Том 2, Выпуск 1
Стр. 3–15 (2024)

УДК 512.714
MSC 14A05

Теорема Гильберта о нулях

Б.М. Беккер, С.В. Востоков, Р.П. Востокова

Аннотация. Теорема о нулях, доказанная Гильбертом в 1890 году, является одним из основополагающих результатов современной алгебраической геометрии. В нашей работе мы приводим разнообразные формулировки и доказательства этой теоремы, каждая из которых используется в алгебраической геометрии. Все понятия и факты, выходящие за рамки стандартного курса алгебры, объясняются в статье.

Ключевые слова: теорема о нулях, расширение поля, степень трансцендентности, результант, точка поля.

DOI: 10.26907/2949-3919.2024.1.3-15

1. Формулировки теоремы. Обсуждение частных случаев

Пусть K – алгебраически замкнутое поле произвольной характеристики (читатель, не знакомый с соответствующими понятиями, может без значительного ущерба для понимания считать, что K – поле комплексных чисел или поле всех алгебраических чисел, т. е. корней алгебраических уравнений с рациональными коэффициентами и старшим коэффициентом 1). Пусть $K[x_1, \ldots, x_n]$ – кольцо многочленов от переменных $x_1, \ldots, x_n$ с коэффициентами из поля K. Если $n = 1$, то мы имеем дело с обычными многочленами от одной переменной (в этом случае в обозначении переменной индекс будем опускать). Теорема Гильберта дает необходимое и достаточное условие несовместности системы алгебраических уравнений

$$\begin{aligned} &f_1(x_1, \ldots, x_n) = 0, \\ &\cdots \\ &f_k(x_1, \ldots, x_n) = 0. \end{aligned} \tag{1}$$

Теорема 1 (теорема Гильберта о нулях)**.** *Система* (1) *не имеет решений в* K *в том и только том случае, если существуют многочлены* $g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ *такие, что*

$$f_1(x_1, \ldots, x_n)g_1(x_1, \ldots, x_n) + \cdots + f_k(x_1, \ldots, x_n)g_k(x_1, \ldots, x_n) = 1. \tag{2}$$

Поступила: 01.08.2023. Принята: 16.01.2024. Опубликована: 11.04.2024.

В одну сторону утверждение теоремы очевидно: если равенство (1) имеет место для некоторых $g_1(x_1,\dots,x_n),\dots,g_k(x_1,\dots,x_n)\in K[x_1,\dots,x_n]$, то подстановка любого решения $(c_1,\dots,c_n)$ системы (1) в левую часть равенства (2) приводит к противоречию. Таким образом, нетривиальной частью теоремы о нулях является обратное утверждение: если система (1) не имеет решений в K, то некоторая линейная комбинация левых частей системы с многочленными коэффициентами равна единице. Заметим, что если существуют многочлены $g_i(x_1,\dots,x_n)$, для которых справедливо равенство (2), то существуют также и многочлены $g_i(x_1,\dots,x_n)$, для которых справедливо равенство

$$f_1(x_1,\dots,x_n)g_1(x_1,\dots,x_n)+\dots+f_k(x_1,\dots,x_n)g_k(x_1,\dots,x_n)=g(x_1,\dots,x_n),$$

где $g(x_1,\dots,x_n)$ – произвольный наперед заданный многочлен с коэффициентами из K. Действительно, достаточно многочлены $g_i(x_1,\dots,x_n)$, для которых выполняется равенство (2), умножить на $g(x_1,\dots,x_n)$.

Многочлены вида

$$f_1(x_1,\dots,x_n)g_1(x_1,\dots,x_n)+\dots+f_k(x_1,\dots,x_n)g_k(x_1,\dots,x_n),$$

где $f_i(x_1,\dots,x_n)$ – фиксированные многочлены, а многочлены $g_i(x_1,\dots,x_n)$ пробегают кольцо $K[x_1,\dots,x_n]$, образуют идеал кольца $K[x_1,\dots,x_n]$, порожденный многочленами $f_i(x_1,\dots,x_n)$. Таким образом, теорема о нулях утверждает, что система уравнений не имеет решений в том и только том случае, если идеал, порожденный левыми частями уравнений, совпадает со всем кольцом многочленов (т. е. является единичным идеалом). Опять же нетривиальной частью теоремы является утверждение о том, что если система (1) не имеет решений, то идеал, порожденный левыми частями уравнений, является единичным, или, что то же самое, если идеал, порожденный левыми частями уравнений системы, не совпадает со всем кольцом многочленов, то система (1) имеет решение в K.

