Об одном доказательстве теоремы Гильберта о нулях

В. Доценко

Теорема Гильберта о нулях (также известная как теорема Гильберта о корнях и Nullstellensatz[1]), доказанная в 1893 г. (см. [3]), играет фундаментальную роль в коммутативной алгебре и алгебраической геометрии. Она утверждает, что если каждый общий корень системы $\{f_1, \ldots, f_k\}$ многочленов над алгебраически замкнутым полем является корнем многочлена F, то существует такое m, что F^m представляется в виде суммы $\sum_{i=1}^{k} f_i g_i$, где g_i — некоторые многочлены.

Приводимое здесь доказательство этой теоремы для случая, когда основное поле есть поле комплексных чисел[2], является достоянием математического фольклора; хотя оно имеется в ряде русскоязычных источников (и, по-видимому, во множестве англоязычных), обычно о нём узнаю́т за непринуждённой беседой — или не узнаю́т вовсе. Сборник «Математическое Просвещение» идеально приспособлен для того, чтобы исправлять такие ситуации, делая красивые доказательства более доступными. Насколько мне известно[3], автором ключевого шага этого доказательства (лемма 2 в следующем далее тексте) является израильский математик А. Амицур [4]. Одно из первых упоминаний об этой идее на русском языке содержится в статье [1].

Я благодарен М. Финкельбергу за то, что он познакомил меня с этим доказательством, М. Вялому за предложение написать данный текст и моим знакомым, узнавшим это доказательство от меня, реакция которых убедила меня в полезности такого текста. Я также благодарен В. М. Тихомирову, предложившему снабдить вступление общедоступной[4] формули-

[1] М. Рид в книге «Алгебраическая геометрия для всех» пишет: «Советую вам придерживаться немецкого названия, если вы не желаете прослыть невеждами». Я всё же рискну предположить, что название «теорема Гильберта о нулях» несколько более привычно.

[2] Конечно, оно без изменений проходит для произвольного *несчётного* алгебраически замкнутого поля.

[3] Это и следующее утверждение не претендуют на окончательность; я буду признателен за любые уточнения.

[4] Гильберт говорил, что математический результат по-настоящему хорош, если его

ровкой теоремы и ссылкой на статью Гильберта, где эта теорема впервые была доказана в полной общности.

Итак, пусть $R = \mathbb{C}[x_1, \ldots, x_n]$ — кольцо многочленов от n переменных, $f_1 = f_1(x_1, \ldots, x_n)$, $f_2, \ldots, f_k \in R$, I — идеал, порождённый $f_1, \ldots, f_k$, т. е. множество сумм вида $f_1 g_1 + \cdots + f_k g_k$, где $g_1, \ldots, g_k \in R$; иногда для него удобно обозначение $(f_1, \ldots, f_k)$.

Теорема Гильберта о нулях. *Для любого многочлена $F \in R$, для которого $\bigl(\forall\ 1 \leqslant i \leqslant k\ f_i(y_1, \ldots, y_n) = 0\bigr) \Rightarrow (F(y_1, \ldots, y_n) = 0)$ существует такое m, что $F^m \in I$.*

Порядок изложения продиктован желанием доказывать в каждый момент то из ещё не доказанных утверждений, важность которого уже ясна (считая теорему о нулях утверждением, про которое это понятно a priori). Оказывается, теорему о нулях можно вывести из её частного случая. Эта часть доказательства является достаточно общепринятой, см. например, [2, с. 468–469]. (После выхода книги [2] многие стали использовать для приводимого рассуждения название «трюк Рабиновича».)

Лемма 1 (Случай $F = 1$). *Если в условиях теоремы $f_1, \ldots, f_k$ не имеют общих нулей, то $I = R$.*

Особенностью предлагаемого доказательства является как раз способ доказательства этой леммы. Для этого нам потребуется

Лемма 2. *Пусть поле K является не более чем счётномерным пространством над $\mathbb{C}$. Тогда $K \cong \mathbb{C}$.*

Вывод теоремы из леммы 1. Рассмотрим «бóльшее» кольцо $R' = \mathbb{C}[x_1, \ldots, x_n, z]$. В этом кольце лежат многочлены $f_1, \ldots, f_k$ (многочлены от $x_1, \ldots, x_n$ являются и многочленами от $x_1, \ldots, x_n, z$) и $1 - zF$. В условиях теоремы эти многочлены не имеют общих нулей, поэтому существуют многочлены $g_1 = g_1(x_1, \ldots, x_n, z), g_2, \ldots, g_{n+1}$ такие, что

$$1 = f_1 g_1 + \cdots + f_n g_n + (1 - zF) g_{n+1}.$$

Подстановка в это тождество $z = \dfrac{1}{F}$ и приведение к общему знаменателю (который, очевидно, есть степень F) дают то, что нужно.

