МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ

Федеральное государственное бюджетное образовательное учреждение
инклюзивного высшего образования
Московский государственный гуманитарно-экономический университет

Кафедра «Математики»

Н.В. Труб

Множества, функции и отношения

Учебное пособие

Для студентов, обучающихся по специальности «Прикладная математика и информатика» и «Прикладная информатика»

Москва
2014

Индекс ББК
Авторский знак (Запрашивается в библиотеке)

Рецензенты: А.М. Анискин — директор департамента метатехнологий ЗАО «АРМАДА СОФТ», канд. техн. наук.
В.Г. Фомин – проф. кафедры математики, канд. физ.-мат. наук.

Труб Наталья Васильевна. Множества, функции и отношения [Текст] : учеб. пособие для студентов математических и технических специальностей. — М.: МГГЭУ, 2014 год.— 64 с.

Аннотация

В учебном пособии рассмотрены основы теории множеств, элементы алгебры и комбинаторики. Даны определения мощности множества, отношений, функций, базовых алгебраических структур, сочетаний, биномиальных коэффициентов. Сформулированы и доказаны основные теоремы, раскрывающие свойства введенных понятий в их взаимосвязи друг с другом. Изложение ведется в естественной логической последовательности с соблюдением постепенного перехода от простого к сложному. Структура пособия соответствует традиционным тематическим разделам дисциплины «Дискретная математика». Пособие включает большое количество примеров, хорошо иллюстрирующих практическое применение изложенного теоретического материала.Для студентов, обучающихся по специальности «Прикладная математика и информатика» и «Прикладная информатика».

Содержание:

§1. Множества и операции над ними

Понятие множества — одно из основных понятий математики. Под *множеством* понимают совокупность объектов (предметов, понятий), которая рассматривается как одно целое. Объекты, входящие в состав множества, называются его *элементами*. Понятие множества принимается как исходное, первичное, т.е. не сводимо к другим понятиям. Считается, что множество $\boldsymbol{M}$ задано, если о любом объекте можно сказать, является ли он элементом множества $\boldsymbol{M}$ или нет, т.е. входит ли объект в $\boldsymbol{M}$ или нет.

Утверждения «Объект *a,* есть элемент множества $\boldsymbol{M}$», «Объект, *a* принадлежит множеству $\boldsymbol{M}$», которые имеют один и тот же смысл, сокращенно записывают в виде $a \in \boldsymbol{M}$. В противном случае пишут $a \notin \boldsymbol{M}$. Символ ∈ называют *знаком принадлежности*.

Определение 1.1. Два множества $\boldsymbol{A}$ и $\boldsymbol{B}$ называют *равными* и пишут $\boldsymbol{A = B}$, если $\boldsymbol{A}$ и $\boldsymbol{B}$ содержат одни и те же элементы.

Таким образом, множества $\boldsymbol{A}$ и $\boldsymbol{B}$ равны, если для любого $x \in \boldsymbol{A}$ тогда и только тогда, когда $x \in \boldsymbol{B}$.

В связи с этим доказательство равенства двух данных множеств $\boldsymbol{A}$ и $\boldsymbol{B}$ обычно состоит из доказательства двух утверждений:

1) для любого *x*, если $x \in \boldsymbol{A}$, то $x \in \boldsymbol{B}$; 2) для любого *x*, если $x \in \boldsymbol{B}$, то $x \in \boldsymbol{A}$.

Определение 1.2. Множество $\boldsymbol{A}$ называется *подмножеством* множества $\boldsymbol{B}$, если всякий элемент из А является элементом из $\boldsymbol{B}$. Обозначается это как $\boldsymbol{A \subseteq B}$. Если хотят отметить, что $\boldsymbol{A \subseteq B}$, но $\boldsymbol{A \neq B}$, то пишут $\boldsymbol{A \subset B}$. Знаки $\subset$, $\subseteq$ называют *знаками включения*.

Таким образом, $\boldsymbol{A = B}$ тогда и только тогда, когда $\boldsymbol{A \subseteq B}$ и $\boldsymbol{B \subseteq A}$.

Природа элементов множества $\boldsymbol{M}$ может быть какой угодно. Например, множество натуральных чисел **N**, целых чисел **Z**, рациональных $\boldsymbol{Q}$, действительных $\boldsymbol{R}$, комплексных **C** — это все числовые множества. Их элементами являются натуральные (целые, рациональные, действительные и комплексные) числа. Эти множества связаны между собой цепочкой включений $\boldsymbol{N \subset Z \subset Q \subset R \subset C}$.

В качестве множества $\boldsymbol{M}$ может выступать, например, совокупность всех решений данной системы уравнений, совокупность всех людей, живущих в данном городе, совокупность всех дисциплин, изучаемых студентом по данной специальности. Словом, любая совокупность предметов, объектов, понятий, объединенных какими-то свойствами в одно целое.

Но бывает и так, что какие-то множества являются сами элементами некоторого множества. И в этом случае надо четко различать, когда данное множество является элементом, а когда подмножеством. Например, если $\boldsymbol{M}$ — множество студентов на данном факультете, а $\boldsymbol{A}$ — множество студентов этого факультета в группе №1, то множество $\boldsymbol{A}$ является подмножеством множества $\boldsymbol{M}$, т.е. $\boldsymbol{A \subset M}$. Если же $\boldsymbol{M}$ — это множество всех студенческих групп на данном факультете, то в этом случае $\boldsymbol{A \in B}$, т.е. множество $\boldsymbol{A}$ является элементом множества $\boldsymbol{M}$.

Если $\boldsymbol{M} = \{a, b, c\}$ — множество, состоящее из трех элементов, то для каждого из элементов имеем $a \in \boldsymbol{M}$, $b \in \boldsymbol{M}$, $c \in \boldsymbol{M}$. В то же время $\{a\}, \{b\}, \{c\}$ — подмножества множества $\boldsymbol{M}$, состоящие из элементов *a*, *b*, *c*, соответственно. И в этом случае имеем $\{a\} \subset \boldsymbol{M}$, $\{b\} \subset \boldsymbol{M}$, $\{\mathrm{c}\} \subset \boldsymbol{M}$.

Определение 1.3. *Мощностным множеством* множества $\boldsymbol{M}$ называется множество всех подмножеств множества $\boldsymbol{M}$. Обозначается через $\boldsymbol{P}(\boldsymbol{M})$.

Например, если $\boldsymbol{M} = \{a, b, \mathrm{c}\}$, то $\boldsymbol{P}(\boldsymbol{M}) = \{\emptyset, \{a\}, \{b\}, \{\mathrm{c}\}, \{a, b\}, \{a, \mathrm{c}\}, \{b, \mathrm{c}\}, \{a, b, \mathrm{c}\}\}$. В этом примере появилось некоторое множество $\emptyset$.

Определение 1.4. Множество, не содержащее ни одного элемента, называется *пустым* и обозначается через $\emptyset$.

Считается, что пустое множество $\emptyset$ является подмножеством любого множества. Поэтому $\emptyset \in \boldsymbol{P}(\boldsymbol{M})$ для любого множества $\boldsymbol{M}$.

Определение 1.5. Множество $\boldsymbol{M}$ называется *конечным*, если оно состоит из конечного числа элементов. В противном случае множество называется *бесконечным*.

Вопрос о равенстве двух множеств является одной из наиболее важных и сложных проблем математики. Фактически любое утверждение в математике есть утверждение о равенстве некоторых множеств. Например, утверждение о том, что корнями уравнения $sinx = 0$ являются числа вида πk, $k \in \boldsymbol{Z}$, есть утверждение о равенстве множества $\boldsymbol{A}$ корней уравнения $sinx = 0$ и множества $\boldsymbol{B}$ чисел вида πk, $k \in \boldsymbol{Z}$.

При решении вопроса о равенстве двух множеств важную роль играет способ, каким заданы множества. Множество может быть задано различными способами. Рассмотрим наиболее распространенные.

1. Всякое конечное множество может быть задано простым перечислением его элементов. При этом обычно все элементы заключают в фигурные скобки. Например, $\boldsymbol{M} = \{1,2,4,8,16\}$ — множество всех натуральных делителей числа 16. Так как по определению равных множеств порядок следования элементов не играет роли, то $\{1,2,4,8,16\} = \{16,2,8,4,1\}$. Точно также множества $\{1,2,4,8,16\}$ и $\{1,2,4,4,8,8,16\}$ равны между собой, так как они состоят из одних и тех же элементов.

Поэтому при задании множества перечислением его элементов каждый элемент учитывается один раз.

Задание конечного множества перечислением его элементов полностью определяет, из каких элементов множество состоит. Но такое перечисление не всегда проясняет принцип (закон, правило), по которому отбираются элементы множества. Так, множество $\boldsymbol{M} = \{1,2,4,8,16\}$ определяли как множество всех натуральных делителей числа 16. Но это же множество можно определить как множество всех целых неотрицательных степеней числа 2 не превышающих 4. Поэтому чтобы более точно определить элементы данного множества, используют следующий способ задания множеств (см. п.2).

2. Множество задают каким-либо характерным свойством, которым должны обладать все его элементы. При этом записывают $\boldsymbol{M} = \{x|\mathrm{P}(x)\}$ — множество элементов x, которые обладают свойством P. Например, $\boldsymbol{M} = \{x|x \in [0;1]\}$, где свойство P означает для числа x принадлежность отрезку $[0;1]$ (т.е. $0 \le x \le 1$). Определение данного множества $\boldsymbol{M}$ требует уточнения, так как неясно, откуда выбираются числа x. Например, если числа x выбираются среди натуральных чисел, то $\boldsymbol{M} = \{x|x \in [0;1]\}$ состоит из одного элемента 1. Если же x выбирается среди всех действительных чисел $\boldsymbol{R}$, то $\boldsymbol{M} = [0;1]$. Наконец, множество $\boldsymbol{M}$ может

вообще оказаться пустым, если, к примеру, числа x выбираются среди отрицательных действительных чисел. Поэтому, задавая таким образом множество $\boldsymbol{M} = \{x|\mathrm{P}(x)\}$, либо специально оговаривают, откуда выбираются элементы x, либо свойство P определяется так, что ясно, какие элементы x рассматриваются.

Например, $\boldsymbol{M} = \{x \in \mathbf{N}|x \in [0;1]\} = \{x|x \in \mathbf{N} \text{ и } x \in [0;1]\} = \{1\}$. Конечно, при таком способе задания множества $\boldsymbol{M}$ должно быть строго и четко определено свойство P.

3. Третий способ задания множеств — это способ задания с помощью некоторой порождающей процедуры. Порождающая процедура описывает способ получения элементов множества $\boldsymbol{M}$ из уже полученных элементов или из каких-либо других объектов. Например, множество нечетных натуральных чисел можно описать следующей порождающей процедурой: а) $1 \in \boldsymbol{M}$; б) если $m \in \boldsymbol{M}$, то $m + 2 \in \boldsymbol{M}$.

Таким образом, описанное правило называется рекурсивным. Естественно, здесь должно быть точно описано это рекурсивное правило, позволяющее, во-первых, исходя из заданных элементов, получить все элементы множества $\boldsymbol{M}$, а во-вторых, позволяющее для любого элемента x определить, получен ли этот элемент из заданных с помощью данной процедуры или нет.

4. Наконец, четвертый способ задания множеств заключается в том, что из вполне определенных, известных нам множеств с помощью некоторых операций строят новые.

Определение 1.6. *Объединением* множеств $\boldsymbol{A}$ и $\boldsymbol{B}$ называется множество, состоящее из тех и только тех элементов, которые принадлежат хотя бы одному из множеств $\boldsymbol{A}$ или $\boldsymbol{B}$. Обозначается объединение через $\boldsymbol{A} \cup \boldsymbol{B}$.

Итак, $\boldsymbol{A} \cup \boldsymbol{B} = \{x|x \in \boldsymbol{A} \text{ или } x \in \boldsymbol{B}\}$.

Например, если $\boldsymbol{A} = \{1,2,8\}$ и $\boldsymbol{B} = \{2,4,6,8\}$, то $\boldsymbol{A} \cup \boldsymbol{B} = \{1,2,4,6,8\}$. Или, если $\boldsymbol{A}$ есть множество действительных чисел на отрезке $[1;3]$, а $\boldsymbol{B}$ — множество действительных чисел на отрезке $[2;5]$, то $\boldsymbol{A} \cup \boldsymbol{B}$ — множество действительных чисел на отрезке $[1;5]$.

Определение 1.7. *Пересечением* множеств $\boldsymbol{A}$ и $\boldsymbol{B}$ называется множество, состоящее из тех и только тех элементов, которые принадлежат и $\boldsymbol{A}$, и $\boldsymbol{B}$. Обозначается пересечение через $\boldsymbol{A} \cap \boldsymbol{B}$.

Итак, $\boldsymbol{A} \cap \boldsymbol{B} = \{x|x \in \boldsymbol{A} \text{ и } x \in \boldsymbol{B}\}$.

Например, как и выше, для множеств $\boldsymbol{A} = \{1,2,8\}$ и $\boldsymbol{B} = \{2,4,6,8\}$, пересечение $\boldsymbol{A} \cap \boldsymbol{B} = \{2,8\}$. Если $\boldsymbol{A}$ и $\boldsymbol{B}$ — множества действительных чисел на отрезках $[1;3]$ и $[2;5]$ соответственно, то $\boldsymbol{A} \cap \boldsymbol{B}$ — множество действительных чисел на отрезке $[2;3]$.

Теорема 1.1. Для любых множеств $\boldsymbol{A}$ и $\boldsymbol{B}$ следующие условия эквивалентны:

a) $\boldsymbol{A} \subseteq \boldsymbol{B}$;

b) $\boldsymbol{A} \cup \boldsymbol{B} = \boldsymbol{B}$;

c) $\boldsymbol{A} \cap \boldsymbol{B} = \boldsymbol{A}$.

Доказательство. Эквивалентность двух условий означает, что при выполнении одного из условий, обязательно выполняется другое, и, наоборот, при выполнении второго обязательно выполняется первое.

Эквивалентность этих утверждений докажем по схеме:

а) $=>$ b) $=>$ c) $=>$ а), где стрелка а) $=>$ b) означает, что из выполнения утверждения а) следует утверждение b).

а) $=>$ b). Если $x \in \boldsymbol{A} \cup \boldsymbol{B}$, то $x \in \boldsymbol{A}$ или $x \in \boldsymbol{B}$**.** Так как выполнено условие а), т.е. $\boldsymbol{A} \subset \boldsymbol{B}$**,** то из того, что $x \in \boldsymbol{A}$ обязательно следует, что $x \in \boldsymbol{B}$. Итак, в любом случае, если $x \in \boldsymbol{A} \cup \boldsymbol{B}$**,** то $x \in \boldsymbol{B}$, то есть $\boldsymbol{A} \cup \boldsymbol{B} \subseteq \boldsymbol{B}$. Обратно, если $x \in \boldsymbol{B}$, то по определению объединения, $x \in \boldsymbol{A} \cup \boldsymbol{B}$, а значит, $\boldsymbol{B} \subseteq \boldsymbol{A} \cup \boldsymbol{B}$. Эти два включения $\boldsymbol{A} \cup \boldsymbol{B} \subseteq \boldsymbol{B}$ и $\boldsymbol{B} \subseteq \boldsymbol{A} \cup \boldsymbol{B}$ означают, что $\boldsymbol{A} \cup \boldsymbol{B} = \boldsymbol{B}$, т.е. утверждение b) доказано.

b) $=>$ c). Итак, $\boldsymbol{A} \cup \boldsymbol{B} = \boldsymbol{B}$, и надо доказать, что $\boldsymbol{A} \cap \boldsymbol{B} = \boldsymbol{A}$. По определению пересечения имеем $\boldsymbol{A} \cap \boldsymbol{B} \subseteq \boldsymbol{A}$. Покажем обратное включение. Пусть $x \in \boldsymbol{A}$. Тогда, по определению объединения $x \in \boldsymbol{A} \cup \boldsymbol{B} = \boldsymbol{B}$*,* т.е. $x \in \boldsymbol{B}$**.** В таком случае $x \in \boldsymbol{A}$ и $x \in \boldsymbol{B}$*,* а значит, $x \in \boldsymbol{A} \cap \boldsymbol{B}$*,* и обратное включение $\boldsymbol{A} \subseteq \boldsymbol{A} \cap \boldsymbol{B}$ доказано.

c) $=>$ a). Надо показать, что если $\boldsymbol{A} \cap \boldsymbol{B} = \boldsymbol{A}$*,* то $\boldsymbol{A} \subseteq \boldsymbol{B}$. По определению пересечения, $\boldsymbol{A} \cap \boldsymbol{B} \subseteq \boldsymbol{B}$*,* и значит, $\boldsymbol{A} \subseteq \boldsymbol{B}$.

Теорема 1.2. Любые множества $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{C}$ обладают следующими свойствами:

1. $\boldsymbol{A} \cup = \boldsymbol{A}$ — идемпотентность объединения;

$\boldsymbol{A} \cap \boldsymbol{A} = \boldsymbol{A}$ — идемпотентность пересечения;

2. $\boldsymbol{A} \cup \boldsymbol{B} = \boldsymbol{B} \cup \boldsymbol{A}$ — коммутативность объединения;

$\boldsymbol{A} \cap \boldsymbol{B} = \boldsymbol{B} \cap \boldsymbol{A}$ — коммутативность пересечения;

3. $(\boldsymbol{A} \cup \boldsymbol{B}) \cup \boldsymbol{C} = \boldsymbol{A} \cup (\boldsymbol{B} \cup \boldsymbol{C})$ — ассоциативность объединения;

$(\boldsymbol{A} \cap \boldsymbol{B}) \cap \boldsymbol{C} = \boldsymbol{A} \cap (\boldsymbol{B} \cap \boldsymbol{C})$ — ассоциативность пересечения;

4. $\boldsymbol{A} \cup (\boldsymbol{B} \cap \boldsymbol{C}) = (\boldsymbol{A} \cup \boldsymbol{B}) \cap (\boldsymbol{A} \cup \boldsymbol{C})$ — дистрибутивность объединения относительно пересечения;

5. $\boldsymbol{A} \cap (\boldsymbol{B} \cup \boldsymbol{C}) = (\boldsymbol{A} \cap \boldsymbol{B}) \cup (\boldsymbol{A} \cap \boldsymbol{C})$ — дистрибутивность пересечения относительно объединения.

Доказательство. Доказательство всех этих равенств производится на основе определения равенств множеств. Докажем, например, равенство 4.

Пусть $x \in \boldsymbol{A} \cup (\boldsymbol{B} \cap \boldsymbol{C})$, значит, $x \in \boldsymbol{A}$ или $x \in \boldsymbol{B} \cap \boldsymbol{C}$. Рассмотрим два этих случая в отдельности.

а) Если $x \in \boldsymbol{A}$, то по определению $x \in \boldsymbol{A} \cup \boldsymbol{B}$ и $x \in \boldsymbol{A} \cup \boldsymbol{C}$, а значит, $x \in (\boldsymbol{A} \cup \boldsymbol{B}) \cap (\boldsymbol{A} \cup \boldsymbol{C})$.

б). Если $x \in \boldsymbol{B} \cap \boldsymbol{C}$, то $x \in \boldsymbol{B}$ и $x \in \boldsymbol{C}$. Тогда, по определению объединения $x \in \boldsymbol{A} \cup \boldsymbol{B}$ и $x \in \boldsymbol{A} \cup \boldsymbol{C}$, и значит, $x \in (\boldsymbol{A} \cup \boldsymbol{B}) \cap (\boldsymbol{A} \cup \boldsymbol{C})$.

В обоих случаях $x \in (\boldsymbol{A} \cup \boldsymbol{B}) \cap (\boldsymbol{A} \cup \boldsymbol{C})$, то есть $\boldsymbol{A} \cup (\boldsymbol{B} \cap \boldsymbol{C}) \subseteq (\boldsymbol{A} \cup \boldsymbol{B}) \cap (\boldsymbol{A} \cup \boldsymbol{C})$.

Обратно: пусть $x \in (\boldsymbol{A} \cup \boldsymbol{B}) \cap (\boldsymbol{A} \cup \boldsymbol{C})$. Тогда $x \in \boldsymbol{A} \cup \boldsymbol{B}$ и $x \in \boldsymbol{A} \cup \boldsymbol{C}$. Возможны также два случая: $x \in \boldsymbol{A}$ или $x \notin \boldsymbol{A}$, но тогда $x \in \boldsymbol{B}$ и $x \in \boldsymbol{C}$. В первом случае, если $x \in \boldsymbol{A}$, то $x \in \boldsymbol{A} \cup (\boldsymbol{B} \cap \boldsymbol{C})$.

Во втором случае, $x \in \boldsymbol{B} \cap \boldsymbol{C}$, а значит, $x \in \boldsymbol{A} \cup (\boldsymbol{B} \cap \boldsymbol{C})$. В обоих случаях $x \in \boldsymbol{A} \cup (\boldsymbol{B} \cap \boldsymbol{C})$, т.е. обратное включение $(\boldsymbol{A} \cup \boldsymbol{B}) \cap (\boldsymbol{A} \cup \boldsymbol{C}) \subseteq \boldsymbol{A} \cup (\boldsymbol{B} \cap \boldsymbol{C})$ также доказано.

Пусть даны три множества: $\boldsymbol{A}$**,** $\boldsymbol{B}$ и $\boldsymbol{C}$. Объединение трех этих множеств $\boldsymbol{A} \cup \boldsymbol{B} \cup \boldsymbol{C}$ можно определить по-разному. Можно рассмотреть сначала объединение множеств $\boldsymbol{A}$ и $\boldsymbol{B}$, а затем объединение полученного множества с множеством $\boldsymbol{C}$. Можно же рассмотреть объединение множеств $\boldsymbol{B}$ и $\boldsymbol{C}$, а затем объединение множества $\boldsymbol{A}$ с полученным множеством. А можно, по аналогии с определением 1.6, множество $\boldsymbol{A} \cup \boldsymbol{B} \cup \boldsymbol{C}$ определить как множество, состоящее из тех и только тех элементов, которые входят хотя бы в одно из множеств $\boldsymbol{A}$**,** $\boldsymbol{B}$ или

$\boldsymbol{C}$. Согласно свойству 3 теоремы 1.2 все это будет задавать одно и то же множество. Более того, согласно свойству 2 этой же теоремы множества $\boldsymbol{A}$, $\boldsymbol{B}$ и $\boldsymbol{C}$ в этом объединении можно переставлять, к примеру, множества $\boldsymbol{A} \cup \boldsymbol{B} \cup \boldsymbol{C}$ и $\boldsymbol{B} \cup \boldsymbol{C} \cup \boldsymbol{A}$ совпадают. Свойство 3 позволяет ввести определение объединения любого семейства (даже бесконечного) множеств.

