Глава I. Введение в алгебру

§ 1. Множества и отображения

Б.М.Верников

Уральский федеральный университет,

Институт естественных наук и математики,

кафедра алгебры и фундаментальной информатики

1.1. Множества и операции над ними

Множество — исходное, неопределяемое понятие. Оно лежит в основе всех математических построений. Точного определения понятия множества не существует. 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 $x \in S$.

Наивная и аксиоматическая теория множеств

Приведенное выше «определение» множества лежит в основе так называемой «*наивной теории множеств*». Она была общепринятой в математике до конца XIX — начала XX века, когда выяснилось, что в рамках этой теории возникают неразрешимые противоречия. Мы не будем углубляться в этот вопрос. Отметим только, что появление указанных противоречий связано с рассмотрением «очень больших» множеств, таких, например, как множество всех множеств.

Для того, чтобы избежать появления этих противоречий, понятие множества следует вводить аксиоматически. Это означает,что формулируется ряд аксиом и говорится, что множество — это то, что удовлетворяет этим аксиомам. При этом аксиомы формулируются так, чтобы избежать появления противоречий. Такой подход приводит к построению *аксиоматической теории множеств*, свободной от противоречий. Но эта теория далеко выходит за рамки нашего курса.

Мы будем исходить из «наивного» подхода к понятию множества. При этом в рамках нашего курса «слишком больших» множеств, приводящих к появлению неразрешимых противоречий, возникать не будет.

Пустое множество. Подмножество

Допускается ситуация, когда множество не содержит ни одного элемента.

Определение

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

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 $A \subseteq B$ (реже $B \supseteq A$).

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

Равенство множеств

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

Замечание 1.1[1]

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

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

[1] На протяжении всего курса утверждения нумеруются двумя числами, первое из которых означает номер параграфа, в котором появляется данное утверждение.

Собственное подмножество

Определение

Если $A \subseteq B$ и $A \neq B$, то говорят, что множество A *строго содержится* в множестве B или является *собственным подмножеством* множества B. В тех случаях, когда нам будет важно подчеркнуть, что подмножество A множества B является его собственным подмножеством, мы будем писать $A \subset B$ (реже $B \supset A$).

Стандартные числовые множества. Задание множества перечислением его элементов

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 $x_1, x_2, \ldots, x_n$, то этот факт записывается в виде $S = \{x_1, x_2, \ldots, x_n\}$. 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, $S = \{1, 2, 3, \ldots, 60\}$ — множество всех натуральных чисел от 1 до 60.

Задание множества с помощью характеристического свойства

Ясно, что задать бесконечное множество перечислением всех его элементов невозможно в принципе, да и для конечных множеств этот способ далеко не всегда удобен. Поэтому 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:

$$A = \{x \in \mathbb{Z} \mid x = 2k + 1 \text{ для некоторого } k \in \mathbb{Z}\},$$
$$B = \{x \in \mathbb{R} \mid x \geqslant 0\},$$
$$C = \{x \in \mathbb{R} \mid x = \frac{m}{n} \text{ для некоторых } m, n \in \mathbb{Z}, n \neq 0\},$$
$$D = \{x \in \mathbb{R} \mid x^2 + 1 = 0\}.$$

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

Теоретико-множественные операции

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 $\overline{A}$. 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 большого самостоятельного интереса она не представляет.

Универсальное множество

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

Определение

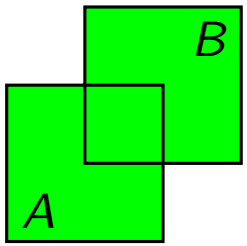
Универсальным множеством для семейства множеств $\{S_i \mid i \in I\}$ называется множество U такое, что $S_i \subseteq U$ для всякого $i \in I$.

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

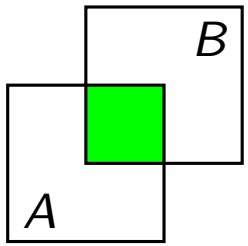
Ясно, что если U — универсальное множество для некоторого семейства множеств, в которое входит множество A, то $\overline{A} = U \setminus A$.

