Логика первого порядка

Логика высказываний

Язык логики высказываний:

- символы P, Q, R, … для «первичных высказываний» (*атомов*) произвольной природы, которые играют роль переменных;
- *пропозициональные связки* — символы

  $\wedge$ — *конъюнкция* (логическое «и»),

  $\vee$ — *дизъюнкция* (логическое «или»),

  $\neg$ — *отрицание* (логическое «не»),

  $\to$ — *импликация* («влечёт за собой»);
- служебные символы — скобки (и).

Пропозициональные формулы определяются рекурсивно:

1) все атомы — формулы;
2) если A и B — формулы, то $A \wedge B$, $A \vee B$, $\neg A$ и $A \to B$ — формулы.

Соглашение о скобках: $(A) \rightsquigarrow A$, $(A \wedge B) \wedge C \rightsquigarrow A \wedge B \wedge C$, $(A \vee B) \vee C \rightsquigarrow A \vee B \vee C$. Скобки также опускаются, если их можно однозначно восстановить по приоритетам: $\neg$, $\wedge$, $\vee$, $\to$.

Длина формулы — число символов (считая повторения и опущенные скобки).

Тавтологии

Введём два «внешних» символа И («истина») и Л («ложь»). *Истинностная оценка* на множестве $\mathscr{P}$ первичных высказываний — это любая функция $\nu\colon \mathscr{P} \to \{\text{И}, \text{Л}\}$. Для каждой истинностной оценки определяется её продолжение $\bar{\nu}$ на все пропозициональные формулы индукцией по длине формулы с помощью общеизвестных таблиц истинности.

Пропозициональная формула A называется *тавтологией*, если $\bar{\nu}(A) = \text{И}$ для любой истинностной оценки $\nu\colon \mathscr{P} \to \{\text{И}, \text{Л}\}$.

Тавтологии играют роль аксиом в логике высказываний. Достаточный набор тавтологий:

$A \wedge B \to A$,
$A \wedge B \to B$,
$A \to (A \vee B)$,
$B \to (A \vee B)$

$A \vee \neg A$,
$A \to (B \to A)$,
$\neg A \to (A \to B)$,
$A \to (B \to (A \wedge B))$,

$(A \to (B \to C)) \to ((A \to B) \to (A \to C))$,
$(A \to C) \to ((B \to C) \to ((A \vee B) \to C))$,
$(A \to B) \to ((A \to \neg B) \to \neg A)$.

Единственное правило вывода в логике высказываний — *modus ponens*, или *правило отделения*, — переход от любых двух формул вида A и $A \to B$ к одной формуле B. Запись: $\frac{A,\ A \to B}{B}$.

Язык логики первого порядка

- символы x, y, z, u, v ... для переменных;
- пропозициональные связки;
- служебные символы — скобки (и) и запятая;
- символ равенства $=$;
- кванторы *существования* $\exists$ («существует») и *всеобщности* $\forall$ («для всех»);
- *сигнатура* — набор Σ нелогических символов, который может включать *предикатные* символы и *функциональные* символы, каждому из которых сопоставлена «арность» — число аргументов. 0-арные функциональные символы называются также *константными* символами.

Термы сигнатуры Σ определяются рекурсивно:

1) все символы переменных и константные символы — термы;
2) если $t_1, \ldots, t_n$ — термы и f — n-арный функциональный символ из Σ, то выражение $f(t_1, \ldots, t_n)$ — терм.

Формулы первого порядка определяются рекурсивно:

1) любое выражение вида $(t_1 = t_2)$ и вида $R(t_1, \ldots, t_2)$, где t_i — термы и R — n-арный предикатный символ — формулы (они называются *атомными формулами* или *атомами*);
2) если φ и φ — формулы, то $\varphi \wedge B$, $\varphi \vee B$, $\neg A$ и $\varphi \to B$ — формулы;
3) если φ — формула и x — символ переменной, то $(\exists x \varphi)$ и $(\forall x \phi)$ — формулы.

Свободные переменные формулы ϕ определяются так:

1) если φ — атом, то свободные переменные формул φ и $\neg\varphi$ — это все переменные, которые встречаются в φ;
2) свободные переменные формул $\varphi \wedge B$, $\varphi \vee B$ и $\varphi \to B$ — это {свободные переменные φ} $\cup$ {свободные переменные ψ};
3) свободные переменные формул $(\exists x \varphi)$ и $(\forall x \phi)$ — это все свободные переменные формулы φ, кроме x.

Когда пишут $\varphi(x_1, \ldots, x_n)$, обычно имеют в виду, что все свободные переменные формулы содержатся среди $x_1, \ldots, x_n$.

Высказывание (или *предложение*) — это любая формула, не содержащая свободных переменных.

Логические аксиомы первого порядка

- Все тавтологии.
- *Аксиомы равенства:*
  - $(x = x)$, $(x = y) \to (y = x)$, $(x = y) \wedge (y = x) \to (x = z)$;
  - для любого функционального символа f $(x = y) \to (f(\dots, x, \dots) = f(\dots, y, \dots))$;
  - для любой формулы φ, в которой x свободна, $(x = y) \to (\varphi(\dots, x, \dots) \to \varphi(\dots, y, \dots))$, если y остаётся свободной.
- Все формулы вида $(\forall x \varphi(x)) \to \varphi(t/x)$ и $\varphi(t/x) \to \exists x \varphi(x)$

  ($\varphi(t/x)$ — формула, которая получается подстановкой t вместо свободных вхождений переменной x, t — любой терм, ни одна переменная которого не становится связанной в процессе подстановки).

