Содержание

1 Множества

Построение множеств:

Определение. Множество - $\{x|A(x)\}$, где $A(x)$ - некоторое свойство.

Определение. $A \subseteq B$, если все элементы A принадлежат множеству B

Определение. $A = B$, если множества A и B состоят из одинаковых элементов.

Определение. $P(A) = \{B|B \subseteq A\}$ - множество всех подмножеств.

Примеры. Парадокс Рассела: $R = \{x|x \notin x\}$ $R \in R$ и $R \notin R$.

Определение. $(a, b) := \{\{a\}, \{a, b\}\}$ - упорядоченная пара.

Определение. $A \times B := \{(a, b)|a \in A \wedge b \in B\}$ - декартого произведение множеств A и B.

Определение. $R \subseteq A \times A$ - бинарное отношение на множестве A.

Определение.

1. Рефлексивность: $\forall x \in A\ xRx$
2. Симметричность: $\forall x, y \in A\ (xRy \to yRx)$
3. Транзитивность: $\forall x, y, z \in A\ (xRy \wedge yRz \to xRz)$
4. Антисимметричность: $\forall x, y \in A\ (xRy \wedge yRx \to x = y)$

Определение. R - отношение частичного порядка, если оно рефлексивно, транзитивно и антисимметрично.

Определение. R - отношение эквивалентности, если оно рефлексивно, транзитивно и симметрично.

Определение. $R(x) := \{y|xRy\}$ - класс эквивалентности элемента x.
$A/R := \{R(x)|x \in A\}$ - фактормножество.

Определение. Γ - разбиение множества A, если:

1. $\Gamma \subseteq P(A)$
2. $\forall B \in \Gamma\ B \neq \varnothing$
3. $\forall x \in A\ \exists!\ B \in \Gamma : x \in B$

Теорема. *A/R - разбиение. Если Γ - разбиение A, то $\exists!\ R : \Gamma = A/R$.*

Доказательство.

1. $A/R \subseteq P(A)$
2. $\forall B \in A/R\ B \neq \varnothing$, потому что $\forall x \in A\ xRx \Longrightarrow x \in R(x)$
3. $\forall x \in A\ \exists B \in A/R : x \in B$. Из-за транзитивности класс B единственный.

$\square$

Определение. $f \subseteq A \times B$ - функция из множества A в множество в B, если $\forall x \in A\ \exists!\ y \in B : (x, y) \in f$.
Если $\forall x, x' \in A\ (f(x) = f(x') \to x = x')$, то f - инъекция.
Если $\forall y \in B\ \exists\ x \in A : y = f(x)$, то f - сюръекция.
f - биекция $\Longleftrightarrow$ f - инъекция и сюръекция.

Определение. Множества A и B равномощны, если существует биекция $f : A \longrightarrow B$. Обозначение: $A \sim B$.

Утверждение. *Ровномощность является отношением эквивалентности.*

Доказательство.

1. $A \sim A$, так как $f : f(x) = x$ - биекция
2. $A \sim B$, тогда $\exists$ биекция $f : A \longrightarrow B \Longrightarrow f^{-1}$ - биекция из B в A
3. Биекция из A в C - композиция биекций

$\square$

Определение. Множество A вложимо в B, если существует инъекция $f : A \longrightarrow B$.

Теорема. *Данное отношение является отношением порядка.*

Доказательство.

1. $A \preceq A$ (так как существует биекция, то существует и инъекция)
2. $A \preceq B \wedge B \preceq C \to A \preceq C$, так как композиция инъекций является инъекцией
3. $A \preceq B \wedge B \preceq A \to A \sim B$ (Теорема Кантора - Бернштейна)

$\square$

Определим натуральные числа так:
$0 = \varnothing$
$1 = \{0\}$

$\vdots$

$n+1 = n \cup \{n\}$ $\omega = \{0, 1, 2, 3, \ldots\}$ - множество натуральных чисел. Принцип индукции Пусть $X \subseteq \omega$, и пусть выполнены свойства:

1. $0 \in X$
2. $\forall n (n \in X \to (n+1) \in X)$

Тогда $X = \omega$.

