

Capitolo 1

Curve algebriche piane

1.1 Curve affini, riducibilità

Mettiamoci in uno spazio affine $\mathbf{A}^n(\mathbf{K})$ e adottiamo un sistema di riferimento $\mathcal{R} = \{\mathbf{O}, \langle \underline{a}_1, \dots, \underline{a}_n \rangle\}$. Se abbiamo una funzione

$$f : \mathbf{K}^n \rightarrow \mathbf{K}$$

possiamo considerarla definita sullo spazio affine (grazie all'isomorfismo tra le n -uple di \mathbf{K}^n e i punti di $\mathbf{A}^n(\mathbf{K})$):

$$f : \mathbf{A}^n(\mathbf{K}) \rightarrow \mathbf{K}.$$

Le funzioni che si studiano in questo contesto sono quelle polinomiali:

$$f \in \mathbf{K}[x_1, \dots, x_n].$$

Sappiamo che si può associare ad ogni polinomio f la rispettiva funzione polinomiale \tilde{f} , e sarà

$$\tilde{f}(\alpha_1, \dots, \alpha_n) \in \mathbf{K}.$$

D'ora in poi ci piacerà confondere i polinomi con le funzioni polinomiali, anche se in realtà può capitare che sia $f \neq g$ e tuttavia $\tilde{f} = \tilde{g}$.

Esempio Sia $\mathbf{K} = \mathbb{Z}_p$ con p primo, $n = 2$. Consideriamo i polinomi:

$$\begin{aligned} f(x, y) &= (x^p - x)y + x + y \\ g(x, y) &= x + y \end{aligned}$$

Chiaramente $f \neq g$ (hanno grado diverso), ma $\forall (\alpha, \beta) \in \mathbb{Z}_p^2$ si ha $\tilde{f}(\alpha, \beta) = \tilde{g}(\alpha, \beta)$.

Per nostra fortuna, però, l'identificazione è comunque possibile se il campo ha infiniti elementi.

Lemma Sia $f \in \mathbf{K}[x_1, \dots, x_n]$. Se $|\mathbf{K}| = \infty$ allora $\tilde{f} \equiv 0 \Rightarrow f = 0$.

Dimostrazione La dimostrazione è possibile per induzione su n ; qui ci limiteremo a mostrare il meccanismo per i primi due casi.

(n = 1) $f \in \mathbf{K}[x]$.

$$f(x) = a_0 x^t + a_1 x^{t-1} + \dots + a_t$$

Se $t = 0$ la tesi è ovvia. Proviamo a supporre $t \geq 1$.

$\tilde{f}(\alpha) = 0 \forall \alpha \in \mathbf{K} \Rightarrow f$ ha infinite radici, assurdo.

(n = 2) $f \in \mathbf{K}[x, y]$. Consideriamo $f \in \mathbf{K}[x][y]$:

$$f(x, y) = a_0(x)y^\delta + a_1(x)y^{\delta-1} + \dots + a_\delta(x) \quad a_0(x) \neq 0 \quad \delta \geq 1$$

$\exists \bar{\alpha} : \tilde{a}_0(\bar{\alpha}) \neq 0$. Definiamo:

$$p(y) = \tilde{a}_0(\bar{\alpha})y^\delta + \tilde{a}_1(\bar{\alpha})y^{\delta-1} + \dots + \tilde{a}_\delta(\bar{\alpha})$$

$$\tilde{p}(\beta) = 0 \quad \forall \beta \in \mathbf{K} \quad \tilde{p}(\beta) = \tilde{f}(\bar{\alpha}, \beta)$$

Quindi f avrebbe infinite radici, assurdo. \square

Proposizione 1.1 Siano $f, g \in \mathbf{K}[x_1, \dots, x_n]$ con $|\mathbf{K}| = \infty$. Allora

$$\tilde{f} = \tilde{g} \Rightarrow f = g.$$

Dimostrazione $\tilde{f} = \tilde{g} \Rightarrow \tilde{f} - \tilde{g} \equiv 0 \Rightarrow \widetilde{(f - g)} \equiv 0 \Rightarrow f - g = 0 \Rightarrow f = g$. \square

Sia ora $|\mathbf{K}| = \infty$, in sostanza $\mathbf{K} = \mathbb{R}$ o $\mathbf{K} = \mathbb{C}$. Sia $f \in \mathbf{K}[x_1, \dots, x_n]$.

Definizione 1.1 Chiamiamo *luogo degli zeri* di f

$$Z(f) = \{P \in \mathbf{A}^n(\mathbf{K}) : f(P) = 0\}.$$

Supponiamo di avere due polinomi $f \neq g$. Può capitare $Z(f) = Z(g)$? Ahinoi, sì.

Esempi

- $g = \sigma f$, $\sigma \in \mathbf{K}^*$ (caso irrilevante).
- $f = x$, $g = x^2$.
- $\mathbf{K} = \mathbb{R}$, $f(x, y) = (x^2 + y^2 + 1)(x - y)$, $g(x, y) = x - y$.

Da queste situazioni non ci possiamo liberare. Per questo l'oggetto del nostro studio saranno le coppie $(Z(f), f)$.

Definizione 1.2 Le coppie $(Z(f), f)$ sono dette *ipersuperfici algebriche affini*; in \mathbf{A}^2 si parla di *curve algebriche affini*. Il luogo degli zeri $Z(f)$ è detto *supporto*.

Digressione Questo è un caso particolare delle *varietà algebriche affini*, definite a partire da un ideale $I \subseteq \mathbf{K}[x_1, \dots, x_n]$ con

$$V(I) = \{P \in \mathbf{A}^n(\mathbf{K}) : f(P) = 0 \forall f \in I\}.$$

Noi consideriamo solo gli ideali principali, ma si noti che anche nel caso più generale si lavora con anelli nötheriani, sicché ogni ideale è comunque finitamente generato.

Vogliamo ora definire la *decomposizione* di una curva. Sia $f \in \mathbf{K}[x, y]$. Sappiamo che un anello di polinomi su un campo è un anello gaussiano o UFD, quindi un polinomio ha un'unica fattorizzazione:

$$f = f_1^{\mu_1} f_2^{\mu_2} \dots f_t^{\mu_t},$$

con gli f_i irriducibili.

Osservazione La fattorizzazione è *essenzialmente* unica, quindi ad esempio

$$f(x, y) = (x - y)(x + y) = \frac{1}{2}(x - y) \cdot 2(x + y).$$

Non faremo troppo caso a questo: la fattorizzazione è unica e ci basta.

Proposizione 1.2 $Z(fg) = Z(f) \cup Z(g)$.

Dimostrazione $(fg)(P) = 0 \Leftrightarrow f(P) \cdot g(P) = 0$. Siccome un campo è privo di divisori dello zero, questo vuol dire $P \in Z(f)$ o $P \in Z(g)$. \square

Proposizione 1.3 $Z(f) = Z(f^\mu)$.

Sia ora $C = (Z(f), f)$ una curva. Consideriamo la fattorizzazione:

$$\begin{aligned} Z(f) &= Z(f_1^{\mu_1}) \cup \dots \cup Z(f_t^{\mu_t}) = Z(f_1) \cup \dots \cup Z(f_t) \\ C_i &= (Z(f_i), f_i) \end{aligned}$$

Scriveremo dunque che C ha decomposizione

$$C = \mu_1 C_1 \cup \dots \cup \mu_t C_t,$$

dove le μ_i sono dette *molteplicità* delle componenti irriducibili.

Definizione 1.3 Se $t = 1$, C è *irriducibile*.

Osservazione Potrebbe essere $f = f_1^3 \Rightarrow t = 1$, $\mu_1 = 3$, nel qual caso il polinomio è riducibile mentre la curva è irriducibile.

Definizione 1.4 Se $\mu_1 = \dots = \mu_t = 1$, C è *ridotta*.

Per studiare le curve potremo limitarci alle irriducibili ridotte.

Osservazione La fattorizzazione non è unica, e.g.

$$Z(f) = Z(f_1) \cup \dots \cup Z(f_n) \cup \emptyset.$$

Se in generale la fattorizzazione non è unica, sotto particolari ipotesi possiamo avvalerci del seguente risultato per considerarla tale.

Lemma (di Study) Siano $f, g \in \mathbb{C}[x, y]$, con g irriducibile. Allora

$$Z(g) \subseteq Z(f) \Rightarrow g \mid f.$$

Esempi È importante che si verifichino le ipotesi prescritte, pena cadere in fallo.

- Se $K = \mathbb{R}$:

$$\begin{aligned} g(x, y) &= x^2 + y^2 + 1 \\ f(x, y) &= x + y \end{aligned}$$

Ora, $\emptyset = Z(g) \subseteq Z(f)$, ma $g \nmid f$.

- Prendendo un polinomio non irriducibile:

$$\begin{aligned} g(x, y) &= x^2 \\ f(x, y) &= x \end{aligned}$$

Ancora, $Z(g) \subseteq Z(f)$ ma $g \nmid f$.

Lo scopo della prima parte del corso sarà studiare i luoghi degli zeri. Useremo sempre un \mathbf{E}^2 reale e fisseremo sempre il sistema di riferimento usuale. Nondimeno, le definizioni che daremo saranno sempre riferite al piano affine complesso $\mathbf{A}^2(\mathbb{C})$.

Esempio Un polinomio verrà studiato in \mathbb{C} :

$$f(x, y) = (x^2 + y^2)(x + y - 1) = (x + iy)(x - iy)(x + y - 1).$$

Se poi vorremo rappresentare il luogo degli zeri lo faremo nel piano euclideo reale.

Definizione 1.5 Si dice *ordine* di una curva $C = (Z(f), f)$

$$\text{ord } C = \text{deg } f.$$

Ha senso chiedersi se le nostre curve sono invarianti per affinità. Consideriamo un'affinità $\alpha : \mathbf{A}^2 \rightarrow \mathbf{A}^2$ che trasformi (x, y) in (x', y') .

$$\alpha : \begin{cases} x' = ax + by + c \\ y' = dx + ey + h \end{cases} \quad \begin{vmatrix} a & b \\ d & e \end{vmatrix} \neq 0$$

$$\alpha^{-1} : \begin{cases} x = a'x' + b'y' + c' \\ y = d'x' + e'y' + h' \end{cases}$$

Ora chiediamoci: cos'è $\alpha(C)$?¹ Chiamiamo

$$\alpha(C) = C'.$$

$$P' \equiv (x', y') \in \alpha(C) \iff \alpha^{-1}(P') \in C$$

Questo è facilmente scrivibile:

$$\underbrace{f(a'x' + b'y' + c', d'x' + e'y' + h')}_{f'(x', y')} = 0.$$

Pertanto $C' = (Z(f'), f')$.

Ci domandiamo ora se α conserva l'ordine di C . Notiamo cosa avviene per ogni singolo termine:

$$f = \dots + qx^\alpha y^\beta + \dots$$

$$f' = \dots + q(a'x' + b'y' + c')^\alpha (d'x' + e'y' + h')^\beta + \dots$$

Pertanto il grado non può aumentare:

$$\text{deg } f \geq \text{deg } f'.$$

Ma α è biunivoca, quindi dall'applicazione dell'affinità inversa ricaviamo anche

$$\text{deg } f' \geq \text{deg } f,$$

da cui l'uguaglianza.

Possiamo applicare lo stesso ragionamento al numero di fattori di f :

$$f = g\tilde{g} \quad \text{due fattori}$$

$$f' = g'\tilde{g}' \quad \text{almeno due fattori}$$

Questo ragionamento si generalizza: il numero di fattori irriducibili si conserva.

Esercizio 1.1.1 Anche la molteplicità è conservata.

Morale: tutte le proprietà che introdurremo sono invarianti per affinità.

¹Piccolo abuso di notazione: intendiamo $Z(f)$, non la coppia.

1.2 Passaggio alla chiusura proiettiva

Il passaggio alla chiusura proiettiva è utile per dedurre proprietà facendo uso degli strumenti proiettivi; si tratta di una strategia molto comoda per ottenere una gran mole d'informazioni.

$$\begin{array}{ccc} \mathbf{E}^2 & \hookrightarrow & \mathbf{A}^2(\mathbb{C}) \\ \downarrow & // & \downarrow \\ \mathbf{P}^2(\mathbb{R}) & \hookrightarrow & \mathbf{P}^2(\mathbb{C}) \end{array}$$

$\mathbf{P}^2(\mathbb{C})$ è l'ambito giusto dove studiare tutte le curve, anche se si tratta di curve del piano affine o euclideo. Solo che adesso bisogna rivedere quanto fatto finora nel piano proiettivo.

Consideriamo $f \in \mathbf{K}[X, Y, U]$. Subito si presenta un problema:

$$\begin{array}{ll} f = X^2 + Y + U & \mathbf{P} \equiv (a : b : c) \\ f(\mathbf{P}) = a^2 + b + c = 0 & \mathbf{P} \equiv (\rho a : \rho b : \rho c) \quad \rho \in \mathbf{K}^* \end{array}$$

Sarà vero anche che

$$f(\mathbf{P}) = \rho^2 a^2 + \rho b + \rho c = a^2 + b + c = 0 ?$$

In verità, non lo sappiamo. C'è però una via d'uscita: considerare solo polinomi omogenei (che d'ora in avanti indicheremo con lettere maiuscole).

$$\begin{array}{l} F \in \mathbf{K}[X, Y, U] \quad \text{omogeneo} \\ F = F(X : Y : U) \end{array}$$

Definizione 1.6 Le coppie $(Z(F), F)$ sono dette *curve algebriche proiettive*.

Anche qui F ammette decomposizione, con gli F_i irriducibili,

$$F = F_1^{u_1} \dots F_t^{u_t}.$$

C'è una cosa che abbiamo in realtà fatto passare sotto il tappeto:

Proposizione 1.4 I polinomi F_i sono omogenei.

Dimostrazione

$$\begin{array}{lll} F = GH & \deg F = n & n = r + s \\ G = G_q + G_{q+1} + \dots + G_s & \deg G = s & q \leq s \\ H = H_p + H_{p+1} + \dots + H_r & \deg H = r & p \leq r \end{array}$$

con $\deg G_i = i$, $\deg H_j = j$. Supponiamo per assurdo $q < s$ o $p < r$.

$$\underbrace{F}_{\text{omog. di grado } n} = \underbrace{G_q H_p + G_{q+1} H_p + G_q H_{p+1} + \dots}_{\text{devono annullarsi tutti}} + \underbrace{G_s H_r}_{\text{omog. di grado } n}$$

Ma per l'ipotesi di assurdo

$$q + p < r + s = n,$$

e le parti non si cancellerebbero (sicuramente $G_q H_p$ non si eliderebbe). \square

Come facciamo per passare alla chiusura proiettiva? Utilizzeremo delle convenzioni molto comode:

$$\begin{aligned} P &\equiv (x, y) && (x : y : 1) \\ & && \left(\frac{X}{U} : \frac{Y}{U} : 1 \right) \\ & && (X : Y : U) \end{aligned}$$

Supporremo dunque che $U = 0$ sia la retta impropria.

Esempio Passiamo al proiettivo sostituendo (x, y) con $\left(\frac{X}{U} : \frac{Y}{U} : 1\right)$:

$$\begin{aligned} f(x, y) &= x^4 + x^3y - y^3 + xy^2 + x^2 + y^2 - x + y - 2 \\ \left(\frac{X}{U}\right)^4 + \left(\frac{X}{U}\right)^3 \frac{Y}{U} - \left(\frac{Y}{U}\right)^3 + \frac{X}{U} \left(\frac{Y}{U}\right)^2 + \left(\frac{X}{U}\right)^2 + \left(\frac{Y}{U}\right)^2 - \frac{X}{U} + \frac{Y}{U} - 2 &= 0 \end{aligned}$$

Moltiplichiamo infine per U^4 :

$$X^4 + X^3Y - Y^3U + XY^2U + X^2U^2 + Y^2U^2 - XU^3 + YU^3 - 2U^4 = 0.$$

In generale, partendo da $f(x, y)$ con $\deg f = n$ risulterà

$$F(X, Y, U) = U^n f\left(\frac{X}{U}, \frac{Y}{U}\right).$$

Definizione 1.7 Chiamiamo *chiusura proiettiva* di $C = (Z(f), f)$ la curva

$$\bar{C} = (Z(F), F).$$

Occupiamoci ora del processo inverso, ovvero: data una curva proiettiva $C = (Z(G), G)$ vogliamo ricavare una curva affine C_a di cui questa sia chiusura proiettiva.

$$C_a = (Z(g), g) \quad g(x, y) = G(x : y : 1)$$

Definizione 1.8 Chiamiamo *affinizzata* di C la curva C_a .

Naturalmente l'affinizzata di una chiusura proiettiva coinciderà sempre con la curva di partenza:

$$C \rightarrow \bar{C} \rightarrow (\bar{C})_a = C.$$

Attenzione però, perché il rovescio in generale non funziona:

$$C \rightarrow C_a \rightarrow \overline{(C_a)} \neq C.$$

Esempio Consideriamo:

$$\begin{aligned} F &= (X^2 + Y^2 + U^2)U^3 \\ C_a &: x^2 + y^2 + 1 \\ \overline{(C_a)} &: X^2 + Y^2 + U^2 \end{aligned}$$

Sicché abbiamo buttato via la retta impropria contata tre volte.

Comunque questo problema non ci interessa, perché noi faremo sempre l'altro tipo di passaggio.

Esempio Sia² $C = (Z(f), f)$, dove

$$f(x, y) = x^3 + y^3 - 1.$$

Stabiliamo quali sono i punti all'infinito di C intersecando la chiusura proiettiva con la retta impropria.

$$\begin{cases} X^3 + Y^3 - U^3 = 0 \\ U = 0 \end{cases} \quad \begin{cases} X^3 + Y^3 = 0 \\ U = 0 \end{cases} \quad \begin{cases} (X + Y)(X^2 - XY + Y^2) = 0 \\ U = 0 \end{cases}$$

Da questo sistema si trovano i tre punti d'intersezione:

$$\begin{array}{ll} (1 : -1 : 0) & \text{uno dei tre è un punto reale,} \\ (1 - i\sqrt{3} : 2 : 0) & \\ (1 + i\sqrt{3} : 2 : 0) & \text{gli altri due hanno coordinate complesse non reali.} \end{array}$$

Osservazione Nel caso dei piani affini è facile stabilire se si ha a che fare con coordinate complesse. Meno facile in ambito proiettivo: ad esempio, a dispetto delle prime apparenze, $(i : i : i) = (1 : 1 : 1)$ è reale.

Esercizio 1.2.1 Sia $f \in \mathbb{C}[x, y]$, $f \notin \mathbb{C}^*$. Allora $Z(f) \neq \emptyset$.

