# Дискретная математика

## Глава 1. Множества и отображения

А. В. Пастор

05.09.2022

Слайды по дискретной математике будут публиковаться по адресу

`https://logic.pdmi.ras.ru/~pastor/ITMO/2022-23/`

## Понятие множества

- Неформально, *множество* — это произвольная совокупность объектов.
  - Объекты, из которых состоит множество, называются *элементами*.
  - Элементами множества могут быть любые рассматриваемые в математике объекты: числа, точки, фигуры, а также другие множества.
  - Принадлежность элемента $x$ множеству $Y$ обозначается $x \in Y$.
  - Множество, не содержащее ни одного элемента, называется *пустым* и обозначается $\varnothing$.

- Можно дать математически строгое определение понятия множества, задав его аксиоматически. Но это сложно и находится за рамками данного курса.
  - Формально, элементами множества тоже являются множества.
  - Другие объекты нужно кодировать при помощи тех или иных множеств.

## Задание множеств

- Перечисление элементов: элементы множества перечисляются через запятую в фигурных скобках.
Этот способ подходит для конечных множеств.

### Пример

$Y = \{1, 3, 7, 19, 2021\}$.

- Задание подмножества при помощи условия:
$Y = \{x \in X \mid \text{условие на } x\}$ — множество, состоящие из всех элементов $X$, удовлетворяющих данному условию.

### Пример

$Y = \{n \in \mathbb{Z} \mid n \,\vdots\, 2\}$ — множество всех четных чисел.

- Если все элементы множества $Y$ принадлежат множеству $X$, то $Y$ называется *подмножеством* множества $X$. Обозначение: $Y \subset X$.
  - $\mathcal{P}(X)$ — множество всех подмножеств множества $X$.
- Можно также писать $Y = \{x \mid \text{условие на } x\}$, но это не обязательно множество!
  - Такие совокупности множеств называют *классами*.

## Проблемы и парадоксы теории множеств



- Попытки задать понятие множества неформально приводят к ряду вопросов, на которые трудно дать ответ.

  1. Может ли множество являться своим элементом?
     То есть, может ли хоть для какого-нибудь множества $x$ быть верно утверждение $x \in x$?
  2. Парадокс Б. Рассела (1901). Рассмотрим множество $Y = \{x \mid x \notin x\}$ (т. е. $Y$ состоит их всех множеств, которые не являются собственными элементами).
     - Вопрос: верно ли, что $Y \in Y$?
     - При любом ответе на этот вопрос возникает противоречие!

- В формальной теории множеств соотношение $x \in x$ запрещено (аксиома регулярности).
- Класс $Y$, определенный в парадоксе Рассела, множеством не является.
- Также не является множеством класс всех множеств.

## Операции над множествами



- Основные операции. Пусть $A, B$ — множества.
  - $A \cap B \stackrel{\text{def}}{=} \{x \in A \mid x \in B\}$ — *пересечение*;
  - $A \cup B \stackrel{\text{def}}{=} \{x \mid (x \in A \vee x \in B)\}$ — *объединение*;
    - *это всегда множество!*
  - $A \setminus B \stackrel{\text{def}}{=} \{x \in A \mid x \notin B\}$ — *разность*;
  - $A \triangle B \stackrel{\text{def}}{=} (A \cup B) \setminus (A \cap B)$ — *симметрическая разность*.
- Дополнение множества. Пусть $U$ — *универсум* (или *объемлющее множество*), т. е. множество, которое содержит все рассматриваемые множества. Тогда
  - $\overline{A} \stackrel{\text{def}}{=} \{x \in U \mid x \notin A\}$
    - *результат этой операции зависит от выбора $U$!*
- Упорядоченные пары.
  - $(x, y) \stackrel{\text{def}}{=} \{\{x\}, \{x, y\}\}$ — *упорядоченная пара* элементов (множеств) $x$ и $y$.
    - Очевидно, что $(a, b) = (c, d)$ тогда и только тогда, когда $a = c$ и $b = d$.

## Декартово произведение множеств



- $A \times B \overset{\text{def}}{=} \{(x, y) \mid (x \in A \,\&\, y \in B)\}$ — *декартово произведение* (или *прямое произведение*) множеств $A$ и $B$.