Теорема. *Всякое не пустое подмножество ω имеет наименьший элемент.*

Доказательство. Пусть $\varnothing \neq A \subseteq \omega$ и в A нет наименьшего элемента, тогда

1. $0 \notin A$, иначе 0 - наименьший элемент
2. $\{0, 1, 2, \ldots, n\} \cap A = \varnothing$, тогда $n+1 \notin A$, иначе $n+1$ - наименьший элемент

Следовательно, по принципу математической индукции $\{0, 1, 2, \ldots, n\} \cap A = \varnothing$ $\forall n \implies A = \varnothing$ - противоречие. $\square$

Определение. Множество называется конечным, если равномощно некоторому натуральному числу.

Лемма. *Если $m \in n$, то $n \setminus \{m\} \sim (n-1)$*

Доказательство. База индукции:
$n = 0$, доказывать нечего.
Пусть верно для n, докажем для $n+1$. Возьмём $m \in (n+1) = n \cup \{n\}$. Если $m = n$, то $(n+1) \setminus \{m\} = n$. Если $m \in n$, то применяем предположение индукции, что $n \setminus \{m\} \sim (n-1)$, то есть существует биекция между $n \setminus \{m\}$ и $(n-1)$. Отобразим $n \to (n-1)$, тем самым продлив биекцию до $(n+1) \setminus \{m\} \to n$. $\square$

Теорема. *(Принцип Дирихле) $\forall m,\ n \in \omega (m \sim n \to m = n)$.*

Доказательство. $\Phi(n) := \forall m \{m \sim n \to m = n)\}$. База индукции:
$n = 0 \implies m \sim \varnothing \implies m = \varnothing$. Пусть верно $\Phi(n)$, докажем $\Phi(n+1)$. Предположим $(n+1) \sim m$, тогда существует биекция $f : n \cup \{n\} \to m$. Пусть $k = f(n)$, тогда $g : n \to m \setminus \{k\}$ - биекция $\implies n \sim m \setminus \{k\}$. По лемме $m \setminus \{k\} \sim (m-1)$ $\implies$ по транзитивности $n \sim m-1$. По предположению индукции $n = m-1 \implies$ $n+1 = m$. $\square$

Определение. Для конечного множества x полагаем, что $|x| = n$, если $x \sim n$.

Определение. Для $m, n \in \omega$ $m < n := m \in n$, $m \leqslant n := m < n \vee m = n$.

Свойства. *1.* $m < n \wedge n < k \to m < k$*(транзитивность)*

2. $m \leqslant n \to m \subseteq n$

3. $n \not< n$*(иррефлексивность)*

4. $n < m \leftrightarrow n + 1 \leqslant m$ *(дискретность вверх)*

5. $n < m \vee m < n \vee m = n$

Лемма. *Если A конечно, то $A \cup \{x\}$ конечно.*

Доказательство. Если $x \in A$, то $A \cup \{x\} = A$ конечно. Пусть $x \notin A$, $A \sim n$, тогда $A \cup \{x\} \sim n + 1$ □

Лемма. *Если A конечно, то $\forall n \in \omega$ $A \cup n$ конечно.*

Доказательство. База индукции: $n = 0$, $A \cup \varnothing = A$ конечно. Пусть $A \cup n$ конечно. Запишем $A \cup (n + 1) = A \cup (n \cup \{n\}) = (A \cup n) \cup \{n\}$ - конечное множество по предположению индукции и по предыдущей лемме, последний переход по транзитивности. □

Лемма. *Если множества A и B конечны и $A \cap B = \varnothing$, то $A \cup B$ конечно.*

Доказательство. Так как B конечно, то $B \sim n \in \omega$, то есть существует биекция $f : B \to n \implies$ существует биекция $g : A \cup B \to A \cup n$, тождественная на A и совпадает с f на B. По транзитивности и предыдущй лемме имеем, что $A \cup B$ конечно. □

Теорема. *Если множества A и B конечны, то $A \cup B$ конечно.*

Доказательство. $A \cup B = (A \backslash B) \cup B$. Докажем, что $A \backslash B$ - конечное множество. $A \backslash B \subseteq A$ и докажем, что любое подмножество C конечного множества конечно. База индукции: $|A| = 0$, тогда $|C| = 0$. Пусть верно для $|A| = n$. Рассмотрим $|A| = n + 1$, если $C = A$, то C конечно. Пусть $C \subset A$, тогда $\exists a \in A$ и $a \notin C$ $\implies |A \setminus \{a\}| = n \implies C \subseteq A \setminus \{a\} \implies$ по предположению индукции C конечно. Значит, $A \setminus B$ конечно. По последней лемме $A \cup B$ конечно. □

Теорема. *Если множества A и B конечны, то $A \times B$ конечно.*

Доказательство. База индукции: $|B| = 0$, тогда □

Определение. $m+n := |A \cup B|$, где $|A| = m$, $|B| = n$, $A \cap B = \varnothing$. $m \cdot n := |A \times B|$, где $|A| = m$, $|B| = n$. $B^A := \{f | f$ - функция из A в B$\}$.