Пусть $\boldsymbol{A_1, A_2, \dots, A_n}$ — произвольные множества. Объединением этих множеств называется множество, состоящее из тех и только тех элементов, которые принадлежат хотя бы одному из множеств $\boldsymbol{A_i}$, где i=1,2,…,n. Обозначается это объединение как $\bigcup_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{A_i}$. Пусть $\{\boldsymbol{A_i}\}$ — некоторое семейство множеств, заиндексированных элементами i из некоторого множества $\boldsymbol{I}$. Аналогично определяется объединение данного семейства множеств, которое обозначается через $\bigcup_{\boldsymbol{i \in I}} \boldsymbol{A_i}$. В частности, если $\boldsymbol{I = N}$, то данное объединение записывается как $\bigcup_{\boldsymbol{i=1}}^{\infty} \boldsymbol{A_i}$.

Все, сказанное выше об объединении, можно перенести на пересечение и определить множества $\bigcup_{\boldsymbol{i=1}}^{\boldsymbol{n}} \boldsymbol{A_i}$, $\bigcup_{\boldsymbol{i \in I}} \boldsymbol{A_i}$, $\bigcup_{\boldsymbol{i=1}}^{\infty} \boldsymbol{A_i}$.

Определение 1.8. *Разностью* множеств $\boldsymbol{A}$ и $\boldsymbol{B}$ называется множество, элементами которого являются элементы из $\boldsymbol{A}$, не принадлежащие $\boldsymbol{B}$. Обозначается разность как $\boldsymbol{A \setminus B}$.

Итак, $\boldsymbol{A \setminus B} = \{x | x \in \boldsymbol{A} \text{и } x \notin \boldsymbol{B}\}$.

Рассмотрим примеры, которые предлагались после определения объединения и пересечения. Если $\boldsymbol{A} = \{1,2,8\}$ и $\boldsymbol{B} = \{2,4,6,8\}$, то $\boldsymbol{A \setminus B} = \{1\}$. Если же $\boldsymbol{A} = [1;3]$ и $\boldsymbol{B} = [2;5]$, то $\boldsymbol{A \setminus B} = [1;2)$. Если для этих же множеств рассмотрим разность $\boldsymbol{B \setminus A}$, то $\boldsymbol{B \setminus A} = \{4,6\}$ в первом случае, и $\boldsymbol{B \setminus A} = (3;5]$ – во втором. Уже на этих примерах видно, что в общем случае $\boldsymbol{A \setminus B \neq B \setminus A}$.

Во многих приложениях теории множеств множества рассматриваются как подмножества некоторого множества $\boldsymbol{U}$. Такое множество $\boldsymbol{U}$ называют универсальным. Например, если мы работаем с числовыми множествами, то в качестве универсального множества $\boldsymbol{U}$ можно рассмотреть множество всех действительных чисел **R** (или множество всех комплексных чисел **C**). Если же мы изучаем подмножества некоторого множества $\boldsymbol{M}$, то в качестве универсального множества $\boldsymbol{U}$ можно взять мощностное множество $\boldsymbol{P(M)}$.

Определение 1.9. Множество $\boldsymbol{U \setminus A}$ называется *дополнением* множества $\boldsymbol{A}$ и обозначается через $\boldsymbol{\overline{A}}$.

Другими словами, множество $\boldsymbol{\overline{A}}$ состоит из тех и только тех элементов, которые не принадлежат множеству $\boldsymbol{A}$.

Теорема 1.3. Для любых множеств $\boldsymbol{A, B \subset U}$ справедливы утверждения:

1. $\boldsymbol{A \cup \overline{A} = U;}$ –
2. $\boldsymbol{A \cap \overline{A} = \emptyset;}$
3. $\boldsymbol{\overline{(\overline{A})} = A;}$
4. Если $\boldsymbol{A \subset B}$, то $\boldsymbol{\overline{B} \subset \overline{A}}$.

Доказательство. Докажем, к примеру, утверждение 4. Итак, $\boldsymbol{A \subset B}$, и пусть $x \in \boldsymbol{\overline{B}}$. По определению, тогда $x \notin \boldsymbol{B}$. Но тогда $x \notin \boldsymbol{A}$, так как если $x \in \boldsymbol{A}$, то $x \in \boldsymbol{B}$, поскольку $\boldsymbol{A \subset B}$. Таким образом $x \notin \boldsymbol{A}$, т.е. $x \in \boldsymbol{\overline{A}}$. Тем самым показали включение $\boldsymbol{\overline{B} \subset \overline{A}}$.

Теорема 1.4. Для любых множеств $\boldsymbol{A, B \subset U}$ справедливы равенства, называемые *законом де Моргана*:

$$\overline{(\boldsymbol{A} \cup \boldsymbol{B})} = \overline{\boldsymbol{A}} \cap \overline{\boldsymbol{B}}$$
$$\overline{(\boldsymbol{A} \cap \boldsymbol{B})} = \overline{\boldsymbol{A}} \cup \overline{\boldsymbol{B}}$$

Доказательство. Докажем сначала первое равенство. Пусть $x \in \overline{(\boldsymbol{A} \cup \boldsymbol{B})}$, т.е. $x \notin \boldsymbol{A} \cup \boldsymbol{B}$. Но в таком случае $x \notin \boldsymbol{A}$ и $x \notin \boldsymbol{B}$. Следовательно, $x \in \overline{\boldsymbol{A}}$ и $x \in \overline{\boldsymbol{B}}$, а значит, $x \in \overline{\boldsymbol{A}} \cap \overline{\boldsymbol{B}}$, т.е. доказано включение $\overline{(\boldsymbol{A} \cup \boldsymbol{B})} \subseteq \overline{\boldsymbol{A}} \cap \overline{\boldsymbol{B}}$. Докажем обратное включение. Пусть $x \in \overline{\boldsymbol{A}} \cap \overline{\boldsymbol{B}}$, т.е. $x \in \overline{\boldsymbol{A}}$ и $x \in \overline{\boldsymbol{B}}$. По определению $x \notin \boldsymbol{A}$ и $x \notin \boldsymbol{B}$, а значит, $x \notin \boldsymbol{A} \cup \boldsymbol{B}$. В таком случае $x \in \overline{(\boldsymbol{A} \cup \boldsymbol{B})}$, т.е. доказано включение $\overline{\boldsymbol{A}} \cap \overline{\boldsymbol{B}} \subseteq \overline{(\boldsymbol{A} \cup \boldsymbol{B})}$.

Второе равенство можно доказать также взаимными включениями. А можно доказать следующим образом. Согласно только что доказанному, $\overline{(\boldsymbol{A} \cup \boldsymbol{B})} = \overline{\boldsymbol{A}} \cap \overline{\boldsymbol{B}}$ для любых множеств $\boldsymbol{A}$ и $\boldsymbol{B}$. Следовательно, для множеств $\overline{\boldsymbol{A}}$ и $\overline{\boldsymbol{B}}$ также справедливо данное равенство, т.е. $\overline{(\overline{\boldsymbol{A}} \cup \overline{\boldsymbol{B}})} = \overline{(\overline{\boldsymbol{A}})} \cap \overline{(\overline{\boldsymbol{B}})}$. Согласно предыдущей теореме $\overline{(\overline{\boldsymbol{A}})} = \boldsymbol{A}$ и $\overline{(\overline{\boldsymbol{B}})} = \boldsymbol{B}$, поэтому $\overline{(\overline{\boldsymbol{A}} \cup \overline{\boldsymbol{B}})} = \boldsymbol{A} \cap \boldsymbol{B}$. Поскольку эти множества равны, то равны и их дополнения, а именно $\overline{\overline{(\overline{\boldsymbol{A}} \cup \overline{\boldsymbol{B}})}} = \overline{\boldsymbol{A} \cap \boldsymbol{B}}$. Отсюда получаем, что $\overline{\boldsymbol{A}} \cup \overline{\boldsymbol{B}} = \overline{(\boldsymbol{A} \cap \boldsymbol{B})}$.

Для наглядности представления множеств и операций над ними используют так называемые диаграммы Эйлера (см. рис.1–6), которые также называют диаграммами Венна. Универсальное множество $\boldsymbol{U}$ обозначают в виде прямоугольника, а сами множества изображают кругом, расположенным внутри прямоугольника. На рис. 1–5 изображены множества $\boldsymbol{A} \cap \boldsymbol{B}$; $\boldsymbol{A} \cup \boldsymbol{B}$; $\boldsymbol{A} \backslash \boldsymbol{B}$; $\boldsymbol{B} \backslash \boldsymbol{A}$; $\overline{\boldsymbol{A}}$ в виде заштрихованных областей. На рис. 6 изображена ситуация $\boldsymbol{A} \subset \boldsymbol{B}$.

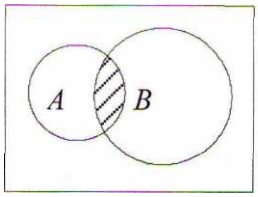


Рис. 1
$\boldsymbol{A \cap B}$

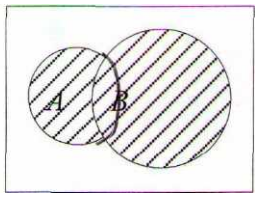
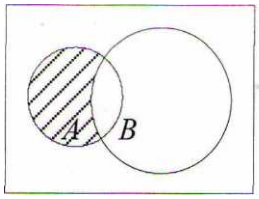
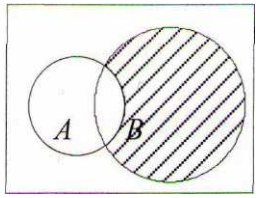


Рис. 2
$\boldsymbol{A \cup B}$



$\boldsymbol{A \setminus B}$
Рис. 3



$\boldsymbol{B \setminus A}$
Рис. 4

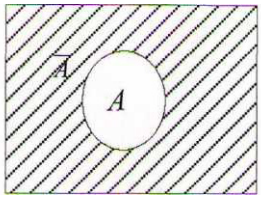


Рис. 5
$\boldsymbol{\overline{A}}$

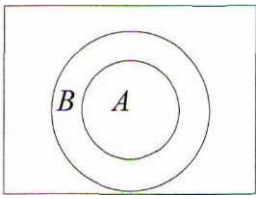


Рис. 6
$\boldsymbol{A \subset B}$

Отметим, что диаграммы Венна иллюстрируют строение множеств, помогают понять, из каких элементов множества состоят. Они служат некоторой подсказкой при доказательстве равенств множеств, при выяснении вопроса о том, как связаны между собой два множества. Но их не рекомендуется применять для доказательства равенства множеств. К примеру, при рассмотрении строения множества $\boldsymbol{A \setminus B}$ надо рассмотреть четыре случая: 1) $\boldsymbol{A \cap B = \emptyset}$; 2) $\boldsymbol{A \subseteq B}$; 3) $\boldsymbol{B \subseteq A}$; 4) $\boldsymbol{A \cap B \neq \emptyset}$ и при этом ни $\boldsymbol{A \nsubseteq B}$, ни $\boldsymbol{B \nsubseteq A}$. Каждый из этих случаев иллюстрируется соответствующими диаграммами Венна (см. рис. 7–10). Разность $\boldsymbol{A \setminus B}$ заштрихована.

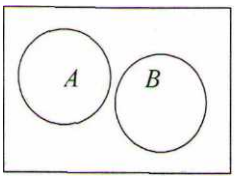


Рис. 7

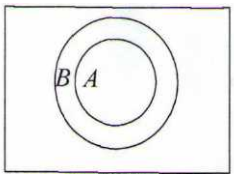


Рис. 8

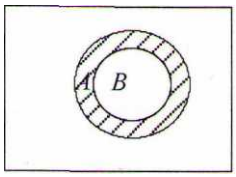


Рис. 9

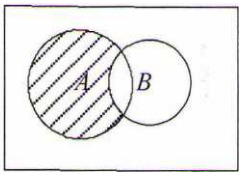


Рис.10

Если же множество $\boldsymbol{X}$ строится из большого числа множеств, скажем, если $\boldsymbol{X} = ((\boldsymbol{A}\backslash\boldsymbol{B}) \cap (\boldsymbol{B}\backslash\boldsymbol{C})) \cup (\boldsymbol{C}\backslash\boldsymbol{D})$, то здесь уже надо рассматривать 16 случаев взаиморасположения множеств *A*, *B*, *C*, *D*. В дальнейшем будет показано, что для *n* множеств $\boldsymbol{A_1}, \boldsymbol{A_2}, \dots, \boldsymbol{A_n}$ имеется ровно 2^n вариантов взаиморасположения множеств $\boldsymbol{A_1}, \boldsymbol{A_2}, \dots, \boldsymbol{A_n}$.

§2. Декартово произведение множеств

Операции над множествами, введенные в предыдущем параграфе, приводят к множествам, состоящим из тех же самых элементов. В этом параграфе рассмотрим еще одну операцию, приводящую к множеству, природа элементов которого в корне отличается от исходных элементов.

Определение 2.1. *Упорядоченной парой* $\langle x, y\rangle$ называется объект из двух элементов *x, y* такой, что $\langle x_1, y_1\rangle = \langle x_2, y_2\rangle$ тогда и только тогда, когда $x_1 = x_2$ и $y_1 = y_2$.

Очевидно, что при таком определении порядок следования элементов *x* и *y* имеет принципиальное значение и $\langle x, y\rangle \neq \langle y, x\rangle$, кроме частного случая, когда $x = $ y.

Определение 2.2. *Декартовым произведением* множеств $\boldsymbol{X}$ и $\boldsymbol{Y}$ называется множество всех упорядоченных пар $\langle x, y\rangle$ таких, что $x \in \boldsymbol{X}$ и $y \in \boldsymbol{Y}$. Обозначается декартово произведение как $\boldsymbol{X} \times \boldsymbol{Y}$.

Таким образом, $\boldsymbol{X} \times \boldsymbol{Y} = \{\langle x, y\rangle | x \in \boldsymbol{X}, y \in \boldsymbol{Y}\}$. Иногда декартово произведение называют прямым произведением множеств $\boldsymbol{X}$ и $\boldsymbol{Y}$.

Пример 2.1. Еще более наглядную иллюстрацию декартова произведения дает пример обычной плоскости. Пусть Λ-плоскость с заданной на ней декартовой системой координат $\boldsymbol{XOY}$. Тогда любая точка плоскости однозначно задается парой $\langle \alpha, \beta\rangle$ действительных чисел $\alpha, \beta \in \boldsymbol{R}$, и плоскость Λ есть не что иное, как произведение $\boldsymbol{R} \times \boldsymbol{R}$. И здесь, как уже отмечалось, $\boldsymbol{R} \not\subset \boldsymbol{R} \times \boldsymbol{R}$. Хотя мы и говорим, что множество действительных чисел $\boldsymbol{R}$ (ось $\boldsymbol{OX}$) входит в плоскость, но на самом деле в $\boldsymbol{R} \times \boldsymbol{R}$ входит множество пар вида $\langle \alpha, 0\rangle$, которое мы отождествляем с множеством действительных чисел $\boldsymbol{R}$.

Определение 2.3. Декартовым произведением n множеств $\boldsymbol{A_1, A_2, \dots, A_n}$ называется совокупность всех упорядоченных наборов $\langle x_1, x_2, \dots, x_n \rangle$, где $x_1 \in \boldsymbol{A_1}$,$x_2 \in \boldsymbol{A_2}$,...,$x_n \in \boldsymbol{A_n}$. Два упорядоченных набора $\langle x_1, x_2, \dots, x_n \rangle$ и $\langle y_1, y_2, \dots, y_n \rangle$ называются равными, если $x_1 = y_1$,...,$x_n = y_n$. Такие упорядоченные наборы называются *кортежами* из n элементов. Иногда их просто называют *n-ками*.

Декартово произведение n экземпляров множества $\boldsymbol{A}$ на себя называется *n-ой степенью* множества $\boldsymbol{A}$. Декартово произведение n множеств и n-я степень обозначаются как $\boldsymbol{A_1 \times A_2 \times \dots \times A_n}$ и $\boldsymbol{A^n}$ соответственно.

Таким образом, $\boldsymbol{A_1 \times A_2 \times \dots \times A_n} = \{\langle x_1, x_2, \dots, x_n \rangle | x_1 \in \boldsymbol{A_1}, x_2 \in \boldsymbol{A_2}, \dots, x_n \in \boldsymbol{A_n}\}$ и $\boldsymbol{A^n} = \{\langle x_1, x_2, \dots, x_n \rangle | x_1, x_2, \dots, x_n \in \boldsymbol{A}\}$

Пример 2.2. Пусть Λ — m-мерное векторное пространство над полем $\boldsymbol{P}$. Если зафиксировать некоторый базис $e_1, e_2, \dots, e_m$ пространства Λ, то каждый вектор x пространства Λ однозначно определяется m-ой $\langle x_1, x_2, \dots, x_m \rangle$, где $x_1, x_2, \dots, x_m \in \boldsymbol{P}$ — координаты вектора x в базисе $e_1, e_2, \dots, e_m$. Таким образом, пространство Λ можно рассматривать как декартову m-ую степень $\boldsymbol{P^m}$ с покоординатным сложением и умножением на элементы из $\boldsymbol{P}$ m-ок $\langle x_1, x_2, \dots, x_m \rangle$.

Рассмотрим некоторые простейшие свойства декартовых произведений.

Теорема 2.1. Для любых множеств $\boldsymbol{A}$, $\boldsymbol{X}$ и $\boldsymbol{Y}$ справедливы утверждения:

1. $\boldsymbol{A \times (X \cap Y) = (A \times X) \cap (A \times Y)}$ и $\boldsymbol{(X \cap Y) \times A = (X \times A) \cap (Y \times A)}$, т.е. декартово произведение дистрибутивно относительно операции пересечения.
2. $\boldsymbol{A \times (2.X \cup Y) = (A \times X) \cup (A \times Y)}$ и $\boldsymbol{(X \cup Y) \times A = (X \times A) \cup (Y \times A)}$, т.е. декартово произведение дистрибутивно относительно операции объединения.

Доказательство утверждения **1**. Пусть $\langle a, x \rangle \in \boldsymbol{A \times (X \cap Y)}$. По определению декартова произведения это означает, что $a \in \boldsymbol{A}$ и $x \in \boldsymbol{X \cap Y}$, то есть $a \in \boldsymbol{A}$, $x \in \boldsymbol{X}$ и $x \in \boldsymbol{Y}$. Тогда $\langle a, x \rangle \in \boldsymbol{A \times X}$ и $\langle a, x \rangle \in \boldsymbol{A \times Y}$, а значит, $\langle a, x \rangle \in \boldsymbol{(A \times X) \cap (A \times Y)}$.

Обратно: пусть $\langle a, x \rangle \in \boldsymbol{(A \times X) \cap (A \times Y)}$, т.е. $\langle a, x \rangle \in \boldsymbol{A \times X}$ и $\langle a, x \rangle \in \boldsymbol{A \times Y}$. По определению декартова произведения тогда $a \in \boldsymbol{A}$, $x \in \boldsymbol{X}$ и $x \in \boldsymbol{Y}$, т.е. $a \in \boldsymbol{A}$ и $x \in \boldsymbol{X \cap Y}$. Это означает, что $\langle a, x \rangle \in \boldsymbol{A \times (X \cap Y)}$, и утверждение 1 доказано.

Утверждение **2** доказывается аналогично.

Теорема 2.2. Для любых множеств $\boldsymbol{A}$, $\boldsymbol{B}$ и $\boldsymbol{X}$ справедливы утверждения:

1. если $\boldsymbol{A \subseteq B}$, то $\boldsymbol{(A \times X) \subseteq (B \times X)}$.
2. если $\boldsymbol{X \neq \emptyset}$ и $\boldsymbol{(A \times X) \subseteq (B \times X)}$, то $\boldsymbol{A \subseteq B}$.

Доказательство утверждения **1**. Пусть $\langle a, x \rangle \in \boldsymbol{A \times X}$. По определению, тогда $a \in \boldsymbol{A}$ и $x \in \boldsymbol{X}$, а так как $\boldsymbol{A \subseteq B}$, то $a \in \boldsymbol{B}$ и $x \in \boldsymbol{X}$. В таком случае $\langle a, x \rangle \in \boldsymbol{B \times X}$, что и требовалось.

Доказательство утверждения **2**. Пусть $a \in \boldsymbol{A}$. Тогда, т.к. $\boldsymbol{X \neq \emptyset}$, существует $x \in \boldsymbol{X}$ такой, что $\langle a, x \rangle \in \boldsymbol{A \times X}$. Поскольку $\boldsymbol{(A \times X) \subseteq (B \times X)}$, то $\langle a, x \rangle \in \boldsymbol{B \times X}$. В таком случае, согласно определению, $a \in \boldsymbol{B}$ и $x \in \boldsymbol{X}$, т.е. $\boldsymbol{A \subseteq B}$.

Теорема 2.3. Для любых множеств $\boldsymbol{A}$, $\boldsymbol{B}$, $\boldsymbol{X}$, $\boldsymbol{Y}$ справедливы равенства:

1. $\boldsymbol{(A \cap B) \times (X \cap Y) = (A \times X) \cap (A \times Y) \cap (B \times X) \cap (B \times Y)}$
2. $\boldsymbol{(A \cup B) \times (X \cup Y) = (A \times X) \cup (A \times Y) \cup (B \times X) \cup (B \times Y)}$
3. $\boldsymbol{(A \cap B) \times (X \cap Y) = (A \times X) \cap (B \times Y)}$
4. $\boldsymbol{(A \cap B) \times (X \cap Y) = (A \times Y) \cap (B \times X)}$

Доказательство. Следующая цепочка равенств, получаемая согласно теореме 2.1, приводит к доказательству утверждения **1**.

$$(\boldsymbol{A} \cap \boldsymbol{B}) \times (\boldsymbol{X} \cap \boldsymbol{Y}) = [\boldsymbol{A} \times (\boldsymbol{X} \cap \boldsymbol{Y})] \cap [\boldsymbol{B} \times (\boldsymbol{X} \cap \boldsymbol{Y})]$$
$$= [(\boldsymbol{A} \times \boldsymbol{X}) \cap (\boldsymbol{A} \times \boldsymbol{Y})] \cap [(\boldsymbol{B} \times \boldsymbol{X}) \cap (\boldsymbol{B} \times \boldsymbol{Y})]$$
$$= (\boldsymbol{A} \times \boldsymbol{X}) \cap (\boldsymbol{A} \times \boldsymbol{Y}) \cap (\boldsymbol{B} \times \boldsymbol{X}) \cap (\boldsymbol{B} \times \boldsymbol{Y})$$

Утверждение **2** доказывается аналогично.

