 6) R транзитивно $\Leftrightarrow R \circ R \subset R$.

Пример 2.4. На множестве $M = \{1, 2, 3, 4\}$ задано отношение R , матрица которого показана на рисунке 2.4. Какими из перечисленных свойств обладает отношение?

R	1	2	3	4
1	1			1
2		1		1
3	1			1
4	1			1

Рисунок 2.4 – Матрица отношения R для примера 2.4

Решение. Данное отношение не обладает никаким из вышеперечисленных свойств.

Рассмотрим следующий пример.

Пример 2.5. Пусть A – множество положительных целых чисел. Определим отношение R , задавая $(x, y) \in R$ условием: y кратно x . Определить, какими свойствами обладает отношение R . Построить матрицу данного отношения.

Решение. Отношение R рефлексивно, поскольку для каждого положительного целого числа n , $n = 1 \cdot n$ и $(n, n) \in R$. Данное отношение не является симметричным, т. к. $(2, 4) \in R$, но $(4, 2) \notin R$, однако R антисимметрично, т. к. если $(m, n) \in R$ и $(n, m) \in R$, тогда n кратно m и m кратно n , так что $m = n$. Отношение R транзитивно, потому что если $(m, n) \in R$ и $(n, p) \in R$, то n кратно m и p кратно n , так что p кратно m и $(m, p) \in R$. Матрица отношения R для множества $A = \{1, 2, 3, \dots, 6\}$ показана на рисунке 2.5.

R	1	2	3	4	5	6
1	1	1	1	1	1	1
2		1		1		1
3			1			1
4				1		
5					1	
6						1

Рисунок 2.5 – Матрица отношения R для примера 2.5

2.4 Отношение эквивалентности

2.4.1 Эквивалентность

Отношение эквивалентности представляет собой экспликацию таких обычных слов как «одинаковость», «неразличимость», «взаимозаменяемость». Эквивалентность – это более слабая форма равенства.

Эквивалентность обозначают знаком $\sim$.

Запись $a \sim b$ означает, что упорядоченная пара (a, b) принадлежит множеству $R \subset A \times A$, т. е. является отношением *эквивалентности* на множестве A .

Эквивалентность обладает свойствами рефлексивности, симметричности, транзитивности:

- 1) $a \sim a$ (рефлексивность);
- 2) если $a \sim b$, то $b \sim a$ (симметричность);
- 3) из $a \sim b$ и $b \sim c$ следует, что $a \sim c$ (транзитивность).

Мы говорим, что целые числа имеют один и тот же *паритет*, если числа оба являются либо четными, либо нечетными.

Определим отношение $a \equiv_2 b$ на $\mathbb{Z}$ следующим образом:

$$a \equiv_2 b \rightarrow \{(a, b) \in \mathbb{Z}^2 \mid a \text{ и } b \text{ имеют один паритет}\}.$$

Легко показать, что $\equiv_2$ рефлексивно ($a \equiv_2 a$ поскольку каждое целое число имеет тот же паритет, что оно само), $\equiv_2$ симметрично (если $a \equiv_2 b$, тогда a имеет тот же паритет как и b , т. е. b имеет тот же паритет, что и a , и, следовательно, $b \equiv_2 a$), и $\equiv_2$ является транзитивным (если $a \equiv_2 b$ и $b \equiv_2 c$, тогда a, b и c имеют один и тот же паритет, поэтому $a \equiv_2 c$). Таким образом, $\equiv_2$ является отношением эквивалентности.

2.4.2 Разбиение

Разбиение множества S – это множество X попарно непересекающихся непустых подмножеств S , объединение которых есть S . Формально X является разбиением множества S тогда и только тогда, когда

$$\forall A \in X (A \neq \emptyset \wedge A \subseteq S) \wedge \forall A, B \in X (A \neq B \rightarrow A \cap B = \emptyset) \wedge \bigcup X = S.$$

Например, $X = \{E, O\}$ является разбиением множества $\mathbb{Z}$. Данное разбиение можно увидеть в примере 2.6.

Пример 2.6. Пусть $E = \{2k | k \in \mathbb{Z}\}$ – множество четных целых чисел, а $O = \{2k + 1 | k \in \mathbb{Z}\}$ – множество нечетных целых чисел. Найти разбиение множества целых чисел $\mathbb{Z}$ при помощи множеств E и O .

Решение. Разбиение множества $\mathbb{Z}$ можно представить как $X = \{E, O\}$. Записать данное разбиение можно следующим образом:

$$\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\} \cup \{\dots, -3, -1, 1, 3, 5, \dots\}$$

2.4.3 Классы эквивалентности

Важнейшее значение эквивалентности состоит в том, что это отношение определяет признак, который допускает *разбиение* множества A на непересекающиеся подмножества, называемые **классами эквивалентности**. Справедливо и обратное утверждение: всякое **разбиение** множества A на непересекающиеся подмножества определяет между элементами этого множества некоторое отношение эквивалентности.

Например, отношение «проживать в одном доме» в множестве жителей города является эквивалентностью и разбивает это множество на пересекающиеся подмножества людей, являющихся соседями по дому.

В принципе наше ухо также реализует в определенном смысле отношение эквивалентности, поскольку различает только частоты, далеко отстоящие друг от друга, и не может различить близко стоящие синусоиды, относя их в один класс эквивалентности.

2.4.4 Классы вычетов по модулю

Рассмотрим отношение сравнения по модулю m на множестве натуральных чисел, что записывается как

$$x = y \pmod{m}$$

и означает: x сравнимо с y по модулю m (m – целое положительное число), если x делится на m . Целые числа, сравнимые по модулю m , связаны соотношением

$$x = y + km$$

(k – целое число) и образуют подмножество целых чисел, имеющих одинаковый остаток q при делении на m . Очевидно, что эти подмножества являются классами

эквивалентности, а в качестве представителя каждого из них естественно выбрать остаток $q = 0, 1, 2, \dots, m - 1$.

Таким образом, отношение сравнения по модулю m определяет разбиение множества натуральных чисел на m классов:

$$A_0, A_1, A_2, \dots, A_{m-1},$$

где $A_q = \{q, q + m, q + 2m, \dots\}$ – счетное множество, называемое **классом вычетов по модулю m** .

Например, при $m = 4$ имеем:

1) $A_0 = \{0, 4, 8, 12, \dots\};$

2) $A_1 = \{1, 5, 9, 13, \dots\};$

3) $A_2 = \{2, 6, 10, 14, \dots\};$

4) $A_3 = \{3, 7, 11, 15, \dots\}.$

Системой представителей отношения эквивалентности являются числа 0, 1, 2 и 3, т. к.:

1) $0 = 4 \pmod{4} = 8 \pmod{4} = \dots;$

2) $1 = 5 \pmod{4} = 9 \pmod{4} = \dots;$

3) $2 = 6 \pmod{4} = 10 \pmod{4} = \dots;$

4) $3 = 7 \pmod{4} = 11 \pmod{4} = \dots.$

Таким образом, множество целых чисел разбивается отношением сравнения по модулю 4 на четыре класса эквивалентности. Внутри каждого класса эти числа неразличимы ($4 \sim 0$, $5 \sim 1$, $6 \sim 2$, $7 \sim 3$ и т. д.).

При $m = 1$ разбиение состоит из единственного класса, который совпадает с исходным множеством, т. е. имеем **полное отношение эквивалентности**, при котором любые два элемента эквивалентны (все целые числа делятся на единицу). Отношение $x = y \pmod{2}$ разбивает множество целых чисел на классы четных и нечетных чисел.

2.5 Отношение порядка

Отношение порядка обладает свойствами рефлексивности, транзитивности и антисимметричности. Его принято обозначать символом $\preceq$. Запись $x \preceq y$ означает, что пара $(x, y) \in R \subset A \times A$. Причем x **предшествует** y . Иногда это читают как « x хотя бы y ».

В принятых обозначениях свойства отношения порядка запишутся следующим образом:

- 1) $x \preceq x$ (рефлексивность);
- 2) если $x \preceq y$ и $y \preceq z$, то $x \preceq z$ (транзитивность);
- 3) из $x \preceq y$ и $y \preceq x$ следует $x = y$ (антисимметричность).

Множество, на котором определено отношение порядка, называют **частично упорядоченным** (ЧУ-множеством) и говорят, что порядок введен этим отношением. ЧУ-множество записывается в виде пары $\langle A, R \rangle$.

Множество **линейно (полностью) упорядочено**, если для любых двух его элементов имеет место, по крайней мере, $x \preceq y$ или $y \preceq x$. То есть если добавляется свойство полноты.

Например, множество натуральных чисел с естественным отношением порядка $<$ («меньше») является линейно упорядоченным.

Типичными примерами частичного порядка являются включение, отношение «быть делителем» и т. п. Другими словами, в ЧУ-мноестве некоторые элементы **несравнимы**, т. е. неверно ни одно из соотношений: ни $x \preceq y$, ни $y \preceq x$.

2.6 Оценка и визуализация качества ранжирования

В данном разделе рассмотрим пример использования понятий теории отношений в машинном обучении на примере задачи оценки эффективности ранжирования.

Под **ранжированием** понимается определение порядка на множестве объектов.

Пусть есть множество $T = P \cup N$ положительных и отрицательных объектов и функция $f(\cdot)$, которая каждому объекту ставит в соответствие некоторое число. Следовательно, мы всегда можем утверждать, что

$$f(t_i) \geq f(t_j) \text{ или } f(t_j) \geq f(t_i), \text{ где } t_i, t_j \in T.$$

То есть функция f вводит порядок на множестве T .

Рассмотрим следующий пример.

Пример 2.7. Допустим, что есть следующий набор объектов с соответствующими оценками, задаваемыми функцией f (рисунок 2.6): $p_1(70)$, $p_2(55)$, $p_3(50)$, $p_4(45)$, $p_5(40)$, $p_6(35)$, $p_7(30)$ и $n_1(50)$, $n_2(40)$, $n_3(30)$, $n_4(25)$, $n_5(15)$, $n_6(10)$, $n_7(10)$. Изобразить кривую покрытия. Посчитать параметр AUC (Area Under Curve).

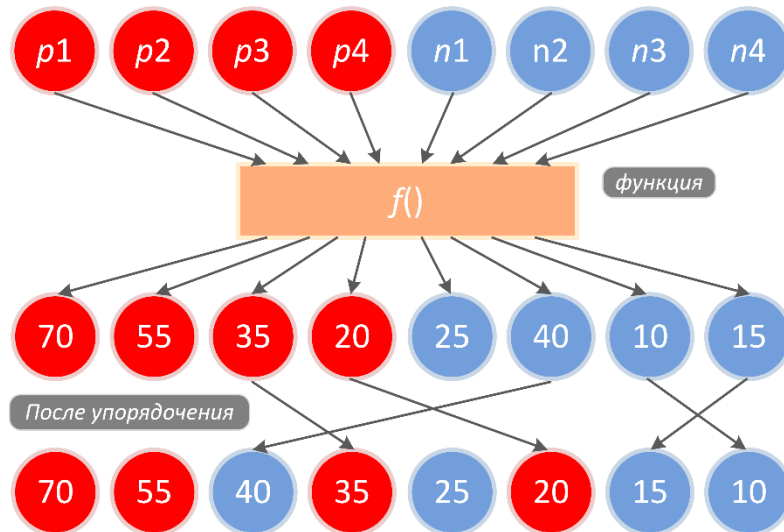


Рисунок 2.6 – Введение отношения порядка на множестве

Решение. В первую очередь возникает вопрос: как оценить *качество ранжирования*, достигаемое при помощи функции $f(\cdot)$?

Введем следующее *отношение* R на множестве $P \times N$.

$$R \subset P \times N = \{(p, n), p \in P, n \in N \mid f(p) > f(n)\}.$$

То есть каждой паре положительного и отрицательного объекта будет соответствовать одна «клетка» на графике отношения. Чем больше $|R|$, тем лучше качество ранжирования, достигаемое при помощи функции $f(\cdot)$.

Основной показатель ранжирования – площадь под кривой покрытия (англ. *AUC* – *area under curve*, рисунок 2.7).

Вычислим AUC для данного примера:

$$AUC = \frac{|R|}{|P \times N|} = \frac{13}{16} = 0,8125.$$

Кусочно-линейная функция, показанная на рисунке 2.7, называется *кривой покрытия*. Чем больше площадь под кривой покрытия, тем лучше качество ранжирования, определяемое соответствующей функцией $f(\cdot)$.

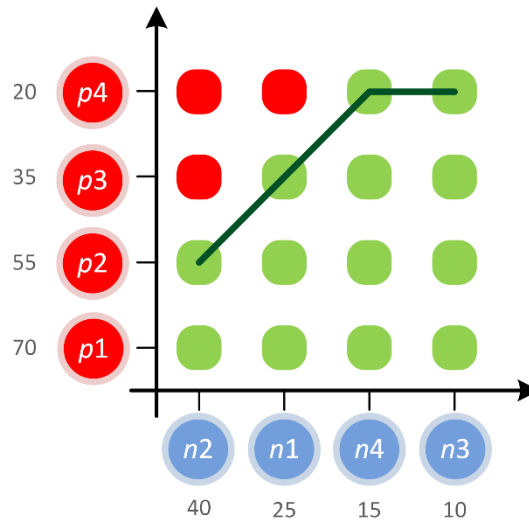


Рисунок 2.7 – Ранжирование

2.7 Композиция отношений

Несколько отношений можно объединить в одно, если соблюдаются определенные условия. Далее мы вводим важное понятия композиции отношений.

Пусть $R \subset A \times B$ – отношение на $A \times B$, а $S \subset B \times C$ – отношение на $B \times C$. **Композицией** отношений S и R называется отношение $T \subset A \times C$, определенное таким образом:

$$T = \{(a, c): \exists b \in B, \text{ что } (a, b) \in R \text{ и } (b, c) \in S \}.$$

Это множество обозначается $T = S \circ R$. Данная запись означает, что вначале выполняется отношение R , а уже после него – отношение S .

Композиция отношений обладает *ассоциативным* законом:

$$T \circ (S \circ R) = (T \circ S) \circ R,$$

но некоммутативна:

$$S \circ R \neq R \circ S.$$

Можно показать, что $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Рассмотрим пример, который показывает, как на практике выполняется композиция отношений.

Пример 2.8. Пусть $A = \{1, 2, 3\}$, $B = \{x, y\}$, а $C = \{\square, \triangle, \bigcirc, \star\}$ и пусть отношения R на $A \times B$ и S на $B \times C$ заданы в следующем виде:

$R = \{(1, x), (1, y), (3, x)\},$
 $S = \{(x, \square), (x, \triangle), (y, \bigcirc), (y, \star)\}.$
 Найти композицию $S \circ R$.

Решение

$$S \circ R = \{(1, \square), (1, \triangle), (1, \bigcirc), (1, \star), (3, \square), (3, \triangle)\},$$

поскольку:

из $(1, x) \in R$ и $(x, \square) \in S$ следует $(1, \square) \in S \circ R$;

из $(1, x) \in R$ и $(x, \triangle) \in S$ следует $(1, \triangle) \in S \circ R$;

из $(1, y) \in R$ и $(y, \bigcirc) \in S$ следует $(1, \bigcirc) \in S \circ R$;

...

из $(3, x) \in R$ и $(x, \square) \in S$ следует $(3, \square) \in S \circ R$.

Рассмотрим еще один пример композиции отношений, в котором отношения заданы на бесконечном множестве.

Пример 2.9. Пусть R и S – отношения на $\mathbb{N}$, заданные в виде

$$R = \{(x, x^2) \mid x \in \mathbb{N}\} \text{ и } S = \{(x, x + 2) \mid x \in \mathbb{N}\}.$$

Найти композицию отношений $R \circ S$ и $S \circ R$.

Решение. $S \circ R = \{(x, x^2 + 2) \mid x \in \mathbb{N}\}, R \circ S = \{(x, (x + 2)^2) \mid x \in \mathbb{N}\}.$

2.7.1 Представление композиции отношений графами

Композиция отношений $A \subset X \times Y$ и $B \subset Y \times Z$ наглядно представляется с помощью графов (рисунок 2.8). Прежде всего необходимо к графу отношения A достроить граф отношения B . Граф отношения $C = B \circ A$ получим, исключив вершины, соответствующие элементам Y . При исключении вершины y_i каждый проходящий через нее путь от вершин x к вершинам z заменяется одной дугой (ребром) с тем же направлением. Параллельные ребра рассматриваются как одно ребро.

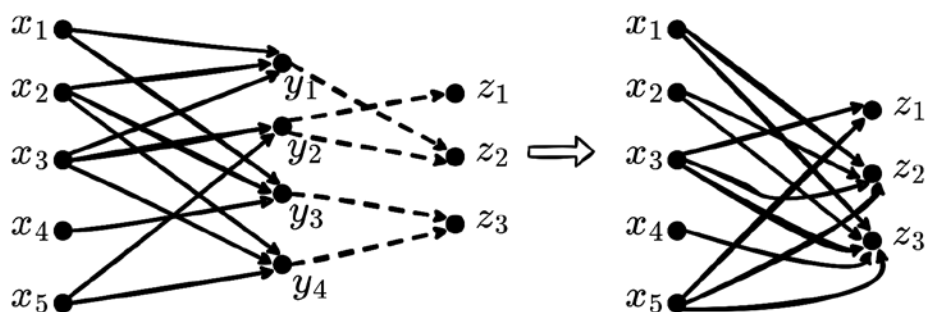


Рисунок 2.8 – Пример построения графа композиции отношений

2.7.2 Представление композиции отношений матрицами

Матрицу композиции $C = B \circ A$ можно получить как произведение матрицы отношений B и A (в порядке их следования), которое выполняется по правилу умножения прямоугольных матриц с последующей заменой отличного от нуля элемента результирующей матрицы единицей.

На рисунке 2.9 представлен пример получения матрицы отношения C из примера, показанного на рисунке 2.8.

$$\begin{array}{c} y_1 \ y_2 \ y_3 \ y_4 \\ \begin{array}{|c|c|c|c|} \hline z_1 & & 1 & \\ \hline z_2 & 1 & 1 & \\ \hline z_3 & & & 1 \ 1 \\ \hline \end{array} \end{array} \quad \begin{array}{c} x_1 \ x_2 \ x_3 \ x_4 \ x_5 \\ \begin{array}{|c|c|c|c|c|} \hline y_1 & 1 & 1 & 1 & \\ \hline y_2 & & & 1 & 1 \\ \hline y_3 & 1 & 1 & & 1 \\ \hline y_4 & & 1 & 1 & 1 \\ \hline \end{array} \end{array} = \begin{array}{c} x_1 \ x_2 \ x_3 \ x_4 \ x_5 \\ \begin{array}{|c|c|c|c|c|} \hline z_1 & & & 1 & 1 \\ \hline z_2 & 1 & 1 & 2 & 1 \\ \hline z_3 & 1 & 2 & 1 & 1 \\ \hline \end{array} \end{array} \rightarrow \begin{array}{c} x_1 \ x_2 \ x_3 \ x_4 \ x_5 \\ \begin{array}{|c|c|c|c|c|} \hline z_1 & & & 1 & 1 \\ \hline z_2 & 1 & 1 & 1 & 1 \\ \hline z_3 & 1 & 1 & 1 & 1 \\ \hline \end{array} \end{array}$$

Рисунок 2.9 – Пример представления композиции отношений матрицами

2.8 Задачи

1 Найдите декартово произведение $R = A \times B$ и $S = B \times A$ множеств A и B , где множество $A = \{1, 2, 3\}$, а множество $B = \{a, b, c\}$.

2 На координатной плоскости постройте следующие множества:

- а) $[1, 2] \times [1, 2]$; б) $\mathbb{R} \times [-1, 1]$.

3 Постройте графики для следующих отношений:

- а) $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y\}$;
 б) $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \geq x\}$;
 в) $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \geq x \text{ и } x \geq 0\}$.

4 Выпишите упорядоченные пары, принадлежащие следующим бинарным отношениям на множествах $A = \{1, 3, 5, 7\}$ и $B = \{2, 4, 6\}$:

- а) $U = \{(x, y) \mid x + y = 9\}$; б) $V = \{(x, y) \mid x < y\}$.