Лемма. $\forall n \in \omega\ B^{n+1} \sim B^n \times B$.

Доказательство. Пусть $f : n \to B$, $b \in B$, тогда построим функцию $g : (n+1) \to B$, которая совпадает с f на множестве n и переводит $n+1$ в b. Она задаёт биекцию между $B^n \times B \to B^{n+1}$. □

Лемма. *Если множество B конечно, то $\forall n \in \omega\ B^n$ конечно.*

Доказательство. По последней теореме и предыдущей лемме по индукции получаем данное утверждение. □

Лемма. *Если $A \sim C$, то $B^A \sim B^C$.*

Доказательство. Пусть дана биекция $g : A \to C$. По функции $f : C \to B$ строим композицию $(f \cdot g) : A \to B$. Это задаёт биекцию B^C на B^A. □

Теорема. *Если множества A и B конечны, то B^A конечно.*

Доказательство. Из двух последних лемм получаем данное утверждение. □

Определение. $m^n := |B^A|$, где $|B| = m$, $|A| = n$.

Определение. Характеристической функцией для любого подмножества A множества X называется функция f такая, что $f(x) = \begin{cases} 1, \text{ если } x \in A \\ 0, \text{ если } x \notin A \end{cases} \quad \forall x \in X$

Теорема. $2^A \sim P(A)$.

Доказательство. Между подмножествами множества A и их характеристическими функция существует биекция, а множество всех характеристических функций равно 2^A. □

Теорема. *Теорема Кантора $|A| < |P(A)|$.*

Доказательство. $A \preceq P(A)$: инъекция $a \to \{a\}$. Предположим, что $f : A \to P(A)$ - биекция, и рассмотрим $B = \{a | a \notin f(a)\}$. □

Теорема. *Даны множество Y, $y_0 \in Y$, функция $h : Y \to Y$. Тогда существует единственная функция $f : \omega \to Y$ такая, что*

1. $f(0) y_0$

2. $\forall n\ f(n+1) = h(f(n))$

Доказательство. Назовём m-функцией такую же функцию, как в формулировке теоремы, но заданную на множестве $m+1$.
База индукции: $\{(0, y_0)\}$ единственная 0-функция.
Шаг индукции: если g - m-функция, то, добавив $\{(m+1, h(g(m)))\}$, получим $m+1$-функцию.
Объединив все m-функции, получим искомую ω-функцию f. □

Определение. Множество A называется счётным, если $A \sim \omega$.

Теорема. *1. Если A конечно, B счётно, то $A \prec B$.*

2. Если A счётно, $B \subseteq A$, то B конечно или счётно.

3. Если A счётно, B конечно или счётно, то $A \cup B$ счётно.

4. Если A счётно, B конечно или счётно, то $A \times B$ счётно.

Доказательство.

1. По транзитивности $A \preceq B$. Пусть $A \sim B$, тогда $\omega \sim n$ по транзитивности. Из того что $n+1 \subseteq \omega$ следует, что $n+1 \preceq n$, что противоречит принципу Дирихле.

2. Пусть $A = \omega$, $B \subseteq A$ бесконечно. По рекурсии построим биекцию $f : \omega \to B$. Сначала построим функцию F такую, что $F(0) = \{min(B)\}$, $F(n+1) = F(n) \cup min(B \setminus F(n))$.

3. Пусть A и B счётны и не пересекаются, тогда предъявим обход по элементам как было в курсе математического анализа в первом семестре.

4. $\omega \times \omega \sim \omega$: канторовская нумерация.

□

Определение. Множество бесконечно по Дедекинду (D-бесконечно), если оно равномощно какому-нибудь своему собственному подмножеству.

Теорема. *1. Конечное множество D-конечно.*

2. Счётное множество D-бесконечно.

