



§5. Il Risultante di Sylvester

Q: $\mathbb{Z}(f) \cup \mathbb{Z}(g) = \mathbb{Z}(\exists?)$ Risposte: $? = f \cdot g$

Q: $\mathbb{Z}(f) \cap \mathbb{Z}(g) = \mathbb{Z}(\exists?)$ Risposte: proviamo con
i fattori comuni $\rightarrow ? := \text{GCD}(f, g)$. **MA:**

$f(x, y) = x, g(x, y) = y \Rightarrow \text{GCD}(f, g) = 1$ senza radici

anche se $(x, y) = (0, 0)$ è una radice comune $\rightarrow$ no.

$\Rightarrow$ Ci vuole una tecnologia più sofisticata.

LEMMA [BÉZOUT]

non ancora
il teorema
di Bézout

A UFD. Allora $f, g \in A[t]$ hanno un **fattore irriducibile** in comune se e soltanto se

$$f(t) \cdot \exists v(t) - g(t) \cdot \exists u(t) \equiv 0$$

$$\deg(v) < \deg(g)$$

$$\deg(u) < \deg(f)$$

Dim.: $\Rightarrow \exists h(t) : f = h \cdot u, g = h \cdot v, \deg(u) < \deg(f), \deg(v) < \deg(g)$
 $\Rightarrow fv = huv = gu \Rightarrow fv - gu \equiv 0.$

$\Leftarrow$ A UFD $\Rightarrow A[t]$ UFD $\Rightarrow (fv - gu \equiv 0 \Rightarrow \prod f_i^{m_i} \prod v_i^{k_i} \equiv \prod g_i^{l_i} \prod u_i^{p_i})$
e siccome $\deg(u) < \deg(f) \Rightarrow \exists g_i | f \Rightarrow h := g_i$ □

Lemma
Gauss

decompongo tutto
in irriducibili

Esempio chiaro / Definizione

$f, g \in A[t]$, A UFD e dominio d'integrità.

$$\begin{cases} f(t) = a_3 t^3 + a_2 t^2 + a_1 t + a_0 \\ g(t) = b_2 t^2 + b_1 t + b_0 \end{cases}$$

Cerchiamo:

$$\begin{cases} u(t) = \gamma t^2 + \delta t + \varepsilon \\ v(t) = \alpha t + \beta \end{cases}$$

$\leftarrow \deg(u) < 3$
 $\leftarrow \deg(v) < 2$

tali che:

$$(a_3 t^3 + a_2 t^2 + a_1 t + a_0)(\alpha t + \beta) - (b_2 t^2 + b_1 t + b_0)(\gamma t^2 + \delta t + \varepsilon) = 0$$

Basta
espandere
 $\rightarrow$

$$\begin{cases} a_3 \alpha - b_2 \gamma = 0 \\ a_2 \alpha + a_3 \beta - b_1 \gamma - b_2 \delta = 0 \\ a_1 \alpha + a_2 \beta - b_0 \gamma - b_1 \delta - b_2 \varepsilon = 0 \\ a_0 \alpha + a_1 \beta - b_0 \delta - b_1 \varepsilon = 0 \\ a_0 \beta - b_0 \varepsilon = 0 \end{cases}$$

sistema lineare:
5 eq & 5 incognite
 $\Rightarrow$ ammette soluzioni non
banali $\Leftrightarrow \det(\dots) = 0$

Ovvero abbiamo una soluzione non banale se e solo se

$$\det \begin{pmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_2 & b_1 & b_0 \end{pmatrix} = 0$$

è la matrice
dei coefficienti
del sistema lineare
sopra, a cui
abbiamo
semplicemente
applicato una
TRASPOSIZIONE
e moltiplicato
alcune righe per (-1)
PER COMODITÀ/CONVENZIONE

Chiamiamole **Syl(f, g)**
[Matrice di Sylvester]

Concludere (per il Lemme di Bézout e argomento sopra)

f, g hanno fattore
irriducibile comune



$$\det(\text{Syl}(f, g)) = 0$$

$=: R(f, g)$ RESULTANTE
DI SYLVESTER -4-

DEF $f, g \in A[t]^{\times}$ ^{non nulli}, A UFD, $f(t) = \sum_{i=0}^n a_i t^i$, $g(t) = \sum_{j=0}^m b_j t^j$.

