Об интерпретациях полей в o-минимальных расширениях вещественно замкнутых полей

Константин Ковалёв

Московский физико-технический институт

Семинар «Вероятностные и субструктурные логические системы»

Определение

Структура $\mathcal{M} = (M, <, \dots)$ *с линейным порядком* $<$ *называется* *о-минимальной*, *если любое определимое с параметрами подмножество* M *является конечным объединением интервалов и точек. Здесь под интервалами имеются ввиду множества вида*

$$(a, b) = \{x \in M \mid a < x < b\},$$

где $a, b \in M \cup \{+\infty, -\infty\}$.

Замечание

Множества такого вида образуют булеву алгебру.

Примеры: DLO и ODAG

1. DLO — теория плотных линейных порядков без наибольшего и наименьшего элементов.

Утверждение

Теория DLO *допускает элиминацию кванторов. Следовательно, любой плотный линейный порядок (например,* $(\mathbb{Q}, <)$, $(\mathbb{R}, <)$, *...) о-минимален.*

2. ODAG — теория делимых упорядоченных абелевых групп.

Утверждение

Теория ODAG *допускает элиминацию кванторов. Следовательно,* $(\mathbb{Q}, +, -, 0, <)$ *и* $(\mathbb{R}, +, -, 0, <)$ *о-минимальны.*

Примеры: вещественно замкнутые поля

3. Теория RCF вещественно замкнутых полей состоит из аксиом упорядоченных полей и схемы теорем о промежуточном значении для всех многочленов. Примеры вещественно замкнутых полей:
   - $(\mathbb{R}, +, -, \cdot, 0, 1, <)$;
   - $(\mathbb{R}_{alg}, +, -, \cdot, 0, 1, <)$;
   - $\{a_n X^{n/q} + a_{n-1} X^{(n-1)/q} + \cdots + a_0 + a_{-1} X^{-1/n} + \cdots \mid a_n, a_{n-1}, \cdots \in R, n, q \in \mathbb{N}, q > 0\}$ с естественными операциями, где $(R+, -, \cdot, 0, 1, <)$ — некоторое вещественно замкнутое поле.

Теорема 1

Теория RCF *допускает элиминацию кванторов. Следовательно, любое вещественно замкнутое поле o-минимально.*

Нам также понадобится следующий хорошо известный факт: если $\mathcal{R}$ — вещественно замкнутое поле, то у него ровно 2 алгебраических расширения: $\mathcal{R}$ и $\mathcal{R}[i]$, которое является алгебраически замкнутым.

Примеры: экспоненциальное поле вещественных чисел

4. Экспоненциальное поле $\mathbb{R}_{\exp} = (\mathbb{R}, +, -, \cdot, 0, 1, <, e^x)$.

Теорема 2 ([Wilkie, 1996])

Любая формула в $\mathbb{R}_{\exp}$ эквивалентна экзистенциальной (то есть теория $Th(\mathbb{R}_{\exp})$ модельно полна).

Теорема 3 ([Khovanskii, 1980])

Множество $\{\vec{a} \in \mathbb{R}^n \mid t_1(\vec{a}) = \cdots = t_m(\vec{a}) = 0\}$ решений системы экспоненциальных уравнений состоит из конечного числа компонент связности.

Следствие

Поле $\mathbb{R}_{\exp}$ o-минимально.

Теорема 4 ([Macintyre and Wilkie, 1996])

В предположении гипотезы Шануэля, теория $Th(\mathbb{R}_{\exp})$ разрешима.

Примеры: аналитические функции

5. $\mathbb{R}_{an} = (\mathbb{R}, +, -, \cdot, 0, 1, <, (F_n)_{n\in\mathbb{N}})$, где $F_n = \{f|_{[-1,1]^n} \mid$ сущ. открытое $U \subseteq \mathbb{R}^n$, т.ч. $[-1,1]^n \subseteq U$ и $f : U \to \mathbb{R}$ аналитична$\}$.

Теорема 5 ([Denef and van den Dries, 1988])

В $\mathbb{R}_{an}$ допустима элиминация кванторов при добавлении функции $x \mapsto x^{-1}$ и она является о-минимальной.

6. $\mathbb{R}_{an,\exp,\log} = (\mathbb{R}, +, -, \cdot, 0, 1, <, (F_n)_{n\in\mathbb{N}}, e^x, \log)$, где $\log x = 0$ при $x \leq 0$.

Теорема 6 ([van den Dries et al., 1994])

В $\mathbb{R}_{an,\exp,\log}$ допустима элиминация кванторов и она является о-минимальной.

.

Утверждение (об определимых подгруппах)

Пусть $\mathcal{G} = (\mathcal{G}_0, \dots)$ *— о-минимальное обогащение группы* $\mathcal{G}_0 = (G, *, (\cdot)^{-1}, e, <)$. *Тогда*

1. $\mathcal{G}_0$ *является группой* *без кручения*;
2. *любая определимая в* $\mathcal{G}$ *подгруппа* $\mathcal{G}_0$ *выпукла*;
3. $\mathcal{G}_0$ *является* *делимой*;
4. $\{e\}$ *и* G *— единственные определимые в* $\mathcal{G}$ *подгруппы* $\mathcal{G}_0$;
5. $\mathcal{G}_0$ *абелева*;

Доказательство.

1. Пусть $g \in G$, $g \neq e$ и $n \in \mathbb{N}$, $n > 1$. Покажем, что $g^n \neq e$. Действительно, если $g > e$, то
$$g^n > eg^{n-1} > \cdots > e,$$
а если если $g < e$, то
$$g^n < eg^{n-1} < \cdots < e.$$
2. Пусть $H \subseteq G$ — определимая подгруппа $\mathcal{G}_0$. Допустим, она не является выпуклой, то есть, найдутся $h_1, h_2 \in H$ и $g \in G \setminus H$, такие что
$$h_1 < g < h_2.$$
Домножая это неравенство на h_1^{-1}, можно считать, что оно имеет вид $e < g < h$, где $h \in H$, $g \in G \setminus H$. Тогда мы имеем цепочку неравенств
$$e < g < h < gh < h^2 < gh^2 < \ldots,$$
в которой на четных позициях стоят элементы H, а на нечетных — элементы $G \setminus H$, что противоречит o-минимальности.

