Министерство образования и науки Российской Федерации
Костромской государственный технологический университет
Кафедра высшей математики

А.В. Чередникова, О.Б. Садовская, Л.А. Каминская

Дискретная математика.
Теория и практика

Рекомендовано редакционно-издательским советом университета
в качестве учебного пособия

Кострома
КГТУ
2011

УДК 519.1 (075)

Чередникова А.В. Дискретная математика. Теория и практика / А.В. Чередникова, О.Б. Садовская, Л.А. Каминская. – Кострома: Изд-во Костром. гос. технол. ун-та, 2011. – 74 с.

В пособии рассматриваются следующие разделы дискретной математики: теория множеств, комбинаторика и общая алгебра. Теоретический материал изложен в доступной форме, но с сохранением необходимого уровня строгости изложения, сопровождается большим количеством примеров и решением типовых задач. Приведены разнообразные задачи и упражнения для самостоятельной работы.

Пособие предназначено для студентов бакалавриата по направлениям подготовки 090900 «Информационная безопасность», 230100 «Информатика и вычислительная техника», 230400 «Информационные системы и технологии».

Рецензенты: кафедра алгебры и геометрии
КГУ им. Н.А.Некрасова;
кандидат физ.-мат. наук, доцент
Н.Л. Марголина

Оглавление

Предисловие

В настоящем учебном пособии рассматриваются элементы следующих разделов дискретной математики: теории множеств (множества, отношения, функции), комбинаторики и общей алгебры (алгебраические системы).

Для краткой записи утверждений будем использовать следующие обозначения символов:

$\forall$ (*квантор общности*) читается «для любого», «для каждого», «для всех»;

$\exists$ (*квантор существования*) – «найдется», «существует», «хотя бы для одного»;

$\Rightarrow$ (*импликация, знак логического следования*) – «если …, то …», «следует»;

$\Leftrightarrow$ (*эквиваленция*, *знак логической равносильности*) – «тогда и только тогда».

Для любых предложений A и B запись $A \overset{def}{\Leftrightarrow} B$ означает, что предложения A и B равносильны по определению (от англ. definition – определение).

Знак будет обозначать конец примера, замечания или доказательства утверждения (при его отсутствии знак будет ставиться непосредственно после формулировки).

Введение

Понятие «дискретный» (от лат. discretus – разделенный, прерывный) является противоположным понятию «непрерывный». С содержательной точки зрения дискретный объект представляет собой нечто, состоящее из строго ограниченных, отделенных друг от друга неделимых частей.

Дискретная математика (или дискретный анализ) – совокупность математических дисциплин, изучающих свойства абстрактных дискретных объектов, которые возникают в математике и в ее приложениях. Эти объекты могут носить как конечный характер, так и бесконечный – в случае отделимости составляющих их элементов или скачкообразности происходящих в них процессов.

Деление математики на дискретную и классическую (непрерывную) математику достаточно условно. Так, например, методы теории множеств используются при изучении и дискретных, и непрерывных объектов. Дискретная математика также использует методы, разработанные в классической математике. Однако характер исследуемых дискретной математикой объектов настолько своеобразен, что методов классической математики не всегда достаточно для их изучения. Важными отличиями дисциплин дискретной математики от классических разделов непрерывной математики являются отсутствие понятия непрерывности и предела последовательности.

В настоящее время методы дискретной математики находят широкое применение в различных областях знаний, наиболее значимой из которых является область компьютерных технологий.

К разделам дискретной математики обычно относятся: теория множеств, комбинаторика, общая алгебра, теория графов, математическая логика, теория алгоритмов, теория кодирования, теория автоматов и многие другие.

Глава 1. Множества

1.1. Множества и их элементы. Способы задания множеств

Понятие множества является одним из фундаментальных понятий математики. Оно было введено в математику создателем теории множеств немецким ученым Георгом Кантором (1845 – 1918). Следуя ему, под *множеством* понимается совокупность объектов произвольной природы, которая рассматривается как единое целое. Объекты, входящие в состав множества, называются его *элементами*.

Это описание понятия множества нельзя считать логическим определением, а всего лишь пояснением. Понятие множества принимается как исходное, первичное, то есть не сводимое к другим понятиям.

Примерами множеств могут служить множество всех книг, составляющих данную библиотеку, множество всех точек данной линии, множество всех решений данного уравнения, множество всех одноклеточных организмов и т.п.

Множества принято обозначать прописными буквами латинского алфавита: A, B, C, … Для числовых множеств будем использовать следующие обозначения:

N – множество натуральных чисел;

N_0 – множество неотрицательных целых чисел;

Z – множество целых чисел;

Q – множество рациональных чисел;

I – множество иррациональных чисел;

R – множество действительных чисел;

C – множество комплексных чисел.

Элементы множества будем обозначать строчными латинскими буквами: a, b, c, …

Предложения вида «объект a есть элемент множества A», «объект a принадлежит множеству A», имеющие один и тот же смысл, кратко записывают в виде $a \in A$. Если элемент a не принадлежит множеству A, то пишут $a \notin A$.

Символ $\in$ называется *знаком принадлежности*.

Множества могут содержать как конечное число элементов, так и бесконечное. Например, множество всех корней уравнения $x^2 - 4x - 5 = 0$ конечно (два элемента), а множество всех точек прямой бесконечно. Рассматривают в математике и множество, не содержащее ни одного элемента.

Определение 1.1. Множество, не содержащее ни одного элемента, называется *пустым* и обозначается символом $\varnothing$.

Число элементов конечного множества называется его *мощностью*. Если множество A содержит n элементов, то будем писать $|A| = n$. Если $A = \varnothing$, то $|A| = 0$. Мощность бесконечного множества является более сложным понятием. Оно будет рассмотрено в главе 3.

Замечание 1.1. Элементами множества могут быть множества. Например, можно говорить о множестве групп некоторого факультета университета.

Элементы этого множества – группы, являющиеся в свою очередь множествами студентов. Но конкретный студент одной из групп уже не является элементом множества групп факультета.

Определение 1.2. Множество, элементами которого являются другие множества, называется *семейством* (*классом*).

Определение 1.3. Если все элементы данной совокупности множеств принадлежат некоторому одному множеству, то такое множество называется *универсальным множеством*, или *универсумом*, и обозначается U.

Множество считают заданным, если о любом объекте можно сказать, принадлежит он этому множеству или не принадлежит. ***Множество можно задать следующими способами***:

1) перечислением всех его элементов (списком);
2) характеристическим свойством элементов множества;
3) порождающей процедурой.

Первый способ задания множеств применим только для конечных множеств, да и то при условии, что число элементов множества невелико. Если a, b, c, d – обозначения *различных* объектов, то множество A этих объектов записывают так: $A = \{a; b; c; d\}$. Запись читают: «A – множество, элементы которого a, b, c, d».

Замечание 1.2. Порядок перечисления элементов множества *не имеет значения*. Так, множества $\{a; b; c; d\}$ и $\{b; c; d; a\}$ совпадают.

Вторым способом можно задавать как конечные, так и бесконечные множества. *Характеристическое свойство* – это такое свойство, которым обладает каждый элемент, принадлежащий множеству, и не обладает ни один элемент, который ему не принадлежит. Обозначив символом $P(x)$ характеристическое свойство элементов множества A, будем писать: $A = \{x| P(x)\}$.

Порождающая процедура описывает способ получения элементов нового множества из уже полученных элементов или из других объектов. Тогда элементами множества считаются все объекты, которые могут быть получены с помощью этой процедуры. С помощью порождающей процедуры можно задавать множества, содержащие любое число элементов.

Пример 1.1. Определим различными способами множество M_{2n-1} всех нечетных чисел, не превышающих 10:

1) $M_{2n-1} = \{1, 3, 5, 7, 9\}$;
2) $M_{2n-1} = \left\{2k-1 \middle| k \in N, k \le 5\right\}$;
3) порождающая процедура определяется правилами:
   а) $1 \in M_{2n-1}$;
   б) если $m \in M_{2n-1}$, то $(m + 2) \in M_{2n-1}$, $m \le 7$.

1.2. Подмножества

Определение 1.4. Множество B называется подмножеством множества A, если каждый элемент множества B принадлежит множеству A.

Пример 1.2. Пусть $A = \{a, b, c, d, e, f, g, h, i, j, k\}$, а $B = \{c, e, g, h, j, k\}$. Множество B является подмножеством множества A, поскольку каждый элемент множества B принадлежит множеству A.

Если множество B является подмножеством множества A, то говорят также, что B содержится в A или B включено в A и пишут $A \subseteq B$. Символ $\subseteq$ называется *знаком включения* (точнее, нестрого включения).

Согласно данному определению подмножества каждое множество является подмножеством самого себя: $(\forall A)\ A \subseteq A$. Кроме того, считается, что пустое множество есть подмножество любого множества A: $(\forall A)\ \varnothing \subseteq A$.

Различают два вида подмножеств множества A. Само множество A и $\varnothing$ называются *несобственными подмножествами* множества A. Любые подмножества множества A, отличные от A и $\varnothing$, называются *собственными подмножествами* множества A.

Определение 1.5. Множества A и B называются *равными* (пишут $A = B$), если они состоят из одних и тех же элементов.

Справедливо следующее утверждение, которое также можно рассматривать в качестве определения равных множеств.

Утверждение 1.1. $A = B \Leftrightarrow A \subseteq B$ и $B \subseteq A$.

Замечание 1.3. Из утверждения 1.1 вытекает *способ доказательства равенства двух множеств*: если доказать, что каждый элемент из множества A является элементом множества B и каждый элемент из множества B является элементом множества A, то делают вывод, что $A = B$.

Говорят, что множество B *строго включено* в множество A или, по-другому, A строго включает B, если $B \subseteq A$ и $B \neq A$. В этом случае пишут $B \subset A$. Символ $\subset$ называется *знаком строгого включения*.

Пример 1.3. Имеют место следующие строгие включения числовых множеств: $N \subset N_0 \subset Z \subset Q \subset R \subset C$, $I \subset R \subset C$.

Определение 1.6. Множество всех подмножеств множества A называется его *булеаном* (или *множеством-степенью*) и обозначается через $P(A)$ (или 2^A).

Пример 1.4. Если $A = \{a, b, c\}$, то
$P(A) = \{\varnothing, \{a\},\{b\},\{c\},\{a, b\},\{b, c\}, \{a, c\},\{a, b, c\}\}$.

1.3. Операции над множествами

Определим операции над множествами, с помощью которых можно получать из любых имеющихся двух множеств новые множества.

Определение 1.7. *Объединением* (*суммой*) $A \cup B$ (или $A + B$) множеств A и B называется множество, состоящее из тех и только тех элементов, которые принадлежат хотя бы одному из множеств A и B.

Таким образом, по определению, $A \cup B = \{x \mid x \in A \text{ или } x \in B\}$.

Заметим, что в объединение двух множеств A и B могут входить элементы из A, не принадлежащие множеству B, элементы из B, не принадлежащие

множеству A, и элементы, принадлежащие множествам A и B одновременно. Следовательно, $(\forall A, B)\ A \subseteq A \cup B$ и $B \subseteq A \cup B$.

Определение 1.8. *Пересечением* (*произведением*) $A \cap B$ (или $A \cdot B$, или AB) множеств A и B называется множество, состоящее из тех и только тех элементов, которые принадлежат обоим множествам A и B одновременно.

Таким образом, по определению, $A \cap B = \{x \mid x \in A \text{ и } x \in B\}$.

Замечание 1.4. Если $A \cap B \neq \varnothing$, то говорят, что множества A и B *пересекаются*. Если $A \cap B = \varnothing$, то в этом случае множества A и B называются *непересекающимися*.

Из определения пересечения следует, что $(\forall A, B)\ A \cap B \subseteq A$ и $A \cap B \subseteq B$.

Определение 1.9. *Разностью* $A \setminus B$ множеств A и B называется множество, состоящее из тех и только тех элементов, которые принадлежат множеству A и не принадлежат множеству B.

Таким образом, по определению, $A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}$.

Замечание 1.5. Если $B \subseteq A$, то в этом случае разность $A \setminus B$ называют *дополнением B до A*.

Определим, опираясь на определения 1.7–1.9, операции симметрической разности и дополнения множества.

Определение 1.10. *Симметрической разностью* (*кольцевой суммой*) $A \Delta B$ (или $A \oplus B$) множеств A и B называется множество, состоящее из тех и только тех элементов, которые принадлежат одному из множеств A либо B, но не являются их общими элементами.

Таким образом, по определению,

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

Определение 1.11. *Дополнением* $\overline{A}$ (или A') множества A (до универсума U) называется множество $U \setminus A$.

Таким образом, по определению, $\overline{A} = U \setminus A = \{x \mid x \in U \text{ и } x \notin A\}$.

Пример 1.5. Пусть $U = \{a, b, c, d, e, f, g, h\}$, $A = \{a, d, e, f, h\}$, $B = \{b, d, f, h\}$. Найти: $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, $A \Delta B$, $\overline{A}$, $\overline{B}$.

Решение. $A \cup B = \{a, b, d, e, f, h\}$, $A \cap B = \{d, f, h\}$, $A \setminus B = \{a, e\}$, $B \setminus A = \{b\} \Rightarrow A \setminus B \neq B \setminus A$, $A \Delta B = \{a, b, e\}$, $\overline{A} = \{b, c, g\}$, $\overline{B} = \{a, c, e, g\}$.

Введем некоторые обобщения вышеприведенных определений. Пусть I – любое конечное или бесконечное множество индексов. Тогда объединение или пересечение произвольного семейства множеств $\{A_i\}$, $i \in I$, определяется следующим образом:

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i, \text{хотя бы для одного } i (i \in I)\},\ \bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ для всех } i (i \in I)\}.$$

Если $I = \{1, 2, \ldots, n\}$, то используются записи $A_1 \cup A_2 \cup \ldots \cup A_n$ и $A_1 \cap A_2 \cap \ldots \cap A_n$, или $\bigcup_{i=1}^{n} A_i$ и $\bigcap_{i=1}^{n} A_i$.

Определение 1.12. Пусть E – некоторое семейство подмножеств множества A, то есть $E = \{E_i\}$, $i \in I$, где $(\forall\ i \in I)\ E_i \subseteq A$. Семейство E называется *по-*

крытием множества A, если каждый элемент множества A принадлежит хотя бы одному множеству семейства E.

Таким образом, $E = \{E_i\}$, $i \in I$, где $(\forall\ i \in I)\ E_i \subseteq A$ – покрытие множества $A \Leftrightarrow A = \bigcup_{i \in I} E_i$.

Пример 1.6. Пусть $A = \{a, b, c, d, e, f, g, h, i, j, k\}$. Выяснить, какие из следующих семейств являются покрытиями множества A:

$E_1 = \{\{a\}, \{c, d\}, \{f, g, h\}, \{i, j, k\}\}$;

$E_2 = \{\{i, j, k\}, \{e, f, g, h\}, \{a, b, c, d\}\}$;

$E_3 = \{\{a, f, i, k, d\}, \{b, c, g, h\}, \{d\}, \{e, j\}\}$;

$E_4 = \{\{c, d, e, f\}, \{a, b, c\}, \{i, j, k\}, \{g, k\}\}$.

Решение. Семейства E_2 и E_3 – покрытия множества A, а семейства E_1 и E_4 не являются покрытиями множества A.

Определение 1.13. Покрытие E называется *разбиением* множества A, если каждый элемент множества A принадлежит в точности одному множеству семейства E.

Таким образом, $E = \{E_i\}$, $i \in I$, где $(\forall\ i \in I)\ E_i \subseteq A$ – разбиение множества $A \Leftrightarrow$ A $= \bigcup_{i \in I} E_i$ и $E_i \cap E_j = \varnothing$, если $i \neq j$.

Пример 1.7. Пусть $B = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Выяснить, какие из следующих семейств образуют разбиения множества B:

$E_1 = \{\{1, 3, 5\}, \{2, 4, 6, 8\}, \{7, 9\}\}$;

$E_2 = \{\{5\}, \{2, 4, 8, 9\}, \{1, 6\}\}$;

$E_3 = \{\{1, 3, 7\}, \{4, 6, 8\}, \{2, 5, 6, 9\}\}$;

$E_4 = \{\{1\}, \{2\}, \{3\}, \{4\}, \{5\}, \{6\}, \{7\}, \{8\}, \{9\}\}$.

Решение. Среди перечисленных семейств только E_1 и E_4 образуют разбиения множества B. Семейство E_2 не является разбиением множества B, так как $B \neq \{5\} \cup \{2, 4, 8, 9\} \cup \{1,6\}$, а семейство E_3 – так как $\{4, 6, 8\} \cap \{2, 5, 6, 9\} \neq \varnothing$.

Рассмотрим основные, наиболее важные свойства операций объединения, пересечения и дополнения над множествами.

Свойства операций над множествами

Пусть задан универсум U. Тогда $(\forall\ A, B, C)\ A, B, C \subseteq U$ выполняются следующие свойства:

1. ***идемпотентность:***

   $A \cup A = A$ (идемпотентность $\cup$), $A \cap A = A$ (идемпотентность $\cap$);

2. ***коммутативность:***

   $A \cup B = B \cup A$ (коммутативность $\cup$), $A \cap B = B \cap A$ (коммутативность $\cap$);

3. ***ассоциативность:***

   $A \cup (B \cup C) = (A \cup B) \cup C$ (ассоциативность $\cup$),

   $A \cap (B \cap C) = (A \cap B) \cap C$ (ассоциативность $\cap$);

4. ***дистрибутивность:***
   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (дистрибутивность $\cup$ относительно $\cap$),
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (дистрибутивность $\cap$ относительно $\cup$);
5. ***поглощение:*** $(A \cap B) \cup A = A$, $(A \cup B) \cap A = A$;
6. ***свойства нуля:*** $A \cup \varnothing = A$, $A \cap \varnothing = \varnothing$;
7. ***свойства единицы:*** $A \cup U = U$, $A \cap U = A$;
8. ***инволютивность (свойство двойного дополнения):*** $\overline{\overline{A}} = A$;
9. ***законы де Моргана:*** $\overline{A \cap B} = \overline{A} \cup \overline{B}$, $\overline{A \cup B} = \overline{A} \cap \overline{B}$;
10. ***свойства дополнения:*** $A \cup \overline{A} = U$, $A \cap \overline{A} = \varnothing$;
11. ***выражение для разности:*** $A \setminus B = A \cap \overline{B}$.

Доказательство. Справедливость каждого из этих свойств можно доказать, используя утверждение 1.1 и замечание 1.3.

В качестве примера приведем доказательство дистрибутивности объединения относительно пересечения: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Пусть $X = A \cup (B \cap C)$, $Y = (A \cup B) \cap (A \cup C)$.

Надо доказать, что множества X и Y равны, то есть (a) $X \subseteq Y$; (b) $Y \subseteq X$.

$X \subseteq Y$, если каждый элемент множества X принадлежит множеству Y. Пусть $x \in A \cup (B \cap C)$. Тогда возможны два случая: (a_1) $x \in A$ и (a_2) $x \in B \cap C$.

В случае (a_1) $x \in A \cup B$ и $x \in A \cup C$; следовательно, $x \in Y$. В случае (a_2) $x \in B$ и $x \in C$, поэтому $x \in A \cup B$ и $x \in A \cup C$; отсюда $x \in Y$. Из произвольности элемента x следует, что $X \subseteq Y$.

Предложим теперь, что $y \in Y$; то есть $y \in (A \cup B) \cap (A \cup C)$, тогда $y \in A \cup B$ и $y \in A \cup C$.

При этом если $y \notin A$, то $y \in B$ и $y \in C$, значит $y \in B \cap C$; следовательно, $y \in A \cup (B \cap C)$. Если же $y \in A$, то $y \in A \cup (B \cap C) = X$. Из произвольности элемента y вытекает, что $Y \subseteq X$.

Из (a) и (b) следует равенство $X = Y$.

1.4. Диаграммы Эйлера – Венна

Для графического (наглядного) изображения множеств и их свойств используются диаграммы Эйлера – Венна (Леонард Эйлер (1707–1783) – швейцарский математик, механик и физик; Джон Венн (1834 – 1923) – английский логик). На них множество отождествляется с множеством точек на плоскости, лежащих внутри некоторых замкнутых кривых, например окружностей (так называемые круги Эйлера). В частности, универсальное множество U изображается множеством точек некоторого прямоугольника.

Проиллюстрируем с помощью диаграмм Эйлера – Венна введенные определения. На рисунках 1.1 – 1.5 результат выполнения операции выделен штриховкой.

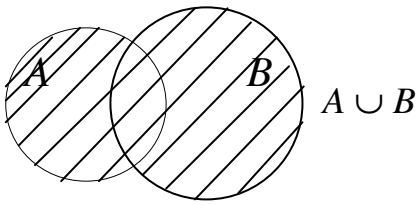


Рис. 1.1

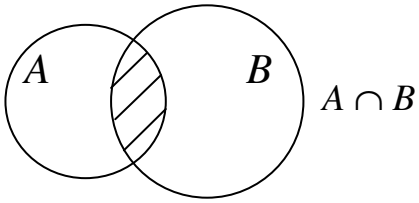


Рис. 1.2

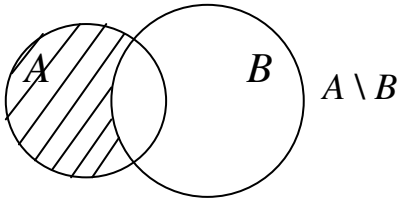


Рис. 1.3

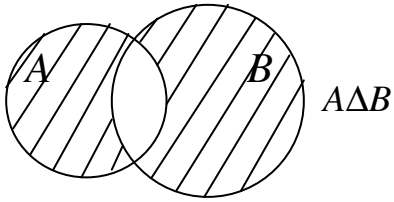


Рис. 1.4

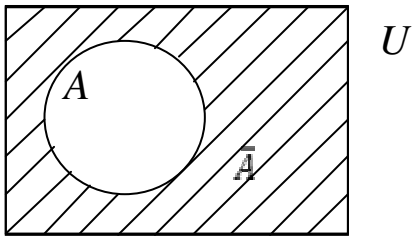


Рис. 1.5

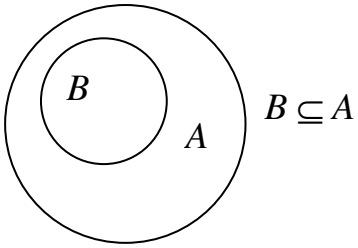


Рис. 1.6

1.5. Прямое произведение множеств

При задании некоторого конечного множества списком его элементов порядок указания элементов этого множества не имеет значения. Например, множества $\{a, b\}$ и $\{b, a\}$ совпадают, так как они состоят из одних и тех же элементов, хотя порядок указания элементов в этих записях различен. Кроме этого, каждый элемент входит в множество в точности один раз, то есть среди элементов множества нет повторяющихся. Так, запись $\{a, a\}$ означает множество, состоящее из единственного элемента a, то есть $\{a, a\} = \{a\}$.

Введем новое исходное понятие – понятие *упорядоченной пары* (a, b), которая представляет собой набор двух объектов a и b, не обязательно различных, первым элементом которого является a, а вторым – b.

Определение 1.14. Упорядоченные пары (a, b) и (c, d) называются *равными* (пишут $(a, b) = (c, d)$), если $a = b$ и $c = d$.

В частности, $(a, b) = (b, a) \Leftrightarrow a = b$ (сравните: из равенства $\{a, b\} = \{b, a\}$ не следует, что $a = b$).

Обобщением понятия упорядоченной пары является понятие *кортежа* (*вектора*) – упорядоченного набора произвольных, не обязательно различных n объектов. Кортеж, состоящий из элементов $x_1, x_2, \ldots, x_n$, обозначается $(x_1, x_2, \ldots, x_n)$ или $< x_1, x_2, \ldots, x_n >$. Элементы x_i $(i = 1, 2, \ldots, n)$ называются *координатами* или *компонентами* кортежа. Число координат называется *длиной кортежа* (*размерностью вектора*). Кортежи длины 2 называют также упорядоченными парами, кортежи длины 3 – упорядоченными тройками и т.д., кортежи длины n – упорядоченными n-ми («энками»).

Определение 1.15. Два кортежа $(x_1, x_2, \ldots, x_n)$ и $(y_1, y_2, \ldots, y_m)$ называются *равными* (пишут $(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_m)$), если:

1) $n = m$;
2) $x_i = y_i$ $(i = 1, 2, \ldots, n)$.

Введем еще одну операцию над множествами.

Определение 1.16. *Прямым* (*декартовым*) *произведением* $A_1 \times A_2 \times \ldots \times A_n$ n множеств $A_1, A_2, \ldots, A_n$ называется множество всех кортежей длины n $(x_1, x_2, \ldots, x_n)$ таких, что $x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n$.

Таким образом, по определению,

$A_1 \times A_2 \times \ldots \times A_n = \{(x_1, x_2, \ldots, x_n) \mid x_1 \in A_1, x_2 \in A_2, \ldots, x_n \in A_n\}$.

В частности, если $n = 2$, то $A \times B = \{(x, y) \mid x \in A, y \in B\}$.

Пример 1.8. Пусть $A = \{a, b, c\}$ и $B = \{1, 2\}$. Тогда

$A \times B = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$;

$B \times A = \{(1, a), (2, a), (1, b), (2, b), (1, c), (2, c)\}$;

$A \times A = \{(a, a), (b, b), (c, c)\}$; $B \times B = \{(1, 1),(2, 2)\}$.

Если $A_1 = A_2 = \ldots = A_n = A$, то множество $A_1 \times A_2 \times .. \times A_n = A \times A \times \underset{n \text{ раз}}{\ldots} \times A$ называется *n-кратным прямым произведением множества A* или *n-й степенью множества A* и обозначается через A^n. При этом будем считать, что $A^1 = A$.

Рассмотрим ***геометрическую интерпретацию прямого произведения двух числовых множеств*** A и B – множество всех точек координатной плоскости Oxy с координатами (x, y) такими, что $x \in A$, а $y \in B$. Тогда для двух заданных числовых множеств можно наглядно изображать их прямое произведение и, обратно, по изображению прямого произведения двух множеств определять их элементы.