На рис. 1 (см. следующий слайд) приведена графическая иллюстрация теоретико-множественных операций. Результат операции закрашен зеленым цветом.

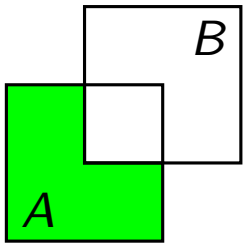
Графическая иллюстрация теоретико-множественных операций



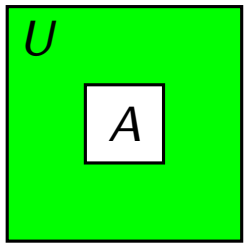
а) $A \cup B$



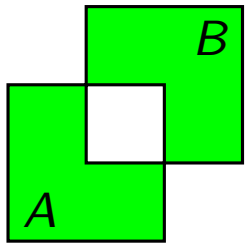
б) $A \cap B$



в) $A \setminus B$



г) $\overline{A}$



д) $A \triangle B$

Рис. 1. Теоретико-множественные операции

Свойства теоретико-множественных операций

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 $A \cap \overline{A} = \varnothing$;
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 $(A \cap B) \setminus C = (A \setminus C) \cap (B \setminus C)$.

Два последних свойства показывают, что разность множеств *дистрибутивна* относительно объединения и пересечения *справа* (свойство 11), но *не дистрибутивна слева* (свойство 10).

Сравнение теоретико-множественных операций с операциями над числами

Объединение и пересечение множеств по своим свойствам во многом, хотя и не во всем, аналогичны сложению и умножению чисел (обычно считается, что объединение — это аналог сложения, а пересечение — аналог умножения). В самом деле, объединение и пересечение, как и сложение и умножение, коммутативны и ассоциативны, дистрибутивность пересечения относительно объединения аналогична дистрибутивности умножения относительно сложения. С другой стороны, не имеют «числовых» аналогов дистрибутивность объединения относительно пересечения, идемпотентность объединения и пересечения, оба закона поглощения.

Порядок выполнения теоретико-множественных операций

Укажем еще одно важное отличие теоретико-множественных операций от операций над числами. Как известно, умножение имеет приоритет перед сложением. Поэтому в выражениях вида $xy + z$ скобок ставить не надо: сначала выполняется умножение, а потом — сложение. С теоретико-множественными операциями ситуация иная.

! *Объединение, пересечение и разность множеств равноправны* (*имеют равный приоритет*). Порядок их выполнения определяется только скобками.

Поэтому выражения вида $A \cup B \cap C$, $A \cap B \cup C$, $A \setminus B \cup C$ или $A \cap B \setminus C$ не имеют смысла. Чтобы они приобрели смысл, необходимо расставить скобки: например, $(A \cup B) \cap C$, $A \cap (B \cup C)$, $(A \setminus B) \cup C$ или $A \cap (B \setminus C)$.

То же самое относится к нескольким подряд идущим операциям разности множеств. Эта операция *не ассоциативна*, т. е. множества $(A \setminus B) \setminus C$ и $A \setminus (B \setminus C)$ в общем случае не равны. Например, если $A = B = C$, то $(A \setminus B) \setminus C = (A \setminus A) \setminus A = \varnothing \setminus A = \varnothing$, а $A \setminus (B \setminus C) = A \setminus (A \setminus A) = A \setminus \varnothing = A$. Поэтому выражение $A \setminus B \setminus C$ некорректно, а чтобы оно стало корректным, в нем надо расставить скобки.

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

Все перечисленные выше 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 замечанию 1.1 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. $\square$

Объединение и пересечение семейств множеств

Поскольку в выражениях вида $S_1 \cup S_2 \cup \cdots \cup S_n$ и $S_1 \cap S_2 \cap \cdots \cap S_n$ скобок можно не ставить, их часто для краткости записывают в виде $\bigcup\limits_{i=1}^{n} S_i$ и $\bigcap\limits_{i=1}^{n} S_i$ соответственно.

