Глава 12

Въпрос 12: Резултанта

За да определим кога полиномите $f, g \in k[x]$ с коефициенти от поле k имат общ делител h от степен $\deg(h) > 0$, достатъчно е да разложим g и h в произведение от неразложими над k множители от $k[x]$ и да определим дали тези разлагания имат поне един общ множител, с точност до мултипликативна константа. Ето още един критерий:

Лема 12.1. *Нека $f, g \in k[x]$ са полиноми от степен $\deg f = l > 0$, $\deg g = m > 0$. В такъв случай, f и g имат общ делител от положителна степен тогава и само тогава, когато съществуват полиноми $A, B \in k[x]$, така че:*
(i) $Af + Bg = 0$;
(ii) поне един от полиномите A или B не се анулира тъждествено;
(iii) $\deg A \leq m - 1$, $\deg B \leq l - 1$.

Доказателство: Ако f и g имат общ делител $h \in k[x]$ от степен $\deg h \geq 1$, то $f = hf_1$, $g = hg_1$ за подходящи полиноми $f_1, g_1 \in k[x]$. Тогава f_1 и g_1 не се анулират тъждествено, имат степени $\deg f_1 \leq l-1$, $\deg g_1 \leq m-1$ и изпълняват тъждеството

$$g_1 f + (-f_1)g = g_1(hf_1) - f_1(hg_1) \equiv 0.$$

С други думи, $A := g_1$ и $B := -f_1$ удовлетворяват посочените условия.
Обратно, да предположим, че $A, B \in k[x]$ изпълняват условията (i), (ii) и (iii). За определеност можем да считаме, че $B \not\equiv 0$. Ако допуснем, че f и g нямат общ делител $h \in k[x]$ от степен $\deg h \geq 1$, то най-големият общ делител $GCD(f, g) = 1$ и по Лема 11.5 съществуват полиноми $\widetilde{A}, \widetilde{B} \in k[x]$ с $\widetilde{A}f + \widetilde{B}g = 1$. Умножаваме последното равенство с B и вземайки предвид $Bg = -Af$ получаваме

$$B = (\widetilde{A}f + \widetilde{B}g)B = \widetilde{A}Bf + \widetilde{B}Bg = \widetilde{A}Bf - \widetilde{B}Af = (\widetilde{A}B - \widetilde{B}A)f.$$

За ненулевия полином B оттук следва, че $\deg B \geq \deg f = l$. Противоречието с (iii) доказва, че f и g имат общ делител $h \in k[x]$ от степен $\deg h \geq 1$, Q.E.D.
Съществуването на полиномите $A, B \in k[x]$ от Лема 12.1 се установява с помощта на линейната алгебра. По-точно, търсим коефициентите $\alpha_j, \beta_i \in k$ на полиномите

$$A = \sum_{j=0}^{m-1} \alpha_j x^j, \quad B = \sum_{i=0}^{l-1} \beta_i x^i,$$

така че да е изпълнено $Af + Bg = 0$ за

$$f = \sum_{i=0}^{l} a_i x^i, \quad g = \sum_{j=0}^{m} b_j x^j$$

с $a_i, b_j \in k$, $a_l \neq 0$, $b_m \neq 0$. Сравняваме с 0 коефициентите на $1, x, \ldots x^{l+m-1}$ в

$$Af + Bg = \sum_{i=0}^{l+m-1} \left(\sum_{s=0}^{i} a_s \alpha_{i-s} \right) x^i + \sum_{i=0}^{l+m-1} \left(\sum_{s=0}^{i} b_s \beta_{i-s} \right) x^i$$

и получаваме

$$\sum_{s=0}^{i} a_{i-s}\alpha_s + b_{j-s}\beta_s = 0 \quad \text{за} \quad \forall 0 \leq i \leq l+m-1. \tag{12.1}$$

