Note del Corso di Istituzioni di Algebra e Geometria A.A. 2026/2027

17 dicembre 2025

Indice

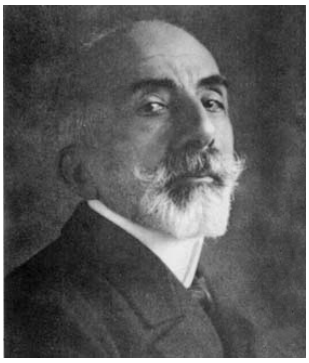
1 Introduzione

Luigi Cremona (Pavia, 1830 – Roma, 1903). Noto per la geometria algebrica birazionale. Oltre alla sua carriera di professore universitario a Bologna e Roma, su senatore attivo nella riforma dell'istruzione pubblica e nell'Accademia dei Lincei.

Questo corso è dedicato allo studio delle curve algebriche piane, ossia degli insiemi di punti che si presentano come luoghi di zeri di un polinomio non nullo in due indeterminate nel caso affine, oppure come luoghi di zeri di un polinomio omogeneo non nullo in tre indeterminate nel caso proiettivo. L'analoga nozione in dimensione superiore conduce al concetto di ipersuperficie algebrica, che rappresenta una naturale generalizzazione delle curve nel contesto della geometria algebrica.

Attraverso l'uso di tecniche algebriche — in particolare strumenti di algebra commutativa e di geometria locale — svilupperemo metodi efficaci per analizzare in modo rigoroso le singolarità delle curve e le loro intersezioni. Ciò consentirà di introdurre e studiare la nozione di molteplicità di intersezione, fondamentale per distinguere, a partire dalle equazioni algebriche, tra intersezioni trasversali e intersezioni tangenziali, e più in generale per comprendere il comportamento locale delle curve.

La teoria delle curve algebriche piane si inserisce in un quadro molto più ampio, quello della Geometria Algebrica, una disciplina dalla storia lunga e stratificata, che affonda le sue radici nell'introduzione delle coordinate cartesiane nel XVII secolo. Un momento cruciale del suo sviluppo si colloca nel XIX secolo, con i lavori di Bernhard Riemann, il quale mostrò che ogni superficie di Riemann compatta — ossia ogni varietà complessa liscia di dimensione uno — può essere realizzata come insieme delle soluzioni di un'equazione polinomiale.



Corrado Segre (Saluzzo 1863 – Torino 1924). Professore di Severi e di Beniamino Segre. Lavorò a Torino, negli stessi anni di Peano.

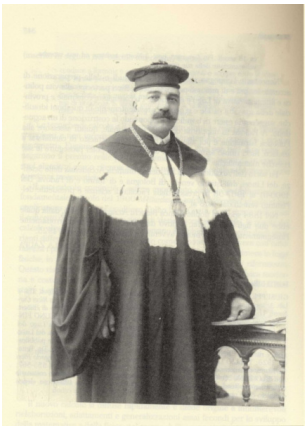
Un contributo particolarmente rilevante allo sviluppo della geometria delle curve e delle ipersuperfici proiettive fu fornito dalla scuola italiana di geometria algebrica, attiva tra la fine dell'Ottocento e l'inizio del Novecento. In questo periodo, geometri come Giacomo Albenese, Eugenio Bertini, Guido Castelnuovo, Luigi Cremona, Federigo Enriques, Corrado Segre, Francesco Severi e Giuseppe Veronese svilupparono un approccio fortemente geometrico allo studio delle varietà algebriche, fondato sull'uso sistematico della geometria proiettiva, dei sistemi lineari di divisori e delle trasformazioni birazionali.

Eugenio Bertini (Forlì, 1846 – Pisa, 1933). Studente di Cremona a Bologna poi assistente di Cremona a Milano, professore alla Sapienza, socio dell'Accademia dei Lincei. Ebbe come studenti Albanese e Fubini.

Nello studio delle curve algebriche, la scuola italiana contribuì in modo decisivo alla comprensione delle nozioni di genere, linearità e birazionalità. In particolare, furono chiarite le relazioni tra il genere di una curva piana proiettiva e le sue singolarità, attraverso formule che collegano il grado della curva, la natura dei punti singolari e gli invarianti topologici della curva liscia normalizzata. Questi risultati portarono allo sviluppo sistematico della teoria dei sistemi lineari di divisori, che costituisce tuttora uno strumento fondamentale per lo studio delle mappe tra curve e delle loro immersioni nello spazio proiettivo.

