Основы теории множеств, 1 курс Математика

Виктор Львович Селиванов [1]

[1]ФМКН СПбГУ

Осенний семестр, 2025

Важная дополнительная информация

Мой адрес:
v.selivanov@spbu.ru

Страница курса в интернете:
https://github.com/vseliv/sets-2025/tree/main

Литература:

1. Н.К. Верещагин, А. Шень. Лекции по математической логике и теории алгоритмов. ч. 1. Начала теории множеств. — М.: МЦНМО, 2012.

2. К. Куратовский, А. Мостовский, Теория множеств. М.: Мир, 1970.

3. Т. Йех, Теория множеств и метод форсинга. М.: Мир, 1973.

4. И.А. Лавров, Л.Л.Максимова, Задачи по теории множеств, математической логике и теории алгоритмов. М.: Наука, 2001.

Зачем нужна теория множеств?

Теория множеств имеет двоякую природу. С одной стороны, это раздел математической логики со своими задачами, открытыми вопросами, подходами и идеями, которой занимается ограниченный круг специалистов.

С другой стороны, она является инструментом для других дисциплин. Эта её роль является особенно существенной, поскольку она выработала общий язык и стала фундаментом для всей математики.

Зачем нужна теория множеств?

Теория множеств имеет двоякую природу. С одной стороны, это раздел математической логики со своими задачами, открытыми вопросами, подходами и идеями, которой занимается ограниченный круг специалистов.

С другой стороны, она является инструментом для других дисциплин. Эта её роль является особенно существенной, поскольку она выработала общий язык и стала фундаментом для всей математики.

Более того, она позволила преодолеть кризис оснований математики, позникший на рубеже 19 и 20 веков, когда в математике были обнаружены противоречия (парадоксы).

Зачем нужна теория множеств?

Важной идеей является возможность сведения одних математических объектов к другим. Один из известнейших примеров такого сведения принадлежит Рене Декарту, который предложил отождествлять вещественные числа с точками на обычной Евклидовой прямой. Это привычное нам сейчас, но тогда совершенно революционное соображение привело к созданию метода координат, перевернувшего всё тогдашнее естествознание, и позволило считать, что геометрия, в определённом смысле, сводится к вещественной арифметике.

Зачем нужна теория множеств?

Важной идеей является возможность сведения одних математических объектов к другим. Один из известнейших примеров такого сведения принадлежит Рене Декарту, который предложил отождествлять вещественные числа с точками на обычной Евклидовой прямой. Это привычное нам сейчас, но тогда совершенно революционное соображение привело к созданию метода координат, перевернувшего всё тогдашнее естествознание, и позволило считать, что геометрия, в определённом смысле, сводится к вещественной арифметике.

Выяснилось, что ВСЕ математические понятия сводятся к понятию множества, т.е. (почти) все математические дисциплины можно считать разделами теории множеств. Т.о., изучая ТМ мы лучше поймем и другие разделы математики. Создание теории множеств заложило прочный фундамент для математики и показало ее единство.

Этапы развития теории множеств

1. Наивная теория множеств.
Идеи, близкие к идеям ТМ, воникали у многих ученых, однако в явном виде она начала развиваться примерно полтора века назад в работах Георга Кантора и его последователей.

Этапы развития теории множеств

1. Наивная теория множеств.
Идеи, близкие к идеям ТМ, воникали у многих ученых, однако в явном виде она начала развиваться примерно полтора века назад в работах Георга Кантора и его последователей.

2. Аксиоматическая ТМ (ZFC и ее варианты).
Возникла как попытка преодоления противоречий, возникших в наивной ТМ (Цермело, Френкель, Гёдель, Бернайс, фон Нейман,...).

Этапы развития теории множеств

1. Наивная теория множеств.
Идеи, близкие к идеям ТМ, воникали у многих ученых, однако в явном виде она начала развиваться примерно полтора века назад в работах Георга Кантора и его последователей.

2. Аксиоматическая ТМ (ZFC и ее варианты).
Возникла как попытка преодоления противоречий, возникшихих в наивной ТМ (Цермело, Френкель, Гёдель, Бернайс, фон Нейман,...).

3. Альтернативы ZFC.
Рассел, Мычельский, Штейнгауз, Мартин-Лёф, Ловер,...

Множества и операции над ними

Все переменные обозначают множества. Принадлежность: $a \in A$.
Равенство: $A = B$ означает $\forall x (x \in A \leftrightarrow x \in B)$.
Включение: $A \subseteq B$ означает $\forall x (x \in A \to x \in B)$.

Множества часто задаются в виде $\{x \mid \varphi(x)\}$, где $\varphi(x)$ — выражение, построенное из переменных и отношений $=, \in$ с помощью логических операций $\wedge, \vee, \to, \neg, \forall, \exists$. Самое популярное множество: $\emptyset = \{x \mid x \neq x\}$.

Множества и операции над ними

Все переменные обозначают множества. Принадлежность: $a \in A$.
Равенство: $A = B$ означает $\forall x (x \in A \leftrightarrow x \in B)$.
Включение: $A \subseteq B$ означает $\forall x (x \in A \to x \in B)$.

Множества часто задаются в виде $\{x \mid \varphi(x)\}$, где $\varphi(x)$ — выражение, построенное из переменных и отношений $=, \in$ с помощью логических операций $\wedge, \vee, \to, \neg, \forall, \exists$. Самое популярное множество: $\emptyset = \{x \mid x \neq x\}$.

Объединение: $A \cup B = \{x \mid x \in A \vee x \in B\}$.
Пересечение: $A \cap B = \{x \mid x \in A \wedge x \in B\}$.
Разность: $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$.
Симметрическая разность: $A \triangle B = (A \setminus B) \cup (B \setminus A)$.
Дополнение: $\overline{A} = U \setminus A$ (если все рассматриваемые множества содержатся в U).

Свойства булевых операций

$A \cup A = A$, $A \cup B = B \cup A$

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

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$\overline{A \cup B} = \overline{A} \cap \overline{C}$, $\overline{\overline{A}} = A$.

Все написанные выше свойства справедливы при замене объединения на пересечение и наоборот.

Свойства булевых операций

$A \cup A = A$, $A \cup B = B \cup A$

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

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

$\overline{A \cup B} = \overline{A} \cap \overline{C}$, $\overline{\overline{A}} = A$.

Все написанные выше свойства справедливы при замене объединения на пересечение и наоборот.

$\triangle$ коммутативна и ассоциативна, $\cap$ дистрибутивна относительно $\triangle$

$A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$

$A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

$A \setminus (A \setminus B) = (A \cap B)$

$A \setminus B = (A \setminus (A \cap B)$

Отношения

Декартово произведение: $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$, где $(a,b) = \{\{a\},\{a,b\}\}$ — упорядоченная пара.
Подмножества $R \subseteq A \times B$ называются отношениями между A и B. Запись $(a,b) \in R$ иногда упрощают до aRb. Бывают также n-местные отношения (подмножества множества $A_1 \times \dots \times A_n$).
$dom(R) := \{a \mid \exists b(aRb)\}$ — область определения R,
$rng(R) := \{b \mid \exists a(aRb)\}$ — область значений R,
$R(a) := \{b \mid aRb\}$ — значение R в точке A.

Отношения

Декартово произведение: $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$, где $(a,b) = \{\{a\},\{a,b\}\}$ — упорядоченная пара.
Подмножества $R \subseteq A \times B$ называются отношениями между A и B. Запись $(a,b) \in R$ иногда упрощают до aRb. Бывают также n-местные отношения (подмножества множества $A_1 \times \cdots \times A_n$).
$dom(R) := \{a \mid \exists b(aRb)\}$ — область определения R,
$rng(R) := \{b \mid \exists a(aRb)\}$ — область значений R,
$R(a) := \{b \mid aRb\}$ — значение R в точке A.

