12 Лекция 3.06

Пусть дана система полиномиальных уравнений

$$S = \begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_k(x_1, \dots, x_n) = 0 \end{cases}$$

над полем $\mathbb{C}$ и $X \subseteq \mathbb{C}^n$ множество решений. С этой системой связаны 2 идела:

1. Идеал системы $I(S) = \{h_1 f_1 + \dots + h_n f_n \mid h_i \in \mathbb{C}[x_1, \dots, x_n]\}$.
2. Идеал решений $I(X) = \{f \in \mathbb{C}[x_1, \dots, x_n] \mid f\mid_X = 0\}$.

Понятно, что $I(S) \subseteq I(X)$. Также известно, что если $I(S_1) = I(S_2)$, то системы S_1, S_2 эквивалентны. В обратную сторону неверно. Контрпример следующий:

$$S_1 = \begin{cases} x_1 = 0 \end{cases}$$

$$S_2 = \begin{cases} x_1^2 = 0 \end{cases}$$

Тогда $I_1 = (x_1) \neq (x_1^2) = I_2$.

Определение 64. *Пусть R — коммутативное кольцо, $I \subseteq R$ какой-то идеал. Радикалом идеала I называется* $\operatorname{rad}(I) = \{r \in R \mid \exists m : r^m \in I\}$. *Нетрудно видеть, что $I \subseteq R$.*

Лемма 17. $\operatorname{rad}(I)$ *всегда является идеалом.*

Доказательство. Для $\forall r \in \operatorname{rad}(I), a \in R$ нужно проверить, что $ar \in \operatorname{rad}(I)$. Тогда $\exists m : r^m \in I$, $(ar)^m = a^m r^m \in I \Rightarrow ar \in \operatorname{rad}(I)$.

Теперь проверим сумму. Возьмем $r_1, r_2 \in \operatorname{rad}(I)$ и проверим, что $(r_1 + r_2)^m \in I$. По определению $\exists m_1, m_2 : r_1^{m_1} \in I, r_2^{m_2} \in I$. Рассмотрим

$$(r_1 + r_2)^{m_1+m_2-1} = \sum_{j=0}^{m_1+m_2-1} \binom{m_1 + m_2 - 1}{j} r_1^j r_2^{m_1+m_2-j-1} \in I$$

Понятно, что если $j \geq m_1$ то попадаем в идеал. И если $m_1 + m_2 - j - 1 \geq m_2 \Leftrightarrow m_1 - 1 \geq j$ то аналогично попадаем в идеал. □

Теорема 17 (Теорема Гильберта о нулях). *Над алгебраически замкнутым полем $I(X) = \operatorname{rad}(I(S))$. То есть многочлен $f \in \mathbb{C}[x_1, \dots, x_n]$ обращается в 0 на множестве решений системы S тогда и только тогда, когда $\exists m : f^m \in (f_1, \dots, f_k)$.*

В одну сторону $\Leftarrow$ очевидно. Представим $f = h_1 f_1 + \dots + h_n f_n$. Потому что если $(\alpha_1, \dots, \alpha_n)$ решение, то $f^m(\alpha_1, \dots, \alpha_n) = 0 \Rightarrow f(\alpha_1, \dots, \alpha_n) = 0$.

В другую сторону это, казалось бы, неверно. Рассмотрим над $\mathbb{R}$ систему

$$\begin{cases} x_1^2 + x_2^2 = 0 \end{cases}$$

Тогда $X = \{(0, 0)\}$. $x_1 \in I(X)$, однако $x_1^m \notin (x_1^2 + x_2^2)$.

Следствие 13. Системы S_1, S_2 эквивалентны над $\mathbb{C} \Leftrightarrow \operatorname{rad}(I(S_1)) = \operatorname{rad}(I(S_2))$.

Вернемся к применению базисов Гребнера.

3. Дана система полиномиальных уравнений

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \vdots \\ f_k(x_1, \dots, x_n) = 0 \end{cases}$$

требуется проверить, существует ли решение над полем $K = \mathbb{C}$. Система не имеет решений $\Leftrightarrow 1 \in G$, где G базис Гребнера $f_1, \dots, f_k$. По теореме Гильберта о нулях у системы нет решений $\Leftrightarrow 1 \in \operatorname{rad}((f_1, \dots, f_k)) \Leftrightarrow 1 \in (f_1, \dots, f_k) \Leftrightarrow 1 \in G(f_1, \dots, f_k)$.