3. Если A счётно, $A \subseteq B$, то B D-бесконечно.

4. A D-бесконечно $\iff$ A содержит счётное подмножество.

5. Если A D-бесконечно, B конечно, то $A \cup B \sim A \setminus B \sim A$.

6. *Если A D-бесконечно, B счётно, то $A \cup B \sim A$.*

Доказательство. 1. По принципу Дирихле.

2. Пусть A счётно, тогда $\omega \subseteq A$ и $A \sim \omega \Longrightarrow$ по определению A D-бесконечно.

3. Построим отображение из B в A,

4. $\Longleftarrow$ По утверждению 3.
$\Longrightarrow$ Пусть $f : A \to B$ - биекция, где $B \subset A$. Если $A \in A \setminus B$, то рассмотрим $\{f(a), f(f(a)), \dots\}$. Таким образом получили искомое счётное множество.

5. Если $C \subseteq A$ - счётное множество, $B \cap A = \varnothing$ и $B \sim n$, то строим биекцию из $A \cup B$ на A: сдвигаем все элементы C на n, а на освободившиеся места отображаем B. $A = (A \setminus B) \cup B$, тогда по утверждению 3 $A \setminus B$ D-бесконечно, так как оно содержит счётное подмножество $C \setminus B$, а по уже доказанному в утверждении пункту получаем, что $A \sim A \setminus B$.

6. Если $C \subseteq A$ счётно, $B \cap A = \varnothing$ и $B \sim \omega$, то строим биекуию из $A \cup B$ на A: удваиваем номера всех элементов C, а на нечётные места отображаем B.

$\square$

Теорема. *Всякое бесконечное множество D-бесконечно.*

Доказательство. Построим инъекцию между бесконечным множеством и ω, тогда по утверждению 4 данное множество D-бесконечно. $\square$

Определение. $c := 2^\omega$ - континуум.

Определение. Пусть $X \neq \varnothing$, $\leqslant$ - бинарное отношение на X

1. $\leqslant$ - (частичный) порядок, если $\leqslant$ - рефлексивно, транзитивно и антисимметрично;

2. $\leqslant$ - линейный порядок, если $\leqslant$ - частичный порядок, а также $\forall x, y \in X$ $(x \leqslant y \vee y \leqslant x)$;

3. $\leqslant$ - полный порядок, если $\leqslant$ - частичный порядок, а также любое непустое подмножество X имеет наименьший элемент.

Обозначение: $x < y := x \leqslant y \wedge x \neq y$. Соответствующие пары $(X, \leqslant)$ называются:

1. (частично) упорядоченным множеством
2. линейно упорядоченным множеством
3. вполне упорядоченным множеством (ВУМ)

Определение. Пусть $\alpha = (X, \leqslant)$, $\beta = (X', \leqslant')$ - вполне упорядоченные множества. Изоморфизмом α на β называется отображение $f : X \to X'$, которое является биекцией и сохраняет порядок, то есть $x \leqslant y \to f(x) \leqslant f(y)$.

Лемма. *Свойства изоморфизмов*

1. $x < y \to f(x) < f(y)$
2. *Если f - изоморфизм α на β, то обратная функция f^{-1} - изоморфизм β на α*
3. *Композиция изоморфизмов - изоморфизм*

Определение. Пусть α, β - вполне упорядоченные множества, тогда α изоморфно β, если существует изоморфизм α на β. Обозначение: $\alpha \cong \beta$.

Лемма. 1. $\alpha \cong \alpha$

2. *Если $\alpha \cong \beta$, то $\beta \cong \alpha$*
3. *Если $\alpha \cong \beta$ и $\beta \cong \gamma$, то $\alpha \cong \gamma$*

Определение. Пусть $\alpha = (X, \leqslant)$ - вполне упорядоченное множество. Начальный отрезок α - подмножество $Y \subseteq X$, замкнутое по убыванию: $\forall y \in Y\ \forall x \in X$ $(x < y \to x \in Y)$.