Часто приходится рассматривать объединение и пересечение бесконечного семейства множеств. Они определяются естественным образом: если $\{S_i \mid i \in I\}$ — произвольное (возможно, бесконечное) семейство множеств, то *объединением* этого семейства называется множество

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

а *пересечением* — множество

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

Прямое произведение множеств

Определение

Прямым (или *декартовым*) *произведением* множеств $S_1, S_2, \ldots, S_n$ называется множество всевозможных упорядоченных n-ок вида $(x_1, x_2, \ldots, x_n)$, где $x_1 \in S_1$, $x_2 \in S_2$, $\ldots$, $x_n \in S_n$. Прямое произведение множеств $S_1, S_2, \ldots, S_n$ обозначается через $S_1 \times S_2 \times \cdots \times S_n$ или $\prod\limits_{i=1}^{n} S_i$. Множество $\underbrace{S \times S \times \cdots \times S}_{n \text{ раз}}$ 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

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

а если $S = \{1, 2, 3\}$, то

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

Свойства прямого произведения (1)

Укажем несколько свойств, которыми обладает прямое произведение множеств. Для любых множеств A_1, A_2, …, A_n и B справедливы равенства:

$$(A_1 \cup A_2 \cup \cdots \cup A_n) \times B = (A_1 \times B) \cup (A_2 \times B) \cup \cdots \cup (A_n \times B),$$
$$(A_1 \cap A_2 \cap \cdots \cap A_n) \times B = (A_1 \times B) \cap (A_2 \times B) \cap \cdots \cap (A_n \times B),$$
$$B \times (A_1 \cup A_2 \cup \cdots \cup A_n) = (B \times A_1) \cup (B \times A_2) \cup \cdots \cup (B \times A_n),$$
$$B \times (A_1 \cap A_2 \cap \cdots \cap A_n) = (B \times A_1) \cap (B \times A_2) \cap \cdots \cap (B \times A_n)$$

(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 $x \in (A_1 \cup A_2 \cup \cdots \cup A_n) \times B$. Тогда $x = (u, v)$, где $u \in A_1 \cup A_2 \cup \cdots \cup A_n$, а $v \in B$. Но тогда $u \in A_i$ для некоторого $i \in \{1, 2, \ldots, n\}$, и потому $x = (u, v)$ лежит в $A_i \times B$. Следовательно, $x \in (A_1 \times B) \cup (A_2 \times B) \cup \cdots \cup (A_n \times B)$. Обратно, пусть $x \in (A_1 \times B) \cup (A_2 \times B) \cup \cdots \cup (A_n \times B)$. Тогда $x \in A_i \times B$ для некоторого $i \in \{1, 2, \ldots, n\}$. Следовательно, $x = (u, v)$, где $u \in A_i$, а $v \in B$. Но тогда $u \in A_1 \cup A_2 \cup \cdots \cup A_n$, и потому $x = (u, v) \in (A_1 \cup A_2 \cup \cdots \cup A_n) \times B$. Свойство доказано. □

Свойства прямого произведения (2)

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

1.2. Отображения

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

«Функциональное» определение отображения

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.

Функциональное определение кажется простым и понятным, но по сути дела оно ничего не определяет. В самом деле, в нем встречается слово «правило». Такой термин ранее не появлялся. Что называется правилом? Единственный возможный ответ на этот вопрос таков: правилом (в указанном выше смысле) называется отображение из A в B. Но тогда получается, что отображением из A в B называется отображение из A в B.

Отображение из одного множества в другое: теоретико-множественное определение

Таким образом, фактически функциональное определение отображения является не определением, а неформальным объяснением того, что мы будем понимать под этим словом (подобно тому «определению» множества, с которого мы начали этот параграф). Такой подход означает, что мы объявляем отображение первоначальным неопределяемым понятием, наряду с понятием множества. Но в этом нет необходимости, поскольку существует вполне строгое определение отображения, не использующее никаких неопределенных ранее понятий, кроме понятия множества. Мы имеем в виду следующее

«Теоретико-множественное» определение отображения

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 $y = \alpha(x)$.

Имеется в виду, что α отображает произвольный элемент $x \in A$ в единственный элемент $y \in B$ с тем свойством, что $(x, y) \in \alpha$.