5 Выпишите упорядоченные пары, принадлежащие следующим бинарным отношениям на множествах $A = \{9, 11, 13, 15\}$ и $B = \{10, 12, 14\}$. Составьте матрицы и графы для отношений U и V :

- а) $U = \{(x, y) \mid x + y < 23\}$; б) $V = \{(x, y) \mid x + \frac{y}{2} > 16\}$.

6 Для каждого из следующих отношений на множестве натуральных чисел $\mathbb{N}$ опишите упорядоченные пары, принадлежащие отношениям:

а) $R = \{(x, y) \mid 2x + y = 9\}$;

б) $S = \{(x, y) \mid x + y < 7\}$;

в) $T = \{(x, y) \mid y = x^2\}$.

7 Пусть R – отношение на множестве $\{1, 2, 3, 4\}$, определяемое условием uRv тогда и только тогда, когда $u + 2v$ – нечетное число. Представьте R каждым из способов:

а) как множество упорядоченных пар;

б) в графической форме;

в) в виде матрицы.

8 Пусть $M = \{1, 2, 3, 4, 5, 6\}$. Задайте в явном виде (списком) и матрицей отношение $R \subset M \times M$, если R означает – «быть строго меньше». Укажите свойства данного отношения.

9 Отношение R на множестве $A = \{a, b, c, d\}$ задано матрицей, представленной на рисунке 2.10. Выпишите все упорядоченные пары.

R	a	b	c	d
a		1	1	
b			1	1
c		1		
d	1	1		1

Рисунок 2.10 – Матрица отношения для задачи 9 раздела 2

10 Отношение R на множестве $A = \{1, 2, 3, 4\}$ представлено графом на рисунке 2.11. Представьте R каждым из способов:

а) как множество упорядоченных пар;

б) в виде матрицы;

в) с помощью характеристического свойства.

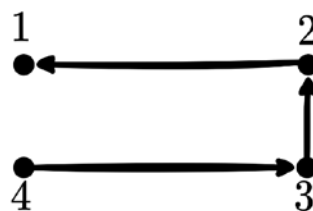


Рисунок 2.11 – Граф для задачи 10 раздела 2

11 Изобразите граф отношения $V = \{(x, y): x < y\}$ между множествами $A = \{1, 3, 5, 7\}$ и $B = \{2, 4, 6\}$.

12 Выпишите множество упорядоченных пар и начертите ориентированный граф отношения R , заданного матрицей на рисунке 2.12.

R	a	b	c	d
1	1	1	1	1
2		1		
3			1	

Рисунок 2.12 – Матрица отношения для задачи 12 раздела 2

13 Для каждого из следующих отношений на множестве натуральных чисел $\mathbb{N}$ опишите упорядоченные пары, принадлежащие отношениям:

а) $R = \{(x, y): 2x + y = 9\}$;

б) $S = \{(x, y): x + y < 7\}$;

в) $T = \{(x, y): y = x^2\}$.

14 На множестве $V = \{a, b, c\}$ задано отношение $E = \{(a, a), (a, b), (b, c), (c, b), (c, a)\}$. Изобразите граф отношения E .

15 На множестве $A = \{1, 2, 3, 4\}$ задано отношение $R = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 3), (3, 4), (4, 4)\}$. Изобразите граф отношения R и укажите свойства данного отношения.

16 Пусть $A = \{(b, a), (c, e), (d, i), (f, o), (g, u)\}$ и $B = \{(v, a), (w, e), (x, i), (y, o), (z, u)\}$. Опишите отношение $T = A^{-1} \circ B$.

17 Пусть $A = \{1, 2, 3, 4, 5\}$, $B = \{6, 7, 8, 9\}$, $C = \{10, 11, 12, 13\}$, $D = \{\square, \triangle, \bigcirc, \star\}$. Пусть $R = A \times B$, $S = B \times C$ и $T = C \times D$ определены следующим образом: $R = \{(1, 7), (4, 6), (5, 6), (2, 8)\}$, $S = \{(6, 10), (6, 11), (7, 10), (8, 13)\}$, $T = \{(11, \triangle), (10, \triangle), (13, \star), (12, \square), (13, \bigcirc)\}$.

Определите следующие отношения:

а) S^{-1} и R^{-1} ;

г) $R^{-1} \circ S^{-1}$;

б) $S \circ R$;

д) $T \circ S$;

в) $S \circ S^{-1}$ и $S^{-1} \circ S$;

е) $T \circ (S \circ R)$.

18 Пусть отношения $U, V \subset R \times R$ определены следующим образом: $U = \{(x, y): y = x^2 + 5\}$ и $V = \{(x, y): y = 3x\}$. Опишите следующие отношения:

а) $U \circ V$;

в) U^{-1} ;

б) $V \circ U$;

г) V^{-1} .

19 Представьте бинарное отношение, заданное графом (рисунок 2.13), как множество упорядоченных пар и запишите его матрицу. Какими свойствами характеризуется данное отношение?

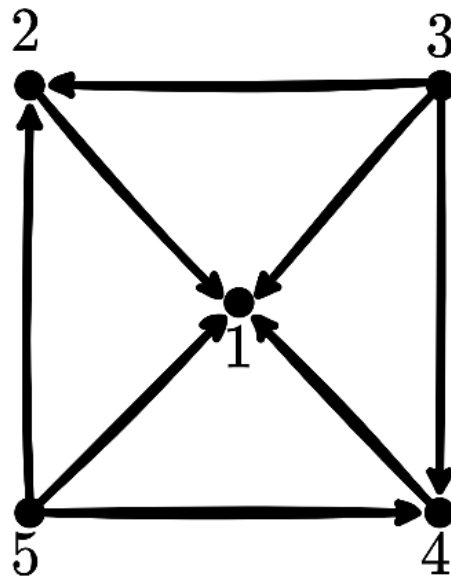


Рисунок 2.13 – Граф для задачи 19 раздела 2

20 Пусть отношение R задано следующей матрицей (рисунок 2.14). Назовите свойства данного отношения.

R	a	b	c	d
a	1	1	1	1
b		1	1	1
c			1	1
d				1

Рисунок 2.14 – Матрица отношения для задачи 20 раздела 2

21 На множестве $A = \{a, b, c, d, e\}$ заданы отношения T_1, T_2, T_3, T_4 (рисунок 2.15). Назовите свойства каждого отношения.

T_1	a	b	c	d	e
a	1	1			
b			1	1	
c	1				1
d					
e				1	

a

T_3	a	b	c	d	e
a	1	1	1		
b	1	1	1		
c	1	1	1		
d				1	
e					1

b

T_2	a	b	c	d	e
a		1			
b	1		1	1	
c		1			
d					1
e					1

b

T_4	a	b	c	d	e
a		1	1		
b	1	1	1		
c	1	1			
d				1	
e					1

z

a – матрица отношения T_1 ; b – матрица отношения T_2 ;

b – матрица отношения T_3 ; z – матрица отношения T_4

Рисунок 2.15 – Матрицы отношений для задачи 21 раздела 2

22 Пусть задано множество $M = \{1, 2, 3, 4, 5, 6\}$. На данном множестве существует отношение $T = \{(x, y): x \text{ — делитель } y\}$. Запишите матрицу отношения T и назовите свойства.

23 Пусть задано множество $M = \{1, 2, 3, 4, 5, 6\}$. На данном множестве существует отношение $T = \{(x, y): \text{mod}(x, y) = 1\}$. Запишите матрицу отношения T и назовите свойства.

24 Какими свойствами обладают бинарные отношения, заданные на некотором множестве людей X и выражающиеся соотношениями (везде имеется в виду, что $x_i, x_j \in X$):

а) « x_i похож на x_j »;

д) « x_i живет в одном доме с x_j »;

б) « x_i знаком с x_j »;

е) « x_i весит больше, чем x_j »;

в) « x_i родственник x_j »;

ж) « x_i подчинен x_j ».

г) « x_i сосед x_j »;

25 Пусть $M = \{1, 2, 3, 4, 5, 6\}$. Задайте матрицей отношение $R \subseteq M \times M$, если R означает – «быть строго меньше». Является ли данное отношение рефлексивным? Антирефлексивным? Симметричным? Антисимметричным? Транзитивным? Полным?

26 Какие из приведенных отношений являются отношением частичного порядка (рисунок 2.16)?

E	a	b	c	d
a	1		1	1
b		1	1	1
c			1	1
d				1

a

F	a	b	c	d
a	1	1		
b		1	1	
c			1	1
d				1

b

G	a	b	c	d
a			1	1
b		1	1	1
c			1	1
d				1

$в$

H	a	b	c	d
a	1	1	1	1
b		1	1	1
c			1	1
d				1

$г$

a – матрица отношения E ; b – матрица отношения F ;

$в$ – матрица отношения G ; $г$ – матрица отношения H

Рисунок 2.16 – Матрицы отношений для задачи 26 раздела 2

27 Укажите свойства, которыми обладают приведенные ниже отношения:

- а) « x кратно y » в множестве целых чисел;
- б) « x имеет общие точки с y » в множестве прямых на плоскости;
- в) « x касается с y » в множестве окружностей на плоскости;
- г) « x знаком с y » в множестве людей.

3 ФУНКЦИИ (ОТОБРАЖЕНИЯ)

Понятие функции является фундаментальным для математики. Термин «отображение» мы считаем синонимом термина «функция», но различаем контексты употребления. Термин «функция» более общий и может употребляться всегда, термин «отображение», напротив, применяется только в тех случаях, когда структура отображаемого множества имеет первостепенное значение. Например, мы говорим «булева функция», но «отображение групп».

В этом разделе мы уточним понятие «отображение» как тройки объектов (двух множеств и правила, сопоставляющего элементы первого множества с элементами второго множества), и определим два новых понятия, связанных с отображениями: «образ» и «прообраз» множества при отображении.

3.1 Функциональные отношения

Отношение $f \subset A \times B$ называется **функцией** из A в B и обозначается через $f: A \rightarrow B$, если $\forall a \in A$, существует единственный элемент $b \in B$, такой, что $(a, b) \in f$ или $b = f(a)$. Таким образом, главное свойство функции – **однозначность**.

Также можно сказать, что f – правило, сопоставляющее каждый элемент $a \in A$ с вполне определенным элементом $f(a) = b \in B$.

Пример 3.1. Определить, являются ли данные отношения функциональными: $f = \{(2, 4), (4, 8), (6, 12)\}$, $g = \{(2, 4), (4, 6), (4, 8), (6, 12)\}$.

Решение. Отношение f является функциональным, а g – не является функциональным, т. к. отсутствует однозначность.

Поскольку функция является отношением, то для нее можно использовать введенные понятия: *область отправления* (A), *область прибытия* (B), *область определения* $\text{Dom } f = \{a \in A \mid \exists b \in B (b = f(a))\}$; *область значений* функции $\text{Im } f = \{b \in B \mid \exists a \in A (b = f(a))\}$.

3.2 Типы отображений (инъекция, сюръекция, биекция)

Мы можем классифицировать функции $f: A \rightarrow B$ по тому, как много элементов x из области отправления A отображается на каждый элемент y из области прибытия B .

Функция f называется **инъективной** (или инъекцией), если каждый элемент y является образом не более одного элемента x (отображение «в», рисунок 3.1).

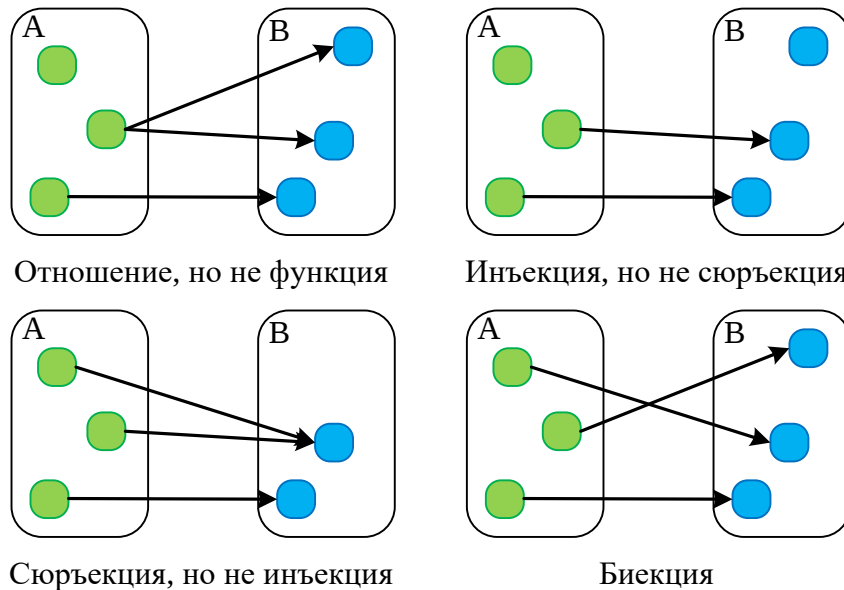


Рисунок 3.1 – Иллюстрация понятий инъекция, сюръекция и биекция

Пример 3.2. Определить, является ли функция $f(x) = x^2$, $f \subset \mathbb{N} \times \mathbb{N}$ инъекцией.

Решение. Да, поскольку каждому элементу из области отправления соответствует не более одного элемента в области прибытия.

Функция f называется **сюръективной** (или сюръекцией), если каждый элемент y является образом не менее одного элемента x (отображение «на», см. рисунок 3.1).

Пример 3.3. Определить, является ли функция $f(x) = x^2$, $f \subset \mathbb{N} \times \mathbb{N}$ сюръекцией.

Решение. Нет, поскольку область значений содержит только квадраты целых чисел, а не все множество $\mathbb{N}$.

Функция f называется **биективной** (или биекцией), если функция одновременно инъективная и сюръективная (взаимно однозначная функция, см. рисунок 3.1).

Если функция *сюръективна*, это значит, что для любого $y \in B$ существует $x \in A$, такой, что $y = f(x)$. Эквивалентный путь показать, что функция сюръективна, – это показать, что область ее значений равна области прибытия.

Рассмотрим несколько примеров.

Пример 3.4. Определить, является ли функция $f(x) = x + 1, f \subset \mathbb{N} \times \mathbb{N}$ сюръекцией.

Решение. Нет, поскольку область значений не содержит 0.

Пример 3.5. Определить, является ли функция $f(x) = x + 1, f \subset \mathbb{Z} \times \mathbb{Z}$ сюръекцией.

Решение. Да, поскольку область значений состоит из элементов $y = x + 1$.

Инъекция отображает различные элементы A в различные элементы B , т. е. если $x \neq y$, то $f(x) \neq f(y)$.

Пример 3.6. Определить, является ли функция $f(x) = x^2, f \subset \mathbb{Z} \times \mathbb{Z}$ инъекцией.

Решение. Нет. Например, $f(-1) = f(1) = 1$.

Пример 3.7. Определить, является ли функция $f(x) = x + 1, f \subset \mathbb{Z} \times \mathbb{Z}$ инъекцией.

Решение. Да.

Биекция является *взаимно однозначным соответствием* (one-to-one correspondence). Любая биекция f имеет обратную функцию $f^{-1} = \{(y, x) \mid (x, y) \in f\}$. Из приведенных примеров только $f(x) = x + 1, f \subset \mathbb{Z} \times \mathbb{Z}$ является биекцией.

Обобщив вышесказанное, сформулируем формальные признаки, по которым можно определить относится ли функция к конкретному типу отображения (таблица 3.1).

Таблица 3.1 – Формальные признаки определения типа отображения функции

Тип отображения	Формальный признак
Не инъекция	Если возможно найти числа $a_1 \neq a_2$, для которых значение функции $f(a_1) = f(a_2)$
Не сюръекция	Если возможно найти число, которое содержится в области значений функции, но оно <i>не является</i> значением функции
Не биекция	Если функция неинъективна и несюръективна

3.3 Композиция функций

Поскольку функции являются частным случаем отношений, для них определена композиция. Если $f: A \rightarrow B$ и $g: B \rightarrow C$, то композиция функций f и g записывается так: $g \circ f$. Этот способ записи объясняется тем, что обозначение функции принято писать слева от списка аргументов:

$$(g \circ f)(x) \stackrel{\text{def}}{=} g(f(x)).$$

Композиция двух функций также является функцией.

Поскольку композиция отношений обладает свойством ассоциативности, то, в частности, имеет место следующая теорема.

Пусть $f: A \rightarrow B$, $g: B \rightarrow C$ и $h: C \rightarrow D$. Тогда $h \circ (g \circ f) = (h \circ g) \circ f$, т. е. композиция функций ассоциативна.

Пример 3.8. Пусть $f(x) = \sqrt{x}$ и $g(x) = x + 3$ – функции, заданные на множестве действительных чисел. Найти $g \circ f$ и $f \circ g$.

Решение

Функция $f(g(x)) = f(x + 3) = \sqrt{x + 3}$.

Функция $g(f(x)) = g(\sqrt{x}) = \sqrt{x} + 3$.

На основе этого примера мы легко можем видеть, что композиция функций некоммутативна, т. е.

$$g \circ f \neq f \circ g.$$

Пусть $I: A \rightarrow A$ определена соотношением $I(a) = a$ для всех $a \in A$. Тогда функция I называется **тождественной** функцией на A .

Тождественная функция коммутативна:

$$I \circ f = f \circ I = f.$$

С понятием тождественной функции тесно связано понятие обратной функции. Пусть $f: A \rightarrow B$. Очевидно, $f \subset A \times B$, т. к. f является отношением на $A \times B$. Обратное отношение $f^{-1} \subset B \times A$ определяется как

$$f^{-1} = \{(b, a) : (a, b) \in f\}.$$

При этом отношение f^{-1} может не быть функцией из B в A , даже если f является функцией из A в B .

Отношение f^{-1} является функциональным и называется **обратной функцией**, если исходная функция f является биекцией.

Если существует обратная функция, то $f \circ f^{-1} = f^{-1} \circ f = I$.

Пример 3.9. Определим две функции: S и P из $\mathbb{Z}$ в $\mathbb{Z}$. Пусть $S(z) = z + 1$ и $P(z) = z - 1$. Показать, что $P^{-1} = S$.

Решение. $P = \{(z, z - 1) : z \in \mathbb{Z}\}$

и $S = \{(z, z + 1) : z \in \mathbb{Z}\} =$

$= \{(z_1 - 1, z_1) : z_1 \in \mathbb{Z}\}$ // подстановка $z_1 = z + 1$

$= \{(z - 1, z) : z \in \mathbb{Z}\}$ // подстановка z для z_1 , которое не используется

$= P^{-1}$

Обратная функция к композиции:

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

3.4 Подстановки

Взаимно однозначное отображение множества $N = \{1, 2, \dots, n\}$ на себя называется подстановкой.

Биективная функция $f: N \rightarrow N$ называется **подстановкой**.

Подстановку удобно задавать таблицей из двух строк: в первой строке аргументы, во второй соответствующие им образы. Например, взаимно однозначное соответствие четырех чисел, заданное множеством упорядоченных пар $\{(1, 2), (2, 4), (3, 3), (4, 1)\}$, запишется как

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

Так как безразлично, в каком порядке следуют упорядоченные пары отображения, то одна и та же подстановка допускает различные представления.

Каждая строка в записи подстановки содержит n различных чисел, расположенных в определенном порядке, т. е. представляет собой некоторую **перестановку**. Число всех *перестановок* из n чисел равно $n!$, следовательно, число всевозможных подстановок также равно $n!$.

Тождественная перестановка переводит каждое число в себя:

$$e_n = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Если в подстановке a поменять местами верхнюю и нижнюю строки, то получим **обратную подстановку** a^{-1} . В силу биективности a обратная подстановка всегда существует.

Произведение (**композиция**) подстановок $c = ba$ определяется как результат последовательного применения: сначала a , затем b .

Пример 3.10. Пусть $a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix}$ и $b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 2 & 3 & 5 \end{pmatrix}$.
Найти $c = ba$.

Решение. Произведением подстановок является их композиция:

$$c = ba = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix}.$$

Теперь определим специальный вид перестановки, называемый циклом.

Цикл – это подстановка вида

$$\sigma_c = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ a_2 & a_3 & \dots & a_1 \end{pmatrix} = (a_1, a_2, \dots, a_n).$$

То есть $\sigma_c(a_k) = a_{k+1}$, $k < n$ и $\sigma_c(a_n) = a_1$. Таким образом, сокращенная запись цикла сводится к перечислению множества элементов, которые циклически переходят друг в друга.

Любую подстановку σ можно единственным способом разложить в **произведение циклов**, которые не имеют общих элементов.