Докажем утверждение **3**. Так как согласно равенству 1 $(\boldsymbol{A} \cap \boldsymbol{B}) \times (\boldsymbol{X} \cap \boldsymbol{Y}) = (\boldsymbol{A} \times \boldsymbol{X}) \cap (\boldsymbol{A} \times \boldsymbol{Y}) \cap (\boldsymbol{B} \times \boldsymbol{X}) \cap (\boldsymbol{B} \times \boldsymbol{Y})$, то $(\boldsymbol{A} \cap \boldsymbol{B}) \times (\boldsymbol{X} \cap \boldsymbol{Y}) \subseteq (\boldsymbol{A} \times \boldsymbol{X}) \cap (\boldsymbol{B} \times \boldsymbol{Y})$.

Обратно, пусть $u \in (\boldsymbol{A} \times \boldsymbol{X}) \cap (\boldsymbol{B} \times \boldsymbol{Y})$. Следовательно, $u = \langle a, x \rangle$, где $a \in \boldsymbol{A}$, $x \in \boldsymbol{X}$ и $u = \langle b, y \rangle$, где $b \in \boldsymbol{B}$ и $x \in \boldsymbol{Y}$. Поскольку $\langle a, x \rangle = \langle b, y \rangle$, то $a = b$ и $x = y$, т.е. $a \in \boldsymbol{B}$ и $x \in \boldsymbol{Y}$. Итак, $a \in \boldsymbol{A} \cap \boldsymbol{B}$, $x \in \boldsymbol{X} \cap \boldsymbol{Y}$, а значит, $u = \langle a, x \rangle \in (\boldsymbol{A} \cap \boldsymbol{B}) \times (\boldsymbol{X} \cap \boldsymbol{Y})$, что и требовалось.

Утверждение **4** доказывается аналогично.

§3. Отношения на множествах

Математическое понятие «отношение», так же как понятие «множество», является очень общим и широким. Мы сначала рассмотрим общие свойства отношений, а затем рассмотрим три специальных типа отношений: функции; отношение порядка; отношение эквивалентности.

Определение 3.1. *Бинарным отношением* называется любое множество ρ упорядоченных пар.

Если $\rho \subset \boldsymbol{A} \times \boldsymbol{B}$, то говорят, что ρ есть отношение между элементами множеств $\boldsymbol{A}$ и $\boldsymbol{B}$. Если $\rho \subset \boldsymbol{A} \times \boldsymbol{A}$, то говорят, что ρ есть бинарное отношение на множестве $\boldsymbol{A}$.

Если ρ — бинарное отношение и $\langle x, y \rangle \in \rho$, то говорят, что x и y связаны отношением ρ, или, что элемент x находится в отношении ρ с элементом y. Вместо записи $\langle x, y \rangle \in \rho$ часто употребляют запись $x \rho y$. Если элемент x не находится в отношении ρ с элементом y, то будем писать $x \bar{\rho} y$.

Таким образом, бинарное отношение между элементами множеств $\boldsymbol{A}$ и $\boldsymbol{B}$ устанавливает некоторую связь, соотношение, свойство, связывающее элементы из $\boldsymbol{A}$ и $\boldsymbol{B}$. При этом бинарное отношение ρ можно определить, задав непосредственно подмножество ρ из $\boldsymbol{A} \times \boldsymbol{B}$, а можно определить именно через свойство, связывающее элементы из $\boldsymbol{A}$ и $\boldsymbol{B}$. Например, на множестве $\boldsymbol{N}$ натуральных чисел отношение ρ зададим следующим образом: $m \rho n$ тогда и только тогда, когда число m нацело делится на n. Это же отношение можно задать, определив непосредственно ρ как подмножество из $\boldsymbol{N} \times \boldsymbol{N}$, а именно $\rho = \{\langle mt, m \rangle | m, t \in \boldsymbol{N}\}$.

Чаще всего отношение ρ легче задать через свойство, связывающее пары элементов, чем определять ρ как подмножество некоторого декартова произведения. Например, пусть $\boldsymbol{A}$ — множество всех прямых на плоскости. Отношение ρ на множестве $\boldsymbol{A}$ определим следующим образом: $l_1 \rho l_2$ тогда и только тогда, когда прямая l_1, перпендикулярна l_2. Таким образом, определенное отношение ρ вполне понятно: если прямые перпендикулярны, то они находятся в отношении ρ, в противном случае – не находятся. И довольно затруднительно задать это отношение как подмножество в $\boldsymbol{A} \times \boldsymbol{A}$.

Определение 3.2. Пусть ρ — некоторое бинарное отношение. Множество всех первых элементов пар из ρ, называется *областью определения* отношения ρ и обозначается через *Dom* ρ. Множество всех вторых элементов пар из ρ, называется *областью значений* отношения ρ и обозначается через *Im* ρ.

Таким образом $Dom\ \rho = \{x | \langle x, y\rangle \in \rho$ для некоторого элемента $y\}$

$$Im\rho = \{y | \langle x, y\rangle \in \rho \text{ для некоторого элемента } x\}$$

Из определения ясно, что $\rho \subseteq Dom\ \rho \times Im\ \rho$

Определение 3.3. Любое подмножество ρ декартова произведения $\boldsymbol{A_1 \times A_2 \times \ldots \times A_n}$ называется *n-арным* (иногда говорят *n-местным*) *отношением* между элементами множеств $\boldsymbol{A_1, A_2, \ldots, A_n}$**.** Если $\rho \subseteq \boldsymbol{A^n}$, то говорят, что ρ — есть *n*-арное (*n*-местное) отношение на $\boldsymbol{A}$.

В дальнейшем будем рассматривать в основном бинарные отношения. Итак, любое бинарное отношение между элементами множеств $\boldsymbol{A}$ и $\boldsymbol{B}$ есть подмножество из $\boldsymbol{A \times B}$. Следовательно, между бинарными отношениями, заданными на одних и тех же множествах $\boldsymbol{A}$ и $\boldsymbol{B}$, можно ввести операции объединения, пересечения, дополнения отношений, а также с помощью этих операций строить более сложные отношения. Пусть $\rho_1 \subset \boldsymbol{A \times B}$ и $\rho_2 \subset \boldsymbol{A \times B}$. В таком случае: $x(\rho_1 \cup \rho_2)y$, тогда и только тогда, когда $x\rho_1 y$ или $x\rho_2 y$; $x(\rho_1 \cap \rho_2)y$, тогда и только тогда, когда $x\rho_1 y$ и $x\rho_2 y$; $x\overline{\rho_1}y$, тогда и только тогда, когда $\langle x, y\rangle \notin \rho_1$. Отсюда становится ясным наше обозначение $x\overline{\rho_1}y$ того, что *x* и *y* не связаны отношением ρ_1.

Пример 3.1. На множестве действительных чисел $\boldsymbol{R}$ зададим два бинарных отношения: $x\rho_1 y$ тогда и только тогда, когда $x \leq y$, и $x\rho_2 y$ тогда и только тогда, когда $x \geq y$.

Геометрически это означает следующее. Множество пар действительных чисел из $\boldsymbol{R \times R}$ можно рассматривать как множество точек плоскости с заданной на ней декартовой системой координат *XOY*. В таком случае $x\rho_1 y$ означает, что точка (x, y) расположена над прямой $y = x$ или на ней. Аналогично, $x\rho_2 y$ означает, что точка (x, y) расположена под прямой $y = x$ или на ней. В таком случае $x(\rho_1 \cup \rho_2)y$ означает, что точка (x, y) расположена или над прямой $y = x$, или на этой прямой, или под ней, т.е. точка (x, y) просто находится на плоскости. Другими словами, любые два числа *x* и *y* находятся в отношении $(\rho_1 \cup \rho_2)$ и $(\rho_1 \cup \rho_2) = \boldsymbol{R \times R}$**.**

Далее, $x(\rho_1 \cap \rho_2)y$ означает, что точка (x, y) находится над прямой $y = x$ или на ней и одновременно под этой прямой или на ней. Это возможно лишь в случае, когда точка (x, y) находится на прямой $y = x$. Следовательно, $x(\mathrm{c}_1 \cap \rho_2)y$ тогда и только тогда, когда $x = y$.

Наконец, $x\overline{\rho_1}y$ означает, что точка (x, y) не находится ни на прямой $y = x$, ни над ней, а значит, эта точка находится строго под прямой $y = x$. Значит, $x\overline{\rho_1}y$ тогда и только тогда, когда $x > y$**.**

Кроме этих теоретико-множественных операций над отношениями можно ввести еще некоторые специальные операции.

Определение 3.4. *Инверсией* бинарного отношения ρ называется множество всех пар $\langle x, y\rangle$ таких, что $\langle y, x\rangle \in \rho$. Обозначается инверсия через ρ^U.

Определение 3.5. Пусть ρ_1и ρ_2 — два бинарных отношения. Множество всех пар $\langle x, y\rangle$ таких, что $\langle x, z\rangle \in \rho_2$ и $\langle z, y\rangle \in \rho_1$ для некоторого элемента z, называется *произведением* отношения ρ_1на ρ_2(*композицией*, *суперпозицией* отношений ρ_1 и ρ_2*)*. Обозначается произведение через $\rho_1\rho_2$**.**

Пример 3.2. Пусть на множестве натуральных чисел $\boldsymbol{N}$ задано отношение ρ следующим образом: $x\rho y$ тогда и только тогда, когда $x = y^2$. Значит, $\rho = \{\langle x^2, x\rangle | x \in \boldsymbol{N}\}$. В таком случае, $\rho^U = \{\langle x, x^2\rangle | x \in \boldsymbol{N}\}$. Пусть $x(\rho\rho)y$, т.е. существует такое число $z \in \boldsymbol{N}$, что $x\rho z$ и $z\rho y$. Это означает, что $x = z^2$ и $z = y^2$. В таком случае, $x(\rho\rho)y$ тогда и только тогда, когда $x = y^4$, т.е. $\rho\rho = \{\langle x^4, x\rangle | x \in \boldsymbol{N}\}$.

Теорема 3.1. Для любых бинарных отношений ρ_1, и ρ_2 справедливо равенство $(\rho_1\rho_2)^U = ({\rho_2}^U{\rho_1}^U)$.

Доказательство. Пусть элемент x находится с элементом y в отношении $(\rho_1\rho_2)^U$, т.е. $x(\rho_1\rho_2)^U y$. Следовательно, $y(\rho_1\rho_2)x$. Это означает, что существует такой элемент z, что $y\rho_2 z$ и $z\rho_1 x$. В таком случае, $z{\rho_2}^U y$ и $x{\rho_1}^U z$. По определению, тогда $x({\rho_2}^U{\rho_1}^U)y$, т.е. элемент x находится с элементом y в отношении ${\rho_2}^U{\rho_1}^U$.

Обратно, пусть элемент x находится с элементом y в отношении ${\rho_2}^U{\rho_1}^U$, т.е. $x({\rho_2}^U{\rho_1}^U)y$. Значит, существует элемент z такой что, $x{\rho_1}^U z$ или $z{\rho_2}^U$y или $z\rho_1 x$ и $y\rho_2 z$. В таком случае, $y(\rho_1\rho_2)x$, а значит $x(\rho_1\rho_2)^U y$.

Итак, показали, что из того, что элемент x находится с элементом yв отношении $(\rho_1\rho_2)^U$, следует, что элемент x находится с y в отношении ${\rho_2}^U{\rho_1}^U$, и наоборот. Это и означает равенство $(\rho_1\rho_2)^U = ({\rho_2}^U{\rho_1}^U)$.

Теорема 3.2. Для любых бинарных отношений ρ_1, ρ_2, ρ_3 справедливо равенство $(\rho_1\rho_2)\rho_3 = \rho_1(\rho_2\rho_3)$, т.е. умножение отношений ассоциативно.

Доказательство. Пусть $x[(\rho_1\rho_2)\rho_3]y$. Это означает, что для некоторого элемента z имеет место $x\rho_3 z$ и $z(\rho_1\rho_2)y$. По определению, тогда существует такой элемент θ, что $z\rho_2\theta$ и $\theta\rho_1 y$. Итак, $x\rho_3 z$, $z\rho_2\theta$ и $\theta\rho_1 y$. В таком случае $x(\rho_2\rho_3)\theta$ и $\theta\rho_1 y$. По определению, тогда $x[\rho_1(\rho_2\rho_3)]y$.

Итак, показали, что из $x[(\rho_1\rho_2)\rho_3]y$ следует $x[\rho_1(\rho_2\rho_3)]y$. Аналогично показывается обратное, а значит, $(\rho_1\rho_2)\rho_3 = \rho_1(\rho_2\rho_3)$.

В заключение этого параграфа рассмотрим вопрос, как бинарные отношения на конечных множествах задаются некоторыми специальными матрицами, и какие операции над этими матрицами соответствуют операциям над отношениями.

Пусть $\boldsymbol{X} = \{x_1, x_2, \dots, x_n\}$ — некоторое множество, и пусть $\rho \subset \boldsymbol{X} \times \boldsymbol{X}$ — некоторое бинарное отношение на множестве $\boldsymbol{X}$. Отношению ρ поставим в соответствие матрицу $\boldsymbol{A} = (a_{ij})$ следующим образом: $a_{ij} = \begin{cases} 1, \text{если } x_i \rho x_j \\ 0, \text{если } x_i \bar{\rho} x_j \end{cases}$

Получим матрицу размера $n \times n$ состоящую из 0 и 1. Всякая такая матрица называется *булевой матрицей.* Легко видеть, что любое отношение ρ на множестве $\boldsymbol{X}$ однозначно определяет некоторую булеву матрицу, и наоборот – всякая булева матрица однозначно определяет некоторое бинарное отношение на множестве $\boldsymbol{X}$.

Пусть ρ — бинарное отношение на множестве $\boldsymbol{X}$ и $\boldsymbol{A} = (a_{ij})$ — его булева матрица. Пусть $\boldsymbol{B} = (b_{ij})$ — булева матрица отношения $\bar{\rho}$. Если $b_{ij} = 1$, то $x_i \bar{\rho} x_j$, а значит $a_{ij} = 0$. Если же $b_{ij} = 0$, то $x_i \bar{\bar{\rho}} x_j$, т.е. $x_i \rho x_j$. Это означает, что $a_{ij} = 1$. Итак, получаем, что если $\boldsymbol{A} = (a_{ij})$ — матрица отношения ρ, то матрицей отношения $\bar{\rho}$ будет матрица $\boldsymbol{B} = (1 - a_{ij})$.

Пусть теперь даны два отношения ρ_1, ρ_2 и $\boldsymbol{A} = (a_{ij})$, $\boldsymbol{B} = (b_{ij})$ — соответствующие им булевы матрицы. Пусть $\boldsymbol{C} = (c_{ij})$ — матрица отношения $\rho_1 \cup \rho_2$. Если $c_{ij} = 1$, то $x_i(\rho_1 \cup \rho_2)x_j$, а значит, $x_i\rho_1 x_j$ или $x_i\rho_2 x_j$. Это означает, что хотя бы одно из чисел a_{ij} или b_{ij} равно 1. Если же $c_{ij} = 0$, то $x_i(\overline{\rho_1 \cup \rho_2})x_j$, или,

согласно закону де Моргана $x_i(\overline{\rho_1} \cap \overline{\rho_2})x_j$. Это означает, что $x_i\overline{\rho_1}x_j$ и одновременно $x_i\overline{\rho_2}x_j$. Следовательно, $a_{ij} = b_{ij} = 0$. Итак, $c_{ij} = 1$ тогда и только тогда, когда хотя бы одно из чисел a_{ij} или b_{ij} равно 1. Это равносильно тому, что $c_{ij} = \max(a_{ij}, b_{ij})$. Итак, получили, что если $\boldsymbol{A} = (a_{ij})$ и $\boldsymbol{B} = (b_{ij})$ — матрицы отношений ρ_1 и ρ_2, соответственно, то матрицей отношения $\rho_1 \cup \rho_2$ будет матрица $\boldsymbol{C} = \big(\max(a_{ij}, b_{ij})\big)$.

Теперь рассмотрим отношение $\rho_1 \cap \rho_2$ и его матрицу $\boldsymbol{C} = (c_{ij})$. Если $c_{ij} = 1$, т.е. $x_i(\rho_1 \cap \rho_2)x_j$, то $x_i\rho_1x_j$ и $x_i\rho_2x_j$. Следовательно, $a_{ij} = 1$ и $b_{ij} = 1$. Если же $c_{ij} = 0$, то $x_i\overline{(\rho_1 \cap \rho_2)}x_j$. По закону де Моргана $x_i(\overline{\rho_1} \cup \overline{\rho_2})x_j$, значит, $x_i\overline{\rho_1}x_j$ или $x_i\overline{\rho_2}x_j$. Это означает, что хотя бы одно из чисел, a_{ij} или b_{ij}, равно 0. Таким образом, $c_{ij} = 1$ тогда и только тогда, когда, $a_{ij} = b_{ij} = 1$. Это равносильно тому, что $c_{ij} = \min(a_{ij}, b_{ij})$. Итак, получили, что если $\boldsymbol{A} = (a_{ij})$, $\boldsymbol{B} = (b_{ij})$ — матрицы отношений ρ_1 и ρ_2 соответственно, то матрицей отношения $\rho_1 \cap \rho_2$ будет матрица $\boldsymbol{C} = \big(\min(a_{ij}, b_{ij})\big)$.

Наконец, выразим матрицу отношения $\rho_1\rho_2$ через матрицы $\boldsymbol{A} = (a_{ij})$, $\boldsymbol{B} = (b_{ij})$. Введем специальную операцию композиции матриц $\boldsymbol{A} \circ \boldsymbol{B} = (c_{ij})$. Для этого элемент c_{ij} определим следующим образом: $c_{ij} = \max\Big(\min(a_{i1}, b_{1j}), \min(a_{i2}, b_{2j}), \dots, \min(a_{in}, b_{nj})\Big)$. Элемент c_{ij}, в определенном смысле, определяется так же, как элемент обычного произведения матриц $\boldsymbol{AB}$. Для обычного произведения $\boldsymbol{AB}$ элемент $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}$. Для композиции $\boldsymbol{A} \circ \boldsymbol{B}$ произведения $a_{ik}b_{kj}$ заменяются на $\min(a_{ik}b_{kj})$, а сумма этих произведений заменяется на максимум полученных минимумов. Покажем, что булева матрица $\boldsymbol{A} \circ \boldsymbol{B}$ как раз и соответствует произведению отношений $\rho_1\rho_2$. Пусть $x_i(\rho_1\rho_2)x_j$, т.е. существует такой элемент x_k, что $x_i\rho_2x_k$ и $x_k\rho_1x_j$. Следовательно, в матрице $\boldsymbol{A}$ $a_{ik} = 1$ и в матрице $\boldsymbol{B}$ $b_{kj} = 1$. В таком случае, $\min(a_{ik}b_{kj}) = 1$, а значит $\max\Big(\min(a_{i1}, b_{1j}), \min(a_{i2}, b_{2j}), \dots, \min(a_{in}, b_{nj})\Big) = 1$, т.е. $c_{ij} = 1$. Пусть теперь $x_i\overline{(\rho_1\rho_2)}x_j$, т.е. не существует такой элемент x_k, что $x_i\rho_2x_k$ и $x_k\rho_1x_j$. Для матриц $\boldsymbol{A}$ и $\boldsymbol{B}$ это означает, что если для какого-то k $a_{ik} = 1$, то соответственно $b_{kj} = 0$. Значит, для всех k имеем $\min(a_{ik}b_{kj}) = 0$, а тогда и $\max\Big(\min(a_{i1}, b_{1j}), \min(a_{i2}, b_{2j}), \dots, \min(a_{in}, b_{nj})\Big) = 0$, т.е. $c_{ij} = 0$. Это и означает, что произведению отношений $\rho_1\rho_2$ соответствует булева матрица $\boldsymbol{A} \circ \boldsymbol{B}$.

§4. Отображения (функции)

Определение 4.1. Бинарное отношение f называется *отображением (функцией),* если для любых *x, y, z* из условия $\langle x, y\rangle \in f$ и $\langle x, z\rangle \in f$ следует, что $y = z$.

Таким образом, отношение f называется отображением, если для любого $x \in Domf$ существует единственный $y \in Imf$ такой, что $\langle x, y\rangle \in f$. Этот единственный элемент *y* обозначается через $f(x)$ и называется значением функции *f* для аргумента *x*. Если $\langle x, y\rangle \in f$, то обычно пишут $y = f(x)$, иногда $f: x \to y$.

Две функции *f* и *g* называются *равными*, если *f* и *g* равны как множества, т.е. для любых *x, y* $\langle x, y\rangle \in f$ тогда и только тогда, когда $\langle x, y\rangle \in g$. Таким образом,

функции f и g равны тогда и только тогда, когда $Domf = Domg$ и для любого $x \in Domf$ $f(x) = g(x)$. Записывают $f = g$.

Если отображение f задано на паре множеств $\boldsymbol{A}$ и $\boldsymbol{B}$, т.е. $f \subset \boldsymbol{A} \times \boldsymbol{B}$, то говорят, что f есть отображение из $\boldsymbol{A}$ в $\boldsymbol{B}$. Если при этом $\boldsymbol{A} = Domf$ и $Imf \subset \boldsymbol{B}$, то записывают $f: \boldsymbol{A} \to \boldsymbol{B}$.

Функция, область определения которой состоит из упорядоченных пар, называется функцией двух переменных, из упорядоченных троек — функцией трех переменных и т.д. В общем случае, если область определения состоит из n-ок, то для функции f от n переменных пишут $f(x_1, x_2, \dots, x_n)$ вместо $f(\langle x_1, x_2, \dots, x_n \rangle)$.