Пусть $R^{-1} := \{(b,a) \mid (a,b) \in R\}$, тогда $R^{-1} \subseteq B \times A$ называется обратным отношением к R. $(R^{-1})^{-1} = R$.
Композицией отношений $R \subseteq A \times B$ и $S \subseteq B \times C$ называется отношение $S \circ R \subseteq A \times C$ такое, что
$a(S \circ R)c \overset{\text{def}}{\iff} \exists b \in B(aRb \wedge bSc)$. Композиция ассоциативна и $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$.

Функции

Отношение $R \subseteq A \times B$ *функционально*, если $\forall a, b, b'(aRb \wedge aRb' \to b = b')$. В этом случае $R(a) = \emptyset$ или $R(a) = \{b\}$ для единственного b; в последнем случае часто пишут $R(a) = b$. Функциональные отношения $R \subseteq A \times B$ известны также как *частичные функции* из A в B.

Функции

Отношение $R \subseteq A \times B$ *функционально*, если $\forall a, b, b'(aRb \wedge aRb' \to b = b')$. В этом случае $R(a) = \emptyset$ или $R(a) = \{b\}$ для единственного b; в последнем случае часто пишут $R(a) = b$. Функциональные отношения $R \subseteq A \times B$ известны также как *частичные функции* из A в B.

Отношение R называется *функцией*, если оно функционально и $dom(R) = A$. В этом случае $R(a) = \{b\}$ для единственного b, которое называют значением функции R в точке a и пишут $R(a) = b$. Для функций используется стандартная терминолгия. Функция f из A в B часто обозначается $f : A \to B$. Композиция функций является функцией.

Функции

Отношение $R \subseteq A \times B$ *функционально*, если $\forall a, b, b'(aRb \wedge aRb' \to b = b')$. В этом случае $R(a) = \emptyset$ или $R(a) = \{b\}$ для единственного b; в последнем случае часто пишут $R(a) = b$. Функциональные отношения $R \subseteq A \times B$ известны также как *частичные функции* из A в B.

Отношение R называется *функцией*, если оно функционально и $dom(R) = A$. В этом случае $R(a) = \{b\}$ для единственного b, которое называют значением функции R в точке a и пишут $R(a) = b$. Для функций используется стандартная терминолгия. Функция f из A в B часто обозначается $f : A \to B$. Композиция функций является функцией.

Функция $f : A \to B$ называется инъекцией (сюръекцией), если $\forall a, a_1 \in A(a \neq a_1 \to f(a) \neq f(a_1))$ ($\forall b \in B \exists a \in A(f(a) = b)$). Функция называется биекцией, если она является и инъекцией, и сюръекцией. Биекции из A на A образуют группу относительно композиции.

Предпорядки и эквивалентности

Некоторые важные свойства отношений $R \subseteq A \times A$:

$\forall a \in A(aRa)$ рефлексивность,
$\forall a \in A\neg(aRa)$ антирефлексивность,

$\forall a, b \in A(aRb \to bRa)$ симметричность,
$\forall a, b \in A(aRb \wedge bRa \to a = b)$ антисимметричность,

$\forall a, b, c \in A((aRb \wedge bRc) \to aRc)$ транзитивность

Предпорядки и эквивалентности

Некоторые важные свойства отношений $R \subseteq A \times A$:

$\forall a \in A(aRa)$ рефлексивность,
$\forall a \in A \neg(aRa)$ антирефлексивность,

$\forall a, b \in A(aRb \to bRa)$ симметричность,
$\forall a, b \in A(aRb \wedge bRa \to a = b)$ антисимметричность,

$\forall a, b, c \in A((aRb \wedge bRc) \to aRc)$ транзитивность

Предпорядок = рефлексивность и транзитивность; типичные обозначения $\leq$, $\preceq$, $\subseteq$, $\sqsubseteq$.
Частичный порядок = антисимметричный предпорядок.
Линейный порядок = Частичный порядок +
$\forall a, b \in A(aRb \vee bRa)$.
Строгий частичный порядок = антирефлексивность и транзитивность; типичные обозначения $<$, $\prec$, $\subset$, $\sqsubset$

Эквивалентность = рефлексивность, симметричность и транзитивность; типичные обозначения $=$, $\simeq$, $\equiv$

Эквивалентности и фактор-множества

Пусть $\equiv$ — эквивалентность на A. Каждому $a \in A$ сопоставим множество $[a] \stackrel{\text{def}}{=} \{a' \in A \mid a' \equiv a\}$, называемое его *классом эквивалентности*. Множество $A/_{\equiv}$ всех таких классов называется фактор-множеством множества A по отношению $\equiv$.

Эквивалентности и фактор-множества

Пусть $\equiv$ — эквивалентность на A. Каждому $a \in A$ сопоставим множество $[a] \overset{\text{def}}{=} \{a' \in A \mid a' \equiv a\}$, называемое его *классом эквивалентности*. Множество $A/_{\equiv}$ всех таких классов называется фактор-множеством множества A по отношению $\equiv$.

ТЕОРЕМА. Если $\equiv$ — эквивалентность на A, то классы эквивалентности непусты, попарно не пересекаются и их объединение равно A.

Эквивалентности и фактор-множества

Пусть $\equiv$ — эквивалентность на A. Каждому $a \in A$ сопоставим множество $[a] \stackrel{\text{def}}{=} \{a' \in A \mid a' \equiv a\}$, называемое его *классом эквивалентности*. Множество $A/_{\equiv}$ всех таких классов называется фактор-множеством множества A по отношению $\equiv$.

ТЕОРЕМА. Если $\equiv$ — эквивалентность на A, то классы эквивалентности непусты, попарно не пересекаются и их объединение равно A.

Д-ВО. В качестве объединения классов эквивалентности множество A представляется: любой элемент $a \in A$ эквивалентен самому себе, а значит принадлежит классу $[a]$. Остаётся показать, что разные классы не пересекаются. Покажем, что если $a \in [b] \cap [c]$, то $[b] = [c]$. В самом деле, пусть $b' \in [b]$, тогда $b' \equiv b$. Но также и $a \equiv b$, что по транзитивности означает, что $b' \equiv a$. Аналогично можно показать, что если $c' \in [c]$, то $c' \equiv a$. Отсюда по транзитивности $b' \equiv c'$, т.е. $b' \equiv c$, т.е. $b' \in [c]$. Таким образом, $[b] \subseteq [c]$.

Натуральные числа в теории множеств

Пусть $\mathbb{N}$ — наименьшее по включению множество, содержащее $\emptyset$ и замкнутое относительно операции $x' = x \cup \{x\}$. Можно проверить, что $(\mathbb{N}; \emptyset, ')$ — структура Пеано (т.е. удовлетворяет условиям $x' \neq \emptyset$, $x' = y' \to x = y$, и $[\emptyset \in P \wedge \forall x \in P (x' \in P)] \to P = \mathbb{N}$, для любого $P \subseteq \mathbb{N}$). Такая структура единственна с точностью до изоморфизма.

Натуральные числа в теории множеств

Пусть $\mathbb{N}$ — наименьшее по включению множество, содержащее $\emptyset$ и замкнутое относительно операции $x' = x \cup \{x\}$.
Можно проверить, что $(\mathbb{N}; \emptyset, ')$ — структура Пеано (т.е. удовлетворяет условиям $x' \neq \emptyset$, $x' = y' \to x = y$, и $[\emptyset \in P \wedge \forall x \in P(x' \in P)] \to P = \mathbb{N}$, для любого $P \subseteq \mathbb{N}$). Такая структура единственна с точностью до изоморфизма.

Определим на $\mathbb{N}$ отношение $<$ и операции $+, \cdot$ так:
$x < y \leftrightarrow x \in y$; $+$ — единственная бинарная операция на $\mathbb{N}$ такая, что $x + 0 = x$ и $x + y' = (x + y)'$; $\cdot$ — единственная бинарная операция на $\mathbb{N}$ такая, что $x \cdot 0 = 0$ и $x \cdot y' = x \cdot y + x$.