- Аналогично понятию упорядоченной пары можно ввести понятия *упорядоченной тройки*, *упорядоченной четверки*, ..., *упорядоченной n-ки*.
  - Это можно сделать по индукции: $(x_1, \ldots, x_{n-1}, x_n) \overset{\text{def}}{=} ((x_1, \ldots, x_{n-1}), x_n)$.

- Понятие декартова произведения также можно обобщить на случай $n$ множеств.
  - $A_1 \times \ldots \times A_n \overset{\text{def}}{=} \{(x_1, \ldots, x_n) \mid (x_1 \in A_1 \,\&\, \ldots \,\&\, x_n \in A_n)\}$.
  - Если $A$ — множество и $n \in \mathbb{N}$, то $A^n \overset{\text{def}}{=} \underbrace{A \times \ldots \times A}_{n}$.
    - Здесь мы формально считаем, что $A^1 = A$.

# Бинарные отношения

## Определение

• *Бинарным отношением* между множествами $X$ и $Y$ называется произвольное подмножество их декартового произведения $R \subset X \times Y$.

• Если $X = Y$, то $R$ — бинарное отношение на $X$.

• Пара $(x, y)$, где $x \in X$ и $y \in Y$, *удовлетворяет* отношению $R$, если $(x, y) \in R$. Обозначение: $xRy$.

## Замечание

• Фактически, бинарное отношение — это свойство, которое для каждой пары $(x, y)$ может либо выполняться, либо не выполняться ($R$ — это множество тех пар, для которых данное свойство выполнено).

• Бинарное отношение $R$ на множестве $X$ можно рассматривать как орграф: элементы множества будут его вершинами, а стрелка из $x$ в $y$ проводится тогда и только тогда, когда выполнено $xRy$.

## Бинарные и $n$-арные отношения



Аналогично можно ввести понятие отношения между $n$ множествами, где $n \in \mathbb{N}$.

### Определение

- *$n$-местным* (или *$n$-арным*) отношением между множествами $X_1, \dots, X_n$ называется произвольное подмножество $R \subset X_1 \times \dots \times X_n$.
- Если $X_1 = \dots = X_n = X$, то $R$ — *$n$-местное отношение* на множестве $X$.

### Примеры

1. Равенство $(a = b)$ — бинарное отношение на $\mathbb{R}$;
2. делимость $(a \,\vdots\, b)$ — бинарное отношение на $\mathbb{Z}$;
3. пусть $G = (V, E)$ — граф, тогда
   - смежность — бинарное отношение на $V$,
   - инцидентность — бинарное отношение между $V$ и $E$;
4. точки $A, B, C$ лежат на одной прямой — трехместное отношение на плоскости.

## Свойства отношений

### Определение

Бинарное отношение $R \subset X^2$ называется

- *рефлексивным*, если $xRx$ выполнено для всех $x \in X$;
- *иррефлексивным* (*антирефлексивным*), если $xRx$ не выполнено ни для каких $x \in X$;
- *симметричным*, если из $xRy$ следует $yRx$;
- *антисимметричным*, если из $xRy$ и $yRx$ следует, $x = y$;
- *транзитивным*, если из $xRy$ и $yRz$ следует $xRz$.

### Определение

Бинарное отношение $\sim$ на множестве $X$ называется *отношением эквивалентности*, если оно рефлексивно, симметрично и транзитивно.

### Замечание

Отношение эквивалентности разбивает множество на *классы эквивалентности* так, что любые два элемента из одного класса эквивалентны, а любые два элемента из разных классов — нет.

# Отношение порядка



## Определение

- Бинарное отношение $\prec$ на множестве $X$ называется *отношением частичного порядка*, если оно антисимметрично и транзитивно.
- Если при этом отношение $\prec$ иррефлексивно, то оно называется *отношением строгого частичного порядка*.
- А если оно рефлексивно — то *отношением нестрогого частичного порядка*.
  - Как правило, для отношения строгого частичного порядка используется знак $\prec$ или $\succ$, а для нестрогого — знак $\preccurlyeq$ или $\succcurlyeq$.
- Множество, на котором задано отношение частичного порядка, называется *частично упорядоченным*.
  - Формально, частично упорядоченное множество — это упорядоченная пара $(X, \prec)$, где $X$ — множество и $\prec$ — отношение частичного порядка на $X$.
  - В частично упорядоченном множестве некоторые пары элементов могут быть *несравнимы*. То есть могут существовать такие $a, b \in X$, что ни одно из утверждений $a = b$, $a \prec b$, $b \prec a$ не выполнено.

