9 Лекция 27.05

Лемма 10. *Если* $ax_1^{k_1} \dots x_m^{k_m}$ *— старший член многочлена* $f(x_1, \dots, x_m)$*, то* $k_1 \geq \dots \geq k_m$.

Доказательство. От противного. Пусть $\exists i : k_i < k_{i+1}$. Тогда возьмем $\tau = (i, i+1)$. Тогда в f входит $ax_1^{k_1} \dots x_i^{k_{i+1}} x_{i+1}^{k_i} \dots x_m^{k_m} > ax_1^{k_1} \dots x_i^{k_i} x_{i+1}^{k_{i+1}} \dots x_m^{k_m}$. Но получаем противоречие. □

Лемма 11. *Пусть* $k_1, \dots, k_m$ *— целые неотрицательные числа. Если* $k_1 \geq \dots \geq g_m$*, то существуют единственные целые неотрицательное* $l_1, \dots, l_m$*, для которых*

$$x_1^{k_1} \dots x_m^{k_m} = L(\sigma_1^{l_1} \dots \sigma_m^{l_m})$$

Доказательство. По лемме о старшем члене

$$L(\sigma_1^{l_1} \dots \sigma_m^{l_m}) = L(\sigma_1)^{l_1} \dots L(\sigma_m)^{l_m}$$

Вспомним, что

$$L(\sigma_1) = x_1, L(\sigma_2) = x_1 x_2, \dots, L(\sigma_k) = x_1 \dots x_k$$

Тогда справедлива следующая система

$$\begin{cases} k_1 = l_1 + \dots + l_m \\ k_2 = l_2 + \dots + l_m \\ \vdots \\ k_m = l_m \end{cases}$$

из которой можно однозначно восстановить $l_1, \dots, l_m$:

$$\begin{cases} l_m = k_m \\ l_{m-1} = k_{m-1} - k_m \geq 0 \\ \vdots \\ l_1 = k_1 - k_2 \geq 0 \end{cases}$$

□

Доказательство. (Теорема о симметрических многочленах) Сначала докажем существование. Сразу считаем, что $f(x_1, \dots, x_n) \neq 0$. Тогда по лемме 11: $L(f) = aL(\sigma_1^{l_1} \dots \sigma_m^{l_m})$. Тогда $f' = f - L(f)$ также симметрический, причем старший член строго уменьшился. Продолжаем процесс. В конце перенесем все кроме f направо, получим выражение для f. Нетрудно видеть, что процесс конечный, потому что $L(f) = ax_1^{k_1} \dots x_m^{k_m} > L(f') = bx_1^{l_1} \dots x_m^{l_m}$, а наборов $k_1 \geq p_1 \geq \dots \geq p_m$ конечное число.

Докажем единственность. От противного. Пусть

$$f = F(\sigma_1, \dots, \sigma_m) = G(\sigma_1, \dots, \sigma_m)$$

Тогда рассмотрим $H(y_1, \dots, y_m) = F - G$. Он ненулевой по предположению от противного. Но тогда $H(\sigma_1, \dots, \sigma_m) = 0$. Поймем, что такое невозможно. Пусть $H_1, \dots, H_s$ — все различные члены H, $w_1, \dots, w_s$ — старшие члены соответствующих $H_i(\sigma_1, \dots, \sigma_m)$ как многочленов от $x_1, \dots, x_m$. Тогда одночлены $w_1, \dots, w_s$ попарно различны по лемме 11. Выберем из них самый старший, wlog это w_1. Тогда w_1 старше всех $H_1(\sigma_1, \dots, \sigma_m), H_2(\sigma_1, \dots, \sigma_m), \dots, H_s(\sigma_1, \dots, \sigma_m)$. Но тогда он не может сократиться. Получаем противоречие с тем, что $H(\sigma_1, \dots, \sigma_m) = 0$. □

Теорема 13 (Теорема Виета для многочленов n-ой степени). *Пусть $\alpha_1, \dots, \alpha_n$ — корни многочлена $a_n x^n + \dots + a_1 x + a_0$. Тогда $\sigma_k(\alpha_1, \dots, \alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}$.*

Доказательство. Приравняем коэффициенты при x^{n-k} в левой и правой части.

$$a_n x^n + \dots + a_1 x + x_0 = a_n(x - \alpha_1) \dots (x - \alpha_n)$$
$$a_{n-k} = a_n \sigma_k(-\alpha_1, \dots, -\alpha_n) = a_n(-1)^k \sigma_k(\alpha_1, \dots, \alpha_n) \Leftrightarrow \sigma_k(\alpha_1, \dots, \alpha_n) = (-1)^k \frac{a_{n-k}}{a_n}$$

□

Из теоремы Виета напрашивается следующий вывод: любой симметрический многочлен от корней выражается через коэффициенты многочлена.