1. Рассмотрим простейший частный случай теоремы: $n=1$, $m=1$. В этом случае система (1) сводится к одному уравнению $f(x)=0$. Критерий разрешимости такого уравнения утверждает, что уравнение $f(x)=0$, где $f(x)$ – ненулевой многочлен, имеет корень в том и только том случае, если степень многочлена $f(x)$ больше нуля. Другими словами, уравнение $f(x)=0$ не имеет решений в K в том и только том случае, если степень многочлена $f(x)$ равна нулю. Последнее условие очевидно равносильно существованию многочлена $g(x)$ такого, что

$$f(x)g(x)=1.$$

Таким образом, в случае $n=1$, $k=1$ теорема Гильберта о нулях равносильна утверждению об алгебраической замкнутости поля K.

2. Пусть $n=1$, а k произвольно. В этом случае система (1) принимает вид

$$f_1(x)=0,\dots,f_k(x)=0. \tag{3}$$

Всякое решение этой системы в K является корнем уравнения $d(x) = 0$, где $d(x)$ – наибольший общий делитель многочленов $f_1(x), \dots, f_k(x)$, и наоборот, всякий корень уравнения $d(x) = 0$ является решением системы (3). Следовательно, система (3) равносильна уравнению $d(x) = 0$, которое в силу алгебраической замкнутости поля K не имеет решений в том и только том случае, если $d(x)$ – ненулевая константа. По теореме о линейном представлении наибольшего общего делителя в кольце $K[x]$ получаем, что система (3) не имеет решений в том и только том случае, если существуют

$$g_1(x), \dots, g_k(x) \in K[x]$$

такие, что

$$f_1(x)g_1(x) + \dots + f_k(x)g_k(x) = 1.$$

Мы видим, что в рассматриваемом случае теорема о нулях является тривиальным следствием алгебраической замкнутости поля K (см. п. 1) и теоремы о линейном представлении наибольшего общего делителя, справедливой в произвольном кольце многочленов от одной переменной. Для многочленов от нескольких переменных линейного представления наибольшего общего делителя нет, и теорему о нулях можно рассматривать как обобщение этого линейного представления: условие взаимной простоты многочленов нужно заменить на отсутствие у них общих корней.

3. Пусть n и k любые, а многочлены $f_i(x_1, \dots, x_n)$ имеют степень 1:

$$f_i(x_1, \dots, x_n) = a_{i1}x_1 + \dots + a_{in}x_n - b_i.$$

В этом случае система (1) имеет вид

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n &= b_2, \\ &\dots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n &= b_n. \end{aligned} \tag{4}$$

Применяя к уравнениям этой системы элементарные преобразования, мы приведем ее к ступенчатому виду. Заметим, что каждое из уравнений полученной ступенчатой системы является линейной комбинацией уравнений исходной системы, т. е. имеет вид

$$c_1(a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n) + \dots + c_k(a_{k1}x_1 + a_{12}x_2 + \dots + a_{kn}x_n) = c_1b_1 + \dots + c_kb_k$$

при некоторых $c_1, \dots, c_k \in K$. Система (4) не имеет решений в том и только том случае, если последнее ненулевое уравнение полученной ступенчатой системы имеет вид

$$0 \cdot x_1 + \dots + 0 \cdot x_n = b,$$

где $b \neq 0$. В силу сказанного выше, это имеет место в том и только том случае, если найдутся такие константы $c_1, \ldots, c_k$, что

$$c_1(a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n) + \cdots + c_k(a_{k1}x_1 + a_{12}x_2 + \cdots + a_{kn}x_n) = 0$$

и

$$c_1b_1 + \cdots + c_kb_k = b \neq 0.$$

Отсюда

$$c_1(a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n - b_1) + \cdots + c_k(a_{k1}x_1 + a_{12}x_2 + \cdots + a_{kn}x_n - b_k) = -b \neq 0,$$
$$\frac{c_1}{-b}(a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n - b_1) + \cdots + \frac{c_k}{-b}(a_{k1}x_1 + a_{12}x_2 + \cdots + a_{kn}x_n - b_k) = 1.$$

Взяв в качестве многочленов $g_i(x_1, \ldots, x_n)$ константы $\frac{c_i}{-b}$, мы получаем утверждение теоремы о нулях.