# Отношение линейного порядка

## Определение

- Бинарное отношение $\prec$ на множестве $X$ называется *отношением (строгого) линейного порядка*, если оно является отношением частичного порядка и для любых $a, b \in X$ выполнено ровно одно из следующих трех утверждений: $a = b$, $a \prec b$ или $b \prec a$.
- В этом случае, пара $(X, \prec)$ называется *линейно упорядоченным множеством*.

## Примеры

1. $a < b$ — отношение линейного порядка на $\mathbb{R}$;
2. $a \,\vdots\, b$ — отношение частичного порядка на $\mathbb{N}$.
3. Пусть $X$ — множество.
   Тогда $A \subset B$ — отношение частичного порядка на $\mathcal{P}(X)$.

## Отображения и функции

- Неформально, *отображение* (*функция*) из множества $X$ в множество $Y$ — это такое правило $f$, которое каждому элементу $x \in X$ ставит в соответствие ровно один элемент $y \in Y$. Этот элемент обозначается $f(x)$.
- Формально понятие отображения можно определить в терминах отношений.

### Определение

- Бинарное отношение $f \subset X \times Y$ называется *отображением* из множества $X$ в множество $Y$, если любой элемент $x \in X$ входит в качестве первого элемента ровно в одну пару $(x, y) \in f$.
- Обозначение: $f : X \to Y$.
- Второй элемент пары $(x, y)$ обозначают $f(x)$ и называют *образом* элемента $x$ при отображении $f$.
- Если $y = f(x)$, то $x$ называют *прообразом* элемента $y$.
- В отличии от образа, прообраз элемента существует не всегда; также прообраз может быть не единственным.

# Инъекция, сюръекция, биекция



## Определение

Отображение $f: X \to Y$ называется

- *инъекцией*, если $f(x) \neq f(y)$ при $x \neq y$;
- *сюръекцией*, если у каждого элемента множества $Y$ есть хотя бы один прообраз в множестве $X$;
- *биекцией*, если $f$ одновременно является инъекцией и сюръекцией.

## Замечание

- Биекция — это *взаимно однозначное соответствие* между множествами $X$ и $Y$: каждому элементу множества $X$ поставлен в соответствие единственный элемент множества $Y$, а каждому элементу множества $Y$ — единственный элемент множества $X$.
- В частности, если $X$ и $Y$ — конечные множества и существует биекция $f: X \to Y$, то в множествах $X$ и $Y$ одинаковое число элементов.

# Композиция отображений и обратное отображение



### Определение

*Композицией* отображений $f\colon X \to Y$ и $g\colon Y \to Z$ называется отображение $g \circ f\colon X \to Z$, задаваемое формулой $(g \circ f)(x) = g(f(x))$.

### Определение

- Отображение $g\colon Y \to X$ называется *обратным* к отображению $f\colon X \to Y$, если обе композиции $f \circ g$ и $g \circ f$ являются тождественными отображениями.
- Т. е. $g(f(x)) = x$, при всех $x \in X$, и $f(g(y)) = y$, при всех $y \in Y$.
- Отображение $f$ называется *обратимым*, если к нему есть обратное.
- Отображение, обратное к $f$, обычно обозначается $f^{-1}$.

## Критерий обратимости



**Теорема**

*Отображение* $f\colon X \to Y$ *обратимо* $\iff f$ *— биекция.*

**Доказательство.**

“$\Leftarrow$”: Для каждого $y \in Y$ обозначим через $f^{-1}(y)$ единственный прообраз элемента $y$.

- Тогда $f^{-1}\colon Y \to X$ — отображение, обратное к $f$.

“$\Rightarrow$”: Пусть $f^{-1}$ — отображение, обратное к $f$.

- $f$ — инъекция, поскольку если $f(x) = f(y)$, то $x = f^{-1}(f(x)) = f^{-1}(f(y)) = y$.
- $f$ — сюръекция, поскольку для любого $y \in Y$ имеем $y = f(f^{-1}(y))$. $\square$

## Конечные множества: немного комбинаторики

- Пусть $X$ — конечное множество. Количество его элементов будем обозначать через $|X|$.
- Мы уже знаем, что $|X| = |Y|$ тогда и только тогда, когда между $X$ и $Y$ можно установить биекцию.

