Лекция 2, 17 сентября (первая половина)

ЧУМ — это множество с частичным порядком

$x \le y$ кососим. транзитивно рефлексивно

$x \le y$ и $y \le z \Rightarrow x \le z$

$x \le x$

$x \le y$ и $y \le x \Rightarrow x = y.$

ЧУМ линейно упорядочен, если любые два элемента сравнимы, т.е. $\forall x, y$ $x \le y$ или $y \le x$.

Линейно упорядоченный ЧУМ вполне упорядочен если в любом подмножестве есть наименьший элемент

Пусть M — любой ЧУМ.

$W(M)$ — множество всех вполне упорядоченных подмножеств в M, включая $\varnothing \subset M$.

Ключевая лемма: Не существует отображения $W(M) \xrightarrow{f} M$, переводящего каждое $W \in W(M)$ в элемент $f(W) \in M$, строго больший всех элементов у W.

Док-во: f-рекурсивные вполне упорядоченные подмножества $W \subset M$, т.е. такие что $\forall w \in W \quad f([w)) = w$,

$$\text{где } [w) = \{x \in W \mid x < w\}$$

Два f-рекурсивных подмножества V и W с одним начальным элементом всегда таковы, что либо $V < W$ либо $W < V$

$u \in V \setminus W$ – наименьший эл-т
$w \in W \setminus V$ – наименьший эл-т
$[u)_V$ и $[w)_W$ оба лежат в $V \cap W$

и совпадают.

Пример f-рекурсивного множества:

$$f(\varnothing) < f(f(\varnothing)) < f(\{f(\varnothing), f(f(\varnothing))\}) < f\dots$$

Возьмем объединение U всех f-рекурсивных W, начинающихся с $f(\varnothing)$.

- U – вполне упорядочено и f рекурсивно

$M \subset U$, то

$[u)_V < [w)_W$

$[x)$ явл. начальным куском в $[w)_W$, то $[x) \cup x$ тоже

$M \cap W$ непусто для какого-то начального куска W в U $\Rightarrow$ $M \cap W$ имеет мин. эл-т

явл. начальным куском в $[w)_w$

$\boxed{x = f([x))} \in U \cap W$

$[u) \subset U$ является начальным интервалом в каком-то $W \subset U$. $f([u)) = u$ в силу f-рекурсивности W.

U с одной стороны содержит все f-рекурсивные W с начальным эл-том $f(\varnothing)$, с другой стороны $f(U) > U$ и $U \cup f(U)$ — это тоже f-рекурсивное множество, не содержащееся в U, но начинающееся с $f(\varnothing)$

Сл: Если каждое вполне упорядоченное $W \subset M$ имеет верхнюю грань, т.е. такое $m \in M$, что $m \geq w$ $\forall w \in W$, то в M имеется максимальный элемент т.е. такой элемент $m^* \in M$, что неравенство $x \geq m^*$ выполняется только

для $x = m^*$.

Зам: вообще говоря неверно, что $m^* \geq x$ для всех $x \in M$

Зам: вообще говоря, максимальных элементов может быть много.

Док-во: Если $\forall m \in M \ \exists m' : m' > m$

То тогда $\forall$ вполне упорядоченного $W \subset M$ можно найти m': $m' > w \ \forall w \in W$ (по условию $\exists m : m \geq W$ и $\exists m' > m$).

Если $\forall W$ выбрать такой $m' \in M$, то мы получим отображение

$$\begin{aligned} W(M) &\longrightarrow M \\ W &\longmapsto m' \end{aligned}$$

которого не может быть.

Сл 2 (более слабая версия предыдущего следствия).

Если у каждого линейно упорядоченного подмножества $W \subset M$ есть верхняя грань, то в M есть максимальный элемент.

[Лема Цорна]

Структура поле

$\mathbb{Q}$ - рациональные числа. - базисный пример поля.

Опр. Множество $\mathbb{F}$ наз. полем, если на нём заданы две операции:

сложение $\mathbb{F}\times\mathbb{F} \to \mathbb{F}$ $(a,b)\mapsto a+b$

множение $\mathbb{F}\times\mathbb{F} \to \mathbb{F}$ $(a,b)\mapsto ab$

$a\cdot b$

со свойствами:

св-ва сложения:

(1) коммутативность: $a+b=b+a$

(2) ассоциативность: $a+(b+c)=(a+b)+c$

(3) $\exists 0\in\mathbb{F}: \forall a\in\mathbb{F}\ a+0=a$

(4) $\forall a\in\mathbb{F}$ $\exists$ противоположный элемент $(-a)$: $a+(-a)=0$

св-ва умножения:

(1) $ab=ba$

(2) $a(bc)=(ab)c$

(3) $\exists 1\in\mathbb{F}: \forall a\in\mathbb{F}\ 1a=a$

→ (4) $\forall a\in\mathbb{F}\setminus\{0\}\ \exists a^{-1}\in\mathbb{F}: a\cdot a^{-1}=1$

связь сложения с умножением:

(1) дистрибутивность $(a+b)c=ac+bc$

(2) нетривиальность: $0\neq 1$

Пример: $\mathbb{F}_2 = \{0,1\}$ $\quad 0+1=1$

$1 \cdot 1 = 1$

все остальные суммы и произведения нулевые.

- $\mathbb{F}_2 = \mathbb{Z}/(2)$ $\quad [0], [1]$ сложение и умножение по модулю 2

$0 =$ "ложь" $\quad 1 =$ "истина"

умножение — это логическое "и"

$ab = 1 \iff$ и $a=1$ и $b=1$

сложение — это "исключающее или"

$a+b=1 \iff$ либо $a=1, b=0$, либо $a=0, b=1$

- Написать многочлен $f(x)$, равный "не x"
- Написать многочлен от x и y, равный x или y

Опр. Множество M с одной операцией "+"

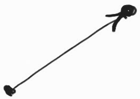
$$M \times M \longrightarrow M$$
$$(a,b) \longrightarrow a+b$$

наз. абелевой группой, если "+" удовл. аксиомам (1)–(4) сложения в поле.

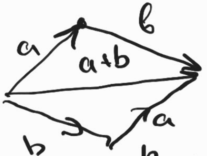
Каждое поле $\mathbb{F}$ это абелева группа по сложению, а множество ненулевых элементов $\mathbb{F}^* \overset{\text{def}}{=} \mathbb{F} \setminus \{0\}$ явл. абелевой группой по умножению.

Геометрический пример абелевой группы:

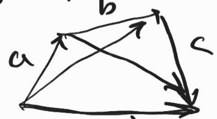
векторы.



направленные отрезки с точностью до параллельного переноса, включая точку = нулевой вектор •



$a+b=b+a$



$(a+b)+c=a+(b+c)$

Дополнительные свойства: В любой абелевой группе A: (1) 0 единствен
(2) элемент $(-a)$ однозначно определяется по a

Проверим: $0_1 = 0_1 + 0_2 \underset{0}{=} 0_2$

$$(-a)_1 = \underbrace{(-a)_1 + \mathrlap{\overbrace{}^{0}}a}_{0} + (-a)_2 = (-a)_2$$

Операция **вычитания**: $a - b := a + (-b)$

корректно определена

В поле: 1 единственна, и b^{-1} однозначно определяется по b, корректно определено

деление $a : b := a \cdot (b^{-1})$