Un ruolo centrale fu giocato dallo studio delle intersezioni tra curve piane, affrontato mediante metodi geometrici che anticipavano, in forma intuitiva, la moderna teoria dell'intersezione. I geometri italiani introdussero e utilizzarono in modo efficace concetti come la molteplicità di intersezione e il principio di conservazione del numero, che permetteva di contare le intersezioni anche in presenza di degenerazioni e sin-

golarità. Tali idee, sebbene formulate in modo non rigoroso secondo i criteri odierni, furono essenziali per lo sviluppo successivo di una teoria algebrica coerente dell'intersezione.



Veronese (Chioggia, 1854 – Padova, 1917). Lavora a Vienna e Zurigo, scrive a proposito dell'Hexagrammum mysticum di Blaise Pascal, apprezzato da Luigi Cremona. Fu senatore, professore di Castelnuovo e Levi-Civita.

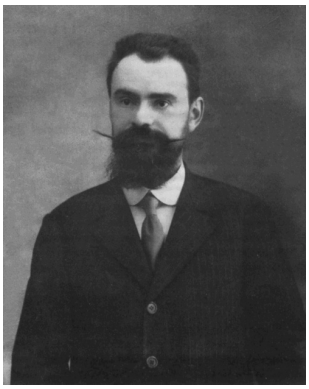
Per quanto riguarda le superfici e le ipersuperfici proiettive, la scuola italiana svolse un ruolo di primo piano nello studio delle superfici razionali e nella loro classificazione. I lavori di Castelnuovo ed Enriques portarono a criteri geometrici per riconoscere la razionalità di una superficie algebrica, e allo sviluppo della teoria delle trasformazioni birazionali, come le trasformazioni di Cremona, che permettono di confrontare modelli proiettivi diversi di una stessa varietà. In questo contesto furono studiate in modo approfondito le singolarità delle ipersuperfici, analizzandone la risoluzione tramite successioni di trasformazioni birazionali, un'idea che anticipa concettualmente la moderna teoria della risoluzione delle singolarità.

Un altro contributo fondamentale riguarda la nascita della teoria della classificazione delle superfici algebriche, culminata nel cosiddetto programma di Enriques–Kodaira, che ha origine proprio nei lavori della scuola italiana. In questo contesto furono introdotti invarianti geometrici come il genere geometrico e il genere aritmetico, e furono studiate in modo sistematico le famiglie di curve contenute in una superficie proiettiva, mettendo in luce il ruolo dei sistemi lineari e delle mappe pluricanoniche.

Vediamo ora nello specifico alcune dei contributi della scuola di geometria algebrica italiana dello scorso secolo.

Un ruolo fondativo fu svolto da **Luigi Cremona** (1830–1903), la cui opera segnò il passaggio dalla geometria proiettiva classica a una visione più moderna delle varietà algebriche. Le **trasformazioni di Cremona**, ossia trasformazioni birazionali dello spazio proiettivo, divennero uno strumento fondamentale per lo studio delle superfici algebriche e delle loro singolarità, permettendo di confrontare modelli proiettivi diversi di una stessa superficie. L'idea che proprietà geometriche profonde potessero essere invarianti per trasformazioni birazionali influenzò profondamente tutta la scuola successiva.

Allievo ideale di Cremona fu **Corrado Segre** (1863–1924), che contribuì in modo decisivo allo studio delle **varietà proiettive di dimensione superiore** e delle loro famiglie di rette e curve. Segre introdusse e sviluppò lo studio sistematico delle **varietà rigate**, delle varietà di Grassmann e delle immersioni proiettive, anticipando concetti che sarebbero stati formalizzati solo più tardi nel linguaggio moderno della geometria algebrica. Il suo lavoro ebbe un'influenza diretta su molti giovani geometri, tra cui Castelnuovo ed Enriques.



Federigo Enriques (Livorno 1871 – Roma 1946). Studente di Castelnuovo, ne sposò la sorella Elbina. Lavorò a Bologna e alla Sapienza.

Accanto a Segre si colloca **Giuseppe Veronese** (1854–1917), noto in particolare per l'introduzione delle **varietà di Veronese**, che forniscono immersioni dello spazio proiettivo in dimensione superiore tramite sistemi lineari completi di forme omogenee. Queste costruzioni, oggi centrali nello studio delle curve e delle ipersuperfici proiettive, permisero di comprendere come equazioni di grado elevato possano essere trattate geometricamente come oggetti lineari in spazi più grandi, un'idea di enorme portata concettuale.