Правила вывода в логике первого порядка:

- *Modus ponens* (правило отделения): $\frac{A,\ A \to B}{B}$.
- *Правила обобщения*: если переменная x не входит в формулу φ в качестве свободной переменной, то

$$\frac{\varphi \to \psi(x)}{\varphi \to \forall y \psi(y)} \quad \text{и} \quad \frac{\psi(x) \to \varphi}{\exists y \psi(y) \to \varphi}.$$

Модели и выводимость

Алгебраическая система для произвольной сигнатуры Σ, или Σ-*система*, — это пара (M, σ), где M — непустое множество и σ — отображение с областью определения Σ такое, что

- если $R \in \Sigma$ — n-арный предикатный символ, то $\sigma(R)$ — n-местное отношение на M (т.е. $\sigma(R) \subset M^n$);
- если $f \in \Sigma$ — n-арный функциональный символ, то $\sigma(f)$ — отображение $M^n \to M$ (т.е. $\sigma(f) \subset M^{n+1}$ и если $(x_1, \ldots, x_n, x), (x_1, \ldots, x_n, y) \in \sigma(f)$, то $x = y$);
- в частности, если $c \in \Sigma$ — константный символ, то $\sigma(c) \in M$.

M — *несущее множество*, σ — *семантическая* (интерпретирующая) *функция*. Обычно алгебраическую систему отождествляют с несущим множеством и вместо (M, σ) пишут просто M (наличие семантической функции подразумевается), а вместо $\sigma(R)$ или $\sigma(f)$ — R^M или f^M.

Теперь, когда мы проинтерпретировали все предикатные и функциональные символы в системе M, выясним, чему в этой системе соответствуют термы — символы переменных и констант, выражения вида $f(x_1, \ldots, x_n)$, где f — n-арный функциональный символ и $x_1, \ldots, x_n$ — символы переменных или констант, выражения вида $g(y_1, \ldots, y_k)$, где g — k-арный функциональный символ и $y_1, \ldots, y_k$ — символы переменных или констант или выражения, полученные на предыдущем шаге (возможно, $g = f$ и $n = k$), и т.д.

Подстановка в системе M для сигнатуры Σ — это отображение s из множества переменных сигнатуры Σ в M. Другими словами, подстановка — это просто приписывание каждому символу переменной конкретного значения из M.

Для каждого терма t сигнатуры Σ рекурсивно определяется его интерпретация — отображение t^M всех подстановок в элементы M: для каждой подстановки s

- если t — константный символ c, то $t^M(s) = c^M$;
- если t — переменная x, то $t^M(s) = s(x)$;
- если $t = f(t_1, \ldots, t_n)$, то $t^M(s) = f^M(t_1^M(s), \ldots, t_n^M(s))$.

Таким образом, отображение t^M просто определяет, какие значения принимают функции f^M, когда их аргументы принимают значения, определённые каждой конкретной подстановкой.

Через $s(a/v)$ обозначим подстановку s', которая приписывает значение a переменной v, а в остальном совпадает с s.

Пусть M — Σ-система и φ — формула сигнатуры Σ. Определим по индукции естественное отношение $M \models \varphi[s]$ (φ выполняется в M при подстановке s):

- $M \models (t_1 = t_2)[s]$ означает, что $t_1^M(s)$ совпадает с $t_2^M(s)$;
- $M \models R(t_1, \ldots, t_n)[s]$ — что $(t_1^M(s), \ldots, t_n^M(s)) \in R^M$;
- $M \models \neg\varphi[s]$ — что $M \models \varphi[s]$ не выполняется;
- $M \models (\varphi \to \psi)[s]$ — что либо $M \models \neg\varphi[s]$, либо $M \models \psi[s]$;
- $M \models (\varphi \wedge \psi)[s]$ — что $M \models \varphi[s]$ и $M \models \psi[s]$;
- $M \models (\varphi \vee \psi)[s]$ — что либо $M \models \varphi[s]$, либо $M \models \psi[s]$;
- $M \models (\exists x\varphi)[s]$ — что $M \models \varphi[s(a/x)]$ для некоторого $a \in M$;
- $M \models (\forall x\varphi)[s]$ — что для всех $a \in M$ выполнено $M \models \varphi[s(a/x)]$.

Справедливость $M \models \varphi[s]$ зависит только от значений $s(x)$ для *свободных* переменных в φ. Если φ — высказывание, пишем $M \models \varphi$.

Определение 1. (Формальное) *доказательство* (вывод) формулы φ из набора высказываний A — это конечный список формул $\psi_1, \ldots, \psi_n = \varphi$, каждая из которых либо является некоторой аксиомой логики первого порядка, либо входит в набор A, либо получена по одному из трёх правил вывода из формул, предшествующих ей в этом списке. Если формула φ имеет доказательство, то мы говорим, что φ *выводима из* A и пишем $A \vdash \varphi$.

Теория T состоит из фиксированной сигнатуры и набора высказываний в этой сигнатуре. Обычно предполагается, что задан список аксиом — высказываний, которые порождают теорию (т.е. любое высказывание из T выводится из аксиом), и что T включает все высказывания, выводимые из аксиом.

Теория (набор формул) T *непротиворечива*, если не существует формулы φ, для которой $T \vdash \varphi$ и $T \vdash \neg\varphi$.

Определение 2. Система M называется *моделью* набора формул T, если $M \models \varphi$ для всех $\varphi \in T$.

Теорема Генкина о существовании модели. *Любое непротиворечивое множество формул произвольной сигнатуры имеет модель.*

Следствие 1. *Теория непротиворечива тогда и только тогда, когда она имеет модель.*

Следствие 2 (теорема Гёделя о полноте). *Формула φ выводима из набора высказываний T тогда и только тогда, когда φ истинна во всех моделях T.*

Теория множеств

Сигнатура теории множеств состоит из единственного предикатного символа $\in$.

Система аксиом ZFC (Zermelo–Fraenkel–choice)

- *Аксиома существования*: множества существуют.

  $\exists x(x = x)$

- *Аксиома объёмности*: два множества равны тогда и только тогда, когда они имеют одни и те же элементы, т.е. каждый элемент одного множества принадлежит другому и наоборот.

