Основы теории множеств. Неофициальный конспект

Лектор: Виктор Львович Селиванов
Конспектировал Леонид Данилевич

I семестр, осень 2022 г.

Оглавление

Лекция I

6 сентября 2022 г.

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.

Глава 1

Наивная теория множеств

1.1 Множества. Отношения и операции

Множества бывают конечные (с $n \in \mathbb{N}_0$ элементами) и бесконечные.

Конечные множества можно задать перечислением $\{1, 3, 8, 21\}$ или свойством $\{x | \phi(x)\}$, например, $\{x | x$ — чётное натуральное$\}$.

Равенство $A = B \iff \forall x : (x \in A \iff x \in B)$.

Включение $A \subset B \iff \forall x : (x \in A \Rightarrow x \in B)$.

Пересечение $A \cap B = \{x | x \in A \wedge x \in B\}$. Ассоциативно и коммутативно. Дистрибутивно относительно $\triangle$.

Объединение $A \cup B = \{x | x \in A \vee x \in B\}$. Ассоциативно и коммутативно.

Разность $A \cup B = \{x | x \in A \wedge x \notin B\}$.

Симметрическая разность $A \triangle B \stackrel{def}{=} (A \backslash B) \cup (B \backslash A)$. Ассоциативно и коммутативно.

Дополнение $A^{\complement} \stackrel{def}{=} U \backslash A$, если все рассматриваемые множества содержатся в универсуме U.

Булеан — множество всех подмножеств A. Обозначается $\mathcal{P}(A) = 2^A = \{X | X \subset A\}$.

1.1.1 Отношения

Декартово произведение $A \times B = \{(a, b) | a \in A \wedge b \in B\}$. Подмножества $R \subset A \times B$ называются бинарными отношениями между A и B. Запись $(a, b) \in R$ иногда упрощают до aRb. Так, типичным отношением является «<». Тогда пишут $a < b$.

Композиция отношений R (между A и B) и S (между B и C):

$$S \circ R = \{(a, c) \in A \times C | \exists b \in B : ((a, b) \in R \wedge (b, c) \in S)\}$$

$R^{-1} = \{(b, a) | (a, b) \in \mathbb{R}\}; R^{-1} \subset B \times A$ — обратное отношение. $\left(R^{-1}\right)^{-1} = R$.

$dom(R) = \{a | \exists b : \ (aRb)\}$ — область определения R.

$rng(R) = \{b | \exists a : \ (aRb)\}$ — область значений R.

Образ $R(A') = \{b \in B | \exists a \in A' : \ aRb\}$ для $A' \subset A$.

Прообраз $R^{-1}(B') = \{a \in A | \exists b \in B' : \ aRb\}$ для $B' \subset B$.

R является функциональным отношением $\iff \forall a, b, b' : \ ((aRb) \wedge (aRb')) \Rightarrow b = b')$.

R — функция, если оно функционально, и $dom(R) = A$. В таком случае пишут $R(a) = b$ для того единственного $b \in B : aRb$.

Можно подчеркнуть, что R — тотальная функция, а если $dom(R) \neq A$, и $R :\subset A \to B$, то это частичная функция.

Функция называется инъекцией, если $\forall a, a' \in A : a \neq a' \Rightarrow f(a) \neq f(a')$.

Функция называется сюръекцией, если $rng(f) = B$.

Функция называется биекцией, если она одновременно является и сюръекцией, и инъекцией.

Типы внутренних бинарных отношений $R \subset A \times A$

Рефлексивность $\forall a \in A :\ aRa$.

Антирефлексивность $\forall a \in A : !(aRa)$.

Симметричность $\forall a, b \in A :\ aRb \iff bRa$.

Антисимметричность $\forall a, b \in A :\ ((aRb) \wedge (bRa)) \Rightarrow a = b$.

Транзитивность $\forall a, b, c \in A :\ (aRb) \wedge (bRc) \Rightarrow aRc$.

Предпорядок — отношение с рефлексивностью и транзитивностью. Обозначается $\leqslant, \preceq, \subseteq, \sqsubseteq$.

Частичный порядок — антисимметричный предпорядок.

Строгий порядок — антирефлексивность и транзитивность. Обозначается $<, \prec, \subset, \sqsubset$.

Эквивалентность — рефлексивность, симметричность, транзитивность. $=, \equiv, \approx, \cong, \simeq$.

Классы эквивалентности

Рассмотрим некое множество A и отношение эквивалентности на нём $\equiv$.

Пусть $[\ ] : A \to 2^A, a \mapsto [a]$, где $[a] = \{x \in A | x \equiv a\}$ — класс эквивалентности, (порождённый элементом | элемента) a.

Предложение: классы эквивалентности образуют разбиение A, т. е. $\forall a \in A : [a] \subset A \wedge [a] \neq \varnothing$, а кроме того $\forall x, y \in A : ([x] = [y]) \vee ([x] \cap [y] = \varnothing)$ и $\bigcup\limits_{a \in A} [a] = A$.

Доказательство. $[a] \neq \varnothing$, так как $a \in [a]$. По этой же причине $\left(\bigcup\limits_{a \in A} [a]\right) \supset \left(\bigcup\limits_{a \in A} a\right) \supset A$, но так как $\forall a \in A : [a] \subset A$, то $\bigcup\limits_{a \in A} [a] = A$.

Если $a \equiv b$, то $\forall x \in [a] : x \in [b]$, (так как раз $a \equiv x$, то по транзитивности $b \equiv x$).

Если же $a \not\equiv b$, то $[a] \cap [b] = \varnothing$. От противного: пусть $\exists x \in A : x \in [a] \wedge x \in [b]$. Тогда по транзитивности $a \equiv b$, противоречие. $\square$

Фактор множества A по отношению эквивалентности $\equiv$ обозначается $A_{/\equiv}$.

$A_{/\equiv} \overset{def}{=} \{s \subset A | \exists a \in A : s = [a]\}$.

Лекция II

13 сентября 2022 г.

1.2 Мощность множества. Сравнение мощностей

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

Определение 1.2.1 (Равномщность)**.** A и B равномощны — $A \simeq B$ — если существует биекция $f : A \to B$.

1.2.1 Свойства отношения равномощности

Отношение рефлексивно, симметрично, транзитивно.

$A \simeq A$, так как id — искомая биекция.

$A \simeq B \Rightarrow B \simeq A$, так как существование биекции $f : A \to B$ влечёт существование обратной биекции $f^{-1} : B \to A$.

$A \overset{f}{\simeq} B \land B \overset{g}{\simeq} C \Rightarrow A \overset{f \circ g}{\simeq} C$.

Таким образом, $\simeq$ является отношением эквивалентности, но ввести фактор множества всех множеств нельзя, так как множества всех множеств не существует.

Определение 1.2.2. Множество A не превосходит по мощности множество B ($A \preceq B$), если существует инъекция $f : A \to B$.

Теорема 1.2.1 (Теорема Кантора — Шрёдера — Бернштейна)**.** $A \preceq B \land B \preceq A \Rightarrow A \simeq B$.