La **MATRICE di SYLVESTER** è:

$$\text{Syl}(f, g) := \begin{pmatrix} a_n & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 \\ \hline b_m & b_{m-1} & b_{m-2} & \cdots & b_0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & b_m & b_{m-1} & b_{m-2} & \cdots & b_0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & b_m & b_{m-1} & b_{m-2} & \cdots & b_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & b_m & b_{m-1} & b_{m-2} & \cdots & b_0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & b_m & b_{m-1} & b_{m-2} & \cdots & b_0 \end{pmatrix} \in M_{n \times m}(A)$$

È il **RISULTANTE di SYLVESTER** è:

$$R(f, g) := \det(\text{Syl}(f, g))$$

TEO

A di integrità e UFD, $f, g \in A[t]^*$. Allora

$$\deg(\text{GCD}(f, g)) > 1 \iff R(f, g) = 0$$

le condizione dominio di integrità
ci assicura che soluz. non banali
del sistema siano non banali sia per u che per v : se $v=0, u \neq 0$
allora $fv = gu \Rightarrow gu = 0 \Rightarrow g = 0$ contraddizione.

Q.: come facciamo se vogliamo una radice in comune?

PROP $K = \bar{K}$, $f, g \in K[t]^*$. Allora:

$$f(\exists t_0) = 0 = g(t_0) \iff R(f, g) = 0$$

Dim.: $K \Rightarrow \text{UFD} \wedge \text{integrità}$. $\Leftarrow) R(f, g) = 0 \Rightarrow \exists h$ IRRID. COMUNE ma

$$K = \bar{K} \Rightarrow \deg(h) = 1 \Rightarrow h(t) = (t - \alpha)^1 \Rightarrow \alpha = t_0.$$

$$\Rightarrow f(t_0) = 0 = g(t_0) \xrightarrow{\text{RUFFINI}} (t - t_0) \mid f \wedge (t - t_0) \mid g \Rightarrow h(t) := (t - t_0)$$

□

§ 6.2. $\Delta :=$ il Discriminante

(DEF) $f \in A[t]$, A UFD a di integrità. Il suo **DISCRIMINANTE** è:

$$\Delta(f) := R(f, f')$$

(PROP) $K = \bar{K}$. $f \in K[t]^*$, $\deg(f) \geq 1$, allora:

$$f \text{ HA UNA RADICE MULTIPLA} \iff \Delta(f) = 0$$

$$\text{Dim.: } \Rightarrow) f(t) = (t - t_0)^{m \geq 2} \cdot g(t) \Rightarrow f'(t) = (t - t_0)^{m-1 \geq 1} \cdot h(t)$$

$$\Rightarrow f(t_0) = f'(t_0) = 0 \Rightarrow R(f, f') = 0 \xrightarrow{\text{DEF}} \Delta(f) = 0$$

PROP PREC.

$$\Leftarrow) \Delta(f) = 0 \Rightarrow R(f, f') = 0 \xrightarrow{K = \bar{K}} f \text{ e } f' \text{ hanno una radice in comune } t_0$$

RUFFINI

$$\xrightarrow{\text{RUFFINI}} f(t) = (t - t_0) \cdot g(t) \xrightarrow{\text{PROP PREC.}} f'(t) = (t - t_0)g'(t) + g(t) \text{ ma } f'(t_0) = 0$$

RUFFINI

$$\Rightarrow (t - t_0) \mid g(t) \xrightarrow{\text{L'ESIM}} g(t) = (t - t_0) \cdot h(t) \Rightarrow f(t) = (t - t_0)^2 \cdot h(t)$$

□

Esempio:

deg=2

$$f(t) = at^2 + bt + c \Rightarrow \Delta(f) = \det \begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix} = (-a) \cdot (b^2 - 4ac)$$

controlle che
sia davvero di
deg=2

discriminante
studiato a
squadra

deg=3

$f(t) = t^3 + at + b$ [forma di Tschirnhaus, ogni polinomio di deg=3 può essere messo in questa forma tramite l'affinità $t \mapsto t - a_1/3$ applicata a $f(t) = t^3 + a_1 t^2 + a_2 t + a_3$]

$$\Rightarrow \Delta(f) = \det \begin{pmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{pmatrix} = -(4a^3 + 27b^2)$$

è omogeneo?