Лемма. *Пусть Y - собственный начальный отрезок вполне упорядоченного множества $(X, <)$. Тогда $Y = \{x | x < a\}$ для некоторого $a \in X$.*

Доказательство. □

Лемма. *Пусть $\alpha = (X, \leqslant)$ - вполне упорядоченное множество, $f : X \to X$ - строго возрастающая функция. Тогда $\forall x \in X\ x \leqslant f(x)$.*

Доказательство. Рассмотрим множество $Y := \{x \in X | f(x) < x\}$. Предположим, что $Y \neq \varnothing$, и пусть x - наименьший элемент в Y. Тогда: $f(f(x)) < f(x)$, так как f строго возрастает. Но так как x - минимальный элемент, то $f(x) \leqslant f(f(x))$ - противоречие. Значит, $Y = \varnothing$. □

Теорема. *Никакие вполне упорядоченное множество не изоморфно своему начальному отрезку.*

Доказательство. Предположим противное, пусть f - изоморфизм $(X, \leqslant)$ на $(Y = \{x \in X | x < a\}, \leqslant'$, где $\leqslant'$ - ограничение $\leqslant$ на Y. Тогда $f(a) < a$, что противоречит предыдущей лемме. $\square$

Теорема. *Теорема Кантора о сравнении вум Пусть α, β - вполне упорядоченные множества, тогда верно ровно одно из 3 утверждений:*

1. *α изоморфно собствееному начальному отрезку β*
2. *β изоморфно собствееному начальному отрезку α*
3. *$\alpha \cong \beta$*

Доказательство. Пусть $\alpha = (X, \leqslant)$, $\beta = (Y, \leqslant')$. Рассмотрим отношение $f := \{(x, y) | x \in X, y \in Y, \{x_1 \in X | x_1 < x\} \cong \{y_1 \in Y | y_1 < y\}\}$

1. По последней теореме для любого x существует не более одного y такого, что $(x, y) \in f$, и для любого y существует не более одного x такого, что $(x, y) \in f$. Следовательно, f - биекция $X_0 \subseteq$ на $Y_0 \subseteq Y$.
2. Докажем, что X_0 - начальный отрезок α и Y_0 - начальный отрезок β. Пусть $x \in X_0$ и $\{x_1 \in X | x_1 < x\} \cong \{y_1 \in Y | y_1 < y\}$. Пусть h - данный изоморфизм. Возьмём $z < x$, тогда, сужая h на z получим $\{x \in X | x < z\} \cong \{y \in Y | y < h(z)\}$. Так как h сохраняет порядок, потому что h - изоморфизм, и у любого элемента множества $\{y \in Y | y < h(z)\}$ есть прообраз, то $z \in X_0$.
3. Докажем, что f сохраняет порядок. Пусть $x \in X_0$, $\{x_1 \in X | x_1 < x\} \cong \{y_1 \in Y | y_1 < y\}$, h - данный изоморфизм и $z < x$. Так же как и в прошлом пункте ограничим h на z, тогда $\{x_1 \in X | x_1 < z\} \cong \{y_1 \in Y | y_1 < h(z)\}$, то есть $f(z) = h(z)$. $h(z) < y = f(x) \implies f(z) < f(x)$, то есть f сохраняет порядок в силу произвольности z.
4. Из предыдущих пунктов имеем, что f - изоморфизм начального отрезка в α на начальный отрезок в β. Если оба этих отрезка собственные, то по предпоследней лемме $X_0 = \{x_1 \in X | x_1 < x\}$ и $Y_0 = \{y_1 \in Y | y_1 < y\}$ для некоторых x и y. Тогда $(x, y) \in f$ по определению f, а значит, $x \in X_0 = \{x_1 \in X | x_1 < x\}$ - противоречие. Следовательно, один из этих отрезков не собственный, то есть остаётся только 3 варианта, перечисленные в условии теоремы, а по предыдущей теореме они не изоморфны друг другу.

□

1.1 Ординальные числа

Определение. Ординальное число (по Кантору) представитель класса эквивалентности по $\cong$.

Теорема. *В любом не пустом множестве S ординальных чисел существует наименьшее.*

Доказательство. Выберем $\alpha \in S$. Рассмотрим $\{\beta \in S | \beta \leqslant \alpha\}$. Среди элементов данного множества есть наименьший, так как в непустом множестве начальных отрезков числа α, которым изоморфны эти β, есть наименьший. □

Теорема. *Теорема о трансфинитной индукции Пусть дано свойство $\Phi(\alpha)$ ординальных чисел, которое наследуется, то есть $\forall\alpha\ (\forall\beta < \alpha\ \Phi(\beta) \to \Phi(\alpha))$. Тогда $\forall\alpha\Phi(\alpha)$.*

Доказательство. Предположим противное, пусть для некоторого α_0 $\Phi(\alpha_0)$ не верно. Рассмотрим $S = \{\beta < \alpha_0 | \Phi(\beta) \text{ не верно}\}$. По предыдущей теореме найдётся наименьшее ординальное число β_0, тогда $\forall\beta < \beta_0\ \Phi(\beta)$ верно. Поскольку Φ наследуется, получаем, что $\Phi(\beta_0)$ верно - противоречие. □

Определение. $\alpha + 1$ получается прибавлением наибольшего элемента к α.