Под произведением функций понимается их произведение как отношений.

Теорема 4.1. Пусть f и g —отображения. Тогда их произведение fg есть также отображение. При этом:

1. $Dom(fg) = \{x | g(x) \in Domf\}$
2. $(fg)\,(\mathrm{x}) = f\,(g(x))$ для любого $x \in Dom(f\ g)$
3. $fg = \{\langle x, f(g(x)) \rangle | g(x) \in Domf\}$

Доказательство. По определению произведение fg есть множество всех пар $\langle x, y \rangle$ таких, что $\langle x, z \rangle \in g$ и $\langle z, y \rangle \in f$ для некоторого z. Так как g — отображение, то $\langle x, z \rangle \in g$ означает, что $z = g(x)$. Поскольку f — отображение, то $\langle z, y \rangle \in f$ означает, что $z = g(x) \in Domf$ и $y = f(z) = f(g(x))$. Следовательно, $fg = \{\langle x, y \rangle | \langle g(x), y \rangle \in f\}$. Далее, $\langle x, y \rangle \in fg$ тогда и только тогда, когда $y = f(g(x))$ и $g(x) \in Domf$ и $fg = \{\langle x, f(g(x)) \rangle | g(x) \in Domf\}$. Значит, fg есть отображение, для которого очевидно выполняются условия 1, 2, 3.

Определение 4.2. Отображение f множества $\boldsymbol{A}$ во множество $\boldsymbol{B}$ называется *инъективным,* если для любых $x, y \in Domf$ из равенства $f(x) = f(y)$ следует $x = y$, т.е. из $\langle x, z \rangle \in f$ и $\langle y, z \rangle \in f$ следует $x = y$.

Отображение f множества $\boldsymbol{A}$ во множество $\boldsymbol{B}$, называется *сюръективным,* если $Imf = \boldsymbol{B}$, т.е. для любого $y \in \boldsymbol{B}$ существует $x \in Domf$ такой, что $y = f(x)$.

Отображение f множества $\boldsymbol{A}$ во множество $\boldsymbol{B}$ называется *биективным,* если оно инъективно и сюръективно одновременно.

Теорема 4.2. Для отображений f и g справедливы утверждения:

1. произведение fg инъективных отображений f и g также инъективно;
2. произведение fg сюръективных отображений f и g также сюръективно;
3. произведение fg биективных отображений f и g также биективно;
4. если произведение fg инъективно, то g инъективно;
5. если произведение fg сюръективно, то f сюръективно.

Докажем эти утверждения.

1. Пусть $(fg)(x) = (fg)(y)$, т.е. $f(g(x)) = f(g(y))$. Так как f — инъективное отображение, то $g(x) = g(y)$. Поскольку g также инъективно, то $x = y$, т.е. fg — инъективное отображение.

2. Пусть $g: \boldsymbol{A} \to \boldsymbol{B}$, $f: \boldsymbol{B} \to \boldsymbol{C}$ и $y \in \boldsymbol{C}$. Так как f сюръективно, то существует $z \in \boldsymbol{B}$ такой, что $y = f(z)$. Поскольку g сюръективно, то существует $x \in \boldsymbol{A}$ такой, что $z = g(x)$. В таком случае, $y = f(z) = f(g(x)) = (fg)(x)$, т.е. отображение fg сюръективно.

3. Очевидным образом следует из 1 и 2.

4. Пусть для некоторых элементов x и y $g(x) = g(y)$. В таком случае, по определению отображения (4.1), $f(g(x)) = f(g(y))$ или $(fg)(x) = (fg)(y)$. Так как отображение fg инъективно, то $x = y$.

5. Пусть $y \in \boldsymbol{C}$, где $g: \boldsymbol{A} \to \boldsymbol{B}$, $f: \boldsymbol{B} \to \boldsymbol{C}$. Поскольку fg сюръективно, то существует $x \in \boldsymbol{A}$ такой, что $(fg)(x) = y$ или $f(g(x)) = $ y. Так как $g(x) \in \boldsymbol{B}$, то для элемента $z = g(x)$ имеем $f(z) = y$, т.е. f сюръективно.

Определение 4.5. Отображение $i_A: \boldsymbol{A} \to \boldsymbol{A}$ такое, что для всех $x \in \boldsymbol{A}$ $i_A(x) = x$, называется *тождественным,* или *единичным* отображением.

Итак, $i_A = \{\langle x, x\rangle | x \in \boldsymbol{A}\}$, и очевидно, что i_A — биективное отображение.

Теорема 4.3. Пусть f — сюръективное отображение множества $\boldsymbol{A}$ в $\boldsymbol{B}$. Инверсия f^U является отображением тогда и только тогда, когда f инъективно. При этом $ff^U = i_B$.

Доказательство. Инверсия f^U является отображением тогда и только тогда, когда из $\langle z, x\rangle \in f^U$ и $\langle z, y\rangle \in f^U$ следует, что $x = y$. Но это равносильно тому, что из условия $\langle x, z\rangle \in f$ и $\langle z, y\rangle \in f$ следует, что $x = y$. А это, в свою очередь равносильно инъективности f.

По определению инверсии $f^U = \{\langle y, x\rangle | \langle x, y\rangle \in f\}$. По определению композиции $ff^U = \{\langle y, z\rangle | \langle y, x\rangle \in f^U$ и $\langle x, z\rangle \in f$ для некоторого элемента $x\}$. Но из $\langle y, x\rangle \in f^U$ следует, что $\langle x, y\rangle \in f$. Таким образом, $\langle x, z\rangle \in f \langle x, y\rangle \in f$, поэтому $z =$ y. Итак, $ff^U = \{\langle y, y\rangle | \langle x, y\rangle \in f$ для некоторого элемента $x\}$. Так как f сюръективно, то для любого y $\in \boldsymbol{B}$ существует $x \in \boldsymbol{A}$ такой, что $\langle x, y\rangle \in f$. Следовательно, $ff^U = \{\langle y, y\rangle | y \in B\}$, а это и означает, что $ff^U = i_B$.

Определение 4.4. Пусть f – сюръективное отображение множества $\boldsymbol{A}$ в $\boldsymbol{B}$. Отображение $\varphi: \boldsymbol{B} \to \boldsymbol{A}$ называется *левым обратным* для f, если $\varphi f = i_A$. Отображением, обладающее левым обратным, называется обратимым слева.

Отображение $\varphi: \boldsymbol{B} \to \boldsymbol{A}$ называется *правым обратным* для f,если $f\varphi = i_B$. Отображение, обладающее правым обратным, называется обратимым справа.

Отображение $\varphi: \boldsymbol{B} \to \boldsymbol{A}$ называется *обратным* для f, если $\varphi f = i_A$ и $f\varphi = i_B$. Отображение называется *обратимым*, если обладает обратным.

Теорема 4.4. Отображение $f: \boldsymbol{A} \to \boldsymbol{B}$ обратимо тогда и только тогда, когда f — биективно. При этом обратное отображение, обозначаемое через f^{-1}, совпадает с f^U.

Доказательство. Если f — биекция, то согласно теореме 4.3 инверсия f^U является отображением и $ff^U = i_B$. Покажем, что $f^U f = i_A$. По определению инверсии $f^U(y) = x$ тогда и только тогда, когда $f(x) = y$.

В таком случае для любого $x \in \boldsymbol{A}$ имеем $(f^U f)(x) = f^U(f(x)) = f^U(y) = x$, т.е. $f^U f = i_A$. Таким образом, $f^U f = i_A$ и $ff^U = i_B$, что и означает, что f^U — обратное отображение для f.

Обратно, пусть f имеет обратное отображение $g: \boldsymbol{B} \to \boldsymbol{A}$, т.е. $gf = i_A$ и $fg = i_B$. Так как i_A инъективно и $gf = i_A$, то по теореме 4.2 отображение f инъективно. Поскольку i_B сюръективно и $fg = i_B$, то f сюръективно, а значит, f биективно. Осталось показать, что $g = f^U$. Для любого $y \in \boldsymbol{B}$ имеем $f^U(y) = i_A\big(f^U(y)\big) = (gf)\big(f^U(y)\big) = \big((gf)f^U\big)(y) = \big(g(ff^U)\big)(y) = g\big((ff^U)(y)\big) = g\big(i_B(y)\big) = g(y)$. Отсюда следует, что $f^U = g$.

Теорема 4.5. Для сюръективного отображения $f: \boldsymbol{A} \to \boldsymbol{B}$ следующие условия эквивалентны:

(1) инверсия f^U и является функцией;

(2) отображение f инъективно;

(3) отображение f обратимо справа;

(4) отображение f обратимо слева;

(5) отображение f обратимо;

(6) все функции, обратные к f (левые, правые, двусторонние) существуют и совпадают с f^U.

Доказательство. Условия **(1)** и **(2)** эквивалентны по теореме 4.3.

$(\mathbf{2}) \Rightarrow (\mathbf{3})$. Пусть f инъективно. Тогда по теореме 4.3 f^U является функцией и $ff^U = i_B$. Значит, f обратимо справа.

$(\mathbf{3}) \Rightarrow (\mathbf{4})$. Пусть f обратимо справа, т.е. для некоторого отображения $g: \boldsymbol{B} \to \boldsymbol{A}$ $fg = i_B$. Так как i_B инъективно, то по теореме 4.2 отображение g инъективно. Значит по теореме 4.6, $g\mathrm{g}^U = i_A$. В таком случае, $f = fi_A = f(g\mathrm{g}^U) = (fg)\mathrm{g}^U = i_B\mathrm{g}^U = \mathrm{g}^U$, .е. $f = \mathrm{g}^U$. Но тогда $g = f^U$ и $fg = g\mathrm{g}^U = i_A$, т.е. g является левым обратным для f и $g = f^U$.

$(\mathbf{4}) \Rightarrow (\mathbf{5})$. Пусть отображение f обратимо слева, т.е. $\varphi f = i_A$ для некоторого отображения $\varphi: \boldsymbol{B} \to \boldsymbol{A}$. Тогда по теореме 4.2 f инъективно и по теореме 4.3 $ff^U = i_B$. В таком случае $\varphi = \varphi i_B = \varphi(ff^U) = (\varphi f)f^U = i_A f^U = f^U$. Таким образом, $ff^U = i_B$ и $f^U f = i_A$. То есть f обратимо, и $f^{-1} = f^U$.

$(\mathbf{5}) \Rightarrow (\mathbf{6})$ и $(\mathbf{6}) \Rightarrow (\mathbf{1})$ очевидны.

§5. Основные алгебраические структуры

В этом параграфе мы познакомимся с некоторым типом отображений, называемых алгебраическими операциями, а также с основными типами алгебраических структур, т.е. множеств, на которых заданы некоторые алгебраические операции с определенными множествами.

Определение 5.1. Пусть дано множество $\boldsymbol{A}$. Всякое отображение $f: \boldsymbol{A} \times \boldsymbol{A} \to \boldsymbol{A}$, для которого $Domf = \boldsymbol{A} \times \boldsymbol{A}$, называется *бинарной алгебраической операцией* на множестве $\boldsymbol{A}$ (или просто бинарной операцией).

Фактически бинарная алгебраическая операция — это некоторое правило, по которому любой упорядоченной паре $\langle a, b\rangle$ элементов из $\boldsymbol{A}$ ставится в соответствие единственный элемент c из множества $\boldsymbol{A}$. Для любого такого правила должны соблюдаться три требования:

1. выполнимость, т.е. любой упорядоченной паре $\langle a, b\rangle$ должен быть поставлен в соответствие элемент;
2. замкнутость, т.е. элемент c, соответствующий паре $\langle a, b\rangle$, обязательно принадлежит множеству $\boldsymbol{A}$;
3. единственность, т.е. для любой пары $\langle a, b\rangle$ элемент c определяется однозначно.

Для операций не принята запись $f(a, b) = c$. Для операций используют какие-либо знаки, типа +, *, ◦, • и т.п., и записывают $c = a + b$, $c = a \bullet b$, $c = a * b$, $c = a^{\circ}b$ и т.п. Наиболее распространенные знаки – это знак суммы (+) и знак произведения (•), которые не надо путать с обычными значками суммы и произведения чисел. То есть когда мы пишем ab (знак произведения •, как правило,

опускают) для элементов a и b из некоторого множества $\boldsymbol{A}$, то имеем в виду, что ab — это тот самый единственный элемент c из $\boldsymbol{A}$, который поставлен в соответствие паре $\langle a, b\rangle$.

Например, обычные операции сложения и умножения действительных (натуральных, целых, рациональных) чисел — это бинарные алгебраические операции. Вычитание на множестве натуральных чисел уже не будет являться бинарной алгебраической операцией, так как, например, результат вычитания $3 - 5 = -2$ не является натуральным числом. Но это же вычитание будет бинарной алгебраической операцией на множестве целых, рациональных, действительных чисел. Так что, говоря о бинарной алгебраической операции, надо обязательно указывать множество, на котором эта операция рассматривается.

Рассмотрим множество $\boldsymbol{P(M)}$ для некоторого множества $\boldsymbol{M}$. Тогда рассмотренные ранее операции пересечения, объединения, разности множеств будут бинарными алгебраическими операциями на множестве $\boldsymbol{P(M)}$.

Для любого множества $\boldsymbol{X}$ обозначим через $\boldsymbol{F(X)}$ множество всех функций из $\boldsymbol{X}$ в $\boldsymbol{X}$. Тогда введенная ранее операция умножения функций будет также бинарной алгебраической операцией на $\boldsymbol{F(X)}$. Если через $\boldsymbol{S(X)}$ обозначим множество всех биективных отображений множества $\boldsymbol{X}$ в $\boldsymbol{X}$, то согласно теореме 4.4, умножение отображений из $\boldsymbol{S(X)}$ будет также бинарной алгебраической операцией на множестве $\boldsymbol{S(X)}$, так как произведение биекций есть снова биекция.

В дальнейшем в этом параграфе, вводя различные определения, мы будем бинарную алгебраическую операцию обозначать значком обычного умножения, а в каждом конкретном случае под этим значком будем понимать обычные операции сложения, умножения чисел, или объединения, пересечения множеств и т.п.

Определение 5.2. Бинарная операция на множестве $\boldsymbol{A}$ называется *коммутативной* (или *абелевой),* если для любых элементов $a, b \in \boldsymbol{A}$ выполняется равенство $ab = ba$.

Определение 5.3. Бинарная операция на множестве $\boldsymbol{A}$ называется *ассоциативной,* если для любых элементов $a, b, c \in \boldsymbol{A}$ выполняется равенство $(ab)c = a(bc)$.

Операции сложения и умножения чисел являются коммутативными и ассоциативными операциями. В то же время операция вычитания на множестве целых чисел не является коммутативной, так как $\mathrm{a} - \mathrm{b} \neq \mathrm{b} - \mathrm{a}$, для любых $\mathrm{a}, \mathrm{b} \in \mathbf{Z}$. Эта же операция не является ассоциативной, так как, к примеру, $(2 - 3) - 2 = -3 \neq 1 = 2 - (3 - 2)$.

Операции объединения и пересечения множеств, как уже отмечалось, являются коммутативными и ассоциативными операциями на множестве $\boldsymbol{P(M)}$. Также отмечалось, что операция разности множеств не будет коммутативной. Легко показать, что эта операция не будет ассоциативной.

Как уже отмечалось в теореме 3.10, произведение функций будет ассоциативной операцией на множестве $\boldsymbol{F(X)}$. В то же время, если множество $\boldsymbol{X}$ состоит более чем из двух элементов, то это произведение не будет коммутативной операцией на множестве $\boldsymbol{F(X)}$. Действительно, выделим во множестве $\boldsymbol{X}$ три элемента $a, b, c \in \boldsymbol{X}$ и определим два отношения $f, \varphi \in \boldsymbol{F(X)}$ следующим образом: $f(a) = b,\ f(b) = c,\ f(c) = a,\ f(x) = x$ для всех $x \neq a, b, c,\ \varphi(a) = c,\ \varphi(b) = b,\ \varphi(c) = a,\ \varphi(x) = x$ для всех $x \neq a, b, c$.

Тогда $(f\varphi)(a) = f\big(\varphi(a)\big) = f(c) = a$ и $(\varphi f)(a) = \varphi(f(a)) = \varphi(b) = b$, т.е. $f\,\varphi \neq \varphi f$.

Определение 5.4. Пусть $\boldsymbol{A}$ — множество с заданной на нем бинарной операцией. Элемент $e \in \boldsymbol{A}$ называется *нейтральным* для данной операции, если для любых элементов $a \in \boldsymbol{A}$ выполняется равенство $ae = ea = a$.

Если данная операция называется умножением, то элемент e принято называть *единичным,* а если операция называется сложением, то e принято называть *нулевым* элементом.

Во множестве целых (рациональных, действительных) чисел 0 является нейтральным элементом относительно операции сложения, а 1 — нейтральный элемент относительно умножения. Относительно операции вычитания эти множества не имеют нейтральных элементов. Действительно, если $a - e = a$, то единственным числом, удовлетворяющим этому равенству, является $e = 0$. Но для $e = 0$ имеем $0 - a = -a$, а должно было быть $e - a = a$, если бы e был нейтральным элементом.

Во множестве $\boldsymbol{P(M)}$ пустое множество $\emptyset$ является нейтральным элементом относительно операции объединения, так как для любого $\boldsymbol{A \subseteq M}$ имеем $\boldsymbol{A \cup \emptyset = \emptyset \cup A = A}$. Относительно операции пересечения нейтральным элементом во множестве $\boldsymbol{P(M)}$ будет само множество $\boldsymbol{M}$, так как для любого $\boldsymbol{A \subseteq M}$ имеем $\boldsymbol{A \cap M = M \cap A = A}$. Относительно разности множество $\boldsymbol{P(M)}$ не имеет нейтральных элементов. Действительно, пусть $\boldsymbol{E \in P(M)}$ — нейтральный элемент относительно разности. Пусть $\boldsymbol{A \backslash E = A}$. Это значит $\boldsymbol{A \cap E = \emptyset}$, но тогда $\boldsymbol{E \backslash A = E}$, а должно быть $\boldsymbol{E \backslash A = A}$.

Во множестве ***F(X)*** нейтральным элементом относительно умножения отображений является тождественное отображение i_x, так как для любой функции $f: \boldsymbol{X \to X}$ имеем $fi_x = i_x f = f$.

В рассмотренных примерах мы указали нейтральные элементы. Естественно возникает вопрос: а может кроме указанных есть еще нейтральные элементы? Следующая теорема говорит о том, что других нейтральных элементов нет.

Теорема 5.1. Если во множестве $\boldsymbol{A}$ с заданной на нем бинарной операцией существует нейтральный элемент e, то он единственен.

Доказательство. Пусть во множестве $\boldsymbol{A}$ существуют два нейтральных элемента e_1 и e_2. Так как e_1 — нейтральный элемент, то для любого $a \in \boldsymbol{A}$ имеем $ae_1 = e_1 a = a$, в частности для e_2 имеем $e_2 e_1 = e_1 e_2 = e_2$. Аналогично, так как e_2 — тоже нейтральный элемент, имеем $e_2 e_1 = e_1 e_2 = e_1$, т.е. $e_1 = e_2$.

Определение 5.5. Пусть $\boldsymbol{A}$ — множество с заданной на нем бинарной операцией и нейтральным элементом e относительно этой операции, и пусть $a \in \boldsymbol{A}$. Элемент $a' \in \boldsymbol{A}$ называется *симметричным* для элемента a, если $aa' = a'a = e$.

Также, как и для нейтрального элемента, если операция называется умножением, то симметричный элемент a' называется *обратным* и обозначается через a^{-1}, и если операция называется сложением, то симметричный элемент a' называется *противоположным* и обозначается через $-a$. Во множестве целых (рациональных, действительных) чисел относительно операции сложения для любого числа a симметричным будет обычное противоположное число $-a$. Во

множестве действительных (рациональных) чисел для элемента $a \neq 0$ относительно операции умножения симметричным будет обратное число $a^{-1} = \frac{1}{a}$.

Так что в этих множествах относительно умножения любой элемент, кроме нуля, имеет симметричный. Если рассмотрим множество целых чисел относительно умножения, то для любого числа $a \neq 0$ и $a \neq \pm 1$,число $\frac{1}{a}$ не будет уже целым. Поэтому во множестве целых чисел относительно умножения только ± 1 имеют симметричные элементы, которые совпадают с ними самими.

Рассмотрим множество $\boldsymbol{P(M)}$ относительно операции объединения. Мы уже отмечали, что в этом случае пустое множество $\emptyset$ является нейтральным элементом. Пусть $\boldsymbol{A} \in \boldsymbol{P(M)}$ и $\boldsymbol{A'}$ — симметричный для $\boldsymbol{A}$ элемент. Значит $\boldsymbol{A} \cup \boldsymbol{A'} = \boldsymbol{A'} \cup \boldsymbol{A} = \emptyset$, а это возможно лишь в одном случае, когда $\boldsymbol{A} = \boldsymbol{A'} = \emptyset$. Итак, относительно операции объединения во множестве $\boldsymbol{P(M)}$ лишь пустое подмножество $\emptyset$ имеет симметричный элемент, который совпадает с самим множеством $\emptyset$. Относительно операции пересечения во множестве $\boldsymbol{P(M)}$ нейтральным элементом является само множество $\boldsymbol{M}$. Если $\boldsymbol{A} \in \boldsymbol{P(M)}$ и $\boldsymbol{A'}$ — симметричный для него элемент, то $\boldsymbol{A} \cap \boldsymbol{A'} = \boldsymbol{A'} \cap \boldsymbol{A} = \boldsymbol{M}$, а это возможно лишь в одном случае: когда $\boldsymbol{A} = \boldsymbol{A'} = \boldsymbol{M}$.

Во множестве $\boldsymbol{F(X)}$ относительно операции умножения отображений отображение $f: \boldsymbol{X} \to \boldsymbol{X}$ имеет симметричный элемент тогда и только тогда, когда f — биекция (см. теорему 4.9).

Теорема 5.2. Пусть $\boldsymbol{A}$ — множество с заданной на нем ассоциативной бинарной операцией и с нейтральным элементом e. Если элемент $a \in \boldsymbol{A}$ имеет симметричный элемент, то этот симметричный элемент единственен.

