Дискриминанта и резултанта.

Да разгледаме полиномът $f(x) \in F[x]$ над поле F от степен $\deg f = n \geq 1$, старши коефициент $a_0 \neq 0$ и корени $\alpha_1, \alpha_2, \ldots, \alpha_n$ принандлежащи на някакво разширение $K \geq F$. Търсим отговор на въпроса дали f има кратен корен. Един подход е да видим, че $(f, f') \neq 1$ и да използваме алгоритъма на Евклид, за да намерим НОД, чиито корени ще бъдат точно кратните корени на f. Друг подход, при $n \geq 2$ е да разгледаме израза $\prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j)$. Ясно е, че f има кратен корен $\iff$ $\prod_{1\leq i<j\leq n}(\alpha_i - \alpha_j) = 0$.

И така, елементът на полето K

$$D(f) = a_0^{2n-2} \prod_{1\leq i<j\leq n} (\alpha_i - \alpha_j)^2 \in K$$

се нарича *дискриминанта на полинома* f. Полиномът f има кратни корени точно когато $D(f) = 0$. При $\deg f = 1$ приемаме, че $D(f) = 1$.

Забеежка:

Дискриминантата $D(f)$ е симетричен полином на $\alpha_1, \alpha_2, \ldots, \alpha_n$ с коефициенти от F и като такъв следва, че $D(f) \in K$. По-точно $D(f)$ е полином на $a_0^{-1}, a_1, \ldots, a_n$ с коефициенти от F.

Пример:

При $n = 2$ разглеждаме полинома $f(x) = a_0x^2 + a_1x + a_2$ със старши коефициент $a_0 \neq 0$ и корени α_1, α_2. Тогава

$$\begin{aligned} D(f) &= a_0^2(\alpha_1 - \alpha_2)^2 = a_0^2\left((\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2\right) \\ &= a_0^2\left(\left(-\frac{a_1}{a_0}\right)^2 - 4\frac{a_2}{a_0}\right) = a_1^2 - 4a_0a_2. \end{aligned}$$

Това напълно съвпада с формулата за дискриминанта на квадратно уравнение, позната от училище.

Твърдение 1. *За дискриминантата на полинома $f \in F[x]$ е в сила равенството*

$$D(f) = a_0^{n-2} f'(\alpha_1) f'(\alpha_2) \dots f'(\alpha_n)(-1)^{\frac{n(n-1)}{2}} = (-1)^{\frac{n(n-1)}{2}} a_0^{n-2} \prod_{k=1}^{n} f'(\alpha_k).$$

Доказателство. Знаем, че $f(x)$ се представя като

$$f(x) = a_0(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_n)$$

Тогава

$$\begin{aligned} f'(x) = a_0(x - \alpha_2) \dots (a - \alpha_n) + \dots \\ + a_0(x - \alpha_1) \dots (x - \alpha_{k-1})(x - \alpha_{k+1}) \dots (x - \alpha_n) + \dots \\ + a_0(x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_{n-1}) \end{aligned}$$

и при $x = \alpha_k$ за $k = 1, 2, \dots, n$ получаваме

$$f'(\alpha_k) = (\alpha_k - \alpha_1) \dots (\alpha_k - \alpha_{k-1})(\alpha_k - \alpha_{k+1}) \dots (\alpha_k - \alpha_n).$$

Сега разписваме формулата за детерминантата и получаваме

$$\begin{aligned} D(f) = {} & a_0(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) \dots (\alpha_1 - \alpha_n) \\ & a_0(\alpha_2 - \alpha_1)(\alpha_2 - \alpha_3) \dots (\alpha_2 - \alpha_n) \dots \\ & a_0(\alpha_n - \alpha_1)(\alpha_n - \alpha_2) \dots (\alpha_n - \alpha_{n-1}) \\ & a_0^{n-2}(-1)^{0+1+\dots+(n-1)}, \end{aligned}$$

а след заместване на изразите за проивзодната достигаме до

$$\begin{aligned} D(f) &= f'(\alpha_1) f'(\alpha_2) \dots f'(\alpha_n) a_0^{n-2} (-1)^{\frac{n(n-1)}{2}} \\ &= (-1)^{\frac{n(n-1)}{2}} a_0^{n-2} \prod_{k=1}^{n} f'(\alpha_k). \end{aligned}$$