### Лемма (принцип произведения)

*Если $|X| = m$ и $|Y| = n$, то $|X \times Y| = mn$.*

Доказательство. Каждый из $m$ элементов множества $X$ входит ровно в $n$ пар с элементами множества $Y$. □

### Следствие

*Если $|X_i| = m_i$, где $i \in [1..k]$, то $|X_1 \times \ldots \times X_k| = m_1 \cdot \ldots \cdot m_k$.*

Доказательство. Индукция по $k$.
База ($k = 2$): см. предыдущую лемму.
Переход ($k \to k+1$): $|X_1 \times \ldots \times X_k \times X_{k+1}| = |(X_1 \times \ldots \times X_k) \times X_{k+1}| =$
$= |X_1 \times \ldots \times X_k| \cdot |X_{k+1}| = (m_1 \cdot \ldots \cdot m_k) \cdot m_{k+1} = m_1 \cdot \ldots \cdot m_k \cdot m_{k+1}$. □

## Конечные множества: количество подмножеств



### Теорема

*Если* $|X| = m$, *то* $|\mathcal{P}(X)| = 2^m$.

Доказательство. Пусть $X = \{x_1, \dots, x_m\}$.

- Для каждого из $i \in [1..m]$ есть два варианта: $x_i$ можно либо включить в подмножество, либо не включать.
- Итого, есть $2^m$ способов выбрать подмножество. $\square$

### Замечание

- Фактически, мы построили следующую биекцию между множествами $\mathcal{P}(X)$ и $\{0,1\}^m$.
  - Подмножеству $A \subset X$ ставится в соответствие последовательность $(a_1, \dots, a_m) \in \{0,1\}^m$, где

$$a_i = \begin{cases} 1, & \text{если } x_i \in A \\ 0, & \text{если } x_i \notin A. \end{cases}$$

# Конечные множества: количество отображений



**Теорема**

*Пусть $|X| = k$ и $|Y| = n$. Тогда*

1. *число отображений из $X$ в $Y$ равно $n^k$;*
2. *число инъекций из $X$ в $Y$ равно $n(n-1)\dots(n-k+1)$.*

**Доказательство.** Пусть $X = \{x_1, \dots, x_k\}$.

1. Для каждого элемента $x_i \in X$ можно $n$ способами выбрать его образ.
2. Образ $x_1$ можно выбрать $n$ способами. После этого останется $n-1$ способ выбрать образ $x_2$, ..., $n-k+1$ способ выбрать образ $x_k$. □

**Замечание**

При $n \geq k$ имеем $n(n-1)\dots(n-k+1) = \frac{n!}{(n-k)!}$,
где $n! = 1 \cdot 2 \cdot \ldots \cdot n$ (и $0! = 1$).

**Вопрос.** А чему равно число сюръекций из $X$ в $Y$?

Об этом мы поговорим позже...

# Конечные множества: перестановки и размещения



## Определение

*Перестановкой* на множестве $X$ называется произвольная биекция $\sigma\colon X \to X$.

## Следствие

*Если $|X| = n$, то число перестановок на множестве $X$ равно $n!$.*

## Определение

1. Число инъекций $f\colon [1..k] \to [1..n]$ называется *числом размещений из $n$ элементов по $k$* и обозначается $A_n^k$.
2. Число отображений $f\colon [1..k] \to [1..n]$ называется *числом размещений с повторениями из $n$ элементов по $k$* и обозначается $\widetilde{A}_n^k$.

Итого, мы доказали следующие формулы.

1. $A_n^k = n(n-1)\dots(n-k+1) = \frac{n!}{(n-k)!}$, при $n \geq k$;
2. $\widetilde{A}_n^k = n^k$.

## Счётные множества

### Определение

Множество $X$ называется *счётным*, если существует биекция $f\colon X \to \mathbb{N}$.

### Замечание

- Это означает, что элементы множества $X$ можно занумеровать натуральными числами: для элемента $a \in X$ число $f(a)$ будет его номером.
- Элементы счётного множества можно записать в виде последовательности: $X = \{x_1, x_2, x_3, \ldots\}$, где $x_k = f^{-1}(k)$.