  $\forall X \forall Y(\forall z(z \in X \leftrightarrow z \in Y) \to X = Y)$

- *Схема аксиом выделения*: любому множеству X и любому свойству φ отвечает множество Y, состоящее в точности из тех элементов множества X, которые обладают свойством φ.

  Если φ — формула, свободные переменные которой содержатся

  среди $X, z, u_1, \ldots, u_n$, то $\quad \forall X \forall u_1, \ldots, u_n \exists Y \forall z(z \in Y \leftrightarrow z \in X \wedge \varphi)$

  Множество всех $y \in X$, обладающих свойством φ, обозначается

  $$\{y \in X : \varphi(y)\}.$$

  По техническим причинам бывает удобно рассматривать совокупность всех множеств x, для которых выполнено данное свойство-формула $\varphi(x)$. Такая совокупность называется *классом*. Запись:

  $$x \in \boldsymbol{C} \leftrightarrow \varphi(x) \qquad \text{или} \qquad \boldsymbol{C} = \{x : \varphi(x)\}.$$

  Классы $\boldsymbol{C} = \{x : \varphi(x)\}$ и $\boldsymbol{D} = \{x : \psi(x)\}$ *равны*, если $\forall x(\varphi(x) = \psi(x))$. Класс, который не равен никакому множеству, называется *собственным*. *Универсальный класс* $\boldsymbol{V}$ — это класс всех множеств:
  $$\boldsymbol{V} = \{x : x = x\}.$$

  Используя аксиому объёмности и схему аксиом выделения, можно определить

  - *пересечение* $X \cap Y = \{z \in X : z \in Y\}$,
  - *разность* $X \setminus Y = \{z \in X : z \notin Y\}$,
  - *пустое множество* $\varnothing = \{y \in X : y \neq y\}$.

- *Аксиома пары*: для любых множеств x и y существует множество $z = \{x, y\}$, состоящее из двух элементов — x и y (*неупорядоченная пара* элементов x и y).

  $\forall x \forall y \exists z(x \in z \wedge y \in z \wedge \forall u(u \in z \to (u = x \vee u = y)))$

  Используя аксиому объёмности и аксиому пары, можно определить

  - неупорядоченную пару $\{x, y\}$,
  - одноэлементное множество $\{x\} = \{x, x\}$,
  - упорядоченную пару $(x, y) = \{\{x\}, \{x, y\}\}$,
  - упорядоченную тройку $(x, y, z) = ((x, y), z)$,
  - $\ldots$

- *Аксиома объединения*: для любого семейства множеств $\mathscr{F}$ существует множество $X = \bigcup \mathscr{F}$ — объединение семейства $\mathscr{F}$; его элементами являются в точности все элементы множеств-элементов семейства $\mathscr{F}$.

  $\forall \mathscr{F} \exists X \forall Y \forall x((x \in Y \wedge Y \in \mathscr{F} \to x \in X) \wedge (x \in X \to \exists Z(Z \in \mathscr{F} \wedge x \in Z)))$.

  Обозначения: $X \cup Y = \bigcup\{X, Y\}$, $X \cup Y \cup Z = \bigcup\{X, Y, Z\}$ и т.д.

- *Схема аксиом подстановки* (*замещения*): если $\varphi(x, y)$ — формула с двумя свободными переменными, причём для любого множества a существует единственное множество b такое, что $\varphi(a, b)$ — истинное высказывание, то для любого данного множества X определено множество Y, элементами которого являются те и только те множества y, для которых $\varphi(x, y)$ истинно при некотором $x \in X$.

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

  Здесь формулу φ можно воспринимать как класс-отображение, которое каждому a ставит в соответствие то единственное множество b, для которого высказывание $\varphi(a, b)$ истинно; тогда Y — не что иное как образ множества X при этом «отображении».

- *Аксиома бесконечности*: существует множество, которое содержит (в качестве элемента) $\varnothing$ и вместе с каждым элементом x содержит и элемент $S(x) = x \cup \{x\}$ ($x \cup \{x\}$ — множество, элементами которого являются все элементы множества x и само множество x).

  $\exists X((\varnothing \in X) \wedge \forall x(x \in X \to (x \cup \{x\}) \in X))$

  Из аксиом объёмности, бесконечности и выделения следует, что существует множество, состоящее из элементов $\varnothing$ (обозначение: 0), $\{\varnothing\}$ (обозначение: 1), $\{\varnothing, \{\varnothing\}\}$ (обозначение: 2), $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$ (обозначение: 3), $\{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}\}$ (обозначение: 4), ... Это множество в теории множеств называется *множеством натуральных чисел* (в этой теории удобно считать, что 0 в него входит) и обозначается ω.

  Назовём множество Y *подмножеством* множества X (обозначение: $Y \subset X$), если $\forall y(y \in Y \to y \in X)$. Если $Y \subset X$ и $\neg(Y = X)$, то Y называется *собственным подмножеством* (обозначение: $Y \subsetneq X$).

- *Аксиома множества подмножеств*: для любого множества X существует множество Y, состоящее из всех подмножеств множества X.

  $\forall X \exists Y \forall z(z \subset X \leftrightarrow z \in Y)$

  Для множества подмножеств множества X используются обозначения $\mathscr{P}(X)$, 2^X и $\exp X$.

  Аксиома множества подмножеств позволяет определить

  декартово произведение $X \times Y$ двух (и любого конечного числа) множеств X и Y, а также понятия отношений и отображений:

  $$X \times Y = \{z \in \mathscr{P}(\mathscr{P}(X \cup Y) : (\exists x \in X)(\exists y \in Y)(z = (x, y))\}.$$

  Множество R называется (бинарным) *отношением*, если $R \subset X \times Y$ для некоторых множеств X и Y. *Область определения* и *область значений* отношения R — это множества

  $$\operatorname{dom} R = \{x \in X : \exists y((x, y) \in R)\} \quad \text{и} \quad \operatorname{ran} R = \{y \in Y : \exists x((x, y) \in R)\}.$$

  Отношение f называется *отображением* (или *функцией*), если

  $$\forall x \forall y \forall x(((x, y) \in f) \wedge ((x, z) \in f) \to y = z).$$

  В случае, когда $\operatorname{dom} f = X$, используют обозначение $f \colon X \to Y$.