2. Сильная теорема о нулях. Частные случаи. Примеры

Из теоремы о нулях, сформулированной в предыдущем разделе (и часто называемой слабой теоремой о нулях), вытекает следующее утверждение.

Теорема 2 (сильная теорема о нулях)**.** *Пусть $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ – многочлен, обращающийся в нуль на каждом решении системы (1). Тогда существует такое натуральное m и такие многочлены $g_i(x_1, \ldots, x_n)$, $i = 1, \ldots, k$, что имеет место равенство*

$$f^m(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n)g_1(x_1, \ldots, x_n) + \cdots + f_k(x_1, \ldots, x_n)g_k(x_1, \ldots, x_n).$$

Доказательство. Заметим, что из сильной теоремы о нулях вытекает слабая. Действительно, пусть система (1) не имеет решений. Тогда условие сильной теоремы о нулях выполняется: взяв в качестве многочлена f константу 1, мы видим, что f обращается в нуль на множестве решений этой системы (на пустом множестве). Следовательно, единица представляется в виде линейной комбинации многочленов f_i, что и утверждается в слабой теореме. Наша цель – доказать, что из слабой теоремы вытекает сильная. Приводимое ниже рассуждение носит название трюка Рабиновича.

Итак, пусть

$$f(x_1, \ldots, x_n), f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n)$$

– многочлены, участвующие в формулировке сильной теоремы о нулях. Рассмотрим кольцо $K[x_1, \ldots, x_n]$ как подкольцо кольца $K[x_1, \ldots, x_n, x_{n+1}]$ многочленов от $(n+1)$-й переменной и следующую систему уравнений от неизвестных $x_1, \ldots, x_n, x_{n+1}$:

$$\begin{aligned}
&f_1(x_1,\dots,x_n)=0,\\
&\dots\\
&f_k(x_1,\dots,x_n)=0,\\
&1-x_{n+1}f(x_1,\dots,x_n)=0.
\end{aligned}\tag{5}$$

По условию многочлен $f(x_1,\dots,x_n)$ обращается в нуль на каждом решении системы (1). Поэтому система (5) решений не имеет. По слабой теореме о нулях (примененной к многочленам от $(n+1)$-й переменной) получаем, что существуют многочлены

$$h_1(x_1,\dots x_n,x_{n+1}),\dots,h_k(x_1,\dots x_n,x_{n+1}),h_{k+1}(x_1,\dots x_n,x_{n+1})$$

такие, что

$$\begin{aligned}
&f_1(x_1,\dots,x_n)h_1(x_1,\dots x_n,x_{n+1})+\dots+f_k(x_1,\dots,x_n)h_k(x_1,\dots x_n,x_{n+1})\\
&+(1-x_{n+1}f(x_1,\dots,x_n))h_{k+1}(x_1,\dots x_n,x_{n+1})=1.
\end{aligned}\tag{6}$$

Подставив $x_{n+1}=1/f(x_1,\dots,x_n)$ в равенство (6), получим

$$f_1(x_1,\dots,x_n)h_1\left(x_1,\dots x_n,\frac{1}{f(x_1,\dots,x_n)}\right)+\dots\\
+f_k(x_1,\dots,x_n)h_k\left(x_1,\dots x_n,\frac{1}{f(x_1,\dots,x_n)}\right)=1.\tag{7}$$

Умножив обе части равенства (7) на достаточную степень многочлена $f(x_1,\dots,x_n)$, чтобы избавиться от знаменателей, мы получим

$$f^m(x_1,\dots,x_n)=f_1(x_1,\dots,x_n)g_1(x_1,\dots,x_n)+\dots+f_k(x_1,\dots,x_n)g_k(x_1,\dots,x_n)$$

для некоторого натурального m. □

Рассмотрим несколько частных случаев.

1. Пусть $n=1$, $k=1$, $f_1(x)=x-c$, где $c\in K$. Сильная теорема о нулях утверждает, что если многочлен $f(x)$ обращается в нуль в точке c, то некоторая степень многочлена $f(x)$ делится на $x-c$; но поскольку $x-c$ неприводим, то и сам многочлен $f(x)$ делится на $x-c$. Это утверждение теоремы Безу.

