**Пример:** На практике берем

$$f = \sum c_d x_1^{d_1} \dots x_n^{d_n}$$

находим самый крайний $x_1^{d_1} x_2^{d_2} \dots x_n^{d_n}$, $d_1 \geq d_2 \geq \dots \geq d_n$ - разбиение $\lambda$

$f - c_d e_{\lambda^*}$ имеет меньшие мономы и с ними продолжаем.

## Лекция №6 Результант и дискриминант.

**Теорема:** $\mathbb{Z}[x_1, \dots, x_n]^{\mathfrak{S}_n} \simeq \mathbb{Z}[e_1, \dots e_n]$

$f(z) = z^n + a_1 z^{n-1} + \dots + a_n = (z - x_1) \dots (z - x_n)$

$a_1 = -e_1, \; a_2 = e_2, \; \dots \; a_i = (-1)^i e_i$

**Алгоритм как вырazить симметрический многочлен от $x_i$ через $e_i$:**

$P(x_1, \dots, x_n) = \sum c_\alpha x^\alpha \qquad c_{123} = c_{321}$

$x^\alpha = x_1^{\alpha_1} \dots x_n^{\alpha_n}$

1) Сведем на однородное слагаемое

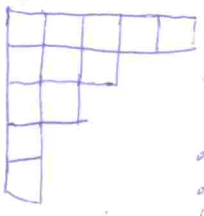
2) $\sum \alpha_i = N$

Упорядочим мономы лексикографически

$x_1^N > \dots > x_n^N$

среди всех $c_\alpha \neq 0$ выберем старший

$\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$ - диаграмма Юнга



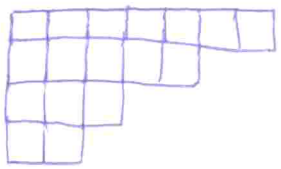
$\alpha_1 = 5$
$\alpha_2 = 3$
$\alpha_3 = 2$ $\Rightarrow \alpha^*$ - двойственная
$\alpha_4 = 1$
$\alpha_5 = 1$
$\alpha_n$

**Факт:** $P = c_\lambda e_{\lambda^*} +$ (остаток из меньших мономов)

$\lambda^* = (\beta_1 \geq \beta_2 \geq \dots)$

$e_{\lambda^*} = e_{\beta_1} \cdot e_{\beta_2} \dots e_{\beta_n}$

$P = c_{\lambda^*} e_1^2 e_2 e_3 e_5$



$\alpha_1 = 7$
$\alpha_2 = 5$
$\alpha_3 = 3$
$\alpha_4 = 2$

$\beta_1 = 4,\ \beta_2 = 4,\ \beta_3 = 3,\ \beta_4 = 2,\ \beta_5 = 2,\ \beta_6 = 1$

$P = c_\lambda\ e_4^2 e_3 e_2^2 e_1^2 + \dots$

---

Пусть $f(z) = a_0 z^n + a_1 z^{n-1} + \dots + a_n =$

$= a_0 (z - x_1)(z - x_2) \dots (z - x_n)$

$\Downarrow$

$a_i = (-1)^i a_0 e_i$

Круговой или циклотомический многочлен

$\Phi_n(z) = \prod_i (z - \zeta_i)$

$\zeta_i$ - корни ур 1 степени равно n - первообразные

$\Phi_1(z) = (z - 1)$

$\Phi_2(z) = (z + 1)$

$\Phi_3(z) = z^2 + z + 1$

$\Phi_4(z) = z^2 + 1$

$\Phi_5(z) = z^4 + z^3 + z^2 + 1$

$\Phi_6(z) = z^2 - z + 1$

Результант

$R(f, g)$

$f(z) = a_0 z^n + a_1 z^{n-1} + \dots + a_n = a_0 (z - x_1) \dots (z - x_n)$

$g(z) = b_0 z^m + b_1 z^{m-1} + \dots + b_m = b_0 (z - y_1) \dots (z - y_m)$

$R(f, g) = 0$ т и ТТК

f и g имеют общий корень

Определение: $R(f,g) = a_0^m b_0^n \prod_{i,j} (x_i - y_j) =$

$a_0^m \prod_i g(x_i) = (-1)^{mn} b_0^n \prod_j f(y_j)$ - симметрический многочлен от $x, y \Rightarrow$

$\Rightarrow$ многочлен от $a, b$.

