Contents

Motivation

We want to find the common divisor for $f(x), g(x)$

$$\begin{aligned} f(x) &= x^2-5x+6 \\ g(x) &= x^3-x-6 \end{aligned}$$

$$\underbrace{r(x)}_{\deg r<3} f(x) = \underbrace{s(x)}_{\deg s<2} g(x)$$

$$\begin{aligned} r(x) &= \alpha_2 x^2 + \alpha_1 x + \alpha_0 \\ s(x) &= \qquad\quad \beta_1 x + \beta_0 \end{aligned}$$

Lets expand $r(x)f(x)$

$$\begin{aligned} (\alpha_2x^2+\alpha_1x+\alpha_0)(1x^2-5x+6) = \alpha_2\cdot 1x^4 + \alpha_2\cdot(-5)x^3 &+ \alpha_2\cdot 6x^2 \\ +\alpha_1\cdot 1x^3 &+ \alpha_1(-5)x^2 + \alpha_1 6x \\ &+ \alpha_0\cdot 1x^2 \quad + \alpha_0(-5)x + \alpha_0 6 \end{aligned}$$

$$= (\alpha_2\alpha_1\alpha_0)\begin{pmatrix} 1 & -5 & 6 & 0 & 0 \\ 0 & 1 & -5 & 6 & 0 \\ 0 & 0 & 1 & -5 & 6 \end{pmatrix}$$

Likewise for $s(x)g(x)$

$$\begin{aligned} (\beta_1x+\beta_0)(1x^2-1x+6) = \beta_1\cdot 1x^4 &\qquad + \beta_1\cdot(-1)x^2 + \beta_1 6x \\ +\beta_0\cdot 1x^3 &\qquad\qquad + \beta_0(-1)x + \beta_0 6 \end{aligned}$$

$$= (\beta_1\beta_0)\begin{pmatrix} 1 & 0 & -1 & 6 & 0 \\ 0 & 1 & 0 & -1 & 6 \end{pmatrix}$$

Since $r(x)f(x) = s(x)g(x)$

$$(\alpha_2\alpha_1\alpha_0)\begin{pmatrix} 1 & -5 & 6 & 0 & 0 \\ 0 & 1 & -5 & 6 & 0 \\ 0 & 0 & 1 & -5 & 6 \end{pmatrix} = (\beta_1\beta_0)\begin{pmatrix} 1 & 0 & -1 & 6 & 0 \\ 0 & 1 & 0 & -1 & 6 \end{pmatrix}$$

$$\Rightarrow (\alpha_2\alpha_1\alpha_0| -\beta_1 - \beta_0)\left(\begin{array}{ccccc} 1 & -5 & 6 & 0 & 0 \\ 0 & 1 & -5 & 6 & 0 \\ 0 & 0 & 1 & -5 & 6 \\ \hline 1 & 0 & -1 & 6 & 0 \\ 0 & 1 & 0 & -1 & 6 \end{array}\right) = 0$$

Definition

$$S = \left(\begin{array}{ccccc} 1 & -5 & 6 & 0 & 0 \\ 0 & 1 & -5 & 6 & 0 \\ 0 & 0 & 1 & -5 & 6 \\ \hline 1 & 0 & -1 & 6 & 0 \\ 0 & 1 & 0 & -1 & 6 \end{array}\right)$$

This is the **Sylvester matrix**. More precisely given

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$$
$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0$$

$$S = \begin{pmatrix} a_n & a_{n-1} & \dots & a_0 & & & \\ & a_n & a_{n-1} & \dots & a_0 & & \\ & & \vdots & & & & \\ & & a_n & a_{n-1} & \dots & a_0 & \\ b_m & b_{m-1} & \dots & b_0 & & & \\ & b_m & b_{m-1} & \dots & b_0 & & \\ & & \vdots & & & & \\ & & b_m & b_{m-1} & \dots & b_0 & \end{pmatrix}$$

The resultant $R(f, g) = \det(S)$.

When $f(x)$ and $g(x)$ share a common divisor then $rf - sg = 0$ for some r, s, and hence $(\alpha_{m-1} \dots \alpha_0 | -\beta_{n-1} \dots -\beta_0$ has a solution.

We now follow the exercises of Dummit & Foote 14.6.29-31.

$R(f, g) = 0 \Leftrightarrow (f(x), g(x))$ are not Coprime

29a: Prove $f(x)$ and $g(x)$ have a common divisor $\Leftrightarrow \exists r(x), s(x) \in A[x] : r(x)f(x) = s(x)g(x)$ where $\deg r < m, \deg s < n$.

Assuming $f(x)$ and $g(x)$ share a single factor $(x - \gamma)$, then the remaining non-shared factors will be $\deg r = \deg g - 1 = m - 1$ and $\deg s = n - 1$.

29b: Prove there is a nontrivial solution iff $R(x, y) = \det S = 0$.

The coefficients of r, s are $m + n$ unknowns. This is a system of $m + n$ homogenous equations. We know that in such a system $\det S \neq 0$ means the trivial solution, whereas $\det S = 0$ means an infinite number of nontrivial solutions. Hence we can find the polynomials r, s.