Отображение из одного множества в другое: сопутствующие определения и обозначения

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 у элемента $y \in B$ может быть любое число (в том числе может не быть ни одного).

Обозначения

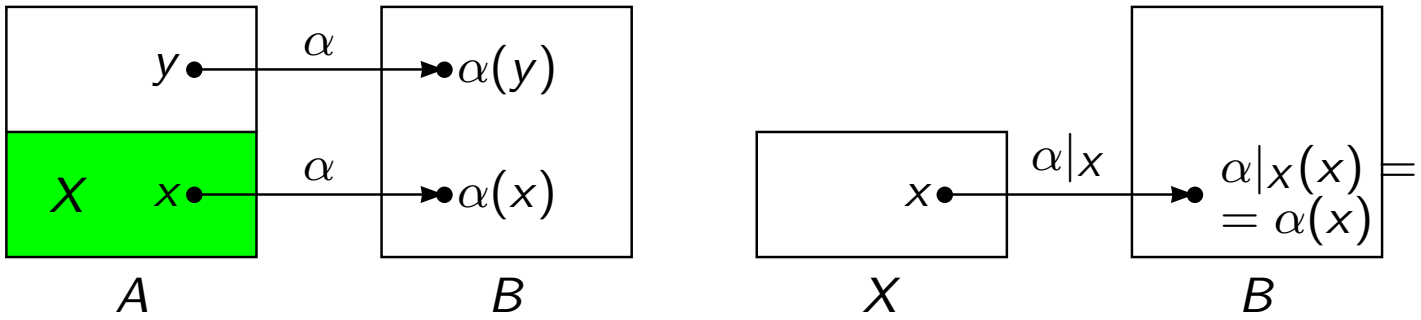
Тот факт, что α — отображение из A в B, обозначается следующим образом: $\alpha\colon A \longrightarrow B$. Если $X \subseteq A$, то через $\alpha(X)$ обозначается множество всех элементов вида $\alpha(x)$, где x пробегает X.

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 $x \in X$.

Понятие ограничения отображения на подмножество иллюстрируется на рис. 2 на следующем слайде.

Ограничение отображения на подмножество (рисунок)



Отображение α Ограничение α на X

Рис. 2. Ограничение отображения α на подмножество X

Типы отображений

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.

- Произвольное отображение $f : A \longrightarrow B$ является сюръективным отображением из A на $f(A)$.
- Как мы увидим ниже, из существования биективного отображения из A на B вытекает существование биективного отображения из B на A.

Не инъективное отображение (рисунок)

На рис. 3 и 4 приведены примеры, соответственно, не инъективного и не сюръективного отображений (на рис. 4 $f(A)$ — часть множества B, закрашенная зеленым цветом).

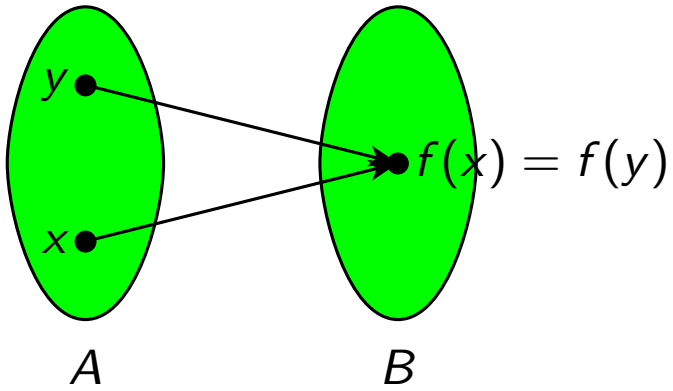


Рис. 3. Не инъективное отображение

Не сюръективное отображение (рисунок)