### Примеры

- $2\mathbb{N} = \{2n \mid n \in \mathbb{N}\}$ — множество всех чётных чисел.

Доказательство. $f(x) = x/2$ — биекция из $2\mathbb{N}$ в $\mathbb{N}$. $\square$

- $\mathbb{Z}$ — множество всех целых чисел.

Доказательство.

$$f(x) = \begin{cases} 2x, & x > 0 \\ 1 - 2x, & x \leq 0 \end{cases}$$ — биекция из $\mathbb{Z}$ в $\mathbb{N}$. $\square$

# Счётность произведения



## Теорема

*Множество* $\mathbb{N} \times \mathbb{N}$ *— счётно.*

Доказательство.
Функция $f(x, y) = \frac{(x+y-1)(x+y-2)}{2} + y$ — биекция из $\mathbb{N} \times \mathbb{N}$ в $\mathbb{N}$. $\square$

## Замечание

- Эта функция перечисляет клетки бесконечной таблицы "по диагоналям".
- Другой пример биекции из $\mathbb{N} \times \mathbb{N}$ в $\mathbb{N}$: $g(x, y) = 2^{x-1}(2y - 1)$.

## Следствие

*Пусть* $X_1, \dots, X_n$ *— счётные множества.*
*Тогда множество* $X_1 \times \dots \times X_n$ *— также счётно.*

Доказательство. Рассмотрим биекции
$f_i : X_i \to \mathbb{N}$ (где $i \in [1..n]$) и $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$.

<u>База $(n = 2)$</u>: отображение $h_2 : X_1 \times X_2 \to \mathbb{N}$, задаваемое формулой

$$h_2(x_1, x_2) \overset{\text{def}}{=} g(f_1(x_1), f_2(x_2)),$$

является биекцией.

## Счётные множества: примеры и свойства



Переход $(n-1 \to n)$:

- Множество $X_1 \times \ldots \times X_{n-1}$ счётно по индукционному предположению.
- Множество $X_n$ счётно по условию.
- Тогда множество $X_1 \times \ldots \times X_{n-1} \times X_n = (X_1 \times \ldots \times X_{n-1}) \times X_n$ является декартовым произведением двух счётных множеств.
- По доказанному в базе, оно счётно. $\square$

### Теорема

*Бесконечное подмножество счётного множества — счётно.*

Доказательство.

Пусть $X$ — счётное множество и $A \subset X$ — его бесконечное подмножество.

- Рассмотрим биекцию $f\colon X \to \mathbb{N}$.
- Тогда $g(x) \stackrel{\mathrm{def}}{=} |\{a \in A \mid f(a) \le f(x)\}|$ — биекция из $A$ в $\mathbb{N}$. $\square$

## Не более чем счётные множества



### Определение

- Множество $X$ — *не более чем счётно*, если $X$ либо конечно, либо счётно.
- Множество $X$ — *несчётно*, если $X$ не является ни конечным, ни счётным.

### Теорема

*Пусть $X \neq \varnothing$. Тогда следующие условия равносильны:*

1. *множество $X$ не более чем счётно;*
2. *существует инъекция $f\colon X \to \mathbb{N}$;*
3. *существует сюръекция $g\colon \mathbb{N} \to X$.*

### Доказательство.

“1. $\Rightarrow$ 3.”: Пусть множество $X$ не более чем счётно.

- Если $X$ бесконечно, то оно счётно.
  - Тогда существует биекция $f\colon X \to \mathbb{N}$.
  - Следовательно, $f^{-1}\colon \mathbb{N} \to X$ — сюръекция.

## Не более чем счётные множества

- Если $X$ конечно, то обозначим $|X| = n$.
  - Тогда существует биекция $f\colon X \to [1..n]$.
  - Пусть $g(y) \stackrel{\text{def}}{=} \begin{cases} f^{-1}(y), & y \le n \\ f^{-1}(n), & y > n. \end{cases}$
  - Легко видеть, что $g\colon \mathbb{N} \to X$ — сюръекция.

"3. $\Rightarrow$ 2.": Пусть $g\colon \mathbb{N} \to X$ — сюръекция.