[Invece per una cubica generica $f(t) = at^3 + bt^2 + ct + d$ sarebbe
 $\Delta(f) = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd$
se $a=0$, specializza al grado 2?

deg=4

$f(t) = t^4 + at^2 + bt + c$ [di nuova forma semplificata da monicità e affinità per eliminare il coeff cubico]

$$\Rightarrow \Delta(f) = 16b(a^2 - 4c)^2 + 4ab^2(36c - a^2) - 27b^4$$

È COSÌ
VIA!

→ Abbiamo uno strumento per generare DISCRIMINANTI.

§ 6.3. Risultante in più indeterminate

Q.: Come si fa per $f, g \in A[x_1, \dots, x_n]$? Pensiamo $f, g \in D[x_n]$.
UFD $\wedge$ integrità
 *$D = A[x_1, \dots, x_{n-1}]$
 ancora UFD integrità*

DEF A UFD $\wedge$ integrità, $D := A[x_1, \dots, x_{n-1}]$, $f, g \in D[x_n]$

$$F(x_n) := \sum_{i=0}^r A_i x_n^i, \quad G(x_n) := \sum_{j=0}^s B_j x_n^j \quad A_i, B_j \in D$$

RISULTANTE di f, g
 nella indeterminata
 x_n

$$R_{x_n}(f, g) := \det$$

$$\begin{pmatrix} A_r & A_{r-1} & A_{r-2} & \cdots & A_0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & A_r & A_{r-1} & A_{r-2} & \cdots & A_0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & A_r & A_{r-1} & A_{r-2} & \cdots & A_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & A_r & A_{r-1} & A_{r-2} & \cdots & A_0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & A_r & A_{r-1} & A_{r-2} & \cdots & A_0 \\ \hline B_s & B_{s-1} & B_{s-2} & \cdots & B_0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & B_s & B_{s-1} & B_{s-2} & \cdots & B_0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & B_s & B_{s-1} & B_{s-2} & \cdots & B_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & B_s & B_{s-1} & B_{s-2} & \cdots & B_0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & B_s & B_{s-1} & B_{s-2} & \cdots & B_0 \end{pmatrix} \in D$$

OSS $\mathbb{K}$. $(\mathbb{Z}(f), f), (\mathbb{Z}(g), g)$ curve algebriche piane affini.

Vogliamo studiare $R_y(f, g) =: R(x)$

① $R(x) \equiv 0 \Rightarrow \exists h(x, y) \mid f, h(x, y) \mid g, \deg_y(h) \geq 1 \Rightarrow$
 $\mathbb{Z}(h)$ è componente comune di $\mathbb{Z}(f)$ e di $\mathbb{Z}(g)$
*↗ ovvero componente
di $\mathbb{Z}(f) \cap \mathbb{Z}(g)$*

② $R(x) = \text{const} \neq 0 \Rightarrow \forall x_0 \in \mathbb{K} \quad f(x_0, y), g(x_0, y)$
non hanno comp. irriducibili comuni $\Rightarrow$ a fortiori no
radici comuni $\Rightarrow \mathbb{Z}(f) \cap \mathbb{Z}(g) = \emptyset$
*↗ non è detto che esistano
se $\mathbb{K} \neq \bar{\mathbb{K}}$*

