Введение в математическую логику

Лекция 11

В следующем разделе мы будем рассуждать в терминах содержательной теории множеств, а не в терминах формальной теории **ZF**.

Полный порядок (содержательная теория множеств)

Порядок на классе A называется *фундированным*, если в любом непустом подклассе класса A имеется минимальный элемент, то есть $B \subset A, B$ непусто $\Rightarrow \exists u(u \in B \wedge \forall v(v < u \rightarrow v \notin B))$.

Фундированный линейный порядок на классе A называется *полным*, а сам класс — *вполне упорядоченным*.

Иными словами, порядок является полным, если нет бесконечной убывающей цепочки $a_0 > a_1 > a_2 > \dots$ — легко заметить, что эти два определения эквивалентны.

Примеры вполне упорядоченных классов: конечный класс с любым линейным порядком, класс натуральных чисел N.

Несколько простых фактов о полном порядке:

(1) В вполне упорядоченном классе A существует наименьший элемент, мы будем обозначать его символом 0.

(2) Любой непустой подкласс вполне упорядоченного класса вполне упорядочен.

(3) Для каждого элемента x, кроме наибольшего, существует единственный непосредственно следующий за ним, то есть такой элемент y, что $x < y$ но не существует такого z, что $x < z < y$. Нужно в качестве y взять наименьший элемент из больших x (такие существуют). Такой элемент мы будем обозначать $x + 1$, следующий за ним $x + 2$ и т.д.

Определение. Элемент x, не являющийся наименьшим и не имеющий непосредственно предшествующего (т.е. $x \neq y + 1$ для всех y) называется *предельным*.

(4) Всякий элемент вполне упорядоченного класса имеет вид $a + n$ для некоторого натурального n и предельного a. Действительно, если x — не предельный, то рассмотрим цепочку $x > x - 1 > x - 2 > \dots$ — цепочка не может быть бесконечной.

(5) Если A и B — вполне упорядоченные классы, то классы $A + B$ и $A \times B$ вполне упорядочены.

Напомним, что если A и B — два упорядоченных множества, то через $A \times B$ мы обозначаем множество пар, порядок на котором задан так: $(a_0, b_0) < (a_1, b_1)$ если $a_0 < a_1$ или $a_0 = a_1$ и $b_0 < b_1$. Если A и B — два непересекающихся упорядоченных множества, то через $A + B$ мы обозначаем множество $A \cup B$, порядок на котором задан так: если $a \in A, b \in B$, то $a < b$ если $a, b \in A(a, b \in B)$ то порядок определяется порядком на $A(B)$.

Действительно, если $C \subset A + B$ содержит элементы из A, то нужно взять наименьший в $C \cap A$, в противном случае — в $C \cap B$. Если $C \subset A \times B$, то сначала найдем наименьший элемент $a_0 \in A$, такой, что $< a_0, b > \in C$ для некоторого $b \in B$. Далее возьмем (непустой) подкласс $\{b | b \in B, < a_0, b > \in C\}$ и найдем в нем наименьший элемент b_0. Ясно, что $< a_0, b_0 >$ будет наименьшим в C.

(6) Классы $N + k, N + N, k \times N, N \times k, N \times N$ вполне упорядочены. Здесь k — конечный набор из k элементов, а запись $N + N$ подразумевает, что мы берем две непересекающиеся копии натурального ряда (впрочем, можно просто вместо $N + N$ взять $2 \times N$). В классе $2 \times N$ есть предельный элемент: $< 1, 0 >$.

Начальные отрезки

Определение. Подкласс B вполне упорядоченного класса A называется *начальным отрезком* класса A, если вместе с каждым элементом он содержит и все меньшие, то есть $a \in B, b < a \Rightarrow b \in B$.

(7) Классы $[0, a)$ (совокупность элементов меньших a) и $[0, a]$ (совокупность элементов не больших a) являются начальными отрезками.

(8) Любой начальный отрезок класса A, отличный от A, имеет вид $[0, a)$. Достаточно взять наименьший элемент, не принадлежащий отрезку.

(9) Объединение любого семейства начальных отрезков является начальным отрезком (из определения).

Определение. Подкласс B упорядоченного класса A *кофинален* классу A, если для любого $a \in A$ найдется $b \in B, a \leqslant b$.