2. Пусть $n=1$, $k=1$, $f_1(x)=a(x-c_1)^{k_1}\cdots(x-c_s)^{k_s}$. Сильная теорема о нулях утверждает, что если некоторый многочлен обращается в нуль в $c_1,\dots,c_s$, то некоторая его степень делится на $f_1(x)$. Это конечно очевидно и без теоремы о нулях: по условию $c_1,\dots,c_s$ являются корнями многочлена $f(x)$. Значит, этот многочлен делится на $x-c_1,\dots,x-c_s$. Пусть m – наибольшая из степеней $k_1,\dots,k_s$. Тогда $f(x)^m$ делится на $f_1(x)$.

3. Пусть $f(x,y),g(x,y)$ – многочлены от переменных x,y с коэффициентами из K. Теорема о нулях утверждает, что если многочлен $f(x,y)$ обращается в нуль во всех нулях многочлена $g(x,y)$, то некоторая степень многочлена $f(x,y)$ делится на $g(x,y)$. В частно-

сти, если многочлен $g(x,y)$ неприводим, то $f(x,y)$ делится на $g(x,y)$. Отсюда вытекает, что уравнение плоской неприводимой аффинной алгебраической кривой (которая определяется как множество всех решений уравнения вида $f(x,y)=0$, где $f(x,y)$ – неприводимый многочлен) определено однозначно с точностью до постоянного множителя. Это конечно легко доказать и без использования теоремы о нулях (см., например, [1]). Аналогичный факт справедлив и для многочленов $f(x_1,\ldots,x_n), g(x_1,\ldots,x_n)$ от произвольного числа переменных. Множество решений уравнения $f(x_1,\ldots,x_n)=0$ в K^n называется аффинной гиперповерхностью. Как же связаны многочлены $f(x_1,\ldots,x_n)$ и $g(x_1,\ldots,x_n)$, если известно, что они задают одну и ту же гиперповерхность? Теорема о нулях дает ответ на этот вопрос: некоторая степень каждого из этих многочленов делится на другой. В случае неприводимых многочленов это означает, что они отличаются на постоянный множитель.

3. Обсуждение различных путей доказательства теоремы о нулях

Напомним, что в предыдущем разделе мы вывели из слабой теоремы о нулях сильную. Осталось доказать слабую теорему о нулях. Существует большое количество доказательств этой теоремы (см., например, [2–5]). В некоторых из них используется понятие результанта и индукцией по числу переменных показывается, что порожденный левыми частями системы идеал неединичный. Одно такое доказательство мы приведем в разделе 6. Другие доказательства основаны на конструкции, аналогичной конструкции присоединения к произвольному полю K корня произвольного неприводимого многочлена $f(x)$ одной переменной, а именно рассмотрения факторкольца кольца $K[x]$ по идеалу, порожденному многочленом $f(x)$. Так как многочлен $f(x)$ неприводим, то идеал $(f(x))$, порожденный многочленом $f(x)$, является простым, а значит, максимальным (поскольку в кольце многочленов от одной переменной любой ненулевой простой идеал является максимальным). Следовательно, факторкольцо $L=K[x]/(f(x))$ является полем. Отождествляя элементы поля K с их образами в L, мы можем считать поле L расширением поля K. Образ переменной x в L и является корнем многочлена $f(x)$ в поле L (именно такой конструкцией получается поле комплексных чисел из поля вещественных). Заметим, что если поле K алгебраически замкнуто, то неприводимые многочлены над K – это в точности многочлены степени 1 и при указанном выше отождествлении $L=K$. Попытаемся провести аналогичные рассуждения в случае многочленов от нескольких переменных. Рассмотрим систему уравнений (1). Пусть I – идеал кольца $K[x_1,\ldots,x_n]$, порожденный левыми частями уравнений этой системы, т. е. множество всех многочленов вида

$$f_1(x_1,\ldots,x_n)g_1(x_1,\ldots,x_n)+\cdots+f_k(x_1,\ldots,x_n)g_k(x_1,\ldots,x_n),$$