Доказательство. Пусть $A \xrightarrow{f} B \xrightarrow{g} A$ — две инъекции.

Пусть $h = f \circ g$. Как композиция инъекций, она является инъекцией.

Пусть $\begin{cases} A_0 = A \\ A_1 = g(B) \\ A_2 = h(A) \end{cases}$ Заметим, что $A_2 \subseteq A_1 \subseteq A_0$.

$A_1 \simeq B$, потому что $g : B \to A_1$ — биекция.

Аналогично $h : A_0 \to A_2$ — биекция.

Утверждается, что достаточно доказать, что $A_0 \simeq A_1$.

Определим бесконечную последовательность $A_{n+2} = h(A_n)$. Из этого определения видно, что $A_{n+1} \subseteq A_n$ и множества, равномощные A_0 — с чётными номерами, а равномощные A_1 — с нечётными.

Пусть $C_n = A_n \backslash A_{n+1}$. Нетрудно видеть, что $h : C_0 \to C_2$ — биекция. Вообще говоря, все C_{2n} равномощны. После этого из картинки видно, что C_{2n} уплотняются, а остальные могут тождественно перейти в себя. Формальнее,

$$u : A_0 \to A_1 \quad u(a) = \begin{cases} h(a), & \exists n \in \mathbb{N} : a \in C_{2n} \\ a, & \text{otherwise} \end{cases}$$

Можно увидеть, что u — искомая биекция.

□

Определение 1.2.3. Множество A меньше по мощности B ($A \prec B$), если

$$\begin{cases} A \preceq B \\ B \not\preceq A \end{cases} \overset{\text{здесь равносильно}}{\iff} \begin{cases} A \preceq B \\ A \not\simeq B \end{cases}$$

Теорема 1.2.2 (Теорема Кантора)**.** Для любого множества A: $A \prec 2^A$.

Доказательство.

Замечание. Если A — конечно и имеет n элементов, то теорема верна, так как $n < 2^n$ для любого $n \in \mathbb{N}_0$.

$A \preceq 2^A$ — рассмотрим инъекцию $a \in A \mapsto \{a\}$. Теперь докажем, что $A \not\simeq 2^A$. Предположим противное: $A \simeq 2^A$. Тогда есть биекция $g : A \to 2^A$. Теперь, сходно с диагональным аргументом для $\mathbb{N} \not\simeq \mathbb{R}$, определим $[B \subseteq A : \quad B = \{a \in A | a \notin g(a)\}$ Очевидно, $\nexists a \in A : B = g(a)$. Однако $B \subseteq A \Rightarrow B \in g(A)$, противоречие. □

1.2.2 Некоторые виды множеств по мощностям

1. Конечные множества. *Комбинаторика*
2. Счётные множества — множества, равномощные $\mathbb{N}$. *Информатика*
3. Континуальные множества — множества, равномощные $2^{\mathbb{N}}$. *Матанализ*

$$\underset{\text{счётное}}{\mathbb{N}} \subset \underset{\text{счётное}}{\mathbb{Z}} \subset \underset{\text{счётное}}{\mathbb{Q}} \subset \underset{\text{континуальное}}{\mathbb{R}} \subset \underset{\text{континуальное}}{\mathbb{C}}$$

Шкала мощностей

$$0, 1, 2, 3, \ldots, (\omega = |\mathbb{N}|), \ldots, (\mathbf{C} = |2^{\mathbb{N}}|), \ldots,$$

Предложение 1.2.1. *Для любого бесконечного множества $A : \mathbb{N} \preceq A$.*

Доказательство. Пусть A — бесконечное множество. Тогда $\exists a_0 \in A$. Заметим, что $A \backslash \{a_0\}$ тоже бесконечно. Дальше по индукции мы можем найти a_n для любого $n \in \mathbb{N}$. Таким образом, мы нашли инъекцию $\mathbb{N} \to A$. □

Вопрос. Существует ли множество $A : \mathbb{N} \prec A \prec \mathbb{R}$?

Континуум гипотеза, CH, утверждает, что таких множеств не существует.

Лекция III

20 сентября 2022 г.

Вопрос. Пусть даны множества A и B: $\left[\begin{array}{l} A \simeq B \\ A \prec B \\ B \prec A \end{array}\right.$. Правда ли, что другого исхода не бывает?

Наиболее популярная система аксиом утверждает, что всё исчерпывается этими тремя случаями.

1.3 Числовые структуры в теории множеств

1.3.1 Натуральные числа

Определим натуральное число, как мощность конечного множества.

$$0 \coloneqq |\varnothing|; \quad 1 \coloneqq |\{\varnothing\}|$$

Сложение: для непересекающихся множеств $|A| + |B| = |A| \sqcup |B|$, но так как множества могут пересекаться, то мы можем их сделать искусственно непересекающимися:

$$|A| + |B| = |(\{0\} \times A) \cup (\{1\} \times B)|$$

Умножение:

$$|A| \cdot |B| = |A \times B|$$

Степень не является основной операцией, но её можно определить красиво:

$$|A|^{|B|} = |A^B|$$

Упорядоченность:

$$|A| \leqslant |B| \overset{def}{\iff} = A \prec B$$

После определения структуры надо доказать свойства (ассоциативность и коммутативность $+$ и $\cdot$, дистрибутивность $\cdot$ относительно $+$, нейтральность 0 и 1, $0 < 1 < 2 < \dots$, между соседними числами нет других чисел, аксиому индукции), но мы этого делать не будем.

Любая структура, удовлетворяющая этим свойствам, изоморфна $\mathbb{N}$.

1.3.2 Целые числа

Построим целые числа из натуральных — $(\mathbb{N}, +, \cdot, \leqslant, 0, 1)$.

Определим $\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$, где $(a, b) \sim (c, d) \overset{def}{\iff} a + d = b + c$. Паре (a, b), неформально говоря, будет соответствовать $a - b$.

Замечание. Здесь и далее тильда над плюсом: $\widetilde{+}$ не имеет никакого отношения к отношению эквивалентности $\sim$, она лишь показывает, что данное сложение отличается от сложения в предыдущей структуре.

$$[a, b] \mathbin{\widetilde{+}} [c, d] \coloneqq [a + c, b + d]$$
$$[a, b] \mathbin{\widetilde{\cdot}} [c, d] \coloneqq [ac + bd, ad + bc]$$
$$[a, b] \mathbin{\widetilde{\leqslant}} [c, d] \coloneqq (a + d) \leqslant (b + c)$$
$$\widetilde{0} \coloneqq [0, 0]; \quad \widetilde{1} \coloneqq [1, 0]$$

После определения операций, и проверки, что эквивалентные пары после равных операций эквивалентны, надо проверить свойства целых чисел:

Это упорядоченное кольцо, то есть:

$\widetilde{+}$, $\widetilde{\cdot}$ ассоциативны и коммутативны; $\widetilde{\cdot}$ дистрибутивна относительно $\widetilde{+}$, $\widetilde{0}$ нейтральны относительно $\widetilde{+}, \widetilde{\cdot}$,

$$\forall x : \ \exists y : x + y = 0$$
$$\forall x, y, z : x \leqslant y \Rightarrow x + z \leqslant y + z$$
$$\forall x, y, z : x \leqslant y \land z > 0 \Rightarrow xz \leqslant yz$$

1.3.3 Рациональные числа в теории множеств

Уже есть $\mathbb{N} \subset \mathbb{Z}$ — внутри Z есть подмножество, изоморфное $\mathbb{N}$.

