

Глава I. Введение в алгебру

§ 1. Множества и отображения

Б.М.Верников

Уральский федеральный университет,
Институт математики и компьютерных наук,
кафедра алгебры и дискретной математики

Множество — исходное, неопределяемое понятие. Оно лежит в основе всех математических построений. Точного определения понятия множества не существует. Точнее говоря, множества определяются аксиоматически. Иными словами, приводится список некоторых утверждений, принимаемых без доказательства и называемых *аксиомами теории множеств*, и говорится, что множество — это произвольный объект, удовлетворяющий этим утверждениям. Этот подход непригоден для первоначального знакомства с предметом и выходит за рамки нашего курса. Но для того, чтобы иметь дело с множествами, надо иметь какое-то представление о том, что мы имеем в виду, употребляя этот термин. Это представление дает следующее

Как бы «определение»

Под словом *множество* понимается любая совокупность объектов любой природы, выделенных по некоторому признаку и рассматриваемых как единое целое. Упомянутые объекты называются *элементами множества*. При этом говорят, что элемент *принадлежит* множеству, а множество *содержит* элемент. Тот факт, что элемент x принадлежит множеству S , обозначается через $x \in S$.

Допускается ситуация, когда множество не содержит ни одного элемента. (При аксиоматическом построении теории множеств существование такого множества принимается в качестве одной из аксиом.)

Определение

Множество, которое не содержит ни одного элемента, называется *пустым* и обозначается символом \emptyset .

Введем еще одно очень важное понятие.

Определение

Говорят, что множество A *содержится* в множестве B или является *подмножеством* множества B , если всякий элемент множества A является элементом множества B . Этот факт обозначается через $A \subseteq B$.

Очевидно, что $\emptyset \subseteq A$ и $A \subseteq A$ для всякого множества A .

Определение

Если $A \subseteq B$ и $A \neq B$, то A называется *собственным подмножеством* множества B . В тех случаях, когда нам будет важно подчеркнуть, что подмножество A множества B является его собственным подмножеством, мы будем писать $A \subset B$.

Определение

Говорят, что множества A и B *равны*, если всякий элемент множества A является элементом множества B , а всякий элемент множества B является элементом множества A . Тот факт, что множества A и B равны, будем обозначать обычным образом: $A = B$.

Сравнивая два последних определения, получаем следующее очевидное

Наблюдение о равенстве множеств

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

При всей своей очевидности, это наблюдение принципиально важно, так как на нем основано несметное количество доказательств математических фактов.

Обозначения

Зафиксируем общепринятые обозначения для нескольких часто возникающих числовых множеств:

\mathbb{N} — множество всех натуральных чисел;

\mathbb{Z} — множество всех целых чисел;

\mathbb{Q} — множество всех рациональных чисел;

\mathbb{R} — множество всех действительных чисел.

Если множество S конечно и состоит из элементов x_1, x_2, \dots, x_n , то этот факт записывается в виде $S = \{x_1, x_2, \dots, x_n\}$. Иногда, если элементов в множестве много, но принадлежность элемента множеству подчиняется некоторой закономерности, ясной из контекста, при задании списка элементов, из которых состоит множество, используется многоточие. Например, $S = \{1, 2, 3, \dots, 60\}$ — множество всех натуральных чисел от 1 до 60.

Ясно, что задать бесконечное множество перечислением всех его элементов невозможно в принципе. В этом случае чаще всего используется следующий способ задания множества. Пусть S — некоторое множество, а \mathcal{P} — свойство, которым могут как обладать, так и не обладать элементы из S . Тогда через

$$\{x \in S \mid x \text{ обладает свойством } \mathcal{P}\}$$

обозначается множество, элементами которого являются элементы множества S , обладающие свойством \mathcal{P} , и только они. Например:

$$A = \{x \in \mathbb{Z} \mid x = 2k + 1 \text{ для некоторого } k \in \mathbb{Z}\},$$

$$B = \{x \in \mathbb{R} \mid x \geq 0\},$$

$$C = \{x \in \mathbb{R} \mid x = \frac{m}{n} \text{ для некоторых } m, n \in \mathbb{Z}, n \neq 0\},$$

$$D = \{x \in \mathbb{R} \mid x^2 + 1 = 0\}.$$

Очевидно, что A — множество всех нечетных целых чисел, B — множество всех неотрицательных действительных чисел, $C = \mathbb{Q}$, а $D = \emptyset$.