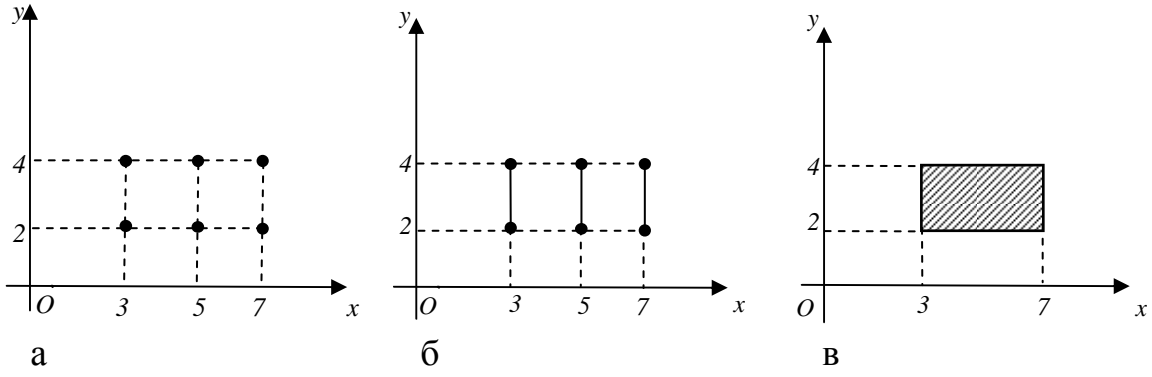
Пример 1.9. Изобразить на координатной плоскости Oxy $A \times B$, если:

а) $A = \{3, 5, 7\}$, $B = \{2, 4\}$;

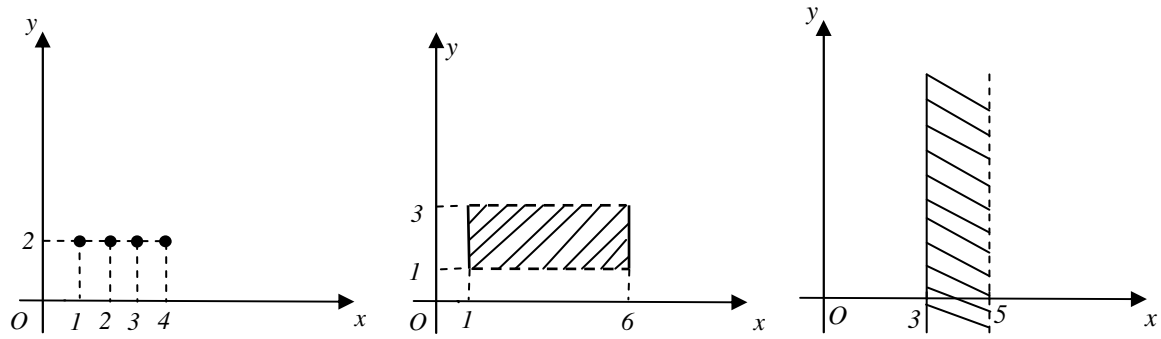
б) $A = \{3, 5, 7\}$, $B = [2; 4]$;

в) $A = [3, 7]$, $B = [2; 4]$.

Решение.



Пример 1.10. Определить, прямое произведение каких множеств A и B изображено на рисунках:



а б в

Решение. а – $A = \{1,2,3,4\}$, $B = \{2\}$; б – $A = [1;6]$, $B = (1;3)$; в – $A = [3;5)$, $B = R$.

1.6. Метод математической индукции

Метод математической индукции используется для доказательства утверждений, в формулировке которых участвует натуральный параметр n. Он основан на так называемом *принципе математической индукции* (одна из аксиом формальной теории натуральных чисел): утверждение «для любого $n \in N$ выполняется $P(n)$» считается доказанным, если оно доказано для $n = 1$ и для любого натурального числа k из предположения, что $P(n)$ истинно для $n = k$, доказана его истинность для $n = k + 1$.

Запись принципа математической индукции в символической форме выглядит так: $[P(1) \wedge (\forall k \in N)(P(k) \Rightarrow P(k+1))] \Rightarrow (\forall n \in N)\, P(n)$.

Для доказательства утверждений методом математической индукции используется схема рассуждений, состоящая из следующих этапов:

1. *База индукции.* Доказывается истинность утверждения $P(n)$ для $n = 1$ (обычно это удается сделать непосредственной проверкой).
2. *Индуктивное предположение*. Допускается, что утверждение $P(n)$ верно для всех $1 \le n \le k$.
3. *Индукционный переход*. Исходя из индуктивного предположения, доказывается истинность $P(n)$ для $n = k + 1$.
4. *Вывод.* На основании первых трех этапов и принципа математической индукции делается вывод о справедливости утверждения для любого $n \in N$.

Замечание 1.6. Если требуется доказать утверждение $P(n)$, где $n \in N_0$, то база индукции начинается с $n = 0$.

Замечание 1.7. Иногда бывает нужно доказать справедливость некоторого утверждения $P(n)$, зависящего от натурального параметра n, для всех $n \ge m$, где m – фиксированное натуральное число. В этом случае принцип математической индукции можно записать в виде:

$[P(m) \wedge (\forall k \ge m)(P(k) \Rightarrow P(k+1))] \Rightarrow (\forall n \ge m)\, P(n)$.

Замечание 1.8. С помощью принципа математической индукции можно давать индукционные определения. При этом для определения понятия

$P(n)$ ($n \in N$), во-первых, задается значение $P(1)$; во-вторых, для любого натурального числа k задается правило получения значения $P(k + 1)$ по числу k и значению $P(k)$.

Пример 1.11. Доказать, что для любого натурального числа n справедливо равенство: $\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)}=\frac{n}{n+1}$.

Доказательство. Обозначим через $S(n)$ левую часть равенства, а через $R(n)$ правую: $S(n)=\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{n(n+1)}$, $R(n)=\frac{n}{n+1}$.

Докажем истинность данного равенства методом математической индукции.

1. *База индукции*. Проверим истинность равенства при $n=1$:

$S(1)=\frac{1}{1\cdot 2}=\frac{1}{2}$, $R(1)=\frac{1}{1+1}=\frac{1}{2}$, $S(1) = R(1)$, значит, данное равенство верно для $n=1$.

2. *Индуктивное предположение*. Предположим истинность равенства при $n=k$:

$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{k(k+1)}=\frac{k}{k+1}$, то есть $S(k)=R(k)$.

3. *Индукционный переход*. Докажем истинность равенства при $n=k+1$:

$\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{k(k+1)}+\frac{1}{(k+1)(k+2)}=\frac{k+1}{k+2}$. Преобразуем левую часть этого равенства:

$$S(k+1)=\frac{1}{1\cdot 2}+\frac{1}{2\cdot 3}+\frac{1}{3\cdot 4}+\cdots+\frac{1}{k\cdot(k+1)}+\frac{1}{(k+1)(k+2)}=S(k)+\frac{1}{(k+1)(k+2)}.$$

Так как в силу индуктивного предположения $S(k)=R(k)$, то $S(k+1)=R(k)+\frac{1}{(k+1)\cdot(k+2)}$. Поскольку $R(k)=\frac{k}{k+1}$, то $S(k+1)=\frac{k}{k+1}+\frac{1}{(k+1)(k+2)}$.

Приведем дроби к общему знаменателю, сложим их и, воспользовавшись формулой сокращенного умножения, выполним сокращение:

$$S(k+1)=\frac{k\cdot(k+2)}{(k+1)(k+2)}+\frac{1}{(k+1)(k+2)}=\frac{k^2+2k+1}{(k+1)(k+2)}=\frac{(k+1)^2}{(k+1)(k+2)}=\frac{k+1}{k+2}.$$

$R(k+1)=\frac{k+1}{(k+1)+1}=\frac{k+1}{k+2}$, значит, $S(k+1)=R(k+1)$.

Получили, что из истинности равенства при $n=k$ (k – произвольное натуральное число) следует его истинность при $n=k+1$.

4. На основании пунктов 1 – 3, приведенных выше, и принципа математической индукции следует, что данное равенство истинно для любого $n \in N$.

1.7. Соответствия

Определение 1.17. *Соответствием* между множествами A и B (между элементами множеств A и B) называется подмножество $R \subseteq A \times B$.

Если $(a, b) \in R$, то говорят, что элемент b соответствует элементу a при соответствии R.

Проиллюстрировать соответствия между двумя различными множествами можно с помощью диаграмм, которые в дальнейшем будут называться *графами соответствий*. На них множества изображаются с помощью кругов (или любых других связных фигур) на плоскости, а элементы множеств – точками внутри соответствующих кругов. Каждой упорядоченной паре (a, b) из соответствия R сопоставляется отрезок прямой (или любая другая линия без самопересечений), соединяющий точки a и b и имеющий направление, указываемое стрелкой, от первого элемента упорядоченной пары ко второму.

Пример 1.12. Пусть $A = \{a, b, c, d, e\}$ и $B = \{1, 2, 3, 4\}$. Соответствие R между множествами A и B задано списком его элементов:
$R = \{(a, 2), (b, 1), (c, 2), (d, 4)\}$.

На рис. 1.7 представлен граф соответствия R.

Определение 1.18. Множество всех первых элементов упорядоченных пар, входящих в соответствие R, называется его *областью определения* и обозначается через $Dom\ R$. $R \subseteq A \times B \Rightarrow Dom R = \{x \in A \mid \exists y \in B : (x; y) \in R\}$.

Здесь и далее знак «:» заменяет слова «такой, что».

Определение 1.19. Множество всех вторых элементов упорядоченных пар, входящих в соответствие R, называется его *областью значений* и обозначается через $Im\ R$.

$R \subseteq A \times B \Rightarrow \mathrm{Im} R = \{y \in B \mid \exists a \in A : (x; y) \in R\}$.

Пример 1.13. Найдем область определения и область значений соответствия R из примера 1.12: $Dom\ R = \{a, b, c, d\}$, $Im\ R = \{1, 2, 4\}$.

Определение 1.20. Если $Dom\ R = A$, то соответствие R называется *всюду* (*полностью*) *определенным*. В противном случае соответствие R называется *частичным* (*частично определенным*).

Определение 1.21. Если $Im\ R = B$, то соответствие R называется *сюръективным* (*сюръекцией*).

Пример 1.14. На рис. 1.7 изображен граф частичного соответствия R, так как $Dom\ R \neq A$. Соответствие S, граф которого представлен на рис. 1.8, является всюду определенным и сюръективным, так как $Dom\ S = \{a, b, c, d, e\} = A$ и $Im\ S = \{1, 2, 3, 4\} = B$.

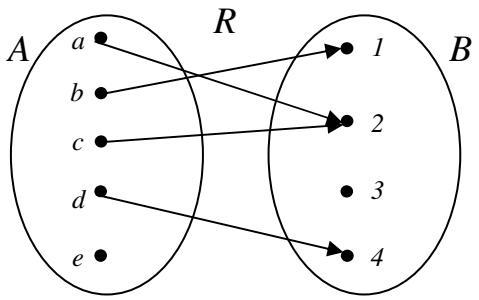


Рис. 1.7

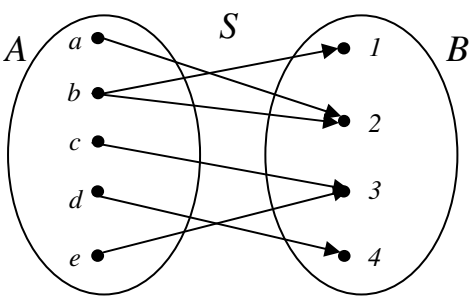


Рис. 1.8

Определение 1.22. Множество всех $b \in B$, соответствующих элементу $a \in A$, называется *образом элемента a* в *B* при соответствии *R* и обозначается через $R(a)$.

Определение 1.23. Множество всех $a \in A$, которым соответствует элемент $b \in B$, называется *прообразом элемента b* в *A* при соответствии *R* и обозначается через $R^{-1}(b)$.

Определение 1.24. Если $C \subseteq Dom\ R$, то *образом множества C* при соответствии *R* называется объединение образов всех элементов множества *C* и обозначается через $R(C)$.

Определение 1.25. Если $D \subseteq Im\ R$, то *прообразом множества D* при соответствии *R* называется объединение прообразов всех элементов множества *D* обозначается через $R^{-1}(D)$.

Пример 1.15. Рассмотрим соответствие *S* (см. рис. 1.8). Тогда $S(a) = 2$, $S(b) = \{1, 2\}$, $S^{-1}(3) = \{c, e\}$, $S^{-1}(4) = \{d\}$. Если $C = \{a, c, d\}$, $D = \{1, 2, 3\}$, то $S(C) = \{2, 3, 4\}$ и $S^{-1}(D) = \{a, b, c, e\}$.

Определение 1.26. Соответствие *R* называется *инъективным* (*инъекцией*), если прообразом любого элемента из *Im R* является единственный элемент из $Dom\ R = A$.

Определение 1.27. Соответствие *R* называется *функциональным* (или однозначным), если образом любого элемента из *Dom R* является единственный элемент из *Im R*.

Определение 1.28. Соответствие *R* между множествами *A* и *B* называется *взаимно однозначным* (*биекцией*), если оно всюду определено, сюръективно, функционально и инъективно.

Другими словами, соответствие между *A* и *B* является взаимно однозначным, если каждому элементу множества *A* сопоставляется единственный элемент множества *B* и каждый элемент множества *B* соответствует единственному элементу множества *A*.

Пример 1.16. На рис. 1.7 – 1.10 изображены графы соответствий *R*, *S*, *P* и *Q*. Соответствие *S* (см. рис. 1.8) не является инъективным, так как, например, $\left|R^{-1}(3) \neq 1\right|$. Соответствие *P* (рис. 1.9) инъективно, так как $(\forall\ b \in Im\ P)\ \left|R^{-1}(b) = 1\right|$.

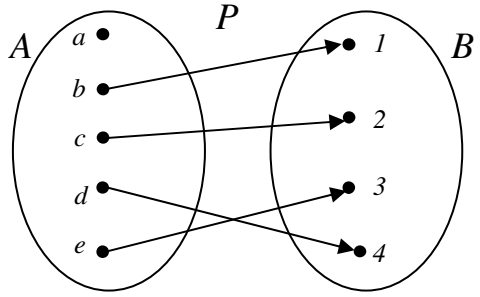


Рис. 1.9

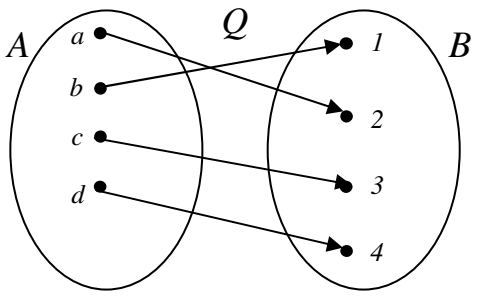


Рис. 1.10

Среди соответствий *R*, *S*, *P* и *Q* функциональными являются соответствия *R* (рис. 1.7), *P*, *Q* (рис. 1.10), и только *Q* – взаимно однозначное соответствие между *A* и *B*.

Утверждение 1.2. Если между конечными множествами *A* и *B* существует взаимно однозначное соответствие, то мощности этих множеств равны.

Доказательство. Предположим противное. Пусть $|A| \neq |B|$. Тогда либо $|A| > |B|$, либо $|A| < |B|$.

Если $|A| > |B|$, то в множестве A существуют по крайней мере два различных элемента, которым соответствует один и тот же элемент из множества B, так как соответствие всюду определено. Это означает, что соответствие не является инъективным, что противоречит условию утверждения.

Если $|A| < |B|$, то в множестве B существует по крайней мере два различных элемента, соответствующих одному и тому же элементу из множества A, так как соответствие сюръективно. Следовательно, соответствие не является функциональным, что также противоречит условию утверждения.

Замечание 1.9. На основании утверждения 1.2 можно выполнить следующие действия:

1) установить равенство мощностей двух множеств, не вычисляя этих мощностей;
2) вычислить мощность множества, установив его взаимно однозначное соответствие с множеством, мощность которого известна или легко вычисляется.

1.8. Задачи, связанные с определением мощности конечного множества

Теорема 1.1. Если A – конечное множество, то мощность его булеана $P(A)$ равна $2^{|A|}$.

Доказательство. Пусть $|A| = n$. Будем использовать математическую индукцию по n.

1. *База индукции*. Если $n = 0$, то $A = \varnothing$ и $P(A) = \{\varnothing\}$. Следовательно, $|P(A)| = |\{\varnothing\}| = 1 = 2^0 = 2^{|A|}$.
2. *Индуктивное предположение.* Пусть для любого множества A мощности $n < k$ теорема справедлива, то есть $|P(A)| = 2^{|A|} = 2^n$.
3. *Индукционный переход.* Докажем справедливость теоремы для $n = k$. Рассмотрим $A = \{a_1, a_2, \ldots, a_k\}$, $|A| = k$. Положим $A_1 = \{X \in P(A) | a_k \in X\}$ и $A_2 = \{Y \in P(A) | a_k \notin Y\}$. Имеем: $P(A) = A_1 \cup A_2$ и $A_1 \cap A_2 = \varnothing$. Между элементами множеств A_1 и A_2 можно установить следующее взаимно однозначное соответствие: каждому элементу X множества A_1 сопоставить элемент $Y = X \setminus \{a_k\}$ множества A_2. Тогда, по утверждению 1.2, $|A_1| = |A_2|$. Так как $A_2 = P(\{a_1, a_2, \ldots, a_{k-1}\})$, то, по индукционному предположению, $|A_1| = |A_2| = 2^{k-1}$ и $|P(A)| = |A_1| + |A_2| = 2^{k-1} + 2^{k-1} = 2 \cdot 2^{k-1} = 2^k = 2^{|A|}$. Следовательно, теорема верна для любых n.

Теорема 1.2. Пусть $X_1, X_2, \ldots, X_n$ $(n \geq 2)$ – конечные множества и

$|X_1| = m_1$, $|X_2| = m_2$, …, $|X_n| = m_n$. Тогда мощность множества $X_1 \times X_2 \times \ldots \times X_n$ равна произведению мощностей $X_1, X_2, \ldots, X_n$: $|X_1 \times X_2 \times \ldots \times X_n| = m_1 \cdot m_2 \cdot \ldots \cdot m_n$.

Доказательство. Воспользуемся методом математической индукции по n.

1. *База индукции*. Очевидно, что для $n = 1$ теорема верна.
2. *Индуктивное предположение.* Пусть теорема справедлива для $n = k$.
3. *Индукционный переход*. Докажем справедливость теоремы для $n = k + 1$. Возьмем произвольный кортеж $(x_1, x_2, \ldots, x_k) \in X_1 \times X_2 \times \ldots \times X_k$ и припишем справа элемент $x_{k+1} \in X_{k+1}$. Так как $|X_{k+1}| = m_{k+1}$, то это можно сделать m_{k+1} разными способами. В результате получим m_{k+1} различных кортежей из $X_1 \times X_2 \times \ldots \times X_{k+1}$. По индуктивному предположению, $|X_1 \times X_2 \times \ldots \times X_k| = m_1 \cdot m_2 \cdot \ldots \cdot m_k$. Следовательно, из всех $m_1 \cdot \ldots \cdot m_k$ кортежей из $X_1 \times X_2 \times \ldots \times X_k$ приписыванием справа элемента из X_{k+1} можно получить $m_1 \cdot \ldots \cdot m_k \cdot m_{k+1}$ кортежей из $X_1 \times X_2 \times \ldots \times X_{k+1}$, причем все они различны, и никаких других кортежей в $X_1 \times X_2 \times \ldots \times X_{k+1}$ не содержится. Поэтому теорема верна для $n = k+1$, следовательно, верна для любых n.

Следствие. $|X^n| = |X|^n$.

Поставим задачу подсчитать мощность объединения n конечных множеств, которые могут иметь непустые пересечения между собой.

Пусть X_1, X_2 – два конечных множества. Если $X_1 \cap X_2 = \varnothing$, то $|X_1 \cup X_2| = |X_1| + |X_2|$. Если теперь $X_1 \cap X_2 \neq \varnothing$, то в $|X_1 \cup X_2|$ каждый элемент из $X_1 \cap X_2$ будет учтен два раза. Следовательно,

$$|X_1 \cup X_2| = |X_1| + |X_2| - |X_1 \cap X_2|. \qquad (1)$$

В общем случае имеет место следующая теорема.

Теорема 1.3 (*включений и исключений*). Пусть $X_1, X_2, \ldots, X_n$ ($n \geq 2$) – конечные множества. Тогда

$$|X_1 \cup \ldots \cup X_n| = \sum_{1 \leq i_1 \leq n} |X_{i_1}| - \sum_{1 \leq i_1 < i_2 \leq n} |X_{i_2} \cap X_{i_2}| + \ldots + (-1)^{k+1} \cdot \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} |X_{i_1} \cap X_{i_2} \cap \ldots \cap X_{i_k}| + \ldots$$

$$+ (-1)^{n+1} \cdot |X_1 \cap X_2 \cap \ldots \cap X_n| = (|X_1| + \ldots + |X_n|) - (|X_1 \cap X_2| + |X_1 \cap X_3| + \ldots + |X_{n-1} \cap X_n|) +$$

$$+ (|X_1 \cap X_2 \cap X_3| + \ldots + |X_{n-2} \cap X_{n-1} \cap X_n|) - \ldots + (-1)^{n+1} \cdot |X_1 \cap \ldots \cap X_n|. \qquad (2)$$

Доказательство. Доказательство проведем методом математической индукции по n.

1. *База индукции*. Для $n = 2$ формула (2) совпадает с (1).
2. *Индуктивное предположение.* Пусть формула (2) верна для случая $n - 1$ множеств, где $n \geq 3$.
3. *Индукционный переход*. Докажем справедливость формулы (2) для n множеств. Для этого разобьем множества $X_1, X_2, \ldots, X_n$ на две группы: $X_1, X_2, \ldots, X_{n-1}$ и X_n. Тогда согласно формуле (1) получаем

$$|X_1 \cup \ldots \cup X_n| = |(X_1 \cup \ldots \cup X_{n-1}) \cup X_n| = |(X_1 \cup \ldots \cup X_{n-1})| + |X_n| - |(X_1 \cup \ldots \cup X_{n-1}) \cap X_n| =$$

$$= |(X_1 \cup \ldots \cup X_{n-1})| + |X_n| - |Y_1 \cup \ldots \cup Y_{n-1}|, \qquad (3)$$

где $Y_i = X_i \cap X_n$, $i = 1, 2, \ldots, n-1$.

По индуктивному предположению, имеем:

$$|X_1 \cup \ldots \cup X_{n-1}| = (|X_1| + \ldots + |X_{n-1}|) - (|X_1 \cap X_2| + |X_1 \cap X_3| + \ldots + |X_{n-2} \cap X_{n-1}|) +$$
$$+ (|X_1 \cap X_2 \cap X_3| + \ldots + |X_{n-3} \cap X_{n-2} \cap X_{n-1}|) - \ldots + (-1)^n |X_1 \cap \ldots \cap X_{n-1}|; \quad (4)$$

$$|Y_1 \cup \ldots \cup Y_{n-1}| = (|Y_1| + \ldots + |Y_{n-1}|) - (|Y_1 \cap Y_2| + |Y_1 \cap Y_3| + \ldots + |Y_{n-2} \cap Y_{n-1}|) +$$
$$+ (|Y_1 \cap Y_2 \cap Y_3| + \ldots + |Y_{n-3} \cap Y_{n-2} \cap Y_{n-1}|) - \ldots + (-1)^n |Y_1 \cap \ldots \cap Y_{n-1}| =$$
$$= (|X_1 \cap X_n| + \ldots + |X_{n-1} \cap X_n|) - (|X_1 \cap X_2 \cap X_n| + |X_1 \cap X_3 \cap X_n| + \ldots + |X_{n-2} \cap X_{n-1} \cap X_n|) + \ldots +$$
$$+ (-1)^n \cdot |X_1 \cap \ldots \cap X_n|. \quad (5)$$

Из (3), учитывая (4) и (5), получаем формулу (2).

Формула (2) называется *формулой включений и исключений*. Ее частный случай при $n = 3$ имеет вид:

$$|X_1 \cup X_2 \cup X_3| = |X_1| + |X_2| + |X_3| - |X_1 \cap X_2| - |X_1 \cap X_3| - |X_2 \cap X_3| + |X_1 \cap X_2 \cap X_3|. \quad (6)$$

Следствие. Пусть X – конечное множество, $X_1, X_2, \ldots, X_n$ – подмножества X. Тогда

$$|X \setminus (X_1 \cup \ldots \cup X_n)| = |X| - (|X_1| + \ldots + |X_n|) + (|X_1 \cap X_2| + \ldots + |X_{n-1} \cap X_n|) -$$
$$- \ldots + (-1)^n |X_1 \cap \ldots \cap X_n|. \quad (7)$$

Доказательство. Рассмотрим множества $X \setminus (X_1 \cup \ldots \cup X_n)$ и $X_1 \cup \ldots \cup X_n$. Имеем

$$[X \setminus (X_1 \cup \ldots \cup X_n)] \cup (X_1 \cup \ldots \cup X_n) = X, \; [X \setminus (X_1 \cup \ldots \cup X_n)] \cap (X_1 \cup \ldots \cup X_n) = \varnothing.$$

Тогда согласно формуле (1)

$$|[X \setminus (X_1 \cup \ldots \cup X_n)] \cup (X_1 \cup \ldots X_n)| = |X| = |X \setminus (X_1 \cup \ldots \cup X_n)| + |X_1 \cup \ldots X_n|,$$

и, следовательно,

$$|X \setminus (X_1 \cup \ldots \cup X_n)| = |X| - |X_1 \cup \ldots \cup X_n|. \quad (8)$$

Подставляя (2) в (8), получаем формулу (7).

Пример 1.17. Студенты третьего курса, изучающие информационные технологии в университете, могут изучать и дополнительные дисциплины по выбору. В этом году 30 из них выбрали дисциплину «Информационные технологии моделирования интерьера», 35 предпочли дисциплину «Информационные технологии в рекламе», а 20 решили изучать дисциплину «Информационные технологии моделирования ландшафта». Кроме того, 15 студентов изъявили желание посещать «Информационные технологии моделирования интерьера» и «Информационные технологии в рекламе», 7 – «Информационные технологии в рекламе» и «Информационные технологии моделирования ландшафта», 10 – «Информационные технологии моделирования интерьера» и «Информационные технологии моделирования ландшафта», 3 – все три дисциплины. Сколько студентов выбрали по крайней мере одну дополнительную дисциплину? Сколько из них предпочли только дисциплину «Информационные технологии в рекламе»?

Решение. Пусть A – множество студентов, выбравших дисциплину «Информационные технологии моделирования интерьера», B –

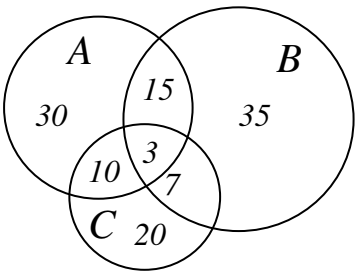


Рис. 1.11

«Информационные технологии в рекламе», *C* – «Информационные технологии моделирования ландшафта». Для составления математической модели задачи удобно использовать диаграммы Эйлера – Венна. Из диаграммы (рис. 1.11) видно, что на теоретико-множественном языке формулировка первого вопроса – «Чему равна мощность множества $A \cup B \cup C$?», а второго – «Какова мощность множества $B \setminus [(A \cap B) \cup (B \cap C)]$?».

На основании формулы (6), имеем:

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |A \cap C| + |A \cap B \cap C| = 30 + 35 + 20 - 15 - 10 - 7 + 3 = 56.$

Используя последовательно формулы (8) и (1), получаем:

$|B \setminus [(A \cap B) \cup (B \cap C]| = |B| - |(A \cap B) \cup (B \cap C)| = |B| - [|A \cap B| + |B \cap C| - |A \cap B \cap C|] =$

$= 35 - (15 + 7 - 3) = 16.$

Таким образом, 56 студентов выбрали по крайней мере одну дополнительную дисциплину и 16 – только дисциплину «Информационные технологии в рекламе».

Задачи и упражнения к главе 1

1. Какие из следующих высказываний истинны и какие ложны? Дайте обоснование ответа:
   а) $\pi \in R$;
   б) $\cos \frac{\pi}{3} \in Q$;
   в) $0{,}1010010001... \in Q$;
   г) $\varnothing \in \varnothing$;
   д) $\varnothing \in \{\varnothing\}$;
   е) $a \in \{\{a, b\}\}$;
   ж) $\{a, b\} \in \{\{a, b\}\}$;
   з) $\{a, b\} \in \{\{a, b\}; \{a, c\}; a; b\}$.
2. Равны ли множества:
   а) $\{1, 3, 5\}$ и $\{1, 3, 5, 1\}$;
   б) $\{11, 13\}$ и $\{\{11, 13\}\}$;
   в) $\{a, b, c\}$ и $\{a, b, a, c\}$;
   г) $\{a, b, c\}$ и $\{\{a\}, \{b\}, \{c\}\}$;
   д) $\{\{a, b\}, c\}$ и $\{a, \{b, c\}\}$;
   е) $\{x \in R \mid 22 \le x \le 3\}$ и $\varnothing$.
3. Вставьте между множествами символ $\in$ или $\subseteq$ так, чтобы получилось истинное высказывание:
   а) $\{1\}$ и $\{1, \{1, 2\}\}$;
   б) $\{1, 2\}$ и $\{1, 2, \{1\}, \{2\}\}$;

в) $\{1, 2\}$ и $\{1, 2, \{1, 2\}\}$;

г) $\varnothing$ и $\{1, 2, \{1\}, \{\varnothing\}\}$;

д) $\varnothing$ и $\{\varnothing\}$;

е) $\varnothing$ и $\{\{\varnothing\}\}$;

ж) $\{1, 2\}$ и $\{1, 2\}$.