  Множества можно возводить в степень:

  $$Y^X = \{f \subset X \times Y : f \text{ — функция}, \operatorname{dom} f = X, \operatorname{ran} f \subset Y\}.$$

- *Аксиома регулярности* (*фундирования*): каждое непустое множество X содержит элемент x такой, что $X \cap x = \varnothing$.

  $\forall X(\neg(X = \varnothing) \to (\exists x \in X)(x \cap X = \varnothing)$

Следствие: не существует бесконечной последовательности множеств $x_0, x_1, x_2, \dots$ такой, что $x_0 \ni x_1 \ni x_2 \ni \dots$ (в частности, $\nexists X(X \in X)$) — достаточно рассмотреть $X = \{x_0, x_1, x_2, \dots\}$ и применить аксиому. Из аксиомы выбора следует, что верно и обратное: из несуществования бесконечной последовательности $x_0 \ni x_1 \ni x_2 \ni \dots$ вытекает аксиома регулярности — иначе $(\exists X \neq \varnothing)(\forall x \in X)(x \cap X \neq \varnothing)$ и по аксиоме выбора существует множество $\{x_0, x_1, x_2, \dots\}$, в котором $x_0 \in X$, $x_1 \in X \cap x_0$, $x_2 \in X \cap x_1$ и т.д.

- *Аксиома выбора* (AC): для каждого семейства $\mathscr{F}$ непустых множеств существует *функция выбора* на $\mathscr{F}$, т.е. отображение $f\colon \mathscr{F} \to \bigcap \mathscr{F}$ с тем свойством, что $f(X) \in X$ для каждого $X \in \mathscr{F}$.

  $\forall \mathscr{F}((\forall X \in \mathscr{F})(X \neq \varnothing) \to (\exists f\colon \mathscr{F} \to \bigcup \mathscr{F})(\forall X \in \mathscr{F})(f(X) \in X))$

Модели теории множеств

Согласно данному выше определению модель теории множеств — это пара (M, σ), где M — непустое множество и σ — отображение с одноточечной областью определения $\{\in\}$, которое сопоставляет предикатному символу $\in$ отношение $\sigma(\in)$, т.е. некоторое подмножество множества $M \times M$. Как правило, в теории множеств рассматривают только *стандартные* модели, для которых $\sigma(\in) = \in$. Кроме того, наибольший интерес представляют *транзитивные* модели, т.е. модели, содержащие все элементы всех своих элементов: $\forall x(x \in M \to x \subset M)$. Нестандартные и/или нетранзитивные модели рассматриваются крайне редко. Мы тоже в дальнейшем будем рассматривать только стандартные транзитивные модели. Для выражения «стандартная транзитивная модель» используется аббревиатура СТМ.

Итак, стандартная транзитивная модель теории множеств — это просто некоторое транзитивное множество M. В этой модели M интерпретируется как класс всех множеств, а множествами считаются элементами модели M. То, что M является моделью именно теории множеств, означает, что в ней выполнены все аксиомы теории множеств, т.е. $M \models \varphi$ для всех аксиом φ из системы ZFC (см. определение отношения $\models$ выше). Например, выполнение аксиомы существование означает, что $a = a$ для некоторого $a \in M$, т.е. множество M непусто, выполнение аксиомы пары — что для любых $x, y \in M$ имеем $\{x, y\} \in M$, аксиома множества подмножеств — что для любого $x \in M$ имеем $\mathscr{P}^M(X) = \{y \in M : y \subset X\} \in M$ и т.д.

Вообще, истинность высказывания φ в модели M (т.е. выражение $M \models \varphi$) означает, что высказывание, полученное из φ заменой всех выражений вида $\exists x$ и $\forall x$ на $\exists x \in M$ и $\forall x \in M$, истинно.

Ординалы и кардиналы

Порядок

Частичный порядок, или просто *порядок*, на множестве X — это отношение на X (подмножество $\leq$ декартова квадрата $X \times X$), обладающее следующими свойствами (мы пишем $x \leq y$ вместо $(x, y) \in \leq$; кроме того, мы иногда пишем $y \geq x$ вместо $x \leq y$):

- $((x \leq y) \wedge (y \leq z)) \to (x \leq z)$ (*транзитивность*);
- $\forall x \in X (x \leq x)$ (*рефлексивность*);
- $((x \leq y) \wedge (y \leq x)) \to (x = y)$ (*антисимметричность*).

Множество X вместе с заданным на нём порядком (т.е. пара $(X, \leq)$) называется (*частично*) *упорядоченным множеством*; про множество X говорят, что оно (*частично*) *упорядочено отношением* $\leq$. Запись $x \leq y$ читается «элемент x не больше элемента y» или «элемент x не превосходит элемента y», а запись $x \geq y$ — «элемент x не меньше элемента y».

Для каждого порядка $\leq$ на X однозначно определено соответствующее отношение $<$ *строгого порядка*: $x < y$, если $x \leq y$ и $x \neq y$. При этом говорят, что элемент x *меньше* элемента y, а y *больше* x. И наоборот, по строгому порядку $<$ очевидным образом восстанавливается порядок $\leq$, которому он соответствует.

Два элемента x и y множества X, упорядоченного отношением $\leq$, *сравнимы*, если либо $x \leq y$, либо $y \leq x$. Элементы x и y *совместимы*, если существует $z \in X$ такой, что $z \leq x$ и $z \leq y$.

Говорят, что $y \in X$ лежит *между* $x \in X$ и $z \in X$, если $x \leq y \leq z$.