□

Твърдение 2. *За* $\forall k \in \mathbb{N}$ *изразът*

$$S_k = \alpha_1^k + \alpha_2^k + \cdots + \alpha_n^k$$

се нарича k*-ти степенен сбор на* $\alpha_1, \alpha_2, \ldots, \alpha_n$*. Приемаме, че* $S_0 = n$*. Тогава е в сила*

$$D(f) = a_0^{2n-2} \underbrace{\begin{vmatrix} S_0 & S_1 & \ldots & S_{n-1} \\ S_1 & S_2 & \ldots & S_n \\ S_2 & S_3 & \ldots & S_{n+1} \\ \ldots & \ldots & \ddots & \ldots \\ S_{n-1} & S_n & \ldots & S_{2n-2} \end{vmatrix}}_{\Delta}.$$

Доказателство. Детерминантата Δ е от ред n и (i,j)-тият ѝ елемент е S_{i+j-2}. Разглеждаме детерминантата на Вандермонд

$$W = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_n \\ \ldots & \ldots & \ddots & \ldots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \ldots & \alpha_n^{n-1} \end{vmatrix} = \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i).$$

В такъв случай $D(f) = a_0^{2n-2} W^2$. Умножаваме $W.W$ по правилото ред по ред. В W i-тият ред е $\alpha_1^{i-1}, \alpha_2^{i-1}, \ldots, \alpha_n^{i-1}$, а j-тият ред е $\alpha_1^{j-1}, \alpha_2^{j-1}, \ldots, \alpha_n^{j-1}$. Тогава в W^2 (i,j)-тият елемент е $\alpha_1^{i+j-2} + \alpha_2^{i+j-2} + \cdots + \alpha_n^{i+j-2} = S_{i+j-2}$. По този начин се оказва, че $W^2 = \Delta$, което доказва твърдението. $\square$

Пример: Нека разгледаме полинома от трета степен

$$f(x) = a_0 x^3 + a_1 x^2 + a_2 x + a_3.$$

След полагане $x = y - \dfrac{a_1}{3a_0}$ и деление на a_0 $f(x)$ приема вида

$$g(y) = y^3 + py + q.$$

Тогава $D(f) = a_0^4 D(g)$. Нека $\beta_1, \beta_2, \beta_3$ са корените на $g(y)$. Пресмятаме степенните сборове с помощта на формулите на Виет:

$$\begin{aligned}
&S_0 = 3, \\
&S_1 = \beta_1 + \beta_2 + \beta_3 = 0, \\
&S_2 = \beta_1^2 + \beta_2^2 + \beta_3^3 = (\beta_1 + \beta_2 + \beta_3)^2 - 2(\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3) = -2p, \\
&S_3 = \beta_1^3 + \beta_2^3 + \beta_3^3 = -p\beta_1 - q - p\beta_2 - q - p\beta_3 - q = -p(\beta_1 + \beta_2 + \beta_3) - 3q = -3q, \\
&S_4 = \beta_1^4 + \beta_2^4 + \beta_3^4 = -p\beta_1^2 - q\beta_1 - p\beta_2^2 - q\beta_2 - p\beta_3^2 - q\beta_3 = -pS_2 - qS_1 = 2p^2.
\end{aligned}$$

Сега, според Твърдение 2

$$D(g) = 1^{2.3-2} \begin{vmatrix} S_0 & S_1 & S_2 \\ S_1 & S_2 & S_3 \\ S_2 & S_3 & S_4 \end{vmatrix} = \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix}$$
$$= -12p^3 + 8p^3 - 27q^2 = -4p^4 - 27q^2.$$

Нека $f(x) = a_0x^n + \cdots + a_n, a_0 \neq 0, n \geq 1$ и $g(x) = b_0x^s + \cdots + b_s, b_0 \neq 0, s \geq 1$ са два полинома над F. Питаме се как да разберем дали f и g имат общ корен. Един подход е да използваме алгоритъма на Евклид и да проверим дали $(f, g) \neq 1$.