Введем несколько стандартных операций над множествами.

Определения

Объединением множеств A и B называется множество, состоящее из всех элементов, которые принадлежат либо A , либо B (включая те, которые принадлежат и A , и B). Объединение множеств A и B обозначается через $A \cup B$. **Пересечением** множеств A и B называется множество, состоящее из всех элементов, которые принадлежат одновременно и A и B . Пересечение множеств A и B обозначается через $A \cap B$. **Разностью** множеств A и B называется множество, состоящее из всех элементов, которые принадлежат A , но не принадлежат B . Разность множеств A и B обозначается через $A \setminus B$ (читается как « A без B »). **Дополнением** множества A называется множество, состоящее из всех элементов, не принадлежащих A . Дополнение множества A обозначается через \bar{A} . Четыре перечисленные операции часто объединяют термином **теоретико-множественные операции**.

Иногда в число теоретико-множественных операций включают также операцию **симметрической разности** множеств A и B , которая обозначается через $A \triangle B$ и определяется равенством $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Но эта операция большого самостоятельного интереса не представляет. Поэтому далее мы о ней упоминать не будем.

Операцию дополнения множества можно рассматривать как частный случай операции разности множеств. Для этого требуется ввести одно новое понятие.

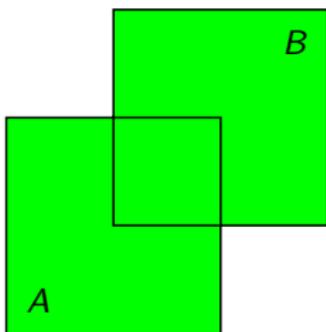
Определение

Универсальным множеством для семейства множеств $\{S_i \mid i \in I\}$ называется множество U такое, что $S_i \subseteq U$ для всякого $i \in I$.

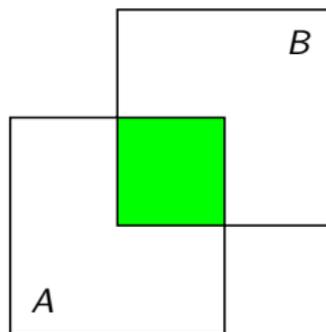
Понятие универсального множества относительно: одно и то же множество может быть универсальным для одного семейства множеств и не быть таковым для другого семейства.

Ясно, что если U — универсальное множество для некоторого семейства множеств, в которое входит множество A , то $\bar{A} = U \setminus A$.

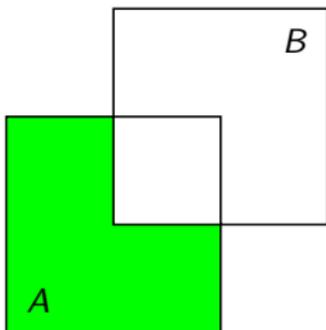
На рис. 1 (см. следующий слайд) приведена графическая иллюстрация теоретико-множественных операций.



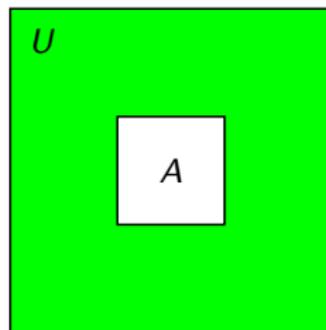
а) $A \cup B$



б) $A \cap B$



в) $A \setminus B$



г) \bar{A}

Рис. 1. Теоретико-множественные операции

Перечислим основные свойства теоретико-множественных операций. Если A , B и C — произвольные множества, то:

- 1) $A \cup B = B \cup A$ и $A \cap B = B \cap A$ (*коммутативность* объединения и пересечения);
- 2) $(A \cup B) \cup C = A \cup (B \cup C)$ и $(A \cap B) \cap C = A \cap (B \cap C)$ (*ассоциативность* объединения и пересечения);
- 3) $A \cup A = A$ и $A \cap A = A$ (*идемпотентность* объединения и пересечения);
- 4) $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$ и $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$ (*дистрибутивность* пересечения относительно объединения и объединения относительно пересечения);
- 5) $(A \cup B) \cap A = A$ и $(A \cap B) \cup A = A$ (*законы поглощения*);
- 6) $\overline{\overline{A}} = A$ (*закон снятия двойного отрицания*);
- 7) $\overline{A \cup B} = \overline{A} \cap \overline{B}$ и $\overline{A \cap B} = \overline{A} \cup \overline{B}$ (*законы де Моргана*);
- 8) $A \cup \overline{A} = U$ и $A \cap \overline{A} = \emptyset$;
- 9) $A \setminus B = A \cap \overline{B}$;
- 10) $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$ и $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;
- 11) $(A \cup B) \setminus C = (A \setminus C) \cup (B \setminus C)$ и $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$.

Доказательство свойств теоретико-множественных операций (на примере одного из них)

Все перечисленные на предыдущем слайде свойства операций над множествами легко проверяются исходя из определений этих операций. Продемонстрируем это на примере дистрибутивности объединения относительно пересечения. Требуется доказать, что $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$. Согласно наблюдению о равенстве множеств, требуется убедиться в том, что $(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C)$ и $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$. Проверим сначала первое включение. Пусть $x \in (A \cap B) \cup C$. Это означает, что либо $x \in A \cap B$, либо $x \in C$. Если $x \in A \cap B$, то $x \in A$ и $x \in B$. Но тогда $x \in A \cup C$ и $x \in B \cup C$, и потому $x \in (A \cup C) \cap (B \cup C)$. Если же $x \in C$, то вновь получаем, что $x \in A \cup C$ и $x \in B \cup C$, и потому $x \in (A \cup C) \cap (B \cup C)$. Таким образом, последнее включение выполнено в любом случае. Включение $(A \cap B) \cup C \subseteq (A \cup C) \cap (B \cup C)$ доказано. Докажем противоположное включение. Пусть $x \in (A \cup C) \cap (B \cup C)$. Это означает, что $x \in A \cup C$ и $x \in B \cup C$. Итак, во-первых, x принадлежит либо A , либо C , а во вторых, x принадлежит либо B , либо C . Если $x \in C$, то $x \in (A \cap B) \cup C$. Если же $x \notin C$, то, в силу сказанного, x принадлежит как A , так и B . Но тогда $x \in A \cap B$, и потому $x \in (A \cap B) \cup C$. Итак, последнее включение имеет место в любом случае. Включение $(A \cup C) \cap (B \cup C) \subseteq (A \cap B) \cup C$ доказано. □

Объединение и пересечение семейств множеств (определения)

Операции объединения и пересечения множеств можно определить не только для двух множеств, но и для произвольного (возможно, бесконечного) семейства множеств.

Определение

Пусть $\{S_i \mid i \in I\}$ — произвольное семейство множеств. *Объединением* семейства $\{S_i \mid i \in I\}$ называется множество

$$\bigcup_{i \in I} S_i = \{x \mid x \in S_i \text{ для некоторого } i \in I\},$$

а *пересечением* этого семейства — множество

$$\bigcap_{i \in I} S_i = \{x \mid x \in S_i \text{ для всякого } i \in I\}.$$

Если семейство множеств $\{S_i \mid i \in I\}$ конечно и состоит из множеств S_1, S_2, \dots, S_k , то наряду с обозначением $\bigcup_{i \in I} S_i$ могут использоваться

обозначения $\bigcup_{i=1}^k S_i$ или $S_1 \cup S_2 \cup \dots \cup S_k$, а наряду с обозначением $\bigcap_{i \in I} S_i$ —

обозначения $\bigcap_{i=1}^k S_i$ или $S_1 \cap S_2 \cap \dots \cap S_k$. Поскольку операции объединения и пересечения множеств ассоциативны, в выражениях вида $S_1 \cup S_2 \cup \dots \cup S_k$ и $S_1 \cap S_2 \cap \dots \cap S_k$ скобок можно не ставить.