$R(f, g)$ is a Linear Combination $r(x)f(x) + s(x)g(x)$

Remembering there are m followed by n rows.

$$S \begin{pmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \vdots \\ x \\ 1 \end{pmatrix} = \begin{pmatrix} a_n x^{n+m-1} + & a_{n-1} x^{n+m-2} + & \dots & a_0 x^{m-1} & & & \\ & a_n x^{n+m-2} + & a_{n-1} x^{n+m-3} + & \dots + & a_0 x^{m-2} & & \\ & & \vdots & & & & \\ & & a_n x^n + & a_{n-1} x^{n-1} + & \dots + & a_0 & \\ b_m x^{n+m-1} + & b_{m-1} x^{n+m-2} + & \dots & b_0 x^{n-1} & & & \\ & b_m x^{n+m-2} + & b_{m-1} x^{n+m-3} + & \dots + & b_0 x^{n-2} & & \\ & & \vdots & & & & \\ & & b_m x^m + & b_{m-1} x^{m-1} + & \dots + & b_0 & \end{pmatrix}$$

$$= \begin{pmatrix} x^{m-1} f(x) \\ x^{m-2} f(x) \\ \vdots \\ f(x) \\ x^{n-1} g(x) \\ x^{n-2} g(x) \\ \vdots \\ g(x) \end{pmatrix}$$

Let S' denote the matrix of cofactors. Then a basic rule of matrices is that

$$S'S = \det(S)I$$

Denote coefficients on the final row of S' as k_i

$$S' = \begin{pmatrix} & \cdots & \\ k_0 & \cdots & k_{m+n} \end{pmatrix}$$

Left multiply the above equations by S'

$$\begin{aligned} S'S \begin{pmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \vdots \\ x \\ 1 \end{pmatrix} &= \det(S) \begin{pmatrix} x^{n+m-1} \\ x^{n+m-2} \\ \vdots \\ x \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} x^{n+m-1}R(f,g) \\ x^{n+m-2}R(f,g) \\ \vdots \\ xR(f,g) \\ R(f,g) \end{pmatrix} \\ &= S' \begin{pmatrix} x^{m-1}f(x) \\ x^{m-2}f(x) \\ \vdots \\ f(x) \\ x^{n-1}g(x) \\ x^{n-2}g(x) \\ \vdots \\ g(x) \end{pmatrix} \end{aligned}$$

Observing the last row, we see

$$\begin{aligned} R(f,g) &= k_0x^{m-1}f(x) + k_1x^{m-2}f(x) + \cdots + k_{m-1}f(x) + k_mx^{n-1}g(x) + \cdots + k_{m+1}x^{n-2}g(x) + \cdots + k_{n+m-1}g(x) \\ &= r(x)f(x) + s(x)g(x) \end{aligned}$$

Reciprocity

We create the ring

$$\begin{aligned} A_0 &= R[a_n, b_m, x_1, \ldots, x_n, y_1, \ldots, y_m] \\ f(x) &= a_n(x - x_1)\cdots(x - x_n) \\ g(x) &= b_m(y - y_1)\cdots(y - y_m) \end{aligned}$$

So therefore a_n divides all the coefficients of $f(x)$.

31b: show $R(f,g)$ is $a_n^m b_m^n$ times a symmetric function in $x_1, \ldots, x_n, y_1, \ldots, y_m$.

Each coefficient of f is an elementary symmetric function of the roots $x_1, \ldots, x_n$. For example

$$(X - a)(X - b)(X - c) = X^3 - (a + b + c)X^2 + (ab + ac + bc)X - abc$$

We can use determinant expansion by minors to cancel a_n from the first m rows, then continue by cancelling b_m from the remaining n rows. We therefore see that $R(f,g)$ is a multiple of $a_n^m b_m^n$.

The remaining values which are the coefficients divided out are symmetric functions on the roots.

Therefore $R(f,g)$ is equal to $a_n^m b_m^n$ times a symmetric function of $x_1, \ldots, x_n, y_1, \ldots, y_m$.

31c: $R(f,g)$ is divisible by $(x_i - y_j)$.

$R(f,g)$ is 0 if f, g share a common root. This means when $f(x)$ and $g(x)$ share a root such that $x_i = y_j$ for some i, j then $R(f,g)$ must be zero.

Lets consider $R(f,g)$ as an indeterminate over x_k (same argument for y_k) then $R(f,g)$ will be 0 when $x_k = y_j$ for any y_j. Therefore we can divide $R(f,g) \in A[x_k]$ by $(x_k - y_j)$.

Applying this argument for all $x_i, y_j \in A_0$, we see that

$$R(f, g) = a_n^m b_m^n \prod_{i=1}^{n} \prod_{j=1}^{m} (x_i - y_j)$$

31d: final reciprocity

We can now very easily rewrite the above as

$$R(f, g) = a_n^m \prod_{i=1}^{n} g(x_i) = (-1)^{nm} b_m^n \prod_{j=1}^{m} f(y_j)$$

References

- Resultants, Discriminants, Bezout, Nullstellensatz, etc,