Рассмотрим $\mathbb{Q} \coloneqq (\mathbb{Z} \times (\mathbb{N} \backslash \{0\})) / \sim$, где $(a, b) \sim (c, d) \overset{def}{\iff} ad = bc$.

Теперь введём операции:

$$[a,b]\widetilde{+}[c,d] \overset{def}{=} [ad+bc,bd]$$
$$[a,b]\widetilde{\cdot}[c,d] \overset{def}{=} [ac,bd]$$
$$[a,b] \leqslant [c,d] \overset{def}{\iff} ad \leqslant bc$$
$$\widetilde{0} \coloneqq [0,1]; \quad \widetilde{1} \coloneqq [1,1]$$

После определения операций, и проверки, что эквивалентные пары после равных операций эквивалентны, надо проверить свойства рациональных чисел:

Это упорядоченное поле, такое, что любой элемент получается делением целого числа на натуральное.

1.3.4 Вещественные числа в теории множеств

Уже определены $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q}$.

Определим $\mathbb{R} \coloneqq S/\sim$, где S — множество всех последовательностей Коши $\{q_i\}_{i\in\mathbb{N}}$ рациональных чисел: $\forall n \in \mathbb{N} : \exists m \in \mathbb{N} : \forall i,j \in \mathbb{N} : i,j > m : \quad (|q_i| - |q_j|) < 2^{-n}$.

$$\{q_i\} \sim \{r_i\} \overset{def}{\iff} \lim_{i\to\infty}(q_i - r_i) = 0$$
$$[\{q_i\}] \;\widetilde{+}\; [\{r_i\}] \overset{def}{=} [\{q_i + r_i\}]$$
$$[\{q_i\}] \;\widetilde{\cdot}\; [\{r_i\}] \overset{def}{=} [\{q_i \cdot r_i\}]$$
$$[\{q_i\}] \;\widetilde{\leqslant}\; [\{r_i\}] \overset{def}{=} \exists n,m \in \mathbb{N} : \forall i,j \in \mathbb{N} : i,j > m : \quad q_i - r_j < -2^{-n}$$
$$\widetilde{0} \coloneqq [\{0,0,\dots\}]; \quad \widetilde{1} \coloneqq [\{1,1,\dots\}]$$

После определения операций, и проверки, что эквивалентные последовательности Коши после равных операций эквивалентны, надо проверить, что получилось полное упорядоченное поле, (то есть любое непустое ограниченное сверху множество имеет супремум).

1.3.5 Комплексные числа

Уже определены $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$.

Из аксиом упорядоченного кольца R можно доказать $\nexists i \in R : i^2 = -1$. Поле комплексных чисел есть наименьшее расширение поля вещественных чисел, обладающее таким элементом.

Определим $\mathbb{C} \coloneqq \mathbb{R} \times \mathbb{R}$.

Теперь введём операции

$$(a,b)\widetilde{+}(c,d) \overset{def}{=} [a+c,b+d]$$
$$(a,b)\widetilde{\cdot}(c,d) \overset{def}{=} (ac-bd,ad+bc)$$
$$\widetilde{0} \coloneqq (0,0); \quad \widetilde{1} \coloneqq (1,0); \quad i = (0,1)$$

Можно проверить, что полученная структура — поле, являющееся расширением $\mathbb{R}$ (содержит подмножество, изоморфное $\mathbb{R}$) и содержащее мнимую единицу.

Глава 2

Аксиоматика Цермело — Френкеля с аксиомой выбора.

2.1 Противоречивость наивной теории множеств

К сожалению, наивная теория множеств противоречива. Например, вот пример противоречия: $y \coloneqq \{x | x \notin x\}$. Тогда $y \in y \iff y \notin y$.

Лекция IV

21 сентября 2022 г.

2.2 Аксиомы Цермело — Френкеля с аксиомой выбора, ZFC

Множества обозначаются латинскими буквами, переменными: $x, y, z, \ldots$. Для формул ϕ, ψ определены также формулы $(\phi \vee \psi), (\phi \wedge \psi), (\phi \Rightarrow \psi), ((\phi \iff \psi) \overset{def}{=} (\phi \Rightarrow \psi \wedge \psi \Rightarrow \phi)), \neg\phi$. Также для получения новых формул пишут $\forall x\phi$ или $\exists x\phi$.

Запись $A = \{x | \phi(x)\}$ определяет не множество, но новый класс, который может не быть множеством. Класс — неформальное понятие о формуле.

Для классов определены булевские операции $A \cup B, A \cap B, \neg A$, что на самом деле просто модифицирует задающие класс формулы. Так, $A \cup B = \{x | \phi_A(x) \vee \phi_B(x)\}$.

0. Существует хотя бы одно множество. $\exists x : \ x = x$. Аксиома не всегда приводится, иногда опускается.

1. Аксиома объёмности. $\forall X, Y : \ (\forall u : (u \in X \iff u \in Y)) \iff X = Y$.

2. Аксиома (неупорядоченной) пары. $\forall u, v : \ (\exists \{u, v\} = X$ (это такое обозначение множества) $: \forall z : (z \in X \iff z = u \vee z = v))$.

   Определение 2.2.1 (Упорядоченная пара)**.** Упорядоченной парой из элементов x, y называется множество $(x, y) \overset{def}{=} \{x, \{x, y\}\}$.

   Определение 2.2.2 (Одноэлементное множество)**.** $\{x\} \overset{def}{=} \{x, x\}$.

   Предложение 2.2.1. $(x, y) = (x', y') \iff x = x' \wedge y = y'$.

3. Аксиома выделения. $\forall X, \phi(u)$ ($\phi(u)$ — формула от свободной переменной) $: \ (\exists \{x \in X | \phi(x)\} = Y : \ u \in Y \iff (u \in X \wedge \phi(u)))$. Пересечение класса со множеством – множество.

   Теорема 2.2.1. Существует пустое множество

Доказательство. Рассмотрим множество из Аксиомы 0, назовём его x, рассмотрим $\varnothing \stackrel{def}{=} \{u \in x | \neg(u = u)\}$. Видно, что $\forall x : x \in \varnothing \iff x \neq x$, откуда получаем $\forall x : \neg(x \in o)$. □

Теорема 2.2.2. Существует разность множеств $X \backslash Y$.

Доказательство. Определим её, как $\{u \in X | u \notin Y\}$. □

4. Аксиома объединения. $\forall X : \ \exists Y : \ (\forall z : \ u \in z \wedge z \in X \Rightarrow u \in Y)$. Аксиома говорит, что существует множество, содержащее объединение элементов X.

   Теорема 2.2.3. Существует объединение элементов X, обозначаемое $\left(\bigcup\limits_{z \in X} z\right)$.