Элемент x множества $Y \subset X$ называется *минимальным* (*максимальным*) элементом этого множества, если $\forall y \in Y ((y \leq x) \to (y = x))$ (соответственно $\forall y \in Y ((x \leq y) \to (y = x))$).

Элемент x *ограничивает* множество $Y \subset X$ *сверху* (*снизу*), или является *верхней* (*нижней*) *гранью* множества Y, если $\forall y \in Y (y \leq x)$ (соответственно $\forall y \in Y (x \leq y)$). Если при этом x принадлежит множеству Y, то он называется *наименьшим* (*наибольшим*) элементом Y и обозначается $\min Y$ ($\max Y$).

Множество, у которого есть верхняя (нижняя, верхняя и нижняя) грань называется *ограниченным сверху* (*ограниченным снизу*, *ограниченным*).

Наименьшая (наибольшая) верхняя (нижняя) грань множества Y, если она существует, называется также *точной верхней* (*нижней*) *гранью*, или *супремумом* (*инфимумом*), множества Y и обозначается $\sup Y$ ($\inf Y$).

Интервалом упорядоченного множества $(X, \leq)$ называется любое его подмножество I с тем свойством, что для любых $x, y \in I$ всякий элемент $z \in X$ между x и y принадлежит I. Интервалы бывают восьми типов:

$$\begin{array}{ll} \text{а)}\ \{x : x < a\}, & \text{д)}\ \{x : a \leq x \leq b\} = [a, b], \\ \text{б)}\ \{x : x \leq a\}, & \text{е)}\ \{x : a < x < b\} = (a, b), \\ \text{в)}\ \{x : a < x\}, & \text{ё)}\ \{x : a \leq x < b\} = [a, b), \\ \text{г)}\ \{x : a \leq x\}, & \text{ж)}\ \{x : a < x \leq b\} = (a, b], \end{array}$$

где $a, b \in I$. Интервалы типа а) называют *начальными интервалами*.

Порядок $\leq$ на X называется *линейным*, если любые два элемента x и y множества X сравнимы. В этом случае пара $(X, \leq)$ называется *линейно упорядоченным множеством*, а пара $(X, <)$ — *строго линейно упорядоченным множеством*.

Порядок $\leq$ на X *полон*, если он линеен и любое непустое множество $Y \subset X$ содержит наименьший (в Y) элемент. Пара $(X, \leq)$, где $\leq$ — полный порядок, называется *вполне упорядоченным множеством*, а пара $(X, <)$ — *строго вполне упорядоченным множеством*. Всякое

непустое вполне упорядоченное множество имеет наименьший элемент (хотя наибольший элемент существовать не обязан), и для всякого его элемента, который не является наибольшим, определён элемент, непосредственно следующий за ним.

Порядок $\leq$ на X называется *фундированием*, если любое непустое множество $Y \subset X$ содержит минимальный (в Y) элемент.

На каждом подмножестве Y упорядоченного множества $(X, \leq)$ естественно возникает *индуцированный* порядок, или *сужение* порядка $\leq$ на Y — это пересечение порядка $\leq$ (который является подмножеством $X \times X$) с $Y \times Y$. Как легко видеть, индуцированный порядок линеен или полон, если таковым является порядок $\leq$ на X. В дальнейшем, рассматривая подмножества упорядоченных множеств, мы всегда будем считать, что они снабжены индуцированным порядком.

Отображение $f\colon X \to Y$ между упорядоченными множествами $(X, \leq)$ и $(Y, \preccurlyeq)$ называется *порядковым изоморфизмом*, а сами эти упорядоченные множества — *порядково изоморфными*, если f взаимно однозначно и для любых $x, y \in X$ соотношение $x \leq y$ выполнено тогда и только тогда, когда $f(x) \preccurlyeq f(y)$. В случае линейно упорядоченных множеств любая сохраняющая порядок (т.е. «монотонно неубывающая») биекция является порядковым изоморфизмом.

Теорема об изоморфизме

Теорема 1. *Пусть $(X, \leq)$ и $(Y, \preccurlyeq)$ — любые вполне упорядоченные множества. Тогда либо существует $x_* \in X$ такой, что начальный интервал $\{x \in X : x < x_*\}$ множества X порядково изоморфен вполне упорядоченному множеству Y, либо существует $y_* \in Y$ такой, что вполне упорядоченное множество X порядково изоморфно начальному интервалу $\{y \in Y : y \prec y_*\}$ множества Y, либо сами множества $(X, \leq)$ и $(Y, \preccurlyeq)$ порядково изоморфны.*

Замечание 1.

1. Пусть $f\colon P \to P$ — сохраняющее порядок биективное отображение вполне упорядоченного множества P в себя. Тогда $f(x) \geq x$ для каждого $x \in P$.
2. Вполне упорядоченное множество не изоморфно никакому своему начальному интервалу.

Ординалы

Определение 3. Множество S *транзитивно*, если оно содержит все элементы всех своих элементов: $\forall x (x \in S \to x \subset S)$.

Из аксиомы регулярности немедленно вытекает, что всякое транзитивное множество содержит $\varnothing$ в качестве элемента.

Определение 4. Множество называется *ординалом* (*порядковым числом*), если оно транзитивно и строго вполне упорядочено отношением $\in$.

Из этого определения видно, что каждое натуральное число, также как множество ω всех натуральных чисел (см. аксиому бесконечности), является ординалом. Очевидно, привычный порядок на натуральных чисел как раз и есть отношение принадлежности.

Ординалы обычно обозначают буквами α, β, γ, $\ldots$. Вместо $\alpha \in \beta$ часто пишут $\alpha < \beta$. Запись $\alpha \leq \beta$ означает, что либо $\alpha \in \beta$, либо $\alpha = \beta$.

Класс всех ординалов обозначается Ord или On.