...

Доказательство.

3. Пусть $n \in \mathbb{N}$, $n > 1$. Рассмотрим определимую подгруппу

$$H := \{h \in G \mid \exists g(h = g^n)\}.$$

Она не ограничена сверху, так как для всякого $g \in G \setminus \{e\}$,

$$g < \max\{g^n, e\} \in H.$$

Аналогично показывается, что она не ограничена снизу. По пункту 2 H выпукла, а значит, $H = G$.

...

Доказательство.

4. Пусть $H \subseteq G$ — определимая подгруппа и $H \neq \{e\}$. Тогда в H не может быть наибольшего элемента, так как для всякого $h \in H$, $h > e$, верно $h^2 > h$. Аналогично, в H нет наименьшего элемента. Следовательно, по пункту 2 и о-минимальности получаем, что H является интервалом (a, b) для некоторых $a, b \in G \cup \{+\infty, -\infty\}$, причем $a < e < b$.
   Покажем, что $a = -\infty$, $b = +\infty$ (то есть, $H = G$). Допустим, $b \in G$. Пусть h — такой (единственный) элемент, что $h^2 = b$. Тогда $e < h < b$ и, кроме того, $h^{-1}b \in H$. Но тогда
   $$b = h(h^{-1}b) \in H,$$
   противоречие. Если $a \in G$, то $e < a^{-1} \in H$, а значит и $a \in H$, противоречие. В итоге получаем, что $H = G$.

...

Доказательство.

5. Пусть $g \in G$, покажем, что g коммутирует со всеми элементами G. Случай $g = e$ тривиален, пусть $g \neq e$. Рассмотрим определимую подгруппу

$$H := \{h \in G \mid gh = hg\}$$

элементов, коммутирующих с g. Она не равна $\{e\}$, так как $g \in H$. По пункту 4 получаем, что $H = G$.

$\square$

Утверждение ([van den Dries, 1998])

Пусть $\mathcal{R} = (R, +, -, 0, 1, <, \dots)$ — o-минимальное обогащение упорядоченной группы, $0 < 1$. Тогда в $\mathcal{R}$ есть определимые сколемовские функции.

Доказательство.

По доказанному, $(R, +, -, 0, <, \dots)$ абелева и делима. Пусть $\varphi(x, \vec{y})$ — некая формула в языке $\mathcal{R}$. Для удобства обозначим через $A(\vec{y})$ определимое множество $\{x \in R \mid \varphi(x, \vec{y})\}$. Тогда функция

$$f_\varphi(\vec{y}) := \begin{cases} \min A(\vec{y}), & \text{если он существует,} \\ 0, & \text{если } A(\vec{y}) = R, \\ b - 1, & \text{если } (-\infty, b) \text{ является самым левым интервалом в } A(\vec{y}), \\ a + 1, & \text{если } (a, +\infty) \text{ является самым левым интервалом в } A(\vec{y}), \\ (a + b)/2, & \text{если } (a, b) \text{ является самым левым интервалом в } A(\vec{y}), \\ 0, & \text{иначе} \end{cases}$$

является определимой сколемовской функцией для $\varphi(x, \vec{y})$, т.е.

$$\mathcal{R} \models \exists x \varphi(x, \vec{a}) \to \varphi(f_\varphi(\vec{a}), \vec{a}).$$

□

Определение

Модель $\mathcal{M}_0$ теории T называется простой моделью T, если для любой $\mathcal{M} \models T$ модель $\mathcal{M}_0$ элементарно вкладывается в $\mathcal{M}$.

Пример

$(\mathbb{R}_{alg}, +, -, \cdot, 0, 1, <)$ является простой моделью RCF.

Утверждение

Пусть в $\mathcal{M}$ есть определимые сколемовские функции. Тогда у $Th(\mathcal{M})$ есть простая модель.

Свойства о-минимальных групп

Указание

Множество

$$M_0 \;=\; \{x \in M \mid x \text{ определимо в } \mathcal{M} \text{ формулой без параметров}\}$$

будет носителем элементарной подстурктуры, она и будет простой моделью теории $Th(\mathcal{M})$.

Следствие

Пусть $\mathcal{R} = (R, +, -, 0, 1, <, \dots)$ *— о-минимальное обогащение упорядоченной группы,* $0 < 1$. *Тогда у* $Th(\mathcal{R})$ *есть простая модель.*

Свойства о-минимальных структур

Здесь $\mathcal{R}$ — о-минимальное обогащение вещественно замкнутого поля.

Утверждение (о дифференцируемости, [van den Dries, 1998])

Пусть $f : U \to R^n$ *— определимая в* $\mathcal{R}$ *функция,* $U \subseteq R^m$ *— определимое открытое множество,* $k \in \mathbb{N}$*. Тогда существует определимое открытое плотное* $D \subseteq U$*, т.ч.* $f|_D$ *является* k *раз дифференцируемой.*

Утверждение ([van den Dries, 1998])

Пусть $X \subseteq R^n$ *— определимое,* a *— предельная точка* X*. Тогда найдется* $\varepsilon > 0$ *и определимое непрерывное инъективное* $\gamma : (0, \varepsilon) \to X$*, т.ч.* $\lim\limits_{t \to 0} \gamma(t) = a$*.*

Доказательство.

Рассмотрим определимое множество

$$L := \{r \in R \mid \exists x \in X(|x - a| = r)\}.$$

В любом интервале вида $(0, \delta)$ содержится бесконечное число точек из L, а значит, по о-минимальности L содержит интервал вида $(0, \varepsilon_1)$. Рассмотрим определимую сколемовскую функцию $\gamma_1 : (0, \varepsilon_1) \to X$, т.ч.

$$|\gamma(\delta) - a| = \delta$$

для всех $\delta \in (0, \varepsilon_1)$. По утверждению о дифференцируемости, найдется такое определимое плотное открытое $D \subseteq (0, \varepsilon_1)$, что $\gamma_1|_D$ непрерывно. Пусть (a, b) — самый левый интервал в D, тогда он имеет вид $(0, \varepsilon)$ в силу плотности D. Следовательно, $\gamma := \gamma_1|_{(0,\varepsilon)}$ — искомая функция. □

Об интерпретациях

Под интерпретацией мы понимаем многомерные интепретации с параметрами и «мягким» равенством.