Guido Castelnuovo (1865–1952) occupa una posizione chiave nello sviluppo della teoria delle **curve algebriche** e delle **superfici razionali**. I suoi risultati sulla classificazione delle curve proiettive, sulle relazioni tra grado, genere e immersioni proiettive, e i criteri di razionalità per le superfici algebriche rappresentano tuttora pietre miliari della disciplina. In particolare, il cosiddetto **criterio di Castelnuovo** per la razionalità di una superficie fu uno dei primi tentativi sistematici di classificazione birazionale.

Il sodalizio scientifico tra Castelnuovo e **Federigo Enriques** (1871–1946) fu straordinariamente produttivo. Enriques contribuì in modo decisivo allo sviluppo della **teoria della classificazione delle superfici algebriche**, introducendo invarianti come il genere geometrico e aritmetico e studiando il ruolo dei sistemi lineari canonici e pluricanonici. Insieme, Castelnuovo ed Enriques posero le basi di quello che sarebbe poi diventato il **programma di classificazione delle superfici**, successivamente completato in chiave moderna da Kodaira.

Guido Castelnuovo (Venezia, 1865 – Roma, 1952). Studente prima di Veronese, poi di Segre, infine di Cremona, di cui assume la cattedra alla Sapienza. Fu eletto senatore a vita.

Un'altra figura centrale fu **Francesco Severi** (1879–1961), allievo di Segre e protagonista indiscusso della fase più matura della scuola italiana. Severi diede contributi fondamentali allo studio delle **famiglie di curve su superfici**, alla teoria delle **varietà di Picard** e alla nozione di equivalenza algebrica dei cicli. Il suo lavoro sul **teorema di completezza del sistema canonico** e sul comportamento delle curve in famiglie anticipa molti temi della moderna geometria dei moduli, sebbene alcune sue affermazioni richiedessero successivamente chiarimenti e correzioni formali.

In questo contesto si inserisce anche l'opera di **Eugenio Bertini** (1846–1933), noto soprattutto per il **teorema di Bertini**, che afferma, in forme diverse, la genericità della liscezza delle sezioni iperpiane di una varietà algebrica. Questo risultato, nato da considerazioni geometriche intuitive, è oggi uno strumento fondamentale nello studio delle **ipersuperfici proiettive** e delle loro singolarità, e trova applicazioni pervasive in tutta la geometria algebrica moderna.

Francesco Severi (Arezzo, 1879 – Roma, 1961). Studente di Segre. Assistente di Enriques a Bologna e di Bertini a Pisa. Lavora a Padova e a Roma, vince premi, è membro di accademie nazionali e internazionali.

Infine, **Giacomo Albanese** (1890–1947) rappresenta un ponte naturale verso sviluppi più moderni. A lui si deve l'introduzione della **varietà di Albanese** associata a una varietà algebrica, che generalizza la nozione di Jacobiana di una curva. Questa costruzione, nata nello studio delle superfici e delle loro famiglie di curve, si rivelò fondamentale per collegare la geometria algebrica con l'analisi complessa e la teoria delle varietà abeliane.

Nel loro insieme, questi matematici condivisero una visione profondamente geometrica delle curve e delle **ipersuperfici proiettive**: oggetti da studiare non solo attraverso equazioni, ma tramite le loro mappe, le loro famiglie, le loro degenerazioni e le trasformazioni birazionali che le collegano. Questa impostazione, pur priva del rigore formale moderno, ha lasciato un'impronta duratura e continua a influenzare in modo sostanziale il linguaggio e le intuizioni della geometria algebrica contemporanea.

Inoltre, lo studio delle famiglie di curve e di ipersuperfici e delle loro degenerazioni portò a una prima comprensione di concetti oggi centrali, quali lo spazio dei moduli e la variazione degli invarianti in famiglie algebriche. Sebbene questi risultati fossero spesso espressi in termini geometrici e intuitivi, essi anticipavano idee che sarebbero state formalizzate solo molti decenni più tardi con l'introduzione degli schemi e delle tecniche coomologiche.

Nel complesso, l'eredità della scuola italiana risiede non solo nei singoli risultati, ma anche nell'impostazione concettuale: lo studio delle curve e delle ipersuperfici proiettive come oggetti globali, da analizzare attraverso le loro mappe, le loro famiglie e le loro degenerazioni. Questa visione ha profondamente influenzato lo sviluppo della geometria algebrica moderna e rimane alla base di molti degli strumenti utilizzati ancora oggi.