где $g_i(x_1,\ldots,x_n)$ пробегают кольцо $K[x_1,\ldots,x_n]$. Предположим, что этот идеал неединичный. Тогда он содержится в некотором максимальном идеале M кольца $K[x_1,\ldots,x_n]$. Факторкольцо $L=K[x_1,\ldots,x_n]/M$ является полем. Отождествляя элементы поля K с их образами в L, мы можем считать поле L расширением поля K. Пусть $c_1,\ldots,c_n$ – образы переменных $x_1, \ldots, x_n$ в поле L. Тогда набор $(c_1, \ldots, c_n)$ является решением системы (1) в поле L. Но нам нужно было найти решение системы не в каком-то расширении поля K, а в самом K. Если бы L было алгебраическим расширением K, то в силу алгебраической замкнутости K выполнялось бы равенство $L = K$ и найденное решение лежало бы в K, что доказывало бы слабую теорему о нулях. Оказывается, L действительно алгебраично над K, и разные доказательства теоремы о нулях в этом направлении сводятся к доказательству этого факта.

Наконец, можно напрямую доказать следующее утверждение.

Если система (1) имеет решение $(c_1, \ldots, c_n)$ в некотором расширении F поля K, то она имеет решение и в самом поле K, не доказывая равенство $L = K$. А именно, если $(c_1, \ldots, c_n)$ алгебраичны над K , то в силу алгебраической замкнутости K они содержатся в K, и доказывать нечего. Если же они не являются алгебраическими над K, т. е. грубо говоря, содержат переменные, то идея состоит в том, чтобы подставить в место этих переменных некоторые элементы из K и получить в результате решение в K. Доказательство, основанное на этой идее, изложено, например, в [3] и приведено в разделе 7.

4. Доказательство слабой теоремы о нулях в случае алгебраически замкнутого поля бесконечной степени трансцендентности над простым подполем

Пусть K – алгебраически замкнутое поле и K_0 – его простое подполе. Пусть F – подполе поля K, порожденное над K_0 коэффициентами левых частей уравнений системы (1). Поле F является конечно порожденным расширением поля K_0. Предположим, что идеал I кольца $K[x_0, \ldots, x_n]$, порожденный многочленами стоящими в левых частях системы (1), неединичный. Тогда $I \cap F[x_1, \ldots, x_n]$ является неединичным идеалом кольца $F[x_1, \ldots, x_n]$ и, значит, лежит в некотором максимальном идеале M этого кольца.

Факторкольцо $L = F[x_1, \ldots, x_n]/M$ является конечно порожденным расширением поля F конечной степени трансцендентности. Степень трансцендентности K над F бесконечна, так как по условию степень трансцендентности K над K_0 бесконечна, а степень трансцендентности F над K_0 конечна. Следовательно, существует вложение ϕ поля L в K, тождественное на F. Пусть $\bar{x}_1, \ldots, \bar{x}_n$ – образы переменных $x_1, \ldots, x_n$ в L. Очевидно, $(\bar{x}_1, \ldots, \bar{x}_n)$ является корнем всех многочленов из M, а значит, и решением системы (1) в поле L. Тогда $(\phi(\bar{x}_1), \ldots, \phi(\bar{x}_n))$ является решением системы в K.

5. Доказательство слабой теоремы о нулях в случае несчетного алгебраически замкнутого поля

Пусть K – произвольное несчетное поле произвольной характеристики. Точно так же, как и раньше, рассмотрим максимальный идеал M кольца многочленов $K[x_1, \ldots, x_n]$, содержащий многочлены, стоящие в левых частях системы, и соответствующее поле

$L = K[x_1, \dots, x_n]/M$. Степень расширения L/K не более чем счетна. Как отмечалось в разделе 3, для доказательства равенства $L = K$ достаточно показать, что расширение алгебраично. Доказательство проведем от противного. Пусть $t \in L$ трансцендентен над K. Тогда подполе поля L, порожденное над K элементом t, изоморфно полю рациональных функций $K(t)$. Рассмотрим следующий несчетный набор элементов поля $K(t)$:

$$\left\{ \frac{1}{t-c}, \text{ где } c \in K \right\}.$$

Элементы этого набора линейно независимы над K. Действительно, пусть для какого-нибудь конечного набора различных элементов $c_1, \dots, c_n$ при некоторых $\lambda_1, \dots, \lambda_n \in K$ справедливо равенство

$$\lambda_1 \frac{1}{t-c_1} + \dots + \lambda_n \frac{1}{t-c_n} = 0.$$

Освобождаясь от знаменателей и подставляя в полученное равенство последовательно $t = c_1, \dots, c_n$, мы имеем $\lambda_1, \dots, \lambda_n = 0$. Таким образом, мы получили противоречие с тем, что степень L/K не более чем счетна.