Алгоритм:

- 1) выберем произвольный элемент a из числа аргументов подстановки σ ;
- 2) образуем цикл $(a, \sigma(a), \sigma^2(a), \dots, \sigma^k(a))$, где $\sigma^{k+1}(a) = a$;
- 3) выберем произвольный элемент b из числа аргументов подстановки σ , который не содержится ни в одном из полученных циклов, и повторим шаг 2. Если таких элементов нет, значит, разложение подстановки σ на произведение циклов завершено.

Таким образом, любая подстановка разбивает множество N на классы эквивалентности.

Пример 3.11. Разложить подстановку σ на непересекающиеся циклы:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 7 & 8 & 6 & 1 & 5 \end{pmatrix}.$$

Решение

1) Выберем элемент 1 и начнем образовывать первый цикл:

1, $\sigma(1) = 4$, $\sigma(4) = 7$, $\sigma(7) = 1$. Цикл сформирован: (1, 4, 7);

2) выберем элемент 2 и начнем образовывать второй цикл:

2, $\sigma(2) = 3$, $\sigma(3) = 2$. Цикл сформирован: (2, 3);

3) выберем элемент 5 и начнем образовывать третий цикл:

5, $\sigma(5) = 8$, $\sigma(8) = 5$. Цикл сформирован: (5, 8);

4) выберем элемент 6 и начнем образовывать четвертый цикл:

6, $\sigma(6) = 6$. Цикл сформирован: (6). Больше элементов нет.

Таким образом,

$$\sigma = (1, 4, 7)(2, 3)(5, 8)(6).$$

Поскольку циклы не пересекаются, то порядок циклов не меняет перестановку. По желанию одноэлементные циклы можно опускать, поскольку они реально ничего не меняют.

3.5 Рекурсивно-определенные функции

В случае когда функция F задана формулой, мы можем найти ее значение для любого элемента ее области отправления. Например, если функция $F: \mathbb{N} \rightarrow \mathbb{N}$ определяется формулой $F(n) = 3n + 2$, мы можем напрямую вычислить ее значение для аргумента $n = 100$, $F(100) = 3 \cdot 100 + 2 = 302$.

Однако функции не обязательно определяются таким непосредственным образом. Рассмотрим функцию $G: \mathbb{N} \rightarrow \mathbb{N}$, определенную как $G(0) = 2$ и $G(n) = G(n - 1) + 3$. Тогда

$$G(4) = G(3) + 3 \Rightarrow$$

$$G(2) + 3 + 3 \Rightarrow$$

$$G(1) + 3 + 3 + 3 \Rightarrow$$

$$G(0) + 3 + 3 + 3 + 3 \Rightarrow$$

$$2 + 4 \cdot 3 = 14.$$

Если мы захотим узнать $G(3112)$, то нам необходимо вычислить все предыдущие значения $G(1), G(2), \dots, G(3111)$. В данной ситуации говорят, что G определена **рекурсивным** образом.

Как вы заметили, две функции F и G на самом деле являются одинаковыми: $F(n) = G(n)$. Функция $F(n)$ является **замкнутой формой** для G .

Рассмотрим несколько примеров.

Пример 3.12. Функция $F: \mathbb{N} \rightarrow \mathbb{N}$ определяется как $F(n) = 3^n$. Задать данную функцию рекурсивно.

Решение. Функцию $F(n)$ можно определить рекурсивно как $F(0) = 1$ и $F(n) = 3 \cdot F(n-1)$ для $n \geq 1$.

Пример 3.13. Сумма первых k элементов последовательности $a_1, a_2, \dots, a_n$ может быть определена как $SUM(k) = a_1 + a_2 + \dots + a_k$. Задать последовательность в виде рекурсивной функции.

Решение. Рекурсивно эта же функция может быть определена как $S(1) = a_1$ и $S(k) = S(k-1) + a_k$ для $k \geq 1$.

Пример 3.14. Сумма первых n членов геометрической прогрессии $a + ac + ac^2 + \dots + ac^{n-1}$. Задать последовательность в виде рекурсивной функции.

Решение. Последовательность может быть определена как $g(0) = a$ и $g(k) = g(k-1) + ac^k$ для $k \geq 1$.

3.6 Задачи

1 Определите, какие отношения являются функциями:

- а) отношение « x – брат или сестра y » на множестве всех людей;
- б) отношение на множестве $\mathbb{Z}$, заданное парами: $\{(x, x^2)\}$;
- в) отношение на множестве $\mathbb{R}$, заданное парами: $\{(x, y): x = y^2\}$.

2 Определите, какие из приведенных ниже отношений являются функциями (x и $y \in \mathbb{R}$):

- а) $y^2 = x^2 + 4$;
- б) $y^3 = x^3 + 4$;
- в) $y = 5$;
- г) $y = \sqrt{x^2 - 2}$;
- д) $x = 7$.

3 Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ (действительные числа). Найдите область определения и множество значений функций:

а) $f(x) = x^2 + 4$;

г) $f(x) = 1 / (x^2 + 4)$;

б) $f(x) = 1 / (\sqrt{x - 2})$;

д) $f(x) = 1 / (x^2 - 4)$;

в) $f(x) = \sqrt{x - 2}$;

е) $f(x) = |x|$.

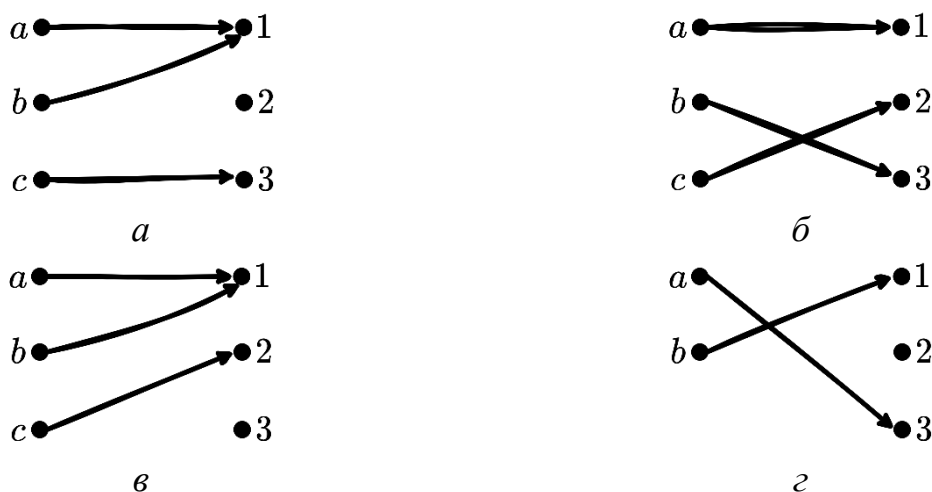
4 Определите, какие из следующих отношений между множествами $A = \{a, b, c\}$ и $B = \{1, 2, 3\}$ являются функциями $f: A \rightarrow B$:

а) $f = \{(a, 1), (a, 2), (b, 3), (c, 2)\}$;

б) $g = \{(a, 1), (b, 2), (c, 1)\}$;

в) $h = \{(a, 1), (c, 2)\}$.

5 Определите, какие из функций, показанных на рисунке 3.2, инъективны, а какие сюръективны. Перечислите все биекции.



a – граф функции E ; $б$ – граф функции F ;

$в$ – граф функции G ; $г$ – граф функции H

Рисунок 3.2 – Графы отношений для задачи 5 раздела 3

6 Определите, какие из следующих функций являются сюръекциями:

а) $F_1: \mathbb{R} \rightarrow \mathbb{R}$ где $F_1(x) = x^2 - 1$;

в) $F_3: \mathbb{Z} \rightarrow \mathbb{Z}$ где $F_3(x) = x^3$;

б) $F_2: \mathbb{R} \rightarrow \mathbb{Z}$ где $F_2(x) = [x]$;

г) $F_4: \mathbb{R} \rightarrow \mathbb{R}$ где $F_4(x) = x^3$.

7 Пусть $X = \{-1, 0, 1, 2\}$ и $Y = \{-4, -2, 0, 2\}$. Определим функцию $f: X \rightarrow Y$ как $f(x) = x^2 - x$. Является ли f биекцией?

8 Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ определяется выражением $f(x) = x^n$, где n фиксированное число из $\mathbb{N}$. Для каких значений n функция f является биекцией?

9 Пусть $f: \mathbb{R} \rightarrow \mathbb{R}$ определяется выражением $f(x) = n2^x$, где n фиксированное положительное целое число. Для каких n функция f является сюръекцией?

10 Функции R и S определены диаграммами, показанными на рисунке 3.3. Найдите $S \circ R$. Композицию изобразите в виде диаграммы.



a – граф функции R ; $б$ – граф функции S

Рисунок 3.3 – Графы отношений для задачи 10 раздела 3

11 Пусть $X = \{1, 2, 3, 4\}$. Пусть $f: X \rightarrow \mathbb{R}$ функция, определяемая как множество упорядоченных пар $\{(1, 2), (2, 3), (3, 4), (4, 5)\}$. Также пусть $g: \mathbb{R} \rightarrow \mathbb{R}$ функция $g(x) = x^2$. Что из себя будет представлять $g \circ f$?

12 Для функций f и g , заданных на множестве действительных чисел $\mathbb{R}$, найдите $f(g(x))$ и $g(f(x))$:

- а) $f(x) = x^2 + 1$; $g(x) = x + 3$;
- б) $f(x) = \sqrt{x^2 + 2}$; $g(x) = x^2 + 3$;
- в) $f(x) = 1 / x$; $g(x) = 2x + 3$.

13 Функции F, G и H определены графами, показанными на рисунке 3.4. Найдите следующие композиции:

- а) $G \circ F$;
- б) $H \circ (G \circ F)$;
- в) $(H \circ G) \circ F$.

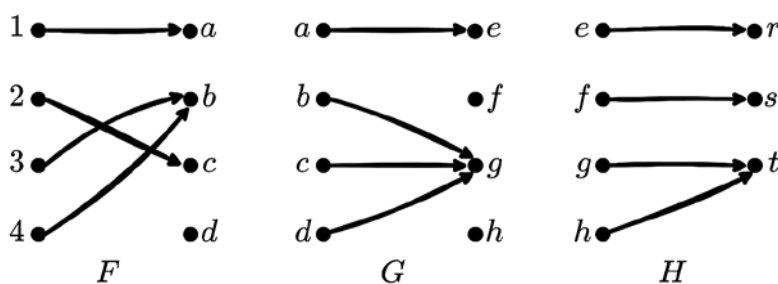


Рисунок 3.4 – Графы функций F, G и H для задачи 13 раздела 3

14 Пусть $X = \{1, 2, 3, 4\}$. Функции F, G и H определены следующим образом:
 $F(1) = 3, F(2) = 2, F(3) = 2, F(4) = 4$;
 $G(1) = 1, G(2) = 3, G(3) = 4, G(4) = 2$;
 $H(1) = 2, H(2) = 4, H(3) = 1, H(4) = 3$.

Найдите следующие композиции:

а) $F \circ G$;

в) $G \circ H$;

б) $H \circ F$;

г) $F \circ G \circ H$.

15 Пусть $f(x) = (2x - 3) / (x + 4)$ и $g(x) = x^2 + 5$. Найдите $f \circ g$, $g \circ f$, $f \circ f$, $g \circ g$.

16 Найдите композиции $f \circ g$, $g \circ f$, а также подстановки f^{-1} и g^{-1} :

а) $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$;

в) $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$;

б) $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$;

г) $f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$, $g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$.

17 Определите, какие из следующих функций являются инъективными, сюръективными, биективными. Для биекций найдите обратные функции. Область значений и область определения – множество действительных чисел $\mathbb{R}$.

а) $f_1(x) = |x|$;

г) $f_4(x) = x + |x|$;

б) $f_2(x) = x^2 + 4$;

д) $f_5(x) = x(x - 2)(x + 2)$.

в) $f_3(x) = x^3 + 6$;

18 Найдите обратные функции $f^{-1}(x)$:

а) $f_1(x) = (x + 4) / 2$;

в) $f_3(x) = (x - 2) / (x + 3)$;

б) $f_2(x) = x^3$;

г) $f_4(x) = (4x + 3) / (2x + 5)$.

19 Запишите приведенные ниже перестановки в виде непересекающихся циклов:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 4 & 7 & 8 & 6 & 1 & 5 & 2 \end{pmatrix}$;

в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 1 & 7 & 3 & 6 & 5 \end{pmatrix}$;

б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 7 & 8 & 3 & 6 & 9 & 1 & 5 \end{pmatrix}$;

г) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$.

20 Найдите $\sigma \circ \tau$, где:

а) $\sigma = (1, 3, 4)(2, 5)$ и $\tau = (1, 2)(3, 4)(5)$;

б) $\sigma = (1, 2)(3, 4)(5, 6)$ и $\tau = (1, 2)(3, 4)(5, 6)$;

в) $\sigma = (1, 2, 3)(4, 5, 6)$ и $\tau = (1, 2)(3, 4)(5, 6)$;

г) $\sigma = (1, 2, 3, 8)(4, 5, 6)(7)$ и $\tau = (1, 2)(3, 8)(4, 5)(6, 7)$.

21 Найдите первые шесть членов последовательности элементов, определенной как $F(0) = 5$, $F(1) = 10$ и $F(n) = F(n - 1) - 2F(n - 2)$ для $n \geq 2$.

22 Найдите первые шесть членов последовательности элементов, определенной как $F(0) = 1$, $F(1) = 3$, $F(2) = 5$, и $F(n) = 3F(n - 1) + 2F(n - 2) - 3F(n - 3)$ для $n \geq 3$.

23 Найдите замкнутую, а также рекурсивную форму функций для следующих последовательностей:

а) $0, 2, 4, 6, 8, \dots$;

в) $1, 3, 5, 7, 9, 11, 13, \dots$;

б) $1, 2, 4, 8, 16, \dots$;

г) $1, 1, 3, 3, 5, 5, 7, 7, \dots$.

24 Пусть $a, b \in \mathbb{N}$ и пусть Q определена рекурсией

$$Q(a, b) = \begin{cases} 0, & \text{если } a < b; \\ Q(a - b, b) + 1, & \text{если } a \geq b. \end{cases}$$

Определите, что делает функция Q . Найдите:

а) $Q(2, 5)$;

б) $Q(12, 5)$;

в) $Q(5861, 7)$.

4 АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

4.1 Общее понятие алгебры

Алгебраические методы находят широкое применение при формализации различных предметных областей. То есть при построении модели предметной области все начинается с введения подходящих обозначений для операций и отношений с последующим исследованием их свойств. Таким образом, владение алгебраической терминологией входит в арсенал средств, необходимых для абстрактного моделирования, предшествующего практическому программированию конкретной предметной области.

Алгеброй называется раздел математики, изучающий системы операций над элементами некоторого множества.

В этом универсальном смысле слово «алгебра» употребляется вместе с подходящим прилагательным: «общая алгебра», «универсальная алгебра», «абстрактная алгебра». Нам уже известны конкретные примеры таких алгебр – «алгебра подмножеств», «булева алгебра», «матричная алгебра».

Всюду определенная функция $\varphi: M^n \rightarrow M$ называется *n -арной операцией* на M (иногда говорят *n -местная операция*). Чаще всего мы сталкиваемся с *бинарными* ($n = 2$) операциями

$$\varphi: M \times M \rightarrow M,$$

и *унарными* операциями $n = 1$.

Множество M вместе с набором операций $\Sigma = \{\varphi_1, \dots, \varphi_m\}$, $\varphi_i: M^{n_i} \rightarrow M$, где n_i -арность операций φ_i , называется *алгебраической структурой*, или просто *алгеброй*. Множество M называется *основным* (или *несущим*) множеством; множество Σ называется *сигнатурой* алгебры.

Для обозначения алгебры используют следующий способ $\mathcal{A} = \langle A; \Sigma \rangle$. Иногда сигнатуру опускают.

Например, алгебра $\langle \mathcal{P}(M); \cup, \cap, ^- \rangle$ – алгебра подмножеств над множеством M .

4.2 Таблица Кэли

Вместо $y = \varphi(x_1, x_2)$ будем писать $y = x_1 \circ x_2$, если у операции нет традиционного обозначения, такого, как $y = x_1 + x_2$ или $y = x_1 x_2$.

Пусть X – конечное множество. Обозначим через $\langle X, \circ \rangle$ алгебру с одной бинарной операцией. Результаты операций на конечных множествах представлять с помощью так называемых **таблиц Кэли**. Таблица Кэли строится следующим образом: слева и сверху квадратной таблицы выписываются все элементы множества; на пересечении строки, соответствующей элементу x , и столбца, соответствующего элементу y , указывают результат действия над парой (x, y) , т. е. $x \circ y$.

Например, пусть $B = \{0, 1\}$, а X – булеан множества B . Очевидно, что элементами X являются

$$x = \emptyset, \quad y = \{0\}, \quad z = \{1\}, \quad w = \{0, 1\}.$$

Видно, что операции объединения $\cup$ и пересечения $\cap$ подмножеств B могут быть заданы таблицами Кэли (рисунок 4.1).

$\cup$	x	y	z	w
x	x	y	z	w
y	y	y	w	w
z	z	w	z	w
w	w	w	w	w

a

$\cap$	x	y	z	w
x	x	x	x	x
y	x	y	x	y
z	x	x	z	z
w	x	y	z	w

б

Рисунок 4.1 – Таблицы Кэли для операции объединения (а) и пересечения (б)

4.3 Свойства операций

Некоторые часто встречающиеся свойства операций имеют специальные названия (таблица 4.1).

1 Ассоциативные операции: сложение и умножение чисел, объединение и пересечение множеств, композиция отношений. Неассоциативные операции: возведение в степень, вычитание множеств.

Пример 4.1. Проверить на ассоциативность операцию возведения в степень, т. е. пусть $a \circ b = a^b$.

Решение. Для того чтобы операция была ассоциативной, необходимо, чтобы $(a \circ b) \circ c = a \circ (b \circ c)$.

Распишем левую и правую часть тождества применительно к операции возведения в степень.

$$(a \circ b) \circ c = (a^b) \circ c = (a^b)^c = a^{bc};$$

$$a \circ (b \circ c) = a \circ (b^c) = a^{b^c}.$$

То есть левая и правая часть не равны, следовательно, операция неассоциативна.

Таблица 4.1 – Свойства алгебраических операций

Свойство	Математическое описание
Коммутативность	$a \circ b = b \circ a$
Ассоциативность	$(a \circ b) \circ c = a \circ (b \circ c)$
Дистрибутивность слева	$a \diamond (b \circ c) = (a \diamond b) \circ (a \diamond c)$
Дистрибутивность справа	$(a \circ b) \diamond c = (a \diamond c) \circ (b \diamond c)$
Поглощение	$(a \circ b) \diamond a = a$
Идемпотентность	$a \circ a = a$

Пример 4.2. Проверить на ассоциативность операцию вычитания множеств.

Решение. Чтобы показать, что какое-то свойство не выполняется, достаточно привести один контрпример: $\{a, b\} \setminus (\{a\} \setminus \{a\}) = \{a, b\}$, $(\{a, b\} \setminus \{a\}) \setminus \{a\} = \{b\}$.

Таким образом, вычитание множеств неассоциативно.

2 Коммутативные операции: сложение и умножение чисел, объединение и пересечение множеств. Некоммутативные операции: умножение матриц, композиция отношений, возведение в степень.

3 Дистрибутивные операции: умножение относительно сложения чисел. Недистрибутивные операции: возведение в степень дистрибутивно относительно умножения справа, но не слева: $(ab)^c = a^c b^c$, $a^{bc} = a^b a^c$.

$$a \circ b = ab, \quad a \diamond b = a^b \text{ – дистрибутивно справа.}$$

$$(a \circ b) \diamond c = (a \diamond c) \circ (b \diamond c).$$

Распишем левую часть:

$$(a \circ b) \diamond c = ab \diamond c = (ab)^c.$$

И правую часть:

$$(a \diamond c) \circ (b \diamond c) = (a^c) \circ (b^c) = a^c b^c = (ab)^c.$$

4 Пересечение поглощает объединение, объединение поглощает пересечение. Сложение и умножение не поглощают друг друга.