4. Проверка на принадлежность радикалу, то есть $f \in \operatorname{rad}(f_1, \dots, f_k)$. Утверждается, что

Следствие 14. $f \in \operatorname{rad}(f_1, \dots, f_k) \Leftrightarrow 1 \in (f_1, \dots, f_k, 1 - yf) \subseteq \mathbb{C}[x_1, \dots, x_n, y]$. Обозначим за $J = (f_1, \dots, f_k, 1 - yf)$.

Доказательство. Если $f^m \in (f_1, \dots, f_k)$, то

$$1 = (1 - yf)(1 + yf + \dots + y^{m-1} f^{m-1}) + y^m f^m$$

тогда $(1 - yf)(1 + yf + \dots + y^{m-1} f^{m-1}) \in J$, $y^m f^m \in J$. В обратную сторону, если $1 \in J$, то множество решений $f_1 = 0, \dots, f_k = 0, 1 - yf = 0$ пусто. Тогда $f = 0$ на любом множестве решений системы $f_1 = 0, \dots, f_k = 0$. Но тогда по теореме Гильберта о нулях $f \in \operatorname{rad}(f_1, \dots, f_k)$. □

Можно также рассмотреть другое решение, которое строит базис в радикале (сложно).

5. Эквивалентность систем.

$$\begin{cases} f_1 = 0 \\ \vdots \\ f_k = 0 \end{cases} \overset{?}{\Leftrightarrow} \begin{cases} p_1 = 0 \\ \vdots \\ p_s = 0 \end{cases}$$

Достаточно проверить, что $f_1, \dots, f_k \in \operatorname{rad}(p_1, \dots, p_s)$, $p_1, \dots, p_s \in \operatorname{rad}(f_1, \dots, f_k)$.

6. Конечность числа решений. Хотим по системе

$$\begin{cases} f_1 = 0 \\ \vdots \\ f_k = 0 \end{cases}$$

проверить, конечно ли множество решений. Утверждается, что оно конечно $\Leftrightarrow \forall i \; \exists g_i : L(g_i) = x_i^{m_i}$, где $G = \{g_1, \dots, g_s\}$ — базис Гребнера.

Доказательство. $\Rightarrow$. Пусть X — множество решений (оно конечно). Тогда $\forall x_i$ принимает на X конечное число значений. Обозначим их как $\alpha_{i1}, \dots, \alpha_{ip}$. Посмотрим на $f = (x_i - \alpha_{i1}) \dots (x_i - \alpha_{ip})$. Тогда $f\ |_X = 0$. Тогда по теореме Гильберта о нулях $f^m \in (f_1, \dots, f_k)$. Заметим, что $L(f^m) = x_i^{mp_i}$. По определению БГ $\exists g_j \ : \ L(g_j) \mid L(f_m)$. Ну и тогда $L(g_j) = x_i^{m_i}$

$\Leftarrow$. Посмотрим на $g_n = x_n^{m_n} + \dots \Rightarrow g_n = g_n(x_n)$. Следовательно $g_n(x_n)$ имеет конечное число корней. Тогда координата x_n на множестве решений конечное число значений. Аналогично $g_{n-1} = x_{n-1}^{m_{n-1}} + \dots \Rightarrow g_{n-1} = g_{n-1}(x_{n-1}, x_n)$. Так как x_n принимает конечное число значений, если подставить их все в g_{n-1} и получим, что x_{n-1} также принимает конечное число значений. Продолжаем рассуждение для $n-2, \dots, 1$. □

Факт 7. Если число решений конечно, то решение системы сводится к решению конечного числа полиномиальных уравнений от одной переменной.

Теорема 18 (Абель). $f(x) = a_n x^n + \dots + a_1 x + a_0 = 0$, *где* $a_n \neq 0, n \geq 5$, *не решается. То есть его корни не выражаются в радикалах через коэффициенты.*