6. Доказательство для произвольного алгебраически замкнутого поля K с применением результанта и индукции по числу переменных

Вначале докажем простое вспомогательное утверждение.

Лемма 3. *Пусть $f \in K[X_1, \dots, X_n]$, $n \geq 2$ – непостоянный многочлен полной степени d. Тогда существуют такие $\lambda_1, \dots, \lambda_{n-1} \in K$, что коэффициент при x_n^d в многочлене*

$$f(x_1 + \lambda_1 x_n, \dots, x_{n-1} + \lambda_{n-1} x_n, x_n)$$

отличен от нуля.

Доказательство. Пусть f_d – старшая однородная компонента многочлена f. Коэффициент при x^n в многочлене $f(x_1 + \lambda_1 x_n, \dots, x_{n-1} + \lambda_{n-1} x_n, x_n)$ равен $f_d(\lambda_1, \dots, \lambda_{n-1}, 1)$. Поле K бесконечно, так как оно алгебраически замкнуто. Следовательно, существуют такие $\lambda_1, \dots, \lambda_{n-1} \in F$, что $f_d(\lambda_1, \dots, \lambda_{n-1}, 1) \neq 0$. □

Перейдем к доказательству самой теоремы 1. Пусть I – идеал, порожденный левыми частями системы (1), и пусть $I \neq K[x_1, \dots, x_n]$. Нам нужно доказать существование решения системы (1) в K. Доказательство теоремы проведем индукцией по n. Для $n = 1$ утверждение очевидно. Пусть $n \geq 2$. Заметим, что замена переменных, указанная в лемме, обратима. Рассмотрим произвольный непостоянный многочлен из I; пусть d – его степень. Воспользуемся леммой и рассмотрим замену переменных, переводящую этот полином в полином с ненулевым коэффициентом при x_n^d. Произведем во всех полиномах из I такую замену переменных. Мы получим новый идеал кольца многочленов. Если мы докажем, что у всех многочленов из этого идеала есть общий корень, то, применяя к этому корню обратную замену переменных, мы найдем общий корень для многочленов исходного идеала. Поэтому можно считать с самого начала, что идеал I содержит какой-нибудь многочлен g с ненулевым коэффициентом при x_n^d, где d – степень g. Более того, можно считать, что идеал I содержит какой-нибудь многочлен g с коэффициентом при x_n^d, равным единице.

Рассмотрим идеал I', состоящий из всех полиномов в I, не содержащих переменной x_n. Так как $1 \notin I$, то идеал I' неединичный. В силу индукционного предположения существуют такие $a_1, \dots, a_{n-1}$, что $f(a_1, \dots, a_{n-1}) = 0$ для всех $f \in I'$.

Далее рассмотрим идеал J в $K[x_n]$, состоящий из многочленов

$$f(a_1, \dots, a_{n-1}, x_n),$$

где $f \in I$. Докажем, что $J \neq K[x_n]$. Будем рассуждать от противного. Пусть $1 \in J$. Тогда существует такой многочлен f в I, что

$$f(a_1, \dots, a_{n-1}, x_n) = 1.$$

Представим f в виде $f = f_0 + f_1 x_n + \dots + f_k x_n^k$, где $f_i \in K[x_1, \dots, x_{n-1}]$. Очевидно, что

$$f_0(a_1, \dots, a_{n-1}) = 1, \quad f(a_1, \dots, a_{n-1}) = \dots = f(a_1, \dots, a_{n-1}) = 0.$$

С другой стороны,

$$g = g_0 + g_1 x_n + \dots + g_{d-1} x_n^{d-1} + x_n^d,$$

где $g_i \in K[x_1, \dots, x_{n-1}]$. Рассмотрим результант R полиномов f и g относительно переменной x_n. Известно, что R является линейной комбинацией полиномов f и g с коэффициентами в $K[x_1, \dots, x_{n-1}]$. Поэтому $R \in I$. Так как $R \in K[x_1, \dots, x_{n-1}]$, то $R \in I'$. Но прямое вычисление показывает, что $R(a_1, \dots, a_{n-1}) = 1$. Это противоречит тому, что все многочлены из I' обращаются в нуль в точке $(a_1, \dots, a_{n-1})$. Таким образом, идеал J неединичный. Значит, $J = (h(x_n))$, где h – многочлен, не равный ненулевой константе. Пусть a_n – его корень в K. Тогда $f(a_1, \dots, a_{n-1}, a_n) = 0$ для всех $f \in I$. В частности, $(a_1, \dots, a_{n-1}, a_n)$ – решение системы (1).