5 Идемпотентные операции: наибольший общий делитель натуральных чисел,

$$\text{НОД}(a, a) = a,$$

объединение и пересечение множеств:

$$A \cap A = A, \quad A \cup A = A.$$

Неидемпотентные операции: сложение и умножение чисел.

4.4 Алгебры с одной операцией

К алгебрам с одной операцией относят полугруппы, моноиды и группы. В данном подразделе мы рассмотрим первые две, а третью, в силу ее важности, рассмотрим в отдельном подразделе.

Множество с одной ассоциативной операцией на нем называется *полугруппой*.

Для обозначения операции чаще других используется мультипликативная форма записи. Это означает, что операцию называют умножением и обозначают значком $\cdot$ (точка). Если не возникает разночтения, символ точки можно опускать, например, вместо $a \cdot b$ можно писать ab . Используют также аддитивную запись, когда операцию называют сложением и обозначают знаком $+$. Будем пользоваться, если особо не оговорено противное, мультипликативной записью.

Например, $\langle \mathbb{N}; + \rangle$, $\langle \mathbb{Z}; + \rangle$, $\langle \mathbb{N}; \cdot \rangle$ и $\langle \mathbb{Z}; \cdot \rangle$ – являются полугруппами. Другими словами, операция сложения и умножения ассоциативны в $\mathbb{N}$ и $\mathbb{Z}$.

Пример 4.3. Является ли полугруппой $\langle \mathbb{N}; - \rangle$?

Решение. Нет. Операция вычитания не является замкнутой.

Если операция *коммутативна*, то полугруппу называют *абелевой*.

В полугруппе все элементы «равноправны» и не имеют каких-либо отличительных свойств. В моноиде, в отличие от полугруппы, появляется нейтральный элемент со специфическими свойствами. Далее мы дадим более формальное определение моноида.

Если в полугруппе найдется элемент $e \in A$, такой, что

$$\forall a \in A, \quad a \cdot e = e \cdot a = a,$$

то e называется **нейтральным элементом**. В случае мультипликативной записи полугруппы нейтральный элемент называется **единицей** и обозначается символом 1. При аддитивной записи элемент e называют **нулем** и обозначают символом 0.

Полугруппа с единицей называется **моноидом**.

Пример 4.4. Докажите, что в моноиде единица единственна.

Решение. От противного. Допустим, что существуют две единицы $e_1 \neq e_2$, тогда

$$e_1 \cdot e_2 = e_1 \text{ и}$$

$$e_1 \cdot e_2 = e_2 \Rightarrow$$

$$e_1 = e_2,$$

что противоречит изначальному допущению.

Рассмотрим еще один пример.

Пример 4.5. Является ли моноидом коммутативная полугруппа $\langle \mathbb{Z}, \star \rangle$, где $\star$ определяется как $a \star b = \min\{a, b\}$?

Решение. Пусть некоторое $a \in \mathbb{Z}$ претендует на роль нейтрального элемента. Тогда $a + 1 \in \mathbb{Z}$, и $a \star (a + 1) = a + 1$. Это показывает, что a не является нейтральным элементом. Поскольку a это произвольный элемент $\mathbb{Z}$, мы показали, что в данной алгебраической структуре не существует нейтрального элемента.

Рассмотрим один весьма часто встречающийся моноид.

Множество S матриц размерностью $n \times n$ является моноидом $\langle S, \cdot \rangle$. Единицей в данном случае будет матрица I с единицей в качестве элементов главной диагонали и нулем в качестве прочих элементов, так, что

$$I_{ij} = \begin{cases} 1, & \text{если } i = j; \\ 0, & \text{если } i \neq j. \end{cases}$$

Например, единичная матрица размерностью 3×3 имеет вид

$$I = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

4.5 Группы

Теория групп является ярчайшим примером мощи алгебраических методов, позволяющих получить из немногих базовых понятий и аксиом множество важнейших следствий.

4.5.1 Определение группы

Группа – это моноид, в котором $\forall a \exists a^{-1}$, такой, что

$$a \circ a^{-1} = a^{-1} \circ a = e.$$

Элемент a^{-1} называется **обратным** для элемента a .

Другими словами, в группе должны выполняться следующие условия (аксиомы группы):

- 1) множество G должно быть замкнуто относительно групповой операции;
- 2) групповая операция должна быть ассоциативной;
- 3) в группе должен существовать нейтральный (единичный) элемент e , обладающий свойством

$$e \cdot a = a \cdot e = a, \quad \forall a \in G;$$

- 4) каждый элемент $a \in G$ имеет обратный a^{-1} :

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

Данные аксиомы порождают колоссальное разнообразие. Теория необозрима. Некоторые задачи принципиально не решаются (например, проблема тождества слов), доказательства некоторых теорем занимают сотни страниц, а самые простые результаты плохо укладываются в голову.

Для группы $\langle G, \circ \rangle$ – мощность носителя G называется **порядком группы** и обозначается $|G|$.

Рассмотрим следующие следствия групповых аксиом.

Пример 4.6. Докажите, что обратный элемент единственен.

Решение. Пусть $a \circ a^{-1} = a^{-1} \circ a = e$ и $a \circ b = b \circ a = e$. Тогда $a^{-1} = a^{-1} \circ e = a^{-1} \circ (a \circ b) = (a^{-1} \circ a) \circ b = e \circ b = b$.

То есть имеется противоречие, поскольку вначале мы полагали, что $a^{-1} \neq b$.

Следующий пример показывает связь между групповой операцией и процессом поиска обратного элемента в группе.

Пример 4.7. Докажите, что в группе выполняется следующее соотношение: $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Решение

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ e \circ a^{-1} = a \circ a^{-1} = e.$$

В группе разрешимы линейные уравнения, что отражено в следующем примере.

Пример 4.8. Докажите, что в группе всегда однозначно разрешимо уравнение вида $ax = b$.

Решение. «Домножим» слева данное уравнение на a^{-1} :

$$a^{-1}(ax) = a^{-1}b,$$

откуда по аксиоме ассоциативности и по определению обратного элемента получаем $x = ab^{-1}$.

4.5.2 Циклическая группа

Если групповая операция применяется два или более раз к одному и тому же элементу группы, то можно использовать степенное обозначение:

$$a \circ a = a^2.$$

Циклической называется группа, в которой каждый элемент может быть записан в виде степени некоторого фиксированного элемента, называемого *образующей группы*.

Циклическая группа обозначается как C_n , где n – порядок группы.

Каждая конечная циклическая группа имеет вид

$$G = \{a^0, a^1, a^2, \dots, a^{n-1}\},$$

где a – образующая группы; a^0 – единичный (нейтральный) элемент; n – порядок группы; a элемент, обратный к a^i , равен a^{n-i} .

Чтобы задать группу, необходимо, чтобы выполнялось равенство:

$$a^n = a^0.$$

Важнейшей циклической группой с n элементами является группа, обозначаемая как $\mathbb{Z}_n$ и задаваемая множеством

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

с операцией сложения по модулю n в качестве групповой операции. Например, в $\mathbb{Z}_6$ справедливо $3 + 4 = 1 \pmod{6}$ поскольку $3 + 4 = 7 = 6 \times 1 + 1$.

Группа $\mathbb{Z}_n$ может быть выбрана в качестве стандартного прототипа циклической группы с n элементами. Любую циклическую группу G с n элементами можно отобразить (т. е. существует изоморфизм) в $\mathbb{Z}_n$ с заменой групповой операции в G на сложение по модулю n .

Минимальное число q в равенстве $b^q = 1$ называют **порядком** или **периодом** элемента b и обозначают через $|b|$.

Пример 4.9. Доказать, что в циклической группе с n элементами выполняется равенство $(a^i)^{-1} = a^{n-i}$.

Решение

$$a^i \cdot b = a^0.$$

Для циклической группы мы имеем $a^n = a^0$, следовательно,

$$a^i \cdot b = a^n.$$

Умножим правую и левую часть на a^{-i} :

$$a^{-i} \cdot (a^i \cdot b) = a^{-i} \cdot a^n;$$

$$a^0 \cdot b = a^{n-i};$$

$$b = a^{n-i}, \text{ следовательно, } (a^i)^{-1} = a^{n-i}.$$

Рассмотрим важные примеры циклических групп.

Аддитивная группа $\langle \mathbb{Z}_q, + \rangle$ вычетов по модулю q .

Мультипликативная группа $\langle \mathbb{Z}_p, \times \rangle$ вычетов по модулю p , где p – простое число. Ее элементами являются $p - 1$ чисел $1, 2, \dots, p - 1$, а групповая операция равна остатку от деления обычного произведения ab на p , т. е.

$$a \times b = ab \pmod{p}.$$

4.5.3 Диэдральная группа

Диэдральная группа D_n ($n \geq 3$) определяется как группа *симметрий* правильного n -угольника.

Правильный n -угольник имеет $2n$ различных симметрий:

- n поворотов вокруг центра;
- n осевых отражений.

При определении диэдральной группы мы использовали термин симметрия. Но что такое симметрия?

На простом уровне ее можно описать так: **симметрия фигуры** описывается теми движениями, в результате которых она совмещается сама с собой.

Более сложное определение звучит следующим образом. Для любого подмножества S плоскости $\mathbb{R}^2$ можно определить его симметрию как сохраняющую расстояние биекцию:

$$f: \mathbb{R}^2 \rightarrow \mathbb{R}^2,$$

такую, что $f(x) \in S, \forall x \in S$. Последнее условие можно переписать так:

$$f(S) = S.$$

На языке геометрии симметрия подмножества S – это *жесткое движение* плоскости, которое оставляет S на месте, хотя может перемещать отдельные точки из S .

Обозначим через s отражение относительно оси, проходящей через вершину 1 и центр многоугольника ($s: i \mapsto (n + 2 - i) \bmod n$). При повороте

$$r: i \mapsto (i + 1) \bmod n.$$

Примеры диэдральных групп D_3 и D_4 даны на рисунке 4.2.

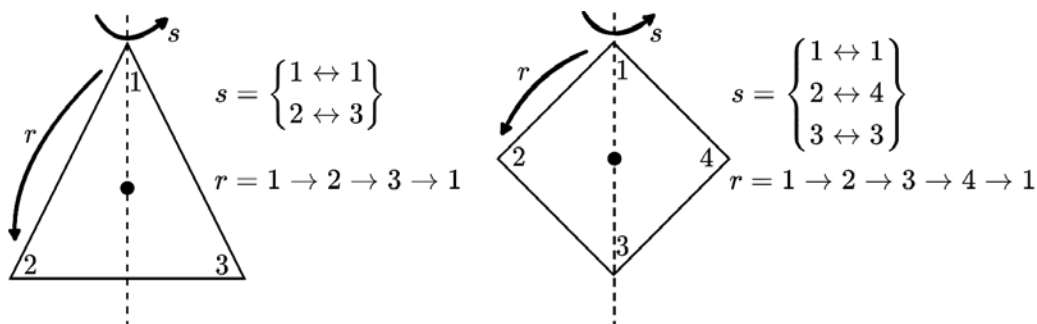


Рисунок 4.2 – Диэдральные группы D_3 и D_4

Для диэдральной группы имеют место следующие соотношения:

$$r^n = e; \quad s^2 = e; \quad srs = r^{-1}.$$

Таким образом, диэдральная группа состоит из $2n$ элементов:

$$D_n = \{e, r, \dots, r^{n-1}, s, rs, \dots, r^{n-1}s\}.$$

4.5.4 Произведение групп

По заданным двум группам G и S можно построить новую группу T , которая называется произведением групп G и S :

$$T = G \times S.$$

Элементами T являются упорядоченные пары элементов (g, s) , где $g \in G$, $s \in S$. Групповая операция определяется как

$$(g_1, s_1) \circ (g_2, s_2) = (g_1 \circ g_2, s_1 \circ s_2).$$

В этом выражении обозначение операции $\circ$ используется в трех разных смыслах. Рассмотрим группу $\mathbb{Z}_2 \times \mathbb{Z}_3$, ее множество имеет вид

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0, 0), (0, 1), (0, 2), (1, 0), (1, 1), (1, 2)\}.$$

Типичным элементом таблицы «сложения» в $\mathbb{Z}_2 \times \mathbb{Z}_3$ является

$$(1, 2) + (0, 2) = (1, 1).$$

4.5.5 Подгруппы

Если $\langle G, \circ \rangle$ – группа, то подмножество H из G является *подгруппой*, если оно образует группу относительно операции $\circ$. Например, в группе $\langle \mathbb{Z}, + \rangle$ множество четных чисел образует подгруппу.

Если элементы h и k лежат в подгруппе H , то должны выполняться такие условия:

$$1) \quad h \circ k \in H;$$

$$2) \quad h^{-1} \in H,$$

а отсюда следует, что

$$3) \quad I = h \circ h^{-1} \in H.$$

Верно и обратное, что если выполняются условия 1, 2, то можно утверждать, что H подгруппа, поскольку закон ассоциативности обязательно выполняется в H , если он выполняется в G .

Один из способов построения подгруппы H конечной группы G состоит в том, чтобы, выбрав некоторый элемент h из G , формировать элементы множества H в виде последовательных степеней этого элемента: $h, h^2, h^3, \dots$. Так как группа G конечна, то элемент последовательности обязательно начнет повторяться. Первым должен повториться сам элемент h , а непосредственно предшествующий ему элемент является нейтральным (единичным) элементом группы.

Пример 4.10. Найти подгруппы группы $\langle \mathbb{Z}_6, + \rangle$.

Решение

1) Возьмем $h = 2$ и будем искать степени этого элемента, пока вновь не получим h :

$$h^2 = 2 + 2 \bmod 6 = 4;$$

$$h^3 = h^2 + h = 4 + 2 \bmod 6 = 0 \quad (= e);$$

$$h^4 = h^3 + h = 0 + 2 \bmod 6 = 2 \quad (= h);$$

2) возьмем элемент $h = 3$ и найдем все его степени:

$$h^2 = 3 + 3 \bmod 6 = 0 \quad (= e);$$

$$h^3 = h^2 + h = 0 + 3 \bmod 6 = 3 \quad (= h).$$

Легко заметить, что порядок подгруппы в нашем примере делит порядок группы. Добавим сюда тривиальные подгруппы $\{0\}$, которая имеет порядок 1, и $\{\mathbb{Z}_6\}$, которая имеет порядок 6. Получается, что группа $\mathbb{Z}_6$ порядка 6 имеет подгруппы порядков 1, 2, 3 и 6. Не требуется особых способностей, чтобы заметить, что все эти числа *делят* 6.

Так может *порядок подгруппы всегда делит порядок группы*? Да! Соответствующая теорема была доказана Лагранжем *раньше*, чем возникло абстрактное понятие группы.

4.5.6 Группа подстановок (симметрическая группа)

В этом пункте рассматривается одна из важнейших групп, называемая группой *подстановок* или *симметрической* группой.

Группы подстановок играют ключевую роль при изучении конечных групп, поскольку *других конечных групп не бывает*. Точнее говоря, конечные группы с точностью до изоморфизма исчерпываются подгруппами группы подстановок (теорема Кэли).

Множество всех подстановок вида

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \quad e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

с операцией композиции называют *симметрической группой* порядка n и обозначают S_n . $|S_n| = n!$.

Всякая конечная группа G порядка n изоморфна подгруппе симметрической группы S_n .

Пример 4.11. Найти порядок элемента h в симметрической группе S_5 :

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}.$$

Решение

$$h^2 = hh = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix};$$

$$h^3 = h^2h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix};$$

$$h^4 = h^3h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix};$$

$$h^5 = h^4h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix};$$

$$h^6 = h^5h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 3 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix} = h^0.$$

Таким образом, степени перестановки h , а именно: $h^0 = e$, h^1 , h^2 , h^3 , h^4 , h^5 образуют циклическую группу. Можно проверить, что эта группа коммутативна.

4.5.7 Перестановочные матрицы

Если $f: 1 \dots n \rightarrow 1 \dots n$ – подстановка, то матрицей подстановки называется квадратная булева матрица $P_f[i, j] := (f(i) == j)$.

В каждой строке и в каждом столбце одна единица, остальные элементы – нули, например:

$$r = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad P_r = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

4.6 Гомоморфизм

Пусть $(S, \cdot)$ и $(T, \circ)$ – полугруппы и $f: S \rightarrow T$ – такая функция, что

$$f(s \cdot s') = f(s) \circ f(s').$$

Функция f называется **гомоморфизмом** из S в T .

Пусть $S = \{0, 1, 2, 3\}$ с операцией сложения по модулю 4, а $T = \{0, 1\}$ с операцией сложения по модулю 2. Тогда $f(x) = x \bmod 2$ определяет **гомоморфизм**. Проверим:

$$(3 + 3) \bmod 4 = 2, \text{ и } f(2) = 0 \text{ (левая часть условия);}$$

$$(f(3) + f(3)) \bmod 2 = (1 + 1) \bmod 2 = 0 \text{ (правая часть условия).}$$

Понятие гомоморфизма является одним из ключевых понятий алгебры. Каждая алгебраическая структура определенным образом выделяет класс «разумных» отображений между объектами с данной структурой, согласованных с операциями этой структуры. Вообще говоря, любая алгебра задается с точностью до изоморфизма.

Биективный гомоморфизм называется **изоморфизмом**.

Таким образом, под **изоморфизмом** понимается взаимно однозначное отображение одной группы в другую, сохраняющее операцию, т. е. отображение, при котором различные элементы имеют различные образы и образ произведения элементов равен произведению образов этих элементов.

Понятие изоморфизма является одним из центральных, оправдывающих применимость алгебраических методов в различных областях. Изоморфные группы имеют одинаковую абстрактную структуру и различаются лишь элементами.

Введем важное понятие коммутативной диаграммы. Пусть $\mathcal{A} = \langle A; \varphi \rangle$, $\mathcal{B} = \langle B; \psi \rangle$, и гомоморфизм $f: A \rightarrow B$. Действие функций φ, ψ, f можно изобразить с помощью диаграммы, представленной на рисунке 4.3.

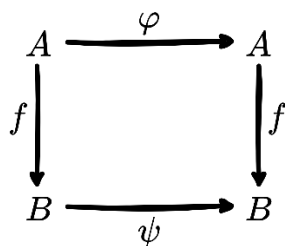


Рисунок 4.3 – Коммутативная диаграмма

Если взять конкретное значение $a \in A$ и двигаться по двум различным путям на диаграмме, то получится один и тот же элемент $b \in B$, т. к. $f(\varphi(a)) = \psi(f(a))$. В таком случае диаграмма называется коммутативной, потому что условие гомоморфизма можно переписать так:

$$f \circ \varphi = \psi \circ f,$$

где $\circ$ – суперпозиция функций.

Пусть $\mathcal{A} = \langle \mathbb{R}_+; \cdot \rangle \sim \mathcal{B} = \langle \mathbb{R}; + \rangle$, $f: \mathcal{A} \rightarrow \mathcal{B}$ и $f(x) = \ln x$, тогда если $p, q \in A$ и $\varphi(p, q) = pq = z \in A$, то $f(z) = \ln z \in B$ (проход по одной ветке). Также верно, что $f(p) = \ln p$, $f(q) = \ln q$, и $\psi(\ln p, \ln q) = \ln p + \ln q$ (проход по второй ветке). Следовательно, $\ln pq = \ln p + \ln q$.

4.7 Общее понятие о кольцах

Мы переходим к изучению алгебр с двумя операциями.

Кольцом называется множество R с двумя бинарными операциями: сложением (+) и умножением ($\cdot$) при следующих условиях:

- 1) $\langle R, + \rangle$ – абелева группа;
- 2) $\langle R, \cdot \rangle$ – полугруппа (т. е. произведение $ab \in R \forall a, b \in R$. «Замкнутость»; умножение ассоциативно: $a(bc) = (ab)c$;

3) выполняется дистрибутивный закон, определяющий взаимодействие сложения и умножения:

$$\begin{aligned} p \cdot (q + r) &= p \cdot q + p \cdot r; \\ (q + r) \cdot p &= q \cdot p + r \cdot p. \end{aligned}$$

Сложение в кольце всегда коммутативно, а умножение – нет.

Кольцо называется **коммутативным**, если $ab = ba$ для всех $a, b \in R$.

Кольцо, обладающее единицей относительно умножения, называется **кольцом с единицей**. По-другому можно сказать, что если структура $\langle R, \cdot \rangle$ – моноид, то $\langle R, +, \cdot \rangle$ – кольцо с единицей.