   Доказательство. Рассмотрим для данного X Y из данной аксиомы. Используя аксиому выделения, получим $\left(\bigcup\limits_{z \in X} z\right) \stackrel{def}{=} \{u \in Y | \exists z \in X : u \in z\}$. □

   Теорема 2.2.4. Существует пересечение элементов X, обозначаемое $\left(\bigcap\limits_{z \in X} z\right)$

   Доказательство. Рассмотрим для данного X Y из данной аксиомы. Используя аксиому выделения, получим $\left(\bigcap\limits_{z \in X} z\right) \stackrel{def}{=} \{u \in Y | \forall z \in X : u \in z\}$. □

5. Аксиома степени. $\forall X : \ \exists \mathcal{P}(X) = 2^X : \ (u \in 2^X \iff u \subseteq X)$.

   Определение 2.2.3 (Подмножество)**.** $Y \subseteq X \stackrel{def}{\iff} \forall u : (u \in Y \Rightarrow u \in X)$.

   Теорема 2.2.5. Для множеств A, B существует множество $A \times B = \{(a, b) | a \in A \wedge b \in B\}$.

   Доказательство.

   - $\{x\} \in \mathcal{P}(X) \subseteq \mathcal{P}(X \cup Y)$
   - $\{x, y\} \in \mathcal{P}(X \cup Y)$
   - $(x, y) = \{x, \{x, y\}\} \in \mathcal{P}(\mathcal{P}(X \cup Y))$.
   - $X \times Y \stackrel{def}{=} \{z \in \mathcal{P}(\mathcal{P}(X \cup Y)) | \exists x \in X, y \in Y : z = (x, y)\}$ □

6. Аксиома замены.

   $\forall \phi(u, v) : (\forall x, y, y' : \ \phi(x, y) \wedge \phi(x, y') \Rightarrow y = y') \Rightarrow \forall X : \ (\exists Y : \ (\forall u, v : u \in X \wedge \phi(u, v) \Rightarrow v \in Y)$. Неформальнее, если ϕ — функциональное отношение (быть может не везде определённая функция), то существует множество, содержащее образ $\phi(X)$.

   Используя аксиому выделения, можно доказать существование множества, *являющегося* образом $\phi(X)$.

7. Аксиома бесконечности. $\exists Y : (\varnothing \in Y \wedge (\forall y : y \in Y \Rightarrow (y \cup \{y\}) \in Y))$.

   Несложно видеть, что $\varnothing \in Y, \{\varnothing\} \in Y, \{\varnothing, \{\varnothing\}\} \in Y, \ldots$

8. Аксиома фундирования (иногда называется аксиомой регулярности).

   $\forall X : \ (X \neq \varnothing \Rightarrow \exists x : \ (x \in X \wedge \forall u \in x : u \notin X))$.

Неформально говоря, для бинарного отношения $\in$ на непустом множестве X существует минимальный элемент внутри X.

Предложение 2.2.2. $\nexists X : X \in X$.

Доказательство. Предположим, что существует $X \in X$. Для противоречия рассмотрим $\{X\}$. Из определения $\{X\}$ единственный $Y \in \{X\}$ — это X. Но тогда противоречие с аксиомой фундирования, ведь $X \in X$. $\square$

9. Аксиома выбора. $\forall X : \ \exists f : (2^X \setminus \{\varnothing\}) \to X : \ \forall Y \subseteq X : \ (Y = \varnothing \vee f(Y) \in Y)$.

   Замечание. Функция f — особое множество пар.

   Часто использование аксиомы выбора подчёркивается отдельно, так как она неконструктивна и из неё подчас следуют странные, контринтуитивные вещи.

Факт 2.2.1. *В ZF AC равносильна следующему: $\forall$ бесконечного $A : A \simeq A \times A$.*

Теорема 2.2.6. $A \prec B \vee B \prec A \vee A \simeq B$ в ZFC

Доказательство. Будет подальше (раздел 2.5) $\square$

Лекция V

22 сентября 2022 г.

2.3 Вполне упорядоченные множества. Ординалы

Пусть $(P; \leqslant)$ — частичный порядок: антирефлексивность ($x < y \iff x \leqslant y \wedge x \neq y$), транзитивность.

Можно писать и $(P; \leqslant)$, и $(P; <)$, так как понятно, как из $<$ получить $\leqslant$, и наоборот (равенство считаем уже заданным на множестве).

Определение 2.3.1 (Фундированный порядок)**.** P — фундированный порядок, если любое подмножество имеет минимальный элемент: $\forall X \subseteq P : \exists x \in P : \nexists y : y < x$.

Определение 2.3.2 (Линейный порядок)**.** Любые два элемента сравнимы: $\forall x, y \in P : \left[\begin{array}{l} x < y \\ y < x \\ x = y \end{array}\right.$

Определение 2.3.3 (Верхняя граница для множества $X \subseteq P$)**.** Такое число $y \in P : \forall x \in X : x \leqslant y$.

Определение 2.3.4 (Точная (наименьшая) верхняя граница, supremum)**.** Наименьшее число в множестве верхних границ. $y = \sup X$.

Рассмотрим множество $M = \left\{x \in \mathbb{Q} \middle| x^2 < 2\right\}$ в каком-то порядке. Тогда $\sup_{(\mathbb{R};\leqslant)} M = \sqrt{2}$; $\nexists \sup_{(\mathbb{Q};\leqslant)} M$.

Определение 2.3.5 (Начальный сегмент, задаваемый элементом p)**.** $\widehat{p} = \{x \in P | x < p\}$.

Пусть $(P, <)$ и $(Q, \prec)$ — частичные порядки.

Определение 2.3.6 (Изоморфизм из P на Q)**.** Биекция $f : P \to Q$, такая, что $\forall x, y \in P :$ $x < y \iff f(x) \prec f(y)$.

Определение 2.3.7 (Изоморфность частичных порядков P и Q)**.** Существование изоморфизма из P в Q.

Факт 2.3.1. *Изоморфизм — отношение эквивалентности.*

Определение 2.3.8 (Вложение)**.** Инъекция $f : P \to Q$, сохраняющая порядок: $\forall x, y \in P :$ $x < y \iff f(x) \prec f(y)$.

Определение 2.3.9 (Полный порядок или вполне упорядоченное множество $(P; <)$)**.** Линейный фундированный порядок $(P; <)$: в любом подмножестве есть минимум, все элементы сравнимы.

2.3.1 Свойства полных порядков

$(P;<)$ и $(Q;\prec)$ ниже — полные порядки.

1. Для любого вложения в себя $f : P \to P$ верно: $\forall p : p \leqslant f(p)$.

   Доказательство. От противного: $\exists p \in P : p \nleqslant f(p)$. Тогда $\{p \in P | f(p) < p\} \neq \varnothing$, а ещё в этом множестве есть минимальный элемент p_0. Минимальность означает следующее:

   $$\forall x \in P : x < p \Rightarrow x \leqslant f(x)$$

   Но вложение сохраняет порядок, из $f(x) < f(p_0)$ и транзитивности следует $\forall x \in \widehat{p_0} : x < f(p_0)$ Тогда $f(p_0)$ – верхняя грань $\widehat{p_0}$. В то же время $p_0 = \sup \widehat{p_0}$, откуда $p_0 \leqslant f(p_0)$ □

2. Никакой полный порядок не может быть изоморфен своему начальному сегменту $\forall p \in P : P \ncong \widehat{p}$.