Доказательство. Пусть $a', a" \in \boldsymbol{A}$ — симметричные элементы для элемента $a \in \boldsymbol{A}$. По определению имеем $aa' = a'a = e$ и $aa" = a"a = e$. В таком случае $a' = a'e = a'(aa") = (a'a)a" = ea" = a"$, т.е. $a' = a"$, и единственность доказана.

Определение 5.6. Множество с заданной на нем ассоциативной операцией называется *полугруппой.*

Определение 5.7. Полугруппа, обладающая нейтральным элементом, называется *моноидом.*

Определение 5.8. Моноид, в котором каждый элемент имеет симметричный, называется *группой.*

Итак, группа — это множество с заданной на нем бинарной операцией, относительно которой существует нейтральный элемент и каждый элемент имеет симметричный.

Множество натуральных чисел относительно операции сложения образует полугруппу. Множество целых (рациональных, действительных) чисел относительно сложения образуют группу. Относительно умножения моноидом является множество натуральных (целых, рациональных, действительных) чисел, но они не являются группой, так как не каждый элемент имеет симметричный. Множество всех отличных от нуля рациональных (действительных) чисел относительно умножения образует группу. Множество, состоящее из двух чисел ± 1 относительно операции умножения, образуют также группу.

Множество $\boldsymbol{P(M)}$ относительно операции объединения (пересечения) образует моноид, но не группу. Множество $\boldsymbol{F(X)}$ относительно операции

умножения отображений также образует моноид, но не группу. А вот множество ***S(X)*** всех биекций множества ***X*** на ***X*** относительно этой операции образует группу.

Отметим, что если операция в полугруппе (моноиде, группе) коммутативна, то такая полугруппа (моноид, группа) называется *абелевой*.

Мы рассмотрели основные алгебраические структуры, которые обладают одной бинарной операцией. Существуют алгебраические структуры, которые обладают несколькими операциями. Основными из них являются кольцо и поле.

Определение 5.9. Множество ***K*** называется *кольцом,* если на нем заданы две бинарные операции, называемые сложением и умножением, причем:

1) относительно сложения ***K*** является абелевой группой;

2) сложение и умножение связаны законами дистрибутивности, т.е. для любых $a, b, c \in \boldsymbol{K}$ справедливы равенства $a(b+c) = ab + ac$ и $(b+c)a = ba + ca$.

Если умножение ассоциативно, то кольцо называется *ассоциативным*.

Если относительно умножения имеется нейтральный элемент, то кольцо называется кольцом с единицей.

Если умножение коммутативно, то кольцо называется *коммутативным*.

Примерами колец являются множества целых, рациональных, действительных чисел относительно обычных операций сложения и умножения чисел.

Определение 5.10. Множество ***P*** называется *полем,* если оно есть кольцо, в котором все ненулевые элементы относительно умножения образуют абелеву группу.

Множество рациональных (действительных) чисел относительно операций сложения и умножения чисел образуют поле.

В заключение этого параграфа рассмотрим, как задаются операции на конечных множествах с помощью таблиц Кэли (см. табл.1–3).

Пусть $\boldsymbol{A} = \{a, b, c\}$. Запишем таблицу 1, в которой на пересечении строки и столбца содержится результат умножения элемента строки на элемент столбца.

Например, $a * b = b$, $c * c = b$ и т.д.

Так как $b * c = a$ и $c * b = c$, то эта операция не коммутативна. Поскольку $(b * c) * a = c$ и $b * (c * a) = b$, то операция не ассоциативна. Легко видеть, что нейтрального элемента нет, а значит, не может быть речи о симметричных элементах.

Таблица 1

*	*a*	*b*	*c*
a	*c*	*b*	*a*
b	*b*	*c*	*a*
c	*a*	*c*	*b*

Следующие две таблицы (табл. 2–3) задают на множестве $\boldsymbol{A} = \{a, b, c\}$ две операции, относительно которых ***A*** становится полем.

Таблица 2

+	*a*	*b*	*c*
a	*a*	*b*	*c*
b	*b*	*c*	*a*
c	*c*	*a*	*b*

Таблица 3

•	*a*	*b*	*C*
a	*a*	*a*	*A*
b	*a*	*b*	*C*
c	*a*	*c*	*B*

Все свойства операций, необходимые для поля, можно проверить непосредственным перебором.

Наконец, отметим, что наряду с бинарными операциями рассматриваются общие операции. Всякое отображение множества A^n в $\boldsymbol{A}$ называется *n-арной* операцией. В частности, при $n = 1$, операция называется *унарной,* при $n = 2$ получаем бинарную операцию.

Фиксированный элемент во множестве $\boldsymbol{A}$ (например, нейтральный) иногда называется *0-арной* операцией (нуль-арной).

§6. Отношения порядка

Для любого множества чисел $\boldsymbol{A}$ и любых элементов $a, b \in \boldsymbol{A}$ всегда можно сказать, какое из чисел a и b больше, а какое меньше. В этом смысле можно говорить, что элементы множества $\boldsymbol{A}$ упорядочены отношением «больше-меньше». Понятие «больше-меньше» есть не что иное, как некоторое отношение ρ на множестве $\boldsymbol{A}$**,** а именно: $a\rho b$ тогда и только тогда, когда $a \leq b$.

Интуитивно ясно, как можно сравнить множества $\boldsymbol{A}, \boldsymbol{B} \in \boldsymbol{P}(\boldsymbol{M})$. Если $\boldsymbol{A} \subset \boldsymbol{B}$, то можно считать, что элемент $\boldsymbol{A}$ меньше $\boldsymbol{B}$. В этом смысле элементы множества $\boldsymbol{P}(\boldsymbol{M})$ тоже определенным образом упорядочены, но не все, так как может быть $\boldsymbol{A} \not\subset \boldsymbol{B}$ и $\boldsymbol{B} \not\supset \boldsymbol{A}$.

В этом параграфе мы рассмотрим общие принципы введения порядка на произвольном множестве, то есть общие принципы понятия «больше-меньше» для элементов любого множества.

Определение 6.1. Бинарное отношение ρ на множестве $\boldsymbol{A}$ называется *рефлексивным*, если для любого элемента $x \in A$ имеем $x\rho x$, т.е. $\langle x, x\rangle \in \rho$.

Бинарное отношение ρ на множестве $\boldsymbol{A}$ называется *антирефлексивным* (или иррефлексивным), если любой элемент $x \in A$ не находится с самим собой в отношении ρ, т.е. $x\bar{\rho}x$, т.е. $\langle x, x\rangle \notin \rho$.

Другими словами, отношение ρ рефлексивно тогда и только тогда, когда $i_A \subset \rho$, и антирефлексивно тогда и только тогда, когда $i_A \cap \rho = \emptyset$.

Отношения параллельности прямых на плоскости, подобия треугольников, делимости нацело на множестве натуральных чисел — рефлексивные отношения.

Отношения перпендикулярности прямых на плоскости, неравенства на множестве чисел — примеры антирефлексивных отношений.

В то же время бинарное отношение может не быть ни рефлексивным, ни антирефлексивным. В этом случае говорят, что отношение просто *нерефлексивно* (не путать нерефлексивность с антирефлексивностью). Например, пусть на множестве целых чисел $\boldsymbol{Z}$ задано отношение: $x\rho y$ тогда и только тогда, когда $x + y = 2$. Это отношение не является рефлексивным, так как например, $2 + 2 \neq 2$, т.е. число 2 не находится с самим собой в отношении ρ. В то же время ρ не

является антирефлексивным, так как $1+1=2$, т.е. число 1 находится с самим собой в отношении ρ.

Определение 6.2. Бинарное отношение ρ на множестве $\boldsymbol{A}$ называется *транзитивным*, если для любых $x, y, z \in \boldsymbol{A}$ из соотношений $x\rho y,\ y\rho z$ следует, что $x\rho z$. В противном случае, если существует хотя бы одна тройка элементов $x, y, z \in \boldsymbol{A}$, для которых $x\rho y,\ y\rho z$, но $x\bar{\rho}z$, то отношение ρ не транзитивно.

Другими словами, отношение ρ транзитивно тогда и только тогда, когда $\rho^{\circ}\rho \subset \rho$.

Например, отношение делимости нацело на множестве целых чисел транзитивно, так как если a делится на b, а b делится на c, то очевидно, что a делится на c. Аналогично, отношение параллельности прямых на плоскости тоже транзитивно, поскольку если прямая l_1 параллельна прямой l_2, а прямая l_2 параллельна прямой l_3, то прямая l_1 параллельна прямой l_3. В то же время отношение перпендикулярности прямых на плоскости не транзитивно, так как если прямая l_1 перпендикулярна прямой l_2, а прямая l_2 перпендикулярна прямой l_3, то отсюда следует, что прямая l_1, параллельна прямой l_3, но не перпендикулярна. Аналогично, отношение неравенства на множестве действительных чисел не транзитивно, поскольку если $a \neq b$, $b \neq c$,то не обязательно $a \neq$ c. (Например, $2 \neq 3$ и $3 \neq 2$, но отсюда следует, что $2 = 2$).

Определение 6.3. Бинарное отношение ρ на множестве $\boldsymbol{A}$ называется *симметричным*, если для любых $x, y \in \boldsymbol{A}$ из условия $x\rho y$ всегда следует, что $y\rho x$.

Бинарное отношение ρ на множестве $\boldsymbol{A}$ называется *антисимметричным*, если для любых элементов $x, y \in \boldsymbol{A}$ из одновременного выполнения соотношений $x\rho y$ и $y\rho x$ всегда следует, что $x = y$.

Другими словами, отношение ρ симметрично тогда и только тогда, когда $\rho = \rho^{U}$, и отношение ρ антисимметрично тогда и только тогда, когда $\rho \cap \rho^{U} \subset i_A$.

К примеру, отношения параллельности, перпендикулярности прямых на плоскости — симметричные отношения. Отношение делимости на множестве натуральных чисел антисимметрично, поскольку если a делится нацело на b и наоборот, то $a = b$. Отношение включения на множестве $\boldsymbol{P}(\boldsymbol{M})$ также антисимметрично, так как если $\boldsymbol{A} \subseteq \boldsymbol{B}$ и $\boldsymbol{B} \subseteq \boldsymbol{A}$, то $\boldsymbol{A} = \boldsymbol{B}$ по определению.

Следует отметить, что надо быть аккуратным с антисимметричностью. В определении из условий $x\rho y$ и $y\rho x$ требуется совпадение именно самих элементов x и y, а не каких-либо свойств, их характеризующих. Например, пусть $\boldsymbol{A}$ — множество всех треугольников на плоскости, и отношение ρ на $\boldsymbol{A}$ задано следующим образом: $\Delta_1 \rho \Delta_2$ тогда и только тогда, когда их площади $S(\Delta_1)$ и $S(\Delta_2)$ связаны соотношением $S(\Delta_1) \leq S(\Delta_2)$. Для данного отношения ρ из условий $S(\Delta_1) \leq S(\Delta_2)$ и $S(\Delta_2) \leq S(\Delta_1)$ следует, что $S(\Delta_1) = S(\Delta_2)$. Но из равенства площадей двух треугольников вовсе не следует, что треугольники равны ($\Delta_1 = \Delta_2$), т.е. ρ не является антисимметричным. В то же время, если $\boldsymbol{A}$ — множество квадратов на плоскости и ρ — аналогичное отношение на $\boldsymbol{A}$, то оно антисимметрично. Действительно, из $S(\square_1) \leq S(\square_2)$ и $S(\square_2) \leq S(\square_1)$ следует, что $S(\square_1) = S(\square_2)$, т.е. $a^2 = b^2$, где a, b — стороны квадратов $\square_1$ и $\square_2$ соответственно. Отсюда $a = b$, а значит $\square_1 = \square_2$.

В §3 для конечного множества $\boldsymbol{X} = \{x_1, x_2, \ldots, x_n\}$ мы рассмотрели, как любое отношение $\rho \subset \mathrm{X} \times \mathrm{X}$ определяется однозначно некоторой булевой матрицей $\boldsymbol{A} = (a_{ij})$. А именно:

$$a_{ij} = \begin{cases} 1, \text{если } x_i \rho x_j \\ 0, \text{если } x_i \bar{\rho} x_j \end{cases}$$

Если ρ рефлексивно, т.е. $x_i \rho x_i$ для всех $i = 1,2,\dots,n$, то в матрице $\boldsymbol{A}$ на главной диагонали стоят единицы. Если ρ антирефлексивно, то, наоборот, на главной диагонали стоят нули. Матрица $\boldsymbol{A}$ будет симметричной для симметричного отношения, поскольку если $x_i \rho x_j$ (т.е. $a_{ij} = 1$),то $x_j \rho x_i$ (т.е. $a_{ji} = 1$). Для антисимметричного отношения при $i \neq j$ обязательно $a_{ij} \neq a_{ji}$, т.е. если $a_{ij} = 1$, то $a_{ji} = 0$, и если $a_{ij} = 0$, то $a_{ji} = 1$. Наконец, для транзитивного отношения, если какой-либо элемент матрицы $\boldsymbol{A^2}$ равен 1, то соответствующий элемент $\boldsymbol{A}$ также равен 1 (произведение булевых матриц было введено в §3).

Определение 6.4. Бинарное отношение ρ на множестве $\boldsymbol{A}$ называется *отношением порядка* на $\boldsymbol{A}$ или просто *порядком* на $\boldsymbol{A}$, если оно антисимметрично и транзитивно.

Порядок называется *нестрогим*, если он рефлексивен, и *строгим* — если антирефлексивен.

Порядок ρ называется *линейным*, если для любых $x, y \in \boldsymbol{A}$ либо $x \rho y$, либо $y \rho x$, либо $x = y$. Нелинейный порядок называется *частным*.

Пример 6.1.

1) Обычное отношение неравенства $<$ на любом числовом множестве — это строгий линейный порядок.

2) Отношение неравенства $\leq$ — нестрогий линейный порядок.

3) Отношение включения $\subset$ на множестве $\boldsymbol{P(M)}$ является строгим частичным порядком.

4) Отношение $\subseteq$ на множестве $\boldsymbol{P(M)}$ — нестрогий частичный порядок.

5) Отношение делимости на множестве натуральных чисел является нестрогим частичным порядком.

Определение 6.5. *Упорядоченным множеством* называется пара $\langle \boldsymbol{A}, \rho \rangle$, где $\boldsymbol{A}$ — множество, а ρ — порядок на множестве $\boldsymbol{A}$. Если ρ — линейный порядок, то $\langle \boldsymbol{A}, \rho \rangle$ называется *линейно упорядоченным* множеством, и $\langle \boldsymbol{A}, \rho \rangle$ называется *частично упорядоченным* множеством, если ρ — частичный порядок.

Отношение порядка — это обобщение естественного порядка меньше (больше) на множествах чисел. Поэтому частичный порядок часто обозначают значками $\preccurlyeq$ или $\prec$ для нестрогого и строгого порядков, соответственно. Обычно, если не возникает путаницы, порядок обозначают обычными значкам $\leq$ или $<$.

Определение 6.6. Пусть $\langle \boldsymbol{A}, \leq \rangle$ — частично упорядоченное множество. Элемент $a \in \boldsymbol{A}$ называется *наибольшим (наименьшим)* элементом во множестве $\boldsymbol{A}$, если для любого $x \in \boldsymbol{A}$ выполняется соотношение $x \leq a$ (соответственно, $a \leq x$).

Элемент $a \in \boldsymbol{A}$ называется *максимальным (минимальным)* во множестве A, если для любого $x \in \boldsymbol{A}$ из условия $a \leq x$ (соответственно, $x \leq a$) следует, что $x = a$.

Из определения очевидным образом следует, что наибольший (наименьший) элемент является максимальным (минимальным). Обратное, вообще говоря, неверно. Пусть, к примеру, на множестве $\boldsymbol{N}$ натуральных чисел задано отношение: $a \leq b$ тогда и только тогда, когда a нацело делится на b. Так как любое натуральное число делится на 1, то для любого $n \in \boldsymbol{N}$ и $1 \leq n$, т.е. 1 — наименьший элемент. Наибольшего элемента нет, так как если a — наибольший элемент, то

условие $n \leq a$ для любого $n \in \boldsymbol{N}$ означает, что a делится на любое натуральное число, а таких натуральных чисел a не существует. Если же $\boldsymbol{N_1}$ — множество натуральных чисел без единицы и $\leq$ — тот же порядок, то $\boldsymbol{N_1}$ уже не содержит наименьшего элемента. Действительно, если a — наименьший элемент, то условие $a \leq n$ для любого $n \in \boldsymbol{N_1}$означает, что $a \neq 1$ делит нацело любое натуральное число, что невозможно. В то же время всякое простое число будет минимальным. В самом деле, если p — простое число и $n \leq p$, то это означает, что простое число p делится нацело на натуральное число $n \neq 1$. Ввиду простоты числа p получаем, что $n = p$.

Определение 6.7. Линейно упорядоченное множество называется *вполне упорядоченным,* если каждое непустое подмножество имеет наименьший элемент.

Например, множество натуральных чисел $\boldsymbol{N}$ с отношением $<$ вполне упорядоченно, а множество действительных чисел $\boldsymbol{R}$ с этим же отношением не является вполне упорядоченным.

Теорема 6.1. В любом частично упорядоченном множестве $\langle \boldsymbol{A}, \leq \rangle$ может существовать не более одного наименьшего и не более одного наибольшего элемента.

Доказательство. Пусть 0 и 0^* — два наименьших элемента. Так как 0 — наименьший элемент, то для всех $a \in \boldsymbol{A}$ справедливо соотношение $0 \leq a$. В частности, $0 \leq 0^*$. Поскольку 0^* — наименьший элемент, то аналогично $0^* \leq 0$. Так как отношение порядка антисимметрично, то $0^* = 0$.

Определение 6.8. Пусть $\boldsymbol{S}$ — некоторое подмножество частично упорядоченного множества $\langle \boldsymbol{A}, \leq \rangle$. Элемент $a \in \boldsymbol{A}$ называется *нижней (верхней) границей* множества $\boldsymbol{S}$, если для всех $x \in \boldsymbol{S}$ справедливо соотношение $a \leq x$ (соответственно $x \leq a$).

Элемент $a \in \boldsymbol{A}$ называется *нижней (верхней) гранью* множества $\boldsymbol{S}$, если он является нижней (верхней) границей множества $\boldsymbol{S}$ и для любой нижней (верхней) границы $\bar{a}$ множества $\boldsymbol{S}$ справедливо соотношение $\bar{a} \leq a$ (соответственно, $a \leq \bar{a}$).

Нижняя (верхняя) грань множества $\boldsymbol{S}$ обозначается через $inf\boldsymbol{S}$ (соответственно, через $sup\boldsymbol{S}$). Читается «инфимум *S*» (соответственно, «супремум *S»).*

Другими словами, нижняя грань (верхняя грань) множества $\boldsymbol{S}$ — это самая большая (соответственно, самая маленькая) из нижних (соответственно, верхних) границ множества $\boldsymbol{S}$. Подмножество $\boldsymbol{S}$ может иметь не одну нижнюю (верхнюю) границу. В то же время аналогично теореме 6.1 можно доказать, что любое подмножество $\boldsymbol{S}$ может иметь не более одной нижней (верхней) грани.

Пример 6.1. Рассмотрим множество $\boldsymbol{R}$ действительных чисел с обычным отношением $\leq$, а в качестве подмножества $\boldsymbol{S}$ возьмем какой-либо интервал (a, b). В таком случае, любое число, меньшее a, будет нижней границей множества $\boldsymbol{S}$, а любое число, большее b, — это верхняя граница. В то же время $inf\boldsymbol{S} = a$ и $sup\boldsymbol{S} = b$.

Пример 6.2. Пусть $\boldsymbol{P(M)}$ — множество всех подмножеств множества $\boldsymbol{M}$ с обычным отношением включения $\subseteq$, и пусть $\boldsymbol{S} = \{\boldsymbol{M_1}, \boldsymbol{M_2}, \ldots, \boldsymbol{M_n}\}$,где $\boldsymbol{M_i} \in \boldsymbol{P(M)}$. Тогда $inf\boldsymbol{S} = \bigcap_{i=1}^{n} \boldsymbol{M_i}$ и $sup\boldsymbol{S} = \bigcup_{i=1}^{n} \boldsymbol{M_i}$, а любое подмножество и $\bigcap_{i=1}^{n} \boldsymbol{M_i}$ (содержащее в себе $\bigcup_{i=1}^{n} \boldsymbol{M_i}$) будет нижней (соответственно, верхней) границей для множества $\boldsymbol{S}$.

Определение 6.9. Пусть $\langle \boldsymbol{A}, \leq \rangle$ — частично упорядоченное множество, и a, b — два различных элемента из $\boldsymbol{A}$. Говорят, что элемент b доминирует над a, если, во-первых, $a < b$, и во-вторых, не существует элемента $x \in \boldsymbol{A}$ такого, что он отличен от a и b и $a \leq x \leq b$. Другими словами, если для некоторого $x \in \boldsymbol{A}$ имеем $a \leq x \leq b$, то либо $x = a$, либо $x = b$.

Пусть $\boldsymbol{A}$ — некоторое конечное множество чисел с обычным отношением порядка $\leq$. Известно, что для любых чисел $x, y \in \boldsymbol{A}$ таких, что $x < y$, во множестве $\boldsymbol{A}$ всегда найдутся такие числа $x_0, x_1, \dots, x_k \in \boldsymbol{A}$, что $x = x_0 < x_1 < \cdots < x_k = y$ и между x_{i-1} и x_i уже нельзя вставить ни одного числа из $\boldsymbol{A}$ (т.е. каждое x_i доминирует над x_{i-1}), $i = 1, \dots, k$.

Следующая теорема говорит о том, что данное утверждение справедливо для любого конечного множества $\boldsymbol{A}$ (не обязательно числового) и для любого отношения частичного порядка на множестве $\boldsymbol{A}$.

Теорема 6.2. Пусть $\langle \boldsymbol{A}, \leq \rangle$ — конечное частично упорядоченное множество $a, b \in \boldsymbol{A}$ — два таких различных элемента из $\boldsymbol{A}$, что $a \leq b$. Тогда множество $\boldsymbol{A}$ содержит по крайней мере одну цепь элементов $a = x_0 \leq x_1 \leq \cdots \leq x_k = b$, в которой каждый элемент x_i доминирует над x_{i-1}, $i = 1, \dots, k$.

