✱ Digression ✱✱ The Euler-Sylvester resultant (eliminant)

Lecture VI

K: field $\quad K[x]$: polynomials with coefficients in K

Recall: $f, g \in K[x] \Rightarrow \exists\, h \in K[x]$ s.t.

(i) $h \mid f$, $h \mid g$ $\quad$ ($\mid$: divides)

(ii) $k \mid f$, $k \mid g \Rightarrow k \mid h$

(iii) $\exists\, A, B \in K[x]$ such that $h = Af + Bg$

h: highest common divisor of f and g

✱ Euclidean algorithm

we shall take $K = \mathbb{C}$

Elimination theory

f and g as above have a common factor $\Leftrightarrow$ h is not a constant

In order to find a common factor, one could employ the Euclidean Algorithm; however, this is tedious in general.

Alternative route

the alternative convention can be chosen: $f = a_0 x^n + a_1 x^{n-1} + \dots a_n$, $n, m \geq 1$; the final result is unchanged

$$f = a_0 + a_1 x + \dots a_n x^n \qquad a_n \neq 0$$
$$g = b_0 + b_1 x + \dots b_m x^m \qquad b_m \neq 0$$

✱ **Theorem**: f and g have a common non-constant factor $\Leftrightarrow$ $\exists\ \phi, \psi$ (non-zero polynomials) $\deg \phi < n$, $\deg \psi < m$ such that

$$\psi \cdot f = \phi \cdot g$$

Proof. ($\Rightarrow$) $f = h\phi$, $g = h\psi \Rightarrow \psi \cdot f = \psi h \phi = \phi \cdot h\psi = \phi g$

($\Leftarrow$) Let $\psi f = \phi \cdot g$. Factor g: then its non constant factors appear in $\psi \cdot f$, but not all of them can appear in ψ, since $\deg \psi < g$, so at least one of them appears in f. Therefore f & g share a common non constant factor $\square$

Theorem f and g have a non constant factor $\iff$

determinant

$$R = \begin{vmatrix} a_0 & a_1 & \cdots & a_n & & 0 \\ & a_0 & \cdots & a_{n-1} & a_n & \\ 0 & & a_0 & \cdots & & a_n \\ b_0 & b_1 & \cdots & b_m & & 0 \\ & b_0 & \cdots & b_{m-1} & b_m & \\ 0 & & b_0 & \cdots & & b_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix} a \\ a \\ a \end{matrix}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{matrix} b \\ b \\ b \end{matrix}}\right\} n \text{ rows} \end{matrix} = 0$$

R : resultant (or eliminant) of f, g

(notation : $R_{f,g}$) R is a polynomial in a_i and b_j

Proof

Let $\psi f = \phi g$

$\phi = \alpha_1 + \alpha_2 x + \cdots \alpha_n x^{n-1}$ $(\alpha_1 \ldots \alpha_n) \neq (0 \ldots 0)$

$\psi = \beta_1 + \beta_2 x + \cdots \beta_m x^{m-1}$ $(\beta_1 \ldots \beta_m) \neq (0 \ldots 0)$

Then

$$\begin{cases} a_0 \beta_1 = b_0 \alpha_1 \\ a_1 \beta_1 + a_0 \beta_2 = b_1 \alpha_0 + b_0 \alpha_1 \\ \vdots \\ a_n \beta_m = b_m \alpha_n \end{cases}$$

$$\left\{ \begin{matrix} \beta_1 + \beta_2 x + \cdots \beta_m x^{m-1} & \psi \\ a_0 + a_1 x + \cdots a_n x^n & f \\ & \\ \alpha_1 + \alpha_2 x + \cdots \alpha_n x^{n-1} & \phi \\ b_0 + b_1 x + \cdots b_m x^{m-1} & g \end{matrix} \right.$$

caveat: multiply the columns involving the b's by -1 and transpose the resulting matrix

i.e we have a linear system in the unknowns $\beta_1 \ldots \beta_m, \alpha_1 \ldots \alpha_n$, possessing a non-trivial solution if and only if $R = 0$

→ Why is R also called eliminant ?