1.3 Studio delle curve algebriche

Teorema 1.1 Sia $C \subset \mathbb{P}^2(\mathbb{C})$, e sia $L \not\subseteq C$ una retta. Allora

$$\sum_{P \in L \cap C} \nu_P(L, C) = n,$$

dove $n = \text{ord}(C)$ e $\nu_P(L, C)$ è la molteplicità d'intersezione in P tra L e C . (Ovvero: se la retta non appartiene alla curva, i punti in comune sono esattamente n , a patto di contarli con la dovuta molteplicità.)

Dimostrazione In realtà questo teorema è un'assoluta banalità, perché siamo in $\mathbb{P}^2(\mathbb{C})$. Generiamo la retta a partire da due punti A e B , e consideriamo un punto P su di essa:

$$\begin{aligned} A &\equiv (X_A : Y_A : U_A) & B &\equiv (X_B : Y_B : U_B) \\ P = \lambda A + \mu B &\equiv (\lambda X_A + \mu X_B : \lambda Y_A + \mu Y_B : \lambda U_A + \mu U_B) \\ P &\equiv (\lambda : \mu) \neq (0 : 0) \end{aligned}$$

Sia la nostra curva $C = (Z(F), F)$.

$$\begin{aligned} F(\lambda X_A + \mu X_B : \lambda Y_A + \mu Y_B : \lambda U_A + \mu U_B) &= \\ = p(\lambda : \mu) &= a_0 \lambda^n + a_1 \lambda^{n-1} \mu + a_2 \lambda^{n-2} \mu^2 + \cdots + a_n \mu^n = 0 \end{aligned}$$

Stiamo cercando le radici di questo polinomio p . Supponiamo e.g. $B \notin C$ (esisterà pure un punto della retta che non sia sulla curva!). B ha coordinate $(0 : 1)$ su L , quindi dev'essere $a_n \neq 0$. Pertanto, per il teorema fondamentale dell'Algebra,

$$a_0 + a_1 \frac{\mu}{\lambda} + a_2 \left(\frac{\mu}{\lambda}\right)^2 + \cdots + a_n \left(\frac{\mu}{\lambda}\right)^n$$

ha esattamente n radici contate con la loro molteplicità, che corrispondono agli n punti di intersezione tra la retta e la curva. \square

²Curve del tipo $x^n + y^n - z^n = 0$ sono dette *curve di Fermat*.

1.3.1 Punti semplici e retta tangente

Sia $C \in \mathbf{P}^2(\mathbb{C})$. Vogliamo definire l'insieme dei punti singolari $\text{Sing}(C)$.

Definizione 1.9 Un punto P è detto *singolare* se

$$\forall \text{retta } L \ni P \quad \nu_P(L, C) \geq 2.$$

Un punto non singolare si dice *semplice*.

Definizione 1.10 Se la curva C non ha punti singolari si dice *liscia*.

Come calcolare $\nu_P(L, C)$? Poniamo $P \in L$ e $P \in C$; l'equazione risolvente avrà le coordinate di P come soluzione. Trasformiamo la risolvente in un'equazione ad una variabile e da questa ricaviamo la molteplicità. Rifacendoci all'ultima dimostrazione, chiamiamo $t = \frac{\mu}{\lambda}$:

$$p(t) = a_0 + a_1 t + a_2 t^2 + \dots + a_n t^n = 0.$$

Diciamo che $P \equiv (\lambda : \mu) = (1 : 0)$ sia soluzione, ovvero $\nu \geq 1$; allora $t = 0$, quindi $a_0 = 0$. Se poi $a_1 = 0$ e $a_2 \neq 0$ sarà $\nu = 2$, e così via. Possiamo dunque inferire ν dai coefficienti dell'equazione risolvente.

Questo conto è indipendente dai sistemi di riferimento affine e proiettivo sulla retta; lo passiamo sotto il tappeto, ma sarebbe da controllare.

Esempi

- Se una curva non è ridotta, tutti i punti delle componenti non ridotte sono singolari. Sia $F = G^2 H$, sia $P \in Z(G)$.

$$p_F(\lambda : \mu) = p_G(\lambda : \mu)^2 p_H(\lambda : \mu) = 0$$

$p_G(\lambda : \mu) = 0$, quindi la molteplicità è almeno 2, dunque $P \in \text{Sing}(F)$.

- Se una curva è ridotta ma non irriducibile ed esiste un punto comune ad almeno due parti ridotte, esso è singolare. Sia $F = GH$, sia $P \in Z(G)$ e $P \in Z(H)$.

$$p_F(\lambda : \mu) = p_G(\lambda : \mu) p_H(\lambda : \mu) = 0$$

La molteplicità di P come radice di $p_F(\lambda : \mu)$ è almeno 2, quindi $P \in \text{Sing}(F)$.

Osservazione Esistono anche punti singolari che appartengono a curve irriducibili ridotte (non si riconducono a questi meccanismi), e sono i più interessanti da studiare.

Completiamo il quadro per i punti non singolari. Consideriamo $P \notin \text{Sing}(C)$.

Proposizione 1.5 Se $P \in C \setminus \text{Sing}(C)$ allora

$$\exists \text{retta } L \ni P : \nu_P(L, C) \geq 2,$$

e la retta L si chiama *retta tangente*.

Come determinare la retta tangente è un problema che può essere risolto solo con l'introduzione di un nuovo strumento: le derivate parziali.

1.3.2 Derivate parziali

Tutti conosciamo dall'Analisi le derivate successive di un polinomio $f \in \mathbb{R}[x]$:

$$\begin{aligned} f(x) &= a_0 + a_1x + a_2x^2 + a_3x^3 + \dots \\ f'(x) &= a_1 + 2a_2x + 3a_3x^2 + \dots \\ f''(x) &= 2a_2 + 6a_3x + \dots \\ &\vdots \end{aligned}$$

Ora dimentichiamo il significato analitico e consideriamo il polinomio come ente algebrico (questo ci serve spesso in generale, soprattutto se e.g. $f \in \mathbb{C}[x]$): la regola analitica induce una regola formale che permette di generalizzare il concetto di derivata a $f \in \mathbf{K}[x]$. Oltre alle stesse regole di derivazione formali, vale lo sviluppo di Taylor:

$$\begin{aligned} f(x_0 + h) &= f(x_0) + f'(x_0)h + \frac{f''(x_0)}{2!}h^2 + \frac{f'''(x_0)}{3!}h^3 + \dots \\ h &= x - x_0 \\ f(x) &= f(x_0) + f'(x_0)(x - x_0) + \frac{f''(x_0)}{2!}(x - x_0)^2 + \dots \end{aligned}$$

Se scegliamo $x_0 = 0$,

$$f(x) = f(0) + f'(0)x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \dots$$

e possiamo considerare ancora il discorso fatto in precedenza sull'annullarsi dei coefficienti di

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots$$

Pertanto la molteplicità di una radice è k se sono nulle tutte le derivate fino all'ordine $k - 1$ e la derivata k -esima è non nulla.

Per quanto riguarda la derivazione delle funzioni composte,

$$x = x(t) \qquad g(t) = f[x(t)]$$

osserviamo la scrittura formale³

$$\left. \frac{dg}{dt} \right|_{\bar{t}} = \left. \frac{dg}{dx} \right|_{\bar{x}} \left. \frac{dx}{dt} \right|_{\bar{t}}$$

Introduciamo ora le derivate parziali. Possiamo vedere $f \in \mathbf{K}[x, y]$ come $f \in \mathbf{K}[y][x]$

$$f(x) = a_0(y) + a_1(y)x + a_2(y)x^2 + \dots$$

e applicare la regola formale appena vista:

$$\frac{\partial f}{\partial x} = a_1(y) + 2a_2(y)x + 3a_3(y)x^2 + \dots$$

Chiaramente questo procedimento possiamo anche farlo rispetto a y .

³Risalente addirittura a Leibnitz.

Esempio

$$\begin{aligned}
f(x, y) &= x^4 + xy^3 + x^3 - y^3 + xy + x - y + 3 \\
\frac{\partial f}{\partial x} &= 4x^3 + y^3 + 3x^2 + y + 1 \\
\frac{\partial f}{\partial y} &= 3xy^2 - 3y^2 + x - 1.
\end{aligned}$$

Possiamo calcolare la derivata anche più volte: $\frac{\partial^2 f}{\partial x^2}$, $\frac{\partial^2 f}{\partial y^2}$; anche derivate miste: $\frac{\partial^2 f}{\partial y \partial x}$. Per fortuna non ha importanza l'ordine delle derivate successive se si lavora con polinomi (o con altre classi di funzioni che non ci interessano).⁴

Possiamo usare questa notazione per una formula di Taylor più generale:

$$\begin{aligned}
f(x, y) &= f(0, 0) + \frac{\partial f}{\partial x} \Big|_{(0,0)} x + \frac{\partial f}{\partial y} \Big|_{(0,0)} y \\
&+ \frac{1}{2!} \left[\frac{\partial^2 f}{\partial x^2} \Big|_{(0,0)} x^2 + 2 \frac{\partial^2 f}{\partial x \partial y} \Big|_{(0,0)} xy + \frac{\partial^2 f}{\partial y^2} \Big|_{(0,0)} y^2 \right] \\
&+ \frac{1}{3!} \left[\frac{\partial^3 f}{\partial x^3} \Big|_{(0,0)} x^3 + 3 \frac{\partial^3 f}{\partial x^2 \partial y} \Big|_{(0,0)} x^2 y + \right. \\
&\quad \left. + 3 \frac{\partial^3 f}{\partial x \partial y^2} \Big|_{(0,0)} xy^2 + \frac{\partial^3 f}{\partial y^3} \Big|_{(0,0)} y^3 \right] + \dots
\end{aligned}$$

È possibile generalizzare la formula di derivazione per le composte:

$$\begin{aligned}
x &= x(t) & y &= y(t) \\
g(t) &= f[x(t), y(t)] \\
\bar{x} &= x(\bar{t}) & \bar{y} &= y(\bar{t}) \\
\frac{\partial g}{\partial t} \Big|_{\bar{t}} &:= \frac{\partial f}{\partial x} \Big|_{(\bar{x}, \bar{y})} \frac{\partial x}{\partial t} \Big|_{\bar{t}} + \frac{\partial f}{\partial y} \Big|_{(\bar{x}, \bar{y})} \frac{\partial y}{\partial t} \Big|_{\bar{t}}
\end{aligned}$$

In ambito proiettivo useremo

$$F_X = \frac{\partial F}{\partial X}, \quad F_Y = \frac{\partial F}{\partial Y}, \quad F_U = \frac{\partial F}{\partial U}.$$

Proposizione 1.6 Le derivate parziali di $F \in \mathbb{C}[X, Y, U]$ sono polinomi omogenei.

Dimostrazione Scegliamo $\deg F = n \geq 1$ (se il polinomio non è costante, almeno una delle derivate parziali non è identicamente nulla).

$$\begin{aligned}
F &= \underbrace{a_0(Y : U)}_{\deg=n} + \underbrace{a_1(Y : U)}_{n-1} X + \underbrace{a_2(Y : U)}_{n-2} X^2 + \dots + \underbrace{a_\delta(Y : U)}_{n-\delta} X^\delta \\
F_X &= \underbrace{a_1(Y : U)}_{\deg=n-1} + \underbrace{2a_2(Y : U)}_{n-2} X + \dots + \underbrace{\delta a_\delta(Y : U)}_{n-\delta} X^{\delta-1}
\end{aligned}$$

F_X è somma di polinomi di grado $n-1$, quindi è omogeneo di grado $n-1$. \square

⁴Vale infatti il teorema di Schwarz.

Qualora una delle derivate parziali sia identicamente nulla, il polinomio dipende solo dalle altre due variabili. Notiamo cosa succede nei seguenti casi.

- $F_X = F_Y = 0$, $F_U \neq 0$. Sarà $F = aU^n$ ($a \neq 0$), e U^n è la retta $U = 0$ contata n volte. Ovviamente la cosa è simmetrica anche per gli altri due casi in cui due derivate parziali sono nulle.
- $F_U = 0$. Se una sola derivata parziale è nulla, abbiamo e.g.

$$F = a_0X^n + a_1X^{n-1}Y + a_2X^{n-2}Y^2 + \dots + a_nY^n.$$

Essendo in \mathbb{C} possiamo spezzare il polinomio in n fattori lineari:

$$F = (\alpha_1X + \beta_1Y)(\alpha_2X + \beta_2Y) \cdots (\alpha_nX + \beta_nY).$$

Allora $(Z(F), F) \subset \mathbf{P}^2(\mathbb{C})$ è spezzata in n rette passanti per l'origine del sistema di riferimento affine $(0 : 0 : 1)$. I punti singolari saranno tale origine più i punti di eventuali rette contate più volte. Lo stesso identico discorso si può fare se $F_X = 0$ o $F_Y = 0$.

Questi ultimi due casi non sono difficili da studiare. Quelli interessanti sono quelli in cui le derivate sono tutte non-nulle.

Per poter continuare questa trattazione ci manca ancora un ingrediente.⁵

Teorema 1.2 (di Eulero sulle funzioni omogenee) Sia $\deg F = n \geq 1$.

$$XF_X + YF_Y + UF_U = nF.$$

Dimostrazione Se $n = 1$ il teorema è ovvio:

$$\begin{aligned} F &= aX + bY + cU \\ F_X &= a, \quad F_Y = b, \quad F_U = c. \end{aligned}$$

Sia $n \geq 2$. Consideriamo il singolo monomio di F , sia $\alpha + \beta + \gamma = n$ con $\alpha, \beta, \gamma \geq 1$.

$$\begin{aligned} F &= \dots + aX^\alpha Y^\beta U^\gamma + \dots \\ F_X &= \dots + \alpha a X^{\alpha-1} Y^\beta U^\gamma + \dots \\ F_Y &= \dots + \beta a X^\alpha Y^{\beta-1} U^\gamma + \dots \\ F_U &= \dots + \gamma a X^\alpha Y^\beta U^{\gamma-1} + \dots \\ XF_X + YF_Y + UF_U &= \dots + a(\alpha + \beta + \gamma) X^\alpha Y^\beta U^\gamma + \dots = nF \end{aligned}$$

Se invece fosse $\alpha = 0$, $\beta, \gamma \geq 1$, $\beta + \gamma = n$:

$$\begin{aligned} F &= \dots + aY^\beta U^\gamma + \dots \\ F_X &= \dots + 0 + \dots \\ F_Y &= \dots + \beta a Y^{\beta-1} U^\gamma + \dots \\ F_U &= \dots + \gamma a Y^\beta U^{\gamma-1} + \dots \\ XF_X + YF_Y + UF_U &= \dots + a(\beta + \gamma) Y^\beta U^\gamma + \dots = nF \quad \square \end{aligned}$$

⁵Mostriamo questo teorema solo nel caso delle funzioni polinomiali, ma in realtà esso vale per classi più ampie di funzioni.

Esercizio 1.3.1 Far vedere che vale anche il caso dei monomi in una sola indeterminata.

Mostriamo ora delle applicazioni delle derivate parziali.

Sia $C = (Z(F), F) \subset \mathbf{P}^2(\mathbb{C})$. Andiamo a considerare $P \in C$. Vogliamo un criterio che ci dica se $P \equiv (X_0 : Y_0 : U_0)$ è singolare o no.

Fissiamo un'altro punto $Q \equiv (\alpha : \beta : \gamma)$, con il quale P individuerà una retta. Possiamo parametrizzare i punti di tale retta nella forma $P + tQ$.

$$\begin{cases} X = X_0 + t\alpha \\ Y = Y_0 + t\beta \\ U = U_0 + t\gamma \end{cases}$$

Andiamo a intersecare la retta con C .

$$\begin{aligned} F(X_0 + t\alpha : Y_0 + t\beta : U_0 + t\gamma) &= h(t) = h(0) + h'(0)t + \frac{h''(0)}{2!}t^2 + \dots \\ &= a_0 + a_1t + a_2t^2 + \dots \end{aligned}$$

Chiaramente $h(0) = 0$, perché $P \in C$. Una molteplicità d'intersezione di almeno 2 richiede $h'(0) = 0$.

$$\begin{aligned} h'(0) &= \left. \frac{dh}{dt} \right|_{t=0} \\ &= \left. \frac{\partial F}{\partial X} \right|_{\substack{x=X_0 \\ y=Y_0 \\ u=U_0}} \frac{\partial X}{\partial t} \Big|_{t=0} + \left. \frac{\partial F}{\partial Y} \right|_P \frac{\partial Y}{\partial t} \Big|_{t=0} + \left. \frac{\partial F}{\partial U} \right|_P \frac{\partial U}{\partial t} \Big|_{t=0} \\ &= F_X \Big|_P \alpha + F_Y \Big|_P \beta + F_U \Big|_P \gamma = 0 \end{aligned}$$

Questa espressione deve essere 0 per ogni retta, i.e. $\forall \alpha, \beta, \gamma$. Morale:

$$P \in \text{Sing}(C) \Leftrightarrow F_X \Big|_P = F_Y \Big|_P = F_U \Big|_P = 0.$$

Potremmo anche partire da un qualunque $P \in \mathbf{P}^2(\mathbb{C})$: se chiediamo l'appena enunciata condizione di singolarità, il teorema di Eulero ci dice che $P \in C$:

$$nF \Big|_P = X_0 F_X \Big|_P + Y_0 F_Y \Big|_P + U_0 F_U \Big|_P = 0.$$

Esempi Ritroviamo gli esempi già visti.

- Sia $F = H^2G$, sia $P \in Z(H)$.

$$F_X = \frac{\partial}{\partial X}(H^2)G + H^2 \frac{\partial G}{\partial X} = 2HH_XG + H^2G_X$$

Siccome P annulla H , la derivata si annulla (analogamente F_Y e F_U).

- Sia $F = HG$, sia $P \in Z(H) \cap Z(G)$.

$$F_X = H_XG + HG_X$$

Siccome P annulla H e G , abbiamo $F_X \Big|_P = 0$ (analogamente F_Y e F_U).

Prendiamo ora in mano la considerazione che abbiamo fatto, perché questo stesso conto ci permette anche di determinare la retta tangente.

$$h'(0) = F_X|_P \alpha + F_Y|_P \beta + F_U|_P \gamma = 0$$

Se supponiamo che P sia un punto non singolare, sappiamo che almeno una di queste tre derivate è diversa da zero. Ci possiamo allora chiedere quali sono le rette individuate da α , β , γ per le quali quest'espressione è uguale a zero. Bene, risulta che

$$F_X|_P X + F_Y|_P Y + F_U|_P U = 0$$

è l'equazione della retta tangente $T_P(C)$.