Натуральные числа в теории множеств

Пусть $\mathbb{N}$ — наименьшее по включению множество, содержащее $\emptyset$ и замкнутое относительно операции $x' = x \cup \{x\}$. Можно проверить, что $(\mathbb{N}; \emptyset, ')$ — структура Пеано (т.е. удовлетворяет условиям $x' \neq \emptyset$, $x' = y' \to x = y$, и $[\emptyset \in P \wedge \forall x \in P(x' \in P)] \to P = \mathbb{N}$, для любого $P \subseteq \mathbb{N}$). Такая структура единственна с точностью до изоморфизма.

Определим на $\mathbb{N}$ отношение $<$ и операции $+, \cdot$ так: $x < y \leftrightarrow x \in y$; $+$ — единственная бинарная операция на $\mathbb{N}$ такая, что $x + 0 = x$ и $x + y' = (x+y)'$; $\cdot$ — единственная бинарная операция на $\mathbb{N}$ такая, что $x \cdot 0 = 0$ и $x \cdot y' = x \cdot y + x$.

Свойства $(\mathbb{N}; +, \cdot, <, 0, 1)$: $+, \cdot$ ассоциативны и коммутативны; $\cdot$ дистрибутивна относительно $+$; $0, 1$ нейтральны относительно $+, \cdot$; $0 < 1 < 2 < \cdots$ и между соседями нет других чисел; $[P(0) \wedge \forall x(P(x) \to P(x+1))] \to \forall x P(x)$; $\forall x(\forall y < x P(y) \to P(x)) \to \forall x P(x)$.

Целые числа в теории множеств

$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/\sim$, где

$(a, b) \sim (c, d) \leftrightarrow a + d = b + c$.

$[a, b]\tilde{+}[c, d] := [a + c, b + d]$,
$[a, b]\tilde{\cdot}[c, d] := [ac + bd, ad + bc]$,

$[a, b]\tilde{\leq}[c, d] \leftrightarrow a + d \leq b + c$,
$\tilde{0} := [0, 0]$, $\tilde{1} := [1, 0]$.

Целые числа в теории множеств

$\mathbb{Z} := (\mathbb{N} \times \mathbb{N})/\sim$, где

$(a, b) \sim (c, d) \leftrightarrow a + d = b + c$.

$[a, b] \tilde{+} [c, d] := [a + c, b + d]$,
$[a, b] \tilde{\cdot} [c, d] := [ac + bd, ad + bc]$,

$[a, b] \tilde{\leq} [c, d] \leftrightarrow a + d \leq b + c$,
$\tilde{0} := [0, 0]$, $\tilde{1} := [1, 0]$.

Свойства $(\mathbb{Z}; \tilde{+}, \tilde{\cdot}, \tilde{\leq}, \tilde{0}, \tilde{1})$:
Это упорядоченное кольцо
(т.е. $\tilde{+}, \tilde{\cdot}$ ассоциативны и коммутативны;
$\tilde{\cdot}$ дистрибутивна относительно $\tilde{+}$;
$\tilde{0}, \tilde{1}$ нейтральны относительно $\tilde{+}, \tilde{\cdot}$;
$\forall x \exists y (x + y = 0)$,
$\forall x, y, z (x \leq y \to (x + z \leq y + z))$,
$\forall x, y, z (x \leq y \wedge 0 < z \to (x \cdot z \leq y \cdot z)))$,
в котором любой элемент является разностью двух натуральных чисел.

Рациональные числа в теории множеств

$\mathbb{Q} := (\mathbb{Z} \times \mathbb{N} \setminus \{0\})/\sim$, где

$(a, b) \sim (c, d) \leftrightarrow ad = bc$.

$[a, b] \tilde{+} [c, d] := [ad + bc, bd]$,
$[a, b] \tilde{\cdot} [c, d] := [ac, bd]$,

$[a, b] \tilde{\leq} [c, d] \leftrightarrow ad \leq bc$,
$\tilde{0} := [0, 1]$, $\tilde{1} := [1, 1]$.

Рациональные числа в теории множеств

$\mathbb{Q} := (\mathbb{Z} \times \mathbb{N} \setminus \{0\})/\sim$, где

$(a, b) \sim (c, d) \leftrightarrow ad = bc$.

$[a, b]\tilde{+}[c, d] := [ad + bc, bd]$,
$[a, b]\tilde{\cdot}[c, d] := [ac, bd]$,

$[a, b]\tilde{\leq}[c, d] \leftrightarrow ad \leq bc$,
$\tilde{0} := [0, 1]$, $\tilde{1} := [1, 1]$.

Свойства $(\mathbb{Q}; \tilde{+}, \tilde{\cdot}, \tilde{\leq}, \tilde{0}, \tilde{1})$:
это упорядоченное поле (т.е. упорядоченное кольцо, в котором $\forall x \neq 0 \exists y (x \cdot y = 1)$)
такое, что любой элемент получается делением целого числа на положительное целое.

Вещественные числа в теории множеств

$\mathbb{R} := S/\sim$, где S — множество всех последовательностей Коши $\{q_i\}$ рациональных чсел (т.е. $\forall n \exists m \forall i, j > m(|q_i - q_j| < 2^{-n})$),

$\{q_i\} \sim \{r_i\} \leftrightarrow \lim_i (q_i - r_i) = 0.$

$[\{q_i\}]\tilde{+}[\{r_i\}] := [\{q_i + r_i\}]$,
$[\{q_i\}]\tilde{\cdot}[\{r_i\}] := [\{q_i \cdot r_i\}]$,

$[\{q_i\}]\tilde{<}[\{r_i\}] \leftrightarrow \exists n, m \forall i > m(q_i - r_i < -2^{-n})$,
$\tilde{0} := [0, 0, \ldots]$, $\tilde{1} := [1, 1, \ldots]$.

Вещественные числа в теории множеств

$\mathbb{R} := S/\sim$, где S — множество всех последовательностей Коши $\{q_i\}$ рациональных чсел
(т.е. $\forall n \exists m \forall i, j > m(|q_i - q_j| < 2^{-n})$),

$\{q_i\} \sim \{r_i\} \leftrightarrow \lim_i (q_i - r_i) = 0.$

$[\{q_i\}]\tilde{+}[\{r_i\}] := [\{q_i + r_i\}]$,
$[\{q_i\}]\tilde{\cdot}[\{r_i\}] := [\{q_i \cdot r_i\}]$,

$[\{q_i\}]\tilde{<}[\{r_i\}] \leftrightarrow \exists n, m \forall i > m(q_i - r_i < -2^{-n})$,
$\tilde{0} := [0, 0, \ldots]$, $\tilde{1} := [1, 1, \ldots]$.

СВОЙСТВА $(\mathbb{R}; \tilde{+}, \tilde{\cdot}, \tilde{\leq}, \tilde{0}, \tilde{1})$:

Это полное упорядоченное поле (т.е. упорядоченное поле, в котором любое непустое ограниченное сверху множество имеет супремум).

Комплексные числа в теории множеств

$$\mathbb{C} := \mathbb{R} \times \mathbb{R},$$

$$(x, y) \tilde{+} (x_1, y_1) := (x + x_1, y + y_1),$$

$$(x, y) \tilde{\cdot} (x_1, y_1) := (xx_1 - yy_1, xy_1 + yx_1),$$

$$\tilde{0} := (0, 0),\ \tilde{1} := (1, 0),\ \tilde{i} := (0, 1),$$

Комплексные числа в теории множеств

$\mathbb{C} := \mathbb{R} \times \mathbb{R}$,

$(x, y)\tilde{+}(x_1, y_1) := (x + x_1, y + y_1)$,

$(x, y)\tilde{\cdot}(x_1, y_1) := (xx_1 - yy_1, xy_1 + yx_1)$,

$\tilde{0} := (0, 0)$, $\tilde{1} := (1, 0)$, $\tilde{i} := (0, 1)$,

СВОЙСТВА $(\mathbb{C}; \tilde{+}, \tilde{\cdot}, \tilde{0}, \tilde{1})$:

Это поле, содержащее копию поля вещественных чисел $\tilde{\mathbb{R}} := \{(x, 0) \mid x \in \mathbb{R}\})$, в котором есть квадратный корень i из -1, и в котором каждый элемент представим в виде $x + i \cdot y$, $x, y \in \tilde{\mathbb{R}}$.

