Rezultáns

Legyen R egy integritástartomány és

$$f(x), g(x) \in R[x]$$

tetszőleges polinomok, ahol

$$f(x) = f_m x^m + f_{m-1} x^{m-1} + \cdots + f_1 x + f_0,$$

$$g(x) = g_n x^n + g_{n-1} x^{n-1} + \cdots + g_1 x + g_0,$$

$$f_m \neq 0, g_n \neq 0, n, m \in \mathbf{N}.$$

Megjegyzés. Egységelemes zérusosztómentes kommutatív gyűrűt *integritástartománynak* nevezzük.

Tekintsük az R integritástartomány H hányadostestének azt a legszűkebb K bővítését, amelyben a polinomok lineáris faktorokra bomlanak.

Ekkor

$$f(x) = f_m(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_m),$$

$$g(x) = g_n(x - \beta_1)(x - \beta_2)\cdots(x - \beta_n).$$

Definíció. A $\text{res}(f, g)$ szorzatot az f és g polinomok *rezultánsának* nevezzük, ahol

$$\text{res}(f, g) = f_m^n g_n^m (\alpha_1 - \beta_1)(\alpha_1 - \beta_2)\cdots(\alpha_1 - \beta_n)$$

$$\cdot(\alpha_2 - \beta_1)(\alpha_2 - \beta_2)\cdots(\alpha_2 - \beta_n)$$

$$\cdots(\alpha_m - \beta_1)(\alpha_m - \beta_2)\cdots(\alpha_m - \beta_n).$$

Tegyük fel, hogy a két polinomnak van közös gyöke, ekkor van olyan $\alpha \in K$ szám, melyre

$$f_m\alpha^m + f_{m-1}\alpha^{m-1} + \cdots + f_1\alpha + f_0 = 0,$$

$$g_n\alpha^n + g_{n-1}\alpha^{n-1} + \cdots + g_1\alpha + g_0 = 0.$$

A két egyenletet szorozzuk meg rendre

$$\alpha^{n-1}, \alpha^{n-2}, \ldots, \alpha, 1,$$

illetve

$$\alpha^{m-1}, \alpha^{m-2}, \ldots, \alpha, 1$$

számokkal. Ekkor egy $m+n$ egyenletből álló homogén lineáris egyenletrendszert kapunk, melynek

$$\alpha^{m+n-1}, \alpha^{m+n-2}, \ldots, \alpha, 1,$$

a megoldása. Nem triviális megoldás csak akkor létezik, ha az együtthatókból készített determináns zérus.

A következő determináns az f és g polinomok rezultánsa *Sylvester-féle* alakja.

$$D = \begin{vmatrix} f_m & \cdots & \cdots & \cdots & f_0 & \\ & \ddots & & & & \\ & f_m & \cdots & \cdots & \cdots & f_0 \\ g_n & \cdots & g_0 & & & \\ & \ddots & & & & \\ & & g_n & \cdots & \cdots & g_0 \end{vmatrix}$$

Példa. Legyen

$$f(x) = 2x^3 - \alpha x^2 + x + 3 \in \mathbf{Q}[x],$$

$$g(x) = x^2 - 5x + 6 \in \mathbf{Q}[x].$$

Ekkor

$$\operatorname{res}(f,g) = \begin{vmatrix} 2 & -\alpha & 1 & 3 & \\ & 2 & -\alpha & 1 & 3 \\ 1 & -5 & 6 & & \\ & 1 & -5 & 6 & \\ & & 1 & -5 & 6 \end{vmatrix}$$

így

res$(f,g) = 36\alpha^2 - 429\alpha + 1260 = 3(4\alpha - 21)(3\alpha - 20)$
azaz, ha $\alpha = \frac{20}{3}$ vagy $\alpha = \frac{21}{4}$ akkor lehet a két egyenletnek közös gyöke.

Legyen

$$f(x,y) = x^2 + xy + 2x + y - 1 \in \mathbf{Z}[x,y],$$

$$g(x,y) = x^2 + 3x - y^2 + 2y - 1 \in \mathbf{Z}[x,y].$$

Ekkor

$$\mathrm{res}_y(f,g) = \begin{vmatrix} x+1 & x^2+2x-1 & 0 \\ 0 & x+1 & x^2+2x-1 \\ -1 & 2 & x^2+3x-1 \end{vmatrix},$$

így

$$\mathrm{res}_y(f,g) = -x^3 - 2x^2 + 3x,$$

azaz közös gyökök akkor létezhetnek, ha

$$x \in \{-3, 0, 1\}.$$

A közös megoldások: $(-3,1), (0,1), (1,-1)$.

Műveletigény: $O((m+n)^3)$.

Egyszerűsítési lehetőségek: Ha $m \geq n$, akkor létezik olyan $q, r \in R[x]$, hogy

$$g_n^{m-n+1} f = gq + r,$$

ahol $r = 0$ vagy $\deg r < \deg g$. A q polinomot az f és g polinomik *pszeudo-hányadosának,*, az r polinomot *pszeudo-maradékának* nevezzük.

Jelölés: $q = pquo(f, g), r = prem(f, g)$.

Tétel. Tegyük fel, hogy $m \geq n > 0$, ekkor $res(f, g) = 0$ ha $prem(f, g) = 0$, illetve

$$g_n^{(m-n)(n-1)+d} res(f, g) = (-1)^{mn} res(g, r),$$

ha $r = prem(f, g) \neq 0$ és $d = \deg(r)$.