- Каждый ординал α — это множество всех ординалов $\beta < \alpha$
- $\alpha + 1 = \alpha \cup \{\alpha\}$ = множество всех ординалов $\beta \leq \alpha$ — наименьший ординал, больший α

- Для множества ординалов A $\bigcup A = \sup A$ (очень легко проверить). Множество $\sup A$ иногда обозначают $\lim A$.
- Класс ординалов собственный (по аксиоме регулярности).

Сам Кантор понимал ординалы как классы порядково изоморфных вполне упорядоченных множеств и называл их *порядковыми типами*.

Теорема 2. *Каждое вполне упорядоченное множество $(P, \leq)$ порядково изоморфно единственному ординалу.*

Доказательство. P вполне упорядочено $\Longrightarrow$ по аксиоме подстановки можно определить множество S ординалов, каждый из которых изоморфен какому-нибудь начальному интервалу P. Ординал $\alpha = \sup S = \bigcup S$ изоморфен P. Действительно, если это не так, то по теореме об изоморфизме либо α изоморфен начальному интервалу $I \subsetneq P$ (а тогда $\alpha \in \alpha$ в противоречие с аксиомой регулярности), либо P изоморфно начальному интервалу α. Любой начальный интервал α — это некоторый ординал $\beta < \alpha$, который изоморфен начальному интервалу P, а вполне упорядоченное множество не изоморфно никакому своему начальному интервалу. Отсюда же вытекает единственность. ■

Определение 5. Ординал α называется *изолированным*, или *непредельным*, если $\alpha = \beta + 1$ для некоторого β. В противном случае α называется *предельным* ординалом.

Замечание 2. Ординал α является предельным тогда и только тогда, когда $\alpha = \sup \alpha$.

Из аксиом объёмности, бесконечности и выделения следует существование наименьшего непустого предельного ординала ω. Ординалы, меньшие ω (т.е. элементы ω) называются *натуральными числами*, а сам ординал ω называется *множеством натуральных чисел.* Натуральные числа обозначаются $0, 1, 2, \ldots, i, j, k, l, m, n, \ldots$.

(Привычнее было бы сказать, что натуральные числа — непустые элементы множества ω; иногда, а за пределами теории множеств почти(?) всегда, под множеством натуральных чисел имеют в виду $\omega \setminus \{\varnothing\}$, и тогда его обозначают $\mathbb{N}$.)

Теорема Цермело и лемма Цорна

Теорема Цермело. *Любое множество можно вполне упорядочить.*

Лемма Цорна (оригинальная формулировка). *Пусть $\mathscr{X}$ — семейство множеств со свойством: если $\mathscr{Y} \subset \mathscr{X}$ таково, что для любых $X, Y \in \mathscr{Y}$ либо $X \subset Y$, либо $Y \subset X$, то $\bigcup \mathscr{Y} \in \mathscr{X}$. Тогда в семействе $\mathscr{X}$ есть максимальный по включению элемент.*

Лемма Цорна (современная формулировка). *Пусть $(X, \leq)$ — частично упорядоченное множество с тем свойством, что у любого подмножества $Y \subset X$, на котором индуцированный порядок оказывается линейным, имеется верхняя грань. Тогда в X есть максимальный элемент.*

Теорема Цермело и лемма Цорна равносильны аксиоме выбора в том смысле, что

$$\mathrm{ZFC} \vdash \mathrm{ZF} + \text{теорема Цермело}, \quad \mathrm{ZF} + \text{теорема Цермело} \vdash \mathrm{ZFC}$$

и

$$\mathrm{ZFC} \vdash \mathrm{ZF} + \text{лемма Цорна}, \quad \mathrm{ZF} + \text{лемма Цорна} \vdash \mathrm{ZFC}.$$

(см. книгу: Н.К. Верещагин, А. Шень, *Начала теории множеств*, Москва: МЦНМО, 2012).

Пример применения леммы Цорна

Теорема 3. *В любом векторном пространстве V имеется базис. Более того, всякое линейно независимое множество векторов в V можно дополнить до базиса.*

Доказательство. Возьмём в качестве $\mathscr{X}$ семейство всех линейно независимых множеств в V, содержащих данное множество $\mathcal{S}$. Пусть $\mathscr{Y} \subset \mathscr{X}$ удовлетворяет условию в лемме. Возьмём любые $n \in \mathbb{N}$ и $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in \bigcup \mathscr{Y}$. Для $i \in \mathbb{N}$ найдём $\mathcal{S}_i \in \mathscr{Y}$, для которых $\boldsymbol{x}_i \in \mathcal{S}_i$. По условию на $\mathscr{Y}$ множества $\mathcal{S}_1, \ldots, \mathcal{S}_n$ можно упорядочить по включению. Пусть $\mathcal{S}_{k_1} \subset \mathcal{S}_{k_2} \subset \cdots \subset \mathcal{S}_{k_n}$. Тогда $\boldsymbol{x}_1, \ldots, \boldsymbol{x}_n \in \mathcal{S}_{k_n}$. Множество $\mathcal{S}_{k_n}$ линейно независимо $\implies \boldsymbol{x}_1, \ldots, \boldsymbol{x}_n$ линейно независимы $\implies \bigcup \mathscr{Y}$ линейно независимо. Лемма Цорна $\implies$ в $\mathscr{X}$ есть максимальное линейно независимое множество, содержащее $\mathcal{S}$. ■

Понятие вполне упорядоченного множества и теорема Цермело позволяют распространить метод математической индукции на произвольные множества. Пусть X — непустое множество и $\varphi(x)$ — любое высказывание об элементах X. Предположим, что нам удалось ввести полный порядок $\leq$ на X так, что мы умеем доказывать $\varphi(x_0)$ для наименьшего элемента x_0 и умеем выводить утверждение $\varphi(x)$ из утверждения «$\varphi(y)$ верно для всех $y < x$». Тогда мы смело можем утверждать, что утверждение $\varphi(x)$ верно для всех $x \in X$. Действительно, если это не так, т.е. если множество $\{x \in X : \varphi(x) \text{ неверно}\}$ непусто, то мы можем взять наименьший элемент в этом множестве и сразу получить противоречие.