Let f and g have a common root x_0 : $f(x_0) = g(x_0) = 0$

From $a_0 + a_1 x_0 + a_2 x_0^2 + \cdots a_n x_0^n = 0$

$b_0 + b_1 x_0 + b_2 x_0^2 + \cdots b_m x_0^m = 0$

we can, via suitable multiplications, eliminate all powers x_0^i, eventually getting $R = 0$

★ Example

this is rather trivial, but let us go through the procedure

$$f = a_0 + a_1 x + a_2 x^2$$
$$g = a_1 + 2a_2 x \qquad (= f')$$

$$a_0 + a_1 x_0 + a_2 x_0^2 = 0$$
$$a_1 + 2a_2 x_0 = 0$$

$$2a_0 + 2a_1 x_0 + 2a_2 x_0^2 = 0$$
$$a_1 x_0 + 2a_2 x_0^2 = 0$$

$$\Rightarrow \qquad 2a_0 + a_1 x_0 = 0$$

$$\begin{cases} a_1 + 2a_2 x_0 = 0 \\ 2a_0 + a_1 x_0 = 0 \end{cases}$$

$$\rightarrow \quad a_1^2 + 2a_2 a_1 x_0 = 0$$
$$2a_0 a_2 + a_1 a_2 x_0 = 0$$
$$\rightarrow \quad 4a_0 a_2 + 2a_1 a_2 x_0 = 0$$

$$\boxed{a_1^2 - 4a_0 a_2 = 0}$$

$\Delta = 0$

f possiede una radice doppia

$R_{f,f'}$: discriminante

* Geometric interpretation

Let $\mathcal{C}$: $\begin{cases} x = \dfrac{P_1(t)}{Q_1(t)} \\ y = \dfrac{P_2(t)}{Q_2(t)} \end{cases}$ be a rational (affine) curve

Let $f = P_1(t) - x\,Q_1(t) \in (\mathbb{C}[x,y])[t]$

$g = P_2(t) - y\,Q_2(t)$ $\in$ polynomials in t with coefficients in $\mathbb{C}[x,y]$

then, if (x_0, y_0) is an image point of t,

then t is a common root of f and g

$\begin{cases} f = 0 \\ g = 0 \end{cases}$ Therefore $R_{f,g}(x_0, y_0) = 0$

Hence $R_{f,g}(x,y) = 0$ is the implicit equation of $\mathcal{C}$, obtained by eliminating t

Example $\begin{cases} x = t^2 \\ y = t^3 - t \end{cases}$ clearly if $t = x^{\frac{1}{2}}$ then $y = x^{\frac{1}{2}}(x-1)$

$y^2 = x(x-1)^2$

$y = x^{3/2} - x^{\frac{1}{2}}$

$= x^{\frac{1}{2}}(x-1)$

$y^2 = x(x-1)^2$

$\begin{cases} -x + t^2 = 0 \\ -y - t + t^3 = 0 \end{cases}$

$$0 = \begin{vmatrix} -x & 0 & 1 & 0 & 0 \\ 0 & -x & 0 & 1 & 0 \\ 0 & 0 & -x & 0 & 1 \\ -y & -1 & 0 & 1 & 0 \\ 0 & -y & -1 & 0 & 1 \end{vmatrix} = -x \begin{vmatrix} -x & 0 & 1 & 0 \\ 0 & -x & 0 & 1 \\ -1 & 0 & 1 & 0 \\ -y & -1 & 0 & 1 \end{vmatrix} + \begin{vmatrix} 0 & -x & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -y & -1 & 1 & 0 \\ 0 & -y & 0 & 1 \end{vmatrix} =$$

$$= \overbrace{-x(-x)}^{x^2} \underbrace{\begin{vmatrix} -x & 0 & 1 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{vmatrix}}_{-x+1} - x \cdot 1 \overbrace{\begin{vmatrix} 0 & -x & 1 \\ -1 & 0 & 0 \\ -y & -1 & 1 \end{vmatrix}}^{(+1)(-x+1)} + \underbrace{\begin{vmatrix} 0 & -x & 1 \\ -y & -1 & 1 \\ 0 & -y & 0 \end{vmatrix}}_{y^2}$$