Утверждение

Если $\mathcal{K}$ интерпретируема в о-минимальном обогащении упорядоченной группы $\mathcal{M}$, то $\mathcal{K}$ интерпретируема в $\mathcal{M}$ с «жестким» равенством (или просто определима).

Основной результат

Теорема 7 ([Otero et al., 1996])

Пусть бесконечная коммутативная область целостности $\mathcal{K}$ *интерпретируема (или определима) в o-минимальной структуре* $\mathcal{R} = (\mathcal{R}_0, \dots)$, *где* $\mathcal{R}_0$ *— вещественно замкнутое поле. Тогда* $\mathcal{K}$ *определимо изоморфно* $\mathcal{R}_0$ *или* $\mathcal{R}_0[i]$.

Смежные результаты были получены и в других работах:

- "одномерные" определимые поля в $\overline{\mathbb{R}} = (\mathbb{R}, +, -, \cdot, 0, 1, <)$ определимо изоморфны $\overline{\mathbb{R}}$ ([Nesin and Pillay, 1991]);
- любая модель арифметики Пресбургера, интерпретируемая в $(\mathbb{N}, +, 0, 1, <)$, определимо изоморфна $(\mathbb{N}, +, 0, 1, <)$ ([Pakhomov and Zapryagaev, 2020]);
- аналогичные результаты есть для алгебраически и вещественно замкнутых нормированных полей ([Hrushovski and Rideau-Kikuchi, 2019] и [Hasson and Peterzil, 2021]).

Начало доказательства

Зафиксируем некоторую o-минимальную структуру $\mathcal{R} = (\mathcal{R}_0, \dots)$, $\mathcal{R}_0$ — вещественно замкнутое поле. Для простоты будем считать, что $\mathcal{R}_0 = \overline{\mathbb{R}}$.
Мы будем использовать следующие обозначения:

- $|x| = |x_1| + \dots + |x_n|$ для $x \in \mathbb{R}^n$;
- $|T| = \sum_{i,j} |T_{i,j}|$ для $T \in \mathbb{R}^{n \times m}$;
- $d_x f = (\frac{\partial f_i}{\partial x_j})_{i,j}$ для дифференцируемой $f : U \to \mathbb{R}^n$, открытого $U \subseteq \mathbb{R}^m$ и $x \in U$.

Замечание

В $\mathbb{R}^n$ все нормы эквивалентны, а потому рассуждение от выбора нормы не зависит.

Лемма

Пусть $U \subseteq \mathbb{R}^m$ — открытый параллелепипед, $f : U \to \mathbb{R}^n$ дифференцируема, $a \in U$. Тогда для всех $x \in U$ верно

$$|f(x) - f(a)| \leq |x - a| \max\{|d_y f| \mid |y - a| \leq |x - a|, y \in U\}.$$

Лемма

Пусть $U \subseteq \mathbb{R}^m$ — открытый параллелепипед, $f : U \to \mathbb{R}^n$ дифференцируема, $f(a) = 0$ для некоторого $a \in U$ и существует $C > 0$ такое, что $|d_x f| \leq C|f(x)|$ для всех $x \in U$. Тогда $f(x) = 0$ для всех $x \in U$.

Доказательство.

Без ограничения общности будем считать $a = 0$. Сначала покажем, что $f = 0$ в некоторой окрестности 0. Допустим, это не так. Рассмотрим множество

$$S := \{x \in U \mid |d_x f| = \max_{|y| \leq |x|} |d_y f|\}.$$

Заметим, что $d_0 f = 0$, а потому, $\max_{|y| \leq |x|} |d_y f|$ не может достигаться в 0 (иначе $f = 0$ в некоторой окрестности 0). Из этого следует, что 0 является предельной точкой S. Для $x \in S$ мы имеем неравенство $|f(x)| \leq |x| \cdot |d_x f|$ и, по нашему предположению, $|d_x f| \leq C|x| \cdot |d_x f|$. Выбирая x достаточно маленьким, получаем противоречие. Далее, заметим, что множество $Z := \{x \in U \mid f(x) = 0\}$ является замкнутым (по непрерывности) и открытым (аналогично рассуждению выше). Так как U связно, получаем $Z = U$. □

Лемма 8

Пусть $U = I_1 \times I_2 \subseteq \mathbb{R}^{m+n}$ *— замкнутый параллелепипед,* $F : U \to \mathbb{R}^{n\times m}$ *определима и дифференцируема,* $(a, b) \in Int(U)$. *Рассмотрим систему уравнений*

$$d_x\varphi = F(x, \varphi(x)),\ \ \varphi(a) = b.$$

Пусть $\varphi_1, \varphi_2 : I_1 \to I_2$ *— два определимых решения этой системы. Тогда* $\varphi_1(x) = \varphi_2(x)$ *для всех* $x \in Int(I_1)$.

Доказательство.

Положим $C := \max_{(x,y)\in U} |d_y F(x, \cdot)|$. Тогда $|F(x, y_1) - F(x, y_2)| \leq C|y_1 - y_2|$ для всех $(x, y_1), (x, y_2) \in Int(U)$. Пусть $\varphi_1, \varphi_2 : I_1 \to I_2$ — определимые решения. Тогда

$$|d_x(\varphi_1 - \varphi_2)| = |F(x, \varphi_1(x)) - F(x, \varphi_2(x))| \leq C|\varphi_1(x) - \varphi_2(x)|$$

для всех $x \in Int(I_1)$. Применяя предыдущую лемму к $\varphi_1 - \varphi_2$, получаем требуемое. $\square$

Об определимых группах

Следующий результат показывает, что определимые группы допускают структуру «определимого многообразия».

Теорема 9 ([Pillay, 1988])

Пусть $\mathcal{G} = (G, *, (\cdot)^{-1}, e)$ — определимая в $\mathcal{R}$ группа. Тогда найдется $n \in \mathbb{N}$, открытые определимые $U_1, \ldots, U_r \subseteq \mathbb{R}^n$, определимые инъективные $\pi_i : U_i \to G$, такие что $G = \bigcup_{i=1}^{r} \pi_i(U_i)$, функции перехода $\pi_i^{-1} \circ \pi_j$ дифференцируемы на своей области определения и, кроме того, $*$ и $(\cdot)^{-1}$ дифференцируемы.

