О семнадцатой проблеме Гильберта

Станислав Сперанский

Математический институт им. В.А. Стеклова РАН
(МЦМУ МИАН)

Дубна 2024

Рассмотрим произвольные поле $\mathfrak{F}$ и $n \in \mathbb{N}$.

Говорят, что $f :\subseteq F^n \to F$ является рациональной функцией над $\mathfrak{F}$ от n переменных, если сущ. $p, q \in F[x_1, \ldots, x_n]$ такие, что

$$f(\vec{r}) = \frac{p(\vec{r})}{q(\vec{r})} \quad \text{для всех } \vec{r} \in F^n.$$

Тут $x_1, \ldots, x_n$ суть переменные, принимающие значения в F. Для удобства обозначим множество всех рациональных функций над $\mathfrak{F}$ от n переменных через $F(x_1, \ldots, x_n)$. На нём можно естественным задать структуру кольца, обозначаемого через $\mathfrak{F}(x_1, \ldots, x_n)$.

Упражнение

$\mathfrak{F}(x_1, \ldots, x_n)$ является полем.

Будем называть $f \in F(x_1, \ldots, x_n)$ неотрицательной, если $f(\vec{r}) \geqslant 0$ для всех $\vec{r} \in \operatorname{dom} f$. При этом, очевидно,

$$\operatorname{dom} f \;=\; \{\vec{r} \in F^n \mid q(\vec{r}) \neq 0\},$$

где q — из определения выше.

17-ая проблема Гильберта

Верно ли, что любую неотрицательную рациональную функцию над $\mathbb{R}$ от n переменных можно представить в виде (конечной) суммы квадратов рациональных функций над $\mathbb{R}$ от n переменных?

Теорема (Артина)

Ответ на вопрос выше — положительный, причём не только над $\mathbb{R}$, но и над произвольным вещественно замкнутым полем.

Исходное доказательство Э. Артина было существенно упрощено А. Робинсоном. Ниже будет приведён набросок по модулю некоторых фактов из алгебры, доказательства котороых можно легко найти в литературе, например в

S. Lang. *Algebra*. 3rd edition, revised. Springer, 2002.

Поле $\mathfrak{F}$ называют формально вещественным, если -1 нельзя представить в виде суммы квадратов элементов F.

Лемма

Пусть $\mathfrak{F}$ — формально вещественное поле, $a \in F$. Предположим, что a нельзя представить в виде суммы квадратов элементов F. Тогда существует упорядочение $\mathfrak{F}$, которое делает a отрицательным.

Под вещественным замыканием $\mathfrak{F}$ понимается (произвольное) вещ. замкнутое поле, которое расширяет $\mathfrak{F}$ и алгебраично над $\mathfrak{F}$.

Лемма

Пусть $\mathfrak{F}$ — поле, $\preccurlyeq$ — его упорядочение. Тогда существует вещественное замыкание $\mathfrak{F}(x_1, \ldots, x_n)$, чей порядок расширяет $\preccurlyeq$.

Схема доказательства (теоремы Артина, в духе Робинсона).

Пусть $\mathfrak{F}$ — вещественно замкнутое поле. Рассмотрим произвольную неотрицательную $f \in F(x_1, \ldots, x_n)$. Рассуждая от противного, предположим, что f нельзя представить в виде суммы квадратов эл-тов $F(x_1, \ldots, x_n)$. Наша цель — получить противоречие.

Легко понять, что $\mathfrak{F}(x_1, \ldots, x_n)$ является формально вещественным. Стало быть, ввиду **первой из лемм**, найдётся упорядочение $\preccurlyeq$ для $\mathfrak{F}(x_1, \ldots, x_n)$ такое, что $f \prec 0$. Пусть $\mathfrak{F}^*$ — вещественное замыкание $\mathfrak{F}(x_1, \ldots, x_n)$, чей порядок расширяет $\preccurlyeq$; его даёт **вторая лемма**.

...

Схема доказательства.

Далее, пусть

$$f(\vec{x}) \;=\; \frac{p(\vec{x})}{q(\vec{x})},$$

где $p, q \in F[x_1, \ldots, x_n]$. Ясно, что полиномы p и q можно воспринимать как σ-термы с параметрами из F. Поэтому выражение

$$\exists \vec{x}\,(p(\vec{x}) \cdot q(\vec{x}) < 0)$$

можно воспринимать как σ-формулу с параметрами из F. Тогда из $f \prec 0$ следует

$$\mathfrak{F}^* \Vdash \exists \vec{x}\,(p(\vec{x}) \cdot q(\vec{x}) < 0).$$

Грубо говоря, причина в том, что вместо каждого x_i можно подставить функцию, соответствующую x_i в $\mathfrak{F}(x_1, \ldots, x_n)$. ...