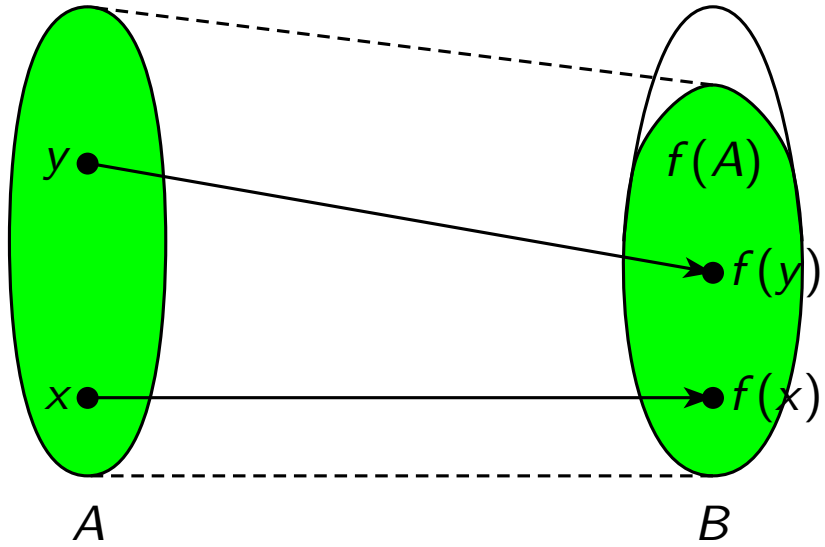


Рис. 4. Не сюръективное отображение

Произведение отображений

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 $h(x) = g\big(f(x)\big)$ для всякого $x \in A$. Произведение f и g обозначается через fg.

Иллюстрацией к этому определению служит рис. 5.

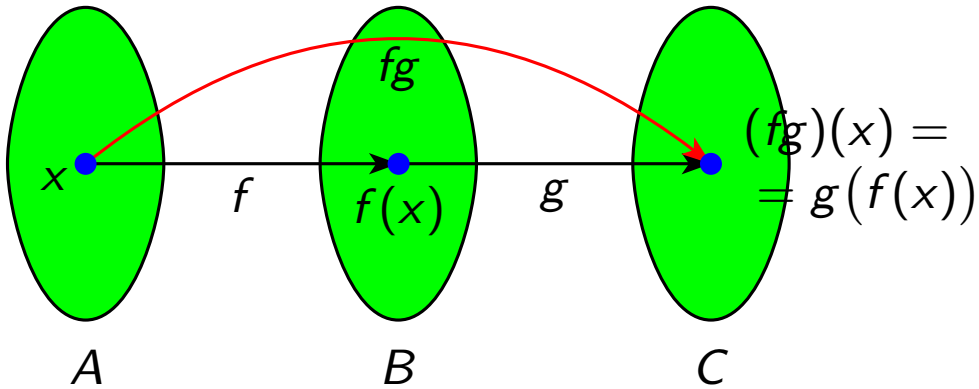


Рис. 5. Произведение отображений

Ассоциативность произведения 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. 6, на котором действие отображения $(fg)h$ изображено красными стрелками, а действие отображения $f(gh)$ — синими).