Определение 54. *Дискриминантом многочлена $h(x) = a_n x^n + \dots + a_1 x + a_0$ с корнями $\alpha_1, \dots, \alpha_n$ называется такое число*

$$D(h) = a_n^{2n-2} \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

Замечание 11. *$D(h) = 0 \Leftrightarrow$ у многочлена $h(x)$ есть кратные корни.*

Замечание 12. *$D(h)$ является многочленом от коэффициентов $h(x)$, так как $\prod(\alpha_i - \alpha_j)^2$ – симметрический многочлен от $\alpha_1, \dots, \alpha_n$.*

Пример. $h(x) = ax^2 + bx + c$. Тогда $D(h) = a^2(\alpha_2 - \alpha_1)^2$, где α_1, α_2 — корни. Упростим

$$D(h) = a^2((\alpha_2 + \alpha_1)^2 - 4\alpha_1\alpha_2) = a^2 \left(\left(\frac{b}{a} \right)^2 - 4\frac{c}{a} \right) = b^2 - 4ac$$

Факт 5. Случайный многочлен степени n не имеет кратных корней.

Базисы Гребнера Пусть мы хотим решать системы полиномиальных уравнений над полем $\mathbb{C}$.

$$\begin{cases} p_1(x_1, \dots, x_n) = 0 \\ \vdots \\ p_n(x_1, \dots, x_n) = 0 \end{cases} \quad \Leftarrow \text{хотим найти множество решений}$$

Мы научимся отвечать на 2 вопроса:

1. Разрешима ли система?

2. Конечно или бесконечно число решений?

Определение 55. *Системы называются эквивалентными, если их множества решений совпадают.*

Определение 56. $I = (p_1, \dots, p_n) \subseteq \mathbb{C}[x_1, \dots, x_n]$ *будет идеалом. Более формально,*

$$I = \{p_1 h_1 + \dots + p_n h_n \mid h_i \in \mathbb{C}[x_1, \dots, x_n]\}$$

Лемма 12. *Если* $p_1(\alpha_1, \dots, \alpha_n) = \dots = p_n(\alpha_1, \dots, \alpha_n) = 0$, *то* $\forall f \in (p_1, \dots, p_n) : f(\alpha_1, \dots, \alpha_n) = 0$.

Доказательство. Очевидно, потому что f это линейная комбинация $p_1, \dots, p_n$. □

Сделаем промежуточный вывод. Если I идеал в кольце многочленов и $I = (p_1, \dots, p_n) = (q_1, \dots, q_m)$, то

1. $\{p\}, \{q\}$ называются базисами идеала
2. Системы p, q эквивалентны, то есть

$$\begin{cases} p_1 = 0 \\ \vdots \\ p_n = 0 \end{cases} \Leftrightarrow \begin{cases} q_1 = 0 \\ \vdots \\ q_m = 0 \end{cases}$$

Но обратное к пункту 2 неверно, то есть из эквивалентности систем не следует $(p_1, \dots, p_n) = (q_1, \dots, q_m)$.

Теорема 14 (Теорема Гильберта о базисе)**.** *Любой идеал в кольце многочленов имеет конечный базис, то есть* $I = (p_1, \dots, p_n)$.

Обозначим за $M_n = \{x_1^{k_1} \dots x_n^{k_n}\}$ множество одночленов. Введем на нем частичный порядок. Скажем, что $x_1^{k_1} \dots x_n^{k_n} > x_1^{l_1} \dots x_n^{l_n}$ тогда и только тогда, когда второй делит первый. Можно перефразировать как $(k_1, \dots, k_n) \geq (l_1, \dots, l_n)$ покоординатно. Тогда справедлива следующая лемма.

Лемма 13 (Диксона)**.** *В любом подмножестве* $S \subseteq M_n$ *число минимальных элементов в этом частичном порядке конечно.*

Лемма 14. *В лексикографическом порядке не существует бесконечных убывающих цепочек.*