Лемма (о гомоморфизмах)

Пусть $\mathcal{G} = (G, *, (\cdot)^{-1}, e)$ — бесконечная определимая в $\mathcal{R}$ группа со структурой дифференцируемого многообразия размерности n. Тогда для любых двух определимых гомоморфизмов $\sigma, \tau : \mathcal{G} \to \mathcal{G}$ верно

1. *σ, τ всюду дифференцируемы на $\mathcal{G}$;*
2. *если $d_g\sigma = d_g\tau$, то σ и τ совпадают в некоторой окрестности g;*
3. *если $\sigma \neq \tau$ и $\mathcal{G}$ определимо связна, то $d_e\sigma \neq d_e\tau$.*

Об определимых группах

Доказательство.

1. По утверждению о дифференцируемости найдется $h \in G$, т.ч. σ дифференцируема в окрестности U точки h. Положим $V := \{x \in G : h * x \in U\}$, по непрерывности умножения это открытое множество. Рассмотрим равенство

$$\sigma(x) = \sigma(h^{-1} * h * x) = \sigma(h^{-1}) * \sigma(h * x),$$

из него следует дифференцируемость σ в V. Аналогично для любой другой точки G.

2. Если $\sigma(g) \neq \tau(g)$, то утверждение тривиально. Пусть $\sigma(g) = \tau(g)$ и $d_g\sigma = d_g\tau$. Для $h \in G$ обозначим через r_h отображение $x \mapsto h * x$. Далее будем опускать $*$ для сокращения записи. Тогда

$$\sigma(x) = \sigma((hg^{-1})(gh^{-1}x)) = r_{\sigma(hg^{-1})}(\sigma(r_{gh^{-1}}(x)))$$

и, следовательно,

$$d_h\sigma = d_{\sigma(g)}(r_{\sigma(hg^{-1})}) \cdot d_g(\sigma) \cdot d_h(r_{gh^{-1}}).$$

...

Следствие

Пусть $\mathcal{G} = (G, *, (\cdot)^{-1}, e)$ *— бесконечная определимая в* $\mathcal{R}$ *группа со структурой дифференцируемого многообразия размерности* n, $\mathcal{G}$ *определимо связна и, кроме того, ее центр* $\{g \in G : \forall h \in G(gh = hg)\}$ *тривиален. Тогда* $\mathcal{G}$ *определимо вкладывается в* $GL_n(\mathbb{R})$.

Доказательство.

Для $g \in G$ определим гомоморфизм

$$\sigma_g : h \mapsto ghg^{-1}.$$

Заметим, что $\sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2}$. Далее, определим отображение $\varphi : \mathcal{G} \to GL_n(\mathbb{R})$ как $g \mapsto d_e \sigma_g$. Это гомоморфизм в силу свойств дифференцирования композиции. По п.3 леммы о гомоморфизмах, $\varphi(g) = I_n$ тогда и только тогда, когда $\sigma_g = id_G$. Но последнее верно только при условии, что g коммутирует со всеми элементами G. Значит, ядром φ будет центр $\mathcal{G}$, который тривиален. Следовательно, φ — вложение. $\square$

Лемма

Пусть $\mathcal{K} = (K, +_K, -_K, \cdot_K, 0_K, 1_K)$ — бесконечное определимое в $\mathcal{R}$ кольцо. Тогда найдется $n \in \mathbb{N}$, открытые определимые $U_1, \ldots, U_r \subseteq \mathbb{R}^n$, определимые инъективные $\pi_i : U_i \to K$, такие что $K = \bigcup\limits_{i=1}^{r} \pi_i(U_i)$, функции перехода $\pi_i^{-1} \circ \pi_j$ дифференцируемы на своей области определения и, кроме того, $+_K$, $-_K$ и $\cdot_K$ дифференцируемы.

Доказательство.

Возьмем такую структуру для группы $(K, +_K, -_K, 0_K)$ из Теоремы 9. Надо проверить дифференцируемость умножения. По лемме о гомоморфизмах, отображения $x \mapsto a \cdot_K x$ и $x \mapsto x \cdot_K a$ всюду дифференцируемы для любого $a \in K$. По утверждению о дифференцируемости найдутся такие открытые непустые $U, V \subseteq K$, что $\cdot_K$ дифференцируемо на $U \times V$. Для краткости далее будем опускать индекс K. Возьмем $x_0 \in U$, $y_0 \in V$. Тогда для любых $x, y, x_1, y_1 \in K$ имеем

$$x \cdot y = (x - (x_1 - x_0)) \cdot (y - (y_1 - y_0)) + (x_1 - x_0) \cdot y + x \cdot (y_1 - y_0) - (x_1 - x_0) \cdot (y_1 - y_0)$$

и, следовательно, $\cdot$ дифференцируемо в окрестности (x_1, y_1). $\square$

Об определимых кольцах

Лемма

Пусть $\mathcal{K} = (K, +_K, -_K, \cdot_K, 0_K, 1_K)$ — бесконечная определимая в $\mathcal{R}$ область целостности. Тогда $\mathcal{K}$ определимо вложимо в $M_n(\overline{\mathbb{R}})$ (кольцо матриц $n \times n$) для некоторого $n \in \mathbb{N}$.

Доказательство.

По предыдущей лемме можно считать, что на $\mathcal{K}$ введена структура определимого многообразия размерности n. Для $a \in K$ рассмотрим гомоморфизм $\lambda_a : x \mapsto ax$ аддитивной группы $\mathcal{K}$. Мы утверждаем, что

$$a \mapsto d_0\lambda_a$$

является вложением $\mathcal{K}$ в $M_n(\overline{\mathbb{R}})$. Действительно, $\lambda_{ab} = \lambda_a \circ \lambda_b$ и, следовательно,

$$d_0\lambda_{ab} = (d_0\lambda_a)(d_0\lambda_b).$$

Также, $d_0\lambda_1 = I_n$ (единичная матрица).

...