   Доказательство. Допустим, для некоего p существует вложение $f : P \to \widehat{p}$. Тогда $f(p) < p$, противоречие. □

3. Для любых P, Q : $\left[\begin{array}{c} P \cong Q \\ \exists p \in P : \widehat{p} \cong Q \\ \exists q \in Q : P \cong \widehat{q} \end{array}\right.$, причём выполняется ровно одно.

   Доказательство.

   - Если выполняются одновременно первое и ещё какое-то, то вполне упорядоченное множество изоморфно своему начальному сегменту.
   - Если одновременно выполняются второе и третье, то тоже существует вложение из P в некое несобственное подмножество — композиция изоморфизмов.
   - Докажем, что выполняется хотя бы одно.
     - Введём отношение $f \overset{def}{=} \{(p,q) \in P \times Q | \widehat{p} \cong \widehat{q}\}$. Это отношение функционально: если $f(p,q)$ и $f(p,q')$, то $\widehat{q} \cong \widehat{q}'$, откуда если $q \neq q'$, то больший из q и q' порождает полный порядок, изоморфный своему начальному сегменту (порождённому меньшим из q и q'). Аналогично это инъекция. Будем писать $f(p) = q$; $f^{-1}(q) = p$.
     - Утверждается, что либо $\operatorname{dom} f = P$, либо $\operatorname{rng} f = Q$.
     - Заметим, что если $p \in \operatorname{rng} f$, то $\forall x < p : \ x \in \operatorname{rng} f$. Рассмотрим некий $x < p$ и покажем, что действительно $\exists y \in Q : \widehat{x} \cong \widehat{y}$.

       Известно, что $\widehat{p} \overset{f_p}{\cong} \widehat{q}$. Пусть данный изоморфизм переводит x в $y = f_p(x)$ $(y \in Q)$. Утверждается, что $\widehat{x} \cong \widehat{y}$. Ну, в самом деле, $\forall a < x : f_p(a) < f_p(x)$ — изоморфизм сохраняет порядок; $\forall b \prec y : f_p^{-1}(b) < f_p^{-1}(y)$ — обратный изоморфизм тоже сохраняет порядок.
     - Аналогично если $q \in \operatorname{dom} f$, то $\forall y \prec q : \ y \in \operatorname{dom} f$.
     - Предположим противное: $\operatorname{dom} f \subsetneq P$. Пусть p — наименьший элемент $P \backslash (\operatorname{dom} f)$ (существует из-за фундированности). Аналогично, q — наименьший элемент, такой, что $q \notin \operatorname{rng}(f)$. Заметим, что $\widehat{p} = \operatorname{dom} f$; $\quad \widehat{q} = \operatorname{rng} f$.

       Утверждается, что $f : \widehat{p} \to \widehat{q}$ — изоморфизм, так как для любых $p_1, p_2 : p_1 < p_2 < p$ изоморфизм, переводящий $\widehat{p_2}$ в $\widehat{q_2}$, переводит p_1 в некий $q_1 : q_1 \prec q_2$. Значит, порядок сохраняется.

       Но тогда получается $\widehat{p} \cong \widehat{q}$, противоречие.

– Итак, $\operatorname{dom} f = P \wedge \operatorname{rng} f = Q$. В любом случае мы нашли изоморфизм между одним порядком, и подмножеством другого. А подмножество — начальный сегмент: уже доказано, что $\operatorname{dom} f$ и $\operatorname{rng} f$ каждый если не совпадают с порядком, то являются начальными сегментами.

□

Лекция VI
4 октября 2022 г.

Комментарии к пункту 3 из предыдущей лекции: Для доказательства достаточно рассмотреть три случая: *Хотя я пока не очень понимаю, почему недостаточно того, что написано выше*

1. P, Q не имеют наибольшего элемента. Этот случай, как сказано на лекции, полностью покрывается приведённым выше доказательством
2. Ровно один порядок, без потери общности, P — содержит наибольший элемент. Тогда у него есть несколько, из-за фундированности — конечное число — предшественников $p_0, p_1, \ldots, p_n$, таких, что $\widehat{p_n}$ не имеет наибольшего элемента.
3. И P, и Q содержат наибольший элемент. ...

Замечание. Фундированное множество — именно то множество, на котором можно использовать метод математической индукции. Для полного порядка $(P; <)$ определим множество $A \subseteq P$, такое, что

$$\forall p \in P : (\widehat{p} \subseteq A \Rightarrow p \in A) \Rightarrow A = P$$

Доказательство. От противного — найти минимальный элемент в $P \backslash A$. □

2.3.2 Ординалы

Определение 2.3.10 (Транзитивное множество S)**.** $\forall x, y : (x \in y \wedge y \in S) \Rightarrow x \in S$.

Определение 2.3.11 (Ординал или порядковое число)**.** Такое транзитивное множество S, что

$$\forall x, y \in S : \left[\begin{array}{l} x \in y \\ y \in x \\ x = y \end{array}\right. \tag{2.1}$$

Несложно видеть, что из-за аксиомы фундированности (регулярности) возможно лишь одно из трёх.

Обозначим ординалы греческими буквами $\alpha, \beta, \ldots$, и класс ординалов обозначим Ord.

Пусть $<$ — сужение отношения $\in$ на Ord. Иначе говоря, для $a, b \in \mathrm{Ord}$ вместо $a \in b$ будем (иногда) писать $a < b$.

Свойства ординалов

1. $x \in \alpha \Rightarrow x \in \mathrm{Ord}$

   Доказательство. $\forall u \in v \in x$: так как α — ординал, то $u, v \in \alpha$, и для u, v выполняется конъюнкция (2.1). Кроме того, она выполняется для u и x, откуда $u \in x$ (остальные альтернативы — $x \in u \vee x = u$ — вызывают противоречие с фундированностью). □

2. $\alpha = \{\beta | \beta < \alpha\}$.

   Доказательство. Оставлю, как упражнение. □

3. Вполне упорядоченные множества изоморфны $(\alpha, <) \cong (\beta, <)$, если и только если они равны $\alpha = \beta$.

Доказательство.

$\Leftarrow$. Очевидно

$\Rightarrow$. $(\alpha, <) \cong (\beta, <) \Rightarrow \exists$ биекция $f : \alpha \to \beta$. Докажем, что $\forall x \in \alpha : x = f(x)$.

Пусть, это не так. Возьмём наименьшее $x \neq f(x)$. Тогда $\forall z < x : f(z) = z$. $x = \{z \in \alpha | z < x\}$. С другой стороны, $f(x) = \{f(z) | z \in \alpha \wedge z < x\}$, откуда $x = f(x)$, противоречие.

Но тогда получается, что $\alpha \subseteq \beta$, а по симметрии — $\alpha = \beta$. □

4. $\alpha < \beta \vee \beta < \alpha \vee \alpha = \beta$.