4. Известно, что $x \in A$. Следует ли отсюда, что:
   а) $x \in A \cap B$; б) $x \in A \cup B$.
5. Известно, что $y \in A \cup B$. Следует ли отсюда, что $y \in A$?
6. Известно, что $z \in A$. Следует ли отсюда, что $z \in A \setminus B$?
7. Даны множества $A = \{a, b, c, d\}$, $B = \{a, b, 4\}$, $C = \{4, 2, c\}$, $D = \{a, b, 3\}$, $E = \{1, b\}$. Найдите a, b, c, d, зная, что $B \subseteq A$, $C \subseteq A$, $D \subseteq A$, $E \subseteq B$.
8. Изобразите с помощью кругов Эйлера – Венна, в каком отношении находятся множества: U – множество четырехугольников плоскости; A – трапеций; B – параллелограммов; C – ромбов; D – прямоугольников; E – квадратов; F – четырехугольников с перпендикулярными диагоналями, G – четырехугольников, диагонали которых делят друг друга пополам.
9. Найдите $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, $A \Delta B$, $\overline{A}$, $\overline{B}$, если $A = \{1, 2, 3\}$, $B = \{2, 3, 4, 5\}$, $U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
10. Найдите $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, если:
    а) $A = \{a, b, c, d, e\}$, $B = \{a, c, e\}$;
    б) $A = \{a, b, c, d, e\}$, $B = \{k, l, m\}$;
    в) $A = \{a, b, c, d, e\}$, $B = \varnothing$.
11. Найдите $A \cup B$, $A \cap B$, $A \setminus B$, $B \setminus A$, если
    а) $A = [2; +\infty)$, $B = (1; 7]$;
    б) $A = [-7; -4]$, $B = (0; 3)$;
    в) $A = (-\infty; 10)$, $B = [-1; 5)$;
    г) A=[0; 3], B=[3; 6).
12. Даны множества $A = \{1, 2, 4, 6, 8\}$, $B = \{3, 4, 6\}$, $C = \{1, 5, 7\}$, $U = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Найти: а) $(A \cap \overline{B}) \setminus (A \cup C)$; б) $(A \cup C) \setminus (A \cap \overline{B})$; в) $\overline{B} \setminus (A \cup C)$; г) $A \Delta B$; д) $A \Delta C$.
13. Упростить выражения, используя свойства операций над множествами:
    а) $(A \cap B \cap C) \cup (\overline{A} \cap B \cap C) \cup \overline{B} \cup \overline{C}$;
    б) $\overline{(A \cup B) \cap (\overline{A} \cup B) \cap (A \cup \overline{B})}$;
    в) $\overline{A} \cup \overline{(A \cup \overline{B} \cap \overline{C})} \cup (B \cap \overline{(A \cup C)})$.
    г) $(A \cap B \cap C \cap \overline{D}) \cup (\overline{A} \cap C) \cup (\overline{B} \cap C) \cup (C \cap D)$;
    д) $(\overline{A} \cup B \cup \overline{C}) \cap (A \cap \overline{B} \cap C) \cap \overline{(A \cup C)}$;
    е) $A \Delta A \Delta A$.

14. В классе 32 учащихся. Из них 18 посещают химический кружок, 12 – биологический, 8 учеников не посещают ни одного из этих кружков. Сколько учени-

ков посещают и химический, и биологический кружок? Сколько учащихся посещают только химический кружок?

15. В группе 30 студентов, из них 18 увлекаются плаванием, а 17 – волейболом.

а) Каким может быть минимальное число студентов, увлекающихся обоими видами спорта?

б) Каким может быть минимальное число студентов, увлекающихся хотя бы одним видом спорта?

16. Среди написанных на доске чисел, полученных случайным образом, 65% делятся на 2, 70% – на 3, 75% – на 5. Каков наименьший процент чисел, кратных 30?

17. Все студенты первого курса КГТУ специальности «ИС» изучают три языка программирования. В этом году 19 студентов предпочли изучать Pascal, 14 выбрали Basic, а 17 решили заниматься Delphi. Кроме того, было 4 студента, слушающих курс по Pascal и Basic, трое изучают Pascal и Delphi, трое – Delphi и Basic. Известно, что никто из студентов не отважился посещать сразу три курса. Сколько студентов в группе «ИС»? Сколько из них были увлечены только Delphi?

18. Опрошено 220 аквариумистов, 85 из них разводят дома сомов, 95 предпочитают гуппи, 100 – золотых рыбок, 26 – сомов и золотых рыбок, 22 – гуппи и золотых рыбок, 17 – сомов и гуппи, 5 опрошенных любуются в своем аквариуме на все три вида рыбок.

а) Сколько аквариумистов держат в своем аквариуме сомов, но не имеют гуппи?

б) Сколько аквариумистов разводят сомов или гуппи, но не любят золотых рыбок?

в) У скольких аквариумистов нет ни сомов, ни гуппи?

г) Сколько аквариумистов разводят не только гуппи?

д) У скольких аквариумистов есть гуппи и золотые рыбки, но нет сомов?

19. Статисты опросили 100 посетителей туристического агентства «Золотой пляж». Выяснилось, что за последние 5 лет 50 человек отдыхали в Турции, среди которых 20 человека были еще и в Греции, 18 человек еще и в Египте, и пять человек побывали за пять лет во всех трех упомянутых странах. С достопримечательностями Греции из всех опрошенных познакомились 50 человек, среди которых 26 человек побывали только в двух странах. Сколько человек посетили страну пирамид?

20. По итогам экзаменов из 40 студентов отличную оценку по математике имели 11 студентов, по физике – 15, по химии – 13, по математике и физике – 4, по математике и химии – 3, по физике и химии – 3, по всем трем предметам – 1. Сколько студентов получили хотя бы по одной отличной оценке?

21. В мае было 12 дождливых, 8 ветреных, 4 холодных, 5 дождливых и ветреных, 3 дождливых и холодных, 2 ветреных и холодных дней, а один день был и дождливый, и ветреный, и холодный. В течение скольких дней в мае было тепло без ветра и без дождя?

22. Каждый из 100 костромичей, отдыхающих этим летом в Анапе, был на экскурсиях, в дельфинарии или в аквапарке. Из них аквапарк посетили 67 человек,

экскурсии – 82, дельфинарий – 67, экскурсии и дельфинарий – 53, экскурсии и аквапарк – 58, дельфинарий и аквапарк – 51. Сколько костромичей было на всех трех мероприятиях?

23. Староста курса представил следующий отчет о физкультурной работе. Всего – 45 студентов. Футбольная секция – 25 человек, баскетбольная секция – 30, шахматная секция – 28, футбольная и баскетбольная – 16, футбольная и шахматная – 18, баскетбольная и шахматная – 17. В трех секциях одновременно занимаются 15 человек. Объясните, почему отчет не был принят?

24. В клубе по борьбе с человеческими страхами из 100 человек 60 боятся пауков, 54 – змей, 55 – мышей, 38 боятся пауков и змей, 34 – змей и мышей, 40 – пауков и мышей, и 20 человек боятся замкнутого пространства.

а) Сколько человек боится пауков или мышей, но не боятся змей?

б) Сколько человек боится только одного вида животных?

в) Сколько человек боится двух из трех видов животных?

г) Сколько человек не боится ни змей, ни пауков?

д) Сколько человек боится только змей?

25. Среди счастливчиков, кому повезло поймать золотую рыбку, пожелавших новую квартиру оказалось 18 человек, дорогую машину – 14, хорошую работу – 28, квартиру и машину – 5, квартиру и работу – 10, машину и работу – 8, все три желания загадало 3 человека. Сколько всего человек поймали золотую рыбку? Сколько среди них загадавших только одно желание?

26. В лыжной, хоккейной и конькобежной секциях 38 студентов потока. Известно, что в лыжной секции занимается 21 студент, среди которых 3 студента занимались еще в конькобежной секции, 6 студента еще в хоккейной секции и один студент занимался одновременно во всех трех секциях. В конькобежной секции занимались 13 студентов, среди которых 5 студентов занимались одновременно в двух секциях. Сколько студентов занималось в хоккейной секции?

27. Преподаватель решил узнать, кто из 40 студентов курса читал книги A, B и C. Результаты опроса оказались таковы: книгу A читали 25 студентов, книгу B – 22, книгу C – также 22. Книгу A или B читали 33 студента, A или C – 32, B или C – 31; все три книги прочли 10 студентов. Сколько студентов прочли только по одной книге? Сколько студентов не читали ни одной из этих трех книг?

28. В группе 25 учащихся. Из них 13 лыжников, 8 пловцов, 17 велосипедистов. Причем каждый спортсмен занимается только двумя видами спорта и учится на «3» или на «4». В группе 6 круглых отличников. Сколько в группе спортсменов? Сколько в группе неуспевающих?

Глава 2. Комбинаторика

Комбинаторика – раздел дискретной математики, который посвящен решению задач пересчета и перечисления элементов множества (обычно конечного), обладающих заданным набором свойств.

Если требуется найти число элементов, принадлежащих данному множеству и обладающих заданными свойствами, то это ***задача пересчета***. Если необходимо выделить все элементы множества, удовлетворяющие заданным свойствам, то это ***задача перечисления***.

Решение многих комбинаторных задач основано на следующих двух правилах.

2.1. Правила суммы и произведения

Пусть X – конечное множество такое, что $|X| = n$. Тогда говорят, что объект x из X может быть выбран n способами. Пусть $X_1, \ldots, X_n$ – попарно непересекающиеся множества, то есть $X_i \cap X_j = \varnothing$ при любых $i \neq j$. Тогда, очевидно, выполняется равенство $\left|\bigcup_{i=1}^{n} X_i\right| = \sum_{i=1}^{n} |X_i|$.

В комбинаторике этот факт называется ***правилом суммы***. Для $n = 2$ оно формулируется следующим образом: «Если объект x может быть выбран m способами, а объект y – другими n способами, то выбор “либо x, либо y” может быть осуществлен $m + n$ способами».

Другим часто применяемым в комбинаторике правилом является ***правило произведения***. Сформулируем и докажем частный случай этого правила для кортежа длины 2: «Если объект x может быть выбран m способами и после каждого из таких выборов объект y в свою очередь может быть выбран n способами, то выбор упорядоченной пары (x, y) может быть осуществлен $m \cdot n$ способами».

Доказательство. Пусть $X = \{a_1, \ldots, a_m\}$ – множество элементов, из которых выбирается объект x, и $X_i = \{(x, y) | \, x = a_i, y$ может быть выбран n способами$\}$, где $i = 1, ..., m$. Тогда множество всех пар (x, y) есть $\bigcup_{i=1}^{m} X_i$. Так как $X_i \cap X_j = \varnothing$ при любых $i \neq j$ и $|X_i| = n$, то по правилу суммы, имеем $\left|\bigcup_{i=1}^{m} X_i\right| = \sum_{i=1}^{m} |X_i| = m \cdot n$.

В общем случае правило произведения формулируется следующим образом: «Если объект x_1 может быть выбран n_1 способами, после чего объект x_2 может быть выбран n_2 способами и для любого i, где $2 \le i \le m - 1$, после выбора объектов $x_1, ..., x_i$ объект x_{i+1} может быть выбран n_{i+1} способами, то выбор кортежа $(x_1, x_2, ..., x_m)$ длины m может быть осуществлен $n_1 \cdot n_2 \cdot \ldots \cdot n_m$ способами».

Правило произведения в общем случае доказывается методом математической индукции.

Пример 2.1. В одной группе учится 25 человек, в другой – 20. Сколькими способами можно выбрать на конференцию:

а) одного делегата от двух групп;

б) по одному делегату от каждой группы?

Решение. Начальный этап решения обеих задач состоит в выборе делегата от первой группы, следующий этап – определение представителя второй группы. В задании под буквой а) существенным является то, что оба действия не могут быть выполнены одновременно, поскольку они взаимно исключают друг друга. Должен быть выполнен либо первый этап, либо второй. Рассуждения соответствуют правилу сложения, по которому получают 20 + 25 = 45 способов. Аналогично, для решения задания под буквой б) необходимо применить правило произведения, согласно которому выбрать по одному делегату от каждой группы можно $20 \cdot 25 = 500$ способами.

2.2. Размещения и сочетания

Определение 2.1. Набор элементов $x_{i_1}, \ldots, x_{i_k}$ из множества $X = \{x_1, .., x_n\}$ называется ***выборкой объема k из n элементов*** или ***(n, k)-выборкой***.

Определение 2.2. Выборка называется ***упорядоченной***, если в ней задан порядок следования элементов.

Таким образом, упорядоченная (n, k)-выборка представляет собой кортеж длины k, составленный из элементов множества мощности n. Следовательно, две различные упорядоченные (n, k)-выборки различаются лишь порядком расположения элементов в них.

Определение 2.3. Выборка называется ***неупорядоченной***, если порядок следования элементов в ней не является существенным.

Две различные неупорядоченные (n, k)-выборки обязательно отличаются друг от друга хотя бы одним элементом.

В выборках могут допускаться или не допускаться повторения элементов.

Определение 2.4. Упорядоченная (n, k)-выборка, в которой элементы могут повторяться, называется ***(n, k)-размещением с повторениями***.

Определение 2.5. Упорядоченная (n, k)-выборка, элементы которой попарно различны, называется ***(n, k)-размещением без повторений***.

Определение 2.6. ***Перестановкой без повторений из n элементов*** (или ***перестановкой множества X мощности n***) называется (n, n)-размещение без повторений.

Определение 2.7. Неупорядоченная (n, k)-выборка, в которой элементы могут повторяться, называется ***(n, k)-сочетанием с повторениями***.

Определение 2.8. Неупорядоченная (n, k)-выборка, элементы которой попарно различны, называется ***(n, k)-сочетанием без повторений***.

Заметим, что любое (n, k)-сочетание без повторений можно рассматривать как k-элементное подмножество n-элементного множества.

Пример 2.2. Пусть $X = \{a, b, c\}$. Тогда

1. $(a, a),(a, b),(a, c),(b, a),(b, b),(b, c),(c, a),(c, b),(c, c)$ – (3,2)-размещения с повторениями;
2. $(a, b), (a, c), (b, a), (b, c), (c, a), (c, b)$ – (3,2)-размещения;

3. $\{a, a\}, \{a, b\}, \{a, c\}, \{b, b\}, \{b, c\}, \{c, c\}$ – (3,2)-сочетания с повторениями;
4. $\{a, b\}, \{a, c\}, \{b, c\}$ – (3,2)-сочетания.

Число (n, k)-размещений с повторениями обозначается через $\overline{A}_n^k$, а без повторений – A_n^k. Число перестановок без повторений из n элементов обозначается через P_n, то есть $P_n = A_n^n$. Число (n, k)-сочетаний с повторениями обозначаем через $\overline{C}_n^k$, а без повторений – C_n^k.

Утверждение 2.1. $\overline{A}_n^k = n^k$.

Доказательство. Каждое (n, k)-размещение с повторениями является кортежем длины k, каждая координата которого может быть выбрана любым из n способов. Следовательно, по обобщенному правилу произведения получаем требуемую формулу.

Соглашение. В дальнейшем для общности формул условимся считать, что $0! = 1$.

Утверждение 2.2. $A_n^k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!}$ при $k \le n$ и $A_n^k = 0$ при $k > n$.

Доказательство. Случай $k > n$ очевиден. Рассмотрим случай, когда $k \le n$. Каждое (n, k)-размещение без повторений является кортежем длины k, координаты которого попарно различны и выбираются из множества мощности n. Тогда первая координата кортежа может быть выбрана n способами, после каждого выбора первой координаты вторая координата может быть выбрана $n - 1$ способами и так далее. Соответственно, после каждого выбора первой и так далее $(k-1)$-й координаты кортежа k-я координата может быть выбрана $n - (k - 1) = n - k + 1$ способами. Следовательно, по обобщенному правилу произведения, получаем требуемую формулу.

Следствие. $P_n = A_n^n = n \cdot (n-1) \cdot \ldots \cdot 1 = n!$.

Утверждение 2.3. $C_n^k = \frac{A_n^k}{k!} = \frac{n!}{k! \cdot (n-k)!}$ при $k \le n$ и $C_n^k = 0$ при $k > n$.

Доказательство. Случай $k > n$ очевиден. Рассмотрим случай, когда $k \le n$. Каждое (n, k)-сочетание можно упорядочить $k!$ способами. Объединение получаемых таким образом попарно непересекающихся множеств (n, k)-размещений для всех возможных (n, k)-сочетаний, очевидно, даст все (n, k)-размещения. Тогда по правилу суммы, имеем $A_n^k = \sum_{i=1}^{m} k!$, где m – число всех (n, k)-сочетаний без повторений, то есть $m = C_n^k$, а значит $A_n^k = C_n^k \cdot k!$, откуда $C_n^k = \frac{A_n^k}{k!}$.

Утверждение 2.4. $\overline{C}_n^k = C_{n+k-1}^k$.

Доказательство. Каждому (n, k)-сочетанию с повторениями B, составленному из элементов множества $X = \{x_1, \ldots, x_n\}$, поставим в соответствие кор-

теж $\alpha(B)$ длины $n + k - 1$, составленный из k нулей и $n - 1$ единиц так, что число нулей, находящихся между $(i - 1)$-й и i-й единицами, где $2 \le i \le n - 1$, будет равно числу элементов x_i, входящих в сочетание B, а число нулей, стоящих перед первой единицей (после $(n - 1)$-й единицы), равно числу элементов x_1 (соответственно x_n), входящих в сочетание B. Иначе говоря, единицы играют роль разграничителей между n элементами исходного множества, и, очевидно, их число равно $n - 1$, а число нулей между единицами (границами) равно числу вхождений соответствующего элемента в (n, k)-выборку. При этом суммарное число нулей равно k. Рассмотренное соответствие между (n, k)-сочетаниями с повторениями и кортежами с $n - 1$ единицами и k нулями является взаимно однозначным. С другой стороны, число кортежей с $n - 1$ единицами и k нулями равно числу k-элементных множеств (номеров нулевых координат в кортежах), являющихся подмножествами $(n + k - 1)$-элементного множества $\{1, 2, \ldots, n + k - 1\}$ (множества всех номеров координат в кортежах), то есть числу $(n + k - 1, k)$-сочетаний без повторений. Таким образом, $\overline{C}_n^k = C_{n+k-1}^k$.

Пример 2.3. Пусть $n = 4$, $k = 8$, $X = \{1, 2, 3, 4\}$, $B = \{1, 1, 1, 2, 3, 3, 4, 4\}$ – (4, 8)-сочетание с повторениями. Тогда $\alpha(B) = (0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0)$. Обратно, если $\alpha(B) = (1, 0, 0, 1, 0, 0, 0, 1, 0)$, то однозначно получаем, что $B = \{2, 2, 3, 3, 3, 4\}$.

Замечание 2.1. При определении выборки предполагалось, что она содержит, по крайней мере, один элемент. Однако для общности рассуждений в число выборок часто включают и пустую выборку, не содержащую элементов. Она единственна для всех рассмотренных нами случаев. Следовательно, $\overline{A}_n^0 = A_n^0 = \overline{C}_n^0 = C_n^0 = 1$. При этом формулы, приведенные в утверждениях 2.1–2.4 остаются справедливыми.

Выше мы определили понятие перестановки без повторений из n элементов. Понятие перестановки с повторениями рассматривается в случае, когда имеется n элементов, которые можно разбить на k групп, так что элементы, входящие в одну группу, неразличимы между собой и отличны от элементов, входящих в другие группы. Пусть число элементов в каждой группе равно соответственно $n_1, n_2, \ldots, n_k$, то есть $n_1 + n_2 + \ldots + n_k = n$.

Определение 2.9. Пусть имеется n элементов, которые можно разбить на k групп так, что элементы, входящие в одну группу, неразличимы между собой и отличны от элементов, входящих в другие группы. ***Перестановкой с повторениями из n элементов*** называется кортеж длины n, составленный из этих элементов.

Если число элементов в каждой группе равно соответственно $n_1, n_2, \ldots, n_k$, то есть $n_1 + n_2 + \ldots + n_k = n$, то число всех перестановок с повторениями из n элементов обозначается через $\overline{P}^n_{n_1, n_2, \ldots, n_k}$.

Утверждение 2.5. $\overline{P}^n_{n_1, n_2, \ldots, n_k} = \dfrac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_k!}$.

Доказательство. Согласно правилу произведения число перемещений элементов, не меняющих данную перестановку равно $n_1! \cdot \ldots \cdot n_k!$. Число всех перестановок без повторений из n элементов равно $P_n = n!$. Тогда

$\overline{P}^{\,n}_{n_1,n_2,\ldots,n_k} \cdot (n_1! \cdot \ldots \cdot n_k!) = n!$. Отсюда $\overline{P}^{\,n}_{n_1,n_2,\ldots,n_k} = \dfrac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_k!}$.

Рассмотренный в параграфах 2.1 и 2.2 теоретический материал можно представить в виде схемы, использование которой может быть полезно при решении задач (рис. 2.1).

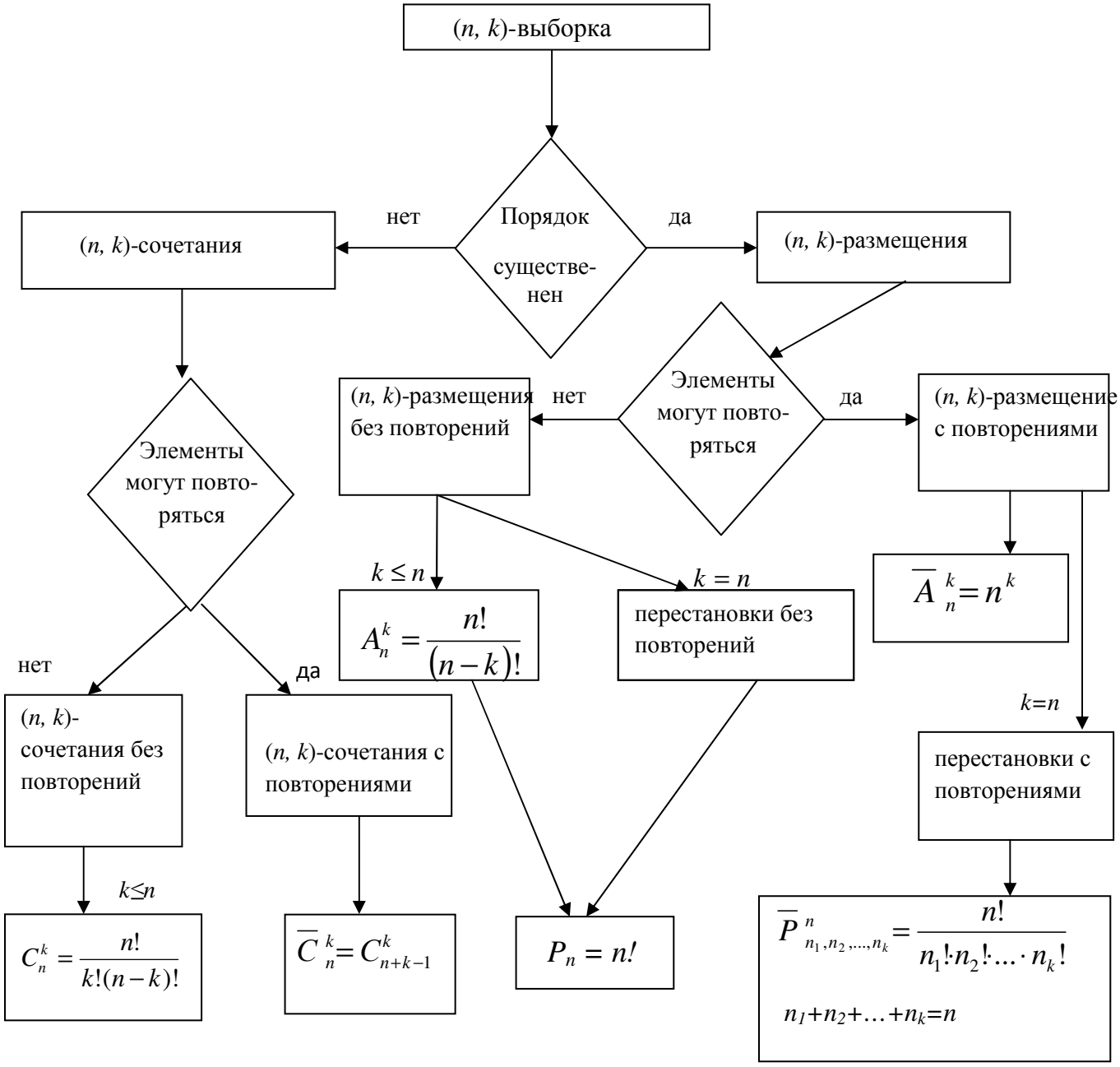


Рис. 2.1. Схема определения вида комбинаторной конфигурации

2.3. Примеры решения задач

Пример 2.4. Бросают две игральные кости (с шестью гранями каждая). Сколькими способами они могут упасть так, что либо на каждой грани выпадет четное число очков, либо на каждой грани выпадет нечетное число очков?

Решение. Пусть A – число способов выпадения на каждой кости четного числа очков, B – число способов выпадения на каждой кости нечетного числа очков. Тогда по правилу суммы, искомое число равно $A + B$. Пусть C – число способов выпадения четного числа очков на первой кости, а D – число способов выпадения четного числа очков на второй кости. Ясно, что $C = D = 3$, а по правилу произведения $A = C\,D = 9$. Аналогично, $B = 9$, а искомое число равно 18.

Пример 2.5. Сколькими способами три награды (за первое, второе и третье места) могут быть распределены между 10 участниками соревнований?

Решение. Требуется найти число способов, сколькими из 10 человек можно выбрать троих, без повторений, так как один человек не может занимать сразу два призовых места. Разные варианты искомых выборок могут быть одинаковыми по составу, но отличаться лишь порядком следования элементов или, иначе говоря, способом распределения призовых мест между выбранными тремя участниками. Задача сводится к нахождению числа всех (10, 3)-размещений без повторений. Следовательно, три награды могут быть распределены между 10 участниками соревнований $A_{10}^{3} = 720$ способами.

Пример 2.6. Имеется 10 различных книг. Сколькими способами их можно расставить на полке?

Решение. Расстановке подлежат все имеющиеся 10 книг, и вариант от варианта отличается только порядком следования книг на полке. Искомое число способов равно числу всех (10, 10)-размещений без повторений или числу всех перестановок без повторений из 10 элементов. Получаем: $A_n^n = \mathrm{P}_{10} = 10! = 3\,628\,000$ способов.

Пример 2.7. Сколько двузначных чисел можно составить, используя цифры 7, 4 и 5?

Решение. Порядок следования цифр в числе важен. Например, 47 и 74 – две различные выборки, удовлетворяющие условию задачи. Кроме этого, комбинация, например, 77 также является одним из решений. Значит, речь идет о размещениях с повторениями из трех по два. Следовательно, количество чисел равно $\overline{A}_3^2 = 3^2 = 9$.