$$x^2(1-x) - x(1-x) + y^2$$

$$= x(1-x)^2 + y^2$$

$$= x(x^2-1) + y^2$$

* Homogeneous polynomials

$$f(tx_1 \dots tx_r) = t^n f(x_1 \dots x_r) \qquad n = \deg f$$

$\Rightarrow$ each monomial is of degree n

* Euler: $$\sum x_i \frac{\partial f}{\partial x_i} = n f$$

more generally:

$$\sum_{I = (i_1 \dots i_s)} x_{i_1} \cdots x_{i_s} \frac{\partial^s F}{\partial x_{i_1} \cdots \partial x_{i_s}} = n(n-1)\cdots(n-s+1) F$$

$$\left[x^I \frac{\partial F}{\partial x^I} = n(n-1)\cdots(n-s+1) F \right]$$

from $F = F(x_1 \dots x_r)$ get its associate $F(1, \tilde{x}_1 \dots \tilde{x}_r)$ (and conversely) $\left(\tilde{x}_i = \frac{x_i}{x_1} \right)$

Theorem
$$F = a_0 x_0^n + a_1 x_0^{n-1} x_1 + \dots + a_n x_1^n$$
$$G = b_0 x_0^m + b_1 x_0^{m-1} x_1 + \dots + b_m x_1^m$$

have a common factor $\Leftrightarrow R_{F,G} = 0$ $\Rightarrow$ no limitations on coefficients

Proof. If $a_n = b_m = 0$, $R = 0$ and F and G have x_0 as a common factor

If $a_n b_m \neq 0$, work with their associated polynomials

If $a_n = 0$, $b_m \neq 0$, let $F = x_0^r F^*$, $x_0 \nmid F^*$ and use F^*, G [notice that every factor of a homogeneous polynomial is homogeneous as well]

The resultant R_{F^*G} differs from $R_{F,G}$ by a factor $\pm b_m^r$.

A similar argument holds for $a_n \neq 0$, $b_m = 0$ $\square$

Theorem

Let
$$F_n = A_n + A_{n-1} x_r + \dots A_0 x_r^n$$
$$G_m = B_m + B_{m-1} x_r + \dots B_0 x_r^m$$

with A_i, B_i homogeneous of degree i in $x_0 \dots x_{r-1}$ and $A_0 B_0 \neq 0$. Let $R(x_1 \dots x_{r-1})$ be the resultant of F_n and G_m w.r. to x_r.

Then either $R = 0$ or R is homogeneous of degree mn

Proof (direct computation)

$$R(tx_1 \dots tx_{r-1}) = \begin{array}{l} \\ m \text{ rows} \\ \\ \\ n \text{ rows} \\ \\ \end{array} \left| \begin{array}{cccccc} t^n A_n & t^{n-1} A_{n-1} & \cdots & A_0 & & \\ & t^n A_n & & tA_1 & A_0 & \\ & & \cdots & & & \\ & & t^n A_n & & & A_0 \\ t^m B_m & t^{m-1} B_{m-1} & \cdots & tB_1 & B_0 & \\ & & \cdots & & & \\ & & t^m B_m & \cdots & & B_0 \end{array} \right|$$

multiply the ith row by t^{m-i+1}

t^{n-j+1}

Then $R(tx_1 \dots tx_{r-1})$ is multiplied by
$$\sum_{i=1}^{m} (m-i+1) + \sum_{j=1}^{n} (n-j+1) = m^2 - \frac{m(m+1)}{2} + m + n^2 - \frac{n(n+1)}{2} + n$$
$$= \frac{m(m+1)}{2} + \frac{n(n+1)}{2} =: p$$

But, in turn, the r.h.s. becomes

$$
\begin{array}{c}
m\left\{\begin{array}{c} \\ \\ \\ \end{array}\right. \\
n\left\{\begin{array}{c} \\ \\ \end{array}\right.
\end{array}
\left|\begin{array}{ccccc}
t^{n+m}A_n & t^{n+m-1}A_{n-1} & \cdots & t^{m}A_0 & 0 \\
0 & t^{n+m-1}A_{n-1} & & t^{m}A_1 & t^{m-1}A_0 \\
 & & \cdots & & \\
 & \cdots & t^{n+1}A_n & \cdots & tA_0 \\
t^{n+m}B_m & t^{n+m-1}B_{m-1} & & t^{n+1}B_1 & \\
 & & \vdots & & \\
 & 0 & t^{m+1}B_m & \cdots & tB_0
\end{array}\right|
$$

i.e.

