Введение в математическую логику

Лекция 10

Мы приступаем к знакомству с системой аксиом (теорией) **ZF**. Эта теория претендует на то, что любое математическое утверждение естественно записывается в виде замкнутой формулы в сигнатуре **ZF**, а доказательство утверждения может быть записано как (синтаксический) вывод в данной теории. Теория **ZF** называется *теорией множеств Цермело — Френкеля.* Имеются разные системы аксиом теории множеств, и **ZF** среди них, по-видимому, наиболее распространенная.

Теория **ZF** является теорией с равенством, сигнатура теории (кроме, конечно, $=$) состоит из единственного имени $\in$ двуместного отношения. Следуя традиции, мы будем использовать запись $a \in b$, а не $\in (a, b)$.

<u>Неформальное замечание</u>: структура, которую мы пытаемся описать с помощью **ZF**, — класс всех "чистых" множеств, то есть множеств, элементами которых являются только множества. Кажется, для целей математики достаточно таких множеств.

Аксиомы ZF

Аксиома объемности:

$$\forall u, v(\forall w(w \in u \equiv w \in v) \to u = v).$$

Хочется для каждой формулы $\Phi(x)$ добавить аксиому $\exists u(\forall v(v \in u \equiv \Phi(v)))$, но теория станет противоречивой (рассмотрите формулу $\Phi(x) = x \notin x$) — парадокс Рассела.

Мы скажем, что набор элементов $\{x | x \notin x\}$ "не является собственным множеством", имея в виду, что хотя элементы с таким свойством могут существовать в описываемой структуре, однако в ней нет такого элемента a, что $\{x | x \in a\} = \{x | x \notin x\}$.

Четыре вида аксиом существования множеств

Аксиомы подмножеств:

$$\forall \bar{t} \forall u \exists s \forall v (v \in s \equiv (v \in u \wedge \Phi(\bar{t}, v)))$$

для любой формулы $\Phi(\overline{x}, y)$.

Иными словами, аксиома гарантирует, что для любых элементов $a, b_0, \ldots, b_k$ нашей структуры набор $\{x \mid x \in a \wedge \Phi(\bar{b}, x)\}$ является собственным множеством.

Аксиомы замены:

$$\forall \bar{t}\Big(\forall u \exists v \forall w\big(w \in v \equiv \Phi(\bar{t}, u, w)\big) \to \forall v \exists s \forall w\big(\exists u(u \in v \wedge \Phi(\bar{t}, u, w)) \equiv w \in s\big)\Big)$$

для любой формулы $\Phi(\overline{x}, y, z)$.

Пусть $b_0, \ldots, b_k$ – некоторые элементы нашей структуры, тогда формуле $\Phi(\bar{b}, y, z)$ соответствует некоторое отображение: каждому элементу a соответствует набор $\{z \mid \Phi(\bar{b}, a, z)\}$. Предположим, что каждый такой набор является собственным множеством. Даже в этом случае объединение семейства таких наборов может не быть собственным множеством.

Аксиома замены гарантирует, что если для каждого a набор $\{z \mid \Phi(\bar{b}, a, z)\}$ является собственным множеством и мы выбираем a из некоторого собственного множества c, то объединение таких наборов, то есть набор $\{z \mid \exists u(u \in c \wedge \Phi(\bar{b}, u, z))\}$, является собственным множеством.

Аксиома степени:

$$\forall u \exists s \forall v (\forall w (w \in v \to w \in u) \equiv v \in s).$$

Мы будем использовать выражение $x \subset y$ как сокращение для формулы $\forall u (u \in x \to u \in y)$. Используя это сокращение, можно сказать, что аксиома степени гарантирует, что для любого элемента a набор $\{x \mid x \subset a\}$ является собственным множеством.