Последните равенства могат да се разглеждат като система от $l+m$ хомогенни уравнения на $l+m$ променливи $\alpha_0, \alpha_1, \ldots, \alpha_{m-1}, \beta_0, \beta_1, \ldots, \beta_{l-1}$. Матрицата на тази система

$$\mathrm{Syl}(f,g,x) = \begin{pmatrix} a_0 & & & & b_0 & & & \\ a_1 & a_0 & & & b_1 & b_0 & & \\ a_2 & a_1 & \ldots & & b_2 & b_1 & \ldots & \\ \ldots & \ldots & \ldots & a_0 & \ldots & \ldots & \ldots & b_0 \\ a_l & & & & b_m & & & \\ & a_l & & & & b_m & & \\ & & \ldots & & & & \ldots & \\ & & & a_l & & & & b_m \end{pmatrix}$$

се нарича матрица на Силвестър на f и g относно x. Първите и m стълба съдържат коефициентите на f, записани последователно, започвайки от $1, 2, \ldots, m$-ти ред. Следващите l стълба се съдържат коефициентите на g, записани последователно, започвайки от $1, 2, \ldots, l$-ти ред. Съществуването на ненулево решение $\alpha_0, \ldots, \alpha_{m-1}, \beta_0, \beta_1, \ldots, \beta_{l-1}$ на разглежданата хомогенна линейна система е еквивалентно на анулирането на детерминантата на матрицата на Силвестър

$$\mathrm{Res}(f,g,x) := \det(\mathrm{Syl}(f,g,x)),$$

наречена резултанта на f и g относно x.

Твърдение 12.2. *Ако $f = \sum_{i=0}^{l} a_i x^i$ и $g = \sum_{j=0}^{m} b_j x^j$ са полиноми на x с коефициенти a_i, b_j от поле k и степени $l, m \in \mathbb{N}$, то резултантата*

$$\mathrm{Res}(f,g,x) \in \mathbb{Z}[a_0, \ldots, a_l, b_0, \ldots, b_m]$$

е полином с цели коефициенти от коефициентите $a_0, \ldots, a_l, b_0, \ldots, b_m$ на f и g. Още повече, f и g имат общ делител $h \in k[x]$ от степен $\deg(h) > 0$ тогава и само тогава, когато $\mathrm{Res}(f,g,x) = 0$.

Доказателство: По определение, детерминантата

$$\det(X) = \sum_{\sigma \in S_n} (-1)^{[\sigma(1),\ldots,\sigma(n)]} x_{1,\sigma(1)} \ldots x_{n,\sigma(n)}$$

на квадратна матрица $X \in k_{n\times n}$ от ред n е полином с цели коефициенти на елементите на тази матрица. В частност, резултантата

$$\mathrm{Res}(f,g,x) = \det \mathrm{Syl}(f,g,x) \in \mathbb{Z}[a_0, \ldots, a_l, b_0, \ldots, b_m]$$

е полином с цели коефициенти на елементите $a_0, \ldots, a_l, b_0, \ldots, b_m$ на матрицата на Силвестър $\mathrm{Syl}(f,g,x)$.

Резултантата $\mathrm{Res}(f,g,x) = 0$ се анулира точно когато хомогенната линейна система (12.1) има ненулево решение. Вече отбелязахме, че това е еквивалентно на съществуването на полиноми $A, B \in k[x]$, изпълняващи условията (i) - (iii) от Лема 12.1. В такъв случай същата лема гарантира съществуването на общ делител $h \in k[x]$ от степен $\deg h > 0$ за $f, g \in k[x]$, Q.E.D.

Произволни полиноми $f, g \in k[x,y]$ могат да се разглеждат като полиноми $f = \sum_{i=0}^{l} f_i(y)x^i$, $g = \sum_{j=0}^{m} g_j(y)x^j$ на x с коефициенти $f_i(y), g_j(y) \in k[y] \subset k(y)$. Тогава резултантата $\mathrm{Res}(f,g,x) \in \mathbb{Z}[f_0(y), \ldots, f_l(y), g_0(y), \ldots, g_m(y)] \subset k[y]$ е полином на y Пресмятането на резултантата на $f, g \in k[x,y]$ относно x е операция, чрез която се елиминира x.