Вполне упорядоченные классы представляют особый интерес, поскольку для них можно проводить доказательство по индукции и давать индуктивные определения примерно так же, как и для натуральных чисел. Индуктивное доказательство основывается на том, что если во вполне упорядоченном классе есть элементы, удовлетворяющие некоторому условию, то найдется наименьший элемент, удовлетворяющий данному условию. Индуктивное определение основано на том, что если значение отображения f на вполне упорядоченном классе A определено на элементе 0 и значение $f(a)$ однозначно определяется набором значений $f(a')$ при $a' < a$, то, используя индукцию нетрудно показать, что такое отображение определено на всем классе A и единственно. Такая индукция называется *трансфинитной* индукцией. Достаточно часто трансфинитное индуктивное определение дается отдельно для предельных и непредельных элементов: значение отображения на непредельном элементе определяется значением на предыдущем элементе, значение на предельном – набором значений на всех меньших. Мы не будем давать формальное определение трансфинитной индукции, ограничившись несколькими примерами.

Пусть A — вполне упорядоченный клас, $f \colon A \to A$ — монотонно возрастающее отображение, то есть $a < b \Rightarrow f(a) < f(b)$. Тогда $f(a) \geqslant a$ для всех $a \in A$. Следовательно образ $f(A)$ кофинален A.

Доказательство. Пусть $a > f(a)$ для некторого $a \in A$, пусть a' — наименьший элемент с таким свойством. Тогда $a' > f(a') \Rightarrow f(a') > f(f(a'))$ (монотонность), т.е. $f(a')$ меньше a', противоречие. $\square$

Следующий результат важен не только как иллюстрация понятий трансфинитная индукция и рекурсия, но и сам по себе.

Теорема об отображении полных порядков.
Пусть A и B — два вполне упорядоченных класса. Тогда или A изоморфно некоторому начальному отрезку B, или B изоморфно некоторому начальному отрезку A, причем этот изоморфизм единственен.

Доказательство. Назовем начальный отрезок I класса A *корректным*, если он изоморфен некоторому начальному отрезку класса B. Пусть I — корректный отрезок, а f_I — соответствующий изоморфизм на I. Нетрудно заметить, что для любого $a \in I$ образ $f_I([0,a))$ является начальным отрезком класса B. Таким образом f_I удовлетворяет (трансфинитному) рекурсивному соотношению $f_I(a) =$ *наименьший элемент* $\{b|b \in B, b \neq f_I(a')$ *для всех* $a' < a\}$. Таким образом, значение $f_I(a)$ полностью определяется значениями $f_I(a')$ при $a' < a$ и $f(0) = 0$. Отсюда по трансфинитной индукции, следует, что такой изоморфизм единственен. Кроме того, если J такой начальный отрезок класса A, что $J \subset I$, то J тоже корректный и (из единственности) $f_I = f_J$ на J. Пусть отрезок I_0 — объединение всех корректных начальных отрезков. Он корректен, поскольку отображение f — объединение всех f_I — будет требуемым изоморфизмом. Если $A = I_0$ или $B = f(I_0)$, то все доказано. Если $I_0 = [0,a)$ для некоторого $a \in A$ и $f(I_0) \neq B$, то доопределим отображение f так, что $f(a) =$ *наименьший элемент класса* $B \setminus f(I_0)$, что противоречит тому, что отрезок $[0,a]$ не корректный. $\square$

Следствие. Подкласс B вполне упорядоченного класса A изоморфен начальному отрезку класса A.

Доказательство. Если B не изоморфен начальному отрезку A, то, по теореме об отображении полных порядков, класс A должен быть изоморфен собственному начальному отрезку B. Это невозможно, поскольку такой отрезок не кофинален A. $\square$

Теорема об отображении полных порядков позволяет ввести отношение порядка на вполне упорядоченных классах. Мы скажем, что класс A меньше класса $B (A < B)$, если A изоморфно собственному начальному отрезку B. Ясно, что для любого A неверно $A < A$, поскольку требуемый изоморфизм единственен (таким образм тождественен). То есть любые два класса A, B или изоморфны, или $A < B$ или $B < A$. Этот порядок на классах является полным в следующем смысле:

В любом семействе вполне упорядоченных классов есть "наименьший элемент" изоморфный начальному отрезку любого другого элемента семейства

Доказательство. Пусть A – некоторый элемент семейства. Если он не "наименьший", то есть элемент семейства, изоморфный $[0,a)$ для некоторого $a \in A$. Найдем такое наименьшее a'. Элемент, изоморфный $[0,a')$ будет наименьшим. $\square$

На первый взгляд вполне упорядоченные классы встречаются достаточно редко, однако мы собираемся вскоре показать, что в некотором смысле любой набор можно вполне упорядочить.

Теперь мы возвращаемся к формальной теории **ZF**.

Полный порядок (формальная теория множеств)

Дадим теперь формальные определения.

Мы скажем, что множество $R \subset a \times a$ является порядком на множестве a, если

(1) оно антисимметрично: $\forall u(u \in a \to < u, u > \notin R)$

(2) транзитивно: $\forall u, v, w(< u, v > \in R \wedge < v, w > \in R \to < u, v > \in R)$

В дальнейшем вместо $< \ u, v \ > \in \ R$ мы будем писать, несмотря на некоторую двусмысленность, $u < v$.