7. Еще одно доказательство слабой теоремы о нулях

Напомним определение точки поля. Пусть Ω – произвольное поле. Присоединив к Ω символ ∞, в полученном множестве $\Omega \cup \infty$ определим следующие действия (везде $a \in \Omega$):

$$\begin{aligned} &a \pm \infty = \infty, \quad a \cdot \infty = \infty, \quad \text{если } a \neq 0;\\ &\infty \cdot \infty = \infty, \quad \frac{1}{\infty} = 0, \quad \frac{1}{0} = \infty. \end{aligned}$$

Выражения $\infty \pm \infty$, $0 \cdot \infty$, $0/0$, ∞/∞ не определены. Ω-значной точкой поля K называется отображение $\varphi\colon K \to \Omega \cup \{\infty\}$; здесь $\varphi(1) = 1$ и равенства $\varphi(a+b) = \varphi(a) + \varphi(b)$, $\varphi(ab) = \varphi(a)\varphi(b)$ выполняются при любых $a, b \in K$, при которых правые части этих равенств определены. Фундаментальная, но просто доказываемая теорема о продолжении утверждает следующее (см. например, [3]).

Теорема 4 (о продолжении гомоморфизмов)**.** *Пусть K – поле, содержащее кольцо R, и φ – гомоморфизм кольца R в некоторое алгебраически замкнутое поле Ω, причем $\varphi(1) = 1$. Тогда φ можно продолжить до Ω-значной точки поля K.*

Определение 5. Пусть L/K – произвольное расширение полей. Пусть

$$x = (x_1, \dots, x_n), x' = (x'_1, \dots, x'_n) \in L^n.$$

Будем говорить, что x' является специализацией точки x над K, если всякий многочлен с коэффициентами из K, обращающийся в нуль в точке x, обращается в нуль и в точке x'.

Пример 6. $L = \mathbb{R}$, $K = \mathbb{Q}$, $x = (\pi, \pi^2) \in \mathbb{R}$, $x' = (1, 1) \in \mathbb{R}$. Очевидно, x' является специализацией точки x над $\mathbb{Q}$.

Следствие 7. *Пусть K – алгебраически замкнутое поле, $L = K(x_1, \dots, x_n)$ – расширение поля K. Пусть $x \in L^n$. Тогда существует точка $x' \in K$, являющаяся специализацией точки x над K.*

Доказательство. Выберем базис трансцендентности поля L над K. Его можно выбрать из элементов $x_1, \dots, x_n$. Можно считать, что этот базис образуют первые r элементов $x_1, \dots, x_n$. Тогда для каждого x_i, где $i > r$, справедливо равенство вида

$$a_m(x_1, \dots, x_r)x_i^m + a_{m-1}(x_1, \dots, x_r)x_i^{m-1} + \dots + a_0(x_1, \dots, x_r) = 0, \tag{8}$$

где $a_i(x_1, \dots, x_r) \in K[x_1, \dots, x_r]$ и $a_m(x_1, \dots, x_r)$ – ненулевой многочлен. Пусть $x'_1, \dots, x'_r \in K$ такие, что $a_m(x'_1, \dots, x'_r) \neq 0$. Рассмотрим гомоморфизм φ_0 кольца многочленов $K[x_1, \dots, x_r]$ в K, переводящий каждый элемент x_i в x'_i и оставляющий на месте все элементы поля K. Используя теорему о продолжении гомоморфизмов, продолжим его до K-значной точки φ поля $K(x_1, \dots, x_n)$. Для любого i значение $\varphi(x_i)$ отлично от ∞. Действительно, для $i \leq r$ это ясно по построению гомоморфизма φ_0. Если для некоторого $i > r$ выполняется равенство $\varphi(x_i) = \infty$, то, разделив обе части равенства (8) на x_i^m, мы получим

$$a_m(x_1, \dots, x_r) + a_{m-1}(x_1, \dots, x_r)\frac{1}{x_i} + \dots + a_0(x_1, \dots, x_r)\frac{1}{x_i^m} = 0. \tag{9}$$