Come determinare la tangente in un punto ad una curva affine? Siano $C = (Z(f), f) \subset \bar{C}$, $P_0 \equiv (x_0, y_0) \in C$, $P_0 \equiv (x_0 : y_0 : 1)$. Quello che vogliamo mostrare è che la retta tangente in P_0 a C è

$$\frac{\partial f}{\partial x}|_{P_0} (x - x_0) + \frac{\partial f}{\partial y}|_{P_0} (y - y_0) = 0.$$

Dimostrazione Supponiamo di avere una delle tre derivate parziali, F_X , e facciamo vedere che

$$F_X|_{(x_0 : y_0 : 1)} = \frac{\partial f}{\partial x}|_{(x_0, y_0)}.$$

Sappiamo innanzitutto che

$$f(x, y) = F(x : y : 1).$$

Consideriamo:

$$\begin{aligned} F &= \underbrace{a_0(Y : U)}_{\text{deg}=n} + \underbrace{a_1(Y : U)}_{n-1} X + \cdots + \underbrace{a_k(Y : U)}_{n-k} X^k \\ F_X &= a_1(Y : U) + 2a_2(Y : U)X + \cdots + ka_k(Y : U)X^{k-1} \\ F_X|_{(x_0 : y_0 : 1)} &= a_1(y_0 : 1) + 2a_2(y_0 : 1)x_0 + \cdots + ka_k(y_0 : 1)x_0^{k-1} \end{aligned}$$

Adesso andiamo a vedere cos'è invece l'espressione di destra della nostra tesi:

$$\begin{aligned} f(x, y) &= a_0(y : 1) + a_1(y : 1)x + \cdots + a_k(y : 1)x^k \\ \frac{\partial f}{\partial x} &= a_1(y : 1) + 2a_2(y : 1)x + \cdots + ka_k(y : 1)x^{k-1} \\ \frac{\partial f}{\partial x}|_{(x_0, y_0)} &= a_1(y_0 : 1) + 2a_2(y_0 : 1)x_0 + \cdots + ka_k(y_0 : 1)x_0^{k-1} \end{aligned}$$

Morale: la relazione è vera. Con lo stesso procedimento avremo

$$F_Y|_{(x_0 : y_0 : 1)} = \frac{\partial f}{\partial y}|_{(x_0, y_0)}.$$

Per calcolare la retta tangente abbiamo però bisogno anche del valore della derivata parziale F_U , e qui non possiamo invocare una relazione analoga alle altre due. Usiamo quindi il teorema di Eulero:

$$\begin{aligned} nF &= XF_X + YF_Y + UF_U \\ 0 &= x_0 F_X|_{P_0} + y_0 F_Y|_{P_0} + F_U|_{P_0} \\ F_U|_{P_0} &= -x_0 F_X|_{P_0} - y_0 F_Y|_{P_0} \end{aligned}$$

Adesso abbiamo tutti gli ingredienti per andare a descrivere l'equazione della retta tangente nel punto P_0 :

$$\frac{\partial f}{\partial x}\Big|_{(x_0, y_0)} X + \frac{\partial f}{\partial y}\Big|_{(x_0, y_0)} Y + \left(-x_0 \frac{\partial f}{\partial x}\Big|_{(x_0, y_0)} - y_0 \frac{\partial f}{\partial y}\Big|_{(x_0, y_0)} \right) U = 0.$$

A noi interessa l'affinizzata di questa retta,

$$f_x\Big|_{P_0} x + f_y\Big|_{P_0} y - x_0 f_x\Big|_{P_0} - y_0 f_y\Big|_{P_0} = 0,$$

che era esattamente il nostro obiettivo. \square

Definizione 1.11 Sia $P_\infty \in \overline{C}$ punto reale con tangente reale diversa dalla retta impropria. Diciamo che in P_∞ la curva C ammette un *asintoto*, che è la retta tangente in tale punto a \overline{C} .

1.3.3 Finitzza dei punti singolari

Vogliamo ora dimostrare che il numero di punti singolari per una curva ridotta è finito. Per farlo però dobbiamo prima conoscere il teorema più importante di tutta questa prima parte del corso.

Teorema 1.3 (di Bézout) Siano $C, C' \subset \mathbf{P}^2(\mathbb{C})$ di ordini rispettivi n, n' e che non abbiano componenti irriducibili in comune. Allora

$$\sum_{P \in C \cap C'} \nu_P(C, C') = nn'.$$

La dimostrazione di questo teorema la vedremo quando avremo a disposizione altri marchingegni di carattere algebrico.

Noi al momento non sappiamo calcolare il numero $\nu_P(C, C')$, ma solo il caso particolare $\nu_P(L, C)$. Anticipiamo però fin d'ora che se un punto P sta nell'intersezione di due curve C, C' allora $\nu_P(C, C') \geq 1$.

Proposizione 1.7 Una curva C ridotta ha un numero finito di punti singolari.

Dimostrazione Procediamo in due passi.

- *Se C è irriducibile e ridotta.* Sia $C = (Z(F), F) \subset \mathbf{P}^2(\mathbb{C})$. I suoi punti singolari sono nell'intersezione delle curve C_X, C_Y, C_U associate alle rispettive derivate parziali di F . Esaminiamo prima i casi in cui una o due delle derivate parziali sono nulle, perché in tali casi abbiamo solo una o due curve e il ragionamento che faremo dopo non vale.
 - *Se 2 derivate parziali sono nulle.* Sarà e.g. $F = aX^n$, con $a \neq 0$ e $n = \text{ord } C$. Ad una curva del genere il teorema è applicabile solo se $n = 1$, ed è ovvio in quanto una retta non ha punti singolari.
 - *Se 1 sola derivata parziale è nulla.* La curva è un insieme di rette che passano per uno stesso punto; ma siccome stiamo considerando C irriducibile e ridotta, la curva non può che essere un'unica retta, che non ha punti singolari, quindi il teorema è banalmente vero.

Ora possiamo tranquillamente supporre che tutte e tre le derivate parziali di F siano diverse da zero. Quindi danno luogo a tre curve che, come già abbiamo visto, hanno ordine $n - 1$. Adesso, sappiamo che i punti singolari di C si trovano nell'intersezione $C_X \cap C_Y \cap C_U$. Se C_X, C_Y non hanno componenti irriducibili in comune, per il teorema di Bézout hanno un numero finito di punti in comune e quindi la curva di partenza ha un numero finito di punti singolari.

Osservazione Nonostante C sia ridotta, potrebbe succedere che una o più di queste tre curve siano invece irriducibili e non ridotte.

Esempio Sia $F(X : Y : U) = X^3 + Y^3 - U^3$. Risulta $F_X(X : Y : U) = 3X^2$, che è irriducibile non ridotta anche se F è irriducibile ridotta.

Cosa succede se per sventura C_X, C_Y hanno qualche componente irriducibile in comune? Allora i punti singolari della curva di partenza si troveranno tra i punti comuni a queste due curve fuori da queste componenti in comune e poi, eventualmente, in tutti i punti di queste componenti in comune. Se nessuna di queste componenti irriducibili in comune a C_X, C_Y fa parte di C_U allora le tre curve non hanno componenti irriducibili in comune e quindi hanno un numero finito di punti in comune, quindi C avrebbe un numero finito di punti singolari.

Rimane ora solo il caso in cui una componente irriducibile sia in comune a C_X, C_Y, C_U . Bene, questo caso sciagurato in realtà non capita. Proviamo infatti a supporre che ci sia davvero una componente irriducibile comune alle tre curve, e chiamiamola $(Z(H), H)$. Per il lemma di Study, se

$$Z(H) \subseteq Z(F_X) \cap Z(F_Y) \cap Z(F_U)$$

necessariamente

$$H \mid F_X, \quad H \mid F_Y, \quad H \mid F_U.$$

Potremmo quindi scrivere

$$F_X = HH', \quad F_Y = HH'', \quad F_U = HH''',$$

e per il teorema di Eulero risulterebbe

$$nF = XF_X + YF_Y + UF_U = H(XH' + YH'' + UH'''),$$

da cui $H \mid F$ e C non sarebbe irriducibile. Assurdo.

- Se C è ridotta. La decomposizione della C sarà del tipo

$$C = C_1 \cup C_2 \cup \dots \cup C_q.$$

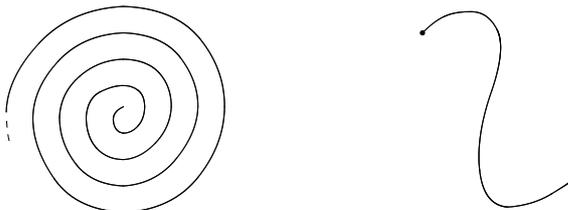
Sappiamo che, presa singolarmente, ciascuna di queste componenti, che è una curva irriducibile ridotta, ha comunque al massimo un numero finito di punti singolari. I punti singolari della curva C possono essere o in ciascuna di queste componenti irriducibili oppure nei punti d'intersezione di queste componenti. Ma questi punti d'intersezione possono solo essere in numero finito. Infatti, esaminiamo e.g. le prime due componenti C_1, C_2 : il teorema di Bézout ci dice che hanno al più un numero finito di punti d'intersezione a meno che esse abbiano una componente irriducibile in comune. Ma, essendo curve irriducibili, non possono avere componenti irriducibili in comune. Questo discorso si ripete per ogni coppia. \square

La nostra strategia per studiare una curva sarà questa: andare prima a studiare quali sono i punti singolari, poi a descrivere come è fatta la curva nei punti *non* singolari.

1.3.4 Analisi dei punti semplici

La nostra analisi tende a descrivere come è fatta una curva del nostro tipo vicino – per il momento – a ciascuno dei suoi punti non singolari. Questo ci porterà ad escludere alcuni tipi di luoghi di zeri, che sicuramente non possono essere il supporto di una curva del nostro tipo.

Esempi Un insieme di punti fatto in uno dei seguenti modi sicuramente non è supporto di alcuna curva algebrica.



L'esempio di sinistra non è valido perché se prendiamo una retta che passa per il centro della spirale questa avrà infiniti punti di intersezione con la curva, mentre noi sappiamo che una curva algebrica e una retta hanno un numero finito di punti d'intersezione. Per quanto riguarda l'esempio di destra, vedremo che una curva algebrica non può a un certo punto finire nel nulla, bloccarsi.

Prendiamo una curva del piano euclideo, consideriamo la sua chiusura proiettiva, scegliamo un punto non singolare e andiamo a vedere cosa succede vicino a questo punto. Siccome le operazioni che facciamo sono invarianti rispetto al sistema di riferimento, possiamo sempre supporre che l'analisi sia fatta per il punto $P \equiv (0 : 0 : 1)$ dal punto di vista proiettivo o $P \equiv (0, 0)$ dal punto di vista affine. Scriviamo lo sviluppo di Taylor del nostro polinomio:

$$f(x, y) = f(0, 0) + \left(\frac{\partial f}{\partial x} \Big|_{(0,0)} x + \frac{\partial f}{\partial y} \Big|_{(0,0)} y \right) + \frac{1}{2} \left(\frac{\partial^2 f}{\partial x^2} \Big|_{(0,0)} x^2 + \dots \right) + \dots$$

Ma il punto $(0, 0)$ sta sulla curva, quindi $f(0, 0) = 0$. Consideriamo ora solo la parte omogenea di primo grado dello sviluppo. Siccome stiamo supponendo che il nostro punto sia non singolare, è chiaro che le due derivate non possono essere entrambe nulle. Di più: questa parte è l'equazione della retta tangente. Possiamo ora cambiare ulteriormente il sistema di riferimento affine scegliendo questa retta come asse delle x . In tal modo, la curva C' nel nuovo sistema di riferimento avrà un polinomio associato come

$$f(x, y) = hy + ax^2 + bxy + cy^2 + \dots$$

Possiamo perfino dividere per $h \neq 0$ giungendo alla forma

$$f(x, y) = y + ax^2 + bxy + cy^2 + \dots$$

Adesso, la prima cosa che ci interessa di capire è quale sia la molteplicità di intersezione nel punto considerato fra la retta tangente $y = 0$ e la curva.

$$f(x, 0) = ax^2 + dx^3 + \dots$$

Ora, è chiaro che la molteplicità della radice $x = 0$ è legata al fatto che a sia o meno nullo.

Supponiamo per il momento che la molteplicità sia il minimo sindacale, 2; ovvero $\alpha \neq 0$. Vediamo come descrivere la curva in questa situazione. La maniera più semplice per farlo è considerare delle funzioni ausiliarie, cioè delle funzioni polinomiali in una terza variabile t che approssimino l'andamento della nostra curva vicino al punto $(0, 0)$.

$$\begin{cases} x = \alpha_0 + \alpha_1 t + \alpha_2 t^2 + \dots \\ y = \beta_0 + \beta_1 t + \beta_2 t^2 + \dots \end{cases}$$

L'idea è di cercare funzioni di questo tipo molto semplici e che ci diano punti che cadano esattamente nel nostro arco di curva. Per fare questo consideriamo:

$$f(x(t), y(t)) = h(t) = h(0) + h'(0)t + \frac{h''(0)}{2}t^2 + \dots$$

Ora, l'approssimazione che una di queste curve darà per la curva di partenza sarà tanto migliore quanto sarà superiore la molteplicità della radice $t = 0$. Per valori di t prossimi a 0 le potenze successive sono tutte trascurabili rispetto alla prima. Partiamo con

$$\begin{cases} x = t \\ y = \lambda t^2 \end{cases} \quad y = \lambda x^2 \quad \lambda \in \mathbb{R}^*$$

Andiamo a considerare questa famiglia di parabole e guardiamo qual è la molteplicità d'intersezione di una curva di questo tipo con la nostra nel punto che stiamo considerando.

$$\begin{aligned} f(t, \lambda t^2) &= \lambda t^2 + \alpha t^2 + b\lambda t^2 + c(\lambda t^2)^2 + dt^3 + \dots \\ &= (\lambda + \alpha)t^2 + (\quad)t^3 + (\quad)t^4 + \dots \end{aligned}$$

Quello che ci interessa è il coefficiente della potenza più bassa, che ci dice che se scegliamo una curva di questa famiglia la molteplicità d'intersezione è in generale 2. Però se noi andiamo a scegliere $\lambda = -\alpha$, la molteplicità d'intersezione è ≥ 3 . Quindi tra quelle parabole ce n'è una sola che approssima la nostra curva in maniera adeguata, e la nostra curva in prossimità del punto considerato si comporta come

$$y = -\alpha x^2.$$

Se la molteplicità d'intersezione diventa 3, ovvero se $\alpha = 0$ e $d \neq 0$, facciamo lo stesso lavoro che abbiamo fatto prima.

$$f(t, \lambda t^2) = \lambda t^2 + (\quad)t^3 + (\quad)t^4 + \dots$$

Quindi ciascuna parabola di questa famiglia ha molteplicità d'intersezione almeno 2 con la curva nel punto, e per avere molteplicità superiore bisogna scegliere $\lambda = 0$. Tuttavia scegliendo $\lambda = 0$ in realtà abbiamo ancora la retta tangente, il che significa che questa approssimazione non serve più a nulla. Proviamo invece:

$$\begin{cases} x = t \\ y = \lambda t^3 \end{cases} \quad y = \lambda x^3 \quad \lambda \in \mathbb{R}^*$$

$$\begin{aligned} f(t, \lambda t^3) &= \lambda t^3 + b\lambda t^3 + c(\lambda t^3)^2 + dt^3 + \dots \\ &= (\lambda + d)t^3 + (\quad)t^4 + (\quad)t^5 \end{aligned}$$

Adesso la molteplicità d'intersezione di una qualunque curva di questo tipo con la nostra nel punto che ci interessa è almeno 3. Se vogliamo una curva specifica che abbia molteplicità superiore dobbiamo scegliere $\lambda = -d$.

Riassumendo, se andiamo a considerare la retta tangente nel punto P della nostra curva sul piano affine reale, l'unica cosa che ci interessa è la molteplicità d'intersezione di questa retta tangente con la curva; anzi ci interessa solo la parità, ovvero se questo è un numero pari oppure dispari. Infatti, è possibile dimostrare che se la molteplicità d'intersezione è pari il comportamento della curva rispetto alla retta tangente è del tipo raffigurato a sinistra, altrimenti è del tipo a destra:

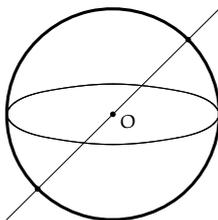


Inoltre la chiusura proiettiva della curva avrà dei punti d'intersezione con la retta impropria, i cosiddetti punti impropri della curva. Se uno di questi individua un asintoto, dobbiamo vedere cosa succede. Il risultato della nostra analisi sarà che anche il comportamento della curva rispetto a un asintoto dipende dalla parità della molteplicità. Precisamente, se la molteplicità d'intersezione è pari il comportamento è come raffigurato a sinistra, se dispari come a destra:

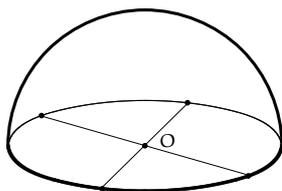


Notiamo che qui se la molteplicità d'intersezione è pari la curva sta in entrambi i semipiani individuati dall'asintoto, mentre se è dispari sta in un solo semipiano; la situazione è quindi all'opposto di quanto accadeva con i punti al finito. Questa apparente discrasia però è in realtà un'uguaglianza, ovvero accade sempre la stessa cosa, anche se di primo impatto non sembrerebbe. Questo perché stiamo facendo dei ragionamenti sul piano proiettivo reinterpretandoli poi sul piano affine. Per capire come mai questo succede dovremo costruirci un modello topologico di $\mathbf{P}^2(\mathbb{R})$.

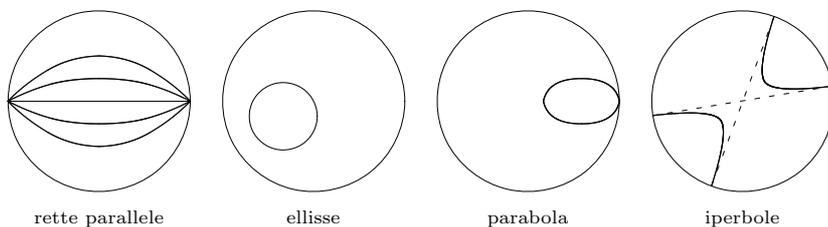
Il metodo visto in Geometria I consisteva nell'immaginare il piano proiettivo come lo spazio affine tridimensionale, escludendo l'origine e con la convenzione che i punti su una stessa retta per l'origine identificano un solo punto proiettivo. Questo modello permette di stabilire una corrispondenza biunivoca tra i punti del piano proiettivo reale e degli enti geometrici che stanno in uno spazio proiettivo euclideo, precisamente le rette che passano per l'origine. Questo modello è però fastidioso, perché fa corrispondere a punti di un piano delle rette dello spazio. Cerchiamo invece un modello in cui a punti corrispondano punti.