③ $\deg(R(x)) \geq 1 \Rightarrow \forall x_0$ tale che $R(x_0) = 0$, **SE** sia
↖ $|\mathbb{Z}(f) \cap \mathbb{Z}(g)| < \infty!$ $f(x_0, y)$ che $g(x_0, y)$ sono polinomi non costanti
in $y \Rightarrow$ hanno una componente irriducibile in y in comune.
Per ogni tale componente irriducibile di grado ≥ 1 , si
ha una radice $y_0 \Rightarrow (x_0, y_0) \in \mathbb{Z}(f) \cap \mathbb{Z}(g)$ e
collezionando tutte queste radici si ottiene $\mathbb{Z}(f) \cap \mathbb{Z}(g)$

Esempio: $f(x,y) = (1-x)y^2 + y + 1$. $g(x,y) = (1-x)y + 1$.

$$\Rightarrow R_y(f,g) = \det \begin{pmatrix} 1-x & 1 & 1 \\ 1-x & 1 & 0 \\ 0 & 1-x & 1 \end{pmatrix} = (1-x)^2 =: R(x) \Rightarrow \deg(R(x)) \geq 1$$

$\Rightarrow$ Supponiamo che $|Z(f) \cap Z(g)| < +\infty$ e andiamo a vedere di quanti punti è fatto l'insieme $Z(f) \cap Z(g)$

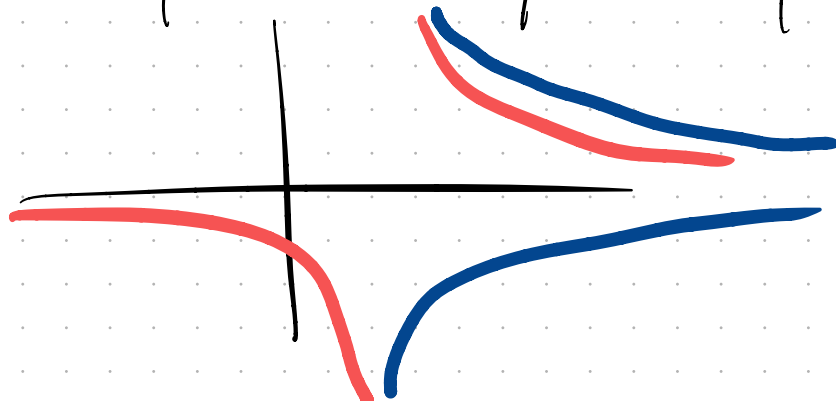
$$R(x_0) = 0 \Rightarrow x_0 = 1 \Rightarrow f(x_0, y) = y + 1, g(x_0, y) = 1$$

e non hanno zeri comuni perché $g(x_0, y)$ è costante

$$\Rightarrow \nexists (x_0, y_0) \in Z(f) \cap Z(g) \Rightarrow Z(f) \cap Z(g) = \emptyset !$$

Questo è accaduto anche se $\deg(R(x)) \geq 1$.

Non accadrà nel proiettivo per campi algebricamente chiusi



§ 6.4. Risultante di polinomi omogenei

(PROP) $F \in K[x_0, \dots, x_n]_{r \geq 1}$, $G \in K[x_0, \dots, x_n]_{s \geq 1}$. Allora

$$R_{x_n}(F, G) = \begin{cases} \equiv 0 & \text{se } F, G \text{ hanno componente} \\ & \text{irriducibile in comune} \\ R \in K[x_0, \dots, x_{n-1}]_{r \cdot s} & \text{altrimenti} \end{cases}$$

TERTIUM NON DATUR! Nel caso proiettivo / omogeneo non c'è il caso costante o polinomio di grado inferiore al prodotto.

Dim.: Al solito $F = \sum_{i=0}^r A_i x_n^i$, $G = \sum_{j=0}^s B_j x_n^j$, $A_r \neq 0 \neq B_s$.

Basta mostrare che:

$$R(tx_0, tx_1) = t^{rs} \cdot R(x_0, x_1) \quad \text{con } R(x_0, x_1) = R_{x_2}(F, G)$$

per $n > 2$ è uguale (ma più lungo da scrivere)
include il caso F, G componente comune $\Rightarrow R \equiv 0$ da Prop PRECEDENTE.