Мощность множества

О мощности множества можно думать, как о количестве его элементов. Однако непонятно, как быть с бесконечными множествами.

Мощность множества

О мощности множества можно думать, как о количестве его элементов. Однако непонятно, как быть с бесконечными множествами.

ОПРЕДЕЛЕНИЕ. 1. A и B равномощны ($A \sim B$), если существует биекция $f : A \to B$.
2. A не превосходит по мощности B ($A \preceq B$), если существует инъекция $f : A \to B$.
3. A меньше по мощности B ($A \prec B$), если $A \preceq B$ и $A \not\sim B$.

Мощность множества

О мощности множества можно думать, как о количестве его элементов. Однако непонятно, как быть с бесконечными множествами.

ОПРЕДЕЛЕНИЕ. 1. A и B равномощны ($A \sim B$), если существует биекция $f : A \to B$.
2. A не превосходит по мощности B ($A \preceq B$), если существует инъекция $f : A \to B$.
3. A меньше по мощности B ($A \prec B$), если $A \preceq B$ и $A \not\sim B$.

СВОЙСТВА. 1. Отношение $\sim$ рефлексивно, симметрично и транзитивно.
2. Отношение $\preceq$ рефлексивно и транзитивно.

Мощность множества

О мощности множества можно думать, как о количестве его элементов. Однако непонятно, как быть с бесконечными множествами.

ОПРЕДЕЛЕНИЕ. 1. A и B равномощны ($A \sim B$), если существует биекция $f : A \to B$.
2. A не превосходит по мощности B ($A \preceq B$), если существует инъекция $f : A \to B$.
3. A меньше по мощности B ($A \prec B$), если $A \preceq B$ и $A \nsim B$.

СВОЙСТВА. 1. Отношение $\sim$ рефлексивно, симметрично и транзитивно.
2. Отношение $\preceq$ рефлексивно и транзитивно.

Заметим, что $\sim$ "неформально" является отношением эквивалентности, но ввести фактор-множество нельзя, так как множества всех множеств не существует (покажем позже).

Теорема Шрёдера-Бернштейна

ТЕОРЕМА. Если $A \preceq B$ и $B \preceq A$, то $A \sim B$.

Теорема Шрёдера-Бернштейна

ТЕОРЕМА. Если $A \preceq B$ и $B \preceq A$, то $A \sim B$.

Д-во. Пусть $f : A \to B$ и $g : B \to A$ — инъекции. Тогда $h = g \circ f : A \to A$ — инъекция.

Пусть $A_1 = g(B), A_2 = h(A)$. Заметим, что $A_2 \subseteq A_1 \subseteq A$ и $A_1 \sim B$, потому что $g : B \to A_1$ — биекция. Аналогично $h : A \to A_2$ — биекция.
Достаточно доказать, что $A \sim A_1$.

Теорема Шрёдера-Бернштейна

ТЕОРЕМА. Если $A \preceq B$ и $B \preceq A$, то $A \sim B$.

Д-во. Пусть $f : A \to B$ и $g : B \to A$ — инъекции. Тогда $h = g \circ f : A \to A$ — инъекция.

Пусть $A_1 = g(B), A_2 = h(A)$. Заметим, что $A_2 \subseteq A_1 \subseteq A$ и $A_1 \sim B$, потому что $g : B \to A_1$ — биекция. Аналогично $h : A \to A_2$ — биекция.
Достаточно доказать, что $A \sim A_1$.

Множество $X \subseteq A$ назовем хорошим, если $X \supseteq (A \setminus A_1) \cup h(X)$ (например, A хорошее). Пересечение хороших множеств — хорошее.

Пусть C — пересечение всех хороших множеств. Тогда C хорошее, $C = (A \setminus A_1) \cup h(C)$, и $h(C) \subseteq A_2$.

Поэтому $id_{A \setminus C} \cup h|_C$ — биекция из A на A_1.

Теорема Кантора

ТЕОРЕМА. Для любого множества A справедливо $A \prec P(A)$, т.е. $A \preceq P(A)$ и $A \not\sim P(A)$.

Теорема Кантора

ТЕОРЕМА. Для любого множества A справедливо $A \prec P(A)$, т.е. $A \preceq P(A)$ и $A \not\sim P(A)$.

ДОКАЗАТЕЛЬСТВО. $A \preceq P(A)$, поскольку $a \mapsto \{a\}$ — инъекция из A в $P(A)$.

Теперь докажем, что $A \not\sim P(A)$. Предположим противное: $A \sim P(A)$, тогда есть биекция $g : A \to P(A)$.

Рассмотриим множество $B = \{a \in A \mid a \notin g(a)\}$. Поскольку $B \in P(A)$, $B = g(a)$ для некоторого $a \in A$. Но тогда

$$a \in B \leftrightarrow a \in g(a) \leftrightarrow a \notin B,$$

противоречие.

Конечные множества

Множество называется конечным, если оно равномощно n для некоторого $n \in \mathbb{N}$. Множества, не являющиеся конечными, называются бесконечными.

Конечные множества

Множество называется конечным, если оно равномощно n для некоторого $n \in \mathbb{N}$. Множества, не являющиеся конечными, называются бесконечными.

ТЕОРЕМА. Для множества A равносильны условия:

1. A конечно.

2. Любое непустое подмножество булеана $P(A)$ имеет максимальный элемент по включению.

3. Любая инъекция $f : A \to A$ является биекцией.

Конечные множества

Множество называется конечным, если оно равномощно n для некоторого $n \in \mathbb{N}$. Множества, не являющиеся конечными, называются бесконечными.

ТЕОРЕМА. Для множества A равносильны условия:

1. A конечно.

2. Любое непустое подмножество булеана $P(A)$ имеет максимальный элемент по включению.

3. Любая инъекция $f : A \to A$ является биекцией.

ТЕОРЕМА. Если A конечно и B бесконечно, то $A \prec B$.

Счетные и несчетные множества

Множество называется счетным, если оно равномощно $\mathbb{N}$. Множества, не являющиеся конечными или счетными, называются несчетными.
Множество называется континуальным, если оно равномощно $P(\mathbb{N})$.

Счетные и несчетные множества

Множество называется счетным, если оно равномощно $\mathbb{N}$. Множества, не являющиеся конечными или счетными, называются несчетными.
Множество называется континуальным, если оно равномощно $P(\mathbb{N})$.

ТЕОРЕМА. Если A счетно и B бесконечно, то $A \preceq B$.

Счетные и несчетные множества

Множество называется счетным, если оно равномощно $\mathbb{N}$.
Множества, не являющиеся конечными или счетными, называются несчетными.
Множество называется континуальным, если оно равномощно $P(\mathbb{N})$.

ТЕОРЕМА. Если A счетно и B бесконечно, то $A \preceq B$.

Шкала мощностей: 0,1,2,..., счетные, несчетные.

Счетные и несчетные множества

Множество называется счетным, если оно равномощно $\mathbb{N}$.
Множества, не являющиеся конечными или счетными, называются несчетными.
Множество называется континуальным, если оно равномощно $P(\mathbb{N})$.

ТЕОРЕМА. Если A счетно и B бесконечно, то $A \preceq B$.

Шкала мощностей: 0,1,2,..., счетные, несчетные.

Континнум-гипотеза (первая проблема Гильберта): если A несчетно, то $P(\mathbb{N}) \preceq A$.

Более простая, но нетривиальная задача: верно ли, что $\forall A, B (A \preceq B \vee B \preceq A)$?

Противоречия наивной теории множеств

Пусть $V = \{x \mid x = x\}$ — множество всех множеств. Тогда $P(V) \subseteq V$, поэтому $P(V) \preceq V$. Однако по теореме Кантора $V \prec P(V)$ — противоречие.

Противоречия наивной теории множеств

Пусть $V = \{x \mid x = x\}$ — множество всех множеств. Тогда $P(V) \subseteq V$, поэтому $P(V) \preceq V$. Однако по теореме Кантора $V \prec P(V)$ — противоречие.

Рассмотрим множество $Y = \{x \mid x \notin x\}$. Имеем $Y \in Y \leftrightarrow Y \notin Y$ — противоречие.