Объединение и пересечение семейств множеств обладает аналогами всех основных свойств операций объединения и пересечения двух множеств. Укажем наиболее важные из них. Если $\{A_i \mid i \in I\}$ — произвольное семейство множеств, а B — произвольное множество, то:

- 1) $(\bigcup_{i \in I} A_i) \cap B = \bigcup_{i \in I} (A_i \cap B)$ и $(\bigcap_{i \in I} A_i) \cup B = \bigcap_{i \in I} (A_i \cup B)$ (*обобщенная дистрибутивность* пересечения относительно объединения и объединения относительно пересечения);
- 2) $\overline{\bigcup_{i \in I} A_i} = \bigcap_{i \in I} \overline{A_i}$ и $\overline{\bigcap_{i \in I} A_i} = \bigcup_{i \in I} \overline{A_i}$ (*обобщенные законы де Моргана*);
- 3) $B \setminus (\bigcup_{i \in I} A_i) = \bigcap_{i \in I} (B \setminus A_i)$ и $B \setminus (\bigcap_{i \in I} A_i) = \bigcup_{i \in I} (B \setminus A_i)$;
- 4) $(\bigcup_{i \in I} A_i) \setminus B = \bigcup_{i \in I} (A_i \setminus B)$ и $(\bigcap_{i \in I} A_i) \setminus B = \bigcap_{i \in I} (A_i \setminus B)$.

Доказываются эти свойства с помощью простых соображений, основанных на определениях операций, подобно тому, как доказываются свойства объединения и пересечения двух множеств.

Определение

Прямым (или **декартовым**) **произведением** множеств S_1, S_2, \dots, S_n называется множество всевозможных упорядоченных n -ок вида (x_1, x_2, \dots, x_n) , где $x_1 \in S_1, x_2 \in S_2, \dots, x_n \in S_n$. Прямое произведение множеств S_1, S_2, \dots, S_n обозначается через $S_1 \times S_2 \times \dots \times S_n$ или $\prod_{i=1}^n S_i$.

Множество $\underbrace{S \times S \times \dots \times S}_{n \text{ раз}}$ называется **n -й декартовой степенью**

множества S и обозначается через S^n . В частности, если $n = 2$, то множество $S^2 = S \times S$ называется **декартовым квадратом** множества S . Кроме того, будем считать, что $S^1 = S$.

Например, если $A = \{0, 1\}$, а $B = \{x, y, z\}$, то

$$A \times B = \{(0, x), (0, y), (0, z), (1, x), (1, y), (1, z)\},$$

а если $S = \{1, 2, 3\}$, то

$$S^2 = \{(1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3), (3, 1), (3, 2), (3, 3)\}.$$

Укажем несколько свойств, которыми обладает прямое произведение двух множеств. Для любых множеств A , B и C справедливы равенства:

$$(A \cup B) \times C = (A \times C) \cup (B \times C), \quad (A \cap B) \times C = (A \times C) \cap (B \times C), \\ A \times (B \cup C) = (A \times B) \cup (A \times C), \quad A \times (B \cap C) = (A \times B) \cap (A \times C)$$

(прямое произведение *дистрибутивно относительно как объединения, так и пересечения, причем как слева, так и справа*).

Докажем в качестве примера первое свойство, остальные проверяются аналогично. Пусть $x \in (A \cup B) \times C$. Тогда $x = (u, v)$, где $u \in A \cup B$, а $v \in C$. Получаем, что либо $u \in A$, либо $u \in B$. Поэтому $x = (u, v)$ лежит либо в $A \times C$, либо в $B \times C$. Следовательно, $x \in (A \times C) \cup (B \times C)$.