Пример 2.8. Сколькими способами можно вытянуть 5 карт трефовой масти из стандартной колоды, содержащей 52 карты?

Решение. Всего в колоде 13 карт трефовой масти. Из этих 13 карт надо выбрать 5, причем без повторений и учета порядка следования карт в выборке. Разные варианты должны отличаться по составу. Следовательно, требуется найти число всех (13,5)-сочетаний: $C_{13}^{5} = \dfrac{13!}{5!\cdot 8!} = 1287$.

Пример 2.9. В магазине продается 4 сорта пирожных: бизе, эклеры, песочные, наполеоны. Сколькими способами можно выбрать 7 пирожных?

Решение. Каждая покупка – это выборка из 4 элементов по 7, причем с повторениями, так как 4 < 7. Порядок следования сорта пирожных внутри выборки не важен. Следовательно, число таких покупок равно числу всех (4, 7)-сочетаний с повторениями: $\overline{C}_4^7 = C_{7+4-1}^7 = C_{10}^7 = \frac{10!}{7! \cdot 3!} = 120.$

Пример 2.10. У врача 3 таблетки одного лекарства, 2 таблетки – другого и 4 таблетки – третьего. Сколькими способами он может распределить прием имеющихся таблеток по одной в день?

Решение. Общее число таблеток 3 + 2 + 4 = 9 равно числу дней приема лекарств, то есть все таблетки входят в выборку, но присутствуют повторяющиеся неразличимые элементы – таблетки одного лекарства. Решение задачи сводится к нахождению числа всех перестановок с повторениями из 9 элементов: $\overline{P}_{3,2,4}^9 = \frac{9!}{3! \cdot 2! \cdot 4!} = 1260.$

2.4. Бином Ньютона

Исторически название бином Ньютона несправедливо, поскольку формулу $(a+b)^n$ знали еще среднеазиатские математики, начиная с Хайяма (Омар Хайям (около 1048 – 1131) – персидский поэт, математик и философ), а в Европе до Ньютона (Исаак Ньютон (1643 – 1727) – английский физик, астроном и математик) ее знал Паскаль (Блез Паскаль (1623 – 1662) – французский математик). Однако заслуга Ньютона заключается в том, что он обобщил эту формулу для нецелого показателя *n* (см. замечание 2.2).

Для натурального показателя *n* формула бинома Ньютона имеет вид:

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k} = C_n^0 a^0 b^n + C_n^1 a^1 b^{n-1} + \ldots + C_n^l a^l b^{n-l} + \ldots + C_n^n a^n b^0. \qquad (9)$$

Доказательство. Для доказательства формулы (9) применим метод математической индукции.

1. *База индукции*. Пусть *n* = 1. Тогда $(a+b)^1 = C_1^0 a^0 b^1 + C_1^1 a^1 b^0 = a + b.$

2. *Индуктивное предположение.* Предположим, что формула (9) верна для *n* – 1.

3. *Индукционный переход*. Докажем справедливость формулы (9) для *n*.

В данном случае получаем

$$(a+b)^n = (a+b)^{n-1}(a+b) = a(a+b)^{n-1} + b(a+b)^{n-1} = \sum_{k=0}^{n-1} C_{n-1}^k a^{k+1} b^{(n-1)-k} + \sum_{k=0}^{n-1} C_{n-1}^k a^k b^{(n-1)-k+1}.$$

Заменим индекс суммирования *k* на *j* так, что *k = j – 1, j = k + 1*. Так как $0 \le k \le n-1$, то $1 \le j \le n$ и следующая формула принимает вид: $\sum_{k=0}^{n-1} C_{n-1}^k a^{k+1} b^{(n-1)-k} = \sum_{j=1}^{n} C_{n-1}^{j-1} a^j b^{n-j}$. Отсюда $(a+b)^n = \sum_{k=1}^{n} C_{n-1}^{k-1} a^k b^{n-k} + \sum_{k=0}^{n-1} C_{n-1}^k a^k b^{n-k}$.

Выровняем пределы изменения индексов суммирования в обеих суммах. Для этого введем дополнительно $C_{n-1}^{-1}=0$ и $C_{n-1}^{n}=0$, тогда $\sum_{k=1}^{n}C_{n-1}^{k-1}a^k b^{n-k}=\sum_{k=0}^{n}C_{n-1}^{k-1}a^k b^{n-k}$ и $\sum_{k=0}^{n-1}C_{n-1}^{k}a^k b^{n-k}=\sum_{k=0}^{n}C_{n-1}^{k}a^k b^{n-k}$.

Отсюда

$$(a+b)^n=\sum_{k=0}^{n}(C_{n-1}^{k-1}+C_{n-1}^{k})a^k b^{n-k}=\left|C_{n-1}^{k-1}+C_{n-1}^{k}=\frac{(n-1)!}{(k-1)!(n-1-k+1)!}+\frac{(n-1)!}{k!(n-1-k)!}=\right.$$

$$=\frac{(n-1)!}{(k-1)!(n-k)!}+\frac{(n-1)!}{k!(n-k-1)!}=\frac{(n-1)!k+(n-1)!(n-k)}{k!(n-k)!}=\frac{(n-1)!(k+n-k)}{k!(n-k)!}=$$

$$=\frac{(n-1)!n}{k!(n-k)!}=\frac{n!}{k!(n-k)!}=C_n^k\Big|=\sum_{k=0}^{n}C_n^k a^k b^{n-k}.$$ Следовательно, формула (9) верна для любого натурального n.

Замечание 2.2. Для нецелого n при $|x|<1$, формула имеет вид

$$(1+x)^{\alpha}=1+\alpha x+\frac{\alpha(\alpha-1)}{2!}x^2+\frac{\alpha(\alpha-1)(\alpha-2)}{3!}x^3+\ldots+\frac{\alpha(\alpha-1)(\alpha-2)\ldots(\alpha-k+1)}{k!}x^k+\ldots$$

2.5. Свойства биномиальных коэффициентов. Треугольник Паскаля

Биномиальное разложение служит основой для многих комбинаторных формул. Например:

1. Пусть $a = b = 1$. Тогда $\sum_{k=0}^{n}C_n^k=2^n$. Так как C_n^k – число k-элементных подмножеств n-элементного множества, то сумма в левой части есть число всех подмножеств n-элементного множества. Таким образом, получили еще одно доказательства того, что мощность булеана n-элементного множества равна 2^n.

2. Пусть $a = -1$, $b = 1$. Тогда $\sum_{k=0}^{n}C_n^k(-1)^k=0$. Следовательно, суммы биномиальных коэффициентов, стоящих на четных и на нечетных местах, равны между собой, и каждая равна 2^{n-1}.

3. $(\forall k: 0\le k\le n)\ C_n^k=C_n^{n-k}$.

Действительно, $C_n^{n-k}=\frac{n!}{(n-k)!(n-n+k)!}=C_n^k$.

4. В ходе доказательства формулы (9) мы получили

$$(\forall k: 0\le k\le n)\ \ C_{n-1}^{k-1}+C_{n-1}^{k}=C_n^k. \qquad (10)$$

Тождество (10) позволяет вычислить значения C_n^k, зная C_{n-1}^{k-1} и C_{n-1}^{k}.

Другими словами, с помощью тождества (10) можно последовательно вычислить C_n^k при $n = 0$, затем при $n = 1$, при $n = 2$ и так далее. Вычисления удобно записывать в виде треугольной таблицы:

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
\qquad
\begin{array}{ccccccccccc}
 & & & & & C_0^0 & & & & & \\
 & & & & C_1^0 & & C_1^1 & & & & \\
 & & & C_2^0 & & C_2^1 & & C_2^2 & & & \\
 & & C_3^0 & & C_3^1 & & C_3^2 & & C_3^3 & & \\
 & C_4^0 & & C_4^1 & & C_4^2 & & C_4^3 & & C_4^4 & \\
C_5^0 & & C_5^1 & & C_5^2 & & C_5^3 & & C_5^4 & & C_5^5
\end{array}
$$

В $(k + 1)$-й строке по порядку стоят числа $C_k^0, C_k^1, \ldots, C_k^k$. Поскольку C_{n-1}^{k-1} и C_{n-1}^k располагаются в этой таблице строкой выше, чем C_n^k, и находятся в этой строке слева и справа от него, то для получения C_n^k надо сложить находящиеся справа и слева от него числа предыдущей строки. Например, значение 10 в шестой строке мы получим, сложив числа 4 и 6 пятой строки.

Эту таблицу называют ***треугольником Паскаля***, по имени французского математика Блеза Паскаля, в трудах которого она встречается. Это название так же, как и бином Ньютона, исторически неточно, поскольку такую таблицу уже знал упомянутый ранее Омар Хайям.

Задачи и упражнения к главе 2

1. Сколько существует способов избрания президента, вице-президента, секретаря и казначея среди членов клуба, включающего 8 студентов последнего курса, 10 студентов предпоследнего курса,15 второкурсников и 20 первокурсников, если:
   а) отсутствуют какие-либо ограничения,
   б) президентом должен быть студент последнего курса,
   в) студент последнего курса не может быть вице-президентом,
   г) первокурсники могут быть избраны только на должность секретаря.
2. Сколькими способами можно рассадить класс, если присутствует 26 человек, а мест 28?
3. Сколькими способами можно вытянуть 5 карт бубновой масти из колоды, содержащей 36 карт?
4. Сколько трехзначных чисел можно составить из цифр 1, 2, 3 так, чтобы цифры в записи числа не повторялись?
5. В кухне 5 лампочек с отдельными выключателями. Сколько существует способов освещения?
6. Сколькими способами можно расставить на полке 12 книг, включающих 4 одинаковых учебника по математике, 6 одинаковых учебников по информатике, 2 одинаковых учебника по химии?
7. В булочной продается 10 различных видов пончиков. Сколькими способами можно выбрать 12 пончиков?
8. Сколько прямых линий можно провести через 7 точек, из которых лишь 3 лежат на одной прямой?

9. На выпускном вечере 20 студентов группы попарно обменялись своими фотографиями. Сколько всего потребовалось сделать фотографий?
10. Сколькими способами в пассажирский поезд из 9 вагонов можно продать четырем пассажирам билеты в разные вагоны и без этого ограничения?
11. Сколькими способами можно обить 6 различных стульев, если имеется 12 сортов обивочного материала?
12. Сколько слов (включая лишенных смысла) можно составить из всех букв слова «миссисипи»?
13. Найти число возможных вариантов выхода в полуфинал первенства по шахматам трех из 20 участников.
14. Сколько существует способов вытащить из колоды, содержащей 52 карты, 13 карт, из которых 9 карт одной масти?
15. Из колоды, содержащей 52 карты, вынули 10 карт. В скольких случаях среди этих карт окажется хотя бы один туз? В скольких случаях ровно один туз? Ровно два туза?
16. Автомобильные номера состоят из трех букв, за которыми идут 4 цифры, например МКМ-07-37.Сколько машин можно снабдить различными номерами, если используется 25 букв?
17. Сколько чисел больше 100 можно записать с помощью цифр 1, 2, 3, 4, если цифры в числе не повторяются?
18. Из 20 сотрудников лаборатории 5 человек должны выехать в командировку. Сколько может быть различных составов отъезжающей группы, если заведующий лабораторией и два ведущих инженера одновременно уезжать не должны?
19. Сколькими способами можно рассадить по жребию восемь рыцарей за круглым столом, чтобы первый и второй рыцари сидели рядом?
20. Двое друзей, А и В, стоят в очереди из 8 человек. Сколько существует вариантов очередей, в которых между А и В стоят два человека.
21. Сколькими способами можно сформировать железнодорожный состав из 9 вагонов так, чтобы второй и четвертый вагоны шли через один?
22. Сколькими способами можно рассадить вокруг круглого стола 6 мальчиков и 6 девочек, если каждая девочка должна сидеть между двумя мальчиками?
23. Сколькими способами можно рассадить случайным образом 12 студентов на 12 первых местах одного партера, чтобы студенты А и В сидели рядом?
24. Сколькими способами 7 человек могут встать в очередь так, чтобы два определенных лица не стояли рядом?
25. Две команды, в каждой из которых по 5 спортсменов, строятся в одну шеренгу. Сколькими способами можно построить шеренгу, чтобы игроки одной команды не стояли рядом?
26. Сколькими способами могут быть размещены дни рождения 12 человек в году, считая, что в нем 365 дней. Во скольких случаях все дни рождения попадут на разные дни года, а во скольких на разные месяцы?
27. Найти разложение $(a+b)^8$, используя треугольник Паскаля.
28. Написать разложение бинома $(x-2y)^5$.

29. В разложении $\left(x^3 - 3y^2\right)^{10}$ найдите коэффициент при $x^9 y^{14}$.

30. Найти член, содержащий x^4 в разложении бинома $\left(\sqrt[3]{x} + \sqrt{x}\right)^9$.

31. Найти члены, не содержащие иррациональности в разложении бинома $\left(\sqrt[7]{2} + \sqrt[5]{3}\right)^{24}$.

32. Решить уравнение $\frac{(n+2)!}{n!} = 72$.

33. Решить уравнение $\frac{A_{x+1}^4 P_{x-4}}{P_{x-1}} = 15$.

34. Решить уравнение $C_{x+1}^{x-1} = 21,\ x \in N$.

35. Решить уравнение $C_{2n}^{n+1} : C_{2n+1}^{n-1} = \frac{7}{13}$.

36. Решить уравнение $A_x^5 = 18A_{x-2}^4$.

Глава 3. Отношения. Отображения

3.1. Понятие отношения

Определение 3.1. *N-арным* (*n-местным*) *отношением P* на множествах $A_1, A_2, \ldots, A_n$ называется любое подмножество прямого произведения $A_1 \times A_2 \times \ldots \times A_n$.

В случае $n = 1$ отношение P называется *унарным* (*одноместным*) и является подмножеством множества A_1.

При $n = 2$ P называется *бинарным* (*двуместным*) *отношением* или *соответствием*. Если $P \subseteq A_1 \times A_2$, то также говорят, что P есть отношение между множествами A_1 и A_2 (между элементами множеств A_1 и A_2) или что P задано (определено) на паре множеств A_1 и A_2. Если $A_1 = A_2 = A$ ($P \subseteq A \times A$), то говорят, что P есть *бинарное отношение на множестве A*.

Пусть P – бинарное отношение и $(x, y) \in P$, тогда говорят, что элемент x находится в отношении P к элементу y, или что x и y связаны отношением P. Вместо записи $(x, y) \in P$ часто пишут xPy.

В дальнейшем речь будет идти о бинарных отношениях, так как они наиболее часто встречаются и хорошо изучены. Если не будет специально оговорено, то под «отношением» будем понимать бинарное отношение. Частично бинарные отношения (соответствия) уже были рассмотрены в параграфе 1.7. Введем еще несколько определений.

Определение 3.2. Пусть $P \subseteq A \times B$, $S \subseteq A \times B$. Отношения P и S называются *равными* (пишут $P = S$), если для любых $x \in A$ и $y \in B$ пара $(x, y) \in P$ тогда и только тогда, когда $(x, y) \in S$.

Другими словами, отношения P и S равны, если P и S равны как множества.

Определение 3.3. Для любого множества A отношение $id_A = \{(x;x) \mid x \in A\}$ называется *тождественным отношением* (*диагональю*), а $U_A = A \times A = \{(x;y) \mid x, y \in A\}$ – *полным отношением* (*универсальным отношением*).

Определение 3.4. *Графиком* бинарного отношения $P \subseteq R^2$ называется множество всех точек координатной плоскости Oxy с координатами (x, y) такими, что $(x,y) \in P$.

Определение 3.5. Пусть $A = \{a_1, a_2, ..., a_n\}$, $B = \{b_1, b_2, ..., b_m\}$ и $P \subseteq A \times B$. *Матрицей* бинарного отношения P называется матрица $\| P \| = (p_{ij})$ размера $n \times m$, элементы p_{ij} которой определяются следующим образом:

$$p_{ij} = \begin{cases} 1, & \text{если } (a_i, b_j) \in P; \\ 0, & \text{если } (a_i, b_j) \notin P. \end{cases}$$

Пример 3.1. Если A – конечное множество мощности n, то матрица тождественного отношения id_A представляет собой единичную матрицу, а матрица полного отношения U_A представляет собой матрицу, все элементы которой равны 1:

$$\| id_A \| = \begin{pmatrix} 1 & 0 & . & . & . & 0 \\ 0 & 1 & . & . & . & 0 \\ . & . & . & . & . & . \\ 0 & 0 & . & . & . & 1 \end{pmatrix}; \qquad \| U_A \| = \begin{pmatrix} 1 & 1 & . & . & . & 1 \\ 1 & 1 & . & . & . & 1 \\ . & . & . & . & . & . \\ 1 & 1 & . & . & . & 1 \end{pmatrix}. \square$$

Замечание 3.1. Матрица бинарного отношения $P \subseteq A \times B$ содержит полную информацию о связях между элементами множеств A и B и позволяет представить эту информацию в графическом виде на компьютере. ***Любая матрица, состоящая из нулей и единиц, является матрицей некоторого бинарного отношения***.

3.2. Способы задания бинарных отношений

Бинарные отношения можно задать одним из перечисленных способов.

1. ***Списком входящих в отношение элементов*** (см. пример 1.12).
2. ***Характеристическим свойством.***

   Пример 3.2. $P = \{(x, y) \in R^2 \mid x^2 + y^2 = 4\}$.
3. ***Графиком*** (***только для подмножеств R^2***).

   Пример 3.3. График, изображенный на рис. 3.1, задает отношение P из примера 3.2.

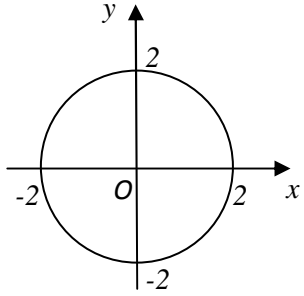


Рис. 3.1

4. ***Графом.*** Понятие графа отношения (или графа соответствия) между двумя различными множествами было введено в параграфе 1.7. Граф, изображенный на рис. 1.7, задает отношение R из примера 1.12. Если отношение P задано на множестве A ($P \subseteq A \times A$), то его *ориентирован-*

ным графом (или просто *графом*) называется следующая геометрическая фигура: точки плоскости (*вершины*), представляющие элементы множества $DomP \cup ImP$, и *ориентированные ребра* – каждой паре $(a,b) \in P$ ставится в соответствие линия (прямая или кривая), соединяющая точки a и b, на которой стрелкой указано направление от точки a к точке b. Ориентированное ребро, соответствующее паре $(a,b) \in P$, где $a = b$, называется *петлей*. Направление обхода петли при изображении графа фиксируется (например, всегда против часовой стрелки).

Любое бинарное отношение на конечном множестве можно представить ориентированным графом. Обратно, любой ориентированный граф представляет бинарное отношение на множестве его вершин.

Пример 3.4. Граф, изображенный на рис. 3.2, задает отношение

$$S = \{(a,a),(a,c),(a,d),(b,e),(b,c),(c,c),(d,e)\}$$

на множестве $A = \{a, b, c, d, e\}$.

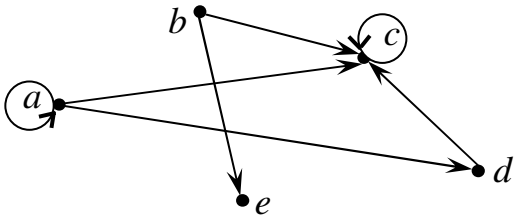


Рис. 3.2

5. ***Матрицей.***

Пример 3.5. Если $A = \{a, b, c, d\}$ и $B = \{1, 2, 3\}$, то матрица

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{pmatrix}$$

задает отношение

$P = \{(a, 1), (a, 2), (b, 2), (c, 3), (d, 1), (d, 3)\} \subseteq A \times B$.

3.3. Операции над бинарными отношениями

Бинарные отношения – это *множества* упорядоченных пар. Следовательно, над ними можно выполнять любые теоретико-множественные операции, в частности, операции *объединения* и *пересечения*. Определим еще две операции над отношениями.

Определение 3.6. Отношением P^{-1}, *обратным* к отношению $P \subseteq A \times B$, называется подмножество прямого произведения $B \times A$ такое, что

$P^{-1} = \{(y,x) \mid (x,y) \in P\}$.

Пример 3.6. Пусть $P = \{(a, 1), (b, 2), (c, 3), (d, 4), (e, 5)\}$. Тогда

$P^{-1} = \{(1, a), (2, b), (3, c), (4, d), (5, e)\}$.

Определение 3.7. *Композицией (суперпозицией) отношений* $P \subseteq A \times B$ и $Q \subseteq B \times C$ называется множество

$P \circ Q = \{(x,y) \mid x \in A, y \in C \wedge (\exists z \in B) : (x,z) \in P, (z,y) \in Q\}$ (рис. 3.3).

Здесь и далее знак «$\wedge$» заменяет союз «и».

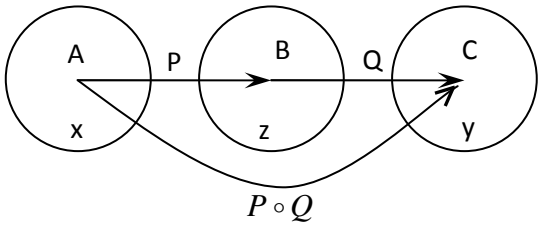


Рис. 3.3

Пример 3.7. Если $P = \{(1, 6), (2, 5), (3, 4), (6, 7)\}$, $Q = \{(5, 8), (6, 1), (3, 7), (4, 2)\}$, то $P \circ Q = \{(1, 1), (2, 8), (3, 2)\}$ и $Q \circ P = \{(6, 6), (4, 5)\}$.

Утверждение 3.1. Для любых бинарных отношений P, Q и R выполняются следующие свойства:

1. $(P^{-1})^{-1} = P$;
2. $(P \circ Q)^{-1} = Q^{-1} \circ P^{-1}$;
3. $(P \circ Q) \circ R = P \circ (Q \circ R)$ (*ассоциативность композиции*).

Доказательство. Каждое из свойств 1 – 3 представляет собой равенство двух множеств. Следовательно, доказательство можно провести на основании определений 1.5, 3.6 и 3.7.

1. $\forall (x, y) \in P \Leftrightarrow (y, x) \in P^{-1} \Leftrightarrow (x, y) \in (P^{-1})^{-1}$.
2. $\forall (x, y) \in (P \circ Q)^{-1} \Leftrightarrow (y, x) \in P \circ Q \Leftrightarrow (\exists z) : (y, z) \in P \wedge (z, x) \in Q \Leftrightarrow (\exists z) : (z, y) \in P^{-1} \wedge$
   $\wedge (x, z) \in Q^{-1} \Leftrightarrow (x, y) \in Q^{-1} \circ P^{-1}$.
3. $\forall (x, y) \in (P \circ Q) \circ R \Leftrightarrow (\exists z) : (x, z) \in P \circ Q \wedge (z, y) \in R \Leftrightarrow (\exists z), (\exists t) : (x, t) \in P \wedge (t, z) \in Q \wedge$
   $\wedge (z, y) \in R \Leftrightarrow (\exists t) : (x, t) \in P \wedge (t, y) \in Q \circ R \Leftrightarrow (x, y) \in P \circ (Q \circ R)$.

3.4. Свойства матриц бинарных отношений

1. Пусть $P, Q \subseteq A \times B$ и $\| P \| = (p_{i,j})$, $\| Q \| = (q_{i,j})$. Тогда $\| P \cup Q \| = \| P \| + \| Q \| = (p_{i,j} + q_{ij})$ и $\| P \cap Q \| = \| P \| * \| Q \| = (p_{i,j} \cdot q_{ij})$. При этом сложение и умножение элементов определяются по правилам: 0 + 0 = 0, 1 + 0 = 0 + 1 = 1, 1 + 1 = 1, 0 · 0 = 0, 1 · 0 = 0 · 1 = 0, 1 · 1 = 1.
2. Пусть $P \subseteq A \times B$, $Q \subseteq B \times C$. Тогда $\| P \circ Q \| = \| P \| \cdot \| Q \|$, где матрицы умножаются по обычному правилу умножения матриц, но произведение и сумма элементов при перемножении матриц находится по правилам п. 1.
3. $\| P^{-1} \| = \| P \|^T$.
4. Пусть $\| P \| = (p_{ij})$, $\| Q \| = (q_{ij})$. Если $P \subseteq Q$, то $(\forall i, j)\ (p_{ij}) \le (q_{ij})$.

Пример 3.8. Пусть $P,\ Q \subseteq A^2,\ A = \{1,\ 2,\ 3\}$. Если $\| P \| = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$, $\| Q \| = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ – соответственно матрицы отношений P и Q, то

$$\| P \cup Q \| = \| P \| + \| Q \| = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix},\ \| P \cap Q \| = \| P \| * \| Q \| = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$\| P \circ Q \| = \| P \| \cdot \| Q \| = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix},\ \| P^{-1} \| = \| P \|^T = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

3.5. Свойства бинарных отношений

Пусть $A \neq \varnothing$ и $P \subseteq A^2$.

Определение 3.8. Отношение P на множестве A называется *рефлексивным*, если $(\forall a \in A)\ \ aPa$.

Примерами рефлексивных отношений являются отношение делимости на множестве целых чисел, отношение включения на булеане непустого множества.

Отношение P рефлексивно тогда и только тогда, когда каждая вершина графа имеет петлю.

Определение 3.9. Отношение P на множестве A называется *антирефлексивным*, если $(\forall a \in A)\ \ (a,a) \notin P$.

Например, отношение неравенства на некотором числовом множестве, отношение перпендикулярности на множестве всех прямых евклидовой плоскости являются антирефлексивными.

Отношение антирефлексивно тогда и только тогда, когда ни одна вершина графа не имеет петли.

Определение 3.10. Отношение P на множестве A называется *симметричным*, если $(\forall a,b \in A)\ \ aPb \Rightarrow bPa$.

Примерами симметричных отношений являются отношение равенства на некотором числовом множестве, отношение параллельности на множестве всех прямых евклидовой плоскости.

Отношение симметрично тогда и только тогда, когда всякий раз вместе с ребром (x, y) граф содержит ребро (y, x).

Определение 3.11. Отношение P на множестве A называется *антисимметричным*, если $(\forall a,b \in A)\ \ aPb \wedge bPa \Rightarrow a = b$.

Например, отношение меньше (<) на множестве действительных чисел, отношение включения на булеане непустого множества.

Отношение антисимметрично тогда и только тогда, когда вместе с каждым ребром (x, y) граф не содержит ребро (y, x). Граф антисимметричного отношения может содержать петли.

Замечание 3.2. Свойство антисимметричности не совпадает со свойством несимметричности. Например, отношение $P = \{(a,b),(b;a),(a;c)\}$ на множестве $A = \{a,b,c\}$ не симметрично, поскольку $(a,c) \in P$, а $(c,a) \notin P$, и не антисимметрично, так как $(a,b) \in P$ и $(b,a) \in P$, но $a \neq b$. Диагональ непустого множества A (id_A) является примером симметричного и антисимметричного отношения. Вообще, ***любое подмножество*** id_A ***обладает одновременно свойствами симметричности и антисимметричности.***

Определение 3.12. Отношение P на множестве A называется *транзитивным*, если $(\forall a,b,c \in A)\ aPb \wedge bPc \Rightarrow aPc$.

Например, отношение параллельности на множестве всех прямых евклидовой плоскости, отношение включения на булеане непустого множества являются транзитивными.

Отношение транзитивно тогда и только тогда, когда вместе с каждой парой ребер (x, y) и (y, z) граф содержит ребро (x, z).