Противоречия наивной теории можеств

Пусть $V = \{x \mid x = x\}$ — множество всех множеств. Тогда $P(V) \subseteq V$, поэтому $P(V) \preceq V$. Однако по теореме Кантора $V \prec P(V)$ — противоречие.

Рассмотрим множество $Y = \{x \mid x \notin x\}$. Имеем $Y \in Y \leftrightarrow Y \notin Y$ — противоречие.

Из каждого из этих противоречий (известных также как парадоксы) можно вывести вообще все возможные утверждения, и истинные, и ложные. Звучит неприятно.

Можно было бы, конечно, разочароваться в самой идее построения оснований математики, но мыслители начала XX века всё-таки не сдались и придумали ряд выходов из положения, предполагающих создание аксиоматической теории множеств, учитывающей ошибки наивного подхода и дающей надежные основания математики.

Множества и классы

Формулы аксиоматической теории множеств строятся так же, как и раньше: с помощью логических операций из простейших формул $x = y, x \in y$; переменные в формулах обозначают множества. Разница с наивной теорией множест состоит в ограничении способов построения множеств. Например, парадоксы показывают, что выражение $\{x \mid \varphi(x)\}$ для некоторых формул не может задавать множества.

Множества и классы

Формулы аксиоматической теории множеств строятся так же, как и раньше: с помощью логических операций из простейших формул $x = y, x \in y$; переменные в формулах обозначают множества. Разница с наивной теорией множест состоит в ограничении способов построения множеств. Например, парадоксы показывают, что выражение $\{x \mid \varphi(x)\}$ для некоторых формул не может задавать множества.

Удобно считать, что такие выражения задают классы $C_\varphi = \{x \mid \varphi(x)\}$, т.е. совокупности объектов x, для которых $\varphi(x)$ истинно. Любое множество является классом, но обратное неверно (например, классы V, Y с предыдущего слайда не являются множествами). Элемент класса всегда является множеством.

Множества и классы

Формулы аксиоматической теории множеств строятся так же, как и раньше: с помощью логических операций из простейших формул $x = y, x \in y$; переменные в формулах обозначают множества. Разница с наивной теорией множест состоит в ограничении способов построения множеств. Например, парадоксы показывают, что выражение $\{x \mid \varphi(x)\}$ для некоторых формул не может задавать множества.

Удобно считать, что такие выражения задают классы $C_\varphi = \{x \mid \varphi(x)\}$, т.е. совокупности объектов x, для которых $\varphi(x)$ истинно. Любое множество является классом, но обратное неверно (например, классы V, Y с предыдущего слайда не являются множествами). Элемент класса всегда является множеством.

Для классов можно определить булевские операции $A \cup B, A \cap B, A \setminus B$, что на самом деле просто модифицирует задающие классы формулы. Так, $A \cap B = \{x \mid \phi_A(x) \wedge \phi_B(x)\}$.

Аксиомы ZFC

0. $\exists x(x = x)$.
1. $\forall u(u \in X \leftrightarrow u \in Y) \to X = Y$.
2. $\forall u \forall v \exists x \forall z(z \in x \leftrightarrow z = u \vee z = v)$.
3. $\forall X \exists Y \forall u(u \in Y \leftrightarrow u \in X \wedge \varphi(u))$.
4. $\forall X \exists Y \forall u \forall z(u \in z \wedge z \in X \to u \in Y)$.
5. $\forall X \exists Y \forall u(u \in Y \leftrightarrow u \subseteq X)$.

6. $\forall x \forall y \forall y'(\varphi(x, y) \wedge \varphi(x, y') \to y = y')$
$\to \forall X \exists Y \forall x \forall y(x \in X \wedge \varphi(x, y) \to y \in Y)$.

7. $\exists Y(\emptyset \in Y \wedge \forall y(y \in Y \to y \cup \{y\} \in Y))$.

8. $\forall X(X \neq \emptyset \to \exists x(x \in X \wedge \forall u(u \in x \to u \notin X)))$.

9. $\forall X \exists f((f : (P(X) \setminus \{\emptyset\}) \to X) \wedge \forall Y(Y \subseteq X \wedge Y \neq \emptyset \to$
$f(Y) \in Y))$.

Примеры следствий аксиом ZFC

1. Существует упорядоченная пара любых двух множеств.
2. Существует пустое множество.
3. Существует объединение всех элементов любого множества, а также пересечение всех элементов данного непустого множества.
4. Существуют объединение, пересечение и разность любых двух данных множеств.

Примеры следствий аксиом ZFC

1. Существует упорядоченная пара любых двух множеств.
2. Существует пустое множество.
3. Существует объединение всех элементов любого множества, а также пересечение всех элементов данного непустого множества.
4. Существуют объединение, пересечение и разность любых двух данных множеств.

5. Теорема о фактор-множестве.
6. Существует декартово произведение любых двух данных множеств.
7. Теоремы Кантора и Шрёдера-Бернштейна.
8. Существует наименьшее по включению индуктивное множество.
9. Существуют изоморфные копии всех числовых структур.

Фундированные порядки

ОПР. 1. Частичный порядок $\mathbb{A} = (A; <_A)$ называют фундированным, если любое непустое подмножество его элементов содержит минимальный элемент.
2. Фундированные линейные порядки называют также вполне упорядоченными множествами.
3. Начальным сегментом $\mathbb{A} = (A; <_A)$ называют любое подмножество A, замкнутое вниз относительно $<_A$. Пример — множество $\hat{a} = \{x \mid x <_A a\}$ для любого $a \in A$.

Фундированные порядки

ОПР. 1. Частичный порядок $\mathbb{A} = (A; <_A)$ называют фундированным, если любое непустое подмножество его элементов содержит минимальный элемент.
2. Фундированные линейные порядки называют также вполне упорядоченными множествами.
3. Начальным сегментом $\mathbb{A} = (A; <_A)$ называют любое подмножество A, замкнутое вниз относительно $<_A$. Пример — множество $\hat{a} = \{x \mid x <_A a\}$ для любого $a \in A$.

ОПР. 1. Изоморфизмом $\mathbb{A}$ на $\mathbb{B}$ называется биекция $f : A \to B$ такая, что $a <_A a_1 \leftrightarrow f(a) <_B f(a_1)$ для любых $a, a_1 \in A$. Инъекция с таким свойством называется вложением $\mathbb{A}$ в $\mathbb{B}$.
2. Частичные порядки $\mathbb{A}$ и $\mathbb{B}$ называются изоморфными ($\mathbb{A} \simeq \mathbb{B}$), если существует изоморфизм $\mathbb{A}$ на $\mathbb{B}$.
3. Запись $\mathbb{A} \sqsubseteq \mathbb{B}$ ($\mathbb{A} \sqsubset \mathbb{B}$) означает, что $\mathbb{A}$ изоморфно некоторому (собственному) начальному сегменту $\mathbb{B}$.

Свойства вполне упорядоченных множеств

1. Отношение $\simeq$ рефлексивно, симметрично и транзитивно.
2. Отношение $\sqsubseteq$ рефлексивно и транзитивно.
3. Для любого вложения $f : \mathbb{A} \to \mathbb{A}$ верно: $\forall a(a \leq_A f(a))$.
4. Отношение $\sqsubset$ антирефлексивно и транзитивно.
5. $\mathbb{A} \sqsubseteq \mathbb{B}$ или $\mathbb{B} \sqsubseteq \mathbb{A}$.
6. $\mathbb{A} \simeq \mathbb{B}$ или $\mathbb{A} \sqsubset \mathbb{B}$ или $\mathbb{B} \sqsubset \mathbb{A}$, причем выполняется ровно одно из условий.
7. Если $\mathbb{A} \sqsubseteq \mathbb{B}$ и $\mathbb{B} \sqsubseteq \mathbb{A}$, то $\mathbb{A} \simeq \mathbb{B}$.

Доказательства свойств в.у.м.

3. Пусть нет: $f(a) <_A a$ для некоторого $a \in A$, и возьмем наименьшее a. Тогда $f(f(a)) <_A f(a) <_A a$ — противоречие.