Порядок линеен, если $\forall u, v(u \in a \wedge v \in a \to (u = v \vee u < v \vee v < u))$

Порядок фундирован, если $\forall u(u \subset a \wedge u \neq \varnothing \to \exists v(v \in u \wedge \forall w(w < v \to w \notin u)))$

Упорядоченное множество a называется вполне упорядоченным (а порядок — полным), если порядок фундирован и линеен.

Мы хотим показать, что любое множество может быть вполне упорядоченно.

Пусть a — некоторое множество, а f — такая функция, что $Dom(f) = P(a) \setminus \{\varnothing\}$, $Ra(f) \subset a$. Мы скажем, что f является *функцией выбора*, если $f(x) \in x$ для любого $x \subset a, x \neq \varnothing$.

Заметим, что если множество может быть вполне упорядочено, то для него есть функция выбора: в качестве f можно взять функцию $f(x) =$ *наименьший элемент множества* x. Следующая важная теорема утверждает, что верно и обратное.

Теорема Цермело. Если для множества существует функция выбора, то оно может быть вполне упорядоченно.

Доказательство. Пусть a — некоторое множество, f — функция выбора для a. Определим функцию дополнительного выбора $g\colon P(a) \setminus \{a\} \to a$ так, что $g(x) = f(a \setminus x)$, то есть $\forall u(u \subset a \wedge u \neq a \to g(u) \in a \setminus u)$.

Пусть b — подмножество a, и $<_b$ — порядок на b. Мы скажем, что пара $< \ b, <_b >$ корректна, если

(1) порядок $<_b$ полный и

(2) $\forall u(u \in b \to u = g(\{v | v \in b, v <_b u\}))$, то есть порядок $<_b$ "согласован" с функцией g.

Ясно, что $\{< b, r > \mid < b, r > —$ *корректная пара*$\}$ является множеством, обозначим его S.

Лемма. Корректные пары согласованы, то есть если $< \ b, <_b>$ и $< \ c, <_c>$ — две корректные пары, то одна из них является начальным отрезком другой.

Действительно, по теореме об отображении полных порядков (проверьте, что и сама теорема и доказательство верны, если рассматривать не классы, а множества и не отображения, а функции) существует изоморфизм одного из упорядоченных множеств на начальный отрезок другого. Пусть h — соответствующий изоморфизм, то есть взаимно однозначная монотонно возрастающая функция, отображающая множество b на начальный отрезок c. Покажем, что функция тождественна, то есть $h(x) = x$ трансфинитной индукцией по элементам b.

Ясно, что h переводит наименьший элемент множества b в наименьший элемент множества c, то есть $h(g(\varnothing)) = g(\varnothing)$.

Пусть d — произвольный элемент множества b и отрезки $[0, d)$ и $[0, h(d))$, как и отношения $<_b$ и $<_c$ на них, по индуктивному предположению совпадают. Тогда $d = g(\{x|x <_b d\})$ и $h(d) = g(\{x|x <_c h(d)\})$, значит $d = h(d)$.

Лемма доказана

Поскольку все корректные пары согласованы, то мы можем рассмотреть множество $U = Un\{b|\exists u(< b, u >\in S)\}$ и определить порядок на U так, что $x < y \Leftrightarrow x <_b y$ *для некоторого* $< b, <_b >\in S$. Это полный порядок, поскольку если $x \subset U, x \neq \varnothing$, то $x \cap b \neq \varnothing$ для некоторого b и наименьший (в смысле порядка $<_b$) элемент в этом пересечении будет наименьшим элементом x. Если $U \neq a$, то возьмем $g(U)$ и доопределим порядок на $U \cup \{g(U)\}$ так, что $x < g(U)$ для любого $x \in U$. Легко проверить, что $U \cup \{g(U)\}$ с этим порядком будет корректной парой, что противоречит определению U. $\square$

Утверждение о наличии функции выбора у произвольного множества выглядит достаточно естественно и может быть добавлено в качестве дополнительной аксиомы.

Аксиома выбора

Для любого множества существует функция выбора, формально:

$$\forall u \exists f(Func(f) \wedge Dom(f) = P(u) \setminus \{\varnothing\} \wedge \forall v(v \in Dom(f) \to f(v) \in v))$$

Теория, полученная добавлением к **ZF** аксиомы выбора, обозначается **ZFC**. С этого момента мы рассматриваем модели этой теории.

Аксиома выбора является аксиомой существования, однако, в отличие от прочих аксиом существования, она не дает никакого способа построить множество (функцию выбора), существование которого она гарантирует.