Теперь, применяя φ к обеим частям равенства (9), имеем

$$a_m(x'_1, \dots, x'_r) = 0.$$

Получили противоречие. Пусть $x'_i = \varphi(x_i)$ для $i > r$. Тогда точка $x' = (x'_1, \ldots, x'_n)$ является специализацией над K точки x. □

Доказательство слабой теоремы о нулях. Мы уже говорили о том, что легко найти решение $x = (x_1, \ldots, x_n)$ системы (1) в некотором конечно порожденном расширении исходного алгебраически замкнутого поля K (см. раздел 3). Тогда точка x', построенная в доказанном следствии 7, будет решением системы (1) в поле K. □

Список литературы

[1] И.Р. Шафаревич, *Основы алгебраической геометрии*, 3-е изд., МЦНМО, 2007.

[2] E. Arrondo, *Another elementary proof of the Nullstellensatzz*, Amer. Math. Monthly **113** (2), 169–171 (2006).
DOI: https://doi.org/10.1080/00029890.2006.11920292

[3] S. Lang, *Introduction to algebraic geometry*, Interscience Publ., N.Y., 1958.

[4] Д. Мамфорд, *Алгебраическая геометрия* I. *Комплексные проективные многообразия*, Мир, М., 1979.

[5] D. Perrin, *Algebraic geometry*, Springer-Verlag, London, 2008.

Борис Меерович Беккер
Санкт-Петербургский государственный университет,
Университетская набережная, д. 7–9, г. Санкт-Петербург, 199034, Россия,
e-mail: bekker.boris@gmail.com

Сергей Владимирович Востоков
Санкт-Петербургский государственный университет,
Университетская набережная, д. 7–9, г. Санкт-Петербург, 199034, Россия,
e-mail: s.vostokov@spbu.ru

Регина Петровна Востокова
Санкт-Петербургский государственный университет,
Университетская набережная, д. 7–9, г. Санкт-Петербург, 199034, Россия,
e-mail: rvostokova@yandex.ru

Volume 2, Issue 1 UDC 512.714
pp. 3–15 (2024) MSC 14A05

Hilbert's Nullstellensatz

B.M. Bekker, S.V. Vostokov, R.P. Vostokova

Abstract. Hilbert's Nullstellensatz proved by him in 1890 is one of the basic results in modern algebraic geometry. We give various statements and proofs of this theorem all of which are used in algebraic geometry. All notions and facts outside the basic algebra course are explained in the paper.

Keywords: theorem on zeros, field extension, transcendence degree, resultant, place of a field.

DOI: 10.26907/2949-3919.2024.1.3-15

References

[1] I.R. Shafarevich, *Basic Algebraic Geometry*, 2 volumes, Springer-Verlag, Heidenberg, 2013.

[2] E. Arrondo, *Another elementary proof of the Nullstellensatz*, Amer. Math. Monthly **113** (2), 169–171 (2006).
DOI: https://doi.org/10.1080/00029890.2006.11920292

[3] S. Lang, *Introduction to algebraic geometry*, Interscience Publ., N.Y., 1958.

[4] D. Mumford, *Algebraic Geometry* I*: Complex Projective Varieties*, Springer-Verlag, Berlin, 1976.

[5] D. Perrin, *Algebraic geometry*, Springer-Verlag, London, 2008.

Boris Meerovich Bekker
St.Petersburg State University,
7–9 Universitetskaya Embankment, St. Petersburg 199034, Russia,
e-mail: bekker.boris@gmail.com

Sergei Vladimirovich Vostokov
St.Petersburg State University,
7–9 Universitetskaya Embankment, St. Petersburg 199034, Russia,
e-mail: s.vostokov@spbu.ru

Received: 01 August 2023. Accepted: 16 January 2024. Published: 11 April 2024.

Regina Petrovna Vostokova
St.Petersburg State University,
7–9 Universitetskaya Embankment, St. Petersburg 199034, Russia,
e-mail: rvostokova@yandex.ru