Ще разгледаме и друг подход. Нека $\alpha_1, \alpha_2, \ldots, \alpha_n$ са корените на f, а $\beta_1, \beta_2, \ldots, \beta_s$ са корените на g. Ясно е, че f и g имат общ корен $\iff$ $\prod_{i=1}^{n}\prod_{j=1}^{s}(\alpha_i - \beta_j) = 0$.

Елементът

$$R(f, g) = a_0^s b_0^n \prod_{i=1}^{n}\prod_{j=1}^{s}(\alpha_i - \beta_j)$$

на разширението, $K \geq F$, съдържащо корените на f и g, сенарича *резултанта на полиномите f и g*. Очевдино f и g имат общ корен $\iff R(f, g) = 0$.

Забележка:
$R(g, f) = (-1)^{ns}R(f, g)$. Наистина, имаме че

$$R(g, f) = b_0^n a_0^s \prod_{j=1}^{s}\prod_{i=1}^{n}(\beta_j - \alpha_i) = a_0^s b_0^n \prod_{i=1}^{n}\prod_{j=1}^{s}(\alpha_i - \beta_j)(-1)^{ns} = (-1)^{ns}R(f, g).$$

Твърдение 3. *$R(f, g) = a_0^s g(\alpha_1)g(\alpha_2)\ldots g(\alpha_n) = a_0^s \prod_{i=1}^{n} g(\alpha_i)$. (Аналогично твърдим, и че $R(f, g) = b_0^n \prod_{j=1}^{s} f(\beta_j)$.)*

Доказателство. Знаейки корените на g, го представяме като

$$g(x) = b_0(x - \beta_1)(x - \beta_2)\ldots(x - \beta_s) = b_0 \prod_{j=1}^{n}(x - \beta_j).$$

Тогава $g(\alpha_i) = b_0 \prod_{j=1}^{s}(\alpha_i - \beta_j)$ за $\forall i = 1, 2, \ldots, n$. Умножаваме всички тези изрази, за да получим, че

$$\prod_{i=1}^{n} g(\alpha_i) = \prod_{i=1}^{n}\left(b_0 \prod_{j=1}^{s}(\alpha_i - \beta_j)\right) = b_0^n \prod_{i=1}^{n}\prod_{j=1}^{n}(\alpha_i - \beta_j).$$

Умножаваме двете страни на равенството с a_0^s и веднага получаваме, че

$$a_0^s \prod_{i=1}^{n} g(\alpha_i) = a_0^s b_0^n \prod_{i=1}^{n} \prod_{j=1}^{s} (\alpha_i - \beta_j) = R(f, g),$$

което искахме да докажем. $\square$

Освен формула за намиране на $R(f, g)$ Твърдение 3 показва и че $R(f, g)$ е симетричен полином с коефициенти от F на $\alpha_1, \alpha_2, \ldots, \alpha_n$ и оттук следва, че всъщност $R(f, g) \in F$. По-точно $R(f, g)$ е полином с коефициенти от F на $a_0, a_1, \ldots, a_n; b_0, b_1, \ldots, b_s$.

Твърдение 4. *Нека F е поле с характеристика $\operatorname{char} F = 0$ и $f(x) \in F[x]$. Тогава*

$$R(f, f') = (-1)^{\frac{n(n-1)}{2}} a_0 D(f).$$

Доказателство. Нека $\deg f = n \geq 1$. Тогава от $\operatorname{char} F = 0$ следва, че $\deg f' = n - 1$. Твърдение 1 ни дава, че

$$D(f) = (-1)^{\frac{n(n-1)}{2}} a_0^{n-2} \prod_{i=1}^{n} f'(\alpha_i),$$

а от Твърдение 3, приложено за f и $g = f'$ имаме, че

$$R(f, g) = a_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i).$$

Сега очевидно

$$D(f)(-1)^{\frac{n(n-1)}{2}} a_0 = a^{n-1} \prod_{i=1}^{n} f'(\alpha_i) = R(f, f'),$$

което трябваше да докажем. $\square$