- Тогда у каждого элемента $x \in X$ есть хотя бы один прообраз.
- Выберем из всех прообразов $x$ наименьший.
- То есть положим $f(x) \stackrel{\text{def}}{=} \min\{y \in \mathbb{N} \mid g(y) = x\}$.
- Легко видеть, что $f\colon X \to \mathbb{N}$ — инъекция.

"2. $\Rightarrow$ 1.": Пусть $f\colon X \to \mathbb{N}$ — инъекция.

- Рассмотрим множество $f(X) \stackrel{\text{def}}{=} \{f(x) \mid x \in X\}$.
- Тогда $f\colon X \to f(X)$ — биекция.
- Поскольку $f(X) \subset \mathbb{N}$, множество $f(X)$ не более чем счётно.
- Если $f(X)$ — конечно, то и $X$ — конечно.
- Если $f(X)$ — счётно, то и $X$ — счётно. □

# Не более, чем счётные множества



## Следствие 1

*Если $f\colon X \to Y$ — инъекция и множество $Y$ — счётно, то множество $X$ — не более чем счётно.*

Доказательство.

- Пусть $g\colon Y \to \mathbb{N}$ — биекция.
- Тогда $g \circ f\colon X \to \mathbb{N}$ — инъекция. $\square$

## Следствие 2

*Если $g\colon Y \to X$ — сюръекция и множество $Y$ — счётно, то множество $X$ — не более чем счётно.*

Доказательство.

- Пусть $f\colon \mathbb{N} \to Y$ — биекция.
- Тогда $g \circ f\colon \mathbb{N} \to X$ — инъекция. $\square$

## Счётность множества рациональных чисел

### Теорема

*Множество $\mathbb{Q}$ всех рациональных чисел — счётно.*

Доказательство. Рассмотрим отображение $g\colon \mathbb{Z}\times\mathbb{N}\to\mathbb{Q}$, задаваемое формулой $g(a,b)\stackrel{\mathrm{def}}{=}\frac{a}{b}$.

- Очевидно, что $g$ — сюръекция.
- Следовательно, $\mathbb{Q}$ — не более, чем счётно.
- Но при этом множество $\mathbb{Q}$ — бесконечно.
- Таким образом, $\mathbb{Q}$ — счётно. □

### Теорема

*Объединение не более, чем счётного множества не более, чем счётных множеств — не более чем счётно.*

### Замечание

То есть, если нам дана конечная или бесконечная последовательность множеств $A_1, A_2, \ldots$, каждое из которых не более чем счётно, то множество $B=\bigcup\limits_i A_i$ также не более чем счётно.

# Объединение не более чем счётных множеств

Доказательство. Пусть $f_i\colon A_i \to \mathbb{N}$ — инъекции.

- Для каждого $x \in B$ пусть $s(x) \stackrel{\text{def}}{=} \min\{n \in \mathbb{N} \mid x \in A_n\}$.
- Рассмотрим отображение $h\colon B \to \mathbb{N} \times \mathbb{N}$, задаваемое формулой $h(x) \stackrel{\text{def}}{=} (s(x), f_{s(x)}(x))$.
- Очевидно, что $h$ — инъекция.
- Следовательно, $B$ — не более, чем счётно. $\square$

## Замечание

В частности, объединение любого конечного или счётного набора счётных множеств всегда счётно.

## Определение

- Вещественное число $\alpha$ называется *алгебраическим*, если $\alpha$ — корень ненулевого многочлена с рациональными коэффициентами.
- В противном случае, число $\alpha$ называется *трансцендентным*.

## Теорема

*Множество всех алгебраических чисел счётно. (Задача.)*

# Пример несчётного множества

## Теорема

*Множество $[0,1)$ несчётно.*

Доказательство. Пусть $f\colon \mathbb{N} \to [0,1)$ — биекция.

- Тогда $[0,1) = \{\alpha_1, \alpha_2, \ldots\}$, где $\alpha_i \stackrel{\text{def}}{=} f(i)$.
- Запишем все $\alpha_i$ в виде бесконечных десятичных дробей: $\alpha_i = \sum\limits_{j=1}^{\infty} \frac{a_{ij}}{10^j}$,

где $a_{ij} \in [0..9]$.