Например, машинная арифметика целых чисел $\langle \mathbb{Z}_{2^{15}}; +, \times \rangle$ – коммутативное кольцо с единицей.

Примерами колец служат различные числовые системы: действительная прямая $\mathbb{R}$, комплексная плоскость $\mathbb{C}$, множество рациональных чисел $\mathbb{Q}$, множество целых чисел $\mathbb{Z}$.

Менее привычные примеры:

– кольцо многочленов $\mathbb{R}[x]$, элементами которого являются формальные выражения:

$$P_n(x) = p_n x^n + \dots + p_1 x + p_0,$$

где $p_k \in \mathbb{R}$. Природа элементов x несущественна. Операции определяются, как для обычных многочленов, что порождает коммутативное кольцо с единицей;

- кольцо квадратных матриц $M_n(\mathbb{R})$;
- $\mathbb{Z}_q$ с операцией сложения и умножения образует кольцо;
- числа вида $a + b\sqrt{2}$ с рациональными или целыми коэффициентами образуют кольцо.

Относительно операции умножения обратные к данному элементу не обязательно существуют, но в кольце с единицей обратные могут существовать. Это означает, что для данного элемента a может существовать элемент b , такой что $ab = 1$. Если это так, то b называется **правым обратным** к a . Аналогично, если существует элемент c , такой, что $ca = 1$, то c называется **левым обратным** к a .

В кольце с единицей:

1) единица единственна;

2) если элемент a имеет и правый обратный b , и левый обратный c , то $b = c$.

В этом случае элемент a называется обратимым, причем обратный элемент единственен и обозначается через a^{-1} ;

3) $(a^{-1})^{-1} = a$.

Рассмотрим в качестве примера кольцо квадратных матриц 2×2 .

Пример 4.12. Пусть дана матрица $A = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}$. Найти правый обратный элемент. Проверить, существует ли обратный левый элемент.

Решение. Задача $A \times A_r^{-1} = I$ имеет решение, т. е. надо просто вычислить обратную матрицу.

Используя метод Крамера, легко найти

$$A_r^{-1} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}.$$

Можно ли найти левый обратный элемент? Ведь произведение матриц не коммутативно. Исходя из приведенной выше теоремы, если левый обратный существует, то он должен быть равен правому. Проверяем:

$$A_r^{-1} \times A = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \times \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I.$$

Следовательно, обратный левый элемент существует.

Аксиома дистрибутивности имеет своим следствием общий закон дистрибутивности:

$$(a_1 + \dots + a_n)(b_1 + \dots + b_m) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j.$$

4.8 Кольцо целых чисел

Целые числа образуют обманчиво простое математическое множество. Ничего, кажется, не может быть более регулярного и равномерного, чем целые числа, но, присмотревшись пристальнее, можно увидеть сложные внутренние связи и модели этого множества.

В кольце целых чисел вычитание возможно всегда, а вот деление – не всегда. Ограниченность деления является одной из причин, делающих кольцо целых чисел столь интересной и богатой структурой.

Говорят, что r делит s (или что r является делителем s), если $s = ra$, где $a \in \mathbb{Z}$. Этот факт записывается символом $r|s$, который читается « r делит s ».

Положительное целое число $p > 1$, которое делится только на себя и на 1, называется **простым**.

Введем важное понятие канонического представления числа.

Любое число N может быть представлено в виде произведения степеней простых чисел, которое называется **каноническим представлением числа**. Такое представление единственно (с точностью до перестановки сомножителей).

Для представления числа N в канонической форме можно использовать следующий алгоритм. Число N делим на наименьшее простое число 2 до тех пор, пока оно делится нацело, затем на 3, на 5 и т. д.

Так, например, число 600 в каноническом виде будет иметь следующее представление: $600 = 2^3 3^1 5^2$.

4.8.1 НОК и НОД чисел

Наибольший общий делитель двух целых чисел r и s обозначается НОД (r, s) и определяется как наибольшее положительное число, которое делит оба из них. То есть $d = (r, s) \Rightarrow d|r$ и $d|s$.

Наименьшее общее кратное двух положительных чисел r и s обозначается НОК (r, s) и определяется как наименьшее положительное число, которое делится на оба из них.

Как находить НОД мы рассмотрим чуть позже, а вот для НОК существует следующее выражение:

$$\text{НОК}(a, b) = \frac{ab}{\text{НОД}(a, b)}.$$

Два числа называются **взаимно простыми**, если их НОД равен 1.

Можно изобразить расположение НОД и НОК чисел a и b на числовой прямой, как показано на рисунке 4.4.

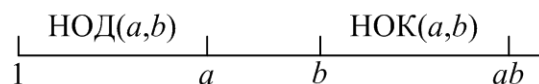


Рисунок 4.4 – Схема расположения НОК и НОД на числовой оси

В кольце целых чисел имеется *слабая форма деления*, известная под названием **деление с остатком**. Любое целое число s единственным образом может быть представлено в виде

$$s = Qt + r,$$

где $Q > 1$ – делитель; t – частное; r – остаток ($0 \leq r < Q$).

Наименьший положительный остаток от деления числа s на число Q называют **вычетом** s по модулю Q .

В практических задачах чаще интересует остаток, чем частное.

4.8.2 Сравнения

Если s и c при делении на Q дают один и тот же остаток, то это записывается в виде

$$s \equiv c \pmod{Q}.$$

Выражение данного вида называется **сравнением** и читается так: « s сравнимо с c по модулю Q ».

Сравнению $a \equiv 0 \pmod{Q}$ удовлетворяют все числа a , кратные Q .

От сравнения можно перейти к равенству:

$$s \equiv c \pmod{Q}$$

справедливо, если

$$s = c + Qt,$$

где t – некоторое целое число. Такая связь позволяет распространить понятие сравнения не только на положительные, но и на отрицательные числа. Например, $12 \equiv 7 \equiv 2 \equiv -3 \equiv -8 \pmod{5}$.

Сравнение не надо путать с операцией нахождения остатка от деления, которая записывается как

$$r = s \bmod Q,$$

читается так: « s равно остатку от деления s на Q ». Еще пишут так:

$$r = \langle c \rangle_Q.$$

Вычисление остатка от сложного выражения облегчается следующей теоремой.

Для фиксированного модуля Q :

$$1) \langle a + b \rangle_Q = \langle \langle a \rangle_Q + \langle b \rangle_Q \rangle_Q;$$

$$2) \langle a \cdot b \rangle_Q = \langle \langle a \rangle_Q \cdot \langle b \rangle_Q \rangle_Q.$$

4.8.3 Алгоритм Евклида (НОД)

Древнейшей задачей геометрии было нахождение «общей меры» длины отрезка. Отрезок измерялся при помощи другого (меньшего) отрезка. Весьма просто измерить отрезок, если второй отрезок укладывается в нем целое число раз. Если же получается остаток, то проверяют сначала, не составляет ли этот остаток $1/2$, $1/3$, $2/3$ или вообще какую-либо дробную часть меньшего отрезка, служащего здесь мерой длины. Если такую дробь удастся найти, то мы получаем, что в отрезке целое

число раз укладывается доля меньшего отрезка. Эта доля и представляет собой их «общую меру».

Настоящем потрясением для философов древности явилось то, что существуют отрезки «несоизмеримые». Например, **сторона и диагональ квадрата несоизмеримы**. В книге «Законы» Платон рассказывает, какое сильное впечатление произвело на него это открытие, когда тот уже в зрелые годы познакомился с ним.

Определение (алгоритм Евклида). Пусть $a, b \in \mathbb{Z}^+$ с $a \geq b$. Пусть $r_0 = a$, $r_1 = b$. Применим алгоритм деления к r_0 и r_1 , чтобы найти такие $q_1, r_2 \in \mathbb{Z}^+$, что $r_0 = r_1 q_1 + r_2$, где $0 \leq r_2 < r_1$. Если мы повторим данный процесс, то получим $r_j = r_{j+1} q_{j+1} + r_{j+2}$, где $0 \leq r_{j+2} < r_{j+1}$ для $j = 0, 1, \dots, n-1$, так что $r_{n+1} = 0$. Тогда $\text{НОД}(a, b) = r_n$.

Пример 4.13. Используя алгоритм Евклида, найти $\text{НОД}(305, 1040)$.

Решение

$$1040 = 305 \cdot 3 + 125;$$

$$305 = 125 \cdot 2 + 55;$$

$$125 = 55 \cdot 2 + 15;$$

$$55 = 15 \cdot 3 + 10;$$

$$15 = 10 \cdot 1 + 5;$$

$$10 = 5 \cdot 2 + 0.$$

Таким образом, $\text{НОД}(305, 1040) = 5$.

Матричные обозначения позволяют кратко записать шаги алгоритма Евклида в виде

$$\begin{bmatrix} r_{j+1} \\ r_{j+2} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_{j+1} \end{bmatrix} \begin{bmatrix} r_j \\ r_{j+1} \end{bmatrix}.$$

Теорема (алгоритм Евклида). Для двух заданных положительных чисел a и b , где $a > b$. Пусть $r_0 = a$ и $r_1 = b$. Решение рекуррентных уравнений

$$q_{j+1} = \left\lfloor \frac{r_j}{r_{j+1}} \right\rfloor,$$

$$\begin{bmatrix} r_{j+1} \\ r_{j+2} \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_{j+1} \end{bmatrix} \begin{bmatrix} r_j \\ r_{j+1} \end{bmatrix}.$$

при $j = 0, \dots, n-1$ дается величиной

$$r_n = \text{НОД}(a, b),$$

где n равно наименьшему целому числу, для которого $r_{n+1} = 0$.

Пример 4.14. Найти НОД(125, 17).

Решение. Вычислим НОД (125, 17) по алгоритму Евклида:

$$r_0 = 125, r_1 = 17.$$

$$1) q_1 = \left[\frac{r_0}{r_1} \right] = \left[\frac{125}{17} \right] = 7 \Rightarrow r_0 = q_1 r_1 + r_2 = 7 \cdot 17 + 6.$$

$$\begin{bmatrix} r_1 \\ r_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -q_1 \end{bmatrix} \begin{bmatrix} r_0 \\ r_1 \end{bmatrix}.$$

$$\begin{bmatrix} 17 \\ 6 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -7 \end{bmatrix} \begin{bmatrix} 125 \\ 17 \end{bmatrix};$$

$$2) q_2 = \left[\frac{r_1}{r_2} \right] = \left[\frac{17}{6} \right] = 2 \Rightarrow r_1 = q_2 r_2 + r_3 = 2 \cdot 6 + 5;$$

$$3) q_3 = \left[\frac{r_2}{r_3} \right] = \left[\frac{6}{5} \right] = 1 \Rightarrow r_2 = q_3 r_3 + r_4 = 1 \cdot 5 + 1;$$

$$4) q_4 = \left[\frac{r_3}{r_4} \right] = \left[\frac{1}{1} \right] = 1 \Rightarrow r_3 = q_4 r_4 + r_5 = 1 \cdot 1 + 0;$$

$$\text{НОД}(125, 17) = 1.$$

Запишем теперь все операции в матричной форме:

$$\begin{bmatrix} r_4 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -7 \end{bmatrix} \begin{bmatrix} 125 \\ 17 \end{bmatrix};$$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 1 & -7 \\ -2 & 15 \end{bmatrix} \begin{bmatrix} 125 \\ 17 \end{bmatrix};$$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 3 & -22 \\ -5 & 37 \end{bmatrix} \begin{bmatrix} 125 \\ 17 \end{bmatrix}.$$

Если записать все шаги алгоритма один за другим, то мы получим

$$\begin{bmatrix} r_n \\ 0 \end{bmatrix} = \left\{ \prod_{j=n}^1 \begin{bmatrix} 0 & 1 \\ 1 & -q_j \end{bmatrix} \right\} \begin{bmatrix} a \\ b \end{bmatrix} = A \begin{bmatrix} a \\ b \end{bmatrix}.$$

Легко проверить, что

$$\begin{bmatrix} 0 & 1 \\ 1 & -q_j \end{bmatrix}^{-1} = \begin{bmatrix} q_j & 1 \\ 1 & 0 \end{bmatrix},$$

поэтому

$$\begin{bmatrix} s \\ t \end{bmatrix} = \left\{ \prod_{r=1}^n \begin{bmatrix} q_j & 1 \\ 1 & 0 \end{bmatrix} \right\} \begin{bmatrix} r_n \\ 0 \end{bmatrix}.$$

Важным следствием, которое является интуитивно непредсказуемым результатом теории чисел, является утверждение, что наибольший общий делитель двух целых чисел равен их линейной комбинации!

Для любых целых чисел a и b найдутся такие целые числа x и y , что

$$\text{НОД}(a, b) = ax + by,$$

причем $x = A_{11}$ и $y = A_{12}$.

4.8.4 Делитель нуля и взаимно обратные элементы в кольце $\mathbb{Z}_n$

Если $ab = 0 \bmod n$, в то время как $a \neq 0$ и $b \neq 0$, то говорят, что a, b **делители нуля**.

Если $cd = 1 \bmod n$, то говорят, что c и d **взаимно обратные**, и обозначают $d = c^{-1} \bmod n$ или $c = d^{-1} \bmod n$.

Если для какого-нибудь элемента $a \in \mathbb{Z}_n$ существует $a^{-1} \in \mathbb{Z}_n$, то говорят, что a обратим в $\mathbb{Z}_n$.

Элемент $0 \neq a \in \mathbb{Z}_n$ обратим тогда и только тогда, когда $\text{НОД}(a, n) = 1$.

Для поиска обратного элемента в кольце $\mathbb{Z}_n$ необходимо использовать алгоритм Евклида.

Пример 4.15. Найти $17^{-1} \pmod{125}$.

Решение. Необходимо найти такой элемент a , что

$$17 \cdot a = 1 \bmod 125$$

или

$$17b + 125a = 1.$$

Вначале вычислим $\text{НОД}(125, 17)$ по алгоритму Евклида:

- 1) $Q^{(1)} = \left\lfloor \frac{125}{17} \right\rfloor = 7 \Rightarrow s = Q^{(1)}t + t^{(1)} = 7 \cdot 17 + 6;$
- 2) $Q^{(2)} = \left\lfloor \frac{t}{t^{(1)}} \right\rfloor = \left\lfloor \frac{17}{6} \right\rfloor = 2 \Rightarrow t^{(0)} = Q^{(2)}t^{(1)} + t^{(2)} = 2 \cdot 6 + 5;$
- 3) $Q^{(3)} = \left\lfloor \frac{t^{(1)}}{t^{(2)}} \right\rfloor = \left\lfloor \frac{6}{5} \right\rfloor = 1 \Rightarrow t^{(1)} = Q^{(3)}t^{(2)} + t^{(3)} = 1 \cdot 5 + 1;$
- 4) $Q^{(4)} = \left\lfloor \frac{t^{(2)}}{t^{(3)}} \right\rfloor = \left\lfloor \frac{1}{1} \right\rfloor = 1 \Rightarrow t^{(2)} = Q^{(4)}t^{(3)} + t^{(4)} = 1 \cdot 1 + 0.$

Запишем теперь все операции в матричной форме:

$$\begin{aligned} \begin{bmatrix} s^{(4)} \\ 0 \end{bmatrix} &= \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & -7 \end{bmatrix} \begin{bmatrix} 125 \\ 17 \end{bmatrix}; \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix} &= \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix} \begin{bmatrix} 1 & -7 \\ -2 & 15 \end{bmatrix} \begin{bmatrix} 125 \\ 17 \end{bmatrix}; \\ \begin{bmatrix} 1 \\ 0 \end{bmatrix} &= \begin{bmatrix} 3 & -22 \\ -5 & 37 \end{bmatrix} \begin{bmatrix} 125 \\ 17 \end{bmatrix}. \end{aligned}$$

Значит, $1 = 3 \cdot 125 - 22 \cdot 17$ и, следовательно,
 $17^{-1} = -22 \bmod 125$ или $17^{-1} = 103 \bmod 125$.

4.9 Китайская теорема об остатках (КТО)

Для рассмотрения китайской теоремы об остатках будем использовать пример 4.16.

Пример 4.16. Четыре мальчика имеют следующие размеры ступни: Джим – 7 дюймов, Джон – 8 дюймов, Джо – 9 дюймов, Билл – 11 дюймов. Каждый мальчик попытался определить размеры некоторой комнаты с помощью своей ступни. Однако при измерениях у Джима осталось 2 дюйма, у Джона – 5, у Джо – 5 и, наконец, у Билла – 6 лишних дюймов. К сожалению, ни один из мальчиков не запомнил, сколько его ступней уложилось в комнате. Однако Билл заявляет, что он может восстановить результат измерений по величине остатков. Какова длина комнаты?

На математическом языке эта задача формулируется так:

$$\begin{aligned}\langle x \rangle_7 &= 2; \\ \langle x \rangle_8 &= 5; \\ \langle x \rangle_9 &= 5; \\ \langle x \rangle_{11} &= 6.\end{aligned}$$

Система

$$\begin{cases} \langle x \rangle_{m_1} = r_1; \\ \langle x \rangle_{m_2} = r_2; \\ \dots \\ \langle x \rangle_{m_K} = r_K \end{cases}$$

обладает единственным решением в кольце вычетов по модулю $M = \prod m_i$.

Доказательство

Сначала запишем величины:

$$M_1 = \frac{M}{m_1}, \quad M_2 = \frac{M}{m_2}, \quad \dots, \quad M_K = \frac{M}{m_K}.$$

Каждое M_i является числом взаимно простым с соответствующим m_i :

$$\text{НОД}(M_i, m_i) = 1.$$

Поэтому можно найти числа N_i , такие, что

$$N_i M_i = 1 \bmod m_i,$$

или (это выражение можно записать иначе)

$$N_i = M_i^{-1} \bmod m_i.$$

Мы утверждаем, что число

$$x = r_1 M_1 N_1 + r_2 M_2 N_2 + \dots + r_K M_K N_K$$

является решением заданной системы уравнений. Найдем вычет по модулю m_1 .

Так как каждое число $M_2, M_3, \dots, M_K$ делится на m_1 , то

$$\langle x \rangle_{m_1} = \langle r_1 M_1 N_1 \rangle_{m_1},$$

но т. к. $\langle M_1 N_1 \rangle_{m_1} = 1$, то имеем

$$\langle x \rangle_{m_1} = r_1.$$

Аналогично

$$\langle x \rangle_{m_i} = r_i.$$

Решение примера 4.16. В нашей задаче $m_1 = 7$, $m_2 = 8$, $m_3 = 9$, $m_4 = 11$. Таким образом:

1) найдем модуль $M = m_1 m_2 m_3 m_4 = 7 \cdot 8 \cdot 9 \cdot 11 = 5544$;

2) выпишем величины:

$$M_1 = \frac{M}{m_1} = 792, M_2 = \frac{M}{m_2} = 693, M_3 = \frac{M}{m_3} = 616, M_4 = \frac{M}{m_4} = 504;$$

3) найдем величины $N_i, i = 1, 2, 3, 4$:

$$N_1 M_1 = \langle 1 \rangle_{m_1} \Rightarrow N_1 \cdot 792 = \langle 1 \rangle_7;$$

$$\langle N_1 \rangle_7 \langle 792 \rangle_7 = \langle 1 \rangle_7;$$

$$\langle N_1 \rangle_7 \cdot 1 = \langle 1 \rangle_7 \Rightarrow N_1 = 1.$$

Аналогично $N_2 = 5, N_3 = 7, N_4 = 5$;

4) формирование результата:

$$x = \sum_{i=1}^4 r_i M_i N_i \bmod M = \langle 2 \cdot 792 \cdot 1 + 5 \cdot 693 \cdot 5 + 5 \cdot 616 \cdot 7 + 6 \cdot 504 \cdot 5 \rangle_{5544} = 142.$$

Китайская теорема об остатках устанавливает взаимно однозначное соответствие между целым числом x и вектором вычетов $(r_1, r_2, \dots, r_K)$ по взаимно простым модулям m_i при условии $x < M$.

4.10 Кольцо многочленов

Многочленом над полем $\mathbb{F}$ называется математическое выражение

$$f(x) = f_n x^n + f_{n-1} x^{n-1} + \dots + f_1 x + f_0,$$

где символ x называется **неопределенной переменной** (его природа несущественна), а $f_i \in \mathbb{F}$. **Степень** многочлена обозначается $\deg f(x)$ и определяется как индекс старшего ненулевого коэффициента. Если старший коэффициент $f_n = 1$, то многочлен называется **приведенным**.

