Введение в математическую логику

Лекция 11

Терминология

- Содержательная теория множеств
- Формальная теория множеств

Полные порядки

(Содержательная теория множеств)

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

Класс *A* называется *вполне упорядоченным*.

• Эквивалентное определение – в *A* нет бесконечной убывающей цепочки $a_0 > a_1 > a_2 > \ldots$.

• Примеры вполне упорядоченных классов:

- конечный класс с любым линейным порядком,
- класс натуральных чисел *N*.

Свойства полного порядка:

1. В A существует наименьший элемент – 0.
2. Непустой подкласс вполне упорядоченного класса вполне упорядочен.
3. Для каждого не наибольшего x существует единственный непосредственно следующий за ним элемент, то есть такой элемент y, что $x < y$, но не существует такого z, что $x < z < y$. Такой элемент y мы будем обозначать $x + 1$.

- Элемент x, не являющийся наименьшим и не имеющий непосредственно предшествующего, называется *предельным*.

4. Всякий элемент вполне упорядоченного класса имеет вид n или $a + n$ для некоторого натурального n и предельного a.

   Д. цепочка $x > x - 1 > x - 2 > . . .$ не может быть бесконечной.

Операции над упорядоченными классами

Если A и B — два упорядоченных класса, то $A \times B$ – это класс пар (a, b), $a \in A$, $b \in B$, упорядоченный так:

$$(a_0, b_0) < (a_1, b_1), \text{ если } a_0 < a_1 \text{ или } a_0 = a_1 \text{ и } b_0 < b_1.$$

Если A и B — два непересекающихся упорядоченных класса, то $A + B$ – это класс $A \cup B$, 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 (на B).

Свойства полного порядка (продолжение):

5. Если A и B — вполне упорядоченные классы, то классы $A + B$ и $A \times B$ вполне упорядочены.
6. Классы $N + k$, $N + N$ $(= 2 \times N)$, $k \times N$, $N \times k$ вполне упорядочены, здесь класс k — конечный.

Начальные отрезки

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

Свойства полного порядка (продолжение):

7. $[0, a)$ и $[0, a]$ являются начальными отрезками.
8. Любой начальный отрезок класса A, отличный от A, имеет вид $[0, a)$.
9. Объединение любого семейства начальных отрезков является начальным отрезком.

- Подкласс B упорядоченного класса A *кофинален* классу A, если для любого $a \in A$ найдется такой $b \in B$, что $b \geq a$.

Трансфинитная индукция

- Индуктивные определения (при всех меньших…)
- Индуктивные доказательства (при всех меньших…)
- Варианты шага, в зависимости от того, предельный или непредельный элемент

Теорема о возрастающем отображении

Пусть A *— вполне упорядоченный класс,*

$f : A \to A$ *— возрастающее отображение,*
то есть $a < b \Rightarrow f(a) < f(b)$.

Тогда $f(a) \geq a$ *для всех* $a \in A$,

образ $f(A)$ *кофинален* A.

Д. Пусть a – наименьший элемент для которого $a > f(a)$. Тогда $f(a) > f(f(a))$ (возрастание f), т.е. $f(a)$ обладает тем же свойством и меньше a, противоречие.

Теорема о вложении 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 единствен.*

Теорема о вложении полных порядков

Д. 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.

• Для любого $a \in I$ $f_I([0, a))$ – начальный отрезок класса B. Значит:

$$f_I(a) = \textit{наименьший элемент } \{b \mid b \in B,\ b \neq f_I(a') \textit{ для всех } a' < a\}.$$

Поэтому $f_I(a)$ полностью определяется значениями f_I на меньших элементах. Кроме того, $f_I(0) = 0$. Отсюда по трансфинитной индукции следует, что такой изоморфизм единствен.

• Если J – начальный отрезок класса A, $J \subset I$, то J тоже корректный и (из единственности) $f_J = f_I$ 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 на a, как *наименьший элемент класса* $B \setminus f(I_0)$, получим противоречие с тем, что отрезок $[0, a]$ уже не корректный.

Порядок на вполне упорядоченных классах

Следствие. Любой подкласс B вполне упорядоченного класса A изоморфен начальному отрезку класса A.

Д. Класс A не может быть изоморфен собственному начальному отрезку B, поскольку такой отрезок не кофинален A.

О. Класс A меньше класса B ($A < B$), если A изоморфно собственному начальному отрезку B.

Для любого A неверно $A < A$, поскольку требуемый изоморфизм единствен.

Любые два класса A, B или изоморфны, или $A < B$ или $B < A$.

В любом непустом семействе вполне упорядоченных классов есть ”наименьший элемент”, изоморфный начальному отрезку любого другого элемента семейства.

Д. Пусть A – элемент семейства и он не ”наименьший”, то есть найдется элемент семейства, изоморфный $[0, a)$ для некоторого $a \in A$.

Найдем наименьший среди таких элементов – a'. Элемент, изоморфный $[0, a')$, будет наименьшим в семействе.

В теории ZF

Множество $R \subset a \times a$ – *порядок* на множестве a, если задаваемое им отношение:

(1) антисимметрично: $\forall u(u \in a \to \neg R(u, u))$,

(2) транзитивно: $\forall u,v,w\, (R(u,v) \wedge R(v,w) \to R(u,w))$.

• Вместо $R(u,v)$ будем писать $u < v$.

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

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

Полный порядок – (1) – (4).

Функция выбора

О. Пусть a — множество, а f — такая функция, что $Dom(f) = P(a)\setminus\{\varnothing\}$, $Ra(f) \subset a$. Тогда f – *функция выбора* для множества a, если $f(x) \in x$ для любого $x \subset a$, $x \neq \varnothing$.

Если множество может быть вполне упорядочено, то для него есть функция выбора: в множестве x выбираем наименьший элемент.

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

Д. Пусть a — некоторое множество, f — функция выбора для a.

О. Определим функцию (дополнит. выбора) $g: P(a) \setminus \{a\} \to a$ так, что $g(x) = f(a \setminus x)$, тогда $\forall u\,(u \subset a \wedge u \neq a \to g(u) \in a \setminus u)$.

О. Пусть b — подмножество a, $<_b$ — порядок на b. Пара $\langle b, <_b \rangle$ корректна, если

(1) порядок $<_b$ полный и

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

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

Д. По теореме о вложении полных порядков существует изоморфизм h, отображающий (например) множество b на начальный отрезок c. Докажем, что тогда $h(x) = x$ трансфинитной индукцией по элементам b.

Ясно, что h переводит наименьший элемент b в наименьший элемент 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.

Но $d = g(\{x \mid x <_b d\})$ и $h(d) = g(\{x \mid x <_c h(d)\})$, значит $d = h(d)$. *Лемма доказана.*

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

Продолжение доказательства.

- Пусть $S = \{ \langle b, r \rangle \mid \langle b, r \rangle$ — *корректная пара*$\}$.
- $U = Un\{b \mid \exists u(\langle b, u \rangle \in S)\}$, порядок на U –

$x < y \Leftrightarrow x <_b y$ для некоторого порядка $\langle b, <_b \rangle \in S$.

- 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 доопределим порядок на $U \cup \{g(U)\}$, положив $x < g(U)$ для любого $x \in U$.

- Получим корректную пару, что противоречит определению U.

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.