Consideriamo una sfera centrata nell'origine del sistema di riferimento. Ogni volta che andiamo a prendere una retta passante per l'origine, questa taglia la nostra sfera in una coppia di punti diametralmente opposti rispetto al centro della sfera, e questa coppia individua univocamente la retta. Pertanto ad un punto del piano proiettivo reale corrisponde una coppia di punti di questo modello. Purtroppo però c'è sempre una scomodità: a un punto ne corrispondono due. Cerchiamo allora di semplificare ulteriormente il modello buttando via metà della superficie sferica. Tuttavia, è necessario tenere tutti i punti della circonferenza equatoriale, che, a coppie, corrispondono ai punti impropri del piano proiettivo.



Ultimo passaggio che possiamo fare è trasformare il modello semisferico in un modello piano più comodo facendo per esempio la proiezione ortogonale dei punti di questa mezza sfera sul piano. Otteniamo così il modello del disco piano, in cui però i punti diametralmente opposti rispetto al centro del disco sono da ritenersi identificati tra loro. La retta impropria sarà pertanto la circonferenza del bordo del disco. Qualche esempio:



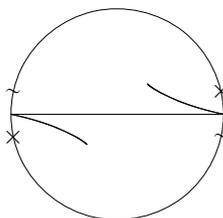
rette parallele

ellisse

parabola

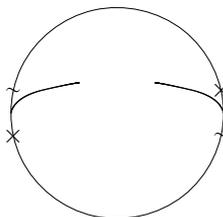
iperbole

Come dimostriamo l'apparente discrepanza notata all'inizio nella descrizione del comportamento della curva? Se la molteplicità è, ad esempio, pari, dobbiamo far vedere che il comportamento della curva rispetto alla retta tangente è come avevamo inizialmente annunciato. Usiamo il modello del disco per tradurre questa situazione nel caso del punto all'infinito.



Ora, bisogna tener conto del fatto che i punti che stanno nelle zone segnate in figura con \times o con \sim sono rispettivamente identificati tra loro. Se volessimo ritagliare un dischetto intorno ad un punto all'infinito, dovremmo ritagliare un semicircoletto da una parte e uno dall'altra del nostro modello a disco; per affiancare poi questi due pezzi in maniera da far combaciare i punti impropri in coppia fra loro dovremmo ribaltare una delle due parti, sicché la curva verrebbe a trovarsi in un solo semipiano come accadeva quando avevamo a che fare con punti propri. Analogamente, se la molteplicità d'intersezione è dispari rispunta la relativa situazione annunciata inizialmente per i punti al finito.

Può infine capitare che in un punto all'infinito la nostra curva presenti come retta tangente la retta impropria. In questa situazione l'analisi finora fatta non funziona. Anche qui ci saranno due possibilità a seconda che la molteplicità d'intersezione tra la curva e la retta impropria sia pari o dispari. Se è pari, è il caso della parabola già esemplificato sopra. Se è dispari, la curva si comporta come in figura:



Esempio Sia $f(x, y) = y^2 - x^3 = 0$. Ci interessa il comportamento all'infinito. Intersechiamo quindi la chiusura proiettiva della nostra curva con la retta impropria.

$$\begin{cases} Y^2U - X^3 = 0 \\ U = 0 \end{cases} \quad \begin{cases} X^3 = 0 \\ U = 0 \end{cases} \quad Y_\infty = (0 : 1 : 0).$$

Vediamo che la curva ha un solo punto improprio, non singolare (verificare!), dove però la retta tangente (la retta impropria) incontra la curva con molteplicità 3. La nostra curva avrà dunque due rami che procedono in verticale comportandosi similmente a rami di parabola.

1.3.5 Punti multipli

Proseguiamo la nostra analisi sempre supponendo che il nostro punto da analizzare, ora singolare, sia l'origine. Inoltre, considerando lo sviluppo nel punto da analizzare della nostra curva,

$$f(x, y) = \phi_0 + \phi_1 + \phi_2 + \phi_3 + \dots$$

non solo manca il termine di grado 0, ma manca anche la componente di grado 1, perché altrimenti quella, eguagliata a zero, ci darebbe l'unica retta tangente.

Bisogna cominciare da una rozza classificazione dei punti singolari, ovvero: ogni punto singolare (per i fatti suoi) ha anch'esso una sua molteplicità.⁶ Si parla dunque di punti doppi, tripli, quadrupli, quintupli, ec.

Definizione 1.12 Un punto si dice *punto doppio* se, salvo al più un numero finito di rette, tutte le altre hanno molteplicità d'intersezione esattamente 2 con la curva nel punto.

Questa definizione si traduce nel fatto che quando uno sposta un punto doppio nell'origine e va a considerare il polinomio $f(x, y)$ ha che il punto è doppio se e solo se il complesso dei termini di II grado è diverso da zero mentre il complesso dei termini di grado 0 e di grado 1 è zero.

$$f(x, y) = ax^2 + bxy + cy^2 + dx^3 + \dots$$

Consideriamo una qualunque retta che esce dall'origine:

$$\begin{cases} x = \alpha t \\ y = \beta t \end{cases}$$

Intersechiamo la retta con la curva.

$$\begin{aligned} f(\alpha t, \beta t) &= a\alpha^2 t^2 + b\alpha\beta t^2 + c\beta^2 t^2 + d\alpha^3 t^3 + \dots \\ &= (a\alpha^2 + b\alpha\beta + c\beta^2)t^2 + (\quad)t^3 + \dots \end{aligned}$$

Esistono delle rette per cui la molteplicità d'intersezione è superiore a 2; il loro numero dipende dalla soluzione dell'equazione

$$a\alpha^2 + b\alpha\beta + c\beta^2 = 0.$$

Le (al massimo) due rette per cui la molteplicità è maggiore di 2 sono quelle corrispondenti alle soluzioni dell'equazione.

Definizione 1.13 Le rette che hanno molteplicità d'intersezione nel punto maggiore della molteplicità del punto si chiamano *tangenti principali*.

Un punto singolare ha tante tangenti principali (contate con la dovuta molteplicità) quanto è la molteplicità del punto.

Notiamo che per avere un punto n -uplo è necessaria una curva di grado almeno n . Ma possiamo dire di più: se una curva ha e.g. grado 3 e presenta un punto triplo, la curva non può che essere costituita dall'unione di tre rette passanti per tale punto. Infatti in tal caso l'addendo di grado 3 è l'unico che compare nella scrittura della curva, quindi abbiamo un polinomio omogeneo; e questo si spezzerà necessariamente in tanti fattori lineari quanto è il grado del polinomio. In generale, una curva di ordine n avente un punto n -uplo è spezzata in n rette eventualmente contate con molteplicità.

1.3.6 Analisi dei punti doppi

Sappiamo che, nel nostro sistema di riferimento, se un punto è doppio abbiamo

$$f(x, y) = \underbrace{ax^2 + bxy + cy^2}_{\varphi_2 \neq 0} + \varphi_3 + \dots$$

⁶Che non va confusa con la molteplicità d'intersezione con una retta.

La molteplicità d'intersezione nel punto in questione tra la curva e la generica retta sarà esattamente 2 salvo un numero finito di queste rette, e precisamente quelle che corrispondono a α, β che soddisfano

$$\begin{cases} x = \alpha t \\ y = \beta t \end{cases} \\ a\alpha^2 + b\alpha\beta + c\beta^2 = 0.$$

e che si chiamano tangenti principali. Può succedere che queste due soluzioni siano due radici complesse coniugate (e quindi le rette siano immaginarie) oppure una sola radice (e quindi una sola retta contata due volte). Esaminiamo caso per caso.

- *Nodo isolato.* (Due rette immaginarie.) Sono rette che non hanno punti reali salvo il punto che stiamo considerando. C'è ben poco da dire: in ambito reale la curva si presenta come un unico punto, e in un opportuno intorno di tale punto non compare alcun altro punto della curva.
- *Nodo ordinario.* (Due rette distinte.) In generale con l'aggettivo "ordinario" si intende un punto multiplo in cui tutte le tangenti principali sono tra loro distinte.

Cambiamo ulteriormente il sistema di riferimento in modo che le due tangenti principali siano i due assi cartesiani $x = 0$ e $y = 0$. In questo nuovo sistema di riferimento il polinomio si scrive così:

$$f(x, y) = xy + ax^3 + bx^2y + cxy^2 + dy^3 + \underbrace{ex^4 + \dots + \varphi_5 + \dots}_{\varphi_4}$$

Andiamo a considerare le curve che parametrizzano i punti della nostra curva nel piano affine reale vicino al punto considerato. Per sapere quale famiglia di curve scegliere, intersechiamo la nostra curva con una delle rette tangenti e andiamo a vedere la molteplicità. Cominciamo a scegliere l'asse delle x .

$$f(x, 0) = ax^3 + ex^4 + \dots$$

La molteplicità d'intersezione sarà almeno 3.

– $\nu_P(y = 0, C) = 3 \Leftrightarrow a \neq 0$. Cominciamo a considerare la famiglia

$$\begin{cases} x = t \\ y = \lambda t^2 \end{cases} \quad (\lambda \neq 0)$$

Intersechiamo la nostra curva con la generica curva della famiglia.

$$\begin{aligned} f(t, \lambda t^2) &= \lambda t^3 + at^3 + b\lambda t^2 + ct(\lambda t^2)^2 + d(\lambda t^2)^3 + e t^4 + \dots \\ &= (\lambda + a)t^3 + (\quad)t^4 + \dots \end{aligned}$$

In generale la molteplicità d'intersezione è esattamente 3; tuttavia per la parabola $y = -ax^2$ la molteplicità d'intersezione è ≥ 4 . Questa

curva ci darà una descrizione locale della nostra per piccoli valori di t .⁷

- $\nu_P(\mathbf{y} = 0, C) = 4 \Leftrightarrow \mathbf{a} = 0, \mathbf{e} \neq 0$. Intersechiamo ancora con la stessa famiglia di curve usata prima e andiamo a fare il medesimo conto:

$$f(t, \lambda t^2) = \lambda t^3 + (\quad) t^4 + \dots$$

Se volessimo molteplicità d'intersezione maggiore di 3 dovremmo scegliere $\lambda = 0$, che è però vietato. Ciò significa che questa famiglia non è quella giusta, quindi proviamo con una famiglia di cubiche.

$$\begin{cases} x = t \\ y = \lambda t^3 \end{cases} \quad (\lambda \neq 0)$$

$$\begin{aligned} f(t, \lambda t^3) &= \lambda t^4 + \mathbf{a} t^3 + \mathbf{b} t^2 \lambda t^3 + \mathbf{c} t (\lambda t^3)^2 + \mathbf{d} (\lambda t^3)^3 + \mathbf{e} t^4 + \dots \\ &= (\lambda + \mathbf{e}) t^4 + (\quad) t^5 + \dots \end{aligned}$$

La cubica $\mathbf{y} = -\mathbf{e}x^3$ descrive quindi il comportamento della nostra curva vicino al punto che stiamo considerando.⁸

Se proseguissimo nell'analisi vedremmo che il risultato dipende solo dalla parità della molteplicità d'intersezione, con comportamento scambiato rispetto a quanto accade per i punti semplici.

Ricordiamo però che questa è l'analisi relativa solo a una delle due tangenti principali, la $\mathbf{y} = 0$ che abbiamo deciso di scegliere. Adesso dovremmo controllare come si comporta la curva rispetto all'altra tangente principale. Ma se noi facessimo i conti otterremmo esattamente gli stessi risultati, basta cambiare le famiglie di curve ausiliarie. Quindi la conclusione alla fine della nostra analisi è che ci sono due rami che passano per il nostro punto, e ciascuno ha un comportamento rispetto alla relativa retta tangente che dipende dalla parità della molteplicità d'intersezione del ramo con la retta.

Definizione 1.14 Un nodo ordinario le cui tangenti presentino una molteplicità pari, l'altra molteplicità dispari, viene detto *flecnode*. Nel caso ci siano due molteplicità pari, viene invece detto *biflecnode*.⁹

Se il punto in questione è all'infinito abbiamo due tangenti distinte parallele, che sono due asintoti. Il comportamento della curva rispetto a questi dipende ancora dalla molteplicità d'intersezione, ed è analogo a quanto visto nel caso dei punti semplici con i dovuti scambi.

⁷Bisogna notare che questa situazione si presenta quando la molteplicità è 3, mentre nel caso dei punti semplici questo accadeva quando era 2. Questo perché ci sono due tangenti principali, e quindi due rami della curva che passano per il punto. Siccome l'altro ramo è trasverso, la molteplicità d'intersezione con quello è 1, e quindi tutte le molteplicità che noi leggiamo adesso sono sempre da intendersi come 1 più la molteplicità d'intersezione con il nostro ramo.

⁸Questa è la situazione che si presentava nel caso dei punti semplici quando la molteplicità d'intersezione era dispari, mentre qui si presenta per molteplicità d'intersezione 4. Ma $4 = 1 + 3$, analogamente a quanto descritto nella precedente nota.

⁹Secondo la terminologia di molti autori, flecnodi e biflecnodi non sono detti nodi ordinari.

- *Punto di natura cuspidale.* (Una sola retta contata due volte.) Supponiamo ancora che questa retta sia l'asse delle x e consideriamo l'intersezione.

$$f(x, y) = y^2 + \underbrace{ax^3 + bx^2y + cxy^2 + dy^3}_{\varphi_3} + \underbrace{ex^4 + \dots}_{\varphi_4} + \varphi_5 + \dots$$

$$f(x, 0) = ax^3 + ex^4 + \dots$$

In generale la molteplicità d'intersezione sarà almeno 3.

– $\nu_P(y=0, C) = 3 \Leftrightarrow a \neq 0$. Partiamo ancora dalla famiglia

$$\begin{cases} x = t \\ y = \lambda t^2 \end{cases} \quad (\lambda \neq 0)$$

e vediamo cosa succede.

$$\begin{aligned} f(t, \lambda t^2) &= \lambda^2 t^4 + at^3 + bt^2 \lambda t^2 + d(\lambda t^2)^2 + et^4 + \dots \\ &= at^3 + (\quad) t^4 + \dots \end{aligned}$$

Ricordiamoci che $a \neq 0$, quindi nessuna di queste parabole ha molteplicità d'intersezione superiore a 3. Questa famiglia non va bene, quindi facciamo come prima e andiamo a considerare una famiglia di cubiche.

$$\begin{cases} x = t \\ y = \lambda t^3 \end{cases} \quad (\lambda \neq 0)$$

$$\begin{aligned} f(t, \lambda t^3) &= \lambda^2 t^6 + at^3 + bt^2 \lambda t^3 + ct(\lambda t^3)^2 + d(\lambda t^3)^3 + et^4 + \dots \\ &= at^3 + (\quad) t^4 + \dots \end{aligned}$$

Tuttavia la situazione non è cambiata: la molteplicità di intersezione è sempre soltanto 3. Qui il tentativo di proseguire lungo questa strada è destinato a naufragare miseramente, perché non ci libereremo mai del monomio di terzo grado. Dobbiamo pertanto cambiare nettamente famiglia; questa è la più semplice funzionante:

$$\begin{cases} x = \lambda t^2 \\ y = t^3 \end{cases} \quad (\lambda \neq 0)$$

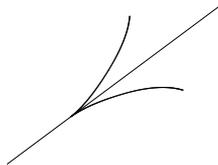
$$\begin{aligned} f(\lambda t^2, t^3) &= t^6 + a(\lambda t^2)^3 + b(\lambda t^2)^2 t^3 + c\lambda t^2 t^6 + et^4 + \dots \\ &= (1 + a\lambda^3)t^6 + (\quad) t^7 + \dots \end{aligned}$$

Vediamo che la molteplicità d'intersezione è almeno 6. Per annullare il primo coefficiente scegliamo

$$\lambda = \sqrt[3]{-\frac{1}{a}}$$

Esiste dunque una curva di questa famiglia che ci dice come è fatta la curva. Le curve di questa famiglia sono descrivibili in questo modo. Pensiamo ad esempio al caso $\lambda = 1$: abbiamo $y^2 = x^3$, che dal punto di vista dell'Analisi¹⁰ può essere visto come $y = \pm x^{3/2}$. Avremo dunque questa situazione:

¹⁰Solo dal punto di vista dell'Analisi! (Non è un polinomio.)



Definizione 1.15 Se la molteplicità d'intersezione tra l'unica tangente principale e la curva nel punto è esattamente 3 si parla di *cuspidi di prima specie*.

– $\nu_P(\mathbf{y} = 0, C) = 4 \Leftrightarrow \mathbf{a} = 0, e \neq 0$. Ripartiamo con le nostre parabole.

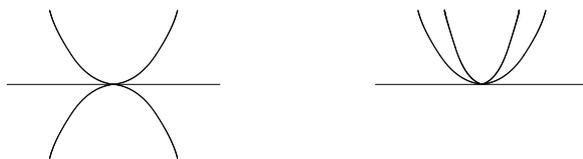
$$\begin{cases} x = t \\ y = \lambda t^2 \end{cases} \quad (\lambda \neq 0)$$

$$\begin{aligned} f(t, \lambda t^2) &= \lambda^2 t^4 + b t^2 \lambda t^2 + c t (\lambda t^2)^2 + d (\lambda t^2)^3 + e t^4 + \dots \\ &= (\lambda^2 + b\lambda + e)t^4 + (\dots)t^5 + \dots \end{aligned}$$

La generica parabola della famiglia interseca quindi la curva con molteplicità d'intersezione 4, ma due parabole avranno molteplicità superiore. Ora, i parametri λ relativi a queste sono le due soluzioni dell'equazione $\lambda^2 + b\lambda + e = 0$, nessuna delle quali può essere 0. Quindi abbiamo due parabole, dette *parabole osculatrici*. Queste possono essere due parabole reali distinte, due complesse coniugate oppure una sola parabola contata due volte.

Definizione 1.16 Se l'equazione ha due soluzioni complesse coniugate il punto si chiama *tacnodo isolato*;¹¹ se le soluzioni sono reali distinte si chiama *tacnodo*.

Comportamento qualitativo di un tacnodo:

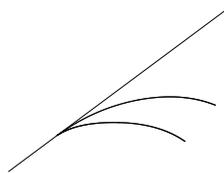


Se la soluzione è invece una sola contata due volte abbiamo una sola parabola osculatrice, e l'analisi non può terminare qui. Bisogna intersecare quest'unica parabola osculatrice con la nostra curva nel punto in questione.

Definizione 1.17 Se la molteplicità d'intersezione è ivi esattamente 5, il punto si dice *cuspidi di seconda specie*.

Il comportamento qualitativo di una tale cuspidi è questo, cioè come si suol dire un "rostro":

¹¹Il comportamento della curva è in tal caso indistinguibile da quello relativo ad un nodo isolato.