4. Пусть $\sqsubset$ не антирефлексивно, т.е. $\mathbb{A} \sqsubset \mathbb{A}$ для некоторого $\mathbb{A}$. Тогда $f : \mathbb{A} \simeq \hat{a}$ для некоторых $a \in A$ и f. Тогда $f(a) <_A a$ — противоречие.

5. Отношение $I = \{(a, b) \mid \hat{a} \simeq \hat{b}\}$, а также обратное отношение I^{-1}, функциональны. Поэтому I — биекция из $D = dom(I)$ на $R = rng(I)$. Если $a_1 <_A a \in D$, то существует $f : \hat{a} \simeq \widehat{I(a)}$, откуда $\hat{a_1} \simeq \widehat{f(a_1)}$, а значит $I(a_1) = f(a_1) <_B I(a)$. Поэтому D — начальный сегмент $\mathbb{A}$, R — начальный сегмент $\mathbb{B}$, и ограничение $I|_D$ — изоморфизм из $\mathbb{D}$ на $\mathbb{R}$.
Заметим, что $D = A$ или $R = B$ (в противном случае $D = \hat{d}$ и $R = \hat{r}$ для некоторых $d \in A$ и $r \in B$, откуда $I(d) = r$ и $d \in D$ — противоречие). В случае $D = A$ получаем $\mathbb{A} \sqsubseteq \mathbb{B}$, а в случае $R = B$ получаем $\mathbb{B} \sqsubseteq \mathbb{A}$.

Фундированность и индукция

ТЕОРЕМА. Фундированность порядка $(X;<)$ равносильна правилу индукции в $(X;<)$, утверждающему, что для любого свойства $P(x)$ элементов множества X выполняется условие $\forall x(\forall y<xP(y)\to P(x))\to\forall xP(x)$.

Фундированность и индукция

ТЕОРЕМА. Фундированность порядка $(X;<)$ равносильна правилу индукции в $(X;<)$, утверждающему, что для любого свойства $P(x)$ элементов множества X выполняется условие $\forall x(\forall y<xP(y)\to P(x))\to\forall xP(x)$.

Теорема справедлива для произвольных фундированных отношений. Отношение $\rho\subseteq X\times X$ называется фундированным, если любое непустое множество $A\subseteq X$ имеет минимальный элемент $a\in A$ (т.е. не существует $b\in A$ такого, что $b\rho a$). Это верно и для случая, когда X является классом (например, это верно для фундированного отношени $\in$ на классе V всех множеств).

Фундированность и индукция

ТЕОРЕМА. Фундированность порядка $(X;<)$ равносильна правилу индукции в $(X;<)$, утверждающему, что для любого свойства $P(x)$ элементов множества X выполняется условие $\forall x(\forall y < xP(y) \to P(x)) \to \forall xP(x)$.

Теорема справедлива для произвольных фундированных отношений. Отношение $\rho \subseteq X \times X$ называется фундированным, если любое непустое множество $A \subseteq X$ имеет минимальный элемент $a \in A$ (т.е. не существует $b \in A$ такого, что $b\rho a$). Это верно и для случая, когда X является классом (например, это верно для фундированного отношени $\in$ на классе V всех множеств).

Нетрудно показать, что на фундированных множествах и классах можно также определять функции по рекурсии; важный частный случай рассмотрим ниже.

Ординалы

ОПРЕДЕЛЕНИЕ. 1. Множество S называется транзитивным, если $\bigcup S \subseteq S$, т.е. $x \in y \in S \to x \in S$.

Ординалы

ОПРЕДЕЛЕНИЕ. 1. Множество S называется транзитивным, если $\bigcup S \subseteq S$, т.е. $x \in y \in S \to x \in S$.

2. Множество S называется ординалом, если оно транзитивно и линейно упорядочено (эквивалентно, вполне упорядочено) отношением $\in$, т.е. $\forall x, y \in S (x \in y \vee y \in x \vee x = y)$.

Ординалы

ОПРЕДЕЛЕНИЕ. 1. Множество S называется транзитивным, если $\bigcup S \subseteq S$, т.е. $x \in y \in S \to x \in S$.

2. Множество S называется ординалом, если оно транзитивно и линейно упорядочено (эквивалентно, вполне упорядочено) отношением $\in$, т.е. $\forall x, y \in S(x \in y \vee y \in x \vee x = y)$.

3. Ординалы обозначаем $\alpha, \beta, \gamma, \ldots$,
класс всех ординалов обозначаем Ord,
сужение отношения $\in$ на Ord обозначаем $<$.

Свойства ординалов

1. $x \in \alpha \to x \in Ord$.
2. $\alpha = \{\beta \mid \beta < \alpha\}$.
3. $(\alpha; <) \simeq (\beta; <) \iff \alpha = \beta$.
4. $\alpha < \beta \vee \beta < \alpha \vee \alpha = \beta$.
5. $\alpha \subseteq \beta \iff \alpha \leq \beta$.
6. $\alpha + 1 = \alpha \cup \{\alpha\}$ — наименьший ординал, больший α.
7. Для любого множества A ординалов, $(A; <)$ есть в.у.м., а $\bigcup A$ — ординал, являющийся супремумом этого множества.
8. Класс Ord не является множеством.
9. Любое в.у.м. $\mathbb{A}$ изоморфно единственному ординалу.

Доказательства свойств ординалов

3. Проверим, что $\alpha \simeq \beta \to \alpha = \beta$. Пусть $f : \alpha \simeq \beta$; достаточно показать $\alpha \subseteq \beta$, а для этого достаточно $\forall x \in \alpha(x = f(x))$. Пусть нет, т.е. $x \neq f(x)$ для некоторого (наименьшего) $x \in \alpha$. Тогда $x = \{z \mid z < x\}$. С другой стороны, $f(x) = \{f(z) \mid z < x\}$, откуда $x = f(x)$, противоречие.

Доказательства свойств ординалов

3. Проверим, что $\alpha \simeq \beta \to \alpha = \beta$. Пусть $f : \alpha \simeq \beta$; достаточно показать $\alpha \subseteq \beta$, а для этого достаточно $\forall x \in \alpha (x = f(x))$. Пусть нет, т.е. $x \neq f(x)$ для некоторого (наименьшего) $x \in \alpha$. Тогда $x = \{z \mid z < x\}$. С другой стороны, $f(x) = \{f(z) \mid z < x\}$, откуда $x = f(x)$, противоречие.

7. Первое — по аксиоме фундирования.
Для второго достаточно транзитивности $\bigcup A$. Пусть $x \in y \in \bigcup A$. Тогда $\exists \alpha \in A (y \in \alpha)$. Тогда $x \in \alpha$ по транзитивности, откуда $x \in \bigcup A$. $\bigcup A$ — верхняя граница A по отношению $<$, поскольку $\forall \alpha \in A (\alpha \leq \bigcup A)$ и $\leq = \subseteq$. Остается д-ть, что $\bigcup A \leq \beta$ для любой верхней границы β для A. Это так, поскольку $\forall \alpha \in A (\alpha \subseteq \beta)$.

Доказательства свойств ординалов

3. Проверим, что $\alpha \simeq \beta \to \alpha = \beta$. Пусть $f : \alpha \simeq \beta$; достаточно показать $\alpha \subseteq \beta$, а для этого достаточно $\forall x \in \alpha(x = f(x))$. Пусть нет, т.е. $x \neq f(x)$ для некоторого (наименьшего) $x \in \alpha$. Тогда $x = \{z \mid z < x\}$. С другой стороны, $f(x) = \{f(z) \mid z < x\}$, откуда $x = f(x)$, противоречие.

7. Первое — по аксиоме фундирования.
Для второго достаточно транзитивности $\bigcup A$. Пусть $x \in y \in \bigcup A$. Тогда $\exists \alpha \in A(y \in \alpha)$. Тогда $x \in \alpha$ по транзитивности, откуда $x \in \bigcup A$. $\bigcup A$ — верхняя граница A по отношению $<$, поскольку $\forall \alpha \in A(\alpha \leq \bigcup A)$ и $\leq = \subseteq$. Остается д-ть, что $\bigcup A \leq \beta$ для любой верхней границы β для A. Это так, поскольку $\forall \alpha \in A(\alpha \subseteq \beta)$.