Схема доказательства.

Поскольку RCF доп. **элиминацию кванторов**, то естественное вложение $\mathfrak{F}$ в $\mathfrak{F}^*$ будет элементарным. Стало быть,

$$\mathfrak{F} \Vdash \exists \vec{x} \left(p(\vec{x}) \cdot q(\vec{x}) < 0 \right).$$

Это противоречит неотрицательности f. $\square$

Appendix: Некоторые «негативные» результаты

Пусть σ — сигнатура упорядоченных колец (с единицей). Обозначим через DOR множество, состоящее из аксиом упоряд. коммутативных колец, а также универсальных замыканий след. σ-формул:

- $0 < 1$;
- $x \leqslant 0 \vee 1 \leqslant x$.

Теорема (о сильной неразрешимости DOR)

Для любого $\Gamma \subseteq \mathrm{Sent}_\sigma$,

$$\Gamma \cup \mathrm{DOR} \text{ непротиворечиво} \quad \Longrightarrow \quad [\Gamma] \text{ неразрешимо.}$$

В частности, теория уп. кольца целых чисел неразрешима; на самом деле, в этом случае наличие $<$ не принципиально.

Пусть ς — сигнатура колец. Для каждого простого числа p возьмём

$\mathcal{R}_p^{\mathsf{fin}}$:= класс всех конечных коммутативных колец характеристики p.

Теорема (о наследственной неразрешимости . . .)

Для любых простого числа p и класса ς-структур $\mathcal{K}$,

$$\mathcal{R}_p^{\mathsf{fin}} \subseteq \mathcal{K} \implies \mathsf{Th}(\mathcal{K}) \text{ неразрешима.}$$

Стало быть, теория конечных колец и теория колец неразрешимы.

Пусть $\mathfrak{N}$ — стандартная модель арифметики. Кроме того, обозначим кольцо целых чисел за $\mathfrak{Z}$, а поле рациональных чисел — за $\mathfrak{Q}$.

Утверждение

$\mathfrak{N}$ и $\mathfrak{Z}$ интерпретируемы друг в друге.

Доказательство.

То, что $\mathfrak{Z}$ интерпретируема в $\mathfrak{N}$, практически очевидно: всякое $p \in \mathbb{Z}$ можно отождествить с

$$\{(n, m) \in \mathbb{N}^2 \mid n - m = p\}.$$

Интерпретацию $\mathfrak{N}$ в $\mathfrak{Z}$ легко построить с помощью т. о четырёх квадратах: $\mathbb{N}$ можно определить в $\mathfrak{Z}$ посредством формулы

$$\mathrm{Nat}\,(x) \;:=\; \exists u_1\, \exists u_2\, \exists u_3\, \exists u_4\, \left(x = u_1^2 + u_2^2 + u_3^2 + u_4^2\right).$$

□

Отметим один важный результат:

Теорема (Дж. Робинсон)

$\mathbb{N}$ определимо в $\mathfrak{Q}$.

Отсюда легко получить

Утверждение

$\mathfrak{Z}$ и $\mathfrak{Q}$ интерпретируемы друг в друге. $\square$

Замечание

Отношение интерпретируемости транзитивно. Поэтому, в частности, $\mathfrak{Q}$ можно проинтерпретировать в $\mathfrak{N}$. С другой стороны, $\mathfrak{N}$ м. проинтерпретировать в $\mathfrak{Q}$ непосредственно с помощью теоремы выше.

Следствие

$\mathrm{Th}(\mathfrak{N})$, $\mathrm{Th}(\mathfrak{N})$ и $\mathrm{Th}(\mathfrak{Q})$ вычислимо эквивалентны друг другу. $\square$

Все эти теории будут сильно неразрешимы — это нетрудно получить из сильной неразрешимости DOR. Стало быть, верно

Утверждение

Теория полей и теория полей характеристики 0 неразрешимы.

Некоторая литература

- G. S. Boolos, J. P. Burgess, R. C. Jeffrey. *Computability and Logic*. 5th Edition. Cambridge University Press, 2007.
- P. J. Cohen. Decision procedures for real and p-adic fields. *Communications of Pure and Applied Mathematics* XXII, 131–151, 1969.
- D. Marker. *Model Theory: An Introduction*. Springer, 2002.