Доказательство. Вытекает из теоремы о вполне упорядоченных множеств и предыдущего свойства. □

5. $\alpha \leqslant \beta \iff \alpha \subseteq \beta$

Доказательство. Докажем, что $\alpha \in \beta \iff \alpha \subsetneq \beta$. В правую сторону очевидно, $\forall x \in \alpha : x \in \beta$ из транзитивности. Но $\alpha \neq \beta$, откуда $\alpha \subsetneq \beta$. В левую сторону — $\alpha \in (\beta \backslash \alpha)$, минимальный элемент разности. □

Определение 2.3.12 (Наименьший ординал, больший α)**.** $\alpha + 1 \overset{def}{=} \alpha \cup \{\alpha\}$. Несложно показать, что $\alpha \cup \{\alpha\}$ — ординал, проверить транзитивность и конъюнкцию (2.1).

6. $\nexists \beta \in \mathrm{Ord} : \alpha < \beta < \alpha + 1$.

Доказательство. От противного: $\beta \in \alpha \cup \{\alpha\}$. Либо $\alpha = \beta$, либо противоречие с аксиомой фундированности, так как $\alpha \in \beta$. □

7. Любое множество ординалов A вполне упорядоченно отношением $<$ (из п. 4), причём $\bigcup A = \sup A$.

Доказательство.

- Любые два ординала сравнимы, причём если ординалы $x, y, z \in A$ и $x \in y \in z$, то $x \in z$.
- $\bigcup A$ — ординал. Проверим транзитивность: $x \in y \in \bigcup A$. Но тогда $\exists \alpha \in A : y \in \alpha$. Тогда $x \in \alpha$ по транзитивности, откуда $x \in \bigcup A$.
- Покажем, что $\bigcup A$ — верхняя граница A по отношению $<$. $\forall \alpha \in A : \alpha \leqslant \bigcup A$. Это всё равно, что $\alpha \subseteq \bigcup A$.
- Покажем, что $\bigcup A = \sup A$ — наименьшая верхняя граница. Покажем, что для любой верхней границы $\beta : \bigcup A \leqslant \beta$. Это верно, так как $\forall \alpha \in A : \alpha \subseteq \beta$. □

8. Класс Ord не является множеством.

Доказательство. Пусть, является. Тогда $\alpha := \bigcup \mathrm{Ord} = \sup \mathrm{Ord}$ — наибольший ординал. Но тогда рассмотрим $\alpha + 1$. □

9. Любое вполне упорядоченное множество изоморфно единственному ординалу.

Доказательство. Единственность очевидна, так как изоморфные ординалы равны.

Рассмотрим вполне упорядоченное множество $(P; \sqsubset)$. Сначала заметим, что $\forall p \in P : \exists \alpha \in \mathrm{Ord} : \widehat{p} \cong \alpha$. Это верно из принципа наименьшего элемента во вполне упорядоченных множествах — для минимального p такого, что $\nexists \alpha \cong \widehat{p}$ подойдёт ординал $\bigcup \{\alpha \in \mathrm{Ord} | \exists q \in \widehat{p} : \alpha \cong \widehat{q}\}$.

Теперь рассмотрим $M = \{\alpha | \exists p \in P : \alpha \cong \widehat{p}\}$. Это множество по аксиоме замены. Но тогда $\bigcup M \cong P$. □

Лекция VII

11 октября 2022 г.

Типы ординалов

0. Нулевой ординал $\varnothing$.
1. Последовательные ординалы (последователи) — ординалы вида $\{\alpha\}+1$
2. Предельные ординалы — все остальные ординалы

Определение 2.3.13 (Натуральное число)**.** Непредельный ординал, все элементы которого также не являются предельными. Множество натуральных чисел обозначается $\omega = \{0, 1, 2, \dots\}$.

Предложение 2.3.1. *Множество ω существует.*

Доказательство. По аксиоме бесконечности $\exists X : (\varnothing \in X \land \forall x \in X : (x \cup \{x\}) \in X))$.

Заметим, что $0 = \varnothing \in X$.

Теперь заметим, что $1 = \{0\} \cup \varnothing \in X$.

Можно доказать по индукции, что любое натуральное число содержится в X.

Теперь воспользуемся аксиомой выделения, получим множество натуральных чисел

$$\omega = \{x \in X | x \text{ — натуральное}\}$$

□

Определение 2.3.14 (Конечное множество)**.** Множество, равномощное некоторому натуральному числу.

Шкала ординалов

$$0, 1, \dots, \omega, \omega+1, (\omega+2 = (\omega+1)+1), \dots, (\omega\cdot 2 = \omega+\omega), \omega\cdot 2+1, \dots, \omega\cdot 3, \dots, \omega\cdot\omega, \dots$$

Теорема 2.3.1 (О рекурсивных определениях по ординалам)**.** Для любой функции-класса $G : V \to V$, где V — класс всех множеств, $\exists!$ функция-класс $F : \mathrm{Ord} \to V : F(\alpha) = G\left(F\big|_\alpha\right)$, где $F\big|_\alpha$ — функция, ограниченная на α, а именно, $F\big|_\alpha \overset{def}{=} \{(\beta, y) \in F | \beta < \alpha\}$. Напоминание: $F(x) = y \overset{def}{\iff} (x, y) \in F$

Доказательство.

- Единственность: пусть существуют две такие функции F, F'. Утверждается, что $\forall \alpha \in \mathrm{Ord} : F(\alpha) = F'(\alpha)$. Предположим, что это не так, возьмём наименьшее α такое, что это не так. Тогда $F\big|_\alpha = F'\big|_\alpha$, откуда $F(\alpha) = F'(\alpha) = G\left(F\big|_\alpha\right)$, противоречие.
- Существование: рассмотрим некоторый класс функций

  $$C = \left\{ f : \alpha \to V \middle| \alpha \in \mathrm{Ord} \land (\forall \beta < \alpha : f(\beta) = G\left(f\big|_\beta\right)\right\}$$

  Заметим, что если $f, f' \in C$, то $f \subseteq f' \lor f' \subseteq f$. Утверждается, что искомая функция-класс

  $$F = \bigcup C$$

  В самом деле, можно заметить, что если некое $\alpha \notin \operatorname{dom} F$, то найдётся функция H, такая, что $\operatorname{dom} H = \alpha + 1$, определённая так: $H(\beta) = \begin{cases} F(\beta), & \beta < \alpha \\ G\left(F\big|_\beta\right), & \beta = \alpha \end{cases}$. □

2.4 Эквивалентные формулировки аксиомы выбора

2.4.1 О наибольшем и максимальном элементах в $(X, \sqsubset)$

Определение 2.4.1 (Наибольший элемент)**.** Элемент $x \in X$ такой, что $\forall y \in X : y \sqsubseteq x$.

Определение 2.4.2 (Максимальный элемент в $(X, \sqsubset)$)**.** Элемент $x \in X$ такой, что $\nexists y : x \sqsubset y$.

В слове *наибольший* есть подстрока «больший», этот элемент, в отличие от максимального, действительно больше остальных.