9. Рассмотрим $I = \{(a, \alpha) \mid \hat{a} \simeq \alpha\}$. Как для в.у.м., I — изоморфизм $\mathbb{D}$ на $\mathbb{R}$ для начальных сегментов $D \subseteq A$, $R \subseteq Ord$ причем $D = A$ или $R = Ord$. Последнее невозможно (поскольку Ord было бы множеством), значит $D = A$ и I — искомый изоморфизм на ординал R.

Рекурсия по ординалам

ТЕОРЕМА. Для любой функции-класса $G : V \to V$ существует единственная функция-класс $F : Ord \to V$ такая, что $F(\alpha) = G\left(F\big|_\alpha\right)$, где $F\big|_\alpha$ — ограничение F на α, т.е. $F\big|_\alpha = \{(\beta, y) \in F \mid \beta < \alpha\}$.

Рекурсия по ординалам

ТЕОРЕМА. Для любой функции-класса $G : V \to V$ существует единственная функция-класс $F : Ord \to V$ такая, что $F(\alpha) = G\left(F\big|_\alpha\right)$, где $F\big|_\alpha$ — ограничение F на α, т.е. $F\big|_\alpha = \{(\beta, y) \in F \mid \beta < \alpha\}$.

Д-ВО. Единственность: пусть есть две такие функции F, F', проверим $\forall \alpha \in Ord : F(\alpha) = F'(\alpha)$. Предположим, что это не так и возьмём наименьшее α такое, что $F(\alpha) \neq F'(\alpha)$. Тогда $F\big|_\alpha = F'\big|_\alpha$, откуда $F(\alpha) = G\left(F\big|_\alpha\right) = F'(\alpha)$ — противоречие.

Рекурсия по ординалам

ТЕОРЕМА. Для любой функции-класса $G : V \to V$ существует единственная функция-класс $F : Ord \to V$ такая, что $F(\alpha) = G\left(F\big|_\alpha\right)$, где $F\big|_\alpha$ — ограничение F на α, т.е. $F\big|_\alpha = \{(\beta, y) \in F \mid \beta < \alpha\}$.

Д-ВО. Единственность: пусть есть две такие функции F, F', проверим $\forall \alpha \in Ord : F(\alpha) = F'(\alpha)$. Предположим, что это не так и возьмём наименьшее α такое, что $F(\alpha) \neq F'(\alpha)$. Тогда $F\big|_\alpha = F'\big|_\alpha$, откуда $F(\alpha) = G\left(F\big|_\alpha\right) = F'(\alpha)$ — противоречие.

Существование: рассмотрим класс функций $C = \{f : \alpha \to V \mid \alpha \in Ord, \forall \beta < \alpha (f(\beta) = G(f|_\beta))\}$. Заметим, что если $f, f' \in C$, то $f \subseteq f' \vee f' \subseteq f$. Утверждается, что $F = \bigcup C$ годится, в частности, $dom(F) = Ord$. В самом деле, если $\alpha \notin dom(F)$ для наименьшего α, то $f = F\big|_\alpha \in C$, откуда $\tilde{f} = f \cup \{(\alpha, G(f))\} \in C$ — противоречие.

Эквиваленты аксиомы выбора

Пусть ZF — множество аксиом 0 – 8 (т.е. все аксиомы, кроме аксиомы выбора AC).

ЛЕММОЙ ЦОРНА (ZL) называется утверждение: Если любое линейно упорядоченное подмножество частичного порядка $\mathbb{X}$ имеет верхнюю границу, то в $\mathbb{X}$ есть максимальный элемент.

ТЕОРЕМОЙ ЦЕРМЕЛО (ZT) называется утверждение: Любое множество можно вполне упорядочить, т.е. на любом множестве A существует фундированный линейный порядок.

Эквиваленты аксиомы выбора

Пусть ZF — множество аксиом 0 – 8 (т.е. все аксиомы, кроме аксиомы выбора AC).

ЛЕММОЙ ЦОРНА (ZL) называется утверждение: Если любое линейно упорядоченное подмножество частичного порядка $\mathbb{X}$ имеет верхнюю границу, то в $\mathbb{X}$ есть максимальный элемент.

ТЕОРЕМОЙ ЦЕРМЕЛО (ZT) называется утверждение: Любое множество можно вполне упорядочить, т.е. на любом множестве A существует фундированный линейный порядок.

ТЕОРЕМА. Из аксиом ZF следует эквивалентность аксиомы выбора, леммы Цорна, и теоремы Цермело.

Эквиваленты аксиомы выбора

Пусть ZF — множество аксиом 0 – 8 (т.е. все аксиомы, кроме аксиомы выбора AC).

ЛЕММОЙ ЦОРНА (ZL) называется утверждение: Если любое линейно упорядоченное подмножество частичного порядка $\mathbb{X}$ имеет верхнюю границу, то в $\mathbb{X}$ есть максимальный элемент.

ТЕОРЕМОЙ ЦЕРМЕЛО (ZT) называется утверждение: Любое множество можно вполне упорядочить, т.е. на любом множестве A существует фундированный линейный порядок.

ТЕОРЕМА. Из аксиом ZF следует эквивалентность аксиомы выбора, леммы Цорна, и теоремы Цермело.

Доказательство по схеме AC $\Longrightarrow$ ZL $\Longrightarrow$ ZT $\Longrightarrow$ AC.

Аксиома выбора влечет лемму Цорна

Пусть AC истинна, а ZL ложна, тогда существует чум $\mathbb{X}$, в котором любое л.у.м. $L \subseteq X$ имеет верхнюю границу, и $\forall x \exists y (x <_X y)$. Тогда $\forall L \exists y (L <_X y)$, т.е. $B(L) = \{y \in X \mid L <_X y\} \neq \emptyset$ для любого л.у.м. $L \subseteq X$. Пусть f — функция выбора на X, и $g(L) = f(B(L))$. Тогда $L <_X g(L)$ для любого л.у.м. $L \subseteq X$.

Аксиома выбора влечет лемму Цорна

Пусть AC истинна, а ZL ложна, тогда существует чум $\mathbb{X}$, в котором любое л.у.м. $L \subseteq X$ имеет верхнюю границу, и $\forall x \exists y (x <_X y)$. Тогда $\forall L \exists y (L <_X y)$, т.е. $B(L) = \{y \in X \mid L <_X y\} \neq \emptyset$ для любого л.у.м. $L \subseteq X$. Пусть f — функция выбора на X, и $g(L) = f(B(L))$. Тогда $L <_X g(L)$ для любого л.у.м. $L \subseteq X$.

Определим функцию-класс $F : Ord \to X$ рекурсией: $F(\alpha) = g(F\big|_\alpha)$ и заметим, что F — вложение частичных порядков (поскольку $\beta < \alpha \to F(\beta) <_X F(\alpha)$), в частности инъекция. По аксиоме выделения, $R = rng(F) \subseteq X$ — множество. Поскольку F^{-1} — биекция из R на Ord, Ord по аксиоме замены есть множество. Противоречие.

Лемма Цорна влечет теорему Цермело

Пусть лемма Цорна верна, надо проверить, что на любом множестве A существует фундированный линейный порядок. Рассмотрим класс X всех инъекций $f : \alpha \to A$, $\alpha \in Ord$. Любому $f \in X$ сопоставим в.у.м. $\mathbb{A}_f = (f(\alpha); \sqsubset)$, $a \sqsubset a_1 \leftrightarrow f^{-1}(a) < f^{-1}(a_1)$. По аксиоме выделения $\mathcal{X} = \{\mathbb{A}_f \mid f \in X\}$ — множество. Поскольку $\alpha \simeq \mathbb{A}_f$ и X — область значений функции $\mathbb{A}_f \mapsto f$, определенной на $\mathcal{X}$, X есть множество по аксиоме замены.