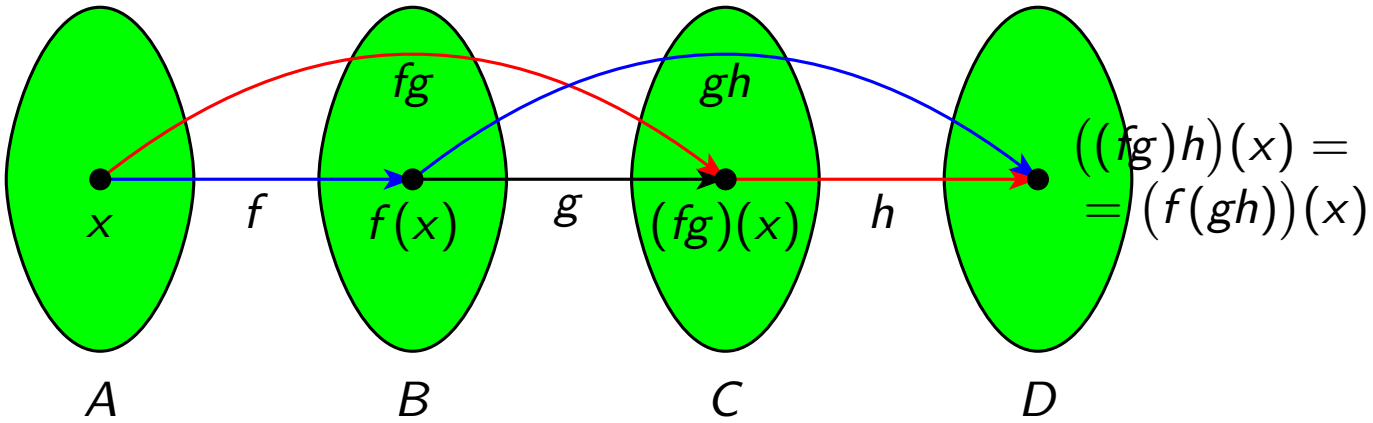


Рис. 6. Ассоциативность произведения отображений

Некоммутативность произведения отображений

Произведение отображений *не коммутативно*. В самом деле, пусть f — отображение из A в B, а g — отображение из B в C. Тогда отображение fg существует, но если $A \neq C$, то отображения gf не существует. Но даже в случае, когда $A = B = C$, равенство $fg = gf$ выполняется не всегда. В этом случае определены оба отображения fg и gf, но равенство $(fg)(x) = (gf)(x)$ выполняться не обязано.

Например, пусть $A = B = C = \mathbb{R}$ и, для всякого $x \in \mathbb{R}$, $f(x) = x^2$, а $g(x) = x - 1$. Тогда $(fg)(x) = x^2 - 1$, а $(gf)(x) = (x-1)^2$. Легко проверяется, что если $x \neq 1$, то $x^2 - 1 \neq (x-1)^2$.

Замечание 1.2

Произведение биективных отображений биективно.

Доказательство. Пусть f — биекция из A на B, а g — биекция из B на C. Проверим сначала, что отображение fg инъективно. Пусть $x_1, x_2 \in A$ и $x_1 \neq x_2$. Поскольку f инъективно, $f(x_1) \neq f(x_2)$. А отсюда и из инъективности g вытекает, что $g\big(f(x_1)\big) \neq g\big(f(x_2)\big)$, т. е. $(fg)(x_1) \neq (fg)(x_2)$. Следовательно, fg инъективно.

Проверим теперь, что отображение fg сюръективно. Пусть $z \in C$. В силу сюръективности g, $z = g(y)$ для некоторого $y \in B$. А из сюръективности f вытекает, что $y = f(x)$ для некоторого $x \in A$. Следовательно, $z = g(y) = g\big(f(x)\big) = (fg)(x)$, и потому fg сюръективно. □

Из доказательства замечания 1.2 непосредственно вытекает следующее утверждение.

Следствие 1.1

Произведение инъективных отображений инъективно, а произведение сюръективных отображений сюръективно. □

Обратное отображение (1)

Определение

Отображение f из множества A в себя, задаваемое правилом $f(x) = x$ для всякого $x \in A$, называется *тождественным*. Тождественное 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 $g\big(f(x)\big) = x$ для всякого $x \in A$. Отображение, обратное к f, обозначается через f^{-1}.

! Обратите внимание, что f^{-1} — отображение не из B в A, а из $f(A)$ в A.

Отображение f^{-1} существует далеко не для всякого отображения f. А именно, справедливо следующее утверждение.

Предложение 1.1 (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.

Обратное отображение (2)

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

$$x_1 = \varepsilon(x_1) = (ff^{-1})(x_1) = f^{-1}\big(f(x_1)\big) = \\ = f^{-1}\big(f(x_2)\big) = (ff^{-1})(x_2) = \varepsilon(x_2) = x_2.$$

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 отображение g из $f(A)$ в A правилом $g(y) = x$. При этом, если $x \in A$, то $(fg)(x) = g\big(f(x)\big) = g(y) = x$, т. е. $fg = \varepsilon$. Следовательно, $g = f^{-1}$, т. е. отображение f^{-1} существует. □

Замечание 1.3

Если f — биективное отображение из A на B, то f^{-1} — биективное отображение из B на A.