Об определимых кольцах

Доказательство.

Далее, обозначим для удобства через P_+ отображение $(x, y) \mapsto x + y$. Тогда $P_+(0, x) = P_+(x, 0) = x$ и, значит, $d_{(0,0)}P_+ = (I_n, I_n)$. Получаем, что

$$\begin{aligned} a + b = c &\implies P_+(\lambda_a, \lambda_b) = \lambda_c \\ &\implies d_{(0,0)}P_+ \begin{pmatrix} d_0\lambda_a \\ d_0\lambda_b \end{pmatrix} = d_0\lambda_c \\ &\implies d_0\lambda_a + d_0\lambda_b = d_0\lambda_c. \end{aligned}$$

Осталось заметить, что при различных a и b гомоморфизмы λ_a и λ_b совпадают только в 0, а потому, в силу п.2 леммы о гомоморфизмах, $d_0\lambda_A \neq d_0\lambda_b$. □

В силу последней леммы, можно ограничится только рассмотрением подколец $M_n(\overline{\mathbb{R}})$.

Лемма

Пусть $\mathcal{K} \subseteq M_n(\mathbb{R})$ — бесконечная определимая в $\mathcal{R}$ область целостности. Тогда $\mathcal{K}$ является $\overline{\mathbb{R}}$-алгеброй.

Доказательство.

Множество

$$\{r \in \mathbb{R} \mid rA \in K \text{ для всех } A \in K\}$$

является бесконечной определимой подгруппой o-минимальной группы $(\mathbb{R}, +, -, 0, <, \dots)$ и, следовательно, совпадает с $\mathbb{R}$ по утверждению об определимых подгруппах. $\square$

Теперь мы готовы доказать основной результат. Пусть $\mathcal{K}$ — определимая в $\mathcal{R}$ область целостности. Тогда

- $\mathcal{K}$ вложимо $M_n(\overline{\mathbb{R}})$ с помощью некоторого определимого отображения φ;
- $\mathcal{K}' := \mathrm{Im}\varphi$ является конечномерной алгеброй над $\overline{\mathbb{R}}$;
- так как $\mathbb{R}$ вещественно замкнуто, то $\dim_{\overline{\mathbb{R}}}\mathcal{K}' \in \{1, 2\}$;
- в первом случае $r \mapsto rI_n$ является изоморфизмом между $\overline{\mathbb{R}}$ и $\mathcal{K}'$, а во втором — $r + ir' \mapsto rI_n + r'J$ является изоморфизмом между $\overline{\mathbb{R}}[i]$ и $\mathcal{K}'$ (тут J — фиксированный корень из -1 в $\mathcal{K}'$).

Размерность множеств

Теперь мы обсудим доказательство использовавшейся ранее теоремы об определимой структуре многообразия на определимых группах. Для простоты мы будем доказывать ее в следующей формулировке.

Теорема 10 ([Pillay, 1988])

Пусть $\mathcal{M}$ — о-минимальная структура и $\mathcal{G} = (G, *, (\cdot)^{-1}, e)$ — определимая в $\mathcal{M}$ группа. Тогда найдется $n \in \mathbb{N}$, открытые определимые $U_1, \ldots, U_r \subseteq M^n$, определимые инъективные $\pi_i : U_i \to G$, такие что $G = \bigcup_{i=1}^{r} \pi_i(U_i)$, функции перехода $\pi_i^{-1} \circ \pi_j$ непрерывны на своей области определения и, кроме того, $*$ и $(\cdot)^{-1}$ непрерывны.

Для этого используются два важных понятия: размерность определимого множества и клеточное разложение. Для удобства мы будем работать в очень насыщенной о-минимальной структуре $\mathcal{M}$ (достаточно κ^+-насыщенности, где κ — размер языка).
Через $\mathrm{dcl}(A)$ мы обозначать множество элементов M, определимых с параметрами из A, то есть

$$\mathrm{dcl}(A) := \{x \in M \mid \text{множество } \{x\} \text{ формулой с параметрами из } A\}.$$

Определение

Оператор $\mathrm{cl} : \mathcal{P}(M) \to \mathcal{P}(M)$ *называется* *предгеометрией*, *если выполнены следующие условия:*

1. cl *монотонно и* $A \subseteq \mathrm{cl}(A)$*;*
2. cl *идемпотентно* $(\mathrm{cl}(\mathrm{cl}(A)) = \mathrm{cl}(A))$*;*
3. cl *финитно, то есть, если* $a \in \mathrm{cl}(A)$*, то* $a \in \mathrm{cl}(\{a_1, \ldots, a_k\})$ *для некоторых* $a_1, \ldots, a_k \in A$*;*
4. *выполнено свойство обмена (exchange property), то есть, если* $b \in \mathrm{cl}(A \cup \{a\}) \setminus \mathrm{cl}(A)$*, то* $a \in \mathrm{cl}(A \cup \{b\})$*.*

Множество B *называется* *независимым* *над* A*, если для любого* $b \in B$ *верно* $b \notin \mathrm{cl}(A \cup (B \setminus \{b\}))$*.*

Примеры предгеометрий:

- линейная оболочка внутри векторного пространства;
- алгебраическое замыкание внутри поля.

Размерность множеств

Утверждение

Для o-минимальных $\mathcal{M}$ оператор dcl *является* *предгеометрией* *на* M.

Определение

Размерностью кортежа $\vec{a} = (a_1, \ldots, a_n) \in M^n$ *над (маленьким)* $A \subseteq M$ *называется наименьшее такое* $k \in \mathbb{N}$, *что для некоторых* $i_1, \ldots, i_k$ *выполнено*

$$\{a_1, \ldots, a_n\} \subseteq \mathrm{dcl}(A \cup \{a_{i_1}, \ldots, a_{i_k}\}).$$

Обозначается как $\dim(\vec{a}/A)$.
Размерностью множества $X \subseteq M^n$, *определимого с параметрами из* A, *называется*

$$\max\{\dim(\vec{a}/A) \mid \vec{a} \in X\}.$$

Обозначается как $\dim X$.
Точка $a \in X$ *такая, что* $\dim(\vec{a}/A) = \dim X$, *называется* *генерической* *над* A.