Allora posto da $R(tx_0, tx_1) =$

$$\begin{pmatrix} A_r(tx_0, tx_1) & A_{r-1}(tx_0, tx_1) & \dots & A_0(tx_0, tx_1) & 0 & 0 & 0 & \dots & 0 \\ 0 & A_r(tx_0, tx_1) & A_{r-1}(tx_0, tx_1) & \dots & A_0(tx_0, tx_1) & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & A_r(tx_0, tx_1) & A_{r-1}(tx_0, tx_1) & A_{r-2}(tx_0, tx_1) & \dots & A_0(tx_0, tx_1) \\ B_s(tx_0, tx_1) & B_{s-1}(tx_0, tx_1) & \dots & 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & B_s(tx_0, tx_1) & B_{s-1}(tx_0, tx_1) & \dots & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 & 0 & B_s(tx_0, tx_1) & \dots & B_0(tx_0, tx_1) \end{pmatrix}$$

E moltiplico ogni riga per un'opportuna potenza di t .
 Riesci a trovare la potenza giusta per ogni riga?
 [soluz sulle note]. Poi usando la multilinearità del determinante e l'omogeneità dei coefficienti A_j, B_j
 si trova che $R(tx_0, tx_1) = t^{rs} R(x_0, x_1)$.

$$A_i(tx_0, tx_1) = t^{r-i} A_i(x_0, x_1)$$

$$B_j(tx_0, tx_1) = t^{s-j} B_j(x_0, x_1)$$



Domanda: cosa significa $A_r \neq 0 \neq B_s$?

Osserviamo che $A_r = F(0,0,1) \wedge B_s = G(0,0,1)$, allora

$$A_r \neq 0 \Leftrightarrow (0:0:1) \notin Z_p(F)$$

$$B_s \neq 0 \Leftrightarrow (0:0:1) \notin Z_p(G)$$

Questo ci sarà molto utile nel prossimo capitolo

PROP $F \in K[x_0, \dots, x_n]_{r \geq 1}$, $G \in K[x_0, \dots, x_n]_{s \geq 1}$, $\text{GCD}(F, G) = 1$. Allora

$$|Z_p(F) \cap Z_p(G)| < +\infty$$

Dim.: Se $(c_0:c_1:c_2) \in Z_p(F) \cap Z_p(G) \Rightarrow F(c_0, c_1, c_2) = 0, G(c_0, c_1, c_2) = 0$ hanno la radice c_2 in comune $\Rightarrow R_{x_2}(F, G)(c_0, c_1) = 0$ e siccome $(0:0:1) \notin Z_p(F), Z_p(G) \Rightarrow (c_0:c_1) \neq (0,0)$.

Quindi abbiamo mostrato che ad ogni elemento di $\mathbb{Z}_p(F) \cap \mathbb{Z}_p(G)$ corrisponde una radice di $R_{x_2}(F, G)$.

$\text{GCD}(F, G) = 1 \xRightarrow{\text{PROP 15.5C}} \deg(R_{x_2}(F, G)) = r \cdot s \geq 1 \Rightarrow R_{x_2}(F, G) \text{ non costante}$
con al più $r \cdot s$ radici, quindi un numero finito.

Infine ad ogni $(c_0 : c_1) : R_{x_2}(F, G)(c_0, c_1) = 0$ possiamo corrispondere al più un numero finito di c_2 tali che $(c_0 : c_1 : c_2) \in \mathbb{Z}_p(F) \cap \mathbb{Z}_p(G)$ altrimenti F, G avrebbero un numero infinito di radici in comune come pol in $x_2 \Rightarrow F \equiv 0 \equiv G$ contraddizione. $\square$

Segue immediatamente:

(COR) [LEMMA di STUDY] $F \in K[x_0, x_1, x_2]_{r \geq 1}, G \in K[x_0, x_1, x_2]_{s \geq 1}$

$$|\mathbb{Z}_p(F) \cap \mathbb{Z}_p(G)| = +\infty \Rightarrow \deg(\text{GCD}(F, G)) \geq 1$$

In particolare se G irriducibile $\Rightarrow G \mid F$ e $\mathbb{Z}_p(G) \subset \mathbb{Z}_p(F)$.