Giacomo Albanese (Geraci Siculo, 1890 – São Paulo, 1948). Studente del Dini e di Bertini. Lavorò in Sicilia, a Pisa, e in Brasile.

La successiva evoluzione dell'algebra commutativa, con i contributi fondamentali di David Hilbert ed Emmy Noether, rese possibile una formalizzazione sistematica e generale della teoria. Le basi rigorose della geometria algebrica moderna furono poi consolidate

nella prima metà del XX secolo grazie ai lavori di Oscar Zariski e André Weil, che riorganizzarono la disciplina su solide fondamenta algebriche.

A partire dagli anni Cinquanta, la teoria conobbe un'ulteriore e profonda trasformazione grazie all'introduzione del linguaggio degli schemi e delle tecniche coomologiche da parte di Alexander Grothendieck, che ampliarono enormemente l'ambito e la potenza della geometria algebrica, permettendo di trattare in modo uniforme problemi di natura aritmetica, geometrica e topologica.

Oggi la geometria algebrica è al centro di numerose interazioni con altri settori della matematica. In particolare, una parte rilevante della teoria dei numeri può essere interpretata come geometria algebrica su campi finiti o anelli aritmetici; un esempio emblematico è la dimostrazione dell'Ultimo Teorema di Fermat. Esistono inoltre connessioni profonde con l'algebra, l'analisi complessa, la topologia, la geometria differenziale, le equazioni alle derivate parziali e la fisica matematica, nonché applicazioni in ambiti più applicativi come la teoria dei codici e la crittografia.

2 Preliminari di algebra e di geometria

2.1 Spazi affini

Sia $\mathbb{K}$ un campo e sia V un $\mathbb{K}$-spazio vettoriale di dimensione finita n.

Definizione 2.1. Uno *spazio affine* $\mathbb{A}$ su V è un insieme non vuoto $\mathbb{A} \neq \emptyset$ su cui è definita un'applicazione $\tau\colon \mathbb{A} \times \mathbb{A} \to V$ tale che:

1. $\forall P, Q, R \in \mathbb{A}$ si ha $\tau(P,Q) + \tau(Q,R) = \tau(P,R)$;
2. $\forall P \in \mathbb{A}$ si ha che $\tau(P, \cdot)\colon \mathbb{A} \to V$ è una biiezione.

Gli elementi di $\mathbb{A}$ sono chiamati *punti*.

Osservazione 2.2. In queste note considereremo principalmente lo *spazio affine standard* $\mathbb{A}^n_{\mathbb{K}} := \mathbb{K}^n$ sullo spazio vettoriale $\mathbb{K}^n$, con l'applicazione

$$\tau\big((a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, b_n)\big) = \begin{pmatrix} b_1 - a_1 \\ b_2 - a_2 \\ \vdots \\ b_n - a_n \end{pmatrix}.$$

In questo caso, quindi, lo spazio affine e lo spazio vettoriale coincidono insiemisticamente, e i loro elementi sono n-uple di scalari.

Per motivi di chiarezza, denotiamo tali n-uple in orizzontale $(a_1, a_2, \ldots, a_n)$ per indicare gli elementi dello spazio affine, mentre la notazione verticale indicherà un vettore $\begin{pmatrix} c_1 \\ c_2 \\ \vdots \\ c_n \end{pmatrix}$.

Definizione 2.3. Un *riferimento affine* in $\mathbb{A}$ è il dato di un punto fissato $O \in \mathbb{A}$, che è chiamato *origine*, e di una base $\mathcal{B} = \{v_1, \ldots, v_n\}$ dello spazio vettoriale V.

Dato un riferimento affine, a ogni punto $P \in \mathbb{A}$ possono essere associate biunivocamente le sue *coordinate affini*, che sono per definizione le coordinate del vettore $\tau(O,P)$ nella base $\mathcal{B}$.

Osservazione 2.4. Nello spazio affine standard considereremo il sistema di riferimento affine standard, e cioè

$$O = (0, 0, \dots, 0), \quad \mathcal{B} = \left\{ \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \right\}.$$

In questo riferimento, ogni n-upla coincide con la propria n-upla di coordinate affini.