Размерность множеств

Определение

Пусть $Y \subseteq X$ *— определимые множества.* Y *называется* **большим**, *если* $\dim(X \setminus Y) < \dim X$.

Утверждение

1. *Размерность множества* X *не зависит от* A.
2. $\dim(\vec{a}/A) = \max\{k \mid a_{i_1}, \dots, a_{i_k}$ *независимы над* A *для некоторых* $i_1, \dots, i_k\}$.
3. $Y \subseteq X$ *большое* $\iff$ Y *содержит все генерические точки* X.
4. *Если* $Z \subseteq Y$ *и* $Y \subseteq X$ *— большие, то и* $Z \subseteq X$ *большое.*
5. $\dim X \geq k \iff$ *найдутся координаты* $i_1, \dots, i_k$, *т.ч. проекция* X *на координаты* $i_1, \dots, i_k$ *имеет непустую внутренность.*
6. *Если* U *— открыто, то* $X \subseteq U$ *большое* $\iff$ X *плотно в* U.
7. *Если* $\varphi(\vec{x}, \vec{y})$ *— формула, то множество*

$$\{\vec{a} \mid \text{для всех генерических } \vec{b} \text{ над } \vec{a}\ \varphi(\vec{a}, \vec{b})\}$$

   определимо.

Неформально, клетками называются «хорошие» определимые множества, определимо гомеоморфные (диффеоморфные) определимому открытому множеству. Сначала поймем, зачем они нужны.

Теорема 11

1. *Каждое определимое множество является дизъюнктным объединением конечного числа клеток;*
2. *Любая клетка определимо связна;*
3. *Для любой клетки $X \subseteq M^n$ найдется $k \in \mathbb{N}$ и координаты $i_1, \ldots, i_k$, т.ч. проекция $\pi : M^n \to M^k$ на координаты $i_1, \ldots, i_k$ является гомеоморфизмом (диффеоморфизмом) X и $\pi[X]$. В этом случае, ее размерность равна k.*

Клеточное разложение

Определение

$(i_1, \ldots, i_k)$-клетки для $i_1, \ldots, i_k \in \{0, 1\}$ определяются индуктивно:

- *$\varnothing$-клеткой называется M^0;*
- *(0)-клеткой называется одноэлементное подмножество M;*
- *(1)-клеткой называется интервал в M;*
- *если X — $(i_1, \ldots, i_k)$-клетка и $f : X \to M$ определима и непрерывна, то график функции f называется $(i_1, \ldots, i_k, 0)$-клеткой;*
- *если X — $(i_1, \ldots, i_k)$-клетка и $f, g : X \to M$ определимы и непрерывны, причем $f(x) < g(x)$ для всех $x \in X$, то множества*

$$\{(x, y) \in X \times M \mid f(x) < y < g(x)\},$$

$$\{(x, y) \in X \times M \mid f(x) < y\},$$

$$\{(x, y) \in X \times M \mid y < g(x)\}$$

называются $(i_1, \ldots, i_k, 1)$-клетками.

Примеры

- $(0, 1)$-клетки — это вертикальные интервалы;
- $(1, 0)$-клетки — это графики непрерывных на интервале функций;
- открытый параллелепипед — это $(1, \ldots, 1)$-клетка.

Доказательство теоремы

Здесь и далее, $\mathcal{G} = (G, *, (\cdot)^{-1}, e)$ — определимая в $\mathcal{M}$ группа. Обогащая $\mathcal{M}$ константами, можно считать, что $\mathcal{G}$ определима без параметров.
Схема доказательства следующая:

1. Выберем большое подмножество множество $V \subseteq G$, т.ч. V определимо гомеоморфно определимому открытому множеству и групповые операции на V непрерывны;
2. С помощью V введем топологию на G так, чтобы $\mathcal{G}$ стала топологической группой; в этой топологии V будет открытым;
3. G можно покрыть конечным числом сдвигов V, то есть, найдутся $a_1, \ldots, a_s \in G$, т.ч. $G = \bigcup_{i=1}^{s} a_i V$;
4. Определим $U := \pi(V)$ для соответствующего гомеоморфизма, тогда $a_i V$ гомеоморфно U для $i = 1, \ldots, s$ и задают покрытие G.

Доказательство теоремы

Утверждение

Найдутся такие определимые $V \subseteq G$ *и* $Y \subseteq V \times V$*, что*

1. V *определимо гомеоморфно определимому открытому множеству;*
2. V *большое в* G*;*
3. Y *большое в* $G \times G$ *и плотное в* $V \times V$*;*
4. $(\cdot)^{-1}|_V : V \to V$ *непрерывно;*
5. $*|_Y : Y \to V$ *непрерывно.*

Утверждение

Положим

$$\tau := \{Z \subseteq G \mid \text{для всех } g \in G,\ (gZ) \cap V \text{ открыто в } V\}.$$

Тогда $(\mathcal{G}, \tau)$ *является топологической группой,* $V \in \tau$*.*

Доказательство.

Разобьем G на дизъюнктное объединение клеток, пусть $U_1, \dots, U_k$ — клетки размерности n. По свойствам клеток, они гомеоморфны открытым определимым подмножествам M^n. Без ограничения общности, можно считать, что эти открытые подмножества не пересекаются. Потому мы далее для простоты будем предполагать, что $U_1, \dots, U_k$ — открытые подмножества M^n. Кроме того, переходя при необходимости к плотным (а, следовательно, и большим) подмножествам U_i, можно считать, что $(\cdot)^{-1}$ непрерывна на U_i. Положим $V_0 := \bigsqcup_{i=1}^{k} U_i$ — большое подмножество G. Для всех $i, j \in \{1, \dots, k\}$ определим

$$U'_{i,j} := \{a \in U_i \mid a^{-1} \in U_j\}.$$

Далее, определим $U_{i,j}$ так: разобьем $U'_{i,j}$ на клетки, выкинем клетки малой размерности и возьмем объединение клеток размерности n. Положим

$$V_1 := \bigsqcup_{i,j} U_{i,j}.$$

...

Выбор большого множества V

Доказательство.

Мы утверждаем, что V_1 является большим в V_0 (и, следовательно, в G) и $(\cdot)^{-1}$ непрерывно на V_1.