То же рассуждение работает в случае, когда $\leq$ — фундирование: если $\varphi(x_0)$ верно для всех минимальных элементов x_0 и из утверждения «для любого $y < x$ $\varphi(y)$ верно» выводится $\varphi(x)$, то $\varphi(x)$ верно для всех $x \in X$ — если $\{x \in X : \varphi(x) \text{ неверно}\} \neq \varnothing$, то существование минимального элемента в этом множестве приводит к противоречию.

Кардиналы

Для каждого множества X Кантор определял мощность $|X|$ как класс всех множеств, находящихся во взаимно однозначном соответствии с X ($|X| = |Y|$, если существует биекция $X \rightleftarrows Y$). Мощности сравниваются так:

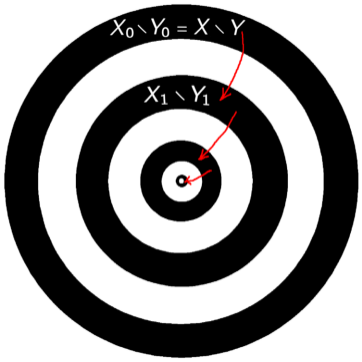
$$|X| \leq |Y|, \qquad \text{если существует инъекция } X \to Y \text{ (или сюръекция } Y \to X)$$

Теорема 4 (Кантора–Бернштейна–Шрёдера). *Если $|X| \leq |Y|$ и $|Y| \leq |X|$, то $|X| = |Y|$.*

Доказательство. Достаточно показать, что если $X_1 \subset Y \subset X$ и $|X_1| = |X|$, то $|X| = |Y|$. Пусть $f\colon X \to X_1$ — биекция. Положим

$$\begin{array}{llll} X_0 = X, & X_1 = f(X_0), & X_2 = f(X_1), & \ldots; \\ Y_0 = Y, & Y_1 = f(Y_0), & Y_2 = f(Y_1), & \ldots. \end{array}$$

Для $x \in X$ положим $g(x) = \begin{cases} f(x), & \text{если } \exists n \in \omega\colon x \in X_n \setminus Y_n, \\ x & \text{в противном случае.} \end{cases}$



Отображение $g\colon X \to Y$ — биекция.

■

Определение 6. *Мощность* $|X|$ множества X — это наименьший ординал α, для которого существует биекция $X \rightleftarrows \alpha$.

Определение 7. Ординал α называется *кардиналом*, если не существует биекции между α и β ни для какого ординала $\beta < \alpha$.

Кардиналы обозначаются буквами κ, λ, ...

Кардиналы называются также *алефами*. Кантор использовал для них обозначение $\aleph_\alpha$, $\alpha \in$ Ord:

- $\aleph_0 = \omega$,
- $\aleph_{\alpha+1}$ = наименьший кардинал, больший $\aleph_\alpha$,
- для предельного ординала α $\aleph_\alpha = \sup_{\beta<\alpha} \aleph_\beta$.

Сейчас наравне с $\aleph_\alpha$ используется обозначение ω_α (которое сам Кантор использовал только для ординалов):

- $\omega_0 = \omega$,
- $\omega_{\alpha+1}$ = наименьший кардинал, больший ω_α,
- для предельного ординала α $\omega_\alpha = \sup_{\beta<\alpha} \omega_\beta$.

Мощность определена для каждого множества. Действительно, по теореме Цермело любое множество можно вполне упорядочить, а каждое вполне упорядоченное множество порядково изоморфно единственному ординалу. Порядковый изоморфизм — биекция, поэтому для любого множества X существуют ординал α и биекция $\alpha \rightleftarrows X$. Значит, множество ординалов $\{\beta \in \alpha + 1 :$ существует биекция $\beta \rightleftarrows X\}$ непусто, и $|X|$ — его наименьший элемент.

Для каждого бесконечного множества X $\exists \alpha \in$ Ord: $|X| = \omega_\alpha$.

Определение 8. Множество X *счётно*, если $|X| = \omega$. Множество X *несчётно*, если $|X| > \omega$.

Теорема Лёвенгейма–Скулема

Теорема Лёвенгейма–Скулема. *Пусть T — любой не более чем счётный набор высказываний первого порядка не более чем счётной сигнатуры. Если у набора T существует модель, то у него существует и счётная транзитивная модель.*

Из этой теоремы вытекает, что если теория множеств непротиворечива, то у неё есть счётная модель. На первый взгляд это противоречит теореме Кантора–Бернштейна–Шрёдера. Действительно, эта теорема выводится из аксиом ZFC, а значит, должна быть верна в любой модели, включая счётную. Но любая счётная модель M обязана содержать множество натуральных чисел ω (по аксиомам бесконечности и выделения). Значит, она обязана содержать и множество $\mathscr{P}^M(X)$ всех подмножеств множества X, принадлежащих этой модели. И хотя $\mathscr{P}^M(X)$ может не содержать некоторых подмножеств множества X, оно обязано быть несчётным по теореме Кантора–Берштейна–Шрёдера. В силу транзитивности множества M имеем $\mathscr{P}^M(X) \subset M$. Значит, модель M не может быть счётной.

Всё дело в том, что счётность — понятие относительное. Счётность модели M означает, что существует биекция между M и ω. Ясно, что эта биекция не может принадлежать модели (напомним, что эта биекция является подмножеством декартова произведения $M \times \omega$) и существует только «снаружи». Внутри модели M мощность множества M вообще не определена, потому что с точки зрения модели сама модель — не множество, а класс. Точно так же, мощность множества $\mathscr{P}^M(X)$ «снаружи» модели, конечно, счётна, но внутри модели она несчётна (биекция $\mathscr{P}^M(X) \rightleftarrows \omega$ не принадлежит множеству M в качестве элемента, а потому не существует с точки зрения модели).