$$t^q \, R(x_1 \ldots x_{r-1}) \quad , \quad q = \sum_{k=1}^{n+m} k = \frac{(n+m)(n+m+1)}{2}$$

Thus $$q - p = \frac{1}{2}\left\{ n^2 + \overbrace{mn + nm}^{2mn} + m^2 + n + m - m^2 - m - n^2 - n \right\}$$

$$= \frac{1}{2} \cdot 2 \cdot mn = mn \qquad \square$$

Let $f = \prod_{i=1}^{n} (x - y_i)$ $g = \prod_{j=1}^{m} (x - z_j)$

Then $\boxed{R = \underset{\neq 0}{a} \prod_{i,j} (y_i - z_j)}$

Proof. If $x = z_1$, then $f = g = 0$

$\Rightarrow$ $y_1 - z_1$ is a common factor of f and g $\Rightarrow R = 0$. Similarly for $y_i - z_j$ $\forall i, j$

Therefore $\prod_{i,j} (y_i - z_j) \mid R$

but $\prod_{i,j} (y_i - z_j)$ and R are both homogeneous of degree mn $\Rightarrow$ $R = a \prod_{i,j} (y_i - z_j)$, $a \neq 0$

(since R does not vanish identically)

★ Discriminant of $f = ax^2 + bx + c$

$\parallel$

resultant of f and f'

$f' = 2ax + b$

$$\begin{array}{c} m\{ \\ \\ n\{ \\ \\ \end{array} \begin{vmatrix} c & b & a \\ b & 2a & 0 \\ 0 & b & 2a \end{vmatrix} = 4a^2c + \underbrace{ab^2 - 2ab^2}_{-ab^2}$$

$$= a(4ac - b^2)$$

$$(= -a\,\Delta_{old})$$

$\Delta_{old} = b^2 - 4ac$

$$\boxed{\Delta = a(4ac - b^2)}$$

Discriminant (= $\underset{\text{resultant}}{\text{eliminant}}$ of f and f')

of $x^3 + px + q$

Δ

$$f = q + px + 0x^2 + x^3$$
$$f' = p + 3x^2$$

$$f \to q \quad p \quad 0 \quad 1$$
$$f' \to p \quad 0 \quad 3 \quad 0$$

$$\begin{array}{c} m = 2 \left\{ \begin{array}{c} \\ \\ \end{array} \right. \\ n = 3 \left\{ \begin{array}{c} \\ \\ \\ \end{array} \right. \end{array} \begin{vmatrix} q & p & 0 & 1 & 0 \\ 0 & q & p & 0 & 1 \\ p & 0 & 3 & 0 & 0 \\ 0 & p & 0 & 3 & 0 \\ 0 & 0 & p & 0 & 3 \end{vmatrix} = q \begin{vmatrix} q & p & 0 & 1 \\ 0 & 3 & 0 & 0 \\ p & 0 & 3 & 0 \\ 0 & p & 0 & 3 \end{vmatrix} + p \begin{vmatrix} p & 0 & 1 & 0 \\ q & p & 0 & 1 \\ p & 0 & 3 & 0 \\ 0 & p & 0 & 3 \end{vmatrix}$$

$$= \underbrace{q \cdot 3 \begin{vmatrix} q & 0 & 1 \\ p & 3 & 0 \\ 0 & 0 & 3 \end{vmatrix}}_{27q^2} + p^2 \underbrace{\begin{vmatrix} p & 0 & 1 \\ 0 & 3 & 0 \\ p & p & 3 \end{vmatrix}}_{\underbrace{p \cdot 3 (\underbrace{3p - p}_{2p})}_{6p^3}} + p \begin{vmatrix} q & p & 1 \\ \cancel{p} & \cancel{0} & \cancel{0} \\ 0 & p & 3 \end{vmatrix}$$

$$\underbrace{-p^2 (\underbrace{3p - p}_{2p})}_{-2p^3}$$

$$= 4p^3 + 27q^2$$

$$\boxed{\Delta = 4p^3 + 27q^2}$$