- Рассмотрим число $\beta = \sum\limits_{i=1}^{\infty} \frac{b_i}{10^i}$, где $b_i = \begin{cases} 4, & a_{ii} = 7 \\ 7, & a_{ii} \neq 7. \end{cases}$
- Тогда $\beta \in [0,1)$, но при этом $\beta$ не совпадает ни с одним из $\alpha_i$ (десятичные записи чисел $\beta$ и $\alpha_i$ отличаются в $i$-м разряде). Противоречие. $\square$

## Следствие

*Существуют трансцендентные числа (т. е. вещественные числа, не являющиеся алгебраическими).*

# Мощность множества



## Определение

Множества $X$ и $Y$ называются *равномощными* (или *эквивалентными*), если существует биекция $f : X \to Y$. Обозначение: $X \sim Y$.

## Замечание

- Легко видеть, что равномощность обладает всеми свойствами эквивалентности:
  1. $X \sim X$ (рефлексивность);
  2. если $X \sim Y$, то $Y \sim X$ (симметричность);
  3. если $X \sim Y$ и $Y \sim Z$, то $X \sim Z$ (транзитивность).
- Тем самым, все множества можно разбить на классы равномощных.
- Каждому классу ставится в соответствие некоторая специальная характеристика, называемая *мощностью* множеств этого класса.

## Мощность множества

- Конечные множества равномощны если и только если они содержат поровну элементов.
  - Мощностью конечного множества называется число его элементов.
- Все счётные множества равномощны.
  - Мощность счётного множества обозначается через $\mathfrak{a}$.
- Множество $X$ имеет *мощность континуума*, если $X \sim [0,1]$.
  - Мощность континуума обозначается через $\mathfrak{c}$.
- Есть разные варианты обозначений для мощности множества $X$:
  - $|X|$; $\quad \#X$; $\quad \overline{\overline{X}}$; $\quad \mathrm{card}(X)$.
  - $\overline{\overline{X}}$ — “двойное отвлечение” (от свойств элементов и от их порядка).
- Мы будем использовать обозначение $|X|$.

## Счётное подмножество бесконечного множества

### Теорема

*В любом бесконечном множестве есть счётное подмножество.*

Доказательство. Пусть $X = X_0$ — бесконечное множество.

- Будем последовательно выбирать из $X_0$ элементы счётного подмножества $A$.
- Пусть $a_1 \in X_0$ и $X_1 \stackrel{\text{def}}{=} X_0 \setminus \{a_1\}$.
  - Множество $X_1$ бесконечно, т. к. иначе $X = X_1 \cup \{a_1\}$ было бы конечно.
- На $k$-м шаге из бесконечного множества $X_{k-1} \subset X$ выбираем элемент $a_k$ и полагаем $X_k \stackrel{\text{def}}{=} X_{k-1} \setminus \{a_k\}$.
  - Аналогично предыдущему, множество $X_k$ бесконечно.
- Продолжая этот процесс, получим последовательность $(a_i)$ элементов множества $X$.
- Тогда, множество $A = \{a_1, a_2, \dots\}$, составленное из членов построенной последовательности, будет счётным подмножеством $X$. $\square$

## Об аксиоме выбора



- В предыдущей теореме мы строили бесконечную последовательность непустых множеств и из каждого из них выбирали по элементу.
- На самом деле, нам нужно *одновременно* сделать такой выбор для всех рассматриваемых множеств.
- То, что можно одновременно выбрать по элементу из бесконечного набора непустых множеств *не является очевидным*.
- Формально, это свойство называется аксиомой выбора.
- Аксиома выбора. Пусть $S$ — множество непустых множеств, $\cup S$ — объединение всех входящих в $S$ множеств. Тогда существует функция $f : S \to \cup S$, такая, что $f(x) \in x$ для каждого $x \in S$.
- Фактически, мы уже использовали аксиому выбора в теореме о счётном объединении счётных множеств.
- Эти две теоремы (равно как и многие другие) невозможно доказать без аксиомы выбора.