Può poi succedere che anche il coefficiente del termine di grado 5 si annulli, e la molteplicità d'intersezione sia ≥ 6 . In questo caso dobbiamo considerare delle curve un po' più complicate. Sia $\bar{\lambda}$ l'unica soluzione di $\lambda^2 + b\lambda + e = 0$.

$$\begin{cases} x = t \\ y = \bar{\lambda}t^2 + \mu t^3 \end{cases}$$

Intersecando la generica curva di questa famiglia con la nostra otteniamo un'altra espressione in cui ci sarà un coefficiente di II grado nella variabile μ . Se questa dà luogo a due soluzioni reali distinte abbiamo due *cubiche osculatrici*, che si presenteranno essenzialmente in uno di questi due modi:



Definizione 1.18 In questo caso il punto viene detto *oscnodo*. Se invece le soluzioni dell'equazione ottenuta sono due valori complessi coniugati si ha un *oscnodo isolato*.

Se per sventura l'equazione di II grado individua un unico valore del parametro μ per cui la molteplicità d'intersezione di questa famiglia di curve con la curva data è superiore alla generica, bisognerà intersecare la cubica osculatrice risultante con la curva e controllare la molteplicità d'intersezione. Se è 7 allora il punto sarà una *cuspidi di III specie*. Altrimenti bisogna andare avanti. È chiaro che pur di andare avanti un numero finito di volte si arriva ad ottenere una curva o due curve che parametrizzano i punti della nostra vicino al punto che stiamo considerando. Non spingeremo la nostra analisi così in fondo;¹² ci basta dire che è possibile farlo.

Esercizio 1.3.2 Ci si può sbizzarrire andando a vedere cosa succede quando il punto doppio da analizzare è improprio e quando la retta impropria è tangente.

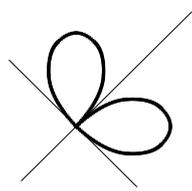
1.3.7 Cenni sui punti tripli

Dopo aver effettuato le consuete trasformazioni affini, il nostro polinomio si presenterà nella forma

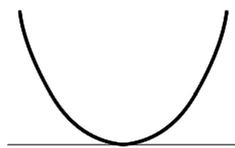
$$f(x, y) = \varphi_3 + \varphi_4 + \varphi_5 + \dots$$

¹²Anche perché non abbiamo (e non avremo) uno strumento adatto allo scopo: bisognerebbe utilizzare le cosiddette *approssimazioni quadratiche*, che vanno al di là del contenuto di questo corso.

con $\varphi_3 \neq 0$. Siccome φ_3 è un polinomio omogeneo nelle due variabili x e y , si potrà spezzare nel prodotto di tre fattori lineari i quali in generale ci daranno le tre tangenti principali fuoriuscenti da un punto triplo. Se le tangenti sono distinte, il punto si dirà *punto triplo ordinario*. Rispetto a ciascuna di queste tangenti principali potremmo fare un'analisi analoga a quella che abbiamo fatto per il punto doppio; la molteplicità d'intersezione con ciascuno di questi rami della curva nel punto si decomporrà in $2 + h$, dove la costante fissa 2 tiene conto della molteplicità d'intersezione di ciascun ramo con gli altri due che passano trasversalmente rispetto a quello, e h sarà la molteplicità relativa al ramo che stiamo considerando. Quindi l'eventuale parità che ci dice se il ramo rispetto alla tangente ha un certo comportamento andrà letta su questo numero, e sarà quindi pressappoco il contrario rispetto a quanto accadeva nel caso dei punti doppi. Potrebbe naturalmente succedere che le tangenti principali non siano tre distinte, ma ve ne siano due o anche tre coincidenti. Ad esempio:



tangente doppia

tangente tripla ($y^3 = x^4$)

Esempio Facciamo un esempio di curva che ha una cuspidi di I specie in un punto improprio.

$$f(x, y) = y - x^3 = 0$$

$$F(X : Y : U) = YU^2 - X^3 = 0$$

Qui possiamo immediatamente dire che Y_∞ è un punto doppio, e che la tangente principale è la retta impropria $U = 0$. Chiaramente se intersechiamo tale retta con la curva vediamo che questa ha con essa molteplicità d'intersezione 3:

$$\begin{cases} YU^2 - X^3 = 0 \\ U = 0 \end{cases} \rightarrow \begin{cases} X^3 = 0 \\ U = 0 \end{cases}$$

Osservazione Perché possiamo dire subito che Y_∞ è punto doppio? In realtà possiamo usare uno stratagemma. Consideriamo:

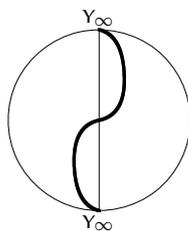
$$f(x, y) = a_0 + a_1(x, y) + a_2(x, y) + \dots + a_n(x, y) \quad \deg a_i = i$$

$$F(X : Y : U) = a_0 U^n + a_1(X : Y)U^{n-1} + a_2(X : Y)U^{n-2} + \dots + a_n(X : Y)$$

Notiamo ora che c'è una relazione tra il comportamento della curva nell'origine e la presenza o meno dei monomi U^q . Tanto per cominciare, la nostra curva passa per l'origine se e solo se $a_0 = 0$, e questo vuol dire in sostanza che è presente il monomio U^n . Supponiamo ora che effettivamente la curva passi per quel punto, e che quindi non esista il monomio U^n . Abbiamo visto che se a_0 non c'è e il punto passa per l'origine la curva ha un punto liscio se e solo se $a_1 \neq 0$; e questo è equivalente a richiedere la presenza di U^{n-1} nella chiusura proiettiva del polinomio. Inoltre la retta tangente si ottiene eguagliando a zero il coefficiente relativo a U^{n-1} . Questa analisi può essere spinta più avanti. Supponiamo di avere un punto doppio: $a_0 = a_1 = 0$, $a_2 \neq 0$. Questo equivale a dire $\nexists U^n$, $\nexists U^{n-1}$, $\exists U^{n-2}$. Inoltre le tangenti principali si ottengono eguagliando a zero $a_2(x, y)$, che non è altro che il coefficiente di U^{n-2} . E così possiamo andare avanti per i punti tripli e tutti gli altri punti multipli. Ora,

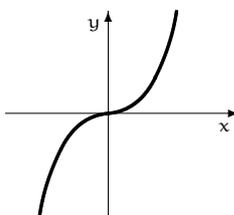
possiamo vedere che la stessa analisi si può trasferire pari pari anche ad altri due punti del piano proiettivo, i.e. $Y_\infty \equiv (0 : 1 : 0)$ e $X_\infty \equiv (1 : 0 : 0)$, perché esiste una proiettività che sposta ovviamente l'origine in uno di questi punti (basta scambiare i nomi delle variabili). Quindi la chiusura proiettiva di una certa curva affine passa per Y_∞ se e solo se non è presente il monomio Y^n , dove n è il grado del polinomio. Se passa per Y_∞ , questo è un punto semplice se e solo se, non essendoci Y^n , è presente Y^{n-1} . Se non c'è neppure Y^{n-1} andiamo a vedere qual è la potenza massima della Y che compare; se questa è $n-2$ allora Y_∞ è punto doppio, e le tangenti principali si ottengono eguagliando a zero il coefficiente di Y^{n-2} . E così via.

Torniamo al nostro esempio. Vediamo che la tangente principale in Y_∞ è $U = 0$ contata due volte. Per vedere che nel punto in questione la curva presenta una cuspidi di I specie dovremmo fare l'intersezione di questa tangente principale con la curva nel punto, e vedere qual è la molteplicità d'intersezione. Ma sappiamo già che questa sarà 3, perché questa è una cubica, e la molteplicità d'intersezione di una cubica in un punto non può superare 3; d'altro canto, siccome $U = 0$ è tangente principale, deve essere ≥ 3 . Il comportamento della nostra curva sarà pertanto questo:

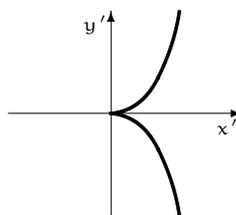


Questa curva si presta anche ad un'altra osservazione. Consideriamo le due curve:

$$\begin{aligned} y - x^3 &= 0 \\ YU^2 - X^3 &= 0 \end{aligned}$$



$$\begin{aligned} y'^2 - x'^3 &= 0 \\ U'Y'^2 - X'^3 &= 0 \end{aligned}$$



Una presenta una cuspidi di I specie nell'origine del sistema di riferimento, l'altra un flesso ordinario. Queste due curve sono in realtà gemellate, e si vede benissimo passando alla chiusura proiettiva delle due. Possiamo realizzare una proiettività tra i due piani proiettivi:

$$\begin{cases} X' = X \\ Y' = U \\ U' = Y \end{cases} \quad \begin{vmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{vmatrix} \neq 0$$

Applicando le sostituzioni indicate, ciascuna delle due curve si trasforma nell'altra, e le due sono quindi proiettivamente equivalenti, ovvero dal nostro punto di vista sono la stessa curva. Questo non è sorprendente, perché ogni curva proiettiva è chiusura proiettiva di tante curve affini, a seconda di quale sia la retta impropria.

Abbiamo fatto tutta l'analisi dei punti multipli portando il punto nell'origine e supponendo che la retta tangente fosse l'asse delle x . Ma chiaramente nei casi concreti il punto non sarà nell'origine, e la tangente non sarà l'asse delle

x. Come ci regoleremo in queste situazioni? Ci sono due modi per risolvere la questione. Il primo modo è quello di operare come abbiamo fatto nell'analisi, cioè si sceglie una trasformazione affine che porti il punto nell'origine in modo che la retta tangente sia l'asse delle x e si fa l'analisi; dopodiché si ritorna con l'affinità inversa alla situazione iniziale.¹³ La seconda strada consiste invece nell'eseguire direttamente tutta l'analisi nel punto senza trasferirlo. Per far questo è opportuno capire come scegliere le famiglie di curve da usare per approssimare l'andamento della nostra curva in questa situazione.

Noi sappiamo come individuare un fascio di coniche nel piano: basta fissare 4 condizioni lineari e andare a considerare le coniche che le soddisfano. Per ottenere tutte le equazioni di una famiglia di coniche è sufficiente fare combinazione lineare di due di queste, solitamente di quelle riducibili. Ci sono poi delle situazioni particolari in cui uno può scegliere ad esempio un fascio di parabole. Nella nostra situazione abbiamo un punto $P_0 = (x_0, y_0)$, la retta tangente r e la retta impropria $U = 0$; prendiamo infine una qualunque retta passante per P_0 contata due volte. Ad esempio prendiamo la retta $X - x_0U = 0$, e diciamo che r abbia equazione $ax + by + c = 0$. Combinando la retta arbitraria contata due volte con la conica costituita dalla retta tangente e della retta impropria

$$\lambda(X - x_0U)^2 + (aX + bY + cU)U = 0$$

abbiamo effettivamente una famiglia di parabole all'interno della quale possiamo andare a cercare le parabole osculatrici alla curva.

1.3.8 Stima dei punti singolari

Trovare i punti singolari di una curva non è molto semplice in generale, perché si tratta di andare a intersecare tre nuove curve che nascono dalla curva di partenza andando ad eguagliare a zero le derivate parziali del polinomio omogeneo. È pertanto opportuno avere una stima *a priori* del massimo numero di punti singolari che una curva può avere. Esistono due stime di questo tipo: una per le curve ridotte e una per le curve irriducibili ridotte.

Lemma Siano $C, C' \subset \mathbf{P}^2(\mathbb{C})$, $P \in C \cap C'$.

$$\nu_P(C, C') \geq \nu_P(C)\nu_P(C').$$

Inoltre vale l'uguaglianza se tutte le tangenti nel punto P sono distinte.

Lemma Sia $C \subset \mathbf{P}^2(\mathbb{C})$, sia $P \in C$ con $\nu_P(C) = k \geq 2$. Sia $C_X = (Z(F_X), F_X)$, con $F_X \neq 0$.

$$\nu_P(C_X) \geq \nu_P(C) - 1.$$

Dimostrazione Possiamo supporre $P \equiv (0 : 0 : 1)$. Sia

$$F = a_k(X : Y)U^{n-k} + a_{k+1}(X : Y)U^{n-(k+1)} + \dots + a_n(X : Y)$$

con $\deg a_i = i$ e $a_k \neq 0$.

$$F_X = \frac{\partial a_k}{\partial X}(X : Y)U^{n-k} + \frac{\partial a_{k+1}}{\partial X}(X : Y)U^{n-(k+1)} + \dots + \frac{\partial a_n}{\partial X}(X : Y)$$

¹³Questo è conveniente soprattutto per analizzare punti all'infinito.

Consideriamo il polinomio omogeneo relativo a U^{n-k} . Siccome $a_k(X : Y)$ è un polinomio omogeneo, la sua derivata parziale rispetto a X o è 0 oppure è un polinomio omogeneo di grado $k-1$. Se non è 0, F_X si scrive partendo con una parte omogenea in $(X : Y)$ di grado $k-1$, quindi la molteplicità della curva C_X nel punto P è esattamente $k-1$. Se invece la derivata che stiamo considerando è 0, vuol dire che la nostra curva si scrive partendo da un polinomio omogeneo di grado k ; se anche questo è nullo bisogna vedere cosa succede dopo, e così via. In ogni caso, la molteplicità che la curva assume nel punto P non può essere minore di $k-1$. \square

Proposizione 1.8 Sia $C \subset \mathbf{P}^2(\mathbb{C})$ ridotta di ordine $n \geq 2$.

$$\sum_{P \in \text{Sing}(C)} \nu_P(C)(\nu_P(C) - 1) \leq n(n-1).$$

Osservazione Questa stima non può essere migliorata, perché tra le curve di questo tipo ci sono quelle spezzate in n rette che passano per un punto, che avrà molteplicità n e sarà l'unico punto singolare della curva. È chiaro che per questo tipo di curve nella formula vale l'uguaglianza.

Dimostrazione Mettiamo a confronto C e C_X (possiamo supporre almeno una delle derivate parziali non nulla, perché altrimenti la curva sarebbe spezzata in n rette passanti per un punto e sappiamo già che in tal caso la relazione è vera). Per poter applicare il teorema di Bézout all'intersezione di queste due curve dobbiamo garantirci che queste non abbiano alcuna componente irriducibile in comune.

Possiamo sempre scegliere un sistema di riferimento in maniera t.c. $X_\infty \notin C$. Questo ci dice che nella scrittura del polinomio della C ci deve essere X^n :

$$F = a_0 X^n + a_1 X^{n-1} + \dots + a_n \quad a_i = a_i(Y : U) \quad \deg a_i = i$$

Supponiamo che esista una componente irriducibile di C che fa parte anche di C_X : supponiamo $F = HG$, con H irriducibile, e che $H \mid F_X$. Siccome F è di grado n nella variabile X , possiamo pensare anche H e G di un certo grado in X . Sicuramente, siccome in F compare il polinomio X^n , il grado di H rispetto a X non può essere 0. Abbiamo:

$$F_X = H_X G + H G_X$$

$$F_X - H G_X = H_X G$$

Siccome $H \mid F_X$ è anche $H \mid (F_X - H G_X)$, e quindi $H \mid H_X G$. Ma H è irriducibile, e $H \nmid H_X$ perché $\deg H_X < \deg H$, quindi $H \mid G$. Questo significa che possiamo scrivere $F = H^2 \overline{G}$ per un certo \overline{G} , sicché la curva di partenza non sarebbe ridotta. Quindi non era possibile supporre che esistesse una componente irriducibile in comune tra C e C_X , e possiamo dunque applicare il teorema di Bézout.

$$\begin{aligned} n(n-1) &= \sum_{P \in C \cap C_X} \nu_P(C, C_X) \geq \sum_{P \in \text{Sing}(C)} \nu_P(C, C_X) \\ &\geq \sum_{P \in \text{Sing}(C)} \nu_P(C) \nu_P(C_X) \geq \sum_{P \in \text{Sing}(C)} \nu_P(C)(\nu_P(C) - 1). \quad \square \end{aligned}$$

Esercizio 1.3.3 Controllare che la disuguaglianza sia vera nel caso $n = 3$, in cui è facile elencare tutti i possibili tipi di curve ridotte (la curva può spezzarsi o in una retta e una conica irriducibile oppure in tre rette).

Osservazione Per le cubiche irriducibili può succedere al massimo che abbiano un punto doppio. Se infatti una tale cubica avesse due punti doppi, potremmo considerare la retta che passa per essi, e questa avrebbe con la curva una molteplicità d'intersezione ≥ 4 in contraddizione al teorema di Bézout. Non può neppure avere un tacnod, perché questo richiede che la tangente cuspidale abbia molteplicità d'intersezione 4.

Nel caso delle curve irriducibili abbiamo una seconda stima, molto più riduttiva. Rimandiamo la dimostrazione alla fine di questo capitolo.

Proposizione 1.9 Sia $C \subset \mathbf{P}^2(\mathbb{C})$ irriducibile ridotta di ordine $n \geq 2$.

$$\sum_{P \in \text{Sing}(C)} \frac{\nu_P(C)(\nu_P(C) - 1)}{2} \leq \frac{(n-1)(n-2)}{2}.$$

Questa stima è molto importante, perché esistono delle curve irriducibili ridotte per cui nella formula vale l'uguaglianza. Queste curve sono in realtà tutte e sole le curve razionali.

Definizione 1.19 Una curva irriducibile ridotta è *razionale* se ha il massimo numero di punti singolari compatibile con il proprio ordine.

Rette e coniche sono le uniche curve razionali lisce. Le curve razionali sono particolarmente belle perché sono le uniche che ammettono una parametrizzazione globale con funzioni razionali. Finora abbiamo descritto una curva algebrica localmente vicino a un punto tramite una coppia di funzioni che erano in realtà dei polinomi in t , ma l'abbiamo fatto per studiare la singolarità della curva nel punto o il suo comportamento in un punto liscio. Uno può però anche chiedersi se per una curva irriducibile ridotta non esista una coppia di funzioni

$$\begin{cases} x = x(t) \\ y = y(t) \end{cases} \quad \text{t.c.} \quad \forall t \in \mathbb{C} \setminus \{t_1, \dots, t_q\} \quad f(x(t), y(t)) = 0.$$

1.4 Curve razionali e criteri di razionalità

Definizione 1.20 Chiamiamo *razionale* una funzione¹⁴

$$\begin{aligned} \varphi : \mathbb{C} &\rightarrow \mathbb{C}^2 \\ t &\mapsto (x(t), y(t)) \end{aligned}$$

definita per¹⁵ $t \in \mathbb{C} \setminus \{t_1, \dots, t_q\}$, dove

$$x(t) = \frac{a(t)}{b(t)}, \quad y(t) = \frac{c(t)}{d(t)} \quad a, b, c, d \in \mathbb{C}[t].$$

Definizione 1.21 Chiamiamo *curva razionale* una curva irriducibile ridotta $C \subset \mathbf{A}^2(\mathbb{C})$ i cui punti, salvo al più un numero finito, si ottengono come valori di una funzione razionale. Ovvero:

$$\forall P \in C \setminus \{P_1, \dots, P_k\} \quad P \equiv (x, y) : \exists t \in \mathbb{C} : \begin{cases} x = x(t) \\ y = y(t) \end{cases}$$

Una curva di $\mathbf{P}^2(\mathbb{C})$ si dirà *razionale* se è la chiusura proiettiva di una curva affine razionale.