Действительно, пусть $a \in G$ — генерическая точка. Покажем, что $a \in V_1$. Так как V_0 большое, то $a \in U_i$ для некоторого i. Понятно, что a^{-1} также генерическая, а потому $a^{-1} \in U_j$ для некоторого j. Значит, $a \in U'_{i,j}$. В силу того, что $U_{i,j}$ большое в $U'_{i,j}$, $a \in U_{i,j}$. Непрерывность $(\cdot)^{-1}$ на V_1 очевидна.

Аналогично можно найти большое $Y_0 \subseteq G \times G$ такое, что $*$ непрерывно на Y_0.

Далее, положим

$$V_1' := \{a \in V_1 \mid \text{для любой генерической } b \in G \text{ над } a, (b, a), (b^{-1}, ba) \in Y_0\}.$$

По свойствам больших множеств, оно определимо. Покажем, что оно большое.

Пусть $a \in G$ — генерическая, тогда для любой генерической над a точки $b \in G$ точка (b, a) тоже генерическая, так как $\dim(a, b) = \dim a + \dim(b/a) = 2n$. В силу того, что (b, a) и (b^{-1}, ba) взаимно определимы, (b^{-1}, ba) тоже генерическая. Так как Y_0 большое, то $(b, a), (b^{-1}, ba) \in Y_0$.

...

Выбор большого множества V

Доказательство.

Теперь определим V_2 через V_1' с помощью выбрасывания клеток малой размерности и положим

$$V \ := \ V_2 \cap V_2^{-1}.$$

Покажем, что V большое и открыто в V_0. Пусть $a \in G$ — генерическая, тогда $a \in V_2$ и, кроме того, a^{-1} тоже является генерической, а значит, $a^{-1} \in V_2$. Таким образом, $a \in V$. Открытость получается засчет того, что на каждом этапе построения мы выкидывали клетки малой размерности. Аналогично, $V \times V$ большое и открыто в $V_0 \times V_0$.

Теперь положим

$$Y \ := \ (V \times V) \cap \{(a, b) \in Y_0 \mid ab \in V\}.$$

Так как умножение непрерывно на Y_0, то Y открыто в $V \times V$, а, значит, и в $V_0 \times V_0$. Кроме того, если $(a, b) \in G \times G$ — генерическая, то и ab тоже, значит, $a, b, ab \in V$, $(a, b) \in Y_0$, то есть, $(a, b) \in Y$. Таким образом, Y большое. Раз $V \times V$ открыто, то Y плотно в $V \times V$. □

Покрытие конечным числом сдвигов

Утверждение

Пусть определимое $X \subseteq G$ *— большое. Тогда для некоторых* $a_1, \ldots, a_s \in G$ *верно*

$$G = \bigcup_{i=1}^{s} a_i X.$$

Доказательство.

Пусть $\mathcal{M}_0$ — элементарная подструктура $\mathcal{M}$ размера κ, содержащая все параметры, над которыми определены X и $\mathcal{G}$. Через $\mathcal{G}^{\mathcal{M}_0}$ и $G^{\mathcal{M}_0}$ обозначим определимую в $\mathcal{M}_0$ группу, определенную формулами, с помощью которых определялась $\mathcal{G}$ и ее носитель соответственно.

Сначала мы покажем, что

$$(*) \qquad \text{для всякого } a \in G \text{ найдется такой } b \in G^{\mathcal{M}_0}, \text{ что } a \in bX.$$

Зафиксируем произвольный $a \in G$.

Покрытие конечным числом сдвигов

Доказательство.

Пусть $c \in G$ — генерическая над M_0 точка G. Рассмотрим тип

$$p_0(x) \ := \ \mathrm{tp}(c/M_0).$$

Лемма

Если $p(\vec{x}) \in S_n(A)$ конечно реализуем с помощью элементов из множества $C \subseteq M^n$ и $B \supseteq A$, то найдется тип $q(\vec{x}) \in S_n(B)$, $p(\vec{x}) \subseteq q(\vec{x})$, конечно реализуемый с помощью элементов из множества C.

По лемме выше, $p_0(x)$ расширить до типа $p(x)$ над $M_0 \cup a$, который конечно реализуем в $\mathcal{M}_0$. Пусть $c' \in G$ реализует тип $p(x)$ (такой существует по насыщенности). Покажем, что точка c' является генерической над $M_0 \cup a$, то есть,

$$\dim(c'/M_0 \cup a) = \dim(c/M_0) = \dim G.$$

Доказательство.

Для удобства обозначим $\dim(c/M_0)$ через k, а $\dim(c'/M_0 \cup a)$ через k'. Понятно, что $k' \leq k$. Пусть $c_0' \subseteq c'$ — подкортеж размера k', т.ч. $c' \subseteq \mathrm{dcl}(M_0 \cup a \cup c_0')$, а c_0 — соответствующий ему подкортеж c (тоже размера k'). Покажем, что $c \subseteq \mathrm{dcl}(M_0 \cup c_0)$, отсюда будет следовать, что $k \leq k'$. Действительно, пусть c' определяется формулой $\varphi(x, a, c_0')$, где φ — формула с параметрами из M_0 (не пишем их явно для сокращения записи). Тогда

$$\mathcal{M} \vDash \exists y \in G(\varphi(c', y, c_0') \wedge \forall x(\varphi(x, y, c_0') \to x = c')),$$

а так как $\mathrm{tp}(c'/M_0) = \mathrm{tp}(c/M_0)$, то

$$\mathcal{M} \vDash \exists y \in G(\varphi(c, y, c_0) \wedge \forall x(\varphi(x, y, c_0) \to x = c)).$$

Далее, $\mathcal{M}_0 \preceq \mathcal{M}$, а значит, для некоторого $b \in G^{\mathcal{M}_0}$, имеем

$$\mathcal{M} \vDash \varphi(c, b, c_0) \wedge \forall x(\varphi(x, b, c_0) \to x = c).$$

Таким образом, $\varphi(x, b, c_0)$ является определяющей формулой для c с параметрами из M_0.

Доказательство.