Определение. Предельное ординальное число не имеет предыдущего.

Утверждение. *Пусь X - произвольное множемтво ординальных чисел, тогда существует орддинальное число α большее любого $\beta \in X$. Если в X нет наибольшего, то существует $\alpha = supX$.*

Теорема. *Парадокс Бурали-Форти Все ординальные числа не образуют ординального числа.*

Доказательство. Так как отношение вложимости ординалов является отношением линейного порядка по теореме сравнения, то из существования наименьшего элемента имеем, что этот порядок полон. Тогда он должен задавать ординальное число, которое больше всех ординальных чисел, но самого большого ординального числа не существует, так как любое число можно увеличить на 1. □

Теорема. *теорема о трансфинитной рекурсии Пусть α_0 - ординальное число, H - функция на ординальных числа. Тогда $\exists!$ функция F на ординальных числах такая, что:*

1. $F(0) = \alpha_0$
2. $F(\alpha + 1) = H(F(\alpha))$
3. $F(\alpha) = sup\{F(\beta) | \beta < \alpha\}$, *если α - предельное ординальное число.*

Введём операции на ординальных числах:

1. Сложение: $\alpha + 0 = \alpha$, $\alpha + (\beta + 1) = (\alpha + \beta) + 1$, $\alpha + \beta = sup\{\alpha + \gamma | \gamma < \beta\}$, если β - предельное ординальное число.
2. Умножение: $\alpha \cdot 0 = 0$, $\alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \alpha$, $\alpha \cdot \beta = sup\{\alpha \cdot \gamma | \gamma < \beta\}$, если β - предельное ординальное число.
3. Возведение в степень: $\alpha^0 = 1$, $\alpha^{\beta+1} = \alpha^\beta \cdot \alpha$, $\alpha^\beta = sup\{\alpha^\gamma | \gamma < \beta\}$, если β - предельное ординальное число.

Определение. Ординал - множество специального вида, обобщение натуральных чисел Фон Неймана.

Теорема. *Теорема счёта Любое вум изоморфно некоторому ординалу.*

1.2 Аксиома выбора

Определение. Если X - семейство не пустых множеств, то существует функция выбора на X. Это функция $f : X \to Y$ такая, что $f(x) \in x \ \forall x \in X$.

Определение. Эквивалентные определения аксиомы выбора:

1. Для всякого непустого семейства множеств существует функция выбора на данном семействе.
2. Если R - отношение эквивалентности на X, то $X/R \preceq X$.
3. Если Γ - разбиение множества X, то $\exists Y \subseteq X : \forall Z \in \Gamma |Y \cap Z| = 1$.
4. Если $f : X \to Y$ - сюръекция, то существует $g : Y \to X$ - инъекция такая, что $\forall y \in Y \ f(g(y)) = y$.

Теорема. *(Теорема Цермело) Всякое множество можно вполне упорядочить.*

Лемма. *(Лемма Цорна) Пусть $(X, \leqslant)$ - частично упорядоченное множество, в котором каждое линейно упорядоченное подмножество ограничено сверху, тогда X имеет наибольший элемент.*

Доказательство. Докажем, что из аксиомы выбора следует лемма Цорна, из неё следует теорема Цермело, а из неё - аксиома выбора.