Osservazione Quest'ultima definizione non è ambigua, perché la razionalità non dipende da un certo numero di punti della curva.

¹⁴È possibile sostituire ogni occorrenza di \mathbb{C} con \mathbb{R} .

¹⁵Potrebbe infatti essere necessario escludere un numero finito di valori, corrispondenti agli zeri dei polinomi $b(t)$ e $d(t)$.

Stabilire se una curva è razionale non è per nulla facile. Esistono però dei criteri di razionalità, di cui presentiamo ora il più diffuso.

Abbiamo già detto che per una curva irriducibile ridotta $C \subset \mathbf{P}^2(\mathbb{C})$ vige

$$\sum_{P \in \text{Sing}(C)} \frac{\nu_P(C)(\nu_P(C) - 1)}{2} \leq \frac{(n-1)(n-2)}{2}$$

e che vale l'uguaglianza se e solo se C è razionale. Potremmo definire *genere* di C il valore

$$g(C) \stackrel{\text{“=”}}{=} \frac{(n-1)(n-2)}{2} - \sum_{P \in \text{Sing}(C)} \frac{\nu_P(C)(\nu_P(C) - 1)}{2}$$

sicché una curva è razionale se e solo se ha genere 0. Il problema è che, mentre questo è vero, non è vero che il genere si può sempre calcolare con questa formula. Non sempre, ma molto spesso; ad esempio, se tutti i punti singolari della curva sono ordinari.

Definizione 1.22 Sia $C \subset \mathbf{P}^2(\mathbb{C})$ una curva irriducibile ridotta di ordine n con δ nodi e k cuspidi di I specie. Dicesi *genere* di C

$$g(C) = \frac{(n-1)(n-2)}{2} - \delta - k.$$

Si può spingere quest'analisi un po' oltre, dicendo che esiste una sorta di contabilità nera che permette di tradurre un certo tipo di punto singolare in termini di nodi. Per esempio, un tacnodo o una cuspidi di II specie conta come 2 nodi, un oscnodo come 3 nodi.

Definizione 1.23 Una curva di genere 1 è detta *curva ellittica*.¹⁶

Esempio Vediamo come non tutti i punti di una curva possano essere raggiunti dal parametro t . Prendiamo

$$\begin{cases} x = \frac{2t}{1+t^2} \\ y = \frac{1-t^2}{1+t^2} \end{cases}$$

che è una rappresentazione parametrica razionale di $x^2 + y^2 = 1$. Notiamo innanzitutto che i denominatori non si annullano mai, e che queste funzioni sono quindi definite su tutto l'asse reale. Tuttavia il punto $(0, -1)$ non si può ottenere con questa parametrizzazione, e anzi possiamo ottenere tutti i punti della circonferenza salvo proprio questo. Il punto è che questa parametrizzazione è stata costruita ragionando nel seguente modo, che vale per ogni conica: si sceglie un punto della conica e si considera il fascio di rette che lo ha per sostegno. Ciascuna retta del fascio incontra la conica in un altro punto: parametrizzando questa famiglia con un parametro affine t , in corrispondenza di ogni valore si hanno 2 punti della conica, di cui quello variabile fornisce la parametrizzazione.

Un altro esempio di questa situazione si presenta nel caso di curve ridotte con un solo punto singolare, e.g. un nodo. Si può allora fare lo stesso ragionamento usando però proprio il nodo come centro del fascio.

Non abbiamo ancora risposto ad una domanda: se assegnamo a casaccio due funzioni razionali nella variabile t , queste sono la rappresentazione parametrica di qualche curva del piano affine complesso? La risposta è sì. La dimostrazione di questo fatto richiede però la conoscenza della teoria del risultante.

¹⁶Le curve ellittiche trovano importanti applicazioni in crittografia.

1.5 Risultante di due polinomi

Sia A un UFD (noi useremo solo $\mathbb{C}[Y : \mathbf{U}]$ o $\mathbb{C}[y]$), e consideriamo due polinomi¹⁷ $f_m, g_n \in A[x]$ con $m, n \geq 1$. La domanda da cui partiamo è: esiste un facile criterio per stabilire se f e g ammettono almeno un fattore irriducibile in comune? È chiaro che la risposta può essere banale se si è disposti a fattorizzare. Il problema è che fattorizzare un polinomio in fattori irriducibili è un'impresa alquanto ardua.

L'osservazione chiave è questa. Supponiamo che esista un fattore irriducibile in comune, possiamo quindi scrivere:

$$\begin{cases} f = hu & \deg u < m \\ g = hv & \deg v < n \end{cases} \\ fv = huv = gu$$

Di questa proprietà vale però anche il viceversa, cioè se supponiamo

$$\begin{aligned} \exists u \neq 0 : \deg u < \deg f \\ \exists v \neq 0 : \deg v < \deg g \end{aligned}$$

con $fv = gu$ allora $\exists h$, ovvero f e g hanno un fattore irriducibile in comune; questo siccome esiste almeno un fattore di f che non compare in u (per via del grado) e che compare quindi in g .

Vediamo ora come utilizzare questa osservazione. Esponiamo, al posto della dimostrazione più generica possibile, un caso che faccia capire come funziona il meccanismo.

$$\begin{aligned} f(x) &= a_0x^3 + a_1x^2 + a_2x + a_3 & m &= 3 \\ g(x) &= b_0x^2 + b_1x + b_2 & n &= 2 \end{aligned}$$

Adesso scriviamo i polinomi u, v t.c. $\deg u < 3, \deg v < 2$ che soddisfino

$$(a_0x^3 + a_1x^2 + a_2x + a_3) \cdot \underbrace{(\alpha x + \beta)}_v - (b_0x^2 + b_1x + b_2) \cdot \underbrace{(\gamma x^2 + \delta x + \varepsilon)}_u = 0.$$

Cerchiamo le condizioni sotto le quali esistano due polinomi u, v (i.e. esistano $\alpha, \beta, \gamma, \delta, \varepsilon$) in maniera tale che quest'espressione sia identicamente nulla. Eseguiamo dunque i prodotti e organizziamo i coefficienti in maniera astuta, mettendo in evidenza come sono ottenuti a partire dai nostri parametri $\alpha, \beta, \gamma, \delta, \varepsilon$.

	α	β	γ	δ	ε
x^4	a_0		$-b_0$		
x^3	a_1	a_0	$-b_1$	$-b_0$	
x^2	a_2	a_1	$-b_2$	$-b_1$	$-b_0$
x^1	a_3	a_2		$-b_2$	$-b_1$
x^0		a_3			$-b_2$

Ora, affinché l'espressione sia identicamente nulla tutti i coefficienti devono essere nulli, e i coefficienti sono queste espressioni in $\alpha, \beta, \gamma, \delta, \varepsilon$. Ma questo non

¹⁷Nel seguito adotteremo la convenzione di indicare in pedice ai polinomi il rispettivo grado.

è altro che un sistema omogeneo di 5 equazioni in 5 incognite, di cui abbiamo scritto la matrice. Un sistema omogeneo ha come unica soluzione la soluzione nulla se e solo se il determinante della matrice associata è diverso da 0. Per avere una soluzione vera dobbiamo quindi richiedere che il determinante di questa matrice sia 0.

Definizione 1.24 Il determinante di questa matrice¹⁸ si dice *risultante* di f e g e si indica con $R(f, g)$.

Per ora abbiamo scritto la matrice così come saltava fuori facendo i conti, ma in realtà la matrice che si utilizza è la trasposta di questa, con i termini relativi a g moltiplicati per -1 .

La regola mnemonica per il calcolo del risultante è questa. Si scrivono sulla prima riga i coefficienti del I polinomio, poi ancora sulla seconda riga ma spostati di una colonna. Si fa questo tante volte quanto è il grado del II polinomio. Si fa quindi la stessa cosa con i coefficienti del II polinomio, tante volte quanto è il grado del I polinomio. Infine si riempiono con 0 gli spazi lasciati vuoti. Risulterà una matrice quadrata il cui ordine sarà la somma dei gradi dei due polinomi. Avremo quindi

$$\begin{vmatrix} a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \end{vmatrix} = R(f, g) \in A.$$

Conclusione: i due polinomi f, g hanno un fattore irriducibile in comune se e solo se questo elemento dell'anello A è lo zero dell'anello.

Osservazione Si potrebbe pensare che se l'anello A non è un campo la conclusione che abbiamo tratto non è valida, perché noi abbiamo introdotto la teoria dei sistemi di equazioni lineari per gli spazi vettoriali, quindi a coefficienti in un campo. In realtà non è così: anche se fossimo in un anello potremmo (siccome abbiamo supposto A UFD) passare al suo campo dei quozienti, e le osservazioni fatte finora andrebbero pari pari, salvo al più eliminare alla fine un certo numero di denominatori che darebbero fastidio.

Osservazione C'è una differenza sostanziale tra l'uso di \mathbb{C} e di \mathbb{R} : se il campo è \mathbb{C} , la nostra conclusione ci dice automaticamente che i due polinomi f, g hanno anche una radice in comune.

Esempio Prendiamo due polinomi particolari, per capire come in realtà conosciamo già una sorta di risultante.

$$\begin{aligned} f(x) &= ax^2 + bx + c & a \neq 0 \\ f'(x) &= \frac{df}{dx} = 2ax + b \end{aligned}$$

Risulta:

$$R(f, f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = ab^2 + 4a^2c - 2ab^2 = -a(b^2 - 4ac)$$

Dobbiamo chiederci quando questo numero reale è 0. Siccome $a \neq 0$, l'unica cosa che conta è $b^2 - 4ac$, che è il cosiddetto *discriminante* dell'equazione di II grado, e che

¹⁸Questa matrice viene chiamata *matrice di Sylvester*.

è zero se e solo se f ha una radice contata due volte. In effetti, poiché un polinomio abbia una radice multipla, questa radice deve essere comune a lui e al suo polinomio derivato.

La più importante applicazione della teoria del risultante è la determinazione dei punti in comune a due curve algebriche piane. Prendiamo due curve $C, C' \subset \mathbf{A}^2(\mathbb{C})$, e sia $A = \mathbb{C}[x]$.

$$\begin{aligned} C &= (Z(f), f) & f \in A[y] & f(x, y) = a_0 y^m + a_1 y^{m-1} + \cdots + a_m \\ C' &= (Z(f'), f') & f' \in A[y] & f'(x, y) = b_0 y^n + b_1 y^{n-1} + \cdots + b_n \end{aligned}$$

È chiaro che se i polinomi sono entrambi nella sola variabile x sappiamo già come procedere, perché tali polinomi sono delle rette parallele all'asse delle y e il problema si riduce a cercare le radici comuni.

Se invece abbiamo a che fare con polinomi generici, l'idea è questa: si fissa un valore \bar{x} e si considera la retta $x = \bar{x}$, che incontrerà ciascuna curva in un certo numero di punti. Le coordinate y di questi punti si troveranno risolvendo

$$f(\bar{x}, y) = 0, \quad f'(\bar{x}, y) = 0.$$

Se andiamo a scegliere un \bar{x} corrispondente ad una retta passante per uno dei punti comuni alle due curve, ci sarà almeno una radice comune alle due equazioni. Possiamo quindi far variare la x e per ogni valore andare a considerare quali sono le eventuali radici comuni di queste due equazioni nella sola variabile y . Sia e.g. $m = 3, n = 2$; dobbiamo controllare se vale 0 il risultante

$$\begin{vmatrix} a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \end{vmatrix} = R(f, f') \in A = \mathbb{C}[x].$$

Attenzione però, perché c'è un problema. Quando avevamo introdotto il risultante ci eravamo premurati di avere $a_0, b_0 \neq 0$, perché solo così il risultante si può scrivere in questa maniera. Nella nostra situazione specifica, quando fissiamo un certo \bar{x} può tranquillamente succedere che questo sia radice di $a_0(x)$ o di $b_0(x)$. In tal caso un polinomio calerebbe di grado, e il risultante andrebbe scritto in un altro modo.

Dobbiamo dunque fare una richiesta preventiva, e cioè che $a_0(x), b_0(x)$ non abbiano radici comuni. Altrimenti il metodo funziona solo per i valori di \bar{x} che non sono radici comuni, e ci possono essere dei punti comuni che sfuggono a questa ricerca.

Osservazione Perché non abbiamo richiesto semplicemente $a_0(x) \neq 0$ e $b_0(x) \neq 0$? Per fortuna, per come è stato definito il risultante, se una sola delle due equazioni cala di grado non è un problema.¹⁹

Esempio Consideriamo:

$$\begin{aligned} C : & (1-x)y^2 + y + 1 = 0 & m &= 2 \\ C' : & (1-x)y + 1 = 0 & n &= 1 \end{aligned}$$

¹⁹Si provi a vedere come cambia in tali casi il calcolo del determinante della matrice.

Calcoliamo il risultante.

$$\begin{vmatrix} 1-x & 1 & 1 \\ 1-x & 1 & 0 \\ 0 & 1-x & 1 \end{vmatrix} = (1-x) + (1-x)^2 - (1-x) = (1-x)^2 = R(x)$$

$$R(x) = 0 \Leftrightarrow x = 1$$

Purtroppo però $x = 1$ è esattamente uno dei casi che devono essere evitati, perché entrambi i coefficienti di grado massimo si annullano; non possiamo pertanto dedurre alcunché dal fatto che $x = 1$ è radice del risultante, e non è detto che in corrispondenza di questa radice ci sia un punto comune alle due curve. Nel caso concreto proviamo a sostituire $x = 1$:

$$\begin{cases} y + 1 = 0 \\ 1 = 0 \end{cases}$$

è impossibile, pertanto in corrispondenza di $x = 1$ non ci sono punti in comune alle due curve. Questo è un esempio talmente sfortunato che il metodo che abbiamo appena introdotto non serve proprio a nulla. Ciò accade perché l'ambito giusto in cui trovare i punti comuni non è il piano affine complesso, bensì il piano proiettivo complesso.

Esercizio 1.5.1 Scoprire dove sono finiti i 6 punti che qui non si vedono.

Parliamo ora di un'altra applicazione della teoria del risultante. Abbiamo visto come sono definite le curve razionali. Se prendiamo

$$\varphi : \begin{cases} x = \frac{a(t)}{b(t)} \\ y = \frac{c(t)}{d(t)} \end{cases} \quad \begin{array}{l} t \in \mathbb{C} \setminus \{t_1, \dots, t_q\} \\ \varphi : \mathbb{C} \setminus \{t_1, \dots, t_q\} \rightarrow \mathbb{C}^2 \end{array}$$

in realtà l'immagine di φ è supporto di una certa curva algebrica, cioè esiste sempre una curva algebrica $C = (Z(f), f)$ tale che

$$f(x(t), y(t)) \equiv 0.$$

La teoria del risultante ci dice anche come trovare f . Scriviamo le nostre espressioni in una maniera un po' diversa:

$$\left. \begin{array}{l} 0 = b(t)x - a(t) = g \\ 0 = d(t)y - c(t) = g' \end{array} \right\} \in \underbrace{\mathbb{C}[x, y][t]}_A$$

Risulta $R(g, g') = f(x, y) \in A$, quindi l'immagine di una funzione razionale del tipo dato è una curva algebrica.

Perché la cosa funziona? È chiaro che il risultante è un polinomio in x, y , e individuerà quindi una certa curva: $R = (Z(f), f)$. Il punto è far vedere che si tratta di una curva algebrica di cui quella data è una rappresentazione parametrica razionale. Prendiamo $(\bar{x}, \bar{y}) \in Z(f)$. Se $f(\bar{x}, \bar{y}) = 0$ significa che

$$\exists \bar{t} : \begin{cases} b(\bar{t})\bar{x} - a(\bar{t}) = 0 \\ d(\bar{t})\bar{y} - c(\bar{t}) = 0 \end{cases}$$

Ma allora questo \bar{t} , salvo alcune eccezioni, è esattamente un valore di \mathbb{C} che piazzato nella parametrizzazione riconduce al punto di coordinate (\bar{x}, \bar{y}) . Con una certa cautela però, perché questo \bar{t} potrebbe essere uno di quei valori che annullano $b(t)$ o $d(t)$; tuttavia questi sono in numero finito, quindi non ci interessa. Potrebbe anche succedere che nel calcolo del risultante entrambi i coefficienti

della potenza di grado massimo si annullino; scrivendo però il polinomio rispetto a t , il coefficiente relativo alla potenza massima sarà un polinomio nella singola variabile x , quindi esiste solo un numero finito di valori che possono annullare i coefficienti di grado massimo della φ . Questo significa che avremo in corrispondenza di questi eventuali valori di x dei punti della curva $(Z(f), f)$ che non avranno una rappresentanza tramite t . Sono però comunque in numero finito, e siccome la definizione di curva razionale è sempre a meno di un numero finito di punti della curva stessa tutto questo non ci preoccupa minimamente.

A voler essere veramente molto pignoli,²⁰ qualcuno potrebbe obiettare che la definizione di curva razionale nel piano affine complesso l'abbiamo data solamente quando la curva è preventivamente irriducibile ridotta, quindi bisognerebbe cautelarsi del fatto che la curva così prodotta soddisfi anche queste richieste. Ma in effetti è così, perché questa è l'immagine di un polinomio che rispetto alla variabile x ha grado 1.

Esercizio 1.5.2 Cercare la curva algebrica razionale parametrizzata da

$$\begin{cases} x = t^2 \\ y = t^3 - t \end{cases} \quad t \in \mathbb{C}.$$

Impostiamo il conto:

$$\begin{cases} g = t^2 - t + y = 0 \\ g' = t^2 - x = 0 \end{cases} \quad \begin{vmatrix} 1 & 0 & -1 & y & 0 \\ 0 & 1 & 0 & -1 & y \\ 1 & 0 & -x & 0 & 0 \\ 0 & 1 & 0 & -x & 0 \\ 0 & 0 & 1 & 0 & -x \end{vmatrix} = 0$$

(Soluzione: $f(x, y) = y^2 - x(x-1)^2$.)