Обратно, пусть $x \in (A \times C) \cup (B \times C)$. Тогда либо $x \in A \times C$, либо $x \in B \times C$. В первом случае $x = (u, v)$, где $u \in A$, а $v \in C$, а во втором $x = (u, v)$, где $u \in B$, а $v \in C$. Иными словами, $x = (u, v)$, где u лежит либо в A , либо в B , а $v \in C$. Это означает, что $x = (u, v) \in (A \cup B) \times C$.

Свойство доказано. □

Прямое произведение множеств не обладает рядом «привычных» свойств. Оно не коммутативно. В самом деле, если $A = \{a\}$, а $B = \{b\}$, то $A \times B = \{(a, b)\}$, а $B \times A = \{(b, a)\}$. Кроме того, оно не ассоциативно. В самом деле, если $A = \{a\}$, $B = \{b\}$, а $C = \{c\}$, то $(A \times B) \times C$ состоит из пары $((a, b), c)$, а $A \times (B \times C)$ — из пары $(a, (b, c))$.

Введем еще одно понятие, появляющееся практически во всех разделах математики и играющее не менее важную роль, чем понятие множества. Его можно двумя различными (разумеется, эквивалентными) способами.

«Теоретико-множественное» определение

Отображением из множества A в множество B называется подмножество α множества $A \times B$ со следующим свойством: для любого $x \in A$ существует, и притом только одно, $y \in B$ такое, что $(x, y) \in \alpha$. Обычно вместо $(x, y) \in \alpha$ пишут $y = \alpha(x)$.

«Функциональное» определение

Отображением α из множества A в множество B называется правило, которое всякому элементу множества $x \in A$ некоторым однозначно определенным образом ставит в соответствие элемент $\alpha(x) \in B$.

- Функциональное определение показывает, что отображение — это аналог понятия функции.

Определение

Если α — отображение из A в B и $x \in A$, то $\alpha(x)$ называется *образом* элемента x , а x — *прообразом* элемента $\alpha(x)$ при отображении α .

Отметим, что образ всякого элемента $x \in A$ существует и определен однозначно, в то время, как прообразов y элемента $y \in B$ может быть любое число (в том числе может не быть ни одного).

Обозначения

Тот факт, что α — отображение из A в B , обозначается следующим образом: $\alpha: A \rightarrow B$. Если $X \subseteq A$, то через $\alpha(X)$ обозначается множество всех элементов вида $\alpha(x)$, где x пробегает X .

Определение

Если α — отображение из A в B , а $X \subseteq A$, то *ограничением* α на X называется отображение из X в B , обозначаемое через $\alpha|_X$ и определяемое правилом: $\alpha|_X(x) = \alpha(x)$ для всякого $x \in X$.

Введем в рассмотрение три важных частных случая понятия отображения.

Определения

Отображение f из A в B называется:

- **взаимно однозначным** отображением (а также **инъективным** отображением или **инъекцией**), если для любых $x, y \in A$ из того, что $x \neq y$, вытекает, что $f(x) \neq f(y)$ (т. е. образы любых двух различных элементов различны);
- отображением A **на** B (а также **сюръективным** отображением или **сюръекцией**), если для любого $y \in B$ существует $x \in A$ такой, что $f(x) = y$ (т. е. каждый элемент из B имеет прообраз);
- **биективным** отображением (а также **биекцией** или **взаимно однозначным соответствием** между A и B), если f инъективно и сюръективно.

Отметим, что произвольное отображение $f: A \rightarrow B$ является сюръективным отображением из A на $f(A)$.

Определение

Пусть f — отображение из A в B , а g — отображение из B в C .

Произведением (а также *композицией* или *суперпозицией*) отображений f и g называется отображение h из A в C , задаваемое правилом $h(x) = g(f(x))$ для всякого $x \in A$. Произведение f и g обозначается через fg .

Иллюстрацией к этому определению служит рис. 2.