Совокупность многочленов $f(x)$ с обычными операциями сложения и умножения образует **кольцо многочленов**, обозначаемое $\mathbb{F}[x]$.

$$f(x) + g(x) = \sum_i (f_i + g_i)x^i;$$

$$f(x)g(x) = \sum_i \left(\sum_{j=0}^i f_j g_{i-j} \right) x^i.$$

В кольце деление многочленов возможно не всегда (вычитание – всегда). Запись $r(x)|s(x)$ означает, что $s(x)$ делится на $r(x)$, или что $r(x)$ делит $s(x)$, или что $r(x)$ является делителем $s(x)$. Это равносильно тому, что $\exists a(x)$ такой, что $r(x)a(x) = s(x)$. Ненулевой многочлен $p(x)$, делящийся только на себя и на константу, называется **неприводимым многочленом**.

Чтобы выяснить, является ли многочлен простым, надо знать поле, над которым он рассматривается. Многочлен $x^4 - 2$ является простым над полем $\mathbb{Q}$, но не над полем $\mathbb{R}$, где он имеет разложение:

$$x^4 - 2 = (x^2 - \sqrt{2})(x^2 + \sqrt{2}).$$

Над полем комплексных чисел каждый из последних многочленов не является простым.

Для каждого многочлена $s(x)$ и ненулевого $d(x)$ существует единственная пара $Q(x)$ (частное) и $r(x)$ (остаток), таких, что

$$s(x) = Q(x)d(x) + r(x).$$

Чаще всего интересен остаток, который записывается в виде

$$r(x) = s(x) \bmod d(x)$$

или

$$r(x) = \langle s(x) \rangle_{d(x)}.$$

Чтобы найти $\langle s(x) \rangle_{d(x)}$, казалось бы, надо выполнить деление. Однако имеются несколько приемов, позволяющих сократить и упростить необходимую для этого работу. Прежде всего заметим, что

$$\langle s(x) \rangle_{d(x)} = \langle s(x) + a(x)d(x) \rangle_{d(x)}.$$

Не изменяя остатка, к $s(x)$ можно прибавить любое значение, кратное многочлену $d(x)$. Следовательно, не изменяя остатка, можно исключить старший коэффициент многочлена $s(x)$, прибавляя соответствующее кратное многочлена $d(x)$. Используем этот метод при приведении многочлена $s(x)$ по модулю приведенного многочлена:

$$d(x) = x^n + \sum_{i=0}^{n-1} d_i x^i.$$

Для упрощения можно член x^n заменить многочленом $-\sum_{i=0}^{n-1} d_i x^i$ всюду, где это удобно. Такой прием упрощает вычисление остатка путем деления многочленов «уголком».

Пример 4.17. Разделить $s(x) = x^3 + 2x + 1$ на $d(x) = x^3 - x^2 - 1$.

Решение

$$\langle s(x) \rangle_{d(x)} = \langle s(x) + a(x)d(x) \rangle_{d(x)}.$$

В нашем случае положим $a(x) = -1$.

$$\begin{aligned} \langle s(x) \rangle_{d(x)} &= \langle s(x) + a(x)d(x) \rangle_{d(x)} = \\ &= \langle x^3 + 2x + 1 - 1(x^3 - x^2 - 1) \rangle_{x^3 - x^2 - 1} = x^2 + 2x + 1. \end{aligned}$$

Другой способ упрощения задачи вычисления остатка от деления дается следующей теоремой.

Если многочлен $d(x) = g(x)h(x)$ для некоторого $h(x)$, то

$$\langle s(x) \rangle_{g(x)} = \langle \langle s(x) \rangle_{d(x)} \rangle_{g(x)}$$

для любого $s(x)$.

Пример 4.18. Разделить многочлен $s(x) = x^7 + x + 1$ на многочлен $d(x) = x^4 + x^3 + x^2 + x + 1$.

Решение

Обычное деление «уголком» было бы утомительным, но если заметить, что $(x - 1)(x^4 + x^3 + x^2 + x + 1) = x^5 - 1$, то можно вначале разделить на $x^5 - 1$, а затем на $d(x)$. Тогда

$$\langle x^7 + x + 1 \rangle_{x^5 - 1} = x^2 + x + 1,$$

и теперь деление на $x^4 + x^3 + x^2 + x + 1$ тривиально, так что

$$\langle x^2 + x + 1 \rangle_{x^4 + x^3 + x^2 + x + 1} = x^2 + x + 1.$$

Другие удобные правила для вычисления остатка даются следующей теоремой.

$$1) \langle a(x) + b(x) \rangle_{d(x)} = \langle a(x) \rangle_{d(x)} + \langle b(x) \rangle_{d(x)};$$

$$2) \langle a(x) \cdot b(x) \rangle_{d(x)} = \langle \langle a(x) \rangle_{d(x)} \cdot \langle b(x) \rangle_{d(x)} \rangle_{d(x)}.$$

4.11 Поля

Поле $\mathbb{P}$ называется множество с двумя бинарными операциями: сложением и умножением при условии:

- 1) относительно сложения поле $\mathbb{P}$ является абелевой группой;
- 2) поле замкнуто относительно умножения, и множество ненулевых элементов образуют абелеву группу по умножению (мультипликативную группу);
- 3) выполняется дистрибутивный закон для любых $p, q, r \in \mathbb{P}$:

$$p \cdot (q + r) = p \cdot q + p \cdot r.$$

Единичный элемент относительно сложения принято называть **нулем** (0), аддитивный обратный элемент к элементу a обозначают $-a$.

Единичный элемент относительно умножения называют **единицей** (1), мультипликативный обратный к элементу a обозначают a^{-1} .

Под вычитанием ($a - b$) понимается $a + (-b)$, под делением (a / b) понимается $b^{-1}a$.

Структура поля гарантирует разрешимость линейных уравнений, что обычно требуется в приложениях, и выделяет поля в особо благоприятные объекты изучения.

Широко известны следующие примеры полей: $\mathbb{R}$ – множество вещественных чисел, $\mathbb{C}$ – множество комплексных чисел, $\mathbb{Q}$ – множество рациональных чисел.

В качестве менее известного поля с бесконечным числом элементов приведем поле комплексных рациональных чисел $\mathbb{Q}(j)$:

$$\mathbb{Q}(j) = \{a + jb\}, \quad a, b \in \mathbb{Q}.$$

Пусть $\mathbb{F}$ – поле. Подмножество $\mathbb{E}$ в $\mathbb{F}$ называется **подполем**, если оно является полем относительно наследуемых операций сложения и умножения; поле $\mathbb{F}$ в этом случае называется **расширением** подполя $\mathbb{E}$. Для обозначения подполей (или расширений поля) используют следующее обозначение:

$$\mathbb{E} \subset \mathbb{F},$$

читается как « $\mathbb{E}$ является подполем $\mathbb{F}$ » или « $\mathbb{F}$ является расширением поля $\mathbb{E}$ ».

Например, $\mathbb{Q} \subset \mathbb{Q}(j)$.

Известные нам поля натуральных, целых, рациональных, действительных и комплексных чисел можно записать в виде следующей **башни полей**:

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

4.12 Поля Галуа

Помимо рассмотренных ранее бесконечных полей существуют поля с конечным числом элементов.

Поле с q элементами, если оно существует, называется **конечным полем**, или **полем Галуа**, и обозначается $GF(q)$.

Что представляет собой наименьшее поле? Оно обязано содержать нулевой элемент и единичный элемент. Этого достаточно для задания поля, если сложение и умножение определить таблицами (рисунок 4.4).

+		0	1
	0	0	1
	1	1	0

a

×		0	1
	0	0	0
	1	0	1

б

Рисунок 4.4 – Таблица сложения (*a*) и умножения (*б*) поля Галуа $GF(2)$

Это поле известно как $GF(2)$. Других полей с двумя элементами не существует (за исключением, конечно, полей, изоморфных $GF(2)$).

Рассмотрим еще один пример поля $GF(3) = \{0, 1, 2\}$ с операциями сложения и умножения (рисунок 4.5).

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

a

×	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

б

Рисунок 4.5 – Таблица сложения (*a*) и умножения (*б*) поля Галуа $GF(3)$

В данном случае легко заметить, что сложение и умножение выполняются по модулю 3.

Рассмотрим также пример поля $GF(4) = \{0, 1, 2, 3\}$ с операциями сложения и умножения (рисунок 4.6).

Заметьте, что в $GF(4)$ умножение не есть умножение по модулю 4, а сложение не есть сложение по модулю 4.

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

a

×	0	1	2	3
0	0	0	0	0
1	1	1	2	3
2	0	2	3	1
3	0	3	1	2

б

Рисунок 4.6 – Таблица сложения (*a*) и умножения (*б*) поля Галуа $GF(4)$

Каждое конечное поле, состоящее из q элементов, изоморфно каждому другому полю из q элементов.

В любом поле выполняются алгебраические тождества, известные из обычной алгебры.

Пример 4.19. Проверить, что в поле $GF(4)$ выполняется алгебраическое соотношение $a^2 - b^2 = (a - b)(a + b)$.

Решение. Пусть $a = 2, b = 3$. Рассмотрим сначала левую часть:

$$a^2 = a \cdot a = 2 \cdot 2 = 3;$$

$$b^2 = b \cdot b = 3 \cdot 3 = 2;$$

$$-b^2 = 2;$$

$$a^2 - b^2 = a^2 + (-b^2) = 3 + 2 = 1.$$

Рассмотрим теперь правую часть:

$$(a - b) = 2 + (-3) = 2 + 3 = 1;$$

$$(a + b) = 2 + 3 = 1;$$

$$(a - b)(a + b) = 1 \cdot 1 = 1.$$

Таким образом, исходное соотношение выполняется.

Мы не будем подробно рассматривать структуру конечных полей, однако остановимся на нескольких важных результатах.

Если p – простое число, то элементы $\{0, 1, 2, \dots, p - 1\}$ образуют поле $GF(p)$ со сложением и умножением по модулю p .

Поле $GF(p)$ называют также **простым полем**.

В любом конечном поле количество элементов равно степени некоторого простого числа p^m . Это поле обозначается $GF(p^m)$.

Поле $GF(p^m)$ называется **расширенным полем**. Оно задается как *векторное пространство размерностью m* .

Произвольный элемент $\mathbf{a} \in GF(p^m)$ линейной комбинацией векторов $\alpha_i \in GF(p^m)$:

$$\mathbf{a} = a_0\alpha_0 + a_1\alpha_1 + \dots + a_{m-1}\alpha_{m-1}$$

с координатами $a_i \in GF(p)$. Линейно независимые вектора α_i образуют базис векторного пространства. Обычно используют степенной базис. Пусть x такой элемент $GF(p^m)$, первые m степеней которого линейно независимы. Множество элементов $1 = x^0, x, x^2, \dots, x^{m-1}$ называют степенным базисом поля $GF(p^m)$.

Теперь рассмотрим, как можно построить конечное поле из p^k элементов и как в нем устроены операции сложения и умножения.

Будем представлять элементы поля многочленами степени $k - 1$ с коэффициентами из поля $GF(p)$. Например, элементы $GF(3^2)$ образуют множество

$$\{0, 1, 2, x, x + 1, x + 2, 2x, 2x + 1, 2x + 2\}.$$

Очевидно, что имеется точно p^k таких элементов.

Казалось бы, естественно определить сложение и умножение как обычное сложение и умножение многочленов. Но такое определение нарушило бы аксиому замкнутости поля относительно операции умножения. Поэтому операции сложения и умножения в $GF(p^k)$ определяются как обычное сложение и умножение с последующей корректировкой. При сложении правильный результат получается, если действия над коэффициентами многочлена выполнять, помня, что они принадлежат конечному полю $GF(p)$. Например, в поле $GF(3^2)$ сложение будет выглядеть так:

$$(2x + 2) + (x + 2) = 1.$$

Для умножения корректировка более сложна, т. к. необходимо исправлять не только значения коэффициентов, но и показатели степеней, которые могут быть больше или равны k и, следовательно, не могут соответствовать элементам поля $GF(p^k)$.

Для выполнения корректировки выбирается неприводимый над $GF(p)$ многочлен $P(x)$ степени k , все коэффициенты которого принадлежат $GF(p)$. Обычно старший коэффициент $P(x)$ равен единице. Тогда коррекция многочлена-произведения с целью исключения степеней x^k и более высоких степеней x будет заключаться в делении полинома-произведения на $P(x)$ и сохранении только остатка.

Пример 4.20. Перемножить $(2x + 2)$ и $(x + 2)$ в поле $GF(3^2)$.

Решение. Рассмотрим поле $GF(3^2)$. Многочлен $P(x) = x^2 + x + 2$ неприводим над полем $GF(3)$, значит, его можно использовать для корректировки произведения элементов из поля $GF(3^2)$. Перемножим элементы $(2x + 2)$ и $(x + 2)$:

$$(2x + 2)(x + 2) = 2x^2 + 2x + 2x + 4 = 2x^2 + x + 1.$$

Далее выполним корректировку:

$$\langle 2x^2 + x + 1 \rangle_{x^2+x+2} = 2x.$$

Каждое конечное поле имеет *первообразный корень* — элемент, степени которого порождают все элементы поля, за исключением 0.

4.13 Задачи

1 Установите свойства деления в множестве положительных рациональных чисел (коммутативность, ассоциативность, идемпотентность, а также дистрибутивность и поглощение относительно умножения).

2 Установите, определена или нет операция умножения в множестве матриц вида $\begin{bmatrix} 0 & 0 \\ x & y \end{bmatrix}$, где $x, y \in \mathbb{R}$. Каковы свойства этой операции?

3 Определите, является ли полугруппой алгебра $\langle A, \Sigma \rangle$, где $A \in \mathbb{Z}$, а $\Sigma = \{-\}$ – операция вычитания.

4 Задано множество $S = \{u, v, w\}$, на котором определена операция « $\times$ » согласно таблице Кэли (рисунок 4.7). Определите, является ли полугруппой алгебра $\langle S, \Sigma \rangle$, где $\Sigma = \{\times\}$ – операция умножения.

$\times$	u	v	w
u	v	w	w
v	w	u	u
w	u	v	v

Рисунок 4.7 – Таблица Кэли для задачи 4 раздела 4

5 Проверьте, является ли группой алгебра $\langle A, \Sigma \rangle$, где $A = \begin{bmatrix} a & 0 \\ a & 0 \end{bmatrix}$, $a \in \mathbb{R} \setminus \{0\}$, а $\Sigma = \{\times\}$ – операция умножения.

6 Проверьте, является ли группой алгебра $\langle A, \Sigma \rangle$, где $A = \begin{bmatrix} a & a \\ a & a \end{bmatrix}$, $a \in \mathbb{R} \setminus \{0\}$, а $\Sigma = \{\times\}$ – операция умножения.

7 Проверьте, является ли группой алгебра $\langle A, \Sigma \rangle$, где $A = a + b\sqrt{5}$, $a, b \in \mathbb{Q}$, а $\Sigma = \{\times\}$ – операция умножения.

8 Проверьте, является ли группой алгебра $\langle A, \Sigma \rangle$, где $A = a + b\sqrt{5}$, $a, b \in \mathbb{Q}$ и $a^2 + b^2 \neq 0$, а $\Sigma = \{\times\}$ – операция умножения.

9 Определите, является ли группой множество подстановок $M = \{a_1, a_2, a_3, a_4, a_5, a_6\}$ относительно операции композиции

$$a_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad a_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$a_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad a_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad a_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

10 Определите, является ли группой следующая алгебра: $\langle \{a, b, c, p\}, \circ \rangle$, где $a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$, $c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$, $p = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$.

11 Образует ли совокупность функций: $x, \frac{1}{x}, 1 - x, \frac{1}{1-x}, \frac{x}{x-1}, \frac{x-1}{x}$ группу по отношению к композиции?

12 Проверьте, образует ли множество классов вычетов по модулю 6 группу относительно сложения. Будут ли образовывать группу относительно умножения?

13 Найдите целые числа, меньшие 12 и взаимно простые с 12. Образуют ли данные числа группу относительно операции умножения по модулю 12?

14 Подгруппы какого порядка может содержать группа, имеющая порядок 399?

15 Найдите порядок элемента $B = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ группы матриц 3×3 относительно операции матричного умножения.

16 Найдите порядок элемента $b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ группы подстановок.

17 Найдите порядок каждого элемента в аддитивной группе $\mathbb{Z}_8$.

18 Определите, является ли группа $G = \{1, 2, 3, 4\}$ с операцией умножения по модулю 5 циклической? Найдите образующий элемент группы.

19 В циклической группе $\mathbb{Z}_{15}$ с операцией сложения по модулю 15 определите число элементов, имеющих порядок 15.

20 Элемент $g = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ является образующим элементом циклической группы (относительно операции умножения). Найдите порядок группы.

21 Запишите перестановки, составляющие симметрическую группу S_3 .

22 Для группы с операцией умножения по mod 7 (мультипликативная группа $\mathbb{Z}_7$), состоящей из элементов $\{1, 2, 3, 4, 5, 6\}$, для каждого элемента укажите обратный.

23 Дана группа $G = \mathbb{Z}_3 \times \mathbb{Z}_3$. Найдите обратный элемент $a^{-1} \in G$ относительно операции умножения и сложения, если $a = (2, 1)$. Чему равен порядок элемента a ?

24 Пусть M – множество матриц размером 2×2 . Является ли функция вычисления детерминанта $\det: M \rightarrow \mathbb{R}$ гомоморфизмом относительно операции сложения и умножения?

25 Является ли $\langle \mathbb{N}, +, \cdot \rangle$ кольцом?

26 Рассмотрим множество $S = \{0, 1\}$ с операциями сложения и умножения (рисунок 4.8). Определите, является ли $\langle S, +, \cdot \rangle$ кольцом?

+	0	1
0	0	1
1	1	0

a

×	0	1
0	1	0
1	0	1

б

Рисунок 4.8 – Таблица сложения (*a*) и умножения (*б*) для задачи 26 раздела 4

27 Образуют ли кольцо числа вида $a + b\sqrt{2 + \sqrt{2}}$, где $a, b \in \mathbb{Q}$?

28 Образуют ли кольцо числа вида $a + b\sqrt{2} + c\sqrt{2 + \sqrt{2}}$, где $a, b, c \in \mathbb{Q}$?

29 Образуют ли кольцо числа вида $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$, где $a, b, c, d \in \mathbb{Q}$?

30 Для кольца чисел вида $p = a + b\sqrt{2}$, где $a, b, c \in \mathbb{Q}$, покажите, как вычисляется обратный элемент (по умножению) p^{-1} .

31 Элемент a кольца R называется делителем нуля, если в кольце существует такой элемент b , что $ab = 0$. Что представляют собой делители нуля в кольце $\mathbb{Z}_{10}$?

32 Запишите в стандартном виде многочлен $h(x) = f(x)g(x)$, где $f(x) = 3x^4 - 2x^3 + 2x^2 + 7$; $g(x) = 5x^3 + 4x - 5$.

33 Непосредственным делением $f(x)$ на $g(x)$ найдите частное и остаток, если $f(x) = 2x^5 + 3x^4 - 6x^3 - 5x + 7$; $g(x) = x^3 + 2x^2 - 3x + 1$.

34 Непосредственным делением $f(x)$ на $g(x)$ найдите частное и остаток, если $f(x) = 2x^4 - x^3 + 5x^2 - 8x + 1$; $g(x) = x^2 - x + 1$.

35 Найдите частное и остаток от деления многочлена $f(x) = 2x^4 + x + 1$ на $g(x) = 2x + 1$ в кольце $\mathbb{Z}_3[x]$.

36 Пусть $a(x) = 3x^2 + 5x + 1$ и $b(x) = 6x + 4$ являются элементами кольца многочленов $Z_7[x]$, найдите, чему равно $a(x) - b(x)$.

37 Даны два многочлена $a(x) = 3x^2 + 5x + 1$ и $b(x) = 6x + 4$. Найдите $\langle a(x)b(x) \rangle_{p(x)}$, где $p(x) = x^3 + x^2 + x + 1$.

38 Пусть $a(x) = 3x^3 + 2x^2 + 3x + 2$ и $b(x) = 5x^2 + 2x + 4$ являются элементами кольца многочленов $Z_7[x]$, найдите, чему равно $a(x) \times b(x)$.