Мы его вычислим

Прим: если есть общий корень у $f(z)$ и $g(z)$, то они не взаимно просты

$\exists$ многочлены $h(z)$ и $k(z)$ степени $\deg h(z) < m$, $\deg k(z) < n$, $h \not\equiv 0$, $k \not\equiv 0$ такие что $\Leftrightarrow$

$$fh = gk$$

$$h = c_0 z^{m-1} + c_1 z^{m-2} + \dots c_{m-1}$$

$$k = d_0 z^{n-1} + d_1 z^{n-2} + \dots + d_{n-1}$$

$$hf = (a_0 z^n + \dots + a_n)(c_0 z^{m-1} + \dots + c_{m-1})$$

$$gk = (b_0 z^m + \dots + b_m)(d_0 z^{n-1} + \dots + d_{n-1})$$

$$a_0 c_0 = b_0 d_0$$

$$a_0 c_1 + a_1 c_0 = b_0 d_1 + b_1 d_0$$

$$a_0 c_2 + a_1 c_1 + a_2 c_0 = b_0 d_2 + b_1 d_1 + b_2 d_0$$

$\Downarrow$

Система линейных уравнений на неизвестные $c$ и $d$: $\{c_0, \dots, c_{m-1}, d_0, \dots, d_{n-1}\}$ $n+m$ шт.

Мы хотим, чтобы было $\not\equiv 0$ решение

Правило Крамера: $\exists$ решение $\not\equiv 0 \Leftrightarrow \det | \ | = 0$

$$\begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_n & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_{n-1} & a_n & 0 & 0 \\ 0 & \dots & \dots & 0 & a_0 & \dots & a_{n-1} & a_n \\ b_0 & \dots & \dots & b_{m-1} & b_m & 0 & \dots & 0 \\ 0 & b_0 & \dots & \dots & b_{m-1} & b_m & 0 & 0 \\ 0 & \dots & 0 & b_0 & \dots & \dots & b_{m-1} & b_m \end{pmatrix} \quad (n+m) \times (n+m)$$

**Теорема** Результант $R(f,g) = \det | \ |$

Д-во: получили два многочлена от $a$ и $b$ с одинаковыми нулями

Осталось проверить, что они имеют одну и ту же степень

$\deg x_i = \deg y_j = 1 \Rightarrow \deg a_i = i, \deg b_j = j$

$\deg a_0 = \deg b_0 = 0$

А определению $\deg R(f,g) = mn$

$\deg \det = mn$

Значит, $R = \det Q(a_0, b_0)^{\pm 1}$

Чтобы удостоиться, что $Q \equiv 1$, достаточно сравнить какой-нибудь коэффициент $\det = a_0^n b_m^n + \dots$

$R = a_0^m b_m^n$

---

$f(x,y) = 0 = g(x,y)$

$\mathbb{C}[x][y]$

$R(f,g)$ как многочлен от $x \Rightarrow$ можно искл. $x$.

**Дискриминант**

$\mathcal{D} f(z)$ равен нулю, когда есть кратные корни

$$a_0^{m-2} \prod_{1 \le i < j \le n} (x_i - x_j)^2 =: \mathcal{D} f$$

**Теорема:**

$a_0 \mathcal{D} f = \pm R(f, f')$

$\mathcal{D} f = \pm \dfrac{R(f,f')}{a_0}$

↳ т.к. $b_0 = n a_0$

Д-во: $R(f,f') = a_0^{n-1} \prod_{i=1}^{n} f'(x_i) = a_0^{2n-2} \prod_{1 \le i \ne j \le n} (x_i - x_j)$

$f = a_0 (z - x_1) \cdots (z - x_n)$

$f'(x_i) = a_0 \prod_{j \ne i} (x_i - x_j)$

□

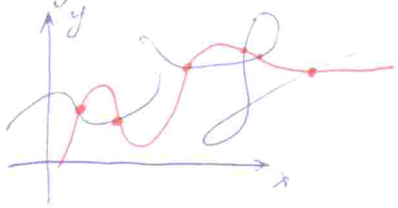
## Приложение: Теорема Безу

$f(x,y)$, $g(x,y)$ многочлены от $x, y$ степеней $m$ и $n$

Если множество общих корней конечно, то число корней $\le mn$

Иначе у $f$ и $g$ есть общий множитель.

Д-во:




Выберем новую координату на плоскости $(\mathbb{Z}, t)$ т.ж. проекции всех общих корней на ось $t$ были бы различны

$f, g \in \mathbb{C}[t][\mathbb{Z}]$ , $R(f,g) \in \mathbb{C}[t]$

Чтобы $t_0$ было проекцией общего корня $R(f,g)\big|_{t_0} = 0$.

Лемма $\deg_t R(f,g) \le mn$

$\deg_{a,b} R = mn$

$\deg a_i = \deg b_i = i$

$f(t,z) = a_0(t) z^n + a_1(t) z^{n-1} + \dots a_n(t)$ , $\deg f = n$

$\deg a_0(t) = 0$, $\deg a_1(t) \le 1$, $\deg a_i(t) \le i$

□

Значит, у $R(f,g)$ не больше $mn$ корней по $t \Rightarrow$

$\Rightarrow$ всего общих точек $\le mn$

Либо $R(f,g) \equiv 0$, тогда $\forall t$ есть общий корень, т.е. у $f, g$ общая компонента