2.4.2 Формулировки

Теорема 2.4.1 (Лемма Цорна, принцип максимального элемента)**.** Если в частичном порядке $(X, \sqsubset)$ любое линейно-упорядоченное множество (любая цепь) имеет верхнюю границу, то в X имеется максимальный элемент.

Теорема 2.4.2 (Теорема Цермело, принцип полного упорядочивания)**.** Любое множество A можно вполне упорядочить:

$$\exists \text{ бинарное отношение } R \subseteq A \times A : (A, R) \text{ — вполне упорядоченное множество}$$

Теорема 2.4.3. Из аксиом ZF следует эквивалентность следующих утверждений:

1. Аксиома выбора, AC.
2. Лемма Цорна, ZL.
3. Теорема Цермело, ZT.

Доказательство.

- $AC \Rightarrow ZL$.

  Рассмотрим некоторое частично-упорядоченное множество $(X, \sqsubset)$, в котором любая цепь ограничена сверху. Докажем, что есть максимальный элемент от противного.

  $\forall x \in X : \exists y \in X : x \sqsubset y$. Рассмотрим $\mathscr{L} = \{L \subseteq X | (L, \sqsubset) \text{ — лум}\}$. Определим $B(L) = \{y | \forall x \in L : (x \sqsubset y)\}$. Из посылки теоремы: $\{y | \forall x \in L : (x \sqsubseteq y)\} \neq \varnothing$; пусть его элемент y. Тогда $B(L) \neq \varnothing$ тоже, так как для y существует $y' : y \sqsubset y'$, такой y' уже строго больше всех элементов из L.

  Заметим, что $B : \mathscr{L} \to \left(2^X \backslash \{\varnothing\}\right)$. Также, по аксиоме выбора, есть функция $f : \left(2^X \backslash \{\varnothing\}\right) \to X$. Рассмотрим композицию этих функций $g = f \circ B : g(L) = f(B(L))$. Тогда заметим, что $\forall L \in \mathscr{L}, \forall x \in L : x \sqsubset g(L)$.

  Пусть $x_0 = g(\varnothing); x_0 \in X$. Фактически, x_0 — любой элемент из X. Построим некоторую функцию F по рекурсии. Для этого сначала скажем, что

  $$G : V \to V, G(z) = \begin{cases} g(\operatorname{rng}(z)), & z \text{ — бинарное отношение (множество пар), и } \operatorname{rng}(z) \in \mathscr{L} \\ x_0, & \text{иначе} \end{cases}$$

  Теперь определим $F : \mathrm{Ord} \to X; \quad F(\alpha) = g\left(\operatorname{rng}\left(F\big|_\alpha\right)\right) = g(\{F(\beta) | \beta < \alpha\})$. Здесь я пишу первую строчку из определения G, так как доказуемо для всех $\alpha \in \mathrm{Ord} : F(\alpha) \in \mathscr{L}$. Заметим, что F — инъекция, так как разные ординалы переходят в разные элементы. Отсюда $F^{-1} : X \to \mathrm{Ord}$ — сюръекция. Тогда по аксиоме замены класс Ord является множеством, противоречие.

- $ZL \Rightarrow ZT$.

  Пусть A — любое множество. Рассмотрим множество

  $$X = \{f : \alpha \to A | (\alpha \in \mathrm{Ord}) \wedge (f \text{ — инъекция})\}$$

Удостоверимся, что X — множество: рассмотрим другое множество

$$Y = \{(P;\sqsubset) | P \subseteq A \text{ и } (P;\sqsubset) \text{ — полный порядок}\}$$

Y является множеством, так как $Y \subseteq 2^A \times (A \times A)$. Тогда утверждается, что всякому элементу Y соответствует ровно один ординал α_p. Несложно видеть, что тогда только множество этих $\{\alpha_p\}$ может быть областью определений функций из X.

Утверждается, что для $(X, \subseteq)$ применима лемма Цорна: любое линейно-упорядоченное подмножество в X ограничено сверху. В самом деле, для $L \in X : \bigcup L \in X$ и $\bigcup L$ — верхняя граница. Значит, существует максимальный элемент в X. Обозначим $(u : \alpha \to A)$ — максимальный элемент в $(X, \subseteq)$.

Докажем, что u — ещё и сюръекция: пусть существует $y \in X$, такой, что $u^{-1}(y) = \varnothing$. Но тогда рассмотрим $u' : (\alpha + 1) \to A; \quad u'(\beta) = \begin{cases} u(\beta), & \beta < \alpha \\ y, & \beta = \alpha \end{cases}$, противоречие с максимальностью u. Отсюда $u : \alpha \to A$ — биекция. Тогда определим полный порядок на множестве A следующим образом: $a < b \iff u^{-1}(a) < u^{-1}(b)$.

- $ZT \Rightarrow AC$

  Докажем, что для любого $X : \exists f : \left(2^X \setminus \{\varnothing\}\right) \to X$, такая, что $f(S) \in S$. Для этого всего лишь найдём полный порядок по теореме Цермело, после чего возьмём минимальный элемент, пользуясь нашей операцией сравнения. $\square$

Лекция VIII

18 октября 2022 г.

2.5 Сравнимость мощностей, шкала кардиналов, кумулятивная иерархия

Теорема 2.5.1. Для любых множеств A и B выполняется ровно одно из условий: $\left[\begin{array}{l} A \cong B \\ A \prec B \\ B \prec A \end{array}\right.$

Доказательство. Мы уже удостоверялись, что любые два условия не могут выполняться одновременно.

По теореме Цермело, любое множество можно вполне упорядочить. Тогда рассмотрим полные порядки $(A; \sqsubset_A)$ И $(B; \sqsubset_B)$.

Но тогда выполняется ровно одно из следующих условий: $\left[\begin{array}{c} A \simeq B \\ \exists! q \in B : A \simeq \widehat{q} \\ \exists! p \in A : B \simeq \widehat{p} \end{array}\right.$

Отсюда очевидно, что есть либо инъекция из A в B, либо — наоборот — инъекция из B в A, либо вдруг даже биекция. $\square$

Определение 2.5.1 (Мощность)**.** Мощность $|A|$ множества A — наименьший ординал, изоморфный A.

Определение 2.5.2 (Кардинал)**.** Ординал, не равномощный никакому меньшему ординалу. Класс всех кардиналов обозначается Card.

Замечание. $\omega + 1 \simeq \omega \cup \{\omega\}$ — тоже счётное множество; $\omega + 1$ — не является кардиналом. Более того, $\omega + \omega$ и даже $\omega \cdot \omega$ не являются кардиналами, они все счётны.

ω_1 — наименьший несчётный ординал. Из аксиом ZFC не ясно, континуален ли ω_1.

Определение 2.5.3 (Следующий кардинал)**.** Для кардинала $\varkappa$ существует $\varkappa^+$ — наименьший ординал, больший $\varkappa$.