Доказательство. Доказательство проведем индукцией по количеству n элементов y таких, что $a \leq y \leq b$ и $y \neq a$, $y \neq b$. Если $n = 0$, то b доминирует над a, и цепочка $a \leq b$ — искомая. Пусть утверждение верно для всех $n < k$, т.е. если между элементами a и b находится $n < k$ указанных элементов y, то искомая цепь существует. Докажем справедливость утверждения для $n = k$. Возьмем произвольный элемент c со свойством $a \leq c \leq b$ и $c \neq a$, $c \neq b$. Тогда количество элементов y со свойством $a \leq y \leq c$ и $y \neq a$, $y \neq c$ и количество элементов z со свойством $c \leq z \leq b$ и $z \neq c$, $z \neq b$ не превосходит $k - 1$. По индуктивному предположению существуют цепи $a = x_0 \leq x_1 \leq \cdots \leq x_s = c$ и $c = y_0 \leq y_1 \leq \cdots \leq y_t = b$, где каждый элемент x_i, y_i доминирует над x_{i-1}, y_{i-1}, соответственно, $i = 1,2, \dots, s$, $j = 1,2, \dots, t$. Тогда очевидно, что цепь $a = x_0 \leq x_1 \leq \cdots \leq x_s = c = y_0 \leq y_1 \leq \cdots \leq y_t = b$ будет искомой цепью.

Известно также, что элементы любого конечного числового множества $\boldsymbol{A}$ можно так занумеровать $\boldsymbol{A} = \{a_1, a_2, \dots, a_n\}$ что меньшее число будет в этой нумерации находиться раньше большего, т.е. если $a_i < a_j$, то $i < j$.

Следующая теорема говорит о том, что данную процедуру можно осуществить в любом конечном частично упорядоченном множестве (не обязательно числовом).

Теорема 6.3. Пусть $\langle \boldsymbol{S}, \leq \rangle$ — конечное частично упорядоченное множество, состоящее из n элементов. Тогда элементы из $\boldsymbol{S}$ можно так занумеровать $\boldsymbol{S} = \{x_1, x_2, \dots, x_n\}$, что из условия $x_i \leq x_j$ следует, что $i < j$.

Доказательство. Рассмотрим произвольную нумерацию множества $\boldsymbol{S} = \{x_1, x_2, \dots, x_n\}$, и пусть $\boldsymbol{X_m} = \{s_1, s_2, \dots, s_m\}$. Построим последовательность биекций β_m множества $\overline{m} = \{1,2, \dots m\}$ в себя таких, что каждое подмножество $\boldsymbol{X_m}$, перенумерованное посредством β_m в $\boldsymbol{X_m} = \{x_1^m, x_2^m, \dots, x_m^m\}$, где $x_i^m = s_{\beta_m(i)}$, будет удовлетворять условию такому, что из $x_i^m \leq x_j^m$ следует $i < j$.

При $m = 1$ биекция β_1 строится однозначно. Пусть биекция $\beta_{n-1}: \overline{n-1} \to \overline{n-1}$ с требуемым свойством уже построена, и построим биекцию $\beta_n: \overline{n} \to \overline{n}$ с требуемым свойством. Пусть k — наименьший среди индексов i со свойством

$s_n \le x_i^{n-1}$. Если такого k нет, т.е. для всех i $x_i^{n-1} \le s_n$, то тогда $x_1^{n-1}, x_2^{n-1}, \dots, x_{n-1}^{n-1}, s_n$ — требуемая нумерация. Поэтому считаем, что такое k есть. Построим биекцию β_n следующим образом:

$$\beta_n(i) = \begin{cases} i, & \text{если } i<k \\ k, & \text{если } i=k \\ i+1, & \text{если } i>k \end{cases}$$

Другими словами, вставим элемент s_n между x_{k-1}^{n-1} и x_k^{n-1}. Получим первую нумерацию $\{x_1^n, x_2^n, \dots, x_n^n\}$ и покажем, что это требуемая нумерация. Пусть $x_i^n \le x_j^n$. Если $x_i^n, x_j^n \in \boldsymbol{X_{n-1}}$, то $i < j$ по предположению индукции. Если $s_n = x_k^n \le x_j^n$, то $k < j$ по построению. Наконец, если $x_i^n \le x_k^n = s_n$, то $x_i^n \le x_k^n \le x_{k+1}^n$, откуда $x_i^n \le x_{k+1}^n$. Но $i < k+1$ по предположению индукции, так как $x_i^n, x_{k+1}^n \in \boldsymbol{X_{n-1}}$. Итак, во всех случаях $i < j$, если $x_i^n \le x_j^n$, и теорема доказана.

В заключение этого параграфа рассмотрим один из порядков на множестве $\boldsymbol{A}$, где $\boldsymbol{A}$ — некоторое линейно упорядоченное множество. Такой порядок называется лексикографическим, и он часто применяется при решении многих задач.

Теорема 6.4. Для n-мерных числовых векторов $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ и $b = (\beta_1, \beta_2, \dots, \beta_n)$ положим $a\rho b$ тогда и только тогда, когда либо $\alpha_i = \beta_i$ для всех $i = 1,2,\dots,n$, либо существует такое k, что $\alpha_k < \beta_k$ и http://pj.ii/$\alpha_i = \beta_i$ для всех $i = 1,2,\dots,k-1$. Тогда ρ есть линейный порядок на множестве n-мерных числовых векторов.

Доказательство. Так как для вектора $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ для любого $i = 1,2,\dots,n$ имеем $\alpha_i = \alpha_i$, то $a\rho a$, т.е. отношение ρ рефлексивно. Пусть $a\rho b$ и $b\rho a$ одновременно, и покажем, что $a = b$. Пусть $a \ne b$. Так как $a\rho b$, то существует такой номер k, что $\alpha_1 = \beta_1, \dots, \alpha_{k-1} = \beta_{k-1}$ и $\alpha_k < \beta_k$. Поскольку $b\rho a$ и $\beta_1 = \alpha_1, \dots, \beta_{k-1} = \alpha_{k-1}$, то по определению либо $\beta_k = \alpha_k$, либо $\beta_k < \alpha_k$. В обоих случаях получаем противоречие с условием $\alpha_k < \beta_k$.

Итак, $a = b$, т.е. отношение ρ антисимметрично. Наконец, пусть $a\rho b$, $b\rho c$, и покажем, что $a\rho c$, где $c = (\gamma_1, \gamma_2, \dots, \gamma_n)$. Понятно, что если $a = b$ или $b = c$, то $a\rho c$. Итак, пусть $a \ne b$ или $b \ne c$. Значит, существуют такие числа k и m, что $\alpha_1 = \beta_1, \dots, \alpha_{k-1} = \beta_{k-1}$, $\alpha_k < \beta_k$ и $\beta_1 = \gamma_1, \dots, \beta_{m-1} = \gamma_{m-1}$, $\beta_m < \gamma_m$. Если $k \le m$, то очевидно, что $\beta_k \le \gamma_k$. В таком случае, $\alpha_1 = \beta_1 = \gamma_1, \alpha_2 = \beta_2 = \gamma_2, \dots, \alpha_{k-1} = \beta_{k-1} = \gamma_{k-1}$ и $\alpha_1 < \beta_k \le \gamma_k$, т.е. $a\rho c$. Если $k > m$, то $\alpha_1 = \beta_1 = \gamma_1, \dots, \alpha_{m-1} = \beta_{m-1} = \gamma_{m-1}$ и $\alpha_m \le \beta_m < \gamma_m$, т.е. снова $a\rho c$, т.е. отношение ρ транзитивно. Итак, показали, что ρ — частичный порядок.

Возьмем два произвольных набора $a = (\alpha_1, \alpha_2, \dots, \alpha_n)$ и $b = (\beta_1, \beta_2, \dots, \beta_n)$. Если для всех i $\alpha_i = \beta_i$, то $a = b$. Пусть не для всех i выполняется равенство $\alpha_i = \beta_i$, и пусть k — наименьший номер, для которого $\alpha_k \ne \beta_k$. Если $\alpha_k < \beta_k$, то имеем $a\rho b$. Если же $\beta_k < \alpha_k$, то $b\rho a$. Таким образом, для любых векторов a и b либо $a\rho b$, либо $b\rho a$, либо $a = b$, т.е. порядок ρ является линейным.

Пример 6.3. Пусть $\boldsymbol{A_3}$ — множество всех трехмерных векторов, координаты которых равны 0 или 1. Легко видеть, что таких векторов будет 8. Тогда лексикографический порядок этих векторов будет следующим: $(0,0,0) < (0,0,1) < (0,1,0) < (0,1,1) < (1,0,0) < (1,0,1) < (1,1,0) < (1,1,1)$.

§7. Отношение эквивалентности

В этом параграфе мы рассмотрим еще один тип отношений — отношение эквивалентности, которое играет важнейшую роль не только в математике, но и в других областях науки. Это отношение, в некотором смысле, устанавливает единые принципы одинаковости рассматриваемых объектов.

Определение 7.1. Бинарное отношение ρ на множестве $\boldsymbol{A}$ называется *отношением эквивалентности,* если оно рефлексивно, симметрично и транзитивно. Если элементы $a, b \in A$ находятся в отношении ρ, то говорят, что элементы a и b *эквивалентны относительно* ρ.

Важность этого отношения связана со следующим фактом.

Определение 7.2. Разбиением множества $\boldsymbol{A}$ называется такая совокупность $S_i \subset \boldsymbol{A}$, $i \in \boldsymbol{I}$, его подмножеств, что: 1) $\boldsymbol{S_i} \cap \boldsymbol{S_j} = \emptyset$ для всех $i, j \in \boldsymbol{I}$, $i \neq j$; 2) $\boldsymbol{A} = \bigcup_{i \in I} \boldsymbol{S_i}$.

Другими словами, каждый элемент $x \in \boldsymbol{A}$ принадлежит одному и только одному подмножеству $\boldsymbol{S_i}$, $i \in \boldsymbol{I}$.

Теорема 7.1. Любое отношение эквивалентности ρ на множестве $\boldsymbol{A}$ задает некоторое разбиение множества $\boldsymbol{A}$. Обратно: всякое разбиение множества $\boldsymbol{A}$ задает на нем некоторое отношение эквивалентности ρ так, что разбиение, определяемое отношением ρ, совпадает с исходным разбиением.

Доказательство. Для каждого элемента $x \in \boldsymbol{A}$ определим подмножество $\rho_x = \{x \in \boldsymbol{A} | \, x \rho z \}$. Покажем, что семейство подмножеств ρ_x определяет некоторое разбиение. Так как ρ рефлексивно, то для любого элемента $x \in \boldsymbol{A}$ имеем $x \rho x$, т.е. $x \in \rho_x$. Это означает, что для любого элемента $x \in \boldsymbol{A}$ имеем включение $x = \cup \rho_x$, т.е. $\boldsymbol{A} = \cup \rho_x$. Теперь покажем, что для любых ρ_x и ρ_y, либо $\rho_x = \rho_y$ либо $\rho_x \cap \rho_y = \emptyset$. Для этого достаточно показать, что если $\rho_x \cap \rho_y \neq \emptyset$, то $\rho_x = \rho_y$. Пусть $\rho_x \cap \rho_y \neq \emptyset$ и $z \in \rho_x \cap \rho_y$. Это означает, что $x \rho z$ и $y \rho z$. Так как ρ симметрично, то имеем $x \rho z$ и $z \rho y$ что, в виду транзитивности ρ, дает $x \rho y$. Теперь покажем, что $\rho_x = \rho_y$. Пусть $t \in \rho_y$, т.е. $y \rho t$. Так как $x \rho y$ и $y \rho t$, то отсюда следует, что $x \rho t$. Это означает, что $t \in \rho_x$, т.е. $\rho_y \subseteq \rho_x$. Аналогично доказывается обратное включение $\rho_x \subseteq \rho_y$, т.е. $\rho_x = \rho_y$.

Обратно: пусть задано некоторое разбиение множества $\boldsymbol{A}$, т.е. $\boldsymbol{A} = \bigcup_{i \in I} \boldsymbol{S_i}$ и $\boldsymbol{S_i} \cap \boldsymbol{S_j} = \emptyset$ для всех $i, j \in \boldsymbol{I}$, $i \neq j$. Положим, $x \rho y$ тогда и только тогда, когда x и y принадлежат одному и тому же подмножеству $\boldsymbol{S_i}$. Покажем, что ρ есть отношение эквивалентности. Так как $x, x \in \boldsymbol{S_i}$, то $x \rho x$, т.е. ρ рефлексивно. Если $x \rho y$, то $x, y \in \boldsymbol{S_i}$. Но тогда и $y, x \in \boldsymbol{S_i}$, т.е. $y \rho x$, а значит ρ симметрично. Наконец, пусть $x \rho y$, $y \rho z$. Это означает, что $x, y \in \boldsymbol{S_i}$ и $y, z \in \boldsymbol{S_i}$. Так как элемент y, по определению разбиения, не может одновременно принадлежать двум разным подмножествам $\boldsymbol{S_i}$ и $\boldsymbol{S_j}$, то $\boldsymbol{S_i} = \boldsymbol{S_j}$. Но в таком случае, $x, z \in \boldsymbol{S_i}$, т.е. $x \rho z$ что означает транзитивность отношения ρ.

Таким образом, любое отношение эквивалентности на данном множестве разбивает это множество на попарно непересекающиеся классы эквивалентных элементов (*классы эквивалентности*).

Определение 7.3. Множество классов эквивалентности относительно отношения эквивалентности ρ на множестве A называется *фактор-множеством* множества A по отношению ρ, которое обозначается через A/ρ.

Класс эквивалентности, содержащий элемент a, обозначается через a/ρ. Если ясно, о каком отношении эквивалентности идет речь, то часто класс эквивалентности a/ρ обозначают через $[a]$. Любой класс эквивалентности a/ρ однозначно определяется любым своим элементом $x \in a/\rho$. Всякий такой элемент x называется *представителем класса* a/ρ.

Примерами отношения эквивалентности является отношение равенства геометрических фигур, отношение подобия геометрических фигур, отношение «иметь одинаковый возраст» на множестве студентов, отношение «иметь одинаковую площадь» на множестве земельных участков и т.п. На самом деле мы обычно имеем дело не с элементами, а с классами эквивалентных элементов относительно какого-либо отношения эквивалентности.

Пример 7.1. Рациональные дроби. Как мы знаем, рациональное число — это число, которое можно представить в виде отношения $\frac{m}{n}$, где $n \neq 0$ и m, n — целые числа. При этом мы говорим, что дроби $\frac{1}{2}$, $\frac{3}{6}$, $\frac{5}{10}$ — это одно и то же число. Хотя формально — это все-таки разные объекты. Так что же такое рациональное число?

Рассмотрим множество пар целых чисел (m, n), где $n \neq 0$. На таких парах введем отношение ρ следующим образом: $(m, n)\rho(k, l)$ тогда и только тогда, когда $ml = nk$. Так как $mn = mn$,то $(mn)\rho(mn)$, т.е. ρ рефлексивно. Если $(m, n)\rho(k, l)$, т.е. $ml = nk$, то $nk = ml$, а поэтому $(k, l)\,\rho(m, n)$. Значит, отношение ρ симметрично. Наконец, если $(m, n)\rho(k, l)$ и $(k, l)\rho(x, y)$, то $ml = nk$ и $ky = lx$. Умножим обе части первого равенства на y. Получаем $mly = nky = nlx$, т.е. $mly = nlx$. Так как $l \neq 0$, то отсюда $my = nx$. Это означает, что $(m, n)\rho(x, y)$, т.е. ρ транзитивно.

Таким образом, отношение ρ является отношением эквивалентности, и значит, ρ разбивает множество указанных пар на классы эквивалентности $\left[\frac{m}{n}\right]$. Класс $\left[\frac{m}{n}\right]$ — это и есть рациональнаядробь $\frac{m}{n}$, которая определяется любым своим представителем, имеющим вид $\frac{mk}{nk}$. Равноправие представителей класса $\left[\frac{m}{n}\right]$ позволяет производить сокращение числителя и знаменателя на одно и то же целое число (поскольку в результате получаем представителя того же класса), доумножать числитель и знаменатель на одно и то же целое число при приведении дробей к общему знаменателю и т.п.

Пример 7.2. Векторы. Рассмотрим в пространстве всевозможные направленные отрезки, т.е. отрезки у которых один из концов задан как начало, а другой — как конец. На множестве этих отрезков введем следующее отношение: $a\rho b$ тогда и только тогда, когда выполнены следующие условия:

1) длины отрезков a и b одинаковы;

2) отрезки a и b одинаково направлены, т.е. находятся на параллельных прямых;

3) отрезки a и b одинаково ориентированы, т.е. если отрезки параллельно перенести на одну прямую, соединив начала, то их концы будут располагаться на прямой по одну сторону от начала.

Тогда ρ есть отношение эквивалентности.

Действительно, рефлексивность, симметричность и транзитивность ρ легко проверяются геометрически, исходя из определения ρ.

Таким образом, множество всех направленных отрезков разбивается на непересекающиеся классы эквивалентных отрезков. Каждый такой класс и есть вектор, который обозначается через $\bar{a}$. Класс $\bar{a}$ полностью определяется любым своим представителем (направленным отрезком). Это позволяет перемещать параллельно (не меняя ориентации) направленные отрезки, проводить над ними операции (складывать, вычитать и т.д.).

Отношение эквивалентности позволяет не только разбивать множество на классы эквивалентности (т.е. каким-либо образом отождествлять элементы), но и строить различные новые конструкции. Пример 7.1 показывает, как, исходя из множества целых чисел, строятся рациональные числа с помощью некоторого отношения эквивалентности. В следующем параграфе рассмотрим очень важную алгебраическую систему, которая также строится с помощью отношения эквивалентности.

§8. Арифметика остатков

Пусть n — некоторое фиксированное натуральное число. Рассмотрим на множестве целых чисел $\boldsymbol{Z}$ следующее отношение: $x\rho y$ тогда и только тогда, когда разность $x - y$ нацело делится на n. Так как $x - x = 0$ делится на n, то $x\rho x$ для любого $x \in \boldsymbol{Z}$, т.е. отношение ρ рефлексивно. Если $x\rho y$, т.е. $x - y$ делится на n, то разность $y - x = -(x - y)$ также нацело делится на n. Значит $y\rho x$, т.е. отношение ρ симметрично. Наконец, пусть $x\rho y$ и $y\rho z$. Это означает, что числа $x - y$ и $y - z$ нацело делятся на n, тогда и их сумма $(x - y) + (y - z) = x - z$ тоже делится на n. Это значит, что $x\rho z$, т.е. отношение ρ транзитивно.

Итак, введенное отношение ρ является отношением эквивалентности. Значит, оно разбивает все множество целых чисел на непересекающиеся классы эквивалентности. Рассмотрим, что из себя представляет каждый из этих классов.

Известно, что каждое целое число m можно поделить с остатком на n, т.е. представить в виде $m = kn + r$, где k — частное, а r — остаток от деления числа m на n. Причем остаток удовлетворяет условию $0 \le r < n$. Всего различных остатков будет ровно n, а именно: $0,1,2,\dots,n-1$. Целое число m делится нацело на n тогда и только тогда, когда $r = 0$. Пусть $m_1 = k_1 n + r_1$ и $m_2 = k_2 n + r_2$, где $0 \le r_1 < n$ и $0 \le r_2 < n$, и рассмотрим разность $m_1 - m_2 = (k_1 - k_2)n + (r_1 - r_2)$. Если $r_1 = r_2$, то из этого равенства следует, что $m_1 - m_2 = (k_1 - k_2)n$, т.е. разность $m_1 - m_2$ нацело делится на n. Обратно, пусть разность $m_1 - m_2$ нацело делится на n: скажем $m_1 - m_2 = nt$. Тогда $r_1 - r_2 = (m_1 - m_2) - (k_1 - k_2)n = n(t - k_1 + k_2)$, т.е. разность $r_1 - r_2$ нацело делится на n. Поскольку $0 \le r_1 < n$ и $0 \le r_2 < n$, то $0 \le |r_1 - r_2| < n$. В таком случае делимость числа $r_1 - r_2$ нацело на n возможна лишь в случае $r_1 - r_2 = 0$, т.е. $r_1 = r_2$.

Итак, получим, что разность двух целых чисел m_1 и m_2 делится нацело на n тогда и только тогда, когда эти числа дают одинаковые остатки при делении на n. Следовательно, два числа m_1 и m_2 попадут в один и тот же класс эквивалентности относительно ρ тогда и только тогда, когда они дадут одинаковые остатки при делении на n.

Таким образом, отношение ρ разбивает все множество целых на n классов. А именно, класс чисел, дающих при делении на n остаток 0, класс чисел, дающих при делении на n остаток 1, класс чисел, дающих при делении на n остаток 2, и т.д. до $n-1$. Обозначим эти классы, соответственно через $[0],[1],[2],\dots,[n-1]$, а все множество классов через $\boldsymbol{Z(n)}$.

Исходя из определения разбиения и из определения данного отношения ρ, можно установить следующие свойства полученных классов.

1) Два класса $[k]$ и $[m]$ совпадают тогда и только тогда, когда $k-m=nt$ для некоторого целого числа t, где $0 \le k, m < n$.

2) Число x принадлежит классу $[k]$ тогда и только тогда, когда x при делении на n дает остаток k, где $0 \le k < n$.

3) Для любого целого числа x класс, содержащий число x, совпадает с классом $[r]$, где r — остаток от деления числа x на n.

Оказывается, на множестве классов $\boldsymbol{Z(n)}$ можно так ввести две операции (сложение и умножение), что множество $\boldsymbol{Z(n)}$ относительно этих операций становится кольцом.