Аксиома бесконечности:

$$\exists s \Big(\exists u \big(u \in s \wedge \forall v (v \notin u) \big) \wedge \forall u \Big(u \in s \to \exists v \big(v \in s \wedge \forall w (w \in v \to (w \in u \vee w = u)) \big) \Big) \Big).$$

Это важная аксиома, однако в данной формулировке она столь сложна, что мы отложим ее обсуждение до того момента, когда мы будем исследовать множество ω. В данный момент заметим лишь, что она безусловно гарантирует существование множеств с некоторыми специальными свойствами. Это отличает ее от аксиом подмножеств, замены и степени, которые позволяли строить множества лишь исходя из существования некоторых других множеств.

Аксиома регулярности (фундирования):

$$\forall u (\exists v (v \in u) \to \exists v (v \in u \wedge \neg \exists w (w \in v \wedge w \in u))).$$

Эта аксиома утверждает, что в любом собственном множестве a есть такой элемент b, что пересечение наборов $\{x \mid x \in a\}$ и $\{x \mid x \in b\}$ пусто. Мы не будем обосновывать эту аксиому, заметим лишь, что она бывает полезна.

Следующие два утверждения выводятся из предыдущих аксиом, но чтобы не загромождать изложение их выводом, мы включим их в теорию.

Аксиома пустого множества:

$$\exists s \forall u (u \notin s).$$

Аксиома пары:

$$\forall u, v \exists s \forall w (w \in s \equiv (w = u \vee w = v)),$$

то есть $\{x \mid x = a \vee x = b\}$ является собственным множеством для любых элементов a и b.

Предварительные замечания и соглашения

Теория множеств понимается и как содержательная теория: утверждения о некоторой структуре "настоящих" множеств; и как анализ формальной теории **ZF** – непротиворечивость, полнота, исследование всевозможных моделей и пр., аналогично арифметике (теории чисел) и арифметике Пеано. Мы, в основном, будем заниматься формальной теорией множеств.

Мы предположим, что у теории **ZF** есть модель, и постараемся понять, как она устроена, в частности, что в такой модели может соответствовать натуральным числам. Это похоже на рассмотрение нестандартных арифметик, с существенным отличием: в случае арифметики мы не предполагали, а были уверены, что модели существуют.

Время от времени мы будем утверждать, что некоторая формула выводима в теории ($\mathbf{ZF} \vdash$). Формально говоря, мы должны были бы представить цепочку формул, являющуюся выводом в теории. Однако мы, вместо этого, постараемся доказать, что данное утверждение истинно во всех моделях теории ($\mathbf{ZF} \models$), и сошлемся на теорему о полноте исчисления предикатов (эквивалентность синтаксической выводимости и семантического следования).

Начиная с данного момента мы используем термины множество, подмножество, функция и пр. только в формальном смысле – в смысле элементов рассматриваемой модели $\mathbf{ZF}$. Таким образом, в дальнейшем вместо "собственное множество" мы будем говорить просто "множество". Для содержательных понятий мы будем использовать термины класс, набор, совокупность, подкласс, отображение и пр. Например, обычный натуральный ряд мы будем называть "совокупностью натуральных чисел".

Чтобы избежать слишком длинных формул, мы будем использовать сокращения. Одно из них – квантор $\exists!$ – означает "существует единственное". Иными словами, запись $\exists! u \Phi(u)$ является сокращением для формулы $\exists u(\Phi(u) \wedge \forall v(\Phi(v) \to u = v))$.

Из аксиомы пустого множества и аксиомы объемности следует, что $\mathbf{ZF} \vdash \exists! s \forall u(u \notin s)$, то есть в модели существует единственный элемент a, удовлетворяющий формуле $\forall u(u \notin a)$. Этот элемент мы будем обозначать символом $\varnothing$. Этот символ мы будем использовать в атомных формулах так же, как имя предмета, однако это просто сокращение: формула $\varnothing \in x$ является сокращением для $\exists u(\forall v(v \notin u) \wedge u \in x)$ или $\forall u(\forall v(v \notin u) \to u \in x)$ — эти формулы равносильны, поскольку $\exists! u \forall v(v \notin u)$. Аналогично для выражений $\varnothing = x$, $x \in \varnothing$.