Утверждение 3.2. Пусть $A \neq \varnothing$ и $P \subseteq A^2$. Тогда справедливы следующие соотношения:

1. P – рефлексивно $\Leftrightarrow$ $id_A \subseteq P$;
2. P – антирефлексивно $\Leftrightarrow P \cap id_A = \varnothing$;
3. P – симметрично $\Leftrightarrow P = P^{-1}$;
4. P – антисимметрично $\Leftrightarrow P \cap P^{-1} \subseteq id_A$;
5. P – транзитивно $\Leftrightarrow P \circ P \subseteq P$.

3.6. Определение свойств бинарного отношения по его матрице

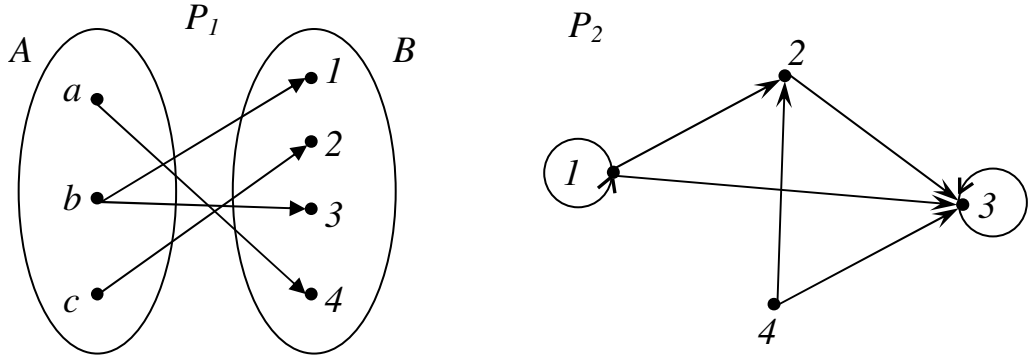
На основании утверждения 3.2 и свойств матриц бинарных отношений можно выяснить, как определять свойства бинарного отношения по его матрице.

1. P – рефлексивно $\Leftrightarrow$ $id_A \subseteq P \Leftrightarrow$ главная диагональ матрицы $\|P\|$ состоит из одних единиц.
2. P – антирефлексивно $\Leftrightarrow$ $P \cap id_A = \varnothing \Leftrightarrow$ главная диагональ матрицы $\|P\|$ состоит из одних нулей.
3. P – симметрично $\Leftrightarrow$ $P = P^{-1} \Leftrightarrow \| P \| = \| P \|^T \Leftrightarrow$ матрица $\|P\|$ симметрична относительно главной диагонали.
4. P – антисимметрично $\Leftrightarrow$ $P \cap P^{-1} \subseteq id_A \Leftrightarrow$ матрица $\| P \cap P^{-1} \|$ вне главной диагонали содержит только нули.

5. P – транзитивно $\Leftrightarrow$ $P \circ P \subseteq P$ $\Leftrightarrow$ $(\forall i, j)$ $q_{ij} \le p_{ij}$, где $\| P \| = (p_{ij})$, $\| P \circ P \| = (q_{ij})$.

Пример 3.9. Пусть $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, $P_1 = \{(a, 4), (b, 1), (b, 3), (c, 2)\}$, $P_2 = \{(1, 1), (1, 2), (1, 3), (2, 3), (3, 3), (4, 2), (4, 3)\}$. Изобразить графы отношений P_1 и P_2, найти матрицу $\| (P_1 \circ P_2)^{-1} \|$. Выяснить с помощью матрицы $\| P_2 \|$, какими свойствами обладает отношение P_2.

Решение. Изобразим графы отношений P_1 и P_2:



Найдем матрицу $\| (P_1 \circ P_2)^{-1} \|$.

$$\| (P_1 \circ P_2)^{-1} \| = \| P_2^{-1} \circ P_1^{-1} \| = \| P_2^{-1} \| \cdot \| P_1^{-1} \| = \| P_2 \|^T \cdot \| P_1 \|^T .$$

$$\| P_1 \| = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \| P_2 \| = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \| P_1 \|^T = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \| P_2 \|^T = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

$$\| (P_1 \circ P_2)^{-1} \| = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

Выясним с помощью матрицы $\| P_2 \|$, какими свойствами обладает отношение P_2.

1. Отношение P_2 не рефлексивно, так как главная диагональ матрицы $\| P_2 \|$ не состоит из одних единиц.
2. Отношение P_2 не антирефлексивно, так как главная диагональ матрицы $\| P_2 \|$ не состоит из одних нулей.
3. Отношение P_2 не симметрично, так как матрица $\| P_2 \|$ не является симметричной относительно главной диагонали.
4. $$\| P_2 \cap P_2^{-1} \| = \| P_2 \| * \| P_2 \|^T = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} * \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Следовательно, отношение P_2 антисимметрично, так как матрица $\| P_2 \cap P_2^{-1} \|$ вне главной диагонали содержит только нули.

$$5.\ \| P_2 \circ P_2 \| = \| P_2 \| \cdot \| P_2 \| = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} = (q_{ij}),\ \| P_2 \| = (p_{ij}).$$

Отношение P_2 транзитивно, так как $(\forall i, j)\ \ q_{ij} \le p_{ij}$.

3.7. Отношение эквивалентности

Определение 3.13. Бинарное отношение на множестве A называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

Отношение эквивалентности обычно обозначают символами ~ или ≡.

Примерами отношения эквивалентности являются отношение равенства на множестве действительных чисел, отношение параллельности на множестве прямых евклидовой плоскости.

Определение 3.14. Пусть R – отношение эквивалентности на множестве A и $a \in A$. *Классом эквивалентности*, *порожденным элементом a*, называется множество $\{x \in A \mid xRa\}$.

Класс эквивалентности, порожденный элементом a, будем обозначать через a/R. Совокупность всех классов эквивалентности отношения R на множестве A обозначается через A/R.

Определение 3.15. *Представителем класса эквивалентности* называется любой элемент этого класса.

Определение 3.16. Пусть A – непустое множество. *Фактор- множеством* множества A по отношению эквивалентности R называется множество A/R всех классов эквивалентности.

Теорема 3.1 (прямая). Пусть R – отношение эквивалентности на непустом множестве A. Тогда фактор-множество A/R является разбиением множества A.

Доказательство. Так как отношение R рефлексивно, то для любого $a \in A$ имеем aRa. Это значит, что каждый элемент a множества A принадлежит классу эквивалентности a/R. Итак, имеем семейство непустых классов a/R (a/R содержит по крайней мере один элемент a) и $\bigcup\limits_{a \in A} a/R = A$. Осталось доказать, что пересечение любых двух различных классов пусто. Для этого достаточно показать, что классы эквивалентности, имеющие хотя бы один общий элемент, совпадают. Пусть a/R и b/R – классы эквивалентности, имеющие общий элемент c. Тогда cRa и cRb. В силу симметричности отношения R из cRa следует aRc. Пусть x – любой элемент из a/R , тогда xRa. Имеем, xRa и aRc. Следовательно, в силу транзитивности отношения R xRc. Имеем, xRc и cRb. Тогда xRb, так как отношение R транзитивно. Следовательно, $x \in b/R$. Таким образом, $a/R \subseteq b/R$. Аналогично доказывается, что $b/R \subseteq a/R$. Следовательно, $a/R = b/R$.

Из теоремы 3.1 непосредственно вытекает следующее следствие.

Следствие. Пусть R – отношение эквивалентности на множестве A. Тогда

1) $(\forall\ a \in A)\ \ a \in a/R$;
2) $\bigcup_{a \in A} a/R = A$;
3) $(\forall\ a, b \in A)\ \ a/R = b/R \Leftrightarrow a\ R\ b$;
4) $a/R \neq b/R \Leftrightarrow a/R \cap b/R = \varnothing$.

Пусть S – разбиение непустого множества A и R_S – бинарное отношение, определяемое следующим образом: (x,y) $\in R_S$ тогда и только, когда x и y принадлежат одному и тому же подмножеству семейства S.

Теорема 3.2 (обратная). Отношение R_S, соответствующее разбиению S непустого множества A, является отношением эквивалентности на A, причем фактор-множество A/R_S совпадает с разбиением S.

Доказательство. 1. Так как S есть разбиение, то $(\forall a \in A)\exists M_i \subseteq S : a \in M_i$. Следовательно, по определению отношения R_S, $aR_s a$, а значит R_S – рефлексивно.

2. Пусть a, b – произвольные элементы из A такие, что aR_Sb. Тогда, по определению отношения R_S, $\exists\ M_j \subseteq S$: $a, b \in M_j$. Следовательно, bR_Sa. Получили, что R_S – симметрично.

3. Пусть a, b, c – произвольные элементы из A такие, что $aR_S\ b \wedge bR_S\ c$. Следовательно, по определению отношения R_S, $\exists\ M_i$, $M_j \subseteq S$: $a, b \in M_i \wedge$ $b, c \in M_j$. Отсюда $b \in M_i \cap M_j$. Но тогда, по определению разбиения, $M_i = M_j$, а значит, $a, c \in M_i$, и, по определению отношения R_S, aR_Sc. Получили, что R_S – транзитивно.

Из п. 1 – 3 следует, что R_S – отношение эквивалентности. Фактор-множество A/R_S совпадает с разбиением S по определению отношения R_S.

Пример 3.10. На множестве $A = \{a, b, c, d, e\}$ задано отношение $R = \{(a, a), (b, b), (b, c), (b, d), (c, b), (c, c), (c, d), (d, b), (d, c), (d, d), (e, e)\}$. Доказать, что R является отношением эквивалентности на множестве A. Найти классы эквивалентности, на которые разбивается множество A отношением R.

Решение. Построим граф отношения R (рис. 3.4), на основании которого заключаем, что R является рефлексивным, симметричным и транзитивным. Следовательно, по определению, R – отношение эквивалентности. В один класс эквивалентности входят элементы, попарно связанные отношением R между собой. Значит, отношение R разбивает множество A на три класса эквивалентности: $A_1 = \{a\}$,

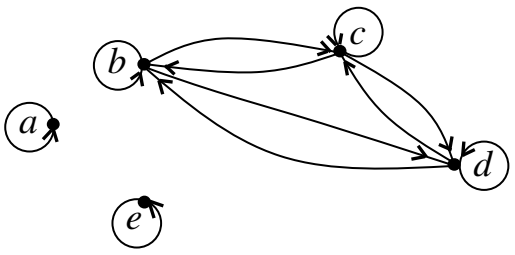


Рис. 3.4

$A_2 = \{b, c, d\}$, $A_3 = \{e\}$.

Замечание 3.3. Частным случаем отношения эквивалентности ~ является отношение равенства элементов некоторого множества A, которое определяет разбиение множества на одноэлементные классы эквивалентности:

$(\forall\ x \in A)\ x/\sim = \{x\}$. В этом случае ***классов эквивалентности оказывается столько же, сколько элементов содержится в множестве A***, так как каждый элемент из A эквивалентен только самому себе.

В другом частном случае все элементы множества A эквивалентны друг другу. При этом фактор-множество $A/\sim$ состоит всего из ***одного класса*** – самого множества A.

В любом другом случае среди классов эквивалентности имеется хотя бы один класс, который содержит больше одного элемента и в то же время не совпадает с самим множеством A.

Замечание 3.4. Понятие отношения эквивалентности имеет большое значение в математике. Дело в том, что элементы, входящие в один класс эквивалентности неразличимы с точки зрения рассматриваемого отношения эквивалентности. Поэтому считают, что класс эквивалентности определяется любым своим представителем (произвольным элементом этого класса). Это позволяет вместо всех элементов множества изучать совокупность представителей каждого класса эквивалентности. Свойства, которыми обладают все элементы некоторого класса эквивалентности, изучаются на одном его представителе.

Отношения эквивалентности играют важную роль в определении математических понятий.

3.8. Счетные и несчетные множества

Определение 3.17. Множества X и Y называются *изоморфными* (пишут $X \cong Y$), если между ними можно установить взаимно однозначное соответствие.

Утверждение 3.3. Бинарное отношение «быть изоморфными» на совокупности множеств является отношением эквивалентности.

По теореме 3.1 все множества относительно отношения «быть изоморфными» разбиваются на классы эквивалентности, каждый из которых состоит из попарно изоморфных между собой множеств.

Определение 3.18. То общее, что есть у всех множеств одного и того же класса эквивалентности по отношению «быть изоморфными» (количество элементов), называется *кардинальным числом* (т.е. количественным) или *мощностью* множеств данного класса.

Таким образом, мощность множества представляет собой обобщение понятия «число элементов» на случай произвольного (конечного или бесконечного) множества. Как и для конечного множества, мощность бесконечного множества X обозначается через $|X|$.

Определение 3.19. Множества X и Y называются *равномощными*, если они изоморфны, то есть между ними можно установить взаимно однозначное соответствие. При этом пишут $|X| = |Y|$.

Пример 3.11. Пусть X – множество действительных чисел, а Y – множество точек координатной прямой. Установим между ними следующее соответствие: каждому действительному числу x сопоставим точку $M(x)$ координатной

прямой. Это соответствие является взаимно однозначным, так как каждому действительному числу сопоставляется единственная точка координатной прямой и, наоборот, каждая точка на координатной прямой соответствует только одному числу. Следовательно, $|X| = |Y|$.

Пример 3.12. Пусть X – множество точек отрезка AB, Y – множество точек отрезка CD, причем длины отрезков AB и CD различны. Между множествами X и Y можно установить взаимно однозначное соответствие так, как показано на рис. 3.5. Следовательно, $|X| = |Y|$.

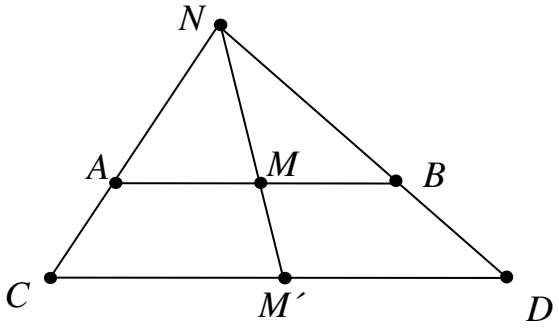


Рис. 3.5

В теории конечных множеств имеет место утверждение: «часть меньше целого».

Пример 3.13. $A = \{a, b, c, d, e\}$, $B = \{b, c, e\} \Rightarrow B \subseteq A \wedge B \neq A$.

Между конечным множеством и его собственным подмножеством нельзя установить взаимно-однозначное соответствие.

Определение 3.20. Множество X называется *конечным*, если X не равномощно никакому его собственному подмножеству.

В противном случае множество называется бесконечным.

Определение 3.21. Множество X называется *бесконечным*, если из множества X можно выделить равномощное ему собственное подмножество.

Пример 3.14. Рассмотрим N и $A = \{x \in N \mid x$ – четное число$\}$. Имеем: $A \subseteq N$, $A \neq N$. Собственное подмножество A равномощно N, так как между N и A можно следующим образом установить взаимно однозначное соответствие:

N: 1 2 3 ... n ...
↓ ↓ ↓ ↓
A: 2 4 6 ... $2n$ ...

Таким образом, в теории бесконечных множеств теряет силу утверждение, что «часть меньше целого».

Определение 3.22. Кардинальное число называется *конечным*, если оно является мощностью конечного множества.

Определение 3.23. Кардинальное число называется *бесконечным*, если оно является мощностью бесконечного множества.

Определение 3.24. Конечные ненулевые кардинальные числа называются *натуральными числами*.

Другими словами, натуральное число – это общее свойство класса конечных непустых равномощных множеств.

Наименьшей бесконечной мощностью является $\aleph_0$ (а́леф-нуль) – мощность множества натуральных чисел. Итак, $|N| = \aleph_0$.

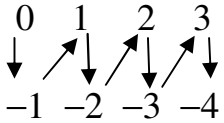
Определение 3.25. Множества, равномощные множеству натуральных чисел, называют *счетными*.

Другими словами, множество является счетным, если его элементы можно перенумеровать. Мощность любого счетного множества равна $\aleph_0$.

Пример 3.15. Множество Z счетно. Покажем, как можно перенумеровать элементы множества Z.

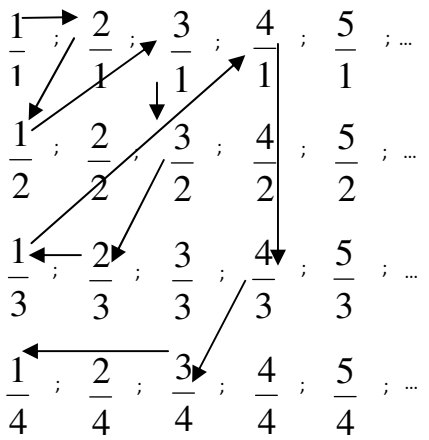
Запишем множество Z в виде двух строк и будем нумеровать по столбцам:

0 – № 1; –1 – № 2; 1 – № 3; –2 – № 4 и т.д.:



Таким образом, все положительные числа и нуль нумеруются нечетными числами, а все отрицательные целые числа – четными.

Пример 3.16. Множество Q счетно. Покажем, как можно перенумеровать элементы множества Q.



Перенумеруем сначала все положительные рациональные числа. Для этого выпишем в виде таблицы сначала все положительные дроби со знаменателем 1, потом все положительные дроби со знаменателем 2, далее со знаменателем 3 и т.д. Нумерацию будем проводить по квадратам. При этом если некоторая дробь занумерована, то последующие дроби, выражающие то же число, будем пропускать. Получим следующую нумерацию: $1, 2, \frac{1}{2}, 3, \frac{3}{2}, \frac{2}{3}, \frac{1}{3}, 4, \frac{4}{3}, \frac{3}{4}, \frac{1}{4}, \ldots$.

После того как занумерованы все положительные рациональные числа, все рациональные числа нумеруются аналогично целым числам. Для этого надо перенумерованные положительные и отрицательные рациональные числа записать отдельно в виде двух строк, и числа одной строки нумеровать четными номерами, а второй – нечетными, оставив еще один номер для нуля.

Теорема 3.3 (Кантора). Множество всех действительных чисел несчетно.

Доказательство. Предположим противное. Пусть все действительные числа занумерованы: $x_1, x_2, \ldots, x_n, \ldots$. Известно [5], что между множеством всех действительных чисел и множеством допустимых десятичных дробей (то есть бесконечных десятичных дробей, не имеющих периода 9) существует взаимно однозначное соответствие. Запишем числа $x_1, x_2, \ldots, x_n, \ldots$ с помощью допустимых десятичных дробей:

$$x_1 = \alpha_0^{(1)}, \alpha_1^{(1)}, \alpha_2^{(1)} \ldots \alpha_m^{(1)} \ldots$$
$$x_2 = \alpha_0^{(2)}, \alpha_1^{(2)}, \alpha_2^{(2)} \ldots \alpha_m^{(2)} \ldots \qquad (11)$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x_n = \alpha_0^{(n)}, \alpha_1^{(n)}, \alpha_2^{(n)} \ldots \alpha_m^{(n)} \ldots$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

В равенствах (11) $\alpha_0^{(n)}$ (n = 1, 2, ...) – целое число с тем или иным знаком, а $\alpha_m^{(n)}$ (m = 1, 2, ... , n = 1, 2, ...) – одна из цифр 0, 1, 2, ... , 9.

Выберем цифру α_n (n = 1, 2, ...) так, чтобы $\alpha_n \neq \alpha_n^{(n)}$ и $\alpha_n \neq 9$. Тогда дробь $0,\alpha_1\alpha_2\ldots\alpha_n\ldots$ является допустимой. Следовательно, $\exists\, n \in N$: $x_n = 0,\alpha_1\alpha_2\ldots\alpha_n\ldots$ С другой стороны, действительного числа $a = 0, \alpha_1\, \alpha_2 \ldots\, \alpha_n \ldots$ нет среди чисел x_n (n = 1, 2, ...), так как десятичная дробь $0,\alpha_1\alpha_2\ldots\, \alpha_n\ldots$ хотя бы одним десятичным знаком отличается от каждой из десятичных дробей (11). Получили противоречие. Следовательно, наше предположение неверно, и множество действительных чисел несчетно.

Мощность множества всех действительных чисел R называют мощностью *континуума* (от лат. continuum – непрерывное) и обозначают древнееврейской буквой $\aleph$ (алеф). Все множества, изоморфные множеству R, имеют мощность континуума. Примерами множеств мощности континуума являются множества точек любого отрезка, луча, прямой.

На множестве кардинальных чисел введем отношение «≤» следующим образом: $|X| \le |Y| \Leftrightarrow X$ изоморфно некоторому подмножеству множества Y. Говорят, что мощность множества X меньше мощности множества Y (пишут $|X| < |Y|$), если $|X| \le |Y|$ и $X \neq Y$.

Известно, что мощность $\aleph_0$ счетных множеств меньше мощности $\aleph$: $\aleph_0 < \aleph$.

Есть ли между $\aleph_0$ и $\aleph$ другие кардинальные числа – знаменитая *проблема* (*гипотеза*) *континуума* в математике, которая в 1963 г. была решена американским математиком П. Коэном. Он доказал независимость гипотезы континуума от других аксиом теории множеств. Проблема континуума решается аналогично проблеме пятого постулата Евклида в геометрии. Ни утверждение проблемы, ни отрицание ее из аксиоматики теории множеств доказать нельзя. Если в качестве аксиомы взять, что между $\aleph_0$ и $\aleph$ есть другие кардинальные числа, то возникает одна ветвь математики, если нет, то другая, совершенно независимая.

Рассмотрим без доказательства несколько теорем, относящиеся к теории бесконечных множеств.

Теорема 3.4. Всякое подмножество счетного множества конечно или счетно.

Теорема 3.5. Объединение счетного числа счетных множеств счетно.

Теорема 3.6. Всякое бесконечное множество X содержит счетное подмножество Y такое, что $X \setminus Y$ есть бесконечное множество.

Теорема 3.7. Всякое бесконечное множество X содержит подмножество $Y \cong X$ такое, что $X \setminus Y$ есть бесконечное множество.

Теорема 3.8. (**Кантора – Бернштейна**). Если каждое из двух множеств X и Y изоморфно подмножеству другого, то множества X и Y изоморфны между собой, то есть $|X| \le |Y| \wedge |Y| \le |X| \Rightarrow |X| = |Y|$.

Замечание 3.5. Сергей Натанович Бернштейн (1880 – 1966) – советский математик.

Теорема 3.9. Для произвольного множества X мощность его булеана $P(X)$ равна $2^{|X|}$.

Теорема 3.10. Булеан $P(X)$ произвольного непустого множества X имеет мощность, большую, чем мощность множества X, то есть $(\forall X)\ |X| < 2^{|X|}$.

3.9. Отношение порядка. Диаграммы Хассе

Пусть A – непустое множество.

Определение 3.26. Отношение $P \subseteq A^2$ называется *предпорядком* (*квазипорядком*), если оно рефлексивно и транзитивно.

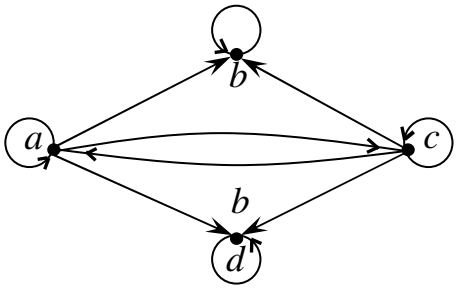


Рис. 3.6

Пример 3.17. Пусть $A = \{a, b, c, d\}$. Отношение $P = \{(a, a), (a, b), (a, c), (a, d), (b, b), (c, a), (c, b), (c, c), (c, d), (d, d)\}$ на множестве A является предпорядком (рис. 3.6).

Заметим, что симметричный предпорядок является отношением эквивалентности.

Определение 3.27. Отношение $P \subseteq A^2$ называется *частичным порядком*, если оно рефлексивно, транзитивно и антисимметрично. Таким образом, частичный порядок представляет собой антисимметричный предпорядок. Частичный порядок обозначается символом $\le$, а обратное ему отношение $\le^{-1}$ – символом $\ge$.

Определение 3.28. Отношение $< \subseteq A^2$ называется *строгим порядком*, если оно определяется по следующему правилу: $(\forall x, y \in A)\ x < y \Leftrightarrow x \le y$ и $x \ne y$.

Отношение строгого порядка не является частичным порядком, так как оно не рефлексивно.

Пример 3.18. Отношение из примера 3.17 не является частичным порядком, а отношение делимости на множестве целых чисел – является.

Определение 3.29. Пусть $\le \subseteq A^2$ и $x, y \in A$. Элементы x и y называются *несравнимыми*, если нельзя сказать, что $x \le y$ или $y \le x$.

Пример 3.19. Пусть $A = \{a, b, c, d\}$. Отношение включения $\subseteq$ на булеане $P(A)$ является частичным порядком. Элементы $B = \{a, c\}$ и $C = \{b, d\}$ из $P(A)$ являются несравнимыми, так как $(B, C) \notin \subseteq$ и $(C, B) \notin \subseteq$.

Определение 3.30. Частичный порядок $\le \subseteq A^2$ называется *линейным порядком*, если $(\forall x, y \in A)\ x \le y$ или $y \le x$.

Определение 3.31. Пусть $A \ne \varnothing$ и $\le$ – частичный (линейный) порядок на A. Упорядоченная пара $< A, \le >$ называется *частично* (*линейно*) *упорядоченным множеством*.

Другими словами, частично (линейно) упорядоченным множеством является непустое множество A, на котором зафиксирован некоторый частичный (линейный) порядок $\leq$.

Пример 3.20. Пара $< Z, \leq >$, где $\leq$ – отношение делимости на множестве Z, является частичным, но не линейным порядком. Пары $< N, \leq >$, $< R, \leq >$ с обычными отношениями $\leq$ образуют линейно упорядоченные множества.

Определение 3.32. Элемент $a \in A$ частично упорядоченного множества $< A, \leq >$ называется *максимальным* (*минимальным*), если $(\forall x \in A)\ a \leq x\ (x \leq a) \Rightarrow \Rightarrow x = a$.

Определение 3.33. Элемент $a \in A$ частично упорядоченного множества $< A, \leq >$ называется *наибольшим* (*наименьшим*), если $(\forall\ x \in A)\ x \leq a\ (a \leq x)$.

Наибольший (наименьший) элемент частично упорядоченного множества $< A, \leq >$ (если он существует) обозначается через *max A (min A*). Наибольший элемент часто называют *единицей*, а наименьший – *нулем* множества $< A, \leq >$.

Теорема 3.11. Пусть $< A, \leq >$ является частично упорядоченным множеством, где A – непустое и конечное множество. Тогда $< A, \leq >$ содержит хотя бы один минимальный элемент, и если он является единственным, то он также является и наименьшим. Аналогично, $< A, \leq >$ содержит хотя бы один максимальный элемент, и если он является единственным, то он также является наибольшим.

Пример 3.21. Частично упорядоченное множество $< A, \leq >$, где $A = \{a, b, c, d\}$, а граф отношения $\leq$ изображен на рис. 3.7, имеет единственный минимальный и он же наименьший элемент a, максимальные элементы c и d, но не имеет наибольшего элемента.

Пример 3.22. Частично упорядоченное множество $< B, \leq >$, где $B = \{1, 2, 3, 4\}$, а граф отношения $\leq$ изображен на рис. 3.8, имеет минимальные элементы 1 и 2, единственный максимальный и он же наибольший элемент 4, но не имеет наименьшего элемента.