Твърдение 12.3. *За произволни полиноми $f, g \in k[x]$ от положителна степен съществуват полиноми $A, B \in k[x]$, така че*

$$Af + Bg = \mathrm{Res}(f, g, x).$$

Още повече, коефициентите на A и B са полиноми с цели коефициенти от коефициентите на f и g.

Доказателство: Ако $\mathrm{Res}(f, g, x) = 0$, то $A = B = 0$ изпълняват условията на твърдението.
Нека $\mathrm{Res}(f, g, x) \neq 0$, така че $f = \sum_{i=0}^{l} a_i x^i$ и $g = \sum_{j=0}^{m} b_j x^j$ нямат общ множител $h \in k[x]$ от степен $\deg h > 0$. Следователно най-големият общ делител $GCD(f, g) = 1$ и съществуват $\widetilde{A}, \widetilde{B} \in k[x]$, удовлетворяващи равенството

$$\widetilde{A}f + \widetilde{B}g = 1.$$

Търсим полиноми $\widetilde{A} = \sum_{i=0}^{m-1} \alpha_i x^i$ и $\widetilde{B} = \sum_{j=0}^{l-1} \beta_j x^j$ от степен $\deg \widetilde{A} = m - 1$, $\deg \widetilde{B} = l - 1$, така че

$$\widetilde{A}f + \widetilde{B}g = \sum_{i=0}^{l+m-1} \left(\sum_{s=0}^{i} a_{i-s}\alpha_s + b_{i-s}\beta_s \right) x^i = 1.$$

Сравнявайки коефициентите на x получаваме линейна система с $l + m$ уравнения на $l + m$ променливи $\alpha_0, \ldots, \alpha_{m-1}, \beta_0, \ldots, \beta_{l-1}$. Матрицата на тази линейна система съвпада с матрицата на Силвестър $\mathrm{Syl}(f, g, x)$, а стълбът на свободните членове е $c = (1, 0, \ldots, 0)^t$. Условието $\mathrm{Res}(f, g, x) = \det \mathrm{Syl}(f, g, x) \neq 0$ гарантира съществуването на единствено решение $(\alpha_0, \ldots, \alpha_{m-1}, \beta_0, \ldots, \beta_{l-1})$ по формулите на Крамер. По-точно,

$$\alpha_{i-1} = \frac{\det \mathrm{Syl}^{(i)}(f, g, x)}{\mathrm{Res}(f, g, x)}, \quad \beta_{j-1} = \frac{\det \mathrm{Syl}^{(m+j)}(f, g, x)}{\mathrm{Res}(f, g, x)},$$

където с $\mathrm{Syl}^{(t)}(f, g, x)$ е означена матрицата, получена от матрицата на Силвестър $\mathrm{Syl}(f, g, x)$ чрез замяна на t-тия стълб със стълба на свободните членове c. Както е обяснено в Твърдение 12.2, всяка от детерминантите

$$\det \mathrm{Syl}^{(t)}(f, g, x) \in \mathbb{Z}[a_0, \ldots, a_l, b_0, \ldots, b_m]$$