Доказательство. Прежде всего, заметим, что отображение f^{-1} существует, так как отображение f инъективно. По определению обратного отображения, f^{-1} — отображение из $f(A)$ в A. Поскольку отображение f сюръективно, $f(A) = B$. Таким образом, f^{-1} отображает B в A. Если $f^{-1}(y_1) = f^{-1}(y_2) = x$ для некоторых $y_1, y_2 \in B$ и $x \in A$, то $f(x) = y_1$ и $f(x) = y_2$. Поскольку элемент $f(x)$ определен однозначно, получаем, что $y_1 = y_2$. Таким образом, отображение f^{-1} инъективно. Далее, если $x \in A$ и $y = f(x)$, то $f^{-1}(y) = x$. Следовательно, отображение f^{-1} сюръективно. □

Свойства обратного отображения (1)

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. 1) Это свойство легко вытекает из определения обратного отображения. Иллюстрацией к нему служит рис. 7.

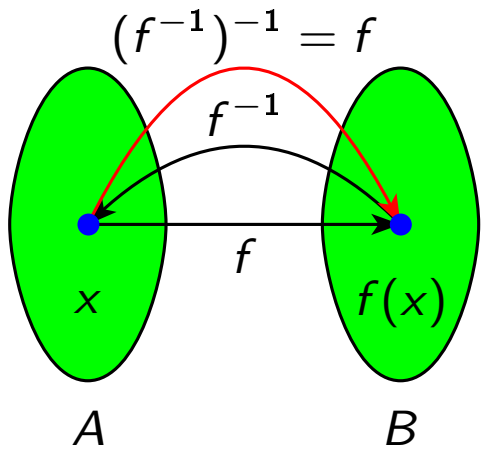


Рис. 7. Свойство 1) обратного отображения

Свойства обратного отображения (2)

2) Иллюстрацией к этому свойству служит рис. 8.

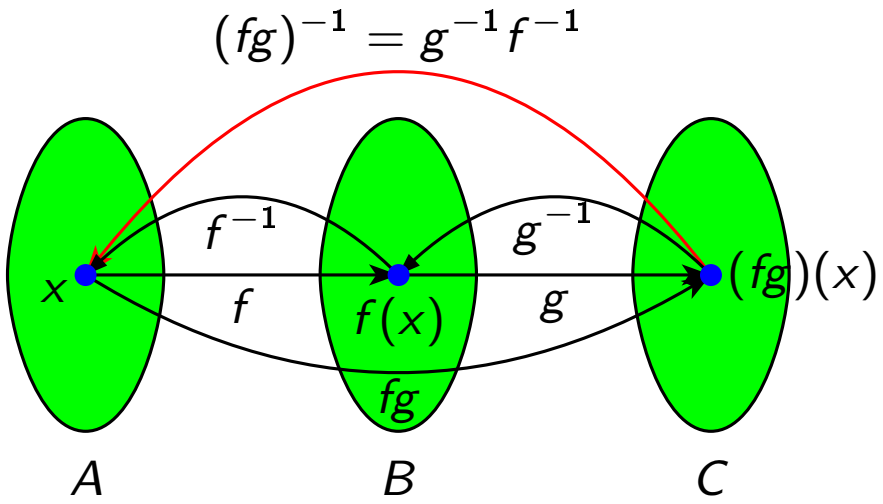


Рис. 8. Свойство 2) обратного отображения

Пусть $x_1, x_2 \in A$. Из критерия существования обратного отображения вытекает, что отображения f и g инъективны. В силу следствия 1.1 отображение fg также инъективно. Поэтому из критерия существования обратного отображения вытекает, что отображение $(fg)^{-1}$ существует.

Свойства обратного отображения (3)

Пусть $x \in A$, $y = f(x)$ и $z = g(y)$. Тогда

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

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

1.3. Мощность конечного множества

Определение

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

Теорема 1.1

Конечные множества A и B равномощны тогда и только тогда, когда они содержат одно и то же число элементов.

Доказательство. *Необходимость.* Предположим, что A и B равномощны, т. е. существует биекция f из A на B. В силу инъективности f, образы различных элементов из A различны. Следовательно, число элементов в B не меньше, чем число элементов в 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, число элементов в B не больше, чем число элементов в A. Это означает, что A и B содержат одно и то же число элементов.