В общем случае, пусть для некоторой формулы $\Phi(\overline{x}, y)$ выполнено $\mathbf{ZF} \vdash \forall \overline{u} \exists! v \Phi(\overline{u}, v)$, то есть $\Phi(\overline{x}, y)$, по существу, задаёт отображение. Тогда мы будем иногда добавлять новый функциональный символ $\varphi(\overline{x})$ и использовать его в атомных формулах, имея в виду, что, например, $y \in \varphi(\overline{x})$ является сокращением для $\exists u(\Phi(\overline{x}, u) \wedge y \in u))$ или $\forall u(\Phi(\overline{x}, u) \to y \in u)$. В частности, $y = \varphi(\overline{x}) \Leftrightarrow \Phi(\overline{x}, y)$.

Из аксиом степени и объемности следует, что $\mathbf{ZF} \vdash \forall u \exists! s \forall v(v \subset u \equiv v \in s)$. Мы введем обозначение $P(x)$ для соответствующего отображения, так что $P(x) = y \Leftrightarrow \forall v(v \subset x \equiv v \in y)$, мы будем называть $P(x)$ множеством подмножеств x.

Из аксиомы пары и объемности следует, что $\mathbf{ZF} \vdash \forall u, v \exists! s \forall w(w \in s \equiv (w = u \vee w = v))$. Соответствующее отображение мы будем обозначать $\{x, y\}$ и называть (неупорядоченной) парой множеств x и y. Пару $\{x, x\}$ мы будем обозначать $\{x\}$.

Класс $Un(x) = \{y \mid \exists u(y \in u \wedge u \in x)\}$ называется объединением множества x. Мы хотим показать, что $Un(x)$ является множеством и это множество определено однозначно. Мы можем воспользоваться аксиомой замены для формулы $\Phi(y, z) = z \in y$, поскольку $\{x \mid x \in a\}$, очевидно, является множеством для любого a. Множество $Un(\{x, y\})$ мы будем обозначать $x \cup y$. Через $x \cap y$ мы будем обозначать *пересечение* множеств — множество $\{z \mid z \in x \wedge z \in y\}$, через $x \setminus y$ — *разность*: $\{z \mid z \in x \wedge z \notin y\}$. Из аксиомы подмножеств непосредственно следует, что пересечение и разность являются множествами и определены однозначно.

Множество $\{\{x\}, \{x, y\}\}$ мы назовем *упорядоченной парой* множеств x, y и будем обзначать $< x, y >$. Нетрудно доказать основное свойство упорядоченных пар:

$$< x, y > = < x', y' > \quad \Leftrightarrow \quad x = x' \wedge y = y',$$

то есть, что $\{\{x\},\{x,y\}\} = \{\{x'\},\{x',y'\}\} \quad \Leftrightarrow \quad x = x' \wedge y = y'$. Постарайтесь сами провести доказательство, рассмотрев как случай $x = y$, так и $x \neq y$.

Упорядоченная тройка $<x,y,z>$ определяется как $<x,<y,z>>$, аналогично определяется упорядоченная n-ка.

Декартово произведение $x \times y$ определяется как класс $\{z \mid \exists u,v(u \in x \wedge v \in y \wedge z =< x,y >\}$. Чтобы доказать, что $x \times y$ является множеством, нам достаточно показать, что все элементы класса содержатся в некотором множестве, и воспользоваться аксиомой подмножеств. Это сделать нетрудно, поскольку $a \in x \times y \Rightarrow a \in P(P(x \cup y))$.