39 Найдите каноническое представление следующих чисел:

а) 398;

б) 572;

в) 987.

40 Найдите все взаимно простые числа с $m = 12$ и меньшие m .

41 Проверьте истинность следующих сравнений:

а) $75 \equiv 18 \pmod{13}$;

б) $174 \equiv 18 \pmod{13}$;

в) $512 \equiv 47 \pmod{15}$.

42 Используя алгоритм Евклида, найдите НОД и НОК следующих пар чисел:

а) 27 и 18;

б) 621 и 437;

в) 377 и 289.

43 НОД(88, 48) = 8. Найдите такие целые числа a и b , чтобы $88a + 48b = 8$.

44 Найдите НОД(162, 99) и выразите его через исходные числа.

45 Используя алгоритм Евклида, найдите $19^{-1} \bmod 26$.

46 Используя алгоритм Евклида, найдите $131^{-1} \bmod 834$.

47 В шкатулке лежали монеты. Пришел Саша и стал раскладывать монеты в кучки по 7 штук. После пришла Юля и решила разложить монеты в кучки по 11 штук. Далее пришел папа и решил разложить монеты в кучки по 13 штук. Сколько всего было монет, если у Саши неиспользованными осталось 5 монет, у Юли 3 монеты, а у папы – 10? То есть по китайской теореме об остатках вычислите x для следующей системы:

$$\begin{cases} x = 5 \bmod 7, \\ x = 3 \bmod 11, \\ x = 10 \bmod 13. \end{cases}$$

48 Юра решил прочитать книгу М. А. Булгакова «Мастер и Маргарита». «Сколько страниц ты прочитал?» – спросил у Юры Андрей. – «Если поделить число страниц на 5, то в остатке будет 2». – «Сколько страниц ты прочитал?» – спросила у Юры Наташа. – «Если поделить число страниц на 17, то в остатке будет 15». – «Сколько страниц ты уже прочитал?» – спросил у Юры Леша. – «Если поделить число страниц на 12, то в остатке будет 5». – ответил Юра. Сколько страниц успел прочитать Юра? То есть по китайской теореме об остатках вычислите x для следующей системы:

$$\begin{cases} x = 2 \bmod 5, \\ x = 15 \bmod 17, \\ x = 5 \bmod 12. \end{cases}$$

49 Перечислите все элементы поля Галуа $GF(2^3)$.

50 Перечислите все элементы поля Галуа $GF(3^2)$.

51 Элементы $a(x) = x^2 + 2x + 1$ и $b(x) = 4x^2 + 3x$ принадлежат полю $GF(5^3)$. Найдите произведение $a(x)b(x)$, если известно, что умножение в поле определено по модулю примитивного многочлена $p(x) = x^3 + 3x + 2$.

52 Рассмотрим конечное поле $GF(2^3)$ с примитивным полиномом $p(x) = x^3 + x + 1$. Является ли элемент $a(x) = x$ первообразным корнем?

ПРИЛОЖЕНИЕ А

Ответы к задачам раздела 1

1 $S = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $C = \{1, 2, 3, 4\}$, $Q = \{1, 2, 3\}$; а) ложно; б) истинно; в) истинно; г) ложно.

2 $P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67\}$.

3 а) $A = \{n \mid n = 18 - 8k, k \in \mathbb{N}\}$; б) $B = \{n \mid n = \pm 3^k, k \in \mathbb{N}\}$; в) $C = \{x \mid x = 1 - 3^{-k}, k \in \mathbb{N}\}$; г) $D = \{x \mid \text{mod}(x, 3) = 0, x \in \mathbb{N}\}$.

4 а) ложно; б) ложно; в) истинно; г) истинно.

5 а) истинно; б) ложно; в) ложно; г) истинно.

6 $\{\emptyset\}$; $\{a\}$; $\{b\}$; $\{c\}$; $\{a, b\}$; $\{a, c\}$; $\{b, c\}$; $\{a, b, c\}$.

7 а) $A = B$; б) $B \subset A$.

8 $\rho(A) = \{\{\emptyset\}, \{4\}, \{3\}, \{3, 4\}, \{2\}, \{2, 4\}, \{2, 3\}, \{2, 3, 4\}, \{1\}, \{1, 4\}, \{1, 3\}, \{1, 3, 4\}, \{1, 2\}, \{1, 2, 4\}, \{1, 2, 3\}, \{1, 2, 3, 4\}\}$. $|\rho(A)| = 2^N = 2^4 = 16$.

9 $A \cup B = \{1, 2, 5, 6, 7, 8, 9\}$, $A \cap B = \{2\}$, $A \setminus B = \{1, 5, 7, 8\}$, $B \setminus A = \{6, 9\}$, $U = \{1, 2, 5, 6, 7, 8, 9\}$.

10 а) $\{1, 2, 3, 8, 9\}$; б) $\{1, 2, 3\}$; в) $\{1, 2, 3, 8, 9\}$; г) $\{8, 9\}$.

11 $A \cup B = \{a, b, c, d, e, p, q, r, s\}$, $A \cap B = \{\emptyset\}$, $A \setminus B = \{a, b, c, d, e\}$, $U = \{a, b, c, d, e, p, q, r, s\}$.

12 Неверно.

13 а) $A \cap B = \{(x, y) \mid (x > 0) \wedge (y > 0)\}$;

б) $A \cup B = \{(x, y) \mid (x > 0) \vee (y > 0)\}$;

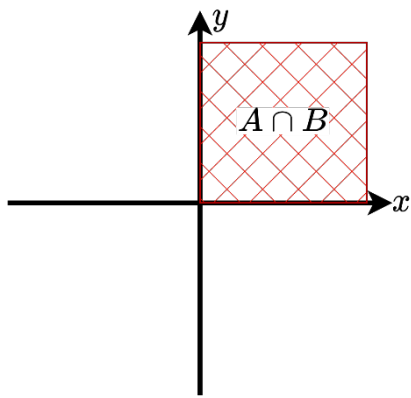
в) $A \setminus B = \{(x, y) \mid (x \leq 0) \wedge (y > 0)\}$;

г) $\overline{A} = \{(x, y) \mid (y < 0)\}$;

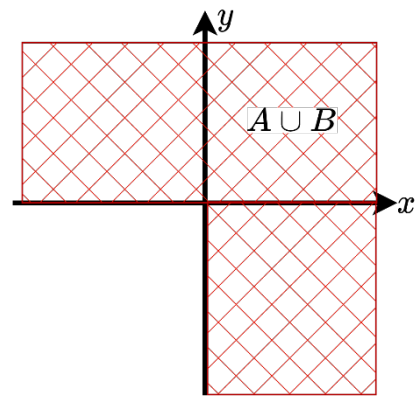
д) $\overline{(A \cap B)} = \{(x, y) \mid (x < 0) \vee (y < 0)\}$;

е) $\overline{(A \cup B)} = U \setminus (A \cup B) = \{(x, y) \mid (x < 0) \wedge (y < 0)\}$.

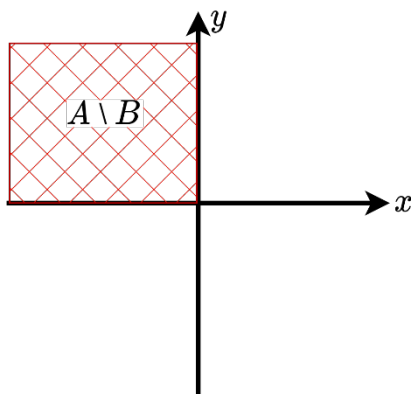
Графически представлено на рисунке А.1.



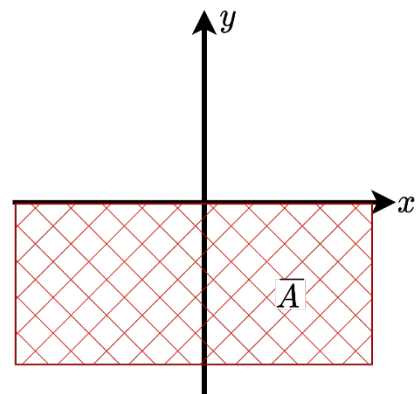
a



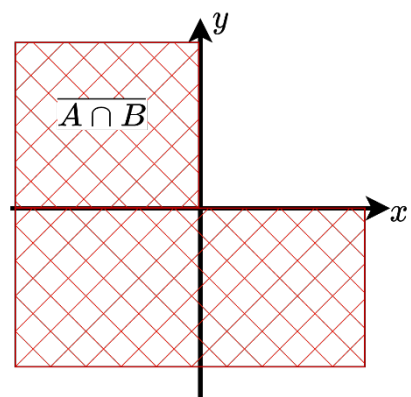
б



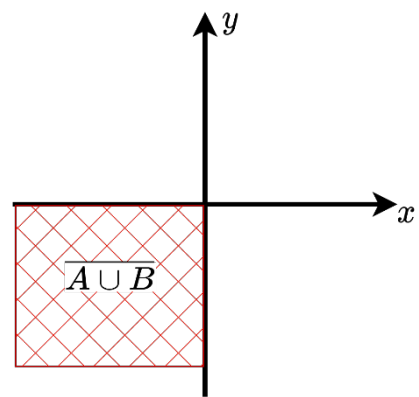
в



г



д



е

$a - A \cap B; б - A \cup B; в - A \setminus B; г - \bar{A}; д - \overline{A \cap B}; е - \overline{A \cup B}$

Рисунок А.1 – Ответы к задаче 13 раздела 1

14 а) неверно; б) верно; в) верно; г) верно; д) верно; е) верно.

15 а) верно; б) неверно (строгое включение); в) неверно.

16 Неверно.

17 Неверно.

18 $\bar{A}$.

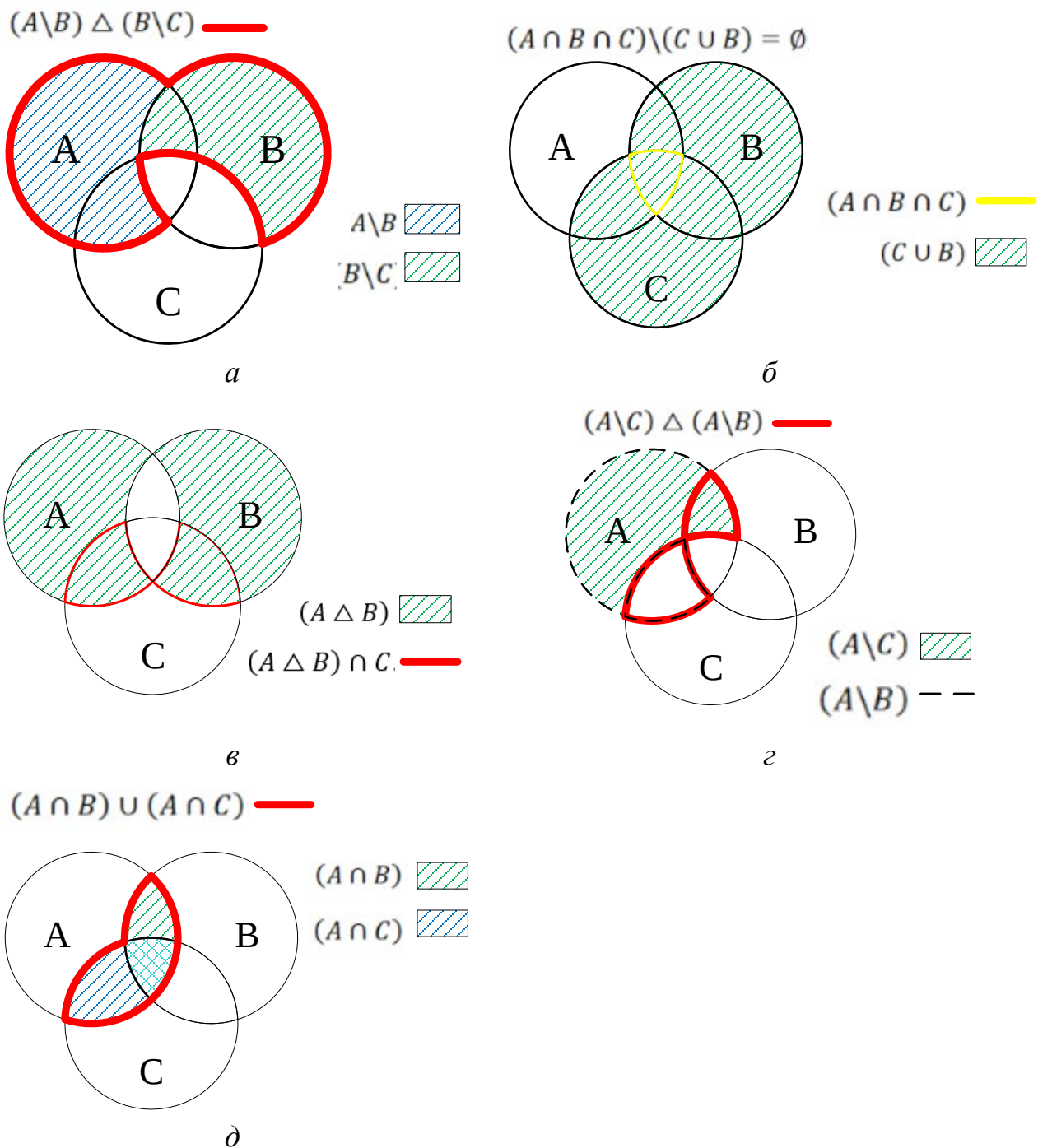
19 C.

20 $\emptyset$.

21 7 человек.

22 96 человек, 4 человека, 20 человек.

23 Рисунок А.2.



$a - (A \setminus B) \Delta (B \setminus C)$; $б - (A \cap B \cap C) \setminus (B \cup C)$; $в - (A \Delta B) \cap C$;

$г - (A \setminus C) \Delta (A \setminus B)$; $д - (A \cap B) \cup (A \cap C)$

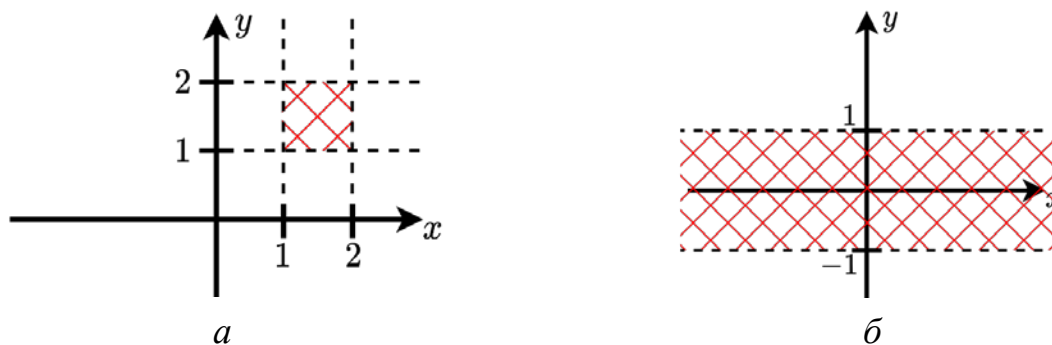
Рисунок А.2 – Ответы к задаче 23 раздела 1

ПРИЛОЖЕНИЕ Б

Ответы к задачам раздела 2

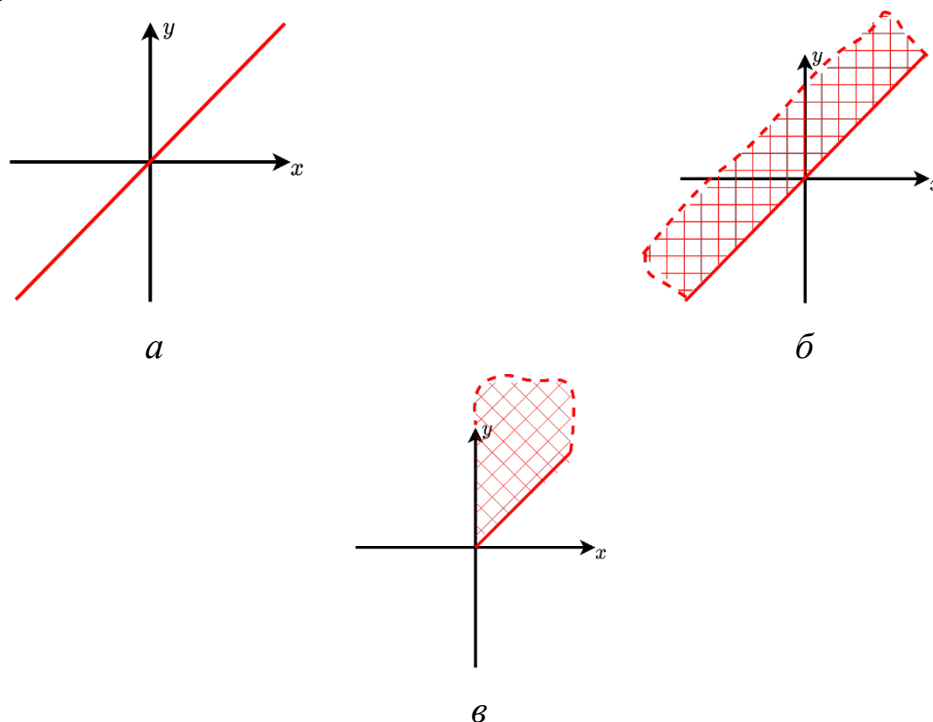
1 $R = A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c), (3, a), (3, b), (3, c)\},$
 $S = B \times A = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3), (c, 1), (c, 2), (c, 3)\}.$

2 Рисунок Б.1.



a – к пункту «а»; $б$ – к пункту «б»
 Рисунок Б.1 – Ответы к задаче 2 раздела 2

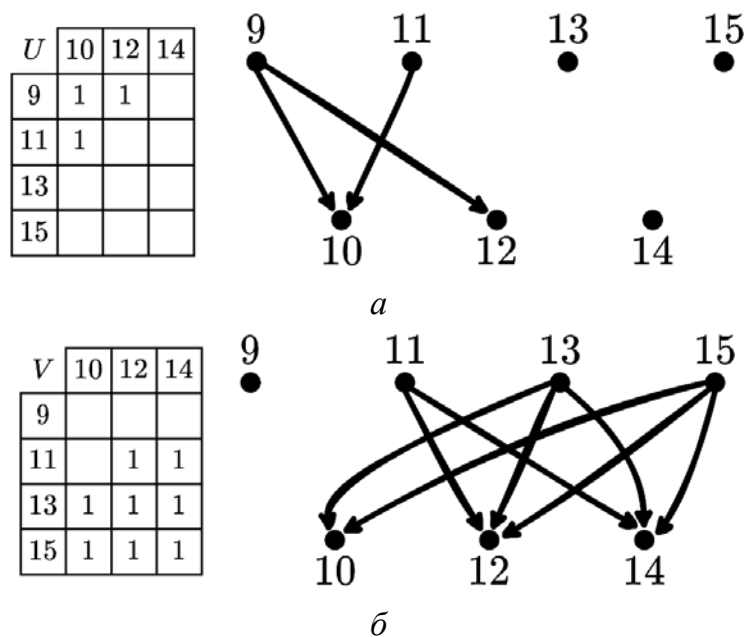
3 Рисунок Б.2.



a – к пункту «а»; $б$ – к пункту «б»; $в$ – к пункту «в»
 Рисунок Б.2 – Ответы к задаче 3 раздела 2

4 а) $U = \{(3, 6), (5, 4), (7, 2)\};$ б) $V = \{(1, 2), (1, 4), (1, 6), (3, 4), (3, 6), (5, 6)\}.$

5 а) $U = \{(9, 10), (9, 12), (11, 10)\};$ рисунок Б.3, а; б) $V = \{(11, 12), (11, 14), (13, 10), (13, 12), (13, 14), (15, 10), (15, 12), (15, 14)\};$ рисунок Б.3, б.



a – к пункту «а»; $б$ – к пункту «б»

Рисунок Б.3 – Ответы к задаче 5 раздела 2

6 а) $R = \{(1, 7), (2, 3), (3, 2), (4, 1)\}$; б) $S = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (2, 1), (2, 2), (2, 3), (2, 4), (3, 1), (3, 2), (3, 3), (4, 1), (4, 2), (5, 1)\}$; в) $T = \{(x, x^2) \mid x \in \mathbb{N}\}$.
 7 а) $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (3, 1), (3, 2), (3, 3), (3, 4)\}$; рисунок Б.4.