Вывод леммы 1 *из леммы* 2. Предположим противное. Пусть $I \neq R$. Ясно, что существует максимальный (по включению) идеал $J \neq R$, содержащий I (это можно вывести из аксиомы выбора или же использовать принцип обрыва возрастающих цепочек идеалов, т. е. *нётеровость* кольца R — см. [2]). Будем теперь иметь дело с J.

суть можно разъяснить человеку «с улицы». Это утверждение достаточно спорно, но теорема о нулях явно подходит под этот критерий.

Факторкольцо R/J есть поле[5)], при этом это поле является (не более чем счётномерным — ведь таково кольцо многочленов!) векторным пространством над $\mathbb{C}$ (очевидно). Из леммы 2 следует, что $R/J \cong \mathbb{C}$. Теперь уже легко понять, как может быть устроен идеал J. Действительно, пусть при проекции $R \to R/J \cong \mathbb{C}$ образующие $x_1, \ldots, x_n$ кольца R переходят в (числа) $a_1, \ldots, a_n$ соответственно. Тогда многочлены $x_1 - a_1, \ldots, x_n - a_n$ переходят в нуль и поэтому лежат в идеале J. Но факторкольцо $R/(x_1 - a_1, \ldots, x_n - a_n)$ уже есть $\mathbb{C}$ (причину этого мы только что обсудили: образующие кольца R после факторизации порождают $\mathbb{C}$), значит, $J = (x_1 - a_1, \ldots, x_n - a_n)$. Поэтому все многочлены из J (а значит, из любого идеала, содержащегося в J) имеют общий нуль: точку $(a_1, \ldots, a_n)$. Противоречие.

Доказательство леммы 2. Ясно, что $K \supset \mathbb{C}$. Предположим противное: пусть $z \in K \setminus \mathbb{C}$. Тогда множество $\{\frac{1}{z-\alpha} \mid \alpha \in \mathbb{C}\}$ имеет мощность континуум (так как оно равномощно $\mathbb{C}$), поэтому это множество не может состоять из линейно независимых над $\mathbb{C}$ элементов. Значит, существуют комплексные числа $\alpha_1, \ldots, \alpha_m, c_1, \ldots, c_m$ такие, что

$$\frac{c_1}{z-\alpha_1} + \cdots + \frac{c_m}{z-\alpha_m} = 0.$$

Осталось привести эти дроби к общему знаменателю, чтобы получить (очевидно, нетривиальное) уравнение на z с комплексными коэффициентами. Поскольку поле $\mathbb{C}$ алгебраически замкнуто, все корни этого уравнения — комплексные числа. Противоречие.

Список литературы

[1] Бернштейн И. Н., Зелевинский А. В. *Представления группы $GL(n, F)$, где F — локальное неархимедово поле* // УМН, 1976. Т. 31. Вып. 3. С. 5–70.

[2] Ван дер Варден Б. Л. *Алгебра.* М.: Наука, 1976.

[3] Гильберт Д. *О полной системе инвариантов* // Гильберт Д. *Избранные труды.* Т. 1. М.: Факториал, 1998. С. 67–116.

[4] Amitsur A. S. *Algebras over infinite fields* // Proc. AMS, 1956. Vol. 7. P. 35–48.

[5)] Можно прочитать доказательство в [2], а можно продумать такую идею: наличие ненулевых идеалов в R/J (не совпадающих со всем кольцом R/J) противоречило бы максимальности J, а если таких (как говорят, «нетривиальных») идеалов нет, то R/J — поле, поскольку любой ненулевой элемент имеет обратный: ведь в идеале, порождённом этим элементом, есть 1.