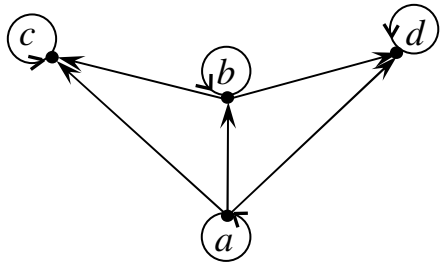


Рис. 3.7

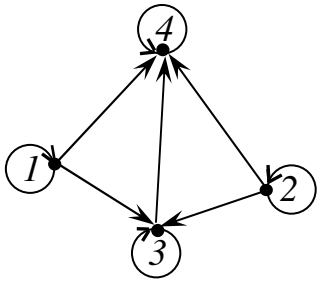


Рис. 3.8

Замечание 3.6. Всякий наибольший элемент частично упорядоченного множества является максимальным, а всякий наименьший элемент – минимальным. Обратное утверждение, вообще говоря, неверно (см. примеры 3.21 и 3.22).

Определение 3.34. Пусть $< A, \leq >$ – частично упорядоченное множество и $B \subseteq A$. Элемент $a \in A$ называется *верхней* (*нижней*) *гранью подмножества B*, если $(\forall\ b \in B)\ b \leq a$ $(a \leq b)$.

Пример 3.23. Рассмотрим частично упорядоченное множество $< R, \leq >$ и $B = [0;1)$. Тогда любое число $x \geq 1$ является верхней гранью B, а любое число $x \leq 0$ – нижней гранью B.

Определение 3.35. Пусть $< A, \leq >$ – частично упорядоченное множество и $B \subseteq A$. *Точной верхней* (*нижней*) *гранью подмножества B* называется наименьшая верхняя (наибольшая нижняя) грань множества B.

Точная верхняя грань подмножества B обозначается через *sup B* (супремум), а точная нижняя грань – через *inf B* (инфимум).

Пример 3.24. В условиях примера 3.21 имеем, что $sup\ B = 1$, $inf\ B = 0$.

Определение 3.36. Линейный порядок $\leq$ на множестве A называется *полным*, если каждое непустое подмножество множества A имеет наименьший элемент.

Определение 3.37. Пусть $\leq$ – полный порядок на непустом множестве A. Упорядоченная пара $< A, \leq >$ называется *вполне упорядоченным множеством*.

Пример 3.25. Упорядоченная пара $< N, \leq >$ является вполне упорядоченным множеством, а $< [-1;1], \leq >$ не является, так как, например, полуинтервал (0;1], являющийся подмножеством [-1;1], не содержит наименьшего элемента.

Пусть $< A, \leq >$ – частично упорядоченное множество и $x, y \in A$. Говорят, что элемент y *покрывает* элемент x, если $x \leq y$ и не существует такого элемента $z \in A$, что $x < z < y$. Если A – любое конечное множество, то частично упорядоченное множество $< A, \leq >$ можно представить в виде схемы, в которой каждый элемент изображается точкой на плоскости, и если элемент y покрывает элемент x, то точки, изображающие элементы x и y, соединяют отрезком, причем точку, соответствующую элементу x, располагают ниже точки, соответствующей элементу y. Такие схемы называются *диаграммами Хассе*.

Пример 3.26. Диаграммы Хассе частично упорядоченных множеств $< A, \leq >$ из примера 3.21 и $< B, \leq >$ из примера 3.22 изображены соответственно на рис.3.9 и 3.10.

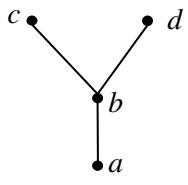


Рис. 3.9

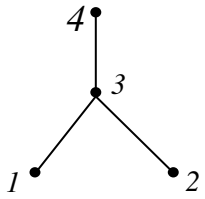
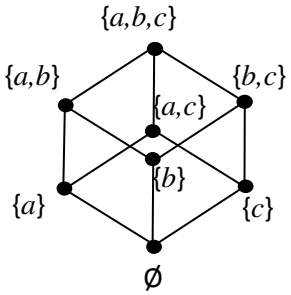


Рис. 3.10

Пример 3.27. а) Рассмотрим частично упорядоченное множество $< P(A), \subseteq >$, где $A = \{a, b, c, d\}$ и $P(A) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$. На рис. 3.11 изображена диаграмма Хассе, соответствующая $< P(A), \subseteq >$. б) Пусть $B = \{1, 2, 3, 4, 5, 6, 8\}$ и $\leq$ – обычное отношение порядка на множестве натуральных чисел, не превосходящих восьми. Диаграмма Хассе,



соответствующая линейно упорядоченному множеству $< B, \leq >$, изображена на рис. 3.12.

Рис. 3.11 Рис. 3.12

3.10. Функции

Определение 3.38. Соответствие $f \subseteq A \times B$ называется *функцией* из множества A в множество B, если f функциональное и полностью определенное. Соответствие f называется *частичной функцией*, если f функциональное и частично определенное.

Таким образом, соответствие $f \subseteq A \times B$ является функцией из A в B, если для любого $x \in A$ существует единственный элемент $y \in B$ такой, что $(x, y) \in f$. При этом элемент y обозначается через $f(x)$ и называется *значением* функции f для *аргумента* x. Функция f из A в B обозначается через $f: A \to B$ или $A \xrightarrow{f} B$. Если $(x, y) \in f$, то используется общепринятая запись $y = f(x)$, а также запись $f: x \mapsto y$ (означает, что функция f ставит в соответствие элементу x элемент y).

Область определения и область значений функции, равные функции определяются так же, как и для соответствий.

Пример 3.28. Какие из соответствий, графы которых изображены на рис. 3.13, являются функциями? Найдите для каждой функции ее область определения и область значений.

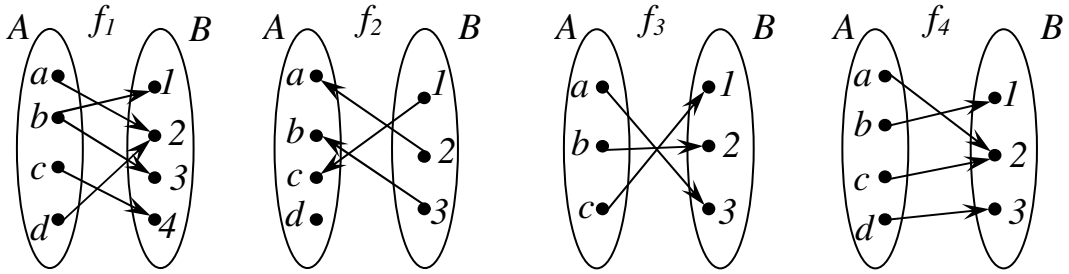


Рис. 3.13

Решение. Соответствия f_2, f_3 и f_4 являются функциями, а f_1 – не является, так как $f_1(b) = \{1, 3\}$. Далее имеем: $Dom\, f_2 = \{1, 2, 3\} = B$, $Im\, f_2 = \{a, b, c\} \subseteq A$; $Dom\, f_3 = \{a, b, c\} = A$, $Im\, f_3 = \{1, 2, 3\} = B$; $Dom\, f_4 = \{a, b, c, d\} = A$, $Im\, f_4 = \{1, 2, 3\} = B$.

Аргументами функции могут являться элементы произвольной природы, в частности, кортежи длины n $(x_1, x_2, \ldots, x_n)$. Функцию $f: A^n \to B$ называют *n-местной функцией* из A в B. Тогда пишут $y = f(x_1, x_2, \ldots, x_n)$ и говорят, что y есть значение функции f при значении аргументов $x_1, x_2, \ldots, x_n$.

Функции называются также *отображениями*. Пусть f – функция из A в B. Если $A = Dom\ f$ и $Im\ f \subseteq$ B, то говорят, что f есть *отображение множества A в множество B*. Если $A = Dom\ f$ и $B = Im\ f$, то говорят, что f есть *отображение множества A на множество B*.

Определение 3.39. Функция $f \subseteq A \times B$ называется *инъективной*, или *инъекцией*, если $(\forall\ x, y \in A)\ f(x) = f(y) \Rightarrow x = y$.

Определение 3.40. Функция $f \subseteq A \times B$ называется *сюръективной*, или *сюръекцией*, если для каждого элемента $y \in B$ существует хотя бы один элемент $x \in A$ такой, что $y = f(x)$.

Заметим, что сюръективная функция $f \subseteq A \times B$ является отображением A на B.

Определение 3.41. Функция $f \subseteq A \times B$ называется *биективной* (*биекцией*) или *взаимно однозначным соответствием между множествами A и B*, если она одновременно инъективна и сюръективна.

Пример 3.29. Какие из соответствий, графы которых изображены на рис. 3.13, являются инъективными, сюръективными, биективными функциями?

Решение. Функции f_2 и f_3 являются инъективными; f_3 и f_4 – сюръективными; f_3 – биективной.

Определение 3.42. Если соответствие, обратное к функции $f \subseteq A \times B$, является функциональным и полностью определенным, то оно называется *функцией*, *обратной* к f и обозначается f^{-1}.

Так как в обратном соответствии образы и прообразы меняются местами, то для существования функции, обратной к функции $f \subseteq A \times B$, необходимо и достаточно, чтобы $Im\ f = B$ и каждый элемент $y \in Im\ f$ имел единственный прообраз.

Утверждение 3.4. Для функции $f\colon A \to B$ существует обратная к ней функция $f^{-1}\colon B \to A$ тогда и только тогда, когда f – биекция.

Определение 3.43. Пусть даны функции $f\colon A \to B$ и $g\colon B \to C$. Функция $h\colon A \to C$ называется *композицией* (*суперпозицией*) *функций f* и g, если $(\forall\ x \in A)\ h(x) = g(f(x))$.

Композиция функций f и g обозначается через $f \circ g$, при этом знак $\circ$ часто опускается.

Задачи и упражнения к главе 3

1. Для бинарного отношения $P \subseteq A \times B$ найти $Dom\ P$, $Im\ P$:

а) $A = \{1, 2, 3, 4, 5\}$, $B = \{\{1\}, \{1,2\}, \{2,5\}, \{3\}\}$, $aPX \Leftrightarrow a \in X$, где $a \in A$, $X \in B$;

б) $A = \{1, 2, 3, 4, 5\}$, $B = \{12, 16\}$, $aPb \Leftrightarrow b \vdots a$ (см. определение 4.26);

в) $A = Z \times Z$, $B = Q$, $(a, b)Pc \Leftrightarrow c = \frac{a}{b}$, где $(a, b) \in Z \times Z$, $c \in Q$;

г) $A = Z$, $B = Q$, $aPb \Leftrightarrow a \cdot b = 1$;

д) $P = \{(x, y) \in R \times R \mid y = x^2 + x + 1\}$;

е) $P = \{(x, y) \in R \times R \mid y = lg(x^2 + 1)\}$;

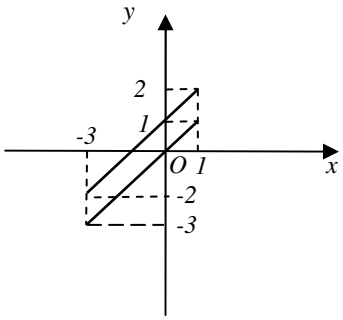
ж) $P = \{(x, y) \in R \times R \mid y = arcos\ x\}$;

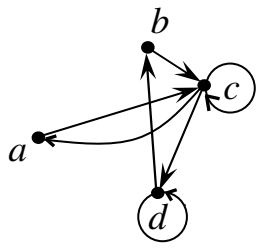
з) $P = \{(x, y) \in R \times R \mid y = tg\ x\}$.

2. График отношения P, заданного на множестве R, изображен на рис. 3.14.

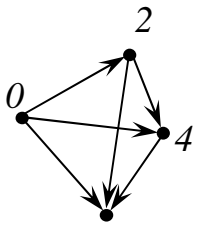
а) Найти *Dom P*, *Im P*;

б) Установите, какие из следующих записей верны: $1P2$, $1P1$, $-3P-1$.

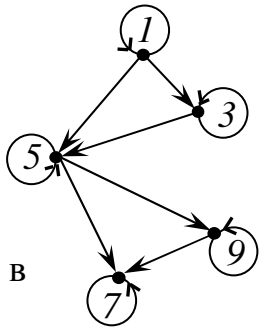




а



б



в

Рис. 3.14

Рис. 3.15

3. На множестве $X = \{2, 4, 6, 8, 10\}$ задано отношение P: «x кратно y».

а) Построить граф отношения P;

б) Перечислить все пары чисел из множества X, находящихся в отношении P;

в) Указать *Dom P*, *Im P*.

4. Изобразить граф отношения $P = \{(a, 1), (a, 2), (b, 2), (b, 3), (c, 1), (c, 4)\}$ и $Q = \{(1, \alpha), (2, \beta), (3, \alpha)\}$. Найти *Dom P*, *Im* Q, Q^{-1}, $P \circ Q$.

5. Определить свойства бинарного отношения по его графу (рис. 3.15).

6. Выяснить, является ли отношение P рефлексивным, симметричным, антисимметричным, транзитивным:

а) $P \subseteq R^2$, $(x, y) \in P \Leftrightarrow x^2 + y^2 = 1$;

б) $P \subseteq Z^2$, $(x, y) \in P \Leftrightarrow x - y$ четно.

7. Дано: $A = \{a, b, c\}$, $B = \{1, 2, 3, 4\}$, $P_1 \subseteq A \times B$, $P_2 \subseteq B^2$, где:

а) $P_1 = \{(a,3), (a,2), (a,4), (b,1), (c,2), (c,4), (c,3)\}$,
$P_2 = \{(1,1), (2,2), (2,1), (3,3), (4,4), (4,3), (1,4), (2,4), (3,2), (3,4)\}$;

б) $P_1 = \{(b,2), (a,3), (b,1), (b,4), (c,1), (c,2), (c,4)\}$,
$P_2 = \{(1,1), (1,2), (1,4), (2,2), (2,4), (3,3), (3,2), (3,4), (4,4)\}$.

Изобразить P_1 и P_2 с помощью графов. Найти матрицу отношения $\left\|(P_1 \circ P_2)^{-1}\right\|$.

Проверить с помощью матрицы $\|P_2\|$, является ли отношение P_2 рефлексивным, антирефлексивным, симметричным, антисимметричным, транзитивным?

8. На рис. 3.16 приведены графы отношений P, Q, S, T. Укажите среди них отношения эквивалентности.

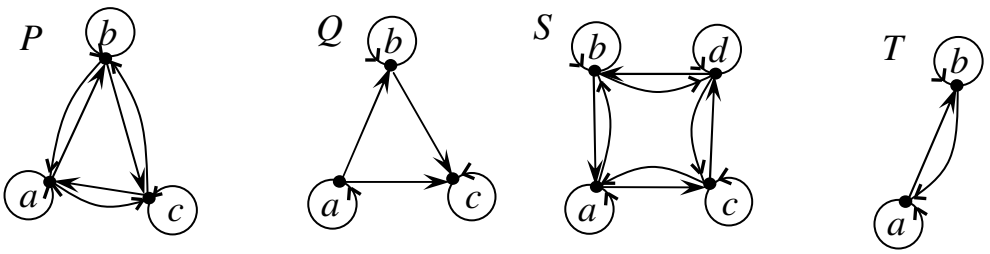


Рис. 3.16

9. На множестве $X = \{a, b, c, d, e\}$ задано отношение $T = \{(a, a), (a, b), (b, b), (b, a), (c, c), (c, d), (d, c), (d, d), (e, e)\}$. Доказать, что T – отношение эквивалентности. Найти классы эквивалентности.

10. На множестве $A = \{1, 2, 3, 4, 5\}$ задано отношение эквивалентности T. Оно определяет разбиение этого множества на классы эквивалентности: $A_1 = \{1, 3, 5\}$, $A_2 = \{2, 4\}$. Построить граф отношения T. Записать все упорядоченные пары чисел, принадлежащих этому отношению.

11. На множестве $X = \{1, 2, 3, 4, 5, 6\}$ задано отношение $S = \{(1,1), (1,2), (2,1), (2,2), (3,3), (4,4), (5,4), (5,5), (6,6), (4,6), (6,4), (5,6), (6,5), (4,5)\}$. Доказать, что S – отношение эквивалентности. Построить граф отношения S. Разбить на классы эквивалентности множество X.

12. На множестве $X = \{a, b, c, d, e, f\}$ задано отношение эквивалентности T. Оно определяет разбиение этого множества на классы эквивалентности $\{a, b\}$, $\{c\}$, $\{d\}$, $\{e, f\}$. Записать все пары элементов, принадлежащих этому отношению. Построить его граф.

13. Доказать, что отношение P: $(a,b)P(c,d) \Leftrightarrow a^2 + b^2 = c^2 + d^2$ является отношением эквивалентности на множестве $R \times R$. Найти классы эквивалентности и изобразить их на координатной плоскости.

14. На множестве N задано бинарное отношение P: $aPb \Leftrightarrow$ последняя цифра в десятичной записи числа a совпадает с последней цифрой в десятичной записи числа b. Доказать, что P – отношение эквивалентности. Сколько элементов в фактор-множестве N/P?

15. Пусть $A = \{1, 2, 3\}$. Доказать, что заданное на $P(A)$ бинарное отношение R: $X\,R\,Y \Leftrightarrow |X| = |Y|$, является отношением эквивалентности. Найти классы эквивалентности.

16. Доказать, что следующие отношения являются отношениями эквивалентности:

а) отношение P на множестве точек плоскости: $(M_1, M_2) \in P \Leftrightarrow$ ординаты точек M_1 и M_2 равны;

б) отношение P на множестве C: $(z_1, z_2) \in P \Leftrightarrow |z_1| = |z_2|$;

в) отношение P на множестве $C \setminus \{0\}$: $(z_1, z_2) \in P \Leftrightarrow arg\ z_1 = arg\ z_2$.

Найти классы эквивалентности. Изобразить их на плоскости.

17. Даны множества: A – множество букв латинского алфавита, $B = \{a, b, c, d, e, f\}$, $C = \{c, f\}$, $D = \{b, a, d\}$, $E = \{k, l, m, n, d\}$, $F = \{k, l, m, n\}$. Рассмотреть между ними отношение P: «быть подмножеством». Построить граф отношения P. Выписать все пары множеств, находящихся в отношении P. Определить свойства этого отношения. Доказать, что $<M, P>$ – частично упорядоченное множество, где M – множество всех множеств, указанных выше. Построить диаграмму Хассе частично упорядоченного множества $<M, P>$. Определить минимальные и максимальные элементы, наименьший и наибольший элементы (если они имеются).

18. Отношение P задано на множестве $A = \{a, b, c, d, e\}$ с помощью графа (рис. 3.17). Доказать, что пара $<A, P>$ – частично упорядоченное множество. Построить диаграмму Хассе.

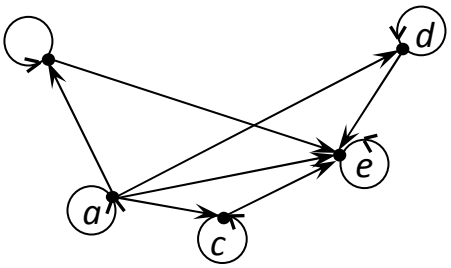


Рис. 3.17

19. Пусть <A, P> – частично упорядоченное множество, имеющее диаграмму Хассе, приведенную на рис. 3.18. Составить список элементов, связанных отношением P. Определить минимальные и максимальные элементы, наибольший и наименьший элементы (если они имеются).

20. Диаграмма Хассе для частично упорядоченного множества $\{a, b, c, d, e, f, g, h, i\}$ представлена на рис. 3.19. Составить список элементов, связанных отношением порядка P и определить максимальные и минимальные элементы, наименьший и наибольший элементы (если они есть).

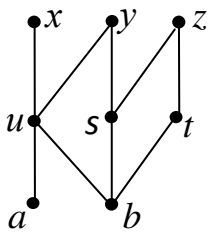


Рис. 3.18

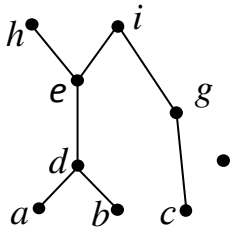


Рис. 3.19

21. Нарисовать диаграммы Хассе для каждого из следующих множеств, упорядоченных отношением делимости: $nRm \Leftrightarrow n$ делит m:

а) {1, 2, 3, 4, 6, 12}; б) {1, 2, 4, 5, 10, 20}; в) {1, 2, 4, 8, 16, 32}.

22. Пусть $A = \{0; 1; 2\}\times\{2; 5; 8\}$. Отношение частичного порядка R на A определено следующим образом: $(a, b)R(c, d) \Leftrightarrow (a + b) \,|\, (c + d)$ ($a + b$ делит $c + d$). Нарисовать диаграмму Хассе для частично упорядоченного множества A. Какие элементы на частично упорядоченном множестве будут являться максимальными, минимальными? Имеет ли A наибольший и наименьший элементы?

23. Определить свойства отображения f (инъективность, сюръективность, биективность). Указать $\mathrm{Im}\, f$.

а) $f\colon N \to N,\ f(x) = x + 2$;

б) $f\colon R \to R,\ f(x) = 2x$;

в) $f\colon R \to R,\ f(x) = 2^x$;

г) $f\colon R \to R,\ f(x) = x^2 - 2x + 2$;

д) $f\colon R_+ \to R,\ f(x) = \lg x$;

е) $f\colon R \to R,\ x \mapsto 2^{x^2+3x+4}$;

ж) $f\colon Z\times Z \to Z,\ (a,b) \mapsto a + b$;

з) $f\colon Z \to Z\times Z,\ a \mapsto (a;a)$;

и) A – конечное множество, $f\colon \mathrm{P}(A) \to N, X \mapsto |X|$;

к) $f\colon R \to R,\ x \mapsto x^3$.

Глава 4. Алгебраические структуры

4.1. Алгебраические операции и их свойства

Бинарные и n-местные алгебраические операции

Пусть A – непустое множество.

Определение 4.1. Отображение множества $A \times A$ в A называется *бинарной алгебраической операцией* на множестве A.

Примерами бинарных алгебраических операций являются обычное сложение и умножение на множестве целых чисел, объединение и пересечение на булеане непустого множества.

Определение 4.2. Отображение множества A^n в A называется *n-арной* (*n-местной*) *алгебраической операцией* на множестве A, а число n ($n \geq 1$) – *рангом операции*. Выделение (фиксация) некоторого элемента множества A называется *нульарной* (*нульместной*) *операцией* на множестве A, число 0 – *рангом нульарной операции*.

Определение 4.3. Частичная функция из множества A^n в A называется *частичной n-арной алгебраической операцией* на множестве A.

Пример 4.1. 1. Пусть $A \neq \varnothing$. Отображение, ставящее в соответствие каждому подмножеству $X \in P(A)$ его дополнение $\overline{X}$, является унарной алгебраической операцией на $P(A)$.

2. Операция деления рациональных чисел является частичной бинарной алгебраической операцией на множестве рациональных чисел.

3. Операция, ставящая в соответствие каждому кортежу натуральных чисел длины n наибольший общий делитель этих чисел, является n-арной алгебраической операцией на множестве N.

Для обозначения n-арной алгебраической операции используется та же форма записи, что и для произвольных отображений. Если f есть n-арная алгебраическая операция на множестве A и $((x_1, x_2, \ldots, x_n), x_{n+1}) \in f$, то пишут $x_{n+1} = f(x_1, x_2, \ldots, x_n)$ и говорят, что x_{n+1} является значением операции f при значениях аргументов $x_1, x_2, \ldots, x_n$.

Свойства бинарных алгебраических операций

Пусть $*$ и $\circ$ – произвольные бинарные алгебраические операции на непустом множестве A.

Определение 4.4. Бинарная алгебраическая операция $*$ называется *коммутативной*, если $(\forall a, b \in A)\ a * b = b * a$.

Определение 4.5. Бинарная алгебраическая операция $*$ называется *ассоциативной*, если $(\forall a, b, c \in A)\ a * (b * c) = (a * b) * c$.

Если операция $*$ ассоциативна, то можно опускать скобки и писать $a * b * c$ вместо $a * (b * c)$ или $(a * b) * c$.

Определение 4.6. Бинарная алгебраическая операция $\circ$ называется *дистрибутивной* относительно бинарной операции $*$, если $(\forall a, b, c \in A)\ (a * b) \circ c = (a \circ c) * (b \circ c)$ и $c \circ (a * b) = (c \circ a) * (c \circ b)$.

Пример 4.2. 1. Сложение и умножение действительных чисел являются коммутативными и ассоциативными бинарными алгебраическими операциями. Умножение действительных чисел дистрибутивно относительно сложения, но сложение не дистрибутивно относительно умножения, так как условие $(\forall a, b, c \in A)\ a + b \cdot c = (a + b) \cdot (a + c)$ не выполняется.

2. Операции объединения и пересечения подмножеств непустого множества A коммутативны, ассоциативны и дистрибутивны относительно друг друга на булеане $P(A)$.

3. Композиция функций есть ассоциативная бинарная алгебраическая операция. Композиция функций не коммутативна, так как условие $(\forall f, g)\ f \circ g = g \circ f$ не выполняется.

Нейтральные элементы

Пусть $*$ – бинарная алгебраическая операция на непустом множестве A.

Определение 4.7. Элемент $e \in A$ называется *нейтральным* относительно операции $*$, если $(\forall a \in A)\ a * e = e * a = a$.

Теорема 4.1. Если нейтральный элемент относительно операции $*$ существует, то он единственен.

Доказательство. Пусть e и e' – нейтральные элементы относительно операции $*$. Тогда $e = e * e' = e'$, то есть $e = e'$.

Пример 4.3. 1. Число 0 есть нейтральный элемент относительно сложения действительных чисел. Число 1 есть нейтральный элемент относительно умножения действительных чисел.

2. На булеане $P(A)$ пустое множество является нейтральным элементом относительно объединения подмножеств непустого множества A, а $P(A)$ – нейтральным элементом относительно пересечения подмножеств.

Симметричные элементы

Пусть $*$ есть бинарная алгебраическая операция на непустом множестве A и элемент $e \in A$ – нейтральный элемент относительно $*$.

Определение 4.8. Элемент $a' \in A$ называется *симметричным* к элементу $a \in A$ относительно операции $*$, если $a * a' = a' * a = e$. В этом случае элемент a называется *симметризуемым*, а элементы a и a' *– взаимно симметричными*.

Пример 4.4. 1. Любое целое число имеет симметричный к нему элемент относительно сложения – то же число, взятое со знаком минус.

2. Любое ненулевое действительное число a имеет симметричный к нему элемент $\frac{1}{a}$, число нуль не имеет симметричного элемента относительно умножения.

Теорема 4.2. Если операция $*$ ассоциативна и элемент a симметризуем, то существует единственный элемент, симметричный к a.

Доказательство. Пусть a', a'' есть элементы, симметричные к элементу a относительно $*$. Следовательно, $a * a' = a' * a = e$ и $a * a'' = a'' * a = e$. Тогда в силу ассоциативности операции $*$ получаем

$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''$, то есть $a' = a''$.

Подмножества, замкнутые относительно бинарной алгебраической операции

Пусть $*$ – бинарная алгебраическая операция на непустом множестве A.

Определение 4.9. Подмножество B множества A называется замкнутым относительно операции $*$, если $(\forall\, a, b \in B)\ a * b \in B$.

Пустое множество замкнуто относительно любой операции $*$.

Пример 4.5. Сложение и вычитание являются бинарными алгебраическими операциями на множестве всех действительных чисел. Множество всех положительных действительных чисел замкнуто относительно сложения, но не замкнуто относительно вычитания.

Аддитивная и мультипликативная форма записи бинарной алгебраической операции

Для обозначения бинарной алгебраической операции $*$ наиболее часто используются аддитивная и мультипликативная формы записи. При аддитивной форме записи операцию $*$ называют *сложением*, а ее результат $a * b$ – *суммой* a и b. При этом вместо $a * b$ пишут $a + b$. Нейтральный элемент относительно сложения называют *нулевым элементом* (или *нулем*) и обозначают символом 0.