Достаточность. Предположим, что A и B содержат по n элементов. Пусть $A = \{x_1, x_2, \ldots, x_n\}$, а $B = \{y_1, y_2, \ldots, y_n\}$. Определим отображение f из A в B правилом $f(x_i) = y_i$ для всякого $i = 1, 2, \ldots, n$. Очевидно, что f — биекция из A на B. □

Определение

Число элементов конечного множества S называется *мощностью* этого множества и обозначается через $|S|$.

Предложение 1.2

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

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

Мощность декартовой степени конечного множества

Из предложения 1.2 немедленно вытекает

Следствие 1.2

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

1.4. Булеан множества

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 «маленьких» множеств и их мощности

S	$\mathcal{B}(S)$	$\lvert S\rvert$	$\lvert\mathcal{B}(S)\rvert$
$\varnothing$	$\{\varnothing\}$	0	1
$\{1\}$	$\{\varnothing, \{1\}\}$	1	2
$\{1,2\}$	$\{\varnothing, \{1\}, \{2\}, \{1,2\}\}$	2	4
$\{1,2,3\}$	$\{\varnothing, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$	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.

Мощность булеана конечного множества (1)

Теорема 1.2

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

Мы приведем два доказательства этого факта. Первое из них опирается на следствие 1.2, второе не использует никаких ранее доказанных утверждений.

Первое доказательство. Если $S = \varnothing$, то $|S| = 0$ и, как мы видели выше, $\left|\mathcal{B}(S)\right| = 1$. Поскольку $2^0 = 1$, в этом случае требуемое равенство выполняется. Поэтому далее можно считать, что $S \neq \varnothing$. Положим $S = \{x_1, x_2, \ldots, x_n\}$ и $B = \{0, 1\}$. В силу следствия 1.2 $|B^n| = 2^n$. Поэтому достаточно проверить, что $\left|\mathcal{B}(S)\right| = |B^n|$, т. е. что существует биекция из множества $\mathcal{B}(S)$ на множество B^n. Определим отображение φ из $\mathcal{B}(S)$ в B^n следующим образом: если $X \subseteq S$, то $\varphi(X) = (b_1, b_2, \ldots, b_n)$, где

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

для всех $i = 1, 2, \ldots, n$.

Мощность булеана конечного множества (2)

Пусть $S_1, S_2 \subseteq S$ и $S_1 \neq S_2$. Без ограничения общности можно считать, что $S_1 \setminus S_2 \neq \varnothing$, 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 $(b_1, b_2, \ldots, b_n) \in B^n$, то, очевидно $(b_1, b_2, \ldots, b_n) = \varphi(X)$, где $X = \{x_i \mid b_i = 1\} \subseteq S$. Это означает, что отображение φ сюръективно. Следовательно, оно биективно. □

Мощность булеана конечного множества (3)

Второе доказательство. Воспользуемся индукцией по n.

База индукции. Если $n = 0$, то $S = \varnothing$ и, как видно из табл. 1, $\left|\mathcal{B}(S)\right| = 1 = 2^0 = 2^{|S|}$.

Шаг индукции. Пусть теперь $n > 0$. Зафиксируем произвольный элемент $x \in S$ и положим $S' = S \setminus \{x\}$. Тогда $|S'| = n - 1$ и, по предположению индукции, $\left|\mathcal{B}(S')\right| = 2^{|S'|} = 2^{n-1}$. Все подмножества множества S можно разбить на два типа: те, которые не содержат x, и те, которые содержат x. Любое подмножество множества S, не содержащее x, содержится в S'. Число таких подмножеств равно мощности булеана множества S', т.е. 2^{n-1}. Далее, любое подмножество множества S, содержащее x, получается из какого-то подмножества, не содержащего x, добавлением к нему x. Поэтому число таких подмножеств равно числу подмножеств, не содержащих x, т.е. 2^{n-1}. Следовательно, общее число подмножеств множества S равно $2^{n-1} + 2^{n-1} = 2 \cdot 2^{n-1} = 2^n$. □