1.6 Il teorema di Bézout

Vogliamo ora applicare la teoria del risultante per dimostrare il teorema di Bézout. Per fare questo abbiamo però bisogno di un preliminare: cosa succede alla teoria del risultante se consideriamo dei polinomi omogenei? Prendiamo due polinomi $F, F' \in \underbrace{\mathbb{C}[X, U]}_A[Y]$

$$\begin{aligned} F &= a_0 Y^m + a_1 Y^{m-1} + \dots + a_m \\ F' &= b_0 Y^n + b_1 Y^{n-1} + \dots + b_n \end{aligned}$$

omogenei e con la ulteriore cautela che siano proprio di grado m e n , ovvero che gli a_i, b_i abbiano grado i .

Lemma $R = R(F, F') = R(X : U)$ è un polinomio omogeneo di grado mn .

Dimostrazione Vediamo il caso $m = 3, n = 2$. Abbiamo

$$R(X : U) = \begin{vmatrix} a_0 & a_1 & a_2 & a_3 & 0 \\ 0 & a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & 0 & 0 \\ 0 & b_0 & b_1 & b_2 & 0 \\ 0 & 0 & b_0 & b_1 & b_2 \end{vmatrix}.$$

²⁰Ma siamo qui anche per fare questo.

Vogliamo ora mostrare $R(tX : tU) = t^\rho R(X : U)$, con $\rho = mn$.

$$R(tX : tU) = \begin{vmatrix} a_0 & ta_1 & t^2a_2 & t^3a_3 & 0 \\ 0 & a_0 & ta_1 & t^2a_2 & t^3a_3 \\ b_0 & tb_1 & t^2b_2 & 0 & 0 \\ 0 & b_0 & tb_1 & t^2b_2 & 0 \\ 0 & 0 & b_0 & tb_1 & t^2b_2 \end{vmatrix}.$$

Avendo raccolto nella scrittura della matrice tutte le t , ora a_i e b_i sono polinomi nelle sole variabili $(X : U)$. Una proprietà del determinante è che se moltiplichiamo tutti i termini di una riga o di una colonna per un certo valore il determinante sarà pari a quello della vecchia matrice moltiplicato per tale numero. Se quindi moltiplichiamo la i -esima riga di ciascun blocco per t^i otteniamo

$$\begin{vmatrix} ta_0 & t^2a_1 & t^3a_2 & t^4a_3 & 0 \\ 0 & t^2a_0 & t^3a_1 & t^4a_2 & t^5a_3 \\ tb_0 & t^2b_1 & t^3b_2 & 0 & 0 \\ 0 & t^2b_0 & t^3b_1 & t^4b_2 & 0 \\ 0 & 0 & t^3b_0 & t^4b_1 & t^5b_2 \end{vmatrix} = R(tX : tU)t^{(1+2)+(1+2+3)}.$$

Notiamo però che sulle colonne compare una potenza successiva crescente della t fino ad arrivare a $m+n$. Applicando dunque la stessa proprietà sulle colonne questo polinomio coincide con $t^{1+2+3+4+5}R(X : U)$, perciò semplificando risulta

$$R(tX : tU) = t^6R(X : U).$$

E in generale? Da una parte avremo la somma dei primi $n + m$ interi, dall'altra la somma dei primi n interi più la somma dei primi m interi, ovvero

$$R(tX : tU) = t^\rho R(X : U)$$

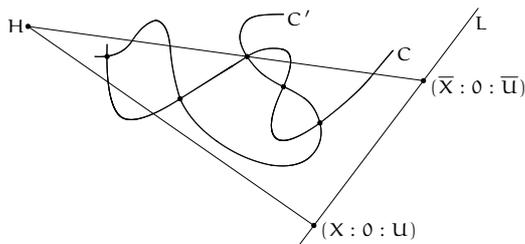
con

$$\begin{aligned} \rho &= \frac{(m+n)(m+n+1)}{2} - \frac{n(n+1)}{2} - \frac{m(m+1)}{2} \\ &= \frac{1}{2}(m^2 + mn + m + mn + n^2 + n - n^2 - n - m^2 - m) = mn. \quad \square \end{aligned}$$

Teorema 1.3 (di Bézout) Siano $C, C' \subset \mathbf{P}^2(\mathbb{C})$ di ordini rispettivi m, n e che non abbiano componenti irriducibili in comune. Allora

$$\sum_{P \in C \cap C'} \nu_P(C, C') = mn.$$

Dimostrazione L'idea è quella di prendere un punto fissato H non appartenente a C né a C' e una retta L che non sia tra le componenti di C né di C' . Dopodiché in un certo senso proiettiamo le nostre due curve sulla retta L dal punto H , ovvero per ogni punto delle due curve andiamo a considerare l'intersezione tra la retta che lo congiunge ad H e la retta L . Se un punto è comune a C, C' allora esso farà parte del gruppo di punti d'intersezione di una retta con la C e del gruppo di punti d'intersezione della stessa retta con la C' .



Per poter fare i conti scegliamo $H = Y_\infty$ e $L \equiv Y = 0$, retta il cui generico punto avrà coordinate $(X : 0 : U)$. Fatta questa scelta possiamo andare a controllare come si presentano i polinomi F, F' relativi a C, C' . Abbiamo osservato a suo tempo che se una curva di \mathbf{P}^2 non passa per Y_∞ allora nel suo polinomio compare sicuramente fra gli addendi il monomio Y^n con coefficiente non-nullo. Possiamo quindi calcolare $R(F, F') = R(X : U)$, che sarà o identicamente nullo oppure omogeneo di grado mn . Se il polinomio è identicamente nullo allora F, F' devono avere qualche fattore irriducibile in comune, quindi C, C' hanno una componente irriducibile in comune, contro le ipotesi.

Andiamo a prendere le coppie $(\bar{X} : \bar{U})$ tali che $R(\bar{X} : \bar{U}) = 0$, e mostriamo che questi punti sulla retta L sono esattamente quelli in corrispondenza dei quali la retta per H ha davvero intersezione con C, C' in un punto comune alle due. Questo perché preso uno di tali valori le radici di $F(\bar{X} : Y : \bar{U}) = 0$, equazione di grado m in Y , ci danno l'ultima coordinata del punto $(\bar{X} : \bar{Y} : \bar{U})$ appartenente a C . Analogamente le radici di $F'(\bar{X} : Y : \bar{U}) = 0$ forniranno le coordinate dei punti di intersezione tra C' e la retta che stiamo considerando. Queste due equazioni hanno una radice in comune se e solo se esiste un punto comune a C, C' . Questo ci dice che il numero di punti comuni alle due curve è finito, perché le radici di $R(X : U) = 0$ sono al più mn e in corrispondenza di ciascuna retta c'è al massimo un numero finito di punti comuni, in quanto può esserci solo un numero finito di radici comuni alle due equazioni di grado finito m o n .

Non abbiamo però ancora concluso la dimostrazione, perché non c'è una corrispondenza biunivoca tra le radici del polinomio e i punti comuni alle due curve. Può infatti tranquillamente succedere che C, C' taglino punti allineati con il punto H e con uno dei punti per cui il risultante si annulla. Abbiamo però visto che il numero di punti comuni alle due curve è finito, e questo ci permette di dire che anche il numero di rette che uniscono coppie di punti comuni a C, C' è finito. Possiamo dunque scegliere un punto H che non stia su alcuna di queste rette²¹ e ripetere lo stesso ragionamento fatto finora. Questa volta però per ogni radice corrispondente a un punto della retta L non è più possibile che esistano due punti allineati con questo punto e con H e comuni a C, C' . Avremo dunque esattamente mn rette, su ciascuna delle quali c'è uno e un solo punto comune a C, C' . Ora, è vero che sulla retta L ci sono mn punti radici della nostra equazione, ma le radici sono mn pur di contarle con la dovuta molteplicità.

Definizione 1.25 La *molteplicità d'intersezione* di due curve in un certo punto è esattamente la molteplicità sulla retta L della radice corrispondente in $R(X : U)$.

Qualcuno potrebbe sospettare che la definizione non sia ben posta, ovvero che cambiando il sistema di riferimento anche questa definizione cambi. E invece no.²²

Detto questo, il teorema è una banalità, perché per come abbiamo definito la molteplicità d'intersezione è ovvio che la somma delle molteplicità d'intersezione è mn . \square

Osservazione Naturalmente se due curve si tagliano trasversalmente la molteplicità d'intersezione è 1, perché questa definizione tiene conto di quante sono le radici relative a punti d'intersezione tra la retta e ciascuna curva che vanno a collassare. Se invece una curva ha un punto doppio e l'altra un punto semplice i punti che vanno a collassare sono 3, e la molteplicità d'intersezione è 2. Le cose si complicano molto se le curve si tagliano in maniera tale da avere una tangente comune, e l'unico modo per scoprire quanti punti vanno a collassare è impostare il conto e andare a vedere qual è la molteplicità della radice in quel punto.

²¹Queste rette del piano costituiscono quello che si chiama un *chiuso di Zariski*. Ogni volta che prendiamo in $\mathbf{P}^2(\mathbb{C})$ un insieme finito di punti o di curve quello che otteniamo è un chiuso di Zariski. Il complementare è un *aperto di Zariski*.

²²La dimostrazione di tale affermazione richiede elementi di topologia di cui ancora non disponiamo. Diamola per buona.

Corollario Siano²³ $C, C' \subset \mathbf{P}^2(\mathbb{C})$, $\text{ord } C = \text{ord } C' = n$, con $C \cap C' = \{n^2 \text{ punti distinti}\}$. Se mn punti, con $0 < m < n$, stanno su una curva D_m irriducibile ridotta allora esiste una curva E_{n-m} passante per gli altri $n^2 - mn$ punti.

Dimostrazione Siano $C = (Z(F), F)$, $C' = (Z(F'), F')$. Consideriamo tutti i polinomi del tipo $\lambda F + \mu F'$, con $(\lambda : \mu) \in \mathbf{P}^1(\mathbb{C})$; tutte le curve di tale fascio passano per i nostri n^2 punti. Se poi prendiamo un altro punto P qualunque, riusciamo a trovare almeno una curva della famiglia passante per quel punto; prendiamo per comodità $P \in D_m$, $P \notin \{C \cap C'\}$. Andando a valutare

$$\lambda F(P) + \mu F'(P),$$

è sempre possibile trovare $(\bar{\lambda} : \bar{\mu})$ t.c. questa espressione sia zero, e in corrispondenza di questa coppia troviamo un polinomio $G = \bar{\lambda}F + \bar{\mu}F'$ che darà luogo ad una certa curva $\Gamma = (Z(G), G)$. Γ è di ordine n , e ha in comune con D_m sicuramente gli nm punti che erano tra gli n^2 , e in più il punto P , in totale $nm+1$ punti. Questo violerebbe il teorema di Bézout, che quindi non si può applicare; le due curve devono dunque avere almeno una componente irriducibile in comune. Ma siccome D_m è già irriducibile ridotta, e il suo ordine è inferiore a quello di Γ_n , l'unica possibilità è

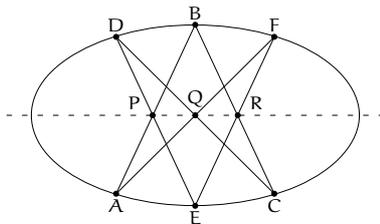
$$\Gamma_n = D_m \cup E_{n-m}$$

per una certa curva E di ordine $n - m$. □

Un'applicazione di questo corollario è il cosiddetto teorema di Pascal sugli esagoni inscritti in una conica. Si tenga presente che in geometria proiettiva un esagono è semplicemente l'insieme di 6 punti e 6 rette che uniscono questi punti secondo una certa regola combinatoria. Queste rette possono anche intrecciarsi, tuttavia manteniamo il concetto combinatorio di opposizione valido per gli esagoni regolari della geometria elementare.

Teorema 1.4 (di Pascal) Se un esagono proiettivo è inscritto in una conica²⁴ allora i punti d'intersezione dei lati opposti dell'esagono sono allineati.

Dimostrazione (caso di una conica irriducibile ridotta)



Individuiamo due curve C, C' che facciano al caso nostro

$$\begin{aligned} C &= \overline{AB} \cup \overline{EF} \cup \overline{CD} \\ C' &= \overline{DE} \cup \overline{BC} \cup \overline{FA} \end{aligned}$$

riducibili e ridotte di ordine 3, che si intersecano in 9 punti:

$$C \cap C' = \{A, B, C, D, E, F, P, Q, R\}.$$

Esiste peraltro una curva $D_2 \supset \{A, B, C, D, E, F\}$ irriducibile ridotta; applicando il risultato precedente con $m = 3$, $n = 2$, esiste una curva di ordine 1 (una retta) passante per P, Q, R . □

²³Si noti che non richiediamo C, C' irriducibili ridotte.

²⁴Ovvero i 6 vertici appartengono alla conica.

1.7 Polarità

Un'altra applicazione di quanto visto permette di generalizzare il concetto di polare già affrontato per le coniche. Consideriamo una curva irriducibile ridotta $C \subset \mathbf{P}^2(\mathbb{C})$, $C = (Z(F), F)$, $\text{ord } C = n$, e un punto $P \notin C$, $P \equiv (a : b : c)$.

Definizione 1.26 La curva associata al polinomio (omogeneo di grado $n - 1$)

$$aF_X + bF_Y + cF_U = 0$$

è detta *curva polare* rispetto al punto P della curva C , e si indica con $\text{Pol}_P(C)$.

Esercizio 1.7.1 Questa espressione non è mai identicamente nulla.

Esercizio 1.7.2 Per una conica liscia questa definizione coincide con quella già nota.

La curva polare così definita è interessante perché vale una sorta di generalizzazione della legge di reciprocità di Plücker già vista.

Proposizione 1.10 Se $Q \in C \setminus \text{Sing}(C)$ allora

$$P \in T_Q(C) \Leftrightarrow Q \in \text{Pol}_P(C).$$

Dimostrazione L'equazione della tangente in Q a C è

$$F_X|_Q X + F_Y|_Q Y + F_U|_Q U = 0.$$

Siccome questa retta passa per P vale

$$F_X|_Q a + F_Y|_Q b + F_U|_Q c = 0.$$

La condizione che ci dice che il punto Q sta sulla polare del punto P rispetto a C è esattamente la stessa. \square

Se vogliamo sapere quante sono le tangenti alla curva C uscenti dal punto $P \notin C$ possiamo quindi intersecare la polare del punto P con la curva C e vedere quanti sono i punti in comune. Quindi, siccome la curva C irriducibile ridotta ha ordine n e la curva polare ha ordine $n - 1$, il numero di punti in comune (pur di contarli con la dovuta molteplicità) è esattamente $n(n - 1)$.

Uno sarebbe dunque tentato di dire che, prendendo un punto $P \notin C$, il numero di tangenti a C uscenti da P è esattamente $n(n - 1)$. Purtroppo però non è esattamente così.

Se e.g. la curva C è singolare, il discorso fatto vale solo per i punti non singolari; in tal caso, inoltre, la polare di un punto $P \notin C$ passa sicuramente per ogni punto singolare della curva (per la definizione). Pertanto non sappiamo come contare la molteplicità.

Ma anche supponendo C liscia, c'è una questione ancora più spinosa. Può cioè succedere che la curva rispetto al punto P presenti delle bitangenti. Per uscirne osserviamo che le rette bitangenti sono comunque sempre in numero finito, quindi non è vero che per ogni punto $P \notin C$ liscia il numero di rette tangenti è proprio $n(n - 1)$, però è vero per un punto P generico, ovvero fuori da un opportuno chiuso di Zariski, costituito dalla curva stessa e da tutte le rette k -tangenti.

Perché possiamo dire che le rette bitangenti sono in numero finito? Ciò dipende dalla dualità. Data una curva irriducibile ridotta liscia $C \subset \mathbf{P}^2$, avremo anche la sua duale $C^* \subset \mathbf{P}^{2*}$ costituita dai punti relativi alle rette tangenti a C in \mathbf{P}^2 . Si può far vedere che anche C^* è irriducibile ridotta, mentre non è detto che sia anch'essa liscia. Notiamo poi che una bitangente ordinaria in \mathbf{P}^2 dà luogo a un nodo ordinario in \mathbf{P}^{2*} . Ora, sappiamo che C^* ha un numero finito di punti singolari, quindi il numero di rette bitangenti a C è finito.

Per quanto riguarda le curve singolari, la questione si può comunque trattare, a patto però che si scelgano delle curve domestiche dal punto di vista della dualità. Queste curve sono le curve irriducibili ridotte con un certo numero di nodi ordinari o tutt'al più cuspidi di I specie. Per tali curve si può dire parecchio sulla curva duale, grazie alle *formule di Plücker*:

	\mathbf{P}^2	\mathbf{P}^{2*}
ordine	n	$n' = m$ classe
nodi	δ	$\delta' = \tau$
cuspidi di I specie	k	$k' = i$
bitangenti ordinarie	τ	$\tau' = \delta$
flessi ordinari	i	$i' = k$

L'ordine della curva duale è la cosiddetta *classe* della curva di partenza. Andare a considerare l'ordine della curva duale vuol dire scegliere una retta generica, intersecarla con la curva duale e contare i punti di intersezione. Intersecare una retta generica con la curva duale significa andare a prendere il punto corrispondente per dualità a questa retta e andare a cercare le rette tangenti alla curva di partenza passanti per il punto. Quindi questa classe della curva di partenza, ordine della duale, è esattamente il numero di rette tangenti uscenti da un punto generico (i.e. fuori da quell'insieme finito di bitangenti o tangenti inflessionali che ci possono essere), ed è

$$m = n(n - 1) - 2\delta - 3k.$$

Esiste anche una formula analoga che permette di calcolare direttamente il numero dei flessi:

$$i = 3n(n - 2) - 6\delta - 8k.$$

Esempio Una cubica piana liscia ha 9 flessi; se ha una cuspidi ha un solo flesso.

Un'ultima relazione afferma

$$g(C^*) = g(C).$$

1.8 Sistemi lineari di curve piane

Finora abbiamo studiato le curve singolarmente. Come si può fare invece per considerarle nella loro interezza? Lo si può fare se se ne fissa l'ordine.

Nel caso dell'ordine $n = 1$ abbiamo in realtà già visto qualcosa di questo tipo: l'insieme di tutte le rette del piano proiettivo contiene infatti a sua volta un altro piano proiettivo, quello duale, vigendo la corrispondenza biunivoca tra rette e punti

$$\mathbf{P}^2 \supset l : aX + bY + cU = 0 \quad \leftrightarrow \quad (a : b : c) \in \mathbf{P}^{2*}.$$

Quello che vogliamo fare ora è generalizzare questa corrispondenza biunivoca al caso in cui le curve abbiano ordine $n \geq 2$.