2.2 Spazi proiettivi

Definizione 2.5. Sia V un $\mathbb{K}$-spazio vettoriale di dimensione finita $n+1$. Lo *spazio proiettivo* $\mathbb{P}(V)$ su V è l'insieme quoziente

$$\mathbb{P}(V) = \frac{V \setminus \{0\}}{\sim},$$

dove $\sim$ è la relazione di proporzionalità: $v \sim w \iff \exists \lambda \in \mathbb{K}^*$ tale che $w = \lambda v$.

Definizione 2.6. Un *sistema di riferimento proiettivo* in $\mathbb{P}(V)$ è il dato di $n+2$ punti

$$P_0, P_1, \dots, P_n, P_{n+1} \in \mathbb{P}(V),$$

quindi $n+2$ classi di vettori di V, tali che ogni scelta di $n+1$ vettori tra di essi risulti linearmente indipendente.
Se $p\colon V \setminus \{0\} \to \mathbb{P}(V)$ indica la proiezione, si può dimostrare facilmente che esiste una base $\{v_0, \dots, v_n\}$ di V tale che

$$p(v_0) = P_0,\ \dots,\ p(v_n) = P_n,\ p(v_0 + v_1 + \cdots + v_n) = P_{n+1}\,.$$

Dato un vettore non nullo $v \in V$, sia $v = a_0 v_0 + a_1 v_1 + \cdots + a_n v_n$ definiamo le *coordinate omogenee* di $P = [v]$ come l'$(n+1)$-upla $(a_0 : a_1 : \cdots : a_n)$. Si osservi che le coordinate omogenee non sono univocamente determinate, bensì sono determinate a meno di un fattore di proporzionalità non nullo.

Osservazione 2.7. Indicheremo con $\mathbb{P}^n_{\mathbb{K}} = \mathbb{P}(\mathbb{K}^{n+1})$ lo spazio proiettivo standard. A meno di specifica indicazione, in esso fisseremo il riferimento proiettivo standard

$$P_0 = [e_0],\ P_1 = [e_1],\ \dots,\ P_n = [e_n],\ P_{n+1} = [e_0 + e_1 + \cdots + e_n]\,,$$

dove i vettori e_i formano la base canonica di $\mathbb{K}^{n+1}$.

2.3 Anelli di polinomi

Denoteremo con

$$\mathbb{K}[x_1, \ldots, x_n]$$

l'anello dei polinomi nelle indeterminate $x_1, \ldots, x_n$ a coefficienti in un campo $\mathbb{K}$.

Definizione 2.8. Sia $f \in \mathbb{K}[x_1, \ldots, x_n]$ un polinomio non nullo. Allora f è *irriducibile* se e soltanto se non è invertibile e non può essere scritto come prodotto di due elementi non invertibili, i.e. $f = g \cdot h$ implica che g oppure h sia invertibile.

Definizione 2.9. Sia R un anello algebrico. L'anello dei polinomi $R[x_1, \ldots, x_n]$ è un *dominio a fattorizzazione unica* (UFD) se ogni polinomio $f \in R[x_1, \ldots, x_n]$ si può fattorizzare in modo unico, a meno di elementi invertibili e a meno di una permutazione dei fattori, nel prodotto di polinomi irriducibili:

$$f(x_1, \ldots, x_n) = f_1(x_1, \ldots, x_n)^{\mu_1} \cdots f_r(x_1, \ldots, x_n)^{\mu_r},$$

con $f_i(x_1, \ldots, x_n)$ irriducibili e a due a due coprimi. L' esponente μ_i è detto *molteplicità algebrica* del fattore irriducibile f_i.

- Il polinomio f si dice *ridotto* se e soltanto se $\mu_1 = \cdots = \mu_r = 1$.
- Il polinomio f si dice *avere un'unica componente irriducibile* se e soltanto se $r = 1$.
- Il polinomio f si dice *irriducibile* se e soltanto se $r = 1$ e $\mu_1 = 1$.

Lemma 2.10 (Lemma di Gauss)**.** *Se R è UFD allora $R[x]$ è UFD.*

Una conseguenza piuttosto utile è la seguente.

Corollario 2.11. *Se $\mathbb{K}$ è un campo allora $\mathbb{K}[x_1, \ldots, x_n]$ è un UFD per ogni n naturale.*

Dimostrazione. La dimostrazione è per induzione su n. Ogni campo è in particolare un UFD, quindi per il lemma di Gauss $\mathbb{K}[x_1]$ è UFD, dimostrando il caso per $n = 1$. Se $\mathbb{K}[x_1, \ldots, x_{n