Так как X большое, то $a^{-1}X$ тоже большое (так как есть определимая биекция между X и $a^{-1}X$). Значит, $c' \in a^{-1}X$ и, следовательно, $a \in c'^{-1}X$. Но т.к. $p(x) = \mathrm{tp}(c'/M_0 \cup a)$ конечно реализуем в $\mathcal{M}_0$, то $a \in bX$ для некоторого $b \in G^{\mathcal{M}_0}$. Мы показали, что

$$(*) \qquad \text{для всякого } a \in G \text{ найдется такой } b \in G^{\mathcal{M}_0}, \text{ что } a \in bX.$$

Допустим, что для любых $a_1, \ldots, a_s \in G^{\mathcal{M}_0}$ неверно, что $G = \bigcup_{i=1}^{s} a_i X$. Рассмотрим частичный тип

$$q(x) := \{(x \in G) \wedge (x \notin bX) \mid b \in G^{\mathcal{M}_0}\}.$$

Он конечно реализуем по нашему предположению, а значит, реализуем (так как $\mathcal{M}$ κ^+-насыщена). Но тогда для элемента, реализующего этот тип, не выполнено условие $(*)$, противоречие. □

Утверждение

Положим

$$\tau \;:=\; \{Z \subseteq G \mid \text{для всех } g \in G,\ (gZ) \cap V \text{ открыто в } V\}.$$

Тогда $(\mathcal{G}, \tau)$ *является топологической группой,* $V \in \tau$.

Лемма

Пусть $a, b \in G$.

1. *Множество* $Z_1 \;:=\; \{x \in V \mid axb \in V\}$ *открыто в* V *и отображение* $x \mapsto axb$ *является гомеоморфизмом* $Z_1 \to aZ_1 b$.
2. *Множество* $Z_2 \;:=\; \{(x, y) \in V \times V \mid axby \in V\}$ *открыто в* $V \times V$ *и отображение* $(x, y) \mapsto axby$ *является непрерывным на* Z_2.
3. *Для* $Z \subseteq V$, aZ *является* τ*-открытым тогда и только тогда, когда* Z *открыто в* V.
4. *Для* $Z \subseteq V \times V$, $(a, b)Z$ *является* τ*-открытым тогда и только тогда, когда* Z *открыто в* $V \times V$.

Выведем утверждение из леммы.

Доказательство.

Зафиксируем такие $a_1, \ldots, a_s \in G$, что $G = \bigcup_{i=1}^{s} a_i V$. По п.3 леммы выше, $a_i V$ являются τ-открытыми.
Покажем, что $(\cdot)^{-1}$ является τ-непрерывно. Пусть $W \subseteq G$ — τ-открытое. Можно считать, что $W \subseteq a_i V$. По п.3 леммы, $a_i^{-1} W \subseteq V$ открыто и, значит, $(a_i^{-1} W)^{-1} = W^{-1} a_i \subseteq V$ тоже открыто, так как $(\cdot)^{-1} : V \to V$ непрерывно. Тогда для любого $g \in G$,

$$(gW^{-1}) \cap V = g(W^{-1} a_i) a_i^{-1} \cap V$$

является гомеоморфным образом открытого множества

$$\{x \in V \mid gxa_i^{-1} \in V\} \cap (W^{-1} a_i)$$

по п.1 леммы и, следовательно, открыто. Значит, W^{-1} является τ-открытым.
...

Доказательство.

Теперь покажем, что умножение непрерывно. Пусть $W \subseteq G$ — τ-открыто. Надо доказать, что множество

$$Z \ := \ \{(x,y) \in G \times G \mid xy \in W\}$$

τ-открыто. Опять же, можно считать, что $W \subseteq a_i W$. Далее, достаточно показать, что τ-открытыми являются множества вида

$$Z_{j,k} \ := \ \{(x,y) \in (a_j V) \times (a_k V) \mid xy \in W\}$$

являются τ-открытыми, так их объединение равно Z. Но

$$\begin{aligned} Z_{j,k} \ &= \ (a_j, a_k)\{(z,w) \in V \times V \mid a_j z a_k w \in W\} \\ &= \ (a_j, a_k)\{(z,w) \in V \times V \mid a_i^{-1} a_j z a_k w \in a_i^{-1} W\}, \end{aligned}$$

причем $\{(z,w) \in V \times V \mid a_i^{-1} a_j z a_k w \in a_i^{-1} W\}$ является открытым по п.2 леммы, и, следовательно, $Z_{j,k}$ является τ-открытым по п.4 леммы. $\square$

Список литературы

Denef, J. and van den Dries, L. (1988).
p-adic and real subanalytic sets.
Annals of Mathematics, 128(1):79–138.

Hasson, A. and Peterzil, Y. (2021).
Interpretable fields in real closed valued fields and some expansions.

Hrushovski, E. and Rideau-Kikuchi, S. (2019).
Valued fields, metastable groups.
Selecta Mathematica.

Khovanskii, A. G. (1980).
A class of systems of transcendental equations.
Dokl. Akad. Nauk SSSR, 255:4.

Macintyre, A. and Wilkie, A. (1996).
On the decidability of the real exponential field.

Nesin, A. and Pillay, A. (1991).
Some model theory of compact lie groups.
Transactions of the American Mathematical Society, 326(1):453–463.

Список литературы

Otero, M., Peterzil, Y., and Pillay, A. (1996).
On groups and rings definable in o–minimal expansions of real closed fields.
Bulletin of the London Mathematical Society, 28(1):7–14.

Pakhomov, F. and Zapryagaev, A. (2020).
Multi-dimensional interpretations of presburger arithmetic in itself.
Journal of Logic and Computation, 30(8):1681–1693.

Pillay, A. (1988).
On groups and fields definable in o-minimal structures.
Journal of Pure and Applied Algebra, 53(3):239–255.

van den Dries, L. (1998).
Tame Topology and O-minimal Structures.
London Mathematical Society Lecture Note Series. Cambridge University Press.

van den Dries, L., Macintyre, A., and Marker, D. (1994).
The elementary theory of restricted analytic fields with exponentiation.
Annals of Mathematics, 140.

Список литературы

Wilkie, A. (1996).
Model completeness results for expansions of the ordered field of real numbers by restricted pfaffian functions and the exponential function.
Journal of the American Mathematical Society, 9.

Спасибо за внимание!