Innanzitutto bisogna considerare come sono fatti i polinomi omogenei in tre variabili X, Y, U quando il grado del polinomio è ≥ 2 . Un tale polinomio sarà costituito da monomi $X^\alpha Y^\beta U^\gamma$ t.c. $\alpha + \beta + \gamma = n$. Per contare i monomi che possono comparire nella scrittura di un polinomio di grado n dobbiamo dunque contare i monomi di questo tipo. Il calcolo combinatorio ci dice che il numero di combinazioni con ripetizione di m oggetti presi a k a k è

$$C_{m,k}^* = \binom{m+k-1}{k}.$$

Quello che noi cerchiamo è

$$C_{3,n}^* = \binom{3+n-1}{n} = \binom{n+2}{n} = \binom{n+2}{2} = \frac{(n+2)(n+1)}{2}.$$

Controprova: nel caso $n = 2$ abbiamo proprio 6 monomi:

$$X^2 \quad XY \quad Y^2 \quad XU \quad YU \quad U^2$$

Chiaramente però i monomi non ci dicono tutto sul polinomio: dobbiamo considerare i coefficienti.

$$a_0 X^2 + a_1 XY + a_2 Y^2 + a_3 XU + a_4 YU + a_5 U^2 = 0$$

Notiamo che dal punto di vista dell'Algebra i polinomi sono individuati dai vari coefficienti, mentre dal punto di vista della teoria delle curve algebriche due polinomi che differiscono per un fattore moltiplicativo non-nullo sono da considerarsi la stessa curva. Siccome a noi interessano le curve, e non i polinomi, possiamo associare a ciascuna di queste curve la sfilza di coefficienti

$$(a_0 : a_1 : a_2 : a_3 : a_4 : a_5) \in \mathbf{P}^5.$$

In generale avremo uno spazio proiettivo \mathbf{P}^N , dove

$$N = \frac{(n+2)(n+1)}{2} - 1 = \frac{n^2 + 3n}{2}.$$

Quindi in sostanza possiamo costituire una corrispondenza biunivoca²⁵

$$\left\{ \begin{array}{l} \text{curve algebriche piane} \\ \text{proiettive di ordine } n \end{array} \right\} \leftrightarrow \mathbf{P}^N, \quad N = \frac{n^2 + 3n}{2}.$$

Una volta capita la corrispondenza, è chiaro che sono particolarmente interessanti i sottoinsiemi corrispondenti a sottoinsiemi particolari di \mathbf{P}^N , per esempio ai sottospazi lineari.

Definizione 1.27 Un *sistema lineare* di dimensione q è un sottoinsieme di curve algebriche piane proiettive che corrisponde tramite questa corrispondenza biunivoca ad un sottospazio lineare di \mathbf{P}^N di dimensione q .

²⁵Questa corrispondenza è stata uno dei motivi che hanno indotto a fine Ottocento i geometri algebrici a considerare gli spazi proiettivi di dimensione più elevata di 2 o 3.

Ora:

- Un punto $A \in \mathbf{P}^N$ corrisponde ad una sola curva.
- Due punti $A, B \in \mathbf{P}^N$ corrispondenti a due curve F_1, F_2 generano una retta in \mathbf{P}^N , e a tutti e soli i punti $P = \lambda A + \mu B$ di questa retta corrispondono tutte e sole le curve individuate da un polinomio della forma $F = \lambda F_1 + \mu F_2$. Quindi ogni volta che ho in \mathbf{P}^N una retta dall'altra parte ho un fascio di curve.
- Tre punti non allineati individuano un piano.

Una nomenclatura abbastanza antica chiama uno spazio lineare di dimensione 1 *fascio*, di dimensione 2 *rete*, di dimensione 3 *tessuto*, dopodiché non ci sono altri nomi specifici.

Come facciamo ad individuare un sottospazio lineare in \mathbf{P}^N ? Abbiamo già visto un modo, e cioè partendo dal basso andare a considerare lo span di un certo numero di punti. Ma in generale uno spazio lineare non viene costruito così. In generale lo si ottiene come intersezione di iperpiani (equazioni cartesiane). Se vogliamo trattare i nostri sistemi lineari da questo punto di vista dobbiamo andare a vedere a quali sottoinsiemi di curve corrisponde il generico iperpiano di \mathbf{P}^N .

La cosa non è così semplice. Ogni volta che consideriamo un iperpiano di \mathbf{P}^N diciamo dall'altra parte che abbiamo imposto alle curve una *condizione lineare*. Pertanto imporre una condizione lineare significa considerare tutte e sole quelle curve che corrispondono a un certo iperpiano di \mathbf{P}^N .

Il problema è che non esiste una maniera univoca per assegnare una condizione lineare, perché alcune condizioni non sono facilmente esprimibili, restano nascoste. La condizione lineare più semplice è il passaggio per un punto. Fissato un certo punto $P \equiv (\alpha : \beta : \gamma) \in \mathbf{P}^2(\mathbb{C})$ possiamo chiederci come sono fatte tutte le curve di ordine n passanti per P . Ad esempio per $n = 2$ la condizione si scrive così:

$$a_0\alpha^2 + a_1\alpha\beta + a_2\beta^2 + a_3\alpha\gamma + a_4\beta\gamma + a_5\gamma^2 = 0.$$

Questa possiamo vederla da un lato come una relazione che impone il passaggio della conica per P , dall'altro come l'equazione di un iperpiano in \mathbf{P}^N . Quindi il passaggio per un punto corrisponde effettivamente ad una condizione lineare.

Tuttavia esistono degli iperpiani che non provengono da questo processo. Se ad esempio consideriamo

$$a_1 + a_3 + a_4 = 0,$$

a tale iperpiano corrisponde un sistema lineare di dimensione $N-1$, e quindi una condizione lineare sulle curve dello spazio proiettivo di partenza. Però questa condizione non è ottenuta richiedendo il passaggio per un certo punto, perché se esistesse un punto il passaggio per il quale corrispondesse a questa condizione lineare dovrebbe succedere

$$\begin{cases} \alpha^2 = 0 \\ \alpha\beta = \rho \\ \beta^2 = 0 \\ \alpha\gamma = \rho \\ \beta\gamma = \rho \\ \gamma^2 = 0 \end{cases} \quad \rho \neq 0$$

da cui $\alpha, \beta, \gamma = 0$, impossibile.

Ma c'è anche un problema più spinoso. Supponiamo di voler considerare le condizioni lineari che provengono semplicemente dal passaggio per un certo numero di punti. Fissiamo pertanto r punti del piano P_1, \dots, P_r . Siccome ad ogni punto corrisponde un certo iperpiano, imponendo il passaggio per r punti nello spazio di partenza stiamo effettivamente intersecando r iperpiani in \mathbf{P}^N . Quando intersechiamo r iperpiani la dimensione dello spazio lineare così ottenuto è $\geq N - r$, e vige l'uguaglianza se gli iperpiani si tagliano trasversalmente. Per calcolare la dimensione consideriamo la matrice dei coefficienti dei vari iperpiani: se questa ha rango massimo allora effettivamente la dimensione è $N - r$. Però la matrice potrebbe avere rango minore. Quindi quando imponiamo r condizioni lineari tutto quello che possiamo dire sulla dimensione del sistema lineare che comunque veniamo a costruire è che deve essere $\geq N - r$. Allora se prendiamo r punti nel piano proiettivo di partenza e le condizioni lineari associate danno luogo ad un sistema lineare di dimensione esattamente $N - r$ diciamo che tali punti sono in *posizione generale*; altrimenti saranno in *posizione particolare*.

Osservazione In generale è ancora un problema aperto stabilire, quando n è abbastanza grande, cosa vuol dire che dei punti sono in posizione generale oppure no.

Esempi

- Per quattro punti allineati ed un punto esterno passano infinite coniche, tutte spezzate in una retta fissa più una retta per il punto esterno. Quindi hanno la stessa dimensione dello spazio lineare delle rette che passano per un punto, i.e. 1 (corrispondono ad una retta nel piano proiettivo duale).
- Per cinque punti allineati passano infinite coniche, spezzate in una retta fissa più una qualsiasi retta del piano. Ma le rette del piano costituiscono un sistema lineare di dimensione 2 (corrispondono al piano proiettivo duale), quindi la dimensione del sistema delle nostre coniche è 2.
- Non è vero che i punti sono sempre in posizione particolare perché un certo loro numero è allineato. Sappiamo che per nove punti in posizione generica passa una e una sola cubica. Consideriamo due cubiche, le quali si tagliano in 9 punti per il teorema di Bézout. Chiaramente per questi nove punti passano tutte le curve del fascio generato dalle due, quindi la dimensione del sistema è 1. Eppure in generale questi punti non sono in posizione particolare rispetto alle curve di ordine più basso di 3: rispetto alle rette e rispetto alle coniche sono in posizione generale!

Un'altra condizione lineare è la richiesta che una curva abbia in un punto prefissato una certa molteplicità minima. La dimensione di questa condizione lineare si può calcolare esattamente.

Supponiamo di prendere un punto P e di considerare le curve che abbiano ivi una certa molteplicità minima. Modulo un cambiamento del sistema di riferimento possiamo supporre che questo punto abbia coordinate $(0 : 0 : 1)$, quindi per considerare la molteplicità della nostra curva possiamo scrivere il polinomio che rappresenta la curva in due sole variabili:

$$f(x, y) = \underbrace{a_0}_{\varphi_0} + \underbrace{a_1x + a_2y}_{\varphi_1} + \underbrace{a_3x^2 + a_4xy + a_5y^2}_{\varphi_2} + \dots$$

Cosa vuol dire che la curva passa per P ? Vuol dire $a_0 = 0$. Cosa vuol dire che la curva passa per quel punto e ha ivi una singolarità di molteplicità almeno 2? Vuol dire $a_1 = 0$ e $a_2 = 0$. E così via.

Osservazione La condizione prevede che la molteplicità sia almeno un certo valore, non esattamente quel valore; se chiediamo che sia esattamente quel valore non scriviamo una condizione lineare.

In generale chiedendo che la molteplicità sia almeno s abbiamo un certo numero di iperpiani da intersecare:

$$1 + 2 + 3 + \dots + s = \frac{s(s+1)}{2}.$$

Inoltre le equazioni degli iperpiani che scriviamo sono tutte l.i., perché date da una singola variabile uguale a zero, quindi la matrice dei coefficienti ha grado massimo. Pertanto la dimensione del sistema lineare è esattamente

$$N - \frac{s(s+1)}{2}.$$

Un'altra condizione lineare è chiedere che una curva passi per un punto e abbia ivi una tangente assegnata. Possiamo sempre scegliere il sistema di riferimento in maniera tale che la tangente voluta sia l'asse delle x . Imporre che la tangente sia l'asse delle x significa in pratica chiedere $\mathbf{a}_1 = 0$. Naturalmente bisogna intendersi, perché il punto potrebbe essere singolare e allora tutte le rette avrebbero molteplicità d'intersezione ≥ 2 . In ogni caso chiedere che la curva passi per il punto e che la molteplicità d'intersezione con la nostra retta sia ≥ 2 dà luogo ad un sistema lineare di dimensione 2.

Cosa succede se invece di un solo punto noi scegliamo un certo numero di punti P_1, \dots, P_h , fissiamo ivi le molteplicità ν_1, \dots, ν_h e chiediamo l'insieme di tutte le curve di ordine n passanti per ciascun punto con una molteplicità non inferiore a quella fissata? Stavolta non siamo più sicuri che queste condizioni siano tutte indipendenti tra di loro. In una situazione di questo tipo tutto quello che possiamo dire è

$$\dim \geq N - \sum_{j=1}^h \frac{\nu_j(\nu_j + 1)}{2}.$$

Arriviamo ora al pretesto con cui abbiamo introdotto la teoria dei sistemi lineari, e cioè la dimostrazione del seguente enunciato.

Proposizione 1.7 Sia $C \subset \mathbf{P}^2(\mathbb{C})$ irriducibile ridotta di ordine²⁶ $n \geq 3$.

$$\sum_{P \in \text{Sing}(C)} \frac{\nu_P(C)(\nu_P(C) - 1)}{2} \leq \frac{(n-1)(n-2)}{2}.$$

Dimostrazione Piano di attacco: costruiremo un sistema lineare di curve opportuno, faremo vedere che contiene almeno una curva, poi intersecheremo questa curva con C_n e utilizzeremo il teorema di Bézout ottenendo la tesi.

Già sappiamo che C ha al più un numero finito di punti singolari P_1, \dots, P_h , ciascuno con una sua molteplicità ν_1, \dots, ν_h (≥ 2).

Andiamo a prendere il sistema lineare

$$\mathcal{D} = \left\{ \begin{array}{l} \text{curve di ordine } n-1, \text{ passanti per } P_1, \dots, P_h \\ \text{con molteplicità almeno } \nu_1 - 1, \dots, \nu_h - 1 \end{array} \right\}.$$

²⁶I casi $n = 1, 2$ sono banali.

Questo è di certo un sistema lineare, perché abbiamo imposto delle condizioni lineari. Dobbiamo verificare che non è vuoto, stimando la sua dimensione con la nostra disuguaglianza:

$$\dim(\mathcal{D}) \geq \frac{(n-1)^2 + 3(n-1)}{2} - \sum_{j=1}^h \frac{(\nu_j - 1)\nu_j}{2} = \eta.$$

Vogliamo ora $\eta > 0$. Già sappiamo che

$$\sum_{j=1}^h \frac{\nu_j(\nu_j - 1)}{2} \leq \frac{n(n-1)}{2}.$$

Ci chiediamo:

$$\eta = \frac{n^2 - 2n + 1 + 3n - 3}{2} - \sum_{j=1}^h \frac{\nu_j(\nu_j - 1)}{2} \stackrel{?}{>} 0$$

ovvero

$$\frac{n^2 + n - 2}{2} \stackrel{?}{>} \sum_{j=1}^h \frac{\nu_j(\nu_j - 1)}{2}.$$

Vogliamo quindi mostrare che

$$\left(\sum_{j=1}^h \frac{\nu_j(\nu_j - 1)}{2} \leq \right) \frac{n(n-1)}{2} < \frac{n^2 + n - 2}{2}.$$

Basta fare i conti.

$$\begin{aligned} n^2 - n &< n^2 + n - 2 \\ 0 &< 2n - 2 \\ n &> 1 \end{aligned}$$

che è vero per ipotesi. Pertanto abbiamo $\eta > 0$. Adesso scelgo η punti $Q_1, \dots, Q_\eta \in C_n$ diversi dai P_j , e vado a considerare il sistema lineare

$$\tilde{\mathcal{D}} = \{\text{curve di } \mathcal{D} \text{ passanti per } Q_1, \dots, Q_\eta\}.$$

Certamente sarà

$$\dim(\tilde{\mathcal{D}}) \geq \dim(\mathcal{D}) - \eta \geq 0,$$

perché abbiamo tagliato \mathcal{D} con η iperpiani. Il fatto che la dimensione sia non-negativa vuol dire che esiste una curva $D_{n-1} \in \tilde{\mathcal{D}}$. Possiamo ora applicare il teorema di Bézout alle curve C_n, D_{n-1} , perché C è irriducibile e, avendo ordine superiore, non può essere una componente di D_{n-1} . Ricaviamo dunque:

$$n(n-1) = \sum_{P \in C \cap D} \nu_P(C, D) \geq \sum_{P \in C \cap D} \nu_P(C) \nu_P(D).$$

Adesso utilizziamo tutto quello che sappiamo.

$$\begin{aligned} \sum_{j=1}^h \nu_{P_j}(C) \nu_{P_j}(D) + \sum_{i=1}^{\eta} \nu_{Q_i}(C) \nu_{Q_i}(D) &\geq \sum_{j=1}^h \nu_j(\nu_j - 1) + \sum_{i=1}^{\eta} 1 \cdot 1 \\ &\geq \sum_{j=1}^h \nu_j(\nu_j - 1) + \eta. \end{aligned}$$

Ora si tratta solo di fare delle manipolazioni algebriche.

$$n(n-1) \geq \sum_{j=1}^h \nu_j(\nu_j-1) + \frac{n^2+n-2}{2} - \sum_{j=1}^h \frac{\nu_j(\nu_j-1)}{2}$$

$$\sum_{j=1}^h \frac{\nu_j(\nu_j-1)}{2} \leq n^2 - n - \frac{n^2+n-2}{2} = \frac{n^2-3n+2}{2} = \frac{(n-1)(n-2)}{2}. \quad \square$$

Digressione Abbiamo considerato le nostre curve algebriche partendo da \mathbf{E}^2 per poi considerare la chiusura proiettiva in \mathbf{P}^2 , e siamo stati interessati principalmente al diagramma reale della curva. Potremmo però considerare la curva in $\mathbf{A}^2(\mathbb{C}) \simeq \mathbb{C}^2$: cosa vuol dire qui considerare il luogo degli zeri del polinomio associato alla curva? Uno è portato a pensare che sia una curva, e in effetti nel nostro caso è sempre stato così. Proviamo però a ragionare in termini diversi. Prendiamo ad esempio la curva $x^2 + y^2 - 1 = 0$ e pensiamola in $\mathbf{A}^2(\mathbb{C})$. Le variabili sono complesse, quindi possiamo sostituire $x = x_1 + ix_2$, $y = y_1 + iy_2$:

$$x_1^2 + 2ix_1x_2 - x_2^2 + y_1^2 + 2iy_1y_2 - y_2^2 - 1 = 0$$

$$\begin{cases} x_1^2 - x_2^2 + y_1^2 - y_2^2 - 1 = 0 \\ x_1x_2 + y_1y_2 = 0 \end{cases}$$

Quindi, usando la biiezione $\mathbb{C}^2 \leftrightarrow \mathbb{R}^4$, la nostra curva è l'insieme di tutti i punti che soddisfano a queste due equazioni in variabili reali. Essa è l'intersezione di due ipersuperfici, che ha in generale dimensione pari alla differenza tra la dimensione dello spazio e il numero di intersezioni ed è dunque un oggetto bidimensionale reale. Morale: le nostre curve algebriche nel piano complesso dal punto di vista reale sono delle superfici.²⁷ Possiamo visualizzare queste curve? Sì, lo possiamo fare in base al genere, che descrive in termini topologici come è fatta una superficie reale proveniente da una curva algebrica dentro \mathbb{R}^4 .

- Se $g = 0$ la superficie è assimilabile ad una sfera (è omeomorfa ad una sfera: a meno di trasformazioni biunivoche e bicontinue è deformabile in una sfera).
- Se $g = 1$ la superficie è torica, una specie di salvagente.²⁸
- Per $g \geq 2$ si procede con una successione infinita di *tori a g buchi*, cioè g ci dà il numero di buchi del nostro toro.

²⁷Infatti vengono chiamate *superfici di Riemann*, cf. Geometria Complessa.

²⁸Ma salvagente quello dei bambini, che dentro è vuoto, si gonfia.