1. Допустим, что $(X, \leqslant)$ удовлетворяет условиям леммы Цорна, но нет наибольшего элемента. Назовём строгой верхней гранью линейно упорядоченного подмножества C множества X такой элемент $x \in X$, что $\forall c \in C$ $c \leqslant x$. Из условия имеем, что для любого линейноупорядоченного подмножества C множества X множество его строгих верхних граней $\psi(C)$ не пусто (из-за отсутствия максимального элемента). Рассмотрим множемтво S - множемтво всех строгих верхних граней линейно упорядоченных подмножеств множества X. S - множество, так как $S \subset P(X)$. По аксиоме выбора существует функция f выбора на множестве S, композиция которой с ψ сопоставляет некоторому линейно упорядоченному множеству его некоторую строгую верхнюю грань. Пусть φ - композиция этих функций. Назовём множество $S \subset X$ кооректным, если:

   (a) $(S, \leqslant)$ вполне упорядочено

   (b) $\forall x \in S$ $\varphi(S_x) = x$, где $S_x = \{y \in S | y < x\}$

   Лемма. *(a) Если множество X и T корректны, то одно из них есть начальный отрезок другого.*

   (b) Объединение любого семейства корректных множества корректно.

   Доказательство. (a) Предположим, что ни одно из этих множеств не является начальным отрезком друго. Пусть $J \subset (S \cap T)$, является начальным отрезком и S, и T, назовём его общим начальным отрезком. Пусть I - множемтво всех общих начал T и S, тогда I - общее начало T и S, так как $\forall x \in I$ $x \in J$ для некоторого начального отрезка $S \Longrightarrow \forall y \in S$ $(y \leqslant x \Longrightarrow y \in J \subset I)$, аналогично для T. Если I совпадает с одним из этих множеств, то лемма доказана. Пусть I не совпадает ни с одним из них. Рассмотрим $s = \min_S(S \setminus I)$ и $t = \min_T T \setminus I$. Тогда $S_s = I = T_t$. В силу $s = \varphi(S_s) = \varphi(T_t) = t$, то есть $I \cup \{s\}$ есть общее начало S и T, большее I - противоречие.

(b) Пусть Σ - семейство корректных множеств и $U = \bigcup \Sigma$. Множество $(U, \leqslant)$ линейно упорядочено по предыдущему пункту. Каждое $S \in \Sigma$ - начальный отрезок U. Иначе $\exists x \in S$ и $\exists y \leqslant x$ такой, что $y \in (U \setminus S)$. Тогда для некоторого корректного $T \in \Sigma$ $y \in (T \setminus S)$, значит, T не является начальным отрезком S. Тогда по первому утверждению S - начальный отрезок T. Противоречие с тем, что $y \leqslant x \in S$ и $y \notin S$.
Докажем, что $(U, \leqslant)$ вполне упорядочено. Пусть $Y \subset U$ не пусто, рассмотрим $y \in Y$ и корректное множество $S \in \Sigma$ такое, что $y \in S$. Поскольку $Y \cap S$ не пусто и вполне упорядочено как подмножество S, тогда $\exists x = \min\limits_S (Y \cap S) \in S$. Поскольку S - начальный отрезок U, тогда x - наименьший элемент $Y \subset U$.
Выберем $S \in \Sigma$ такое, что $x \in S$. Так как S - начальный отрезок U, то $U_x = S_x \Longrightarrow x = \varphi(S_x)\varphi(U_x)$. По определению S корректно. Лемма доказана.

$\square$

Рассмотрим множество Σ всех корректных подмножеств множества X и положим $U = \bigcup \Sigma$. По лемме U вполне упорядочено и, в частности, является линейно упорядоченным множеством, то оно имеет строгую верхнюю грань $\varphi(U)$. Тогда $U \cup \{\varphi(U)\}$ больше U и является корректным множеством, что невозможно по определению Σ. Лемма Цорна доказана.

2. Вполне упорядоченное множество $(S, \leqslant_S)$ назовём вполне упорядоченным подмножеством $(X, \leqslant)$, если $S \subset X$. Рассмотрим $W(X)$ - множество всех вполне упорядоченных подмножеств множества X. Определим на $W(X)$ отношение строгого частичного порядка $\prec$: $(S, \leqslant_S) \prec (T, \leqslant_T)$, если и только если $S \subset T$ есть собственный начальный отрезок T и $\leqslant_S$ совпадает с ограничением $\leqslant_T$ на S.
Рассмотрим произвольное линейно упорядоченное подмножество $C \subset W(X)$. Этому подмножеству соответствует линейно упорядоченное множество возрастающих по включению линейно упорядоченных подмножеств и соответствующих им бинарных отношений. Пусть U - объединение указанных подмножеств, а $\leqslant_U$ - объединение соответствующих отношений. $\leqslant_U$ - отношение линейного порядка на U и $\forall (S, \leqslant_S) \in C$ - начальный отрезок $U \Longrightarrow (U, \leqslant_U)$ - вполне упорядоченное подмножество X, то есть $(U, \leqslant_U) \in W(X)$ и является верхней гранью множества C.
По лемме Цорна в $(W(X), \prec)$ найдётся максимальный элемент $(M, \leqslant_M)$.