# Следствия теоремы о счётном подмножестве

## Следствие 1

*Если $X$ бесконечно и $Y$ не более чем счётно, то $X \cup Y \sim X$.*

Доказательство. Пусть $B \subset X$ — счётное множество;

- $A = X \setminus B$ и $C = Y \setminus X$.
- Тогда $X = A \cup B$ и $X \cup Y = A \cup B \cup C$;
- при этом $A \cap B = A \cap C = \varnothing$,
- множество $C$ не более чем счётно и $B \cup C$ счётно.
- Рассмотрим биекцию $f\colon B \to B \cup C$.
- Тогда отображение $g\colon X \to X \cup Y$, задаваемое формулой

$$g(x) \overset{\text{def}}{=} \begin{cases} f(x), & x \in B \\ x, & x \in A \end{cases}$$ — биекция. $\square$

## Следствие 2

*Если $X$ несчётно и $Y$ не более чем счётно, то $X \setminus Y \sim X$.*

Доказательство. Заметим, что $X = (X \setminus Y) \cup (X \cap Y)$;

- множество $X \setminus Y$ бесконечно и $X \cap Y$ — счётно. $\square$

# О мощности континуума



### Утверждение

*Пусть* $a, b \in \mathbb{R}$ *и* $a < b$. *Тогда множества* $[a, b]$, $[a, b)$, $(a, b]$ *и* $(a, b)$ *имеют мощность континуума.*

### Доказательство.

- Функция $f(x) = (b - a)x + a$ задает биекцию $f : [0, 1] \to [a, b]$.
- Множества $[a, b)$, $(a, b]$ и $(a, b)$ равномощны $[a, b]$, поскольку получаются удалением конечного числа элементов. $\square$

### Утверждение

*Множество* $\mathbb{R}$ *имеет мощность континуума.*

### Доказательство.

Функция $\operatorname{tg} x$ задает биекцию из $(-\frac{\pi}{2}, \frac{\pi}{2})$ на $\mathbb{R}$. $\square$

## Сравнение мощностей



### Определение

Мощность множества $X$ *больше* мощности множества $Y$, если эти множества неравномощны и в $X$ есть подмножество, равномощное $Y$.
Обозначение: $|X| > |Y|$.

### Теорема (Г. Кантор, Ф. Бернштейн)

*Если существуют подмножества* $X_0 \subset X$ *и* $Y_0 \subset Y$, *такие, что* $X_0 \sim Y$ *и* $Y_0 \sim X$, *то* $X \sim Y$. *(б/д)*

- Тем самым, утверждения $|X| > |Y|$ и $|Y| > |X|$ не могут быть выполнены одновременно. То есть сравнение мощностей корректно.
- При помощи аксиомы выбора можно доказать, что любые две мощности сравнимы. То есть для любых $X$ и $Y$ выполнено ровно одно из следующих трех утверждений: либо $|X| > |Y|$, либо $|Y| > |X|$, либо $X \sim Y$.

## Сравнение мощностей

- Мощность конечного множества тем больше, чем больше в нем элементов.
- Мощность счётного множества больше мощности любого конечного множества.
- Обратно, если $|X| < \mathfrak{a}$, то $X$ конечно.
- Мощность континуума больше мощности счетного множества.
- Континуум-гипотеза. *Не существует такого множества* $X$, *что* $\mathfrak{a} < |X| < \mathfrak{c}$.
- К. Гёдель и П. Коэн доказали, что континуум-гипотезу невозможно ни доказать ни опровергнуть в рамках формальной теории множеств.

## Мощность множества всех подмножеств



### Теорема (Г. Кантор)

*Для любого множества* $X$ *выполнено* $|\mathcal{P}(X)| > |X|$.

Доказательство. Пусть $Y = \{\{x\} \mid x \in X\}$.

- Очевидно, что $Y \sim X$ и $Y \subset \mathcal{P}(X)$.
- Пусть $f\colon X \to \mathcal{P}(X)$ — биекция.
- Рассмотрим множество $Z \stackrel{\text{def}}{=} \{x \in X \mid x \notin f(x)\}$.
- Пусть $z \stackrel{\text{def}}{=} f^{-1}(Z)$. Верно ли, что $z \in Z$?
  - Если $z \in Z$, то $z \in f(z)$, откуда $z \notin Z$;
  - если $z \notin Z$, то $z \notin f(z)$, откуда $z \in Z$.
- В любом случае получаем противоречие. □

### Замечание

- Из этой теоремы следует, что не существует множества наибольшей мощности. Следовательно, нет и множества всех множеств.
- Для конечных множеств это означает, что $2^n$ всегда больше $n$.