е полином с цели коефициенти от коефициентите $a_0, \ldots, a_l, b_0, \ldots b_m$ на f и g. По този начин, $A := \mathrm{Res}(f, g, x)\widetilde{A}$ и $B := \mathrm{Res}(f, g, x)\widetilde{B}$ се оказват полиноми на x, чиито коефициенти са от $\mathbb{Z}[a_0, \ldots, a_l, b_0, \ldots, b_m] \subseteq k$. Умножавайки почленно $\widetilde{A}f + \widetilde{B}g = 1$ с $\mathrm{Res}(f, g, x)$ получаваме

$$Af + Bg = \mathrm{Res}(f, g, x),$$

Q.E.D.
Да обясним накратко връзката между резултантата $\mathrm{Res}(f, g, x)$ и най-големия общ делител $GCD(f, g)$. Ако $\mathrm{Res}(f, g, x) \neq 0$, то f и g нямат общ множител $h \in k[x]$ от степен $\deg h > 0$, така че $GCD(f, g) = 1$. Тогава по Лема 11.5 съществуват $\widetilde{A}, \widetilde{B} \in k[x]$, така че

$$\widetilde{A}f + \widetilde{B}g = 1.$$

Съгласно Твърдение 12.3, полиномите $A := \mathrm{Res}(f, g, x)\widetilde{A}$ и $B := \mathrm{Res}(f, g, x)\widetilde{B}$ принадлежат на $k[x]$ и изпълняват равенството

$$Af + Bg = \mathrm{Res}(f, g, x).$$

Пример 12.4. *Полиномите* $f = xy - 1$ *и* $g = x^2 + y^2 - 4$ *от* $k[x, y]$ *имат резултанта*

$$\mathrm{Res}(f, g, x) = \det \begin{pmatrix} y & 0 & 1 \\ -1 & y & 0 \\ 0 & -1 & y^2 - 4 \end{pmatrix} = y^4 - 4y^2 + 1 \neq 0.$$

Следователно $GCD(f, g) = 1$. *Непосредствено се проверява, че*

$$-\left(\frac{y}{y^4 - 4y^2 + 1}x + \frac{1}{y^4 - 4y^2 + 1}\right) f + \frac{y^2}{y^4 - 4y^2 + 1} g = 1$$

в $k(y)[x]$. *Следователно*

$$-(yx + 1)f + y^2 g = y^4 - 4y^2 + 1 = \mathrm{Res}(f, g, x).$$

Произволни полиноми $f, g \in k[x_1, x_2, \ldots, x_n]$ могат да се представят като полиноми $f = \sum_{i=0}^{l} a_i x_1^i$, $g = \sum_{j=0}^{m} b_j x_1^j$ на x_1 с коефициенти $a_i, b_j \in k[x_2, \ldots, x_n]$. Ако f и g са от положителна степен относно x_1, то резултантата $\mathrm{Res}(f, g, x_1)$ относно x_1 е коректно определен полином от $k[x_2, \ldots, x_n]$. За да интерпретираме свойствата на резултантата $\mathrm{Res}(f, g, x_1)$ е необходимо да дадем следното

Определение 12.5. *Ако* I *е идеал в пръстена на полиномите* $k[x_1, x_2, \ldots, x_n]$ *с коефициенти от поле* k, *то* j*-тият елиминационен идеал* I_j *на* I *се определя като идеала*

$$I_j := I \cap k[x_{j+1}, \ldots, x_n]$$

в $k[x_{j+1}, \ldots, x_n]$ *за* $1 \leq j \leq n - 1$.

Съгласно Твърдение 12.3, ако f и g са полиноми на $x_1, x_2, \ldots, x_n$ от положителна степен относно x_1, то тяхната резултанта $\mathrm{Res}(f, g, x_1)$ относно x_1 принадлежи на първия елиминационен идеал $\mathrm{Res}(f, g, x_1) \in \langle f, g\rangle \cap k[x_2, \ldots, x_n] = I_1$ на $I := \langle f, g\rangle \triangleleft k[x_1, \ldots, x_n]$. Твърдение 12.2 уточнява, че $\mathrm{Res}(f, g, x_1) = 0$ тогава и само тогава, когато f и g имат общ множител $\widetilde{h} \in k(x_2, \ldots, x_n)[x_1]$, зависещ от x_1. Съгласно Следствие 11.9, това е еквивалентно на съществуването на общ множител $h \in k[x_1, x_2, \ldots, x_n]$, зависещ от x_1.