Для любых двух классов $[m]$ и $[k]$ положим $[m]+[k]=[m+k]$, т.е. под суммой классов $[m]$ и $[k]$ понимается класс, содержащий число $m+k$. Таким образом, введенная операция действительно является бинарной алгебраической операцией. Для этого надо показать, что любым двум классам $[m]$ и $[k]$ по такому правилу ставится в соответствие единственный класс. Ведь мы сумму $[m]+[k]$ определили как класс $[m+k]$. Но если мы в классах $[m]$ и $[k]$ возьмем какие-то другие представители, скажем $[m]=[m_1]$ и $[k]=[k_1]$, и по нашему правилу определим $[m]+[k]=[m_1]+[k_1]=[m_1+k_1]$, то будут ли классы $[m+k]$ и $[m_1+k_1]$ совпадать? Так как $[m]=[m_1]$ и $[k]=[k_1]$, то $m_1-m=nt$ и $k_1-k=ns$ для некоторых целых чисел t и s. В таком случае $m_1=m+nt,\ k_1=k+ns$, и тогда $[m_1+k_1]=[m+nt+k+ns]=[n+k+n(t+s)]=[m+k]$. Итак, наша операция сложения приводит к однозначному результату. Так как $[m]+[n]=[m+n]=[n+m]=[n]+[m]$, то операция коммутативна. Далее $[m]+[k]+[l]=[m+k]+[l]=[(m+k)+l]=[m+(k+l)]=[m]+[k+l]=[m]+([k]+[l])$, т.е. операция ассоциативна. Очевидно, роль нейтрального элемента выполняет класс $[0]$, а для каждого элемента $[m]$ противоположным будет класс $[-m]$. Таким образом, множество $\boldsymbol{Z(n)}$ относительно введенной операции сложения образует абелеву группу.

Для классов $[m]$ и $[k]$ определим произведение $[m][k]$ как класс, содержащий mk, т.е. $[m][k]=[mk]$. Так же, как для сложения, покажем, что результат $[mk]$ не зависит от выбора представителей классов $[m]$ и $[k]$. Далее, легко установить, что введенная операция умножения является коммутативной, ассоциативной, класс $[1]$ будет нейтральным элементом относительно умножения, а также легко показать, что сложение и умножение связаны законами дистрибутивности.

Таким образом, относительно введенных операций сложения и умножения множество $\boldsymbol{Z(n)}$ становится ассоциативным, коммутативным кольцом с единицей.

Определение 8.1. Построенное выше кольцо $\boldsymbol{Z(n)}$ называется *кольцом вычетов по модулю* n.

На практике в качестве представителей классов $[0],[1]\dots,[n-1]$, как правило, берут числа $0,1,\dots,n-1$. При этом, чтобы сложить (умножить) два

класса, надо сложить (перемножить) их представители и полученный результат поделить с остатком на n. Класс, содержащий полученный остаток, и даст требуемую сумму (произведение).

Пример 8.1. Зададим операции в кольце $\boldsymbol{Z(4)}$ с помощью таблиц Кэли (см. табл. 4–5). Чтобы не загромождать таблицы, будем вместо классов $[0], [1], [2], [3]$ вписывать их представителей $0,1,2,3$.

Таблица 4

Сложение

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

Таблица 5

Умножение

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

Как видно из этого примера, элемент 3 имеет в кольце $\boldsymbol{Z(4)}$ обратный по умножению (он сам и будет для себя обратным), а элемент 2 обратного не имеет. Следующая теорема дает ответ на вопрос, какие элементы в кольце $\boldsymbol{Z(n)}$ имеют обратные относительно умножения.

Теорема 8.1. Элемент $[m]$ имеет в кольце $\boldsymbol{Z(n)}$ обратный относительно умножения тогда и только тогда, когда числа m и n взаимно просты.

Доказательство. Пусть $[m]$ имеет обратный, т.е. $[m][k] = [1]$ для некоторого класса $[k]$. Предположим противное, т.е. что числа m и n не взаимно просты. Следовательно, $m = td$ и $n = sd$, где d — их наибольший общий делитель, причем $1 < d < n$. Но тогда и $1 < s < n$. Умножим обе части равенства $[m][k] = [1]$ на $[s]$. Имеем $[s] = [m][k][s] = [t][d][k][s] = ([t][k])([d][s]) = [t][k][n] = [t][k][0] = [0]$. Итак, получили $[s] = [0]$, что невозможно, так как $1 < s < n$.

Обратно, пусть m и n взаимно просты, и покажем, что класс $[m]$ имеет обратный по умножению. Каждый из классов $[1], [2], \dots, [n-1]$ умножим на $[m]$.

Получим ряд классов $[m], [2m] \dots [(n-1)m]$. Покажем сначала, что все полученные классы различны. Пусть $[km] = [lm]$, где $1 \le k,\ l < n$. Это означает, что $km - lm = (k-l)m$ делится нацело на n. Так как m и n взаимно просты, то тогда $k - l$ делится нацело на n. Но это невозможно, так как $1 \le |k-l| < n$. Итак, имеем $n-1$ различных классов $[m], [2m] \dots [(n-1)m]$. Теперь покажем, что каждый из них отличен от $[0]$. Пусть $[km] = [0]$, где $1 \le k < n$. Значит, число km делится нацело на n. Следовательно, число k делится нацело на n, так как числа m и n взаимно просты. Но это невозможно, поскольку $1 \le k < n$. Таким образом, имеем $n-1$ отличных от $[0]$ различных классов $[m], [2m], \dots, [(n-1)m]$. Значит, эти классы есть не что иное, как классы $[1], [2], \dots, [n-1]$, записанные в каком-то другом порядке. Другими словами, множества $\{[1], [2], \dots, [n-1]\}$ и $\{[m], [2m], \dots, [(n-1)m]\}$ равны. В таком случае $[1] \in \{[m], [2m], \dots, [(n-1)m]\}$, т.е. $[1] = [km] = [k][m]$. Но это и означает, что класс $[k]$ является обратным для класса $[m]$.

Следствие 8.1. Кольцо $\boldsymbol{Z(n)}$ является полем тогда и только тогда, когда число n — простое.

Доказательство. Пусть $\boldsymbol{Z(n)}$ — поле. Следовательно, каждый из элементов $[2], [3], \ldots, [n-1]$ имеет по умножению обратный. По доказанной теореме, каждое из чисел $2, 3, \ldots, n-1$ взаимно просто с n. Это возможно лишь в случае, когда n — простое число.

Обратно, если n — простое число, то у него нет делителей, отличных от 1 и n. Тогда n взаимно просто с каждым из чисел $2, 3, \ldots, n-1$. По доказанной теореме, классы $[2], [3], \ldots, [n-1]$ (и очевидно, $[1]$) имеют по умножению обратные элементы. Но это и означает, что $\boldsymbol{Z(n)}$ — поле.

Определение 8.5. Кольцо $\boldsymbol{Z(n)}$ при простом числе n называется *полем вычетов по модулю* n.

Таблицы Кэли сложения и умножения для задания поля (см. табл.6–7) имеют следующий вид:

Таблица 6

Сложение		
	0	1
0	0	1
1	1	0

Таблица 7

Умножение		
	0	1
0	0	0
1	0	1

Кольцо $\boldsymbol{Z(n)}$ играет огромную роль в теории чисел. Оно также находит большое применение в дискретной математике (особенно поле $\boldsymbol{Z(n)}$), в частности в теории кодирования. Собственно говоря, работа всех вычислительных машин основана на арифметике поля $\boldsymbol{Z(2)}$.

Задание для самостоятельной работы**:** докажите, что $Z(2)$ является полем.

§9. Мощность множества

Теорема 9.1. Пусть множество $\boldsymbol{A}$ находится в отношении ρ со множеством $\boldsymbol{B}$, если существует биекция из $\boldsymbol{A}$ в $\boldsymbol{B}$. Тогда ρ — отношение эквивалентности на классе всех множеств.

Доказательство. Так как для любого множества $\boldsymbol{A}$ отображение $i_A: \boldsymbol{A} \to \boldsymbol{A}$ является биекцией, то AρA. Далее, если $f: \boldsymbol{A} \to \boldsymbol{B}$ — биекция, то $f^U: \boldsymbol{B} \to \boldsymbol{A}$ — тоже биекция (по теореме 4.4). Поэтому из $\boldsymbol{A\rho B}$ следует $\boldsymbol{B\rho A}$. Наконец, пусть $\boldsymbol{A\rho B}$ и $\boldsymbol{B\rho C}$. Это означает существование биекций $f: \boldsymbol{A} \to \boldsymbol{B}$ и $\varphi: \boldsymbol{B} \to \boldsymbol{C}$. В таком случае по теореме 4.4 произведение $\varphi f: \boldsymbol{A} \to \boldsymbol{C}$ также является биекцией. Следовательно, из $\boldsymbol{A\rho B}$ и $\boldsymbol{B\rho C}$ следует $\boldsymbol{A\rho C}$.

Определение 9.1. Два множества $\boldsymbol{A}$ и $\boldsymbol{B}$ называются *равномощными,* если они содержатся в одном классе эквивалентности относительно отношения ρ, указанного в теореме 9.1, т.е. если существует биекция из $\boldsymbol{A}$ в $\boldsymbol{B}$.

Мощность множества $\boldsymbol{A}$ — это такое свойство этого множества, которое присуще любому множеству $\boldsymbol{B}$, равномощному $\boldsymbol{A}$. То есть мощность — это то, что есть общего у всех равномощных (эквивалентных) множеств. Так как у всех эквивалентных между собой конечных множеств этим общим является количество элементов, или одинаковое число, из которых они состоят, то в применении к бесконечным множествам понятие мощности является аналогом понятия количества. Обозначается мощность множества $\boldsymbol{A}$ через $|\boldsymbol{A}|$ (иногда через card$\boldsymbol{A}$). Грубо говоря, мощность конечного множества — это количество элементов в данном множестве.

Определение 9.2. Множество $\boldsymbol{A}$, равномощное множеству натуральных чисел $\boldsymbol{N}$, называется *счетным.* В этом случае говорят, что множество $\boldsymbol{A}$ имеет мощность $\aleph_0$ (алеф-ноль).

Другими словами, счетное множество — это такое множество, все элементы которого можно занумеровать натуральными числами. Действительно, пусть существует биекция $f: \boldsymbol{N} \to \boldsymbol{A}$. Для натурального числа n присвоим номер n элементу $f(n)$, который соответствует данному числу n. Так как f — биекция, то таким образом каждый элемент из $\boldsymbol{A}$ получит один и только один номер из $\boldsymbol{N}$.

Теорема 9.2. Всякое подмножество счетного множества либо конечно, либо счетно.

Доказательство. Пусть подмножество $\boldsymbol{B}$ счетного множества $\boldsymbol{A}$ бесконечно. Покажем, что оно тогда счетно. Так как $\boldsymbol{A}$ счетно, то его можно занумеровать натуральными числами. В результате элементы из множества $\boldsymbol{B}$ также получат какие-то номера. Поскольку множество натуральных чисел вполне упорядоченно относительно естественного порядка $\leq$ (т.е. каждое непустое подмножество имеет наименьший элемент), то среди всех номеров элементов из множества $\boldsymbol{B}$ можно выбрать элемент с наименьшим номером. Обозначим этот элемент через b_1, т.е. некоторому элементу из $\boldsymbol{B}$ мы присвоим номер 1. Пусть мы уже присвоили каким-то элементам номера $1,2,\dots n$, т.е. выделили элементы $b_1, b_2, \dots, b_n$. Так как множество $\boldsymbol{B}$ бесконечно, то множество $\boldsymbol{B}\backslash\{b_1, b_2, \dots, b_n\}$ также бесконечно. Среди всех элементов множества $\boldsymbol{B}\backslash\{b_1, b_2, \dots, b_n\}$ выберем элемент с наименьшим номером (относительно нумерации множества $\boldsymbol{A}$). Обозначим этот элемент через b_{n+1}. Тем самым мы занумеровали натуральными числами все элементы подмножества $\boldsymbol{B}$, т.е. $\boldsymbol{B}$ счетно.

Теорема 9.3. Объединение любого конечного или счетного семейства счетных множеств есть *счетное множество*.

Доказательство. Пусть $\boldsymbol{A_1, A_2, \dots, A_n}$ — счетные множества и пусть $\boldsymbol{A} = \bigcup_{i=1}^{\infty} \boldsymbol{A_i}$. Можно считать, что множества $\boldsymbol{A_i}$ попарно не пересекаются. В самом деле, если это не так, то рассмотрим множества $\boldsymbol{B_1 = A_1}$, $\boldsymbol{B_2 = A_2\backslash A_1}$, $\boldsymbol{B_3 = A_3\backslash (A_1 U A_2)}, \dots, \boldsymbol{B_i = A_i\backslash (A_1 U A_2 U \dots U A_{i-1})}, \dots$. Покажем, что множества $\boldsymbol{B_k}$ и $\boldsymbol{B_m}$ не пересекаются при $k \neq m$. Пусть $x \in \boldsymbol{B_k} \cap \boldsymbol{B_m}$ и пусть $k > m$. Так как $x \in \boldsymbol{B_k\backslash (A_1 U A_2 U \dots U A_m U \dots U A_{k-1})}$, то $x \notin \boldsymbol{(A_1 U A_2 U \dots U A_m U \dots U A_{k-1})}$, а значит $x \notin \boldsymbol{A_m}$. Но в таком случае $x \notin \boldsymbol{A_m\backslash (A_1 U \dots U A_{m-1}) = B_m}$. Полученное противоречие говорит о том, что множества $\boldsymbol{B_1, B_2, \dots, B_n, \dots}$ попарно не пересекаются. Покажем, что $\bigcup_{i=1}^{\infty} \boldsymbol{B_i} = \bigcup_{i=1}^{\infty} \boldsymbol{A_i}$. Если $x \in \bigcup_{i=1}^{\infty} \boldsymbol{B_i}$, то $x \in \boldsymbol{B_k}$ для некоторого k. В таком случае $x \in \boldsymbol{A_k\backslash (A_1 U \dots U A_{k-1})}$. Значит $x \in \boldsymbol{A_k}$, и, следовательно, $x \in \bigcup_{i=1}^{\infty} \boldsymbol{A_i}$.

Обратно, пусть $x \in \bigcup_{i=1}^{\infty} \boldsymbol{A_i}$. Значит, x принадлежит каким-то множествам $\boldsymbol{A_i}$. Выберем среди них множество с наименьшим номером $\boldsymbol{A_k}$. Следовательно, $x \in \boldsymbol{A_k}$ и $x \notin \boldsymbol{A_1}, \dots, x \notin \boldsymbol{A_{k-1}}$. В таком случае, $x \notin \boldsymbol{A_1 U \dots U A_{k-1}}$ и следовательно, $x \in \boldsymbol{A_k\backslash (A_1 U \dots U A_{m-1}) = B_k}$, а значит $x \in \bigcup_{i=1}^{\infty} \boldsymbol{B_i}$.

Таким образом, множество $\boldsymbol{A}$ можно представить всегда в виде объединения попарно непересекающихся множеств $\boldsymbol{B_1, B_2, \dots, B_n, \dots}$ Согласно теореме 9.2, каждое из множеств $\boldsymbol{B_i}$, либо счетно, либо конечно. Значит, элементы каждого из множеств $\boldsymbol{B_i}$ можно пронумеровать $\boldsymbol{B_i} = \{b_{i1}, b_{i2}, \dots, b_{ik}, \dots\}$. Так как множества $\boldsymbol{B_i}$ попарно не пересекаются, то все элементы множества $\boldsymbol{A} = \bigcup_{i=1}^{\infty} \boldsymbol{B_i}$ можно записать в виде следующей матрицы (см. рис. 11).

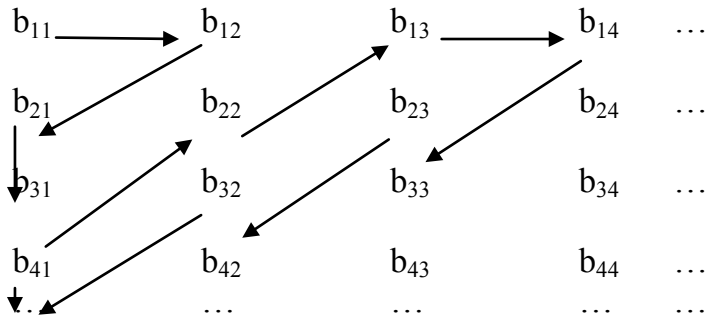


Рис. 11. Матрица элементов множества ***A***

Проведя нумерацию элементов множества A по указанным стрелкам, получим, что множество A счетно.

Теорема 9.4. Всякое бесконечное множество A содержит в себе счетное подмножество.

Доказательство. Выберем в A произвольный элемент и обозначим его через a_1. Так как A бесконечно, то $A\backslash\{a_1\} \neq \emptyset$. Значит, в этой разности можно выбрать элемент a_2. Поскольку A бесконечно, то $A\backslash\{a_1, a_2\} \neq \emptyset$. Значит, в этой разности можно выбрать элемент a_3 и т.д. Этот процесс не оборвется, так как на каждом -ом шаге будем получать бесконечное множество $A\backslash\{a_1, \ldots, a_k\}$, в котором можно выбрать следующий элемент a_{k+1}. В результате получаем счетное подмножество.

Из этих теорем следует, что множество целых чисел, рациональных чисел, точек плоскости (пространства) с рациональными координатами, многочленов с целыми коэффициентами и т.п. — это множества одинаковой счетной мощности.

Следующая теорема говорит о том, что существуют бесконечные множества, элементы которых нельзя пронумеровать, т.е. существуют несчетные множества.

Теорема 9.5. Множество действительных чисел на интервале $(0; 1)$ несчетно.

Доказательство. Предположим, что множество чисел на $(0; 1)$ можно пронумеровать $a_1, a_2, \ldots, a_n, \ldots$ Каждое из этих чисел можно записать в виде десятичной дроби $a_k = 0, \alpha_{k1}\alpha_{k2} \ldots \alpha_{kn}\ldots$,и все пронумерованные числа из интервала $(0; 1)$ запишем в виде таблицы:

$a_1 = 0, \alpha_{11}\alpha_{12} \ldots \alpha_{1n}\ldots$
$a_2 = 0, \alpha_{21}\alpha_{22} \ldots \alpha_{2n}\ldots$
……...
$a_k = 0, \alpha_{k1}\alpha_{k2} \ldots \alpha_{kn}\ldots$
……..

Построим дробь $b = 0, \beta_{11}\beta_{22} \ldots \beta_{nn}\ldots$ так, что для всех $i = 1,2, \ldots \beta_{ii} \neq \alpha_{ii}$, $\beta_{ii} \neq 0$ и $\beta_{ii} \neq 9$. Тогда число b отлично от любого из чисел $a_1, a_2, \ldots, a_n, \ldots$, так как в их записи в виде десятичнойдроби на n-ом месте стоит число, отличное от β_{nn}. Мы выбирали числа β_{ii} отличными от 0 и 9, чтобы не столкнуться с двойной записью дробей, например, $0{,}5 = 0{,}50000\ldots = 0{,}4999\ldots$ Итак, предположив, что a_1,a_2,...,a_n,... — все числа из $(0; 1)$, мы нашли число в $(0; 1)$, не вошедшее в данное

счетное множество. Полученное противоречие говорит о том, что множество чисел на $(0;1)$ несчетно.

Определение 9.3. Мощность любого множества, равномощного множеству действительных чисел на интервале $(0;1)$, называется мощностью *континуум.* Или говорят, что мощность такого множества равна $\aleph$ (алеф).

Пример 9.1. Множество действительных чисел на любом интервале $(a;b)$ имеет мощность континуум.

В самом деле, отображение $f(x) = a + (b-a)x$ является биекцией, отображающей интервал $(0;1)$ на интервал $(a;b)$.

Пример 9.2. Множество всех действительных чисел имеет мощность континуум.

Согласно предыдущему примеру, множество действительных чисел на интервале $\left(-\frac{\pi}{2};\frac{\pi}{2}\right)$ имеет мощность континуум. А функция $f(x) = tg(x)$ осуществляет биективное отображение интервала $\left(-\frac{\pi}{2};\frac{\pi}{2}\right)$ на все множество действительных чисел.

Аналогично теореме 9.3 имеет место следующая теорема, которую приведем без доказательства.

Теорема 9.6. Объединение конечного (счетного, континуального) числа множеств мощности континуум снова имеет мощность континуум. Более того, объединение конечного (счетного, континуального) числа множеств, среди которых хотя бы одно имеет мощность континуум, также имеет мощность континуум.

Итак, согласно определению 9.1, множества $\boldsymbol{A}$ и $\boldsymbol{B}$ имеют одинаковую мощность, если существует биекция, отображающая множество $\boldsymbol{A}$ на множество $\boldsymbol{B}$. Следующая теорема (которую мы приведем без доказательства) говорит о том, что условие существования биекции можно несколько ослабить.

Теорема 9.7 (Кантора-Берштейна). Если для множеств $\boldsymbol{A}$ и $\boldsymbol{B}$ существуют два инъективных отображения, отображающих $\boldsymbol{A}$ в $\boldsymbol{B}$ и, соответственно, $\boldsymbol{B}$ в $\boldsymbol{A}$, то существует биекция, отображающая $\boldsymbol{A}$ в $\boldsymbol{B}$. Другими словами, если во множествах $\boldsymbol{A}$ и $\boldsymbol{B}$ существует такие подмножества $\boldsymbol{A_1} \subset \boldsymbol{A}$ и $\boldsymbol{B_1} \subset \boldsymbol{B}$, что $|\boldsymbol{A}| = |\boldsymbol{B_1}|$ и $|\boldsymbol{B}| = |\boldsymbol{A_1}|$, то $|\boldsymbol{A}| = |\boldsymbol{B}|$.

Теорема Кантора-Берштейна позволяет ввести частичный порядок на множестве всех мощностей.

Теорема 9.8. Для множеств $\boldsymbol{A}$ и $\boldsymbol{B}$ положим $|\boldsymbol{A}| \le |\boldsymbol{B}|$, если существует инъективное отображение из $\boldsymbol{A}$ в $\boldsymbol{B}$. Тогда данное отношение является частичным порядком на множестве всех мощностей.