Множество f пар $<a,b>$ мы будем называть *функцией* и обозначать это как $Func(f)$, если $\forall u,v,w(<u,v> \in f \ \wedge \ <u,w> \in f \quad \to \quad v = w)$. Если f — функция, то множество $\{z \mid \exists u(<z,u> \in f)\}$ называется *областью определения* $(Dom(f))$, а множество $\{z \mid \exists u(<u,z> \in f)\}$ — *областью значений* $(Ra(f))$ функции. Покажите, воспользовавшись аксиомой замены, что это действительно множества. Ясно, как определить *инъективную (взаимно однозначную)* функцию; соответствующую формулу мы обозначим $IFunc(x)$.

Если f — функция, $x \in Dom(f)$, то через $f(x)$ мы будем (не опасаясь некоторой двусмысленности) обозначать единственное множество y, такое, что $<x,y> \in f$.

Натуральные числа (ω)

Теперь мы готовы к тому, чтобы определить, что соответствует в нашей модели набору натуральных чисел. Натуральным числам 0, 1, 2, 3, ... будут соответствовать множества $\varnothing,\ \{\varnothing\},\ \{\varnothing,\{\varnothing\}\},\ \{\varnothing,\{\varnothing\},\{\varnothing,\{\varnothing\}\}\},\ \dots$.

Обозначим через $S(x)$ множество $x \cup \{x\}$. В этих обозначениях можно сказать, что $0 = \varnothing,\ \ 1 = S(0),\ \ 2 = S(1),\ \dots$, а аксиома бесконечности имеет вид

$$\exists s(\varnothing \in s \wedge \forall u(u \in s \to S(u) \in s)).$$

Обозначим через ω пересечение всех таких множеств, то есть

$$\omega = \{x \mid \forall s((\varnothing \in s \wedge \forall u(u \in s \to S(u) \in s)) \to x \in s)\}.$$

Из аксиомы бесконечности и аксиомы подмножеств следует, что ω является множеством, по аксиоме объемности это множество определено однозначно. Символами $n,\ m,\ k,\ \dots$ мы будем в данном разделе обозначать элементы ω.

Теорема индукции: в любом непустом подмножестве ω имеется минимальный элемент, то есть

$$\mathbf{ZF} \vdash \forall u(u \subset \omega \wedge u \neq \varnothing \to (0 \in u \vee \exists v(v \in \omega \wedge v \notin u \wedge S(v) \in u))).$$

Доказательство. Пусть $a \subset \omega,\ \ b = \omega \setminus a$. Предположим, что $\varnothing \in b,\ \ (c \in b \to S(c) \in b)$. Тогда, по определению ω, выполнено $\omega \subset b$, то есть a пусто. □

Определим порядок на ω так, что $x < y \Leftrightarrow x \in y$.

Несколько простых свойств порядка на ω (некоторые из них, выбранные достаточно произвольно, мы докажем, остальные оставим в качестве упражнений):

(0) $n = 0 \ \ \vee \ \ \exists m(n = S(m)),$ (индукция)

(1) $n < S(n),$ (определение)

(2) $x \in n \to x \subset n$.

Доказательство. Возможно, что доказательство написано излишне подробно. Доказываем (2) от противного, по индукции.

Рассмотрим набор $\{y \mid y \in \omega \wedge \exists u(u \in y \wedge \neg(u \subset y))\}$. По аксиоме подмножеств этот набор является множеством, обозначим его a. По предположению $a \neq \varnothing$, следовательно, по теореме индукции, в нем есть минимальный элемент – обозначим его n. По определению a выполнено $0 \notin a$, поэтому $n = S(m)$ для некоторого $m \in \omega \setminus a$.

Если $x \in S(m)$, то, по определению операции S, имеет место $x = m$ или $x \in m$. Если $x = m$, то $x \subset S(m)$ по определению операции S. Если $x \in m$, то $x \subset m$, поскольку $m \notin a$. Тогда $x \subset m \subset S(m)$. □

(3) Порядок транзитивен: $n < m \;\wedge\; m < k \quad \to \quad n < k$, (используем (2))

(4) $\neg(n < n)$, (индукция или аксиома регулярности)

(5) $0 < S(n)$, (индукция)

(6) $n < m \;\to\; m = S(n) \vee S(n) < m$, (индукция по m)

(7) порядок линеен, то есть любые два элемента сравнимы: $(n < m) \;\vee\; (n = m) \;\vee\; (m < n)$.