Элемент, симметричный к элементу a, называют *противоположным* к элементу a и обозначают через $-a$.

При мультипликативной форме записи операцию $*$ называют *умножением*, а ее результат $a * b$ – *произведением* a и b. При этом вместо $a * b$ пишут $a \cdot b$. Нейтральный элемент относительно умножения называют *единичным элементом* (или *единицей*) и обозначают символом 1. Элемент, симметричный к элементу a, называют *обратным* к элементу a и обозначают через a^{-1}.

4.2. Понятие алгебраической структуры

Определение 4.10. *Алгебраической структурой* (*универсальной алгеброй* или просто *алгеброй*) называется упорядоченная пара $\mathcal{A} = < A, \Sigma >$, где A – непустое множество и Σ – множество алгебраических операций на A.

Таким образом, алгебра представляет собой непустое множество A вместе с заданной на нем совокупностью операций $\Sigma = \{f_1, \ldots, f_m, \ldots\}$, где f_i: $A^{n_i} \to A$ и n_i – ранг операции f_i. Множество A называется *основным* (*несущим*) *множеством* или *основой* (*носителем*) алгебры; упорядоченная последовательность рангов $(n_1, \ldots, n_m)$ называется *типом* алгебры; множество операций $\boldsymbol{\Sigma}$ называется *сигнатурой* алгебры.

Если $< A, \Sigma >$ – алгебра, то также говорят, что множество A есть алгебра относительно операций Σ.

Наиболее частым является случай, когда сигнатура конечна. Если $\Sigma = \{f_1, \ldots, f_m\}$, то вместо записи $\mathcal{A} = < A, \{f_1, \ldots, f_m\} >$ обычно употребляется запись $\mathcal{A} = < A, f_1, \ldots, f_m >$.

Замечание 4.1. Для обозначения алгебры везде, где это необходимо, используется рукописная прописная буква латинского алфавита, а для обозначения ее носителя – соответствующая печатная прописная буква.

Определение 4.11. Алгебры $\mathcal{A} = < A, f_1, \ldots, f_m >$ и $\mathcal{B} = < B, f_1', \ldots, f_m' >$ называются *однотипными*, если их типы совпадают, то есть ранг операции f_i совпадает с рангом соответствующей ей операции f_i' для $i = 1,\ldots, m$.

Пример 4.6. 1. Пусть + и · (сложение и умножение) – арифметические операции на множестве действительных чисел. Алгебра $< R, +, \cdot >$ является алгеброй типа (2, 2).

2. Пусть $P(A)$ – булеан непустого множества A и $\cup, \cap, \bar{}$ – операции пересечения, объединения и дополнения над подмножествами множества A. Алгебра $< P(A), \cup, \cap, \bar{} >$ является алгеброй типа (2, 2, 1).

Определение 4.12. Пусть алгебры $\mathcal{A} = < A, f_1, \ldots, f_m >$ и $\mathcal{B} = < B, f_1', \ldots, f_m' >$ – однотипные алгебры. Алгебра $\mathcal{B}$ называется *подалгеброй* алгебры $\mathcal{A}$, если $B \subseteq A$ и любая операция f_i' ($i = 1, \ldots, m$) алгебры $\mathcal{B}$ и соответствующая ей операция f_i алгебры $\mathcal{A}$ удовлетворяют условию:

$(\forall\, b_1, \ldots, b_{n_i} \in B)\ f_i'(b_1, \ldots, b_{n_i}) = f_i(b_1, \ldots, b_{n_i})$, где n_i – ранг операций f_i' и f_i. (12)

Определение 4.13. Пусть $\mathcal{A} = < A, f_1, \ldots, f_m >$ – алгебра и $B \subseteq A$. Подмножество B множества A называется *замкнутым в алгебре* $\mathcal{A}$, если B замкнуто относительно каждой операции f_i ($i = 1, \ldots, m$) алгебры $\mathcal{A}$, то есть выполняется условие: $(\forall\, b_1,\ldots,b_{n_i} \in B)\ f_i(b_1,\ldots,b_{n_i}) \in B$, где n_i – ранг операции f_i. (13)

Если f_i – нульарная операция, которая выделяет элемент $a \in A$, то условие (13) принимает вид $a \in B$.

Из определений 4.12 и 4.13 непосредственно вытекает следующая теорема.

Теорема 4.3. Пусть $\mathcal{A} = < A, f_1, \ldots, f_m >$ – алгебра и B – непустое подмножество множества A, замкнутое в алгебре $\mathcal{A}$. Тогда алгебра $\mathcal{B} = < B, f_1, \ldots, f_m >$ является подалгеброй алгебры $\mathcal{A}$.

Пример 4.7. Рассмотрим алгебру $< N, +, \cdot >$, где + и · – обычные операции сложения и умножения натуральных чисел. Пусть M – множество четных чисел, то есть $M = \{2k \mid k \in N\}$. Множество M замкнуто относительно операций сложения и умножения натуральных чисел. Действительно,

$(\forall\, 2k_1, 2k_2 \in M)\ 2k_1 + 2k_2 = 2(k_1 + k_2) \in M$ и $2k_1 \cdot 2k_2 = 2(2k_1 \cdot k_2) \in M$, так как множество N замкнуто относительно сложения и умножения. Следовательно, по теореме 4.3 алгебра $< M, +, \cdot >$ является подалгеброй алгебры $< N, +, \cdot >$.

4.3. Алгебры с одной бинарной алгебраической операцией

Рассмотрим алгебры, наиболее часто используемые в теории и на практике.

Пусть A – непустое множество.

Определение 4.14. Алгебра $\mathcal{A} = < A, * >$, где $*$ – бинарная алгебраическая операция, называется группоидом.

Таким образом, группоид определяется непустым множеством A и правилом, по которому можно найти значение операции $*$ для любых двух элементов из A.

Если множество A конечно, то эту информацию можно записать в виде таблицы.

Определение 4.15. Пусть на конечном множестве $A = \{a_1, \ldots, a_n\}$ определена бинарная операция $*$. Таблица, состоящая из n строк и n столбцов, в которой на пересечении i-й строки и j-го столбца располагается значение операции $a_i * a_j$, называется *таблицей Кэли*:

$*$	a_1	a_2	…	a_j	…	a_n
a_1	a_1*a_1	a_1*a_2	…	a_1*a_j	…	a_1*a_n
a_2	a_2*a_1	a_2*a_2	…	a_2*a_j	…	a_2*a_n
⋮	⋮	⋮	…	⋮	…	⋮
a_i	a_i*a_1	a_i*a_2	…	a_i*a_j	…	a_i*a_n
⋮	⋮	⋮	…	⋮	…	⋮
a_n	a_n*a_1	a_n*a_2	…	a_n*a_j	…	a_n*a_n

Замечание 4.2. Артур Кэли (1821 – 1895) – английский математик.

Замечание 4.3. 1. Если операция $*$ коммутативна, то таблица Кэли симметрична относительно главной диагонали.

2. Если для некоторого $i \in \{1, 2, \ldots, n\}$ элемент a_i является нейтральным элементом относительно операции $*$, то соответствующие этому элементу i-я строка и i-й столбец таблицы Кэли имеют вид $(a_1, a_2, \ldots, a_n)$.

3. Пусть элемент a_i – нейтральный элемент относительно операции $*$. Для элемента a_j существует симметричный к нему элемент относительно $*$, если в таблице Кэли среди элементов j-й строки и j-го столбца есть элемент a_i.

Определение 4.16. Алгебра $\mathcal{A} = < A, * >$, где $*$ – ассоциативная бинарная алгебраическая операция, называется *полугруппой*.

Пример 4.8. Алгебра $< N, + >$ является полугруппой, так как бинарная операция $+$ (обычная операция сложения натуральных чисел) ассоциативна.

Определение 4.17. Алгебра $\mathcal{A} = < A, * >$, в которой $*$ является ассоциативной бинарной алгебраической операцией и существует нейтральный элемент e относительно $*$, называется *моноидом*.

Другими словами, моноидом является полугруппа с нейтральным элементом.

Пример 4.9. Алгебра $< N, \cdot >$ образует моноид, так как бинарная операция умножения ассоциативна и натуральное число 1 является нейтральным элементом относительно умножения.

Определение 4.18. Алгебра $\mathcal{A} = < A, * >$ называется *группой*, если выполняются условия (аксиомы):

1) $*$ – ассоциативная бинарная операция;
2) существует нейтральный элемент относительно $*$;

3) для каждого элемента $a \in A$ существует симметричный к нему элемент $a' \in A$ относительно операции $*$.

Таким образом, группа – это моноид, в котором каждый элемент симметризуем.

Определение 4.19. Полугруппа, моноид или группа называется *коммутативной* (коммутативным) или *абелевой* (абелевым), если бинарная алгебраическая операция коммутативна.

Замечание 4.4. Нильс Абель (1802 – 1829) – норвежский математик.

Определение 4.20. Если носитель группы имеет конечную мощность, то группа называется *конечной*, а мощность ее носителя – *порядком* группы. В противном случае группа называется *бесконечной*.

Пример 4.10. Полугруппы $< N, + >$ и $< N, \cdot >$ не являются группами, так как в первой из них не существует нейтральный элемент относительно сложения, а во второй для любого элемента, за исключением числа 1, не существует симметричный к нему элемент.

Пример 4.11. Алгебра $< Z, + >$ образует коммутативную аддитивную группу целых чисел. Действительно, бинарная алгебраическая операция сложения ассоциативна, число 0 есть нейтральный (нулевой) элемент, а симметричным (противоположным) к любому $z \in Z$ является число $-z$.

Пример 4.12. Алгебра $< R \setminus \{0\}, \cdot >$ есть коммутативная мультипликативная группа действительных чисел, так как бинарная алгебраическая операция умножения ассоциативна, нейтральным (единичным) элементом является число 1 и для всякого ненулевого действительного числа r существует симметричный (обратный) к нему элемент $\frac{1}{r}$.

Пример 4.13. Доказать, что множество $R \setminus \{1\}$ образует коммутативную группу относительно операции $*$, где $a * b = 2 \cdot (a - 1) \cdot (b - 1) + 1$.

Решение. Покажем, что $R \setminus \{1\}$ замкнуто относительно операции $*$, то есть $(\forall\, a, b \in R \setminus \{1\})\ a * b \in R \setminus \{1\}$.

Действительно, $a * b = 1 \Leftrightarrow 2 \cdot (a - 1) \cdot (b - 1) + 1 = 1 \Leftrightarrow$
$\Leftrightarrow (a - 1) \cdot (b - 1) = 0 \Leftrightarrow a = 1 \vee b = 1$. Отсюда
$(\forall\, a, b \in R)\ a \neq 1 \wedge b \neq 1 \Rightarrow a * b \neq 1$. Далее проверим выполнение аксиом группы.

1. Докажем, что операция $*$ ассоциативна, то есть
$(\forall\, a, b, c \in R \setminus \{1\})\ (a * b) * c = a * (b * c)$.

Рассмотрим левую и правую части этого равенства:
$(a * b) * c = (2 \cdot (a - 1) \cdot (b - 1) + 1) * c = 2 \cdot ((2 \cdot (a - 1) \cdot (b - 1) + 1) - 1) \cdot (c - 1) +$
$+ 1 = 4 \cdot (a - 1) \cdot (b - 1) \cdot (c - 1) + 1,$
$a * (b * c) = a * (2 \cdot (b - 1) \cdot (c - 1) + 1) = 2 \cdot (a - 1) \cdot ((2 \cdot (b - 1) \cdot (c - 1) + 1) - 1) +$
$+ 1 = 4 \cdot (a - 1) * (b - 1) \cdot (c - 1) + 1.$

Итак, первая аксиома группы выполняется. Легко видеть, что операция $*$ коммутативна, то есть $(\forall\, a, b \in R \setminus \{1\})\ a * b = b * a$.

2. Покажем, что существует нейтральный элемент относительно $*$, то есть

$(\forall\, a \in R \setminus \{1\})\ \exists\, e \in R \setminus \{1\}$: $a * e = e * a = a$. Рассмотрим равенство $a * e = a \Leftrightarrow 2\cdot(a-1)\cdot(e-1)+1 = a$. Выразим из этого равенства e:
$2\cdot(a-1)\cdot(e-1)-(a-1)=0 \Leftrightarrow (a-1)\cdot(2e-2-1)=0 \Leftrightarrow (a-1)\cdot(2e-3)=0 \Leftrightarrow$
$\Leftrightarrow 2e-3=0 \Leftrightarrow e=\frac{3}{2} \in R \setminus \{1\}$. Следовательно, $e=\frac{3}{2}$ – нейтральный элемент относительно $*$. Заметим, что $a * e = e * a$, так как $*$ коммутативна.

3. Докажем, что для каждого элемента из $R \setminus \{1\}$ существует симметричный к нему, то есть $(\forall\, a \in R \setminus \{1\})\ \exists\, a' \in R \setminus \{1\}$: $a * a' = a' * a = \frac{3}{2}$. Имеем:

$a * a' = \frac{3}{2} \Leftrightarrow 2\,(a-1)(a'-1)+1 = \frac{3}{2} \Leftrightarrow (a-1)\cdot(a'-1) = \frac{1}{4} \Leftrightarrow a'-1 = \frac{1}{4\cdot(a-1)} \Leftrightarrow$

$\Leftrightarrow a' = \frac{1}{4\cdot(a-1)} + 1 = \frac{1+4a-4}{4\cdot(a-1)} = \frac{4a-3}{4\cdot(a-1)}$. Покажем, что $a' \neq 1$. Действительно, в противном случае получаем

$$\frac{4a-3}{4\cdot(a-1)} = 1 \Leftrightarrow \frac{4a-3}{4\cdot(a-1)} - 1 = 0 \Leftrightarrow \frac{4a-3-4a+4}{4a-4} = 0 \Leftrightarrow 1 = 0.$$

Итак, для любого $a \in R \setminus \{1\}$ существует симметричный к нему элемент $a' = \frac{4a-3}{4\cdot(a-1)} \in R \setminus \{1\}$. Таким образом, алгебра $< R \setminus \{1\}, * >$ есть коммутативная группа.

4.4. Алгебры с двумя бинарными алгебраическими операциями

Среди алгебр с двумя бинарными алгебраическими операциями особо выделяются кольца и поля.

Определение 4.21. Алгебра $\mathcal{A} = < A, +, \cdot >$ называется *ассоциативным кольцом с единицей*, если выполняются следующие условия (аксиомы):

1) алгебра $< A, + >$ есть коммутативная аддитивная группа;
2) алгебра $< A, \cdot >$ есть мультипликативный моноид;
3) умножение дистрибутивно относительно сложения, то есть
$(\forall a, b, c \in A)\,(a+b)\cdot c = a\cdot c + b\cdot c$ и $c\cdot(a+b) = c\cdot a + c\cdot b$.

Замечание 4.5. В дальнейшем под словом «*кольцо*» будем подразумевать ассоциативное кольцо с единицей.

Элементы множества A называются *элементами кольца* $\mathcal{A} = < A, +, \cdot >$.

Определение 4.22. Группа $< A, + >$ называется *аддитивной группой кольца* $\mathcal{A} = < A, +, \cdot >$. Нейтральный элемент относительно сложения называется *нулем кольца* и обозначается через 0 или $0_{\mathcal{A}}$.

Определение 4.23. Моноид $< A, \cdot >$ называется *мультипликативным моноидом кольца* $\mathcal{A} = < A, +, \cdot >$. Нейтральный элемент относительно умножения называется *единицей кольца* $\mathcal{A}$ и обозначается через 1 или $1_{\mathcal{A}}$.

Определение 4.24. Кольцо называется *коммутативным*, если операция умножения коммутативна, т.е. $(\forall a,b\in A)\ \ a\cdot b=b\cdot a$.

Пример 4.14. Алгебра $< Z, +, \cdot >$ образует коммутативное кольцо целых чисел.

Определение 4.25. *Полем* называется коммутативное кольцо, в котором нуль кольца отличен от единицы кольца и для каждого ненулевого элемента существует обратный к нему относительно операции умножения.

Пример 4.15. Кольцо целых чисел $< Z, +, \cdot >$ полем не является, так как ни один ненулевой элемент, кроме 1, не обладает обратным к нему.

Пример 4.16. Множества Q, R и C образуют бесконечные поля относительно обычных операций сложения и умножения, которые соответственно называются полем рациональных чисел, полем действительных чисел и полем комплексных чисел.

Пример 4.17. Выяснить, образует ли алгебра $<\left\{\begin{pmatrix} x & y \\ y & x \end{pmatrix}\middle|\ x,y\in R\right\}, +, \cdot >$ кольцо, поле?

Решение. Докажем сначала, что операции сложения и умножения матриц являются бинарными алгебраическими операциями на множестве $M=\left\{\begin{pmatrix} x & y \\ y & x \end{pmatrix}\middle|\ x,y\in R\right\}$. Для этого достаточно показать замкнутость множества M относительно этих операций.

$$\left(\forall\begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix},\begin{pmatrix} x_2 & y_2 \\ y_2 & x_2 \end{pmatrix}\in M\right)\ \begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix}+\begin{pmatrix} x_2 & y_2 \\ y_2 & x_2 \end{pmatrix}=\begin{pmatrix} x_1+x_2 & y_1+y_2 \\ y_1+y_2 & x_1+x_2 \end{pmatrix}\in M,$$

$$\begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix}\cdot\begin{pmatrix} x_2 & y_2 \\ y_2 & x_2 \end{pmatrix}=\begin{pmatrix} x_1\cdot x_2+y_1\cdot y_2 & x_1\cdot y_2+y_1\cdot x_2 \\ y_1\cdot x_2+x_1\cdot y_2 & y_1\cdot y_2+x_1\cdot x_2 \end{pmatrix}\in M.$$

Следовательно, операции «+» и «·» – бинарные алгебраические операции на M.

Сложение произвольных матриц (если оно определено) коммутативно и ассоциативно. Значит, «+» коммутативно и ассоциативно на M. Очевидно, что матрица $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\in M$ есть нейтральный элемент относительно «+», а $\begin{pmatrix} -x & -y \\ -y & -x \end{pmatrix}\in M$ – противоположный элемент для произвольной матрицы $\begin{pmatrix} x & y \\ y & x \end{pmatrix}$ из множества M. Следовательно, $< M, + >$ – коммутативная группа.

Умножение произвольных матриц (если оно определено), а значит и матриц из множества M, является ассоциативной операцией. Пусть $\begin{pmatrix} x & y \\ y & x \end{pmatrix}$ – произвольная матрица из множества M.

$$\begin{pmatrix} x & y \\ y & x \end{pmatrix}\cdot\begin{pmatrix} a & b \\ b & a \end{pmatrix}=\begin{pmatrix} x & y \\ y & x \end{pmatrix}\Leftrightarrow\begin{pmatrix} xa+yb & xb+ya \\ ya+xb & yb+xa \end{pmatrix}=\begin{pmatrix} x & y \\ y & x \end{pmatrix}\Leftrightarrow\begin{cases} xa+yb=x \\ ya+xb=y \end{cases}\Rightarrow$$

$\Rightarrow b = \frac{y - ya}{x}$ при $x \neq 0$. Отсюда $xa + \frac{y^2 - y^2 a}{x} = x$. Выполним преобразования:

$x^2 a + y^2 - y^2 a = x^2 \Leftrightarrow y^2 (1 - a) = x^2 (1 - a) \Leftrightarrow 1 - a = 0 \Rightarrow a = 1 \Rightarrow b = \frac{y - y}{x} = 0.$

Если $x = 0$, то $\begin{cases} yb = 0 \\ ya = y \end{cases}$. Так как y – произвольное действительное число, то и в этом случае получаем, что $a = 1$ и $b = 0$. Получили, что $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in M$ – нейтральный элемент относительно «·». Следовательно, $< M, \cdot >$ – моноид.

Известно, что умножение дистрибутивно относительно сложения для произвольных матриц (если операции имеют смысл), в частности, и для матриц из множества M.

Таким образом, алгебра $< M, +, \cdot >$ – кольцо.

$$\left(\forall \begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix}, \begin{pmatrix} x_2 & y_2 \\ y_2 & x_2 \end{pmatrix} \in M\right) \begin{pmatrix} x_2 & y_2 \\ y_2 & x_2 \end{pmatrix} \cdot \begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix} = \begin{pmatrix} x_2 \cdot x_1 + y_2 \cdot y_1 & x_2 \cdot y_1 + y_2 \cdot x_1 \\ y_2 \cdot x_1 + x_2 \cdot y_1 & y_2 \cdot y_1 + x_2 \cdot x_1 \end{pmatrix} =$$

$$= \begin{pmatrix} x_1 & y_1 \\ y_1 & x_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 & y_2 \\ y_2 & x_2 \end{pmatrix}.$$

Получили, что «·» – коммутативно. Следовательно, кольцо коммутативно. Нуль кольца отличен от единицы кольца: $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Выясним, для каждого ли ненулевого элемента из множества M существует обратный к нему. Легко видеть, что роль обратного элемента к матрице из M играет обратная к ней матрица.

$$\left(\forall \begin{pmatrix} x & y \\ y & x \end{pmatrix} \in M\right) \exists \begin{pmatrix} x & y \\ y & x \end{pmatrix}^{-1} \Leftrightarrow \begin{vmatrix} x & y \\ y & x \end{vmatrix} \neq 0 \Leftrightarrow x^2 - y^2 \neq 0 \Leftrightarrow x^2 \neq y^2 \Leftrightarrow x \neq \pm y.$$

Значит, множество M содержит ненулевые матрицы, например матрицу $\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$, для которых не существуют обратные к ним.

Итак, алгебра $< M, +, \cdot >$ образует коммутативное кольцо, но не является полем.

4.5. Конечные поля

Наряду с бесконечными полями, существуют конечные поля, называемые *полями Галуа* в честь французского математика Эвариста Галуá (1811 – 1832), который в возрасте около 20 лет создал основы современной алгебры и, в частности, открыл конечные поля. Конечные поля играют центральную роль в криптографии, в математических моделях микромира и др. Рассмотрим основные построения теории конечных полей Галуа.

Определим сначала бинарное отношение делимости на множестве Z.

Определение 4.26. Целое число x *делится* на целое число y, если существует $z \in Z$ такое, что $x = y \cdot z$. При этом пишут $x \vdots y$ и говорят, что «x делится на y», или «x кратно y», или «y делит x».

Предложение «y делит x» записывают также в виде $y \mid x$.

Далее рассмотрим еще одно бинарное отношение $\equiv$ на множестве Z.

Определение 4.27. Целые числа x и y называются *сравнимыми по модулю* n ($n \in N$), если разность $(x - y)$ делится на n.

Если целое число x сравнимо с целым числом y по модулю n, то пишут $x \equiv y \pmod{n}$.

Покажем, что отношение сравнимости по модулю n обладает свойствами рефлексивности, симметричности и транзитивности, то есть является отношением эквивалентности. Действительно:

1) $(\forall x \in Z)\ x - x = 0 \vdots n \Rightarrow x \equiv x \pmod{n} \Rightarrow \equiv$ – рефлексивное отношение;

2) $(\forall x, y \in Z)\ x \equiv y \pmod{n} \Rightarrow y \equiv x \pmod{n}$, так как $(x - y) \vdots n \Rightarrow y - x = -(x - y) \vdots n$. Следовательно, отношение $\equiv$ симметрично.

3) $(\forall x, y, z \in Z)\ x \equiv y \pmod{n} \wedge y \equiv z \pmod{n} \Rightarrow x \equiv z \pmod{n}$, так как если $(x - y) \vdots n \wedge (y - z) \vdots n$, то $(x - y) + (y - z) = x - z \vdots n$. Следовательно, отношение $\equiv$ транзитивно.

По теореме 3.1 отношение эквивалентности $\equiv$ определяет разбиение множества Z на классы эквивалентности, которые называются *классами вычетов по модулю n* и обладают следующими **свойствами**:

1) любые два класса вычетов по модулю n либо совпадают, либо не пересекаются. Объединение всех классов вычетов по модулю n совпадает с множеством Z;

2) пусть A и B – классы вычетов по модулю n, $a \in A$ и $b \in B$. Классы A и B совпадают тогда и только тогда, когда $a \equiv b \pmod{n}$;

3) если A – класс вычетов по модулю n и a – произвольный элемент множества A, то $A = \{a + n \cdot k \mid k \in Z\}$.

Пример 4.18. Пусть A – класс вычетов по модулю 2, и целое число 5 является представителем этого класса. Тогда

$A = \{5 + 2 \cdot k \mid k \in Z\} = \{\ldots, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, \ldots\}$.

Выясним, какова мощность фактор-множества $Z/\equiv$, то есть сколько существует классов вычетов по модулю n.

Утверждение 4.1. Целые числа x и y сравнимы по модулю n тогда и только тогда, когда при делении на n они дают одинаковые остатки.

Существуют n различных остатков при делении целых чисел на n: 0, 1, 2, …, $n - 1$. Согласно утверждению 4.1 получаем, что $|Z/\equiv| = n$.

Итак, множество целых чисел по отношению сравнимости по модулю n разбивается на n классов эквивалентности, которые обозначим следующим образом: $\bar{0}, \bar{1}, \ldots, \overline{n-1}$. Фактор-множество $Z/\equiv$ обозначим через Z_n.

Определение 4.28. Введем на множестве $Z_n = \{\bar{0}, \bar{1}, ..., \overline{n-1}\}$ бинарные операции сложения и умножения следующим образом: $\bar{x} + \bar{y} = \overline{x+y}$ и $\bar{x} \cdot \bar{y} = \overline{x \cdot y}$.

Определение операций сложения и умножения на множестве Z_n корректно, так как если $x_1 \equiv x \pmod{n}$ и $y_1 \equiv y \pmod{n}$, то $x_1 + y_1 \equiv (x + y) \pmod{n}$ и $x_1 \cdot y_1 \equiv x \cdot y \pmod{n}$.

Алгебра $\mathcal{Z}_n = < Z_n, +, \cdot >$ является коммутативным кольцом, которое называется *кольцом вычетов по модулю n*.

Пример 4.19. Рассмотрим кольцо $\mathcal{Z}_2 = < Z_2, +, \cdot >$, где $Z_2 = \{\bar{0}; \bar{1}\}$. Приведем таблицы Кэли операций сложения и умножения в кольце $\mathcal{Z}_2$, где для простоты вместо $\bar{0}$ и $\bar{1}$ будем писать 0 и 1 :

+	0	1
0	0	1
1	1	0

*	0	1
0	0	0
1	0	1

Кольцо $\mathcal{Z}_2$ коммутативно, нулем кольца является класс вычетов $\bar{0}$, который отличен от единицы кольца – класса вычетов $\bar{1}$. Кроме того, единственный ненулевой элемент $\bar{1}$ кольца $\mathcal{Z}_2$ имеет обратный к нему – этот же класс $\bar{1}$, так как $\bar{1} \cdot \bar{1} = \bar{1}$. Следовательно, $\mathcal{Z}_2 = < Z_2, +, \cdot >$ является полем. Оно имеет большое значение для приложений.

Следующая теорема говорит о том, что существует много конечных полей.

Теорема 4.4. Кольцо $\mathcal{Z}_n$ является полем тогда и только тогда, когда n – простое число.

4.6. Булевы алгебры

Рассмотрим понятие булевой алгебры, имеющее большое число приложений в программировании и вычислительной технике. Оно возникло в трудах ирландского математика и логика Джорджа Буля (1815 – 1864) как аппарат символической логики.