Арифметика кардиналов

Для непересекающихся множеств X и Y

- $|X| + |Y| = |X \cup Y|$
- $|X| \cdot |Y| = |X \times Y|$
- $|Y|^{|X|} = |Y^X|$
  (напомним: $Y^X = \{f \subset X \times Y : f$ — отображение $X \to Y\}$)
- в частности, $2^{|X|} = |\{\chi_A : A \subset X\}| = |\mathscr{P}(X)|$
  ($\mathscr{P}(X)$ — множество всех подмножеств X,
  χ_A — характеристическая функция подмножества $A \subset X$)

Свойства арифметических операций:

- $(\kappa + \lambda) + \mu = \kappa + (\lambda + \mu), \quad (\kappa \cdot \lambda) \cdot \mu = \kappa \cdot (\lambda \cdot \mu)$;
- $\kappa + \lambda = \lambda + \kappa, \quad \kappa \cdot \lambda = \lambda \cdot \kappa$;
- $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$;
- если $\kappa \leq \lambda$, то $\kappa + \mu \leq \lambda + \mu$, $\kappa \cdot \mu \leq \lambda \cdot \mu$ и $\kappa^\mu \leq \lambda^\mu$;
- если $1 \leq \kappa$ и $\lambda \leq \mu$, то $\kappa^\lambda \leq \kappa^\mu$;
- если κ бесконечен, то $\kappa \cdot \kappa = \kappa$;
- если хотя бы один из кардиналов κ и λ бесконечен и оба они
- отличны от нуля, то $\kappa + \lambda = \kappa \cdot \lambda = \max\{\kappa, \lambda\}$;
- $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu, \quad (\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu, \quad \kappa^{\lambda \cdot \mu} = (\kappa^\lambda)^\mu$;
- если хотя бы один из кардиналов κ и λ бесконечен, $\kappa \geq 2$ и $\lambda \geq 1$, то

- $\max\{\kappa, 2^\lambda\} \le \kappa^\lambda \le \max\{2^\kappa, 2^\lambda\}$;
- в частности, если λ бесконечен, то $2^\lambda = \kappa^\lambda$ для любого $\kappa \le 2^\lambda$, $\kappa \ge 2$.
- $(\kappa + \lambda) + \mu = \kappa + (\lambda + \mu)$, $\quad (\kappa \cdot \lambda) \cdot \mu = \kappa \cdot (\lambda \cdot \mu)$;
- $\kappa + \lambda = \lambda + \kappa$, $\quad \kappa \cdot \lambda = \lambda \cdot \kappa$;
- $\kappa \cdot (\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$;
- если $\kappa \le \lambda$, то $\kappa + \mu \le \lambda + \mu$, $\kappa \cdot \mu \le \lambda \cdot \mu$ и $\kappa^\mu \le \lambda^\mu$;
- если $1 \le \kappa$ и $\lambda \le \mu$, то $\kappa^\lambda \le \kappa^\mu$;
- если κ бесконечен, то $\kappa \cdot \kappa = \kappa$;
- если хотя бы один из кардиналов κ и λ бесконечен и оба они
- отличны от нуля, то $\kappa + \lambda = \kappa \cdot \lambda = \max\{\kappa, \lambda\}$;
- $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$, $\quad (\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$, $\quad \kappa^{\lambda \cdot \mu} = (\kappa^\lambda)^\mu$;
- если хотя бы один из кардиналов κ и λ бесконечен, $\kappa \ge 2$ и $\lambda \ge 1$, то
- $\max\{\kappa, 2^\lambda\} \le \kappa^\lambda \le \max\{2^\kappa, 2^\lambda\}$;
- в частности, если λ бесконечен, то $2^\lambda = \kappa^\lambda$ для любого $\kappa \le 2^\lambda$, $\kappa \ge 2$.

Теорема Кантора. *Для любого кардинала* κ $\ 2^\kappa > \kappa$.

Доказательство. Надо доказать: $|\mathscr{P}(X)| > |X|$ для любого множества X. Ясно, что $|\mathscr{P}(X)| \ge |X|$. Для любого отображения $f\colon X \to \mathscr{P}(X)$

$$Y = \{x \in X : x \notin f(x)\} \notin \operatorname{ran} f \quad (\operatorname{ran} f \text{ — множество значений } f).$$

Действительно, пусть $Y = f(y)$. По определению множества Y если $y \in Y$, то $y \notin Y$, и если $y \notin Y$, то $y \in Y$.

Не существует сюръекции $X \to \mathscr{P}(X) \implies |\mathscr{P}(X)| > |X|$. ■

Определение 9. Кардинал 2^ω называется *мощностью континуума.*

Континуум-гипотеза

Континуум-гипотеза (CH): $\boxed{2^\omega = \omega_1}$.

CH верна $\iff$ существует сюръекция $\omega_1 \to \mathscr{P}(\omega)$.
CH неверна $\iff$ существует инъекция $\omega_2 \to \mathscr{P}(\omega)$.

Теоремы Гёделя о неполноте. *В любой непротиворечивой формальной системе S, удовлетворяющей определённым условиям (в частности, в теории множеств), существует высказывание φ такое, что $S \nvdash \varphi$ и $S \nvdash \neg\varphi$.*

Более того, в любой такой формальной системе S можно построить высказывание φ, утверждающее непротиворечивость S. Если S непротиворечива, то $S \nvdash \varphi$.

Из теорем Гёделя следует, что, во-первых, непротиворечивость теории множеств нельзя доказать средствами самой этой теории, и во-вторых, если теория множеств непротиворечива, то существует высказывание языка теории множеств, которое нельзя доказать (т.е. его нельзя вывести из аксиом) и нельзя опровергнуть (т.е. отрицание этого высказывания тоже не выводится).

Континуум-гипотеза — одно из таких высказываний.