Определим F, используя рекурсию по ординалам: $F(\alpha) = \begin{cases} 0, & \alpha = 0 \\ F(\beta)^+, & \alpha = \beta + 1 \\ \sup\limits_{\gamma<\alpha} F(\gamma), & \alpha \text{ — предельный ординал} \end{cases}$

Несложно видеть, и несложно доказать по индукции, что $F(\alpha) = \alpha$ для любого конечного $\alpha \in \omega$. $F(\omega) = \omega$, $F(\omega + 1) = \omega^+ = \omega_1$, $F(\omega + \omega) = \sup\{\omega, \omega^+, (\omega^+)^+, \dots\}\dots$

Предложение 2.5.1. *Функция F — функция-класс, устанавливающая изоморфизм между классом ординалов* $(\mathrm{Ord}, <)$ *и классом кардиналов* $(\mathrm{Card}, <)$.

Доказательство. Заметим, что F возрастает, а именно, $\forall \alpha < \beta : F(\alpha) < F(\beta)$. Это несложно проверить.

- Докажем по индукции, что $F(\alpha)$ — кардинал для всякого $\alpha \in \mathrm{Ord}$. Достаточно убедиться про $F(\alpha)$, где α — предельный, остальное очевидно. От противного: пусть $F(\alpha) \cong \delta$, где δ — кардинал, меньший $F(\alpha)$. Есть два случая:
  - $\forall \psi < \alpha : F(\psi) < \delta$. В таком случае $F(\alpha) = \sup\limits_{\psi<\alpha} F(\psi) \leqslant \delta$ и никак не может быть больше δ.
  - $\exists \psi < \alpha : F(\psi) \geqslant \delta$. Так как α — предельный, то $\psi + 1 < \alpha$ тоже. Но $F(\psi) \prec F(\psi + 1)$, откуда $F(\alpha) \prec F(\psi + 1)$. Тогда получаем противоречие, ведь очевидно, что мощность $|F(\dots)|$ возрастает по мере возрастания аргумента.
- Теперь проверим, что всякий ординал лежит в образе F. Опять же пойдём от противного: пусть наименьший ординал, не достигающийся функцией, равен δ.

  Все меньшие достигались, обозначим $\mathcal{M}$ за прообраз всех меньших ординалов.

  Покажем, что $F(\sigma) = \delta$, где σ — наименьший элемент, не лежащий в $\mathcal{M}$.
  - Если σ — предельный, то $F(\sigma) = \sup\limits_{\xi<\sigma} F(\xi)$, что не больше δ.
  - Иначе $\sigma = \xi + 1$ для некоего ординала ξ. $F(\xi) < \delta$, значит по определению $F(\sigma) \leqslant \delta$.

  Но $\sigma \notin \mathcal{M}$, значит, $F(\sigma) = \delta$.

□

2.5.1 Шкала бесконечных кардиналов

$\{\aleph_\alpha\}_{\alpha \in \mathrm{Ord}} \overset{def}{=} F(\omega + \alpha)$.

Определение 2.5.4 (Сумма ординалов)**.** Сумма ординалов $\alpha + \beta$ — ординал, изоморфный полному порядку $(P; <)$, где $P = (\alpha \times \{0\}) \cup (\beta \times \{1\})$ и

$$(x, i) < (y, j) \iff \begin{cases} x < y, & i = j \\ i < j, & i \neq j \end{cases}$$

По сути, мы пририсовали к α справа β и рассмотрели это как новый полный порядок.

2.5.2 Кумулятивная иерархия

Определим рекурсией по ординалам $\{V_\alpha\}_{\alpha \in \mathrm{Ord}}$:

$$V_\alpha = \begin{cases} 0, & \alpha = 0 \\ 2^{F(\beta)}, & \alpha = \beta + 1 \\ \bigcup_{\gamma<\alpha} V_\gamma, & \alpha \text{ — предельный ординал} \end{cases}$$

Эта последовательность V_α — кумулятивная иерархия

Теорема 2.5.2 (Фон Нейман)**.** Всякое множество встретится в $V : \bigcup_{\alpha\in\mathrm{Ord}} = V$, где V — множество всех множеств.

2.5.3 Арифметика кардиналов

$\varkappa^+$ — наименьший кардинал, больший $\varkappa$

$\varkappa + \lambda \overset{def}{=} |\{\{0\} \times \varkappa\} \cup \{\{1\} \times \lambda\}|$

$\varkappa \cdot \lambda \overset{def}{=} |\varkappa \times \lambda|$

$\varkappa^\lambda \overset{def}{=} |\{f : \varkappa \to \lambda\}|$

Свойства

1. Сложение и умножение коммутативны и ассоциативны
2. Умножение дистрибутивно относительно сложения
3. 0, 1 — нейтральны относительно понятно чего
4. $(\varkappa \cdot \lambda)^\mu = \varkappa^\mu \cdot \lambda^\mu$
5. $(\varkappa^\lambda)^\mu = \varkappa^{(\lambda\cdot\mu)}$
6. Нетривиальное свойство, с доказательством от Хаусдорфа: $(\varkappa^+)^\lambda = \varkappa^+ \cdot \varkappa^\lambda$
7. $\aleph_\alpha + \aleph_\beta = \aleph_\alpha \cdot \aleph_\beta = \max\{\aleph_\alpha, \aleph_\beta\}$. Часть про произведение равносильно аксиоме выбора.
8. $\alpha \leqslant \beta \iff \aleph_\alpha^{\aleph_\beta} = 2^{\aleph_\beta}$

Видимо, первые 5 считаются очевидными, остальные — нетривиальными. Как бы то ни было, на лекции не было ни одного доказательства...

2.5.4 Арифметика ординалов

Сумма ординалов уже определена выше.

Произведение ординалов: $\alpha \cdot \beta = (P, \sqsubset)$, где $P = \alpha \times \beta$ и

$$(a, b) \sqsubset (a', b') \iff (b < b') \vee (b = b' \wedge a < a')$$

Также операции можно определить рекурсивно:

$$\alpha + \beta = \begin{cases} \alpha, & \beta = 0 \\ (\alpha + \gamma) + 1, & \beta = \gamma + 1 \\ \sup\limits_{\gamma<\beta} \alpha + \gamma, & \beta \text{ — предельный} \end{cases}$$

$$\alpha \cdot \beta = \begin{cases} 0, & \beta = 0 \\ (\alpha \cdot \gamma) + \alpha, & \beta = \gamma + 1 \\ \sup\limits_{\gamma<\beta} \alpha \cdot \gamma, & \beta \text{ — предельный} \end{cases}$$

$$\alpha^\beta = \begin{cases} 1, & \beta = 0 \\ (\alpha^\gamma) \cdot \alpha, & \beta = \gamma + 1 \\ \sup\limits_{\gamma<\beta} \alpha^\gamma, & \beta \text{ — предельный} \end{cases}$$

Свойства

1. $+, \cdot$ не коммутативны, но ассоциативны.
2. $\cdot$ дистрибутивно слева относительно $+$ (но не справа).
3. 0, 1 нейтральны относительно $\cdot, +$.
4. $\alpha^\beta \cdot \alpha^\gamma = \alpha^{\beta+\gamma}$.
5. $(\alpha^\beta)^\gamma = \alpha^{(\beta\cdot\gamma)}$.