Определение 4.29. Алгебра $\mathcal{A} = < A, \oplus, *, \bar{} >$ типа (2, 2, 1) называется *булевой алгеброй*, если выполняются следующие условия (аксиомы):

A1. Существуют различные элементы $e_1, e_2 \in A$, являющиеся нейтральными относительно бинарных операций $\oplus, *$ соответственно, то есть
$(\forall\, a \in A)\ \exists\, e_1, e_2 \in A$: $a \oplus e_1 = e_1 \oplus a = a \wedge a * e_2 = e_2 * a = a$.

A2. Операции $\oplus, *$ ассоциативны, то есть
$(\forall a, b, c \in A)\ (a \oplus b) \oplus c = a \oplus (b \oplus c) \ \wedge\ (a * b) * c = a * (b * c)$.

A3. Операции $\oplus, *$ коммутативны, то есть
$(\forall a, b \in A)\ a \oplus b = b \oplus a \ \wedge\ a * b = b * a$.

A4. Операции $\oplus, *$ дистрибутивны относительно друг друга, то есть
$(\forall a,b,c\in A)\, a\oplus(b*c)=(a\oplus b)*(a\oplus c)\ \wedge\ a*(b\oplus c)=(a*b)\oplus(a*c)$.
A5. $(\forall a\in A)\,\exists\,\bar{a}\in A: a\oplus\bar{a}=e_2,\ a*\bar{a}=e_1$.

Замечание 4.6. Аксиома A5 может побудить к ошибочному заключению о том, что элемент $\bar{a}$ является симметричным к элементу a, однако это неверно. Если бы $\bar{a}$ был симметричным элементом к a, то $a\oplus\bar{a}=e_1$ и $a*\bar{a}=e_2$. Сравнивая с аксиомой A5, заключаем, что $\bar{a}$ не является симметричным элементом к a ни для одной из бинарных операций.

Бинарную операцию $\oplus$ называют *сложением*, бинарную операцию $*$ – *умножением*, элементы $a\oplus b$ и $a*b$ – *суммой* и *произведением*, соответственно. Унарную операцию « $\bar{}$ » называют *дополнением*, а элемент $\bar{a}$ – *дополнением к элементу a*.

Существует несколько альтернативных способов записи бинарных операций сложения и умножения:

$\oplus$	$*$
$\vee$	$\wedge$
$+$	$\cdot$
$\cup$	$\cap$

Определение 4.30. Для любого выражения булевой алгебры *двойственным выражением* (или *дуализмом*) называется выражение, полученное из исходного, заменой $\oplus$ на $*$, $*$ на $\oplus$, e_1 на e_2, e_2 на e_1.

Заметим, что каждая из аксиом булевой алгебры – это пара аксиом. Внутри каждой пары каждая аксиома является двойственным выражением по отношению к другой.

Пример 4.20. Наиболее простой из булевых алгебр является алгебра $<\{0, 1\}, \vee, \wedge, \bar{}\ >$, в которой две бинарные операции $\vee$ (дизъюнкция), $\wedge$ (конъюнкция) и одна унарная операция $\bar{}$ (отрицание) задаются таблицами Кэли:

$\vee$	0	1
0	0	1
1	1	1

$\wedge$	0	1
0	0	0
1	0	1

a	$\bar{a}$
0	1
1	0

Эта булева алгебра носит название *двоичной алгебры логики*. В ней роль операции сложения играет дизъюнкция, роль операции умножения – конъюнкция, роль операции дополнения – отрицание. Элемент 0 является нейтральным элементом относительно дизъюнкции, а элемент 1 – нейтральным элементом относительно конъюнкции.

Пример 4.21. Пусть A – непустое множество. Тогда $< P(A), \cup, \cap, \bar{}\ >$ есть булева алгебра, носящая название *алгебры множеств* (или *алгебры Кантора*). Носителем ее является булеан множества A, сигнатурой – операции объ-

единения, пересечения подмножеств множества A, дополнения данного подмножества до множества A, играющих соответственно роли сложения, умножения и дополнения. Пустое множество является нейтральным элементом относительно объединения, а само множество A – нейтральным элементом относительно пересечения.

Свойства булевой алгебры

Утверждение 4.2 (принцип двойственности). Для любой теоремы булевой алгебры двойственная теорема также верна.

Теорема 4.5. Нейтральные элементы e_1 и e_2 относительно $\oplus$ и $*$ соответственно единственны.

Теорема 4.6. $(\forall a \in A)\exists! \bar{a} \in A : a \oplus \bar{a} = e_2$, $a * \bar{a} = e_1$.

Замечание 4.7. Знак «!» означает слово «единственный».

Теорема 4.7 (закон идемпотентности).

$(\forall a \in A)\ a \oplus a = a,\ \ a * a = a$.

Теорема 4.8 (закон идентичности).

$(\forall a \in A)\ a \oplus e_2 = e_2,\ \ a * e_1 = e_1 * a = e_1$.

Теорема 4.9 (закон абсорбции или **поглощения).**

$(\forall a,b \in A) a \oplus (a * b) = a,\ \ a * (a \oplus b) = a$.

Теорема 4.10 (закон инволюции).

$(\forall a \in A)\ \bar{\bar{a}} = a$.

Теорема 4.11 (законы де Моргана).

$(\forall a,b \in A)\ \overline{a \oplus b} = \bar{a} * \bar{b},\ \ \overline{a * b} = \bar{a} \oplus \bar{b}$.

Теорема 4.12. $\bar{e}_1 = e_2,\ \ \bar{e}_2 = e_1$.

Докажем, например, теорему 4.11, в частности, $\overline{a \oplus b} = \bar{a} * \bar{b}$.

Из аксиомы А5 следует, что для этого достаточно показать выполнение равенства $(a \oplus b) \oplus (\bar{a} * \bar{b}) = e_2$. Действительно, $(a \oplus b) \oplus (\bar{a} * \bar{b}) = ((a \oplus b) \oplus \bar{a}) * ((a \oplus b) \oplus \bar{b}) =$ $= (\bar{a} \oplus (a \oplus b)) * ((a \oplus b) \oplus \bar{b}) = ((\bar{a} \oplus a) \oplus b) * (a \oplus (b \oplus \bar{b})) = (e_2 \oplus b) * (a \oplus e_2) = e_2 * e_2 = e_2 \Rightarrow$ $\Rightarrow \overline{a \oplus b} = \bar{a} * \bar{b}$.

Второй закон де Моргана верен по принципу двойственности.

4.7. Гомоморфизмы алгебр

Пусть $\mathcal{A} = < A, f_1, \ldots, f_m >$ и $\mathcal{B} = < B, f_1', \ldots, f_m' >$ – однотипные алгебры, то есть для любого $i \in \{1, \ldots, m\}$ операция f_i алгебры $\mathcal{A}$ и соответствующая ей операция f_i' алгебры $\mathcal{B}$ имеют одинаковые ранги. Говорят, что отображение h носителя A в носитель B *сохраняет операцию* f_i алгебры $\mathcal{A}$, если

$$(\forall\ a_1, \ldots,\ a_{n_i} \in A)\ h\ (f_i(a_1, \ldots, a_{n_i})) = f_i'\ (h(a_1), \ldots, h(a_{n_i})), \qquad (14)$$

где n_i – ранг операции f_i.

Определение 4.31. *Гомоморфизмом* алгебры $\mathcal{A}$ в (на) однотипную алгебру $\mathcal{B}$ называют такое отображение h носителя A в (на) носитель B, которое сохраняет все операции алгебры $\mathcal{A}$, то есть для любой операции f_i ($i = 1, \ldots, m$) алгебры $\mathcal{A}$ выполняется условие (∗).

Определение 4.32. Гомоморфизм h алгебры $\mathcal{A}$ в алгебру $\mathcal{B}$ называется *мономорфизмом* (или *вложением*), если h является инъективным отображением носителя A в носитель B.

Определение 4.33. Гомоморфизм алгебры $\mathcal{A}$ на алгебру $\mathcal{B}$ называется *эпиморфизмом*.

Определение 4.34. Гомоморфизм h алгебры $\mathcal{A}$ на алгебру $\mathcal{B}$ называют *изоморфизмом*, если h есть инъективное отображение носителя A на носитель B.

Определение 4.35. Алгебры $\mathcal{A}$ и $\mathcal{B}$ называются *изоморфными*, если существует изоморфизм алгебры $\mathcal{A}$ на алгебру $\mathcal{B}$. При этом пишут $\mathcal{A} \cong \mathcal{B}$.

Другими словами, отображение h является изоморфизмом алгебры $\mathcal{A}$ на алгебру $\mathcal{B}$, если h – биективное отображение носителя A на носитель B.

Определение 4.36. Гомоморфизм алгебры $\mathcal{A}$ в себя называется *эндоморфизмом*.

Определение 4.37. Изоморфизм алгебры $\mathcal{A}$ на себя называется *автоморфизмом*.

На рис. 4.1 представлена схема определения частного случая гомоморфизма.

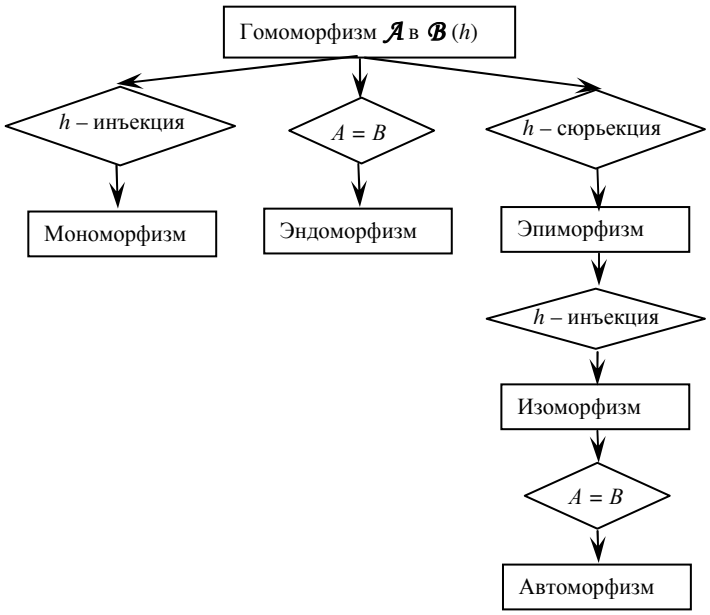


Рис. 4.1

Пример 4.22. Дано отображение

h: $< \{y = ax + b \mid a, b \in R, a \neq 0\}, \circ > \to < R \setminus \{0\}, \cdot >$, где $y = ax + b \mapsto a$.

Выяснить, является ли h гомоморфизмом. Если да, то какой частный случай гомоморфизма имеет место.

Решение. Пусть $A=\{y=ax+b \mid a,b\in R, a\neq 0\}$. Проверим, сохраняет ли h операцию $\circ$, то есть выполняется ли условие:
$(\forall a_1x+b_1, a_2x+b_2\in A)\ h((a_1x+b_1)\circ(a_2x+b_2))= h(a_1x+b_1)\cdot h(a_2x+b_2)$.

Преобразуя левую и правую части равенства, получим:
$h((a_1x+b_1)\circ(a_2x+b_2))=h(a_1(a_2x+b_2)+b_1)=h((a_1a_2)x+(a_1b_2+b_1))=a_1a_2$, (15)
$h(a_1x+b_1)\cdot h(a_2x+b_2)=a_1a_2$. (16)

Из (15) и (16) следует, что h – гомоморфизм алгебры
$<\{y=ax+b \mid a,b\in R, a\neq 0\}, \circ>$ в алгебру $<R\setminus\{0\}, \cdot>$.

Далее выясним, является ли отображение h инъективным или сюръективным.

h – инъекция $\overset{def}{\Leftrightarrow}$ $(\forall a_1x+b_1, a_2x+b_2\in A)\, h(a_1x+b_1)=$
$=h(a_2x+b_2)\Rightarrow a_1x+b_1=a_2x+b_2$.

Это условие не выполняется, так как для любых $b_1\neq b_2$
$h(a_1x+b_1)=h(a_2x+b_2)$. Следовательно, отображение h не является инъективным.

h – сюръекция $\overset{def}{\Leftrightarrow}$ $Im\, h=R\setminus\{0\}$.

Имеем, $(\forall r\in R\setminus\{0\})\, h^{-1}(r)=\{rx+b \mid b\in R\}\neq\varnothing$. Значит, h – сюръекция.

Таким образом, h – эпиморфизм алгебры $<\{y=ax+b \mid a,b\in R, a\neq 0\}, \circ>$ на алгебру $<R\setminus\{0\}, \cdot>$ (см. рис. 4.1).

Пример 4.23. Дано отображение $h:<R, +>\to<R_+, \cdot>$, где $x\mapsto 3^x$ (R_+ – множество положительных действительных чисел).

Решение. Проверим, сохраняет ли h операцию +, то есть выполняется ли условие: $(\forall a,b\in R)\ h(a+b)=h(a)\cdot h(b)$.

Преобразуя левую и правую части равенства, получим:
$h(a+b)=3^{a+b}$, (17)
$h(a)\cdot h(b)=3^a\cdot 3^b=3^{a+b}$. (18)

Из (17) и (18) следует, что h – гомоморфизм алгебры $<R,+>$ в алгебру $<R_+, \cdot>$.

Далее, $(\forall\ a,b\in R\ )\ 3^a=3^b\Rightarrow a=b.$ Следовательно, h – инъекция.

Имеем: $(\forall c\in R_+)\, h^{-1}(c)=\log_3 c$. Следовательно, h – сюръекция.

Значит, h является изоморфизмом алгебры $<R, +>$ на алгебру $<R_+, \cdot>$.

4.8. Алгебраические системы. Решетки

На непустом множестве A, наряду с алгебраическими операциями, можно рассматривать и множество отношений.

Определение 4.38. *Алгебраической системой* называется упорядоченная пара $\mathcal{A} = < A, \Sigma >$, где A – непустое множество и $\Sigma = \Omega \cup \Omega'$, Ω – множество алгебраических операций на A, Ω' – множество отношений на A.

Множество A называется *основным множеством* или *носителем* алгебраической системы, а множество операций и отношений $\mathbf{\Sigma}$ – *сигнатурой* алгебраической системы.

Если множество отношений Ω' пусто, то алгебраическая система $< A, \Sigma > = < A, \Omega >$ является алгеброй. Следовательно, ***алгебры можно считать частным случаем алгебраических систем***. Если множество алгебраических операций Ω пусто, то алгебраическая система $< A, \Sigma > = < A, \Omega' >$ называется *моделью*.

Рассмотрим пример алгебраической системы, который широко используется в математической информатике.

Определение 4.39. *Решеткой* называется алгебраическая система $\mathcal{A} = < A, \leq, \cup, \cap >$, сигнатура которой состоит из одного бинарного отношения $\leq$ частичного порядка и двух бинарных алгебраических операций $\cup$ (объединения) и $\cap$ (пересечения), где бинарные операции определяются следующим образом: $(\forall\, x, y \in A)\ x \cup y = sup\{x, y\}$, $x \cap y = inf\{x, y\}$.

Другими словами, решеткой является частично упорядоченное множество $< A, \leq >$, в котором определены две бинарные алгебраические операции $\cup$ и $\cap$ по вышеуказанным правилам.

Замечание 4.8. Операции $\cup$ и $\cap$ здесь понимаются как абстрактные операции алгебраической системы и отличаются от теоретико-множественных операций объединения и пересечения, определенных в параграфе 1.3, хотя в частных случаях могут с ними совпадать (см. пример 4.24).

Замечание 4.9. Операции $\cup$ и $\cap$ коммутативны и ассоциативны.

Замечание 4.10. Если в алгебраической системе $\mathcal{A}$ ведены операции $\cup$ и $\cap$, то отношение $\leq$ можно по этим операциям восстановить следующим образом: $x \leq y \overset{def}{\Leftrightarrow} x \cup y = y$ или $x \leq y \overset{def}{\Leftrightarrow} x \cap y = x$.

Наименьший элемент решетки (если он существует) называют *нулем* и обозначают через 0. Наибольший элемент решетки (если он существует) называют единицей и обозначают через 1. ***В конечных решетках всегда имеются 0 и 1***.

Пример 4.24. Пусть A – непустое множество, а $P(A)$ – его булеан. Алгебраическая система $< P(A), \subseteq, \cup, \cap >$ является решеткой. Здесь $\cup$ и $\cap$ являются обычными теоретико-множественными операциями объединения и пересечения.

Диаграмма Хассе частично упорядоченного множества $A = \{1, 2, 3\}$ изображена на рис. 4.2. По диаграмме легко видеть, что в этом случае нулем решетки $< P(A), \subseteq, \cup, \cap >$ является $\varnothing$, а единицей – само множество $A = \{1, 2, 3\}$.

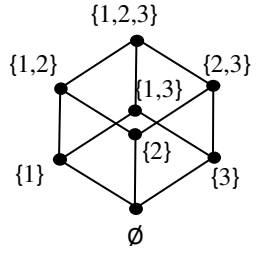


Рис. 4.2

Пример 4.25. Любое линейно упорядоченное мно-

жество $< A, \leq >$, в частности $< R, \leq >$, является решеткой, если в нем определить операции $\cup$ и $\cap$ по правилам:
$(\forall\, x, y \in A)\; x \cup y = max\{x, y\}, x \cap y = min\{x, y\}$.

Определение 4.40. Решетка $\mathcal{A} = < A, \leq >$ называется *дистрибутивной*, если операции объединения и пересечения дистрибутивны относительно друг друга:
$(\forall x, y, z \in A)\; x \cap (y \cup z) = (x \cap y) \cup (x \cap z),\; x \cup (y \cap z) = (x \cup y) \cap (x \cup z)$.

Пример 4.26. Рассмотрим решетку, диаграмма Хассе которой изображена на рис. 4.3. Она не является дистрибутивной, так как $b \cap (d \cup c) = b \cap e = b$, тогда как $(b \cap d) \cup (b \cap c) = a \cup a = a$.

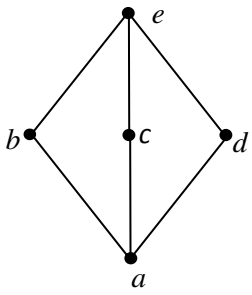


Рис. 4.3

Пример 4.27. Решетка $< P(A), \subseteq, \cup, \cap >$ из примера 4.24 является дистрибутивной, так как обычные теоретико-множественные операции объединения и пересечения дистрибутивны относительно друг друга.

Понятие булевой алгебры является частным случаем понятия решетки.

Определение 4.41. *Булевой алгеброй* называется дистрибутивная решетка $\mathcal{A} = < A, \leq, \cup, \cap >$, в которой имеются различные нуль и единица и $(\forall x \in A)\, \exists\, \bar{x} \in A : x \cup \bar{x} = 1,\; x \cap \bar{x} = 0$. При этом элемент $\bar{x}$ называется дополнением элемента x.

Пример 4.28. Решетка $< P(A), \subseteq, \cup, \cap >$ из примера 4.24 является булевой алгеброй, так как в ней имеются нуль $\varnothing$ и единица A, $\varnothing \neq A$ и
$(\forall\, X \in P(A))\; \exists\; \overline{X} \in P(A)$: $X \cup \overline{X} = A,\; X \cap \overline{X} = \varnothing$.

Задачи к главе 4

1. Является ли операция $(a, b) \mapsto ab - ba$ бинарной алгебраической операцией на множествах N, Z, Q, $2Z$, $2Z + 1$, R, R_+, $Q[\sqrt{2}]$? Если является, то есть ли во множестве нейтральный элемент относительно нее?

2. Пусть $M(2, R) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle|\; a,b,c,d \in R \right\}$. Проверить, является ли подалгеброй алгебры $<M(2,R), \cdot>$ следующее множество матриц:

а) $\left\{ \begin{pmatrix} a & 2b \\ 2b & a \end{pmatrix} \middle|\; a,b \in R \right\}$; б) $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle|\; ad - bc = 1;\; a,b,c,d \in R \right\}$;

в) $\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle|\; a,b,c \in R \right\}$; г) $\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle|\; ad - bc \neq 0;\; a,b,c,d \in R \right\}$;

д) $\left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \middle|\; x \in Z \right\}$; е) $\left\{ \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \middle|\; x \in Z \right\}$.

3. Определить, какими алгебраическими структурами являются следующие алгебры: $< N, + >$; $< Q, +, \cdot >$; $< R \setminus \{0\}, \cdot >$; $< 3Z, + >$; $< Z, - >$; $< C, +, \cdot >$; $< N, \cdot >$; $< Q \setminus \{0\}, \cdot >$; $< R, +, \cdot >$; $< Z, \cdot >$; $< Q, + >$; $< C, + >$.

4. Доказать, что множество степеней числа 2 с целыми показателями образует коммутативную группу относительно обычной операции умножения рациональных чисел.

5. Доказать, что множество геометрических векторов на плоскости, лежащих на одной или параллельных прямых, образует коммутативную группу относительно операции сложения.

6. Пусть $L = \{ax + b \mid a, b \in R\}$ – множество линейных функций. Доказать, что множество L является некоммутативной группой относительно операции композиции функций.

7. Доказать, что множество невырожденных квадратных матриц порядка n образует группу относительно операции умножения матриц.

8. Является ли следующая алгебра группой: а) $<P(\{1,2\}), \cup >$; б) $<P(\{1,2\}), \cap >$?

9. Доказать, что алгебра $<R, * >$, где $a * b = a + b - 2$, является группой.

10. Пусть $E = \{ \varphi_0, \varphi_1, \varphi_2 \}$ есть множество поворотов вокруг центра правильного треугольника, переводящих треугольник в себя, где φ_0, φ_1 и φ_2 – повороты на угол 0, $\frac{2\pi}{3}$, $\frac{4\pi}{3}$ соответственно. На множестве E введем операцию умножения поворотов следующим образом: поворот $\varphi_i \cdot \varphi_j$ получается в результате последовательного выполнения поворотов φ_i и φ_j. Построить таблицу Кэли для операции умножения. Выяснить, какую алгебраическую структуру образует множество E относительно умножения.

11. Выяснить, образует ли кольцо (относительно + и $\cdot$) множество nZ целых чисел, кратных данному натуральному числу n.

12. Доказать, что множество квадратных матриц порядка n с действительными элементами образует некоммутативное кольцо относительно операции сложения и умножения матриц.

13. Укажите, в какой из классов вычетов $\bar{0}, \bar{1}, \ldots, \overline{n-1}$ попадает каждое число: 307, –38, 25, –40, –10, 13, 85, –15, 43, если: а) $n = 10$; б) $n = 2$; в) $n = 5$; г) $n = 7$; д) $n = 6$.

14. Истинно ли высказывание: а) $13 \in \bar{6} \pmod 7$; б) $85 \in \bar{3} \pmod 7$?

15. Построить таблицу Кэли кольца Z_4, указать его обратимые элементы и делители нуля, то есть элементы a, удовлетворяющие условию $a \cdot b = 0$, где b – некоторый ненулевой элемент.

16. Доказать, что алгебра $Z_n = <Z_n, +, \cdot >$ – коммутативное кольцо.

17. Какие из следующих множеств матриц образуют поле относительно сложения и умножения матриц:

а) $\left\{ \begin{pmatrix} x & 1 \\ y & 1 \end{pmatrix} \middle| x, y \in Q \right\}$; б) $\left\{ \begin{pmatrix} x & y \\ 2y & x \end{pmatrix} \middle| x, y \in Q \right\}$;

в) $\left\{\begin{pmatrix} x & x \\ x & x \end{pmatrix} \middle| x \in Q\right\}$; г) $\left\{\begin{pmatrix} x & y \\ 0 & 0 \end{pmatrix} \middle| x, y \in Q\right\}$.

18. Доказать, что множество $Q[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in R\}$ образует поле относительно обычных операций сложения и умножения действительных чисел. Найти в этом поле элемент, обратный к элементу $1 - 2\sqrt{2}$.

19. Выяснить, является ли отображение гомоморфизмом указанных алгебр. Если да, то какой это вид гомоморфизма.

а) $f: < R, + > \to < \{2^x \mid x \in R\}, \cdot >, f(x) = 2^x$.

б) $h: <\left\{\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} \middle| a, b \in Z\right\}, +, \cdot > \to <\{a + b\sqrt{3} \mid a, b \in Z\}, +, \cdot >$,

$h\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} = a + b\sqrt{3}$.

в) $h: <\left\{\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in Z\right\}, +, \cdot > \to < Z, +, \cdot >, h\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = a$.

Список литературы

1. Большакова Л. В. Теория вероятностей для экономистов / Л. В. Большакова. – М.: Финансы и статистика, 2009.
2. Виленкин Н. Я. Популярная комбинаторика / Н. Я. Виленкин. – М.: Наука, 1975.
3. Горелова Г. В. Теория вероятностей и математическая статистика в примерах и задачах с применением Excel / Г. В. Горелова, И. А. Кацко. – Ростов н/Д: Феникс, 2005.
4. Крамор В. С. Алгебра и начало анализа / В. С. Крамор. – М.: Высш. школа, 1981.
5. Кудрявцев Л. Д. Курс математического анализа: в 2 т.: учебник для студентов университетов и втузов / Л. Д. Кудрявцев. – М.: Высш. школа, 1981. – т. I.
6. Кузнецов О. П. Дискретная математика для инженера / О. П. Кузнецов. – СПб.: Лань, 2007.
7. Куликов Л. Я. Алгебра и теория чисел: учеб. пособие для педагогических институтов / Л. Я. Куликов. – М.: Высш. школа, 1979.
8. Куликов Л. Я. Сборник задач по алгебре и теории чисел / Л. Я. Куликов, А. И. Москаленко, А. А. Фомин. – М.: Просвещение, 1993.
9. Логинов Б. М. Лекции и упражнения по курсу «Введение в дискретную математику» / Б. М. Логинов. – Калуга: Калужский филиал МГТУ им. Баумана, 1998.

10. Лунгу К. Н. Сборник задач по высшей математике / К. Н. Лунгу. – М.: Айрис-пресс, 2007.
11. Математический энциклопедический словарь / гл. ред. Ю. В. Прохоров; ред. кол.: С. И. Адян, Н. С. Бахвалов, В. И. Битюцков, А. П. Ершов, Л. Д. Кудрявцев, А. Л. Онищик, А. П. Юшкевич. – М.: Сов. энциклопедия, 1988.
12. Нефедов В. Н. Курс дискретной математики: учеб. пособие / В. Н. Нефедов, В. А. Осипова. – М.: Изд-во МАИ, 1992.
13. Новиков Ф. А. Дискретная математика для программистов / Ф. А. Новиков. – СПб.: Питер, 2000.
14. Палий И. А. Дискретная математика. Курс лекций / И.А. Палий. – М.: Эксмо, 2008.
15. Рыбников К. К. Введение в дискретную математику и теорию решения экстремальных задач на конечных множествах: учеб. пособие для студентов вузов, обучающихся по специальностям в обл. информ. безопасности / К. К. Рыбников. – М.: Гелиос АРВ, 2010.
16. Садовская О. Б. Дискретная математика и математическая логика. Ч. 1. – Кострома: Изд-во Костром. гос. технолог. ун-та, 2003.
17. Соболева Т. С. Дискретная математика: учебник для студ. вузов / Т. С. Соболева, А. В. Чечкин; под ред. А. В. Чечкина. – М.: Академия, 2006.
18. Судоплатов С. В. Дискретная математика: учебник / С.В.Судоплатов, Е. В. Овчинникова. – М.: ИНФРА-М; Новосибирск: Изд-во НГТУ, 2007.
19. Шапорев С. Д. Дискретная математика. Курс лекций и практических занятий / С. Д. Шапорев. – СПб.: БХВ-Петербург, 2006.