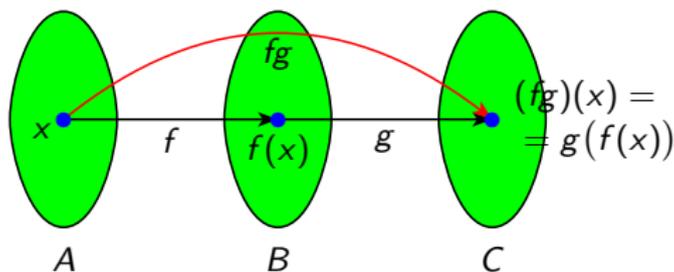


Рис. 2. Произведение отображений

Легко проверяется, что произведение отображений *ассоциативно*, т. е. если f — отображение из A в B , g — отображение из B в C , а h — отображение из C в D , то $(fg)h = f(gh)$ (см. рис. 3, на котором действие отображения $(fg)h$ изображено красными стрелками, а действие отображения $f(gh)$ — синими).

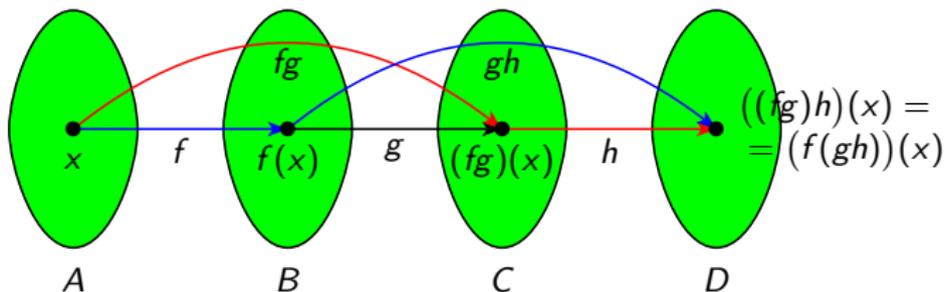


Рис. 3. Ассоциативность произведения отображений

Определение

Отображение f из множества A в себя, задаваемое правилом $f(x) = x$ для всякого $x \in A$, называется **тождественным**. Тожественное отображение будем обозначать буквой ε . Пусть f — отображение из A в B .

Отображение g из $f(A)$ в A называется **обратным к f** , если отображение fg является тождественным, т. е. если $g(f(x)) = x$ для всякого $x \in A$.

Отображение, обратное к f , обозначается через f^{-1} .

Отображение f^{-1} существует далеко не для всякого отображения f . А именно, справедлив следующий

Критерий существования обратного отображения

Пусть f — отображение из A в B . Отображение, обратное к f , существует тогда и только тогда, когда f — инъекция.

Доказательство этого утверждения дано на следующем слайде.

Доказательство. Необходимость. Предположим, что отображение, обратное к f , существует. Если при этом $f(x_1) = f(x_2)$ для некоторых $x_1, x_2 \in A$, то

$$\begin{aligned}x_1 &= \varepsilon(x_1) = (ff^{-1})(x_1) = f^{-1}(f(x_1)) = \\ &= f^{-1}(f(x_2)) = (ff^{-1})(x_2) = \varepsilon(x_2) = x_2.\end{aligned}$$

Таким образом, $x_1 = x_2$, т. е. отображение f инъективно.

Достаточность. Для всякого $y \in f(A)$ существует $x \in A$ такой, что $f(x) = y$. Поскольку по условию отображение f инъективно, элемент x с указанным свойством определен однозначно. Это позволяет определить отображения g из $f(A)$ в A правилом $g(y) = x$. При этом, если $x \in A$, то $(fg)(x) = g(f(x)) = g(y) = x$, т. е. $fg = \varepsilon$. Следовательно, $g = f^{-1}$, т. е. отображение f^{-1} существует. □

Свойства обратного отображения

Пусть A , B и C — множества, f — отображение из A в B , а g — отображение из B в C .

- 1) Если существует отображение f^{-1} , то существует отображение $(f^{-1})^{-1}$ и $(f^{-1})^{-1} = f$.
- 2) Если существуют отображения f^{-1} и g^{-1} , то существует отображение $(fg)^{-1}$ и $(fg)^{-1} = g^{-1}f^{-1}$.