Лемма Цорна влечет теорему Цермело

Пусть лемма Цорна верна, надо проверить, что на любом множестве A существует фундированный линейный порядок. Рассмотрим класс X всех инъекций $f : \alpha \to A$, $\alpha \in Ord$. Любому $f \in X$ сопоставим в.у.м. $\mathbb{A}_f = (f(\alpha); \sqsubset)$, $a \sqsubset a_1 \leftrightarrow f^{-1}(a) < f^{-1}(a_1)$. По аксиоме выделения $\mathcal{X} = \{\mathbb{A}_f \mid f \in X\}$ — множество. Поскольку $\alpha \simeq \mathbb{A}_f$ и X — область значений функции $\mathbb{A}_f \mapsto f$, определенной на $\mathcal{X}$, X есть множество по аксиоме замены.

В чуме $(X; \subseteq)$ всякое л.у.м. $L \subseteq X$ имеет верхнюю границу $\bigcup L$. По лемме Цорна $(X; \subseteq)$ имеет максимальный элемент $f : \alpha \to A$. Заметим, что $rng(f) = A$ (иначе, $f \cup \{(\alpha, a)\}$, где $a \in A \setminus rng(f)$, — собственное расширение f, противоречие). Поскольку $\alpha \simeq \mathbb{A}_f$, $\sqsubset$ — фундированный линейный порядок на A.

Теорема Цермело влечет аксиому выбора

Предполагая теорему Цермело, покажем, что на любом множестве A существует функция выбора $f : P(A) \setminus \{\emptyset\} \to A$, $f(X) \in X$. По теореме Цермело, существует фундированный линейный порядок $<_A$ на A. Для непустого $X \subseteq A$ определим $f(X)$ как $<_A$-наименьший элемент множества X. Иными словами, $f = \{(X, x) \mid x \in X \subseteq A \wedge \forall y <_A x(y \notin X)\}$.

Теорема Цермело влечет аксиому выбора

Предполагая теорему Цермело, покажем, что на любом множестве A существует функция выбора $f : P(A) \setminus \{\emptyset\} \to A$, $f(X) \in X$. По теореме Цермело, существует фундированный линейный порядок $<_A$ на A. Для непустого $X \subseteq A$ определим $f(X)$ как $<_A$-наименьший элемент множества X. Иными словами, $f = \{(X, x) \mid x \in X \subseteq A \wedge \forall y <_A x (y \notin X)\}$.

Теперь можем легко доказать, что в теории ZFC доказуема сравнимость любых двух множеств по мощности.

ТЕОРЕМА. Для любых множеств A и B имеем: $A \preceq B \vee B \preceq A$.

Д-ВО. По теореме Цермело, существуют фундированные линейные порядки $<_A$ на A и $<_B$ на B. По свойству в.у.м., $\mathbb{A} \sqsubseteq \mathbb{B} \vee \mathbb{B} \sqsubseteq \mathbb{A}$. Отсюда следует заключение теоремы.

Числа, измеряющие мощность множеств

ОПРЕДЕЛЕНИЕ. 1. Мощность множества A — наименьший ординал $|A|$, равномощный A.
2. Кардинал — ординал, не равномощный никакому меньшему ординалу. Класс всех кардиналов обозначается $Card$.
3. Шкала ординалов — упорядоченный класс $(Ord; <)$.
4. Шкала кардиналов — упорядоченный класс $(Card; <)$.
5. Для любого кардинала $\varkappa$ существует наименьший кардинал, больший $\varkappa$; он обозначается $\varkappa^+$.

Числа, измеряющие мощность множеств

ОПРЕДЕЛЕНИЕ. 1. Мощность множества A — наименьший ординал $|A|$, равномощный A.
2. Кардинал — ординал, не равномощный никакому меньшему ординалу. Класс всех кардиналов обозначается $Card$.
3. Шкала ординалов — упорядоченный класс $(Ord; <)$.
4. Шкала кардиналов — упорядоченный класс $(Card; <)$.
5. Для любого кардинала $\varkappa$ существует наименьший кардинал, больший $\varkappa$; он обозначается $\varkappa^+$.

Любое в.у.м. $\mathbb{A}$ изоморфно единственному ординалу $o(\mathbb{A})$, а любое множество равномощно единственному кардиналу. Ординалы — числа, измеряющие в.у.м., а кардиналы — числа, измеряющие мощность множества. Заметим, что каждый кардинал является ординалом, но не наоборот.
Начало шкалы ординалов:
$0, 1, 2, \ldots, \mathbb{N} = \omega, \omega + 1, \omega + 2, \ldots, \omega + \omega, \ldots.$
Начало шкалы кардиналов: $0, 1, 2, \ldots, \omega, \omega^+, (\omega^+)^+, \ldots.$

Шкалы ординалов и кардиналов

ТЕОРЕМА. Структуры $(Ord; <)$ и $(Card; <)$ изоморфны.

Шкалы ординалов и кардиналов

ТЕОРЕМА. Структуры $(Ord; <)$ и $(Card; <)$ изоморфны.

Д-ВО. Определим функцию-класс F по индукции: $F(0) = 0$, $F(\alpha + 1) = F(\alpha)^+$, $F(\lambda) = \bigcup_{\beta<\lambda} F(\beta)$.
По индукции ясно, что $F : Ord \to Card$. Индукцией по α легко проверить $\forall \alpha_1 < \alpha(F(\alpha_1) < F(\alpha))$, т.е. F монотонна, а значит и инъективна.

Шкалы ординалов и кардиналов

ТЕОРЕМА. Структуры $(Ord; <)$ и $(Card; <)$ изоморфны.

Д-ВО. Определим функцию-класс F по индукции: $F(0) = 0$, $F(\alpha + 1) = F(\alpha)^+$, $F(\lambda) = \bigcup_{\beta<\lambda} F(\beta)$.
По индукции ясно, что $F : Ord \to Card$. Индукцией по α легко проверить $\forall \alpha_1 < \alpha(F(\alpha_1) < F(\alpha))$, т.е. F монотонна, а значит и инъективна.

Остается проверить сюръективность, т.е. $\forall \kappa \in Card \exists \alpha(\kappa = F(\alpha))$. Для некоторого α имеем $\kappa \leq F(\alpha)$ (поскольку $\kappa \leq F(\kappa)$ аналогично свойству в.у.м.). Возьмем наименьший такой ординал α и проверим $\kappa = F(\alpha)$; достаточно проверить $F(\alpha) \leq \kappa$ в случаях, когда α нулевой, последователь, или предельный ординал.

Шкалы ординалов и кардиналов

ТЕОРЕМА. Структуры $(Ord;<)$ и $(Card;<)$ изоморфны.

Д-ВО. Определим функцию-класс F по индукции: $F(0)=0$, $F(\alpha+1)=F(\alpha)^+$, $F(\lambda)=\bigcup_{\beta<\lambda}F(\beta)$.
По индукции ясно, что $F: Ord \to Card$. Индукцией по α легко проверить $\forall\alpha_1<\alpha(F(\alpha_1)<F(\alpha))$, т.е. F монотонна, а значит и инъективна.

Остается проверить сюръективность, т.е.
$\forall\kappa\in Card\exists\alpha(\kappa=F(\alpha))$. Для некоторого α имеем $\kappa\le F(\alpha)$ (поскольку $\kappa\le F(\kappa)$ аналогично свойству в.у.м.). Возьмем наименьший такой ординал α и проверим $\kappa=F(\alpha)$; достаточно проверить $F(\alpha)\le\kappa$ в случаях, когда α нулевой, последователь, или предельный ординал.

$\{F(\alpha)\}_{\alpha\in Ord}$ — шкала всех кардиналов. Полагая $\aleph_0=\omega$, $\aleph_{\alpha+1}=\aleph_\alpha^+$, $\aleph_\lambda=\bigcup_{\beta<\lambda}\aleph_\beta$, получим шкалу $\{\aleph_\alpha\}_{\alpha\in Ord}$ всех бесконечных кардиналов. Другое обозначение: $\aleph_\alpha=\omega_\alpha$.