Доказательство. Так как для любого множества $\boldsymbol{A}$ отображение $i_A: \boldsymbol{A} \to \boldsymbol{A}$ является инъективным (даже биективным), то $|\boldsymbol{A}| \le |\boldsymbol{A}|$, т.е. введенное отношение $\le$ рефлексивно. Пусть $|\boldsymbol{A}| \le |\boldsymbol{B}|$ и $|\boldsymbol{B}| \le |\boldsymbol{A}|$. По определению существуют инъективные отображения $f: \boldsymbol{A} \to \boldsymbol{B}$ и $\varphi: \boldsymbol{B} \to \boldsymbol{A}$. Согласно теореме Кантора-Берштейна тогда существует биекция из $\boldsymbol{A}$ на $\boldsymbol{B}$, т.е. $|\boldsymbol{A}| = |\boldsymbol{B}|$. Следовательно, данное отношение $\le$ антисимметрично. Наконец, пусть $|\boldsymbol{A}| \le |\boldsymbol{B}|$ и $|\boldsymbol{B}| \le |\boldsymbol{C}|$, т.е. существуют инъективные отображения $f: \boldsymbol{A} \to \boldsymbol{B}$ и $\varphi: \boldsymbol{B} \to \boldsymbol{C}$. Тогда, согласно теореме 4.2, произведение $\varphi f: \boldsymbol{A} \to \boldsymbol{C}$ является инъекцией, и значит $|\boldsymbol{A}| \le |\boldsymbol{C}|$.

Итак, теорема 9.8 вводит на множестве всех мощностей частичный порядок. Оказывается, из теоремы Кантора-Берштейна следует, что этот порядок является линейным. Другими словами, для любых двух множеств всегда существует инъекция, отображающая одно из множеств в другое. Следовательно, для любых двух множеств либо их мощности равны, либо мощность одного больше мощности другого. Согласно теореме 9.4, среди бесконечных мощностей мощность $\aleph_0$ является наименьшей, в частности, $\aleph_0 < \aleph$.

Следующая теорема говорит о том, что существуют множества сколь угодно больших мощностей. Более точно: для любого множества $\boldsymbol{A}$ всегда найдется такое множество $\boldsymbol{A'}$, что $|\boldsymbol{A}| < |\boldsymbol{A'}|$.

Теорема 9.9. Пусть $\boldsymbol{A}$ — произвольное множество. Тогда мощность множества $\boldsymbol{P(A)}$ всех его подмножеств строго больше мощности множества $\boldsymbol{A}$.

Доказательство. Легко видеть, что отображение $f: \boldsymbol{A} \to \boldsymbol{P(A)}$, заданное по правилу $f(a) = \{a\}$, является инъективным. Следовательно, $|\boldsymbol{A}| \le |\boldsymbol{P(A)}|$. Докажем, что неравенство строгое. Для этого надо показать, что не существует биекции из $\boldsymbol{A}$ на $\boldsymbol{P(A)}$. Предположим противное, т.е. что существует биекция $f: \boldsymbol{A} \to \boldsymbol{P(A)}$. Для элемента $x \in \boldsymbol{A}$ элемент $f(x)$ будем обозначать соответствующей заглавной буквой $\boldsymbol{A}$, так что $a \to \boldsymbol{A}$, $b \to \boldsymbol{B}$,..., $x \to \boldsymbol{X}$... Покажем, что элементы $\boldsymbol{A, B, \dots, X, \dots}$ не исчерпывают все множество $\boldsymbol{P(A)}$. Для этого построим такое подмножество $\boldsymbol{X} \subset \boldsymbol{A}$, которому не соответствует ни один элемент из $\boldsymbol{A}$. Пусть $\boldsymbol{X}$ — совокупность всех тех элементов из $\boldsymbol{A}$, которые не входят в соответствующее им множество. Подробно: если $b \to \boldsymbol{B}$ и $b \in \boldsymbol{B}$, то $b \notin \boldsymbol{X}$, и если $b \notin \boldsymbol{B}$, то $b \in \boldsymbol{X}$. Итак, построили подмножество $\boldsymbol{X} \subset \boldsymbol{M}$. Так как $f: \boldsymbol{A} \to \boldsymbol{P(A)}$ — биекция, то существует элемент $x \in \boldsymbol{A}$ такой, что $f(x) = \boldsymbol{X}$, т.е. $x \to \boldsymbol{X}$, если $x \notin \boldsymbol{X}$, то x включаем в $\boldsymbol{X}$, т.е. $x \in \boldsymbol{X}$. Если же $x \in \boldsymbol{X}$, то по построению $x \notin \boldsymbol{X}$. Итак, элемент $x \in \boldsymbol{A}$ одновременно принадлежит и не принадлежит подмножеству $\boldsymbol{X}$. Полученное противоречие говорит о том, что не существует биекции, отображающей $\boldsymbol{A}$ на $\boldsymbol{P(A)}$, значит $|\boldsymbol{A}| < |\boldsymbol{P(A)}|$.

Для любого множества $\boldsymbol{A}$ мощность множества $\boldsymbol{P(A)}$ обозначают через $2^{|\boldsymbol{A}|}$, т.е. $|\boldsymbol{P(A)}| = 2^{|\boldsymbol{A}|}$. Смысл такого обозначения будет разъяснен в следующем параграфе.

§10. Элементы комбинаторики

К задачам комбинаторики относятся задачи следующего типа. Дано множество $\boldsymbol{A}$ из n элементов. Сколькими способами можно из элементов множества $\boldsymbol{A}$ построить множества (не обязательно подмножества $\boldsymbol{A}$), обладающие данным свойством?

Существуют два основных правила комбинаторики.

Правило суммы. Если объект $\boldsymbol{A}$ можно выбрать m способами, а объект $\boldsymbol{B}$ — n способами, и ни один из способов выбора объекта $\boldsymbol{A}$ не совпадает ни с одним из способов выбора объекта $\boldsymbol{B}$, то выбор хотя бы одного из объектов $\boldsymbol{A}$ или $\boldsymbol{B}$ можно осуществить $m + n$ способами.

Правило произведения. Если объект $\boldsymbol{A}$ можно выбрать m способами, и если после каждого такого выбора объект $\boldsymbol{B}$ можно выбрать n способами, то одновременный выбор пары $\boldsymbol{(A, B)}$ можно осуществить mn способами.

Определение 10.1. Пусть имеется n предметов и $1 \le k \le n$.

k-размещением без повторений называется любой упорядоченный набор из k элементов. При этом два -размещения без повторений считаются различными, если либо они отличаются друг от друга хотя бы одним элементом, либо состоят из одних и тех же элементов, но расположенных в различном порядке.

Теорема 10.1. Если A_n^k— общее число k-размещений без повторений, которые можно построить из n элементов, то $A_n^k = n(n-1)(n-2)\dots(n-k+1)$.

Доказательство. Пусть $(a_1, a_2, \dots, a_n)$ — некоторое k-размещение без повторений. Элемент a_1, можно выбрать любым из n способов. После этого элемент a_2 можно выбрать из оставшихся, т.е. его можно выбрать $(n-1)$-им способом. По правилу произведения пару (a_1, a_2) можно выбрать $n(n-1)$ способами. После того, как пара (a_1, a_2) выбрана, элемент a_3 можно выбрать $(n-2)$-мя способами. По правилу произведения тройку (a_1, a_2, a_3) можно выбрать $n(n-1)(n-2)$-мя и далее способами. В конечном итоге на шаге k получаем $A_n^k = n(n-1)(n-2)\dots(n-k+1)$

Определение 10.2. Любое k-размещение без повторений из n элементов при $k = n$ называется *перестановкой* из n элементов.

Теорема 10.2. Если P_n — общее число перестановок из n элементов, то $P_n = n! = n(n-1)(n-2)\cdot\ldots\cdot 2 \cdot 1$.

Доказательство этого утверждения непосредственно следует из предыдущей теоремы, если в формулу для A_n^k вместо k подставим n.

Определение 10.3. Пусть имеется n предметов и $1 \le k \le n$. k-размещение, в котором допускается повторение элементов, называется *k-размещением с повторениями.*

Теорема 10.3. Если $\overline{A_n^k}$ — общее число k-размещений с повторениями, то $\overline{A_n^k} = n^k$.

Доказательство. Доказательство проведем индукцией по k. Размещений по одному элементу можно выбрать в точности n, т.е. $\overline{A_n^1} = n^1$. Предположим, что $\overline{A_n^{k-1}} = n^{k-1}$, и докажем, что $\overline{A_n^k} = n^k$. Возьмем любое $(k-1)$-размещение с повторением $(a_1, a_2, \dots, a_{k-1})$ и припишем к нему произвольный элемент a_k из имеющихся n элементов. Получим некоторое k-размещение с повторением. Таким образом мы получим все k-размещения с повторениями, так как для любых -размещений $(a_1, \dots, a_{k-1}, a_k)$ и $(b_1, \dots, b_{k-1}, b_k)$, таким образом полученных, либо $(a_1, \dots, a_{k-1}) \ne (b_1, \dots, b_{k-1})$, либо $a_k \ne b_k$. По предположению индукции $(k-1)$-размещений с повторениями можно выбрать n^{k-1} способами, а элемент a_k можно выбрать n способами.

Согласно правилу произведения все k-размещения с повторениями можно выбрать $n^{k-1}.n = n^k$ способами, что и требовалось.

Определение 10.4. Пусть даны n элементов и $1 \le k \le n$. Всевозможные наборы из n элементов по k элементов, отличающиеся друг от друга лишь составом элементов, а не их порядком, называются *k-сочетаниями* из n элементов.

Теорема 10.4. Если C_n^k — общее число k-сочетаний из n элементов, то $C_n^k = \frac{n!}{k!(n-k)!}$.

Доказательство. В теореме 10.1. мы определили, что $\mathrm{A_n^k} = n(n-1)(n-2)\dots(n-k+1)$. Посчитаем общее число -размещений другим способом, нежели в теореме 10.1. Возьмем любое k-сочетание из элементов. Переставляя всевозможными способами элементы в этом k-сочетании, согласно теореме 10.2., получим число -размещений без повторений, ровное $k!$ Так как -сочетаний можно выбрать $\mathrm{C_n^k}$ способами, то по правилу произведения получаем $\mathrm{A_n^k} = \mathrm{C_n^k}.k!$. Итак, имеем равенство:

$n(n-1)(n-2)\dots(n-k+1) = C_n^k \cdot k!$. Отсюда получаем:

$$C_n^k = \frac{n(n-1)(n-2)\dots(n-k+1)}{k!} = \frac{n(n-1)(n-2)\dots(n-k+1)(n-k)(n-k-1)\dots 2\cdot 1}{k!\,(n-k)(n-k-1)\dots 2\cdot 1} = \frac{n!}{k!\,(n-k)!}$$

Числа C_n^kполучили название *биноминальных коэффициентов.* Это название происходит от формулы бинома Ньютона.

Теорема 10.5. Для любых чисел a и b и любого натурального n имеет место равенство $(a+b)^n = (a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-2}b^2 + \dots + C_n^{n-1}ab^{n-1} + b^n)$, которое носит название *бином Ньютона.*

Доказательство. Доказательство проведем индукцией по n. При $n = 1$ имеем $(a+b)^1 = a + b$, т.е. равенство справедливо.

Предположим, что равенство справедливо для $n-1$, т.е.

$(a+b)^{n-1} = (a^{n-1} + C_{n-1}^1 a^{n-2}b + C_{n-1}^2 a^{n-3}b^2 + \dots + C_{n-1}^{n-2}ab^{n-2} + b^{n-1})$, и докажем его справедливость для *n.*

Итак, имеем:

$$(a+b)^n = (a+b)(a+b)^{n-1} = (a+b)(a^{n-1} + C_{n-1}^1 a^{n-2}b + C_{n-1}^2 a^{n-3}b^2 + \dots + C_{n-1}^{n-2}ab^{n-2} + b^{n-1}) = a^n + C_{n-1}^1 a^{n-1}b + C_{n-1}^2 a^{n-2}b^2 + \dots + C_{n-1}^{n-2}a^2b^{n-2} + ab^{n-1} + a^{n-1}b + C_{n-1}^1 a^{n-2}b^2 + C_{n-1}^2 a^{n-3}b^3 + \dots + C_{n-1}^{n-2}ab^{n-1} + b^n = a^n + (C_{n-1}^1 + 1)a^{n-1}b + (C_{n-1}^2 + C_{n-1}^1)a^{n-2}b^2 + (C_{n-1}^3 + C_{n-1}^2)a^{n-3}b^3 + \dots + (C_{n-1}^{n-2} + C_{n-1}^{n-3})a^2b^{n-2} + (1 + C_{n-1}^{n-2})ab^{n-1} + b^n$$

Теперь осталось показать, что $(C_{n-1}^1 + 1) = C_n^1$, $(1 + C_{n-1}^{n-2}) = C_n^{n-1}$, а для остальных коэффициентов при произведениях вида $a^{n-k}b^k$ имеем равенство $C_{n-1}^k + C_{n-1}^{k-1} = \mathrm{C_n^k}$.

Итак, докажем эти равенства: $C_{n-1}^1 + 1 = \frac{(n-1)!}{1!(n-2)!} + 1 = \frac{(n-1)!+(n-2)!}{1!(n-2)!} = \frac{(n-2)!(n-1+1)}{1!(n-2)!} = \frac{(n-2)!n}{1!(n-2)!} = \frac{(n-2)!n(n-1)}{1!(n-2)!(n-1)} = \frac{n!}{1!(n-1)!} = C_n^1$. Аналогично, $(1 + C_{n-1}^{n-2}) = C_n^{n-1}$.

Наконец, $C_{n-1}^k + C_{n-1}^{k-1} = \frac{(n-1)!}{k!(n-k-1)!} + \frac{(n-1)!}{(k-1)!(n-k)!} = \frac{(n-1)!(n-k)+(n-1)!k}{k!(n-k)!} = \frac{(n-1)!(n-k+k)}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = \mathrm{C_n^k}$.

В качестве приложений полученных формул (а также методов их доказательства) рассмотрим ряд примеров, играющих важную роль в дискретной математике.

Пример 10.1. Пусть $\boldsymbol{M}$ — конечное множество, состоящее из *n* элементов. Тогда мощностное множество $\boldsymbol{P(M)}$ состоит из 2^n элементов.

Множество $\boldsymbol{P(M)}$ состоит из пустого множества $\emptyset$, одноэлементных подмножеств из $\boldsymbol{M}$, двухэлементных подмножеств из $\boldsymbol{M}$ … $(n-1)$-элементных подмножеств и самого множества $\boldsymbol{M}$. Одноэлементных подмножеств будет C_n^1, двухэлементных будет C_n^2,…, $(n-1)$-элементных множеств будет C_n^{n-1}. В таком случае $|\boldsymbol{P(M)}| = 1 + C_n^1 + C_n^2 + C_n^3 + \dots + C_n^{n-1} + 1 = (1+1)^n = 2^n$.

Итак, для конечного множества $\boldsymbol{M}$ имеем $|\boldsymbol{P}(\boldsymbol{M})| = 2^{|\boldsymbol{M}|}$. Отсюда ясен смысл обозначения $|\boldsymbol{P}(\boldsymbol{M})| = 2^{|\boldsymbol{M}|}$ для бесконечного множества $\boldsymbol{M}$, которое было введено в конце предыдущего параграфа.

Пример 10.2. Пусть $\boldsymbol{A_1}, \boldsymbol{A_2}, \ldots, \boldsymbol{A_n}$ конечные множества. Тогда мощность декартова произведения этих множеств равна произведению мощностей сомножителей, т.е. $|\boldsymbol{A_1}\text{x}\boldsymbol{A_2}\text{x}\ldots\text{x}\boldsymbol{A_n}| = |\boldsymbol{A_1}||\boldsymbol{A_2}| \ldots |\boldsymbol{A_n}|$.

Любой элемент из $\boldsymbol{A_1}\text{x}\boldsymbol{A_2}\text{x}\ldots\text{x}\boldsymbol{A_n}$ — это есть n-ка вида $< a_1, a_2, \ldots, a_n >$, где $a_i \in \boldsymbol{A_i}$, $i = 1, 2, \ldots, n$.

Элемент a_1 из множества $\boldsymbol{A_1}$ можно выбрать n_1 способом, а элемент a_2 из множества $\boldsymbol{A_2}$ — n_2 способами, где $n_1 = |\boldsymbol{A_1}|$, $n_2 = |\boldsymbol{A_2}|$. Тогда пару (a_1, a_2) можно выбрать $n_1 n_2$ способами. Элемент a_3 можно выбрать n_3 способами, где $n_3 = |\boldsymbol{A_3}|$. В таком случае тройку (a_1, a_2, a_3) можно выбрать $n_1 n_2 n_3$ способами. Продолжая эти рассуждения, получим, что все n-ки $< a_1, a_2, \ldots, a_n >$ можно выбрать $|\boldsymbol{A_1}||\boldsymbol{A_2}| \ldots |\boldsymbol{A_n}|$ способами, т.е. $|\boldsymbol{A_1}\text{x}\boldsymbol{A_2}\text{x}\ldots\text{x}\boldsymbol{A_n}| = |\boldsymbol{A_1}||\boldsymbol{A_2}| \ldots |\boldsymbol{A_n}|$.

Пример 10.3. Назовем *булевым вектором* длины n любой упорядоченный набор из нулей и единиц. Если $\boldsymbol{\mathcal{A}_n}$ — множество всех булевых векторов длины n, то $|\boldsymbol{\mathcal{A}_n}| = 2^n$.

Из определения легко видеть, что любой булев вектор длины n — это элемент декартовой степени n множества $\{0,1\}$. В таком случае, $|\boldsymbol{\mathcal{A}_n}| = \{0,1\}\text{x}\{0,1\}\text{x}\ldots\text{x}\{0,1\}$, где сомножители берутся n раз. Согласно предыдущему примеру, $|\boldsymbol{\mathcal{A}_n}| = |\{0,1\}|\text{x}|\{0,1\}|\text{x}\ldots\text{x}|\{0,1\}| = 2 \cdot 2 \cdot \ldots \cdot 2 = 2^n$.

Пример 10.4. В §3 мы ввели понятие булевой матрицы размера $m\text{x}n$. Пусть $\text{M}_{\boldsymbol{m,n}}$ — множество всех булевых матриц размера $m\text{x}n$, т.е. матриц размера $m\text{x}n$, состоящих из нулей и единиц. Пусть $\boldsymbol{X}, \boldsymbol{Y}$ — конечные множества, состоящие из m и n элементов соответственно. В том же §3 показано, что существует биекция между множеством $\text{M}_{\boldsymbol{m,n}}$ и множеством всех бинарных отношений между $\boldsymbol{X}$ и $\boldsymbol{Y}$. В то же время бинарных отношений между элементами множеств $\boldsymbol{X}$ и $\boldsymbol{Y}$, по определению, столько, сколько подмножеств в декартовом произведении $\boldsymbol{X}\text{x}\boldsymbol{Y}$. Значит, количество булевых матриц размера $m\text{x}n$ равно числу подмножеств множества $\boldsymbol{X}\text{x}\boldsymbol{Y}$, т.е. согласно примеру 10.3, равно $2^{|\boldsymbol{X}\text{x}\boldsymbol{Y}|} = 2^{mn}$.

Таким образом получили, что $|\text{M}_{\boldsymbol{m,n}}| = 2^{mn}$. Попутно мы установили, что если $\boldsymbol{X}$, $\boldsymbol{Y}$ — конечные множества мощности m и n, соответственно, то число бинарных отношений между элементами множеств $\boldsymbol{X}$ и $\boldsymbol{Y}$ равно 2^{mn}. Хотя равенство $|\text{M}_{\boldsymbol{m,n}}| = 2^{mn}$ можно было получить и без этого факта. Действительно, любую булеву матрицу размера $m\text{x}n$ можно представить в виде булева вектора длины mn, выписав друг за другом строки матрицы. И очевидно, что количество булевых матриц размера $m\text{x}n$ будет равно количеству булевых векторов длины mn. А количество таких векторов, согласно примеру 10.12, равно 2^{mn}.

Пример 10.5. Булевой функцией f от n переменных называется функция, отображающая n-ю декартову степень множества $\{0,1\}$ во множество $\{0,1\}$, т.е. $f: \{0,1\}\text{x}\{0,1\}\text{x}\ldots\text{x}\{0,1\} \to \{0,1\}$. Другими словами, функция f отображает множество $\boldsymbol{A_n}$ во множество $\{0,1\}$. Пусть $\boldsymbol{F_n}$ — множество всех булевых функций от n переменных, а $\boldsymbol{F}$ — множество всех булевых функций. Очевидно, что $\boldsymbol{F} = \bigcup_{n=1}^{\infty} \boldsymbol{F_n}$.

Пусть $f(x_1, x_2, \ldots, x_n)$ — булева функция от n переменных. Зафиксируем какую-либо нумерацию всех булевых векторов длины n, которых будет 2^n. Пусть

$a_1, a_2, \ldots, a_{2^n}$ — все булевы вектора длины n. Обычно их записывают в порядке возрастания относительно лексикографического порядка, хотя в данном случае это несущественно. Поставим в соответствие функции f булев вектор длины 2^n по правилу $f \rightarrow < f(a_1), f(a_2), \ldots, f(a_{2^n}) >$. Если две булевы функции f и φ различны, то $f(a_i) \neq \varphi(a_i)$ хотя бы для одного индекса i, а значит, соответствующие им булевы вектора $< f(a_1), f(a_2), \ldots, f(a_{2^n}) >$ и $< \varphi(a_1), \varphi(a_2), \ldots, \varphi(a_{2^n}) >$ будут различны.

Следовательно, построенное отображение между булевыми функциями от n переменных и булевыми векторами длины 2^n будет инъективным. Очевидно, что оно сюръективно, а значит, биективно. Итак, количество булевых функций от n переменных равно количеству булевых векторов длины 2^n, т.е. согласно примеру 10.3, равно 2^{2^n}. Итак, $|\boldsymbol{F_n}| = 2^{2^n}$, значит, $\boldsymbol{F}$ — счетное множество как объединение счетного числа конечных множеств.

Литература

1. Биркгоф Г., Барти Т. Современная прикладная алгебра /пер. с англ. Ю.И. Манина. — М.: Мир, 1976. — 400 с.
2. Кузнецов О.П., Адельсон-Вельский Г.М. Дискретная математика для инженера. — М.: Энергия, 1980. — 344 с.
3. Нефедов В.Н., Осипова В.А. Курс дискретной математики. — М.: Наука, 1992. — 264 с.
4. Логинов Б.М. Введение в дискретную математику. — Калуга, 1998. — 424с.
5. Ерусалимский Я.М. Дискретная математика. — М.: Вузовская книга, 2000. — 280 с.
6. Лавров И.А., Максимова Л.Л. Задачи по теории множеств, математический логике и теории алгоритмов.— М.: Физматгиз, 2004.