Если M не совпадает с X, то возьмём $a \in X \setminus M$ и продолжим порядок $\leqslant_M$ на множество $N = M \cup \{a\}$, полагая $x \leqslant_N a \ \forall x \in M$. Тогда $(N, \leqslant_N)$ - вполнеупорядоченное подмножество X и $(M, \leqslant_M) \prec (N, \leqslant_N)$, что противоречит максимальности $(M \leqslant_M)$. Значит, M совпадает с X и M вполне упорядочено. Теорема Цермело доказана.

3. Пусть S - данное семейство не пустых множеств. По теореме Цермело множество $U = \bigcup S$ можно вполне упорядочить. $\forall x \in S \ x \in U$. Пусть $min(x)$ - минимум x в смысле порядка на U. Поскольку $S \neq \varnothing$, то функция $x \to min(x)$ - функция выбора на S.

□

Теорема. *Всякое бесконечное множество D-бесконечно.*

Доказательство. Дано бесконечное множество A. Построим функцию выбора g на множестве $\{B | B \subseteq A, B \neq \varnothing\}$. Затем строим по рекурсии инъекцию $f : \omega \to A$
$f(0) = a_0$ (найдётся, так как A не пусто)
$\vdots$
$f(n+1) = g(A \setminus \{f(0), \ldots, f(n)\})$ (это множество не пусто, так как A бесконечно)
□

Теорема. *(Теорема сравнения мощностей) Для любых множеств X, Y $X \preceq Y$ или $Y \preceq X$.*

Доказательство. По теореме Цермело эти множества можно вполне упорядочить. По теореме Кантора одно из них вложимо в другое. □

Определение. Кардинал - ординал, не равномощный никакому меньшему ординалу.

Утверждение. *Всякий ординал равномощен некоторому кардиналу.*

Доказательство. Если α - не кардинал, то $\{\beta | \beta < \alpha, \beta \sim \alpha\}$ имеет наименьший элемент. Он будет искомым кардиналом. □

Определение. Мощностью множества X называется кардинал, равномощный X.

Определение. По трансфинитной индукции построим последовательность алефов: $\aleph_0 = \omega$, $\aleph_{\alpha+1}$ - наименьший кардинал, который больше $\aleph_\alpha$. Если α - предельный ординал, то $\aleph_\alpha = sup\{\aleph_\beta | \beta < \alpha\}$.

Теорема. *Последовательность алефов содержит все бесконечные кардиналы.*

Доказательство. 1. По трансфинитной индукции $\alpha \leqslant \aleph_\alpha$

2. Если α - бесконечный кардинал, то он не может быть больше всех алефов. В противном случае приходим к противоречию с тем, что все ординалы не образуют ординального числа.

3. Предположим k не алеф. Возьмём наименьшее α, для которого $k < \aleph_\alpha$

   (a) Пусть $\alpha = \beta + 1$, тогда $\aleph_\beta \leqslant k \leqslant \aleph_{\beta+1} \Longrightarrow k = \aleph_\beta$

   (b) Пусть α - предельный ординал. Так как $k < \aleph_\alpha = sup\{\aleph_\beta | \beta < \alpha\}$, то по определению sup найдётся $\beta < \alpha$ для которого $k < \aleph_\beta$ - противоречие выбору α

□

Определение. Операции над кардиналами:

1. $|A| \cdot |B| = |A \times B|$
2. $|A| + |B| = |A \cup B|$ (если $A \cap B = \varnothing$)
3. $|A^B| = |A|^{|B|}$

Обобщённая континуум-гипотеза: $2^{\aleph_\alpha} = \aleph_{\alpha+1}$

Теорема. *Основная теорема о кардинальной арифметике:* $\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = max(\aleph_\alpha, \aleph_\beta)$.

Доказательство. Доказываем по трансфинитной рекурсии для $\aleph_\alpha \cdot \aleph_\alpha$, а дальше по теореме Кантора-Бернштейна. □