Доказательство. Свойство 1) легко вытекает из определения обратного отображения. Докажем свойство 2). Пусть $x_1, x_2 \in A$. Из критерия существования обратного отображения вытекает, что отображения f и g инъективны. Поэтому если $(fg)(x_1) = (fg)(x_2)$, т.е. $g(f(x_1)) = g(f(x_2))$, то $f(x_1) = f(x_2)$, а значит и $x_1 = x_2$. В силу критерия существования обратного отображения получаем, что отображение $(fg)^{-1}$ существует. Пусть $x \in A$, $y = f(x)$ и $z = g(y)$. Тогда

$$\begin{aligned} ((fg) \cdot (g^{-1}f^{-1}))(x) &= (g^{-1}f^{-1})((fg)(x)) = (g^{-1}f^{-1})(g(f(x))) = \\ &= (g^{-1}f^{-1})(g(y)) = (g^{-1}f^{-1})(z) = f^{-1}(g^{-1}(z)) = \\ &= f^{-1}(y) = x. \end{aligned}$$

Следовательно, $(fg) \cdot (g^{-1}f^{-1}) = \varepsilon$, т.е. $(fg)^{-1} = g^{-1}f^{-1}$.



Определение

Мощностью конечного множества S называется число элементов этого множества. Мощность конечного множества S обозначается через $|S|$.

Теорема о равномощности конечных множеств

Мощности конечных множеств A и B равны тогда и только тогда, когда существует биективное отображение из A на B .

Доказательство. Необходимость. Предположим, что $|A| = |B| = n$. Пусть $A = \{x_1, x_2, \dots, x_n\}$, а $B = \{y_1, y_2, \dots, y_n\}$. Определим отображение f из A в B правилом $f(x_i) = y_i$ для всякого $i = 1, 2, \dots, n$. Очевидно, что f — биекция из A на B .

Достаточность. Предположим, что существует биекция f из A на B . В силу инъективности f образы различных элементов из A различны. Следовательно, $|B| \geq |A|$. С другой стороны, в силу сюръективности f каждый элемент из B является образом некоторого элемента из A , а образ любого элемента из A определен однозначно. Следовательно, $|B| \leq |A|$, и потому $|B| = |A|$. □

Теорема о равномощности конечных множеств «оправдывает» следующее

Определение

Множества A и B называются *равномощными*, если существует биективное отображение из A на B .

Для конечных множеств это определение тавтологично, но речь в нем идет о произвольных (в том числе бесконечных) множествах.

Предложение о мощности прямого произведения

Если S_1, S_2, \dots, S_n — конечные множества и $|S_i| = k_i$ для всех $i = 1, 2, \dots, n$, то $|S_1 \times S_2 \times \dots \times S_n| = k_1 k_2 \dots k_n$.

Доказательство проведем индукцией по n . При $n = 1$ доказываемое утверждение очевидно. Пусть теперь $n > 1$. Пусть $S_n = \{x_1, x_2, \dots, x_{k_n}\}$. Для всякого $i = 1, 2, \dots, k_n$ обозначим через T_i множество всех упорядоченных n -ок из множества $S_1 \times S_2 \times \dots \times S_n$, у которых последняя компонента n -ки равна x_i . Ясно, что $S_1 \times S_2 \times \dots \times S_n = T_1 \cup T_2 \cup \dots \cup T_{k_n}$ и множества T_1, T_2, \dots, T_{k_n} попарно пересекаются по пустому множеству. Следовательно, $|S_1 \times S_2 \times \dots \times S_n| = |T_1| + |T_2| + \dots + |T_{k_n}|$. Очевидно, что для всякого $i = 1, 2, \dots, k_n$ существует биекция из T_i в $S_1 \times S_2 \times \dots \times S_{n-1}$, которая упорядоченной n -ке $(y_1, y_2, \dots, y_{n-1}, x_i) \in T_i$ (где $y_i \in S_i$ для всех $i = 1, 2, \dots, n-1$) ставит в соответствие набор $(y_1, y_2, \dots, y_{n-1}) \in S_1 \times S_2 \times \dots \times S_{n-1}$. Следовательно, $|T_i| = |S_1 \times S_2 \times \dots \times S_{n-1}|$ для всякого $i = 1, 2, \dots, k_n$, и потому $|S_1 \times S_2 \times \dots \times S_n| = k_n \cdot |S_1 \times S_2 \times \dots \times S_{n-1}|$. По предположению индукции $|S_1 \times S_2 \times \dots \times S_{n-1}| = k_1 k_2 \dots k_{n-1}$. Следовательно, $|S_1 \times S_2 \times \dots \times S_n| = k_1 k_2 \dots k_{n-1} k_n$, что и требовалось доказать. □