Доказательство. По индукции. Пусть есть несравнимые элементы. Пусть $a = \{x \mid x \in \omega \wedge \exists w(w \in \omega \wedge (x \text{ и } w \text{ не сравнимы}))\}$. Пусть n — минимальный элемент множества a. Из (5) следует, что $n \neq 0$, поэтому $n = S(m)$, $m \notin a$. Пусть n не сравним с k. Однако m сравним с k. Если $k < m$, $k = m$, то $k < n$ из (3). Если $m < k$, то n сравнимо с k из (6). □

Через $n+1$ мы будем обозначать $S(n)$, через $n-1$ — такое (единственное) m, что $n = S(m)$ (если такое m существует), через $[n,m]$ — $\{k \mid k \in \omega,\ n \leqslant k,\ k \leqslant m\}$.

Теперь нетрудно рекурсивно определить сложение на элементах ω как функцию $\Sigma\colon \omega \times \omega \to \omega$, удовлетворяющую следующим рекурсивным соотношениям:

(0) $\Sigma(< n, 0 >) = n$,
(1) $\Sigma(< n, m+1 >) = \Sigma(< n, m >) + 1$.

Докажем стандартной индукцией, что такое единственное Σ существует и является всюду определенной функцией на $\omega \times \omega$.

Доказательство. Скажем, что элемент $k \in \omega$ *корректен*, если существует функция $\Sigma\colon \omega \times [0,k] \to \omega$, удовлетворяющая указанным рекурсивным соотношениям при $m \leqslant k$. Пусть k' — наименьший некорректный элемент. Из (0) следует, что $k' \neq 0$. Если $k' = l+1$, то из корректности l можно доопределить Σ на k' в соответствии с (1). То есть все элементы ω корректны. Единственность Σ доказываем так же, рассмотрев элементы, на которых функция $\Sigma\colon \omega \times [0,k] \to \omega$ не единственна.

Таким образом, для любого $k \in \omega$ существует единственная функция Σ_k, удовлетворяющая рекурсивным соотношениям на множестве $\omega \times [0,k]$. Нетрудно заметить, что $k < k' \Rightarrow \Sigma_k \subset \Sigma_{k'}$. По аксиоме замены $Un(\{\Sigma_k \mid k \in \omega\})$ является функцией. Эта функция и будет сложением. □

Вместо $\Sigma(< n, m >)$ мы будем использовать привычную запись $n + m$.

Теперь нетрудно определить умножение как функцию $\Pi\colon \omega \times \omega \to \omega$, удовлетворяющую рекурсивным соотношениям:

(0) $\Pi(< n, 0 >) = 0$,
(1) $\Pi(< n, m + 1 >) = \Pi(< n, m >) + n$.

Аналогично можно определить и все прочие нужные нам арифметические функции и отношения. Множество целых чисел можно определить как множество пар вида $< 0, n >$ и $< 1, n >$ $(n \in \omega)$, имея в виду, что $< 0, n >$ соответствует положительному числу, а $< 1, n >$ – отрицательному. Множество рациональных чисел нетрудно определить как множество упорядоченных пар целых чисел, множество действительных чисел — как множество Дедекиндовых сечений (подмножеств специального вида в множестве рациональных чисел) и т.д. Вы уже и сами можете понять, как обычные математические утверждения переводятся в формулы теории **ZF** и оценить, насколько сложно перформулировать обычные доказательства в вывод в теории **ZF**.

Мы далее не будем систематически исследовать, как содержательная математика вкладывается в **ZF**, а потратим еще некоторое время на исследование свойств множеств в **ZF**.