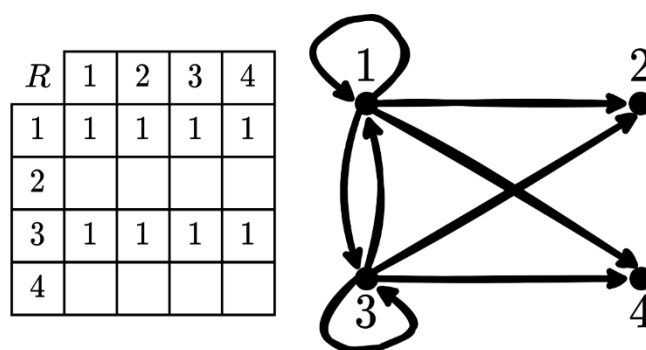


Рисунок Б.4 – Ответы к пунктам «б» и «в» задачи 7 раздела 2

8 $R = (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 3), (2, 4), (2, 5), (2, 6), (3, 4), (3, 5), (3, 6), (4, 5), (4, 6), (5, 6)\}$. Данное отношение: антирефлексивно, антисимметрично, транзитивно, полное (рисунок Б.5).

R	1	2	3	4	5	6
1		1	1	1	1	1
2			1	1	1	1
3				1	1	1
4					1	1
5						1
6						

Рисунок Б.5 – Ответ к задаче 8 раздела 2

9 $R = \{(a, b), (a, c), (b, c), (b, d), (c, b), (d, a), (d, b), (d, d)\}$.

10 а) $R = \{(2, 1), (3, 2), (4, 3)\}$; б) рисунок Б.6; в) $x - y = 1$.

R	1	2	3	4
1		1		
2			1	
3				1
4				

Рисунок Б.6 – Ответ к пункту «б» задачи 10 раздела 2

11 Рисунок Б.7.

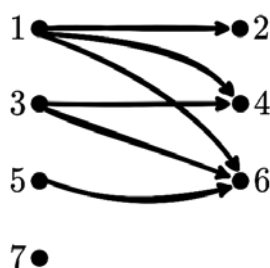


Рисунок Б.7 – Ответ к задаче 11 раздела 2

12 $R = \{(1, a), (1, b), (1, c), (1, d), (2, b), (3, c)\}$. Рисунок Б.8.

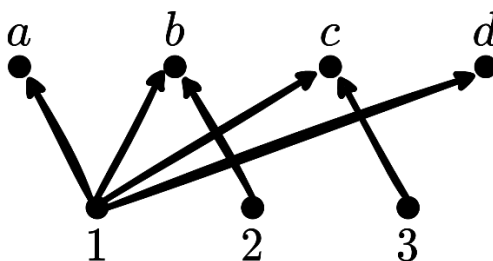


Рисунок Б.8 – Ответ к задаче 12 раздела 2

13 а) $R = \{(1, 7), (2, 5), (3, 3), (4, 1)\}$; б) $S = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 1), (2, 2), (2, 3), (2, 4), (3, 1), (3, 2), (3, 3), (4, 1), (4, 2), (5, 1)\}$; в) $T = \{(1, 1), (2, 4), (3, 9), \dots\}$.

14 Рисунок Б.9.

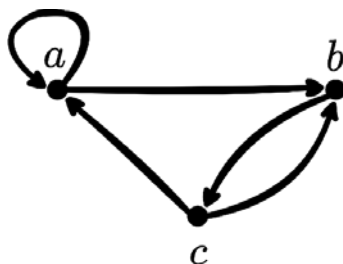


Рисунок Б.9 – Ответ к задаче 14 раздела 2

15 Рисунок Б.10.

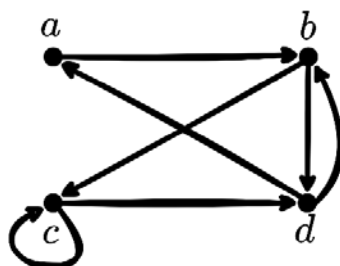


Рисунок Б.10 – Ответ к задаче 15 раздела 2

16 $T = \{(v, b), (w, c), (x, d), (y, f), (z, g)\}$.

17 а) $R^{-1} = \{(7, 1), (6, 4), (6, 5), (8, 2)\}$;

$S^{-1} = \{(10, 6), (11, 6), (10, 7), (13, 8)\}$;

б) $S \circ R = \{(1, 10), (4, 10), (4, 11), (5, 10), (5, 11), (2, 13)\}$;

в) $S \circ S^{-1} = \{(10, 10), (10, 11), (11, 10), (11, 11), (13, 13)\}$;

$S^{-1} \circ S = \{(6, 6), (6, 7), (7, 6), (7, 7), (8, 8)\}$;

г) $R^{-1} \circ S^{-1} = \{(10, 4), (10, 5), (11, 4), (11, 5), (10, 1), (13, 2)\}$;

д) $T \circ S = \{(6, \Delta), (7, \Delta), (8, \star), (8, \bigcirc)\}$;

е) $T \circ (S \circ R) = \{(1, \Delta), (4, \Delta), (5, \Delta), (2, \star), (2, \bigcirc)\}$.

18 а) $U \circ V = \{(x, y): y = 9x^2 + 5\}$; б) $V \circ U = \{(x, y): y = 3x^2 + 15\}$;

в) $U^{-1} = \{(x, y): y = \pm\sqrt{x-5}\}$; г) $V^{-1} = \{(x, y): y = \frac{1}{3}x\}$.

19 $R = \{(2, 1), (3, 2), (3, 1), (3, 4), (4, 1), (5, 4), (5, 1), (5, 2)\}$. Данное отношение R антирефлексивно, антисимметрично (рисунок Б.11).

R	1	2	3	4	5
1					
2	1				
3		1		1	
4	1				
5	1	1		1	

Рисунок Б.11 – Ответ к задаче 19 раздела 2

20 Рефлексивно, антисимметрично, транзитивно, полное.

21 а) антисимметрично; б) не обладает никакими свойствами; в) рефлексивно, транзитивно; г) симметрично, транзитивно.

22 Рефлексивно, антисимметрично, транзитивно (рисунок Б.12).

T	1	2	3	4	5	6
1	1	1	1	1	1	1
2		1		1		1
3			1			1
4				1		
5					1	
6						1

Рисунок Б.12 – Ответ к задаче 22 раздела 2

23 Антирефлексивно, антисимметрично (рисунок Б.13).

T	1	2	3	4	5	6
1		1	1	1	1	1
2						
3		1				
4			1			
5		1		1		
6					1	

Рисунок Б.13 – Ответ к задаче 23 раздела 2

24 а) рефлексивно, симметрично, транзитивно; б) рефлексивно, симметрично; в) рефлексивно, симметрично, транзитивно; г) рефлексивно, симметрично, транзитивно; д) рефлексивно, симметрично, транзитивно; е) антирефлексивно, антисимметрично; ж) антирефлексивно, антисимметрично.

25 Рефлексивное? – нет; антирефлексивное? – да; симметричное? – нет; антисимметричное? – да; транзитивное? – да; полное? – да (рисунок Б.14).

R	1	2	3	4	5	6
1		1	1	1	1	1
2			1	1	1	1
3				1	1	1
4					1	1
5						1
6						

Рисунок Б.14 – Ответ к задаче 25 раздела 2

26 а) рефлексивно, антисимметрично, транзитивно; б) рефлексивно, симметрично; в) рефлексивно, симметрично; г) рефлексивно, симметрично.

27 а) да; б) нет; в) нет; г) да.

ПРИЛОЖЕНИЕ В

Ответы к задачам раздела 3

1 а) не функция; б) функция; в) не функция.

2 а) не функция; б) функция; в) функция; г) функция; д) не функция.

3 а) $\text{Dom} = \mathbb{R}$, $\text{Im} = \{y: y \geq 4\}$; б) $\text{Dom} = \{x: x \geq 2\}$; $\text{Im} = \{y: y \geq 0\}$;
в) $\text{Dom} = \{x: x > 2\}$; $\text{Im} = \{y: y > 0\}$; г) $\text{Dom} = \mathbb{R}$; $\text{Im} = \{y: 0 \leq \frac{1}{4}\}$; д) $\text{Dom} = \mathbb{R} - \{2, -2\}$; $\text{Im} = \{y: y \leq -1/4\} \cup \{y: y > 0\}$; е) $\text{Dom} = \mathbb{R}$; $\text{Im} = \{y: y > 0\}$.

4 а) не функция; б) функция; в) не функция,

5 а) неинъективна, несюръективна, небиективна; б) функция инъективна, сюръективна, биективна; в) неинъективна, сюръективна, небиективна; г) инъективна, несюръективна, небиективна.

6 а) несюръективна; б) сюръективна; в) несюръективна; г) сюръективна.

7 Является биекцией.

8 Для нечетных n .

9 Ни при каких значениях n функция не будет являться сюръекцией.

10 $S \circ R = \{(a, y), (a, x), (b, x)\}$. Рисунок В.1.

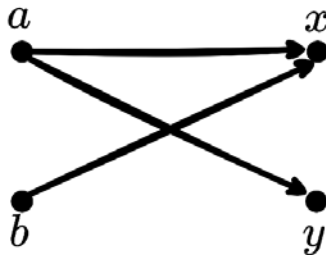


Рисунок В.1 – Ответы к задаче 10 раздела 3

11 $g \circ f = \{(1, 4), (2, 9), (3, 16)\}$.

12 а) $f \circ g = (x + 3)^2 + 1$; $g \circ f = x^2 + 4$; б) $f \circ g = \sqrt{(x^2 + 3)^2 + 2}$;
 $g \circ f = x^2 + 5$; в) $f \circ g = \frac{1}{2x+3}$; $g \circ f = \frac{2}{x} + 3$.

13 а) $G \circ F = \{(1, e), (2, g), (3, g), (4, g)\}$; б) $H \circ (G \circ F) = \{(1, r), (2, t), (3, t), (4, t)\}$; в) $(H \circ G) \circ F = \{(1, r), (2, t), (3, t), (4, t)\}$.

14 а) $F \circ G = \{(1, 3), (2, 2), (3, 4), (4, 2)\}$; б) $H \circ F = \{(1, 1), (2, 4), (3, 4), (4, 3)\}$;
в) $G \circ H = \{(1, 3), (2, 2), (3, 1), (4, 4)\}$; г) $(F \circ G) \circ H = \{(1, 2), (2, 2), (3, 3), (4, 4)\}$.

15 $f \circ g = \frac{2x^2+7}{x^2+9}$; $g \circ f = \frac{(2x-3)^2}{(x+4)^2}$; $f \circ f = \frac{x-18}{6x+13}$; $g \circ g = (x^2 + 5)^2 + 5$.

$$\begin{array}{llll}
16 \text{ а) } f \circ g = & g \circ f = & f^{-1} = & g^{-1} = \\
= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; & = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}; & = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; & = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; \\
\text{б) } f \circ g = & g \circ f = & f^{-1} = & g^{-1} = \\
= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}; & = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}; & = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}; & = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}; \\
\text{в) } f \circ g = & g \circ f = & f^{-1} = & g^{-1} = \\
= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}; & = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}; & = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}; & = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}; \\
\text{г) } f \circ g = & g \circ f = & f^{-1} = & g^{-1} = \\
= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}; & = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}; & = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}; & = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.
\end{array}$$

17 а) неинъективна, несюръективна, небиективна; б) неинъективна, несюръективна, небиективна; в) инъективна, сюръективна, биективна, $f_3^{-1} = \sqrt[3]{x-6}$; г) неинъективна, несюръективна, небиективна; д) неинъективна, сюръективна, небиективна.

$$18 \text{ а) } f_1^{-1} = 2x - 4; \text{ б) } f_2^{-1} = \sqrt[3]{x}; \text{ в) } f_3^{-1} = \frac{-2-3x}{x-1}; \text{ г) } f_4^{-1} = \frac{3-5x}{2x-4}.$$

$$19 \text{ а) } \sigma_1 = \{\{1, 3, 4, 7\}, \{2, 9\}, \{5, 8\}, \{6\}\}; \text{ б) } \sigma_2 = \{\{1, 2, 4, 8\}, \{3, 7, 9, 5\}, \{6\}\};$$

$$\text{в) } \sigma_3 = \{\{1, 2, 4, 7, 5, 3\}, \{6\}\}; \text{ г) } \sigma_4 = \{\{1, 3, 5\}, \{2, 4, 6\}\}.$$

$$20 \text{ а) } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 1 & 4 & 2 \end{pmatrix}; \text{ б) } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}; \text{ в) } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 5 & 1 & 4 & 6 \end{pmatrix}; \text{ г) } \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 1 & 6 & 5 & 7 & 4 & 8 \end{pmatrix}.$$

$$21 \text{ } F(2) = 0, F(3) = -20, F(4) = -20, F(5) = 20, F(6) = 60.$$

$$22 \text{ } F(3) = 18, F(4) = 55, F(5) = 186, F(6) = 614.$$

23 а) $F(n) = 2n$. Рекурсия: $F(0) = 0$, $F(n) = F(n-1) + 2$; б) $F(n) = 2^n$. Рекурсия: $F(0) = 1$, $F(n) = 2F(n-1)$; в) $F(n) = 2n + 1$. Рекурсия: $F(0) = 1$, $F(n) = F(n-1) + 2$; г) $F(n) = \begin{cases} n, & n \text{ нечетное,} \\ n-1, & n \text{ четное.} \end{cases}$ Рекурсия: $F(0) = 1, F(1) = 1, F(n) = F(n-2) + 2$.

24 а) $Q(a, b)$ находит частное от деления a на b ; б) $Q(2, 5) = 0$; в) $Q(12, 5) = 2$; г) $Q(5861, 7) = 837$.

ПРИЛОЖЕНИЕ Г

Ответы к задачам раздела 4

- 1 Ассоциативность – нет, коммутативность – нет, дистрибутивность слева – нет, дистрибутивность справа – нет, поглощение – нет, идемпотентность – нет.
- 2 Операция определена. Свойства: ассоциативна, некоммутативна.
- 3 Не является группой.
- 4 Не является группой.
- 5 Является группой.
- 6 Является группой.
- 7 Не является группой.
- 8 Является группой.
- 9 Является группой.
- 10 Является группой.
- 11 Является группой.
- 12 Является группой относительно сложения, не является группой относительно умножения.
- 13 $\{1, 5, 7, 11\}$. Является группой относительно умножения.
- 14 1, 3, 7, 19, 21, 57, 133, 399.
- 15 $n = 3$.
- 16 $n = 4$.
- 17 $1 \rightarrow n = 8$; $2 \rightarrow n = 4$; $3 \rightarrow n = 8$; $4 \rightarrow n = 4$; $5 \rightarrow n = 8$; $6 \rightarrow n = 4$; $7 \rightarrow n = 8$.
- 18 Является циклической группой $C_4^\times$. Образующие группы: 2, 3.
- 19 Всего восемь элементов: $\{1, 2, 4, 7, 8, 11, 13, 14\}$.
- 20 Порядок $n = 3$.
- 21 $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.
- 22 $a_1^{-1} = 1$, $a_2^{-1} = 4$, $a_3^{-1} = 5$, $a_4^{-1} = 2$, $a_5^{-1} = 3$, $a_6^{-1} = 6$.
- 23 $a_x^{-1}(2, 1) = a(2, 1)$, $a_+^{-1}(2, 1) = a(1, 2)$. Порядок $a^+(2, 1) = 3$, порядок $a^\times(2, 1) = 2$.
- 24 Является гомоморфизмом относительно умножения и не является гомоморфизмом относительно сложения.
- 25 Нет.
- 26 Нет.

27 Нет.

28 Нет.

29 Да.

$$30 \ p^{-1} = -\frac{a}{2b^2-a^2} + \frac{b}{2b^2-a^2}\sqrt{2}.$$

31 Делители нуля в кольце $Z_{10} = \{2, 4, 5, 6, 8\}$.

$$32 \ h = 15x^7 - 10x^6 + 22x^5 - 23x^4 + 53x^3 - 10x^2 + 28x - 35.$$

33 Частное $2x^2 - x + 2$, остаток $-9x^2 + 2x + 5$.

34 Частное $2x^2 + x + 4$, остаток $-5x - 3$.

35 Частное $x^3 + x^2 + x$, остаток 1.

36 Ответ: $3x^2 + 6x + 4$.

37 Ответ: $24x^2 + 8x - 14$.

$$38 \ x^5 + 2x^4 + 3x^3 + 3x^2 + 2x + 1.$$

$$39 \text{ а) } 398 = 2^1 \cdot 199^1; \text{ б) } 572 = 2^2 \cdot 11^1 \cdot 13^1; \text{ в) } 987 = 3^1 \cdot 7^1 \cdot 47^1.$$

40 Ответ: 1, 5, 7, 11.

41 а) ложно; б) истинно; в) истинно.

42 а) НОД(27,18) = 9, НОК(27,18) = 54;

б) НОД(621,437) = 23, НОК(621,437) = 11799;

в) НОД(377,289) = 1, НОК(377,289) = 108953.

$$43 \ a = -1, b = 2.$$

$$44 \ \text{НОД}(162, 99) = 5 \cdot 99 - 3 \cdot 162.$$

$$45 \ \text{Ответ: } 19^{-1} = 11 \bmod 26.$$

$$46 \ \text{Ответ: } 131^{-1} = 191 \bmod 834.$$

47 Всего 834 монеты.

48 Всего 797 страниц.

$$49 \ GF(2^3) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.$$

$$50 \ GF(3^2) = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}.$$

$$51 \ \text{Ответ: } 3x^2 + 2x + 3.$$

52 Является.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Новиков, Ф. А. Дискретная математика : учеб. для вузов / Ф. А. Новиков. – 3-е изд. – СПб. : Питер, 2017. – 496 с.
- 2 Андерсон, Дж. Дискретная математика и комбинаторика / Дж. Андерсон. – М. : Вильямс, 2004. – 960 с.
- 3 Стюарт, Я. Концепции современной математики / Я. Стюарт. – Минск : Выш. шк., 1980 – 384 с.
- 4 Поттосина, С. А. Основы дискретной математики и теории алгоритмов : практикум для студентов специальности «Информационные системы и технологии (в экономике)» / С. А. Поттосина, Т. Г. Пинчук. – Минск : БГУИР, 2009. – 86 с.
- 5 Кривцова, И. Е. Основы дискретной математики : учеб. пособие. Ч. 1 / И. Е. Кривцова, И. С. Лебедев, А. В. Настека. – СПб. : ИТМО, 2016. – 92 с.
- 6 Матвеевко, В. В. Дискретная математика : учеб.-метод. пособие / В. В. Матвеевко, Т. М. Кривоносова. – Минск : БГУИР, 2016. – 66 с.
- 7 Соболева, Т. С. Дискретная математика : учеб. для вузов / Т. С. Соболева, А. В. Чечкин. – М. : Академия, 2006. – 256 с.
- 8 Сигорский, В. П. Математический аппарат инженера / В. П. Сигорский. – М. : Техника, 1975. – 768 с.
- 9 Босс, В. Лекции по математике : учеб. пособие. В 16 т. Т. 8 : Теория групп / В. Босс. – М. : КомКнига, 2007. – 216 с.
- 10 Блейхут, Р. Быстрые алгоритмы цифровой обработки сигналов / Р. Блейхут ; пер. с англ. И. И. Грушко. – М. : Мир, 1989. – 448 с.
- 11 Васильев, Н. Н. Математика алгоритмов : учеб. пособие / Н. Н. Васильев. – СПб. : Изд-во Политехн. ун-та, 2008. – 140 с.
- 12 Бережной, В. В. Дискретная математика : учеб. пособие / В. В. Бережной, А. В. Шапошников ; Северо-Кавказский федеральный университет. – Ставрополь : СКФУ, 2016. – 199 с.

Учебное издание

Вашкевич Максим Иосифович
Порхун Максим Игоревич

ОСНОВЫ ДИСКРЕТНОЙ МАТЕМАТИКИ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *А. Ю. Шурко*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *В. А. Долгая*

Подписано в печать 19.03.2025. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 5,81. Уч.-изд. л. 6,0. Тираж 60 экз. Заказ 148.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
Ул. П. Бровки, 6, 220013, г. Минск