Из предложения о мощности прямого произведения немедленно вытекает

Следствие о мощности декартовой степени

Если S — конечное множество и $|S| = k$, а n — натуральное число,
 $|S^n| = k^n$. □

Определение

Булеаном множества S называется множество всех подмножеств множества S . Булеан множества S обозначается по-разному: $\mathcal{B}(S)$, $\mathcal{P}(S)$, 2^S . Мы будем использовать первое из этих обозначений.

В табл. 1 указаны булеаны и мощности булеанов некоторых небольших множеств. Отметим, что, для всякого конечного множества S , мощность его булеана определяется, очевидно, не тем, из каких именно элементов состоит S , а только числом этих элементов, т. е. мощностью множества S .

Табл. 1. Булеаны некоторых множеств и их мощности

S	$\mathcal{B}(S)$	$ S $	$ \mathcal{B}(S) $
\emptyset	$\{\emptyset\}$	0	1
$\{1\}$	$\{\emptyset, \{1\}\}$	1	2
$\{1, 2\}$	$\{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$	2	4
$\{1, 2, 3\}$	$\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$	3	8

Как видно из табл. 1, если $n = 0, 1, 2, 3$, то булеан n -элементного множества состоит из 2^n элементов. Как мы увидим на следующем слайде, это верно при любом n .

Теорема о булеане конечного множества

Если S — конечное множество и $|S| = n$, то $|\mathcal{B}(S)| = 2^n$.

Доказательство. Если $S = \emptyset$, то $|S| = 0$ и, как мы видели выше, $|\mathcal{B}(S)| = 1$. Поскольку $2^0 = 1$, в этом случае требуемое равенство выполняется. Поэтому далее можно считать, что $S \neq \emptyset$. Положим $S = \{x_1, x_2, \dots, x_n\}$ и $B = \{0, 1\}$. В силу следствия о мощности декартовой степени, $|B^n| = 2^n$. Поэтому достаточно проверить, что $|\mathcal{B}(S)| = |B^n|$, т. е. что существует биекция из множества $\mathcal{B}(S)$ в множество B^n . Определим отображение φ из $\mathcal{B}(S)$ в B^n следующим образом: если $X \subseteq S$, то $\varphi(X) = (b_1, b_2, \dots, b_n)$, где

$$b_i = \begin{cases} 1, & \text{если } x_i \in X, \\ 0, & \text{если } x_i \notin X \end{cases}$$

для всех $i = 1, 2, \dots, n$. Пусть $S_1, S_2 \subseteq S$ и $S_1 \neq S_2$. Без ограничения общности можно считать, что $S_1 \setminus S_2 \neq \emptyset$, и потому $x_i \in S_1 \setminus S_2$ для некоторого i . Тогда i -й элемент в последовательности $\varphi(S_1)$ равен 1, а в последовательности $\varphi(S_2)$ — 0. Следовательно, $\varphi(S_1) \neq \varphi(S_2)$, и потому отображение φ инъективно. Далее, если $(b_1, b_2, \dots, b_n) \in B^n$, то, очевидно $(b_1, b_2, \dots, b_n) = \varphi(X)$, где $X = \{x_i \mid b_i = 1\} \subseteq S$. Это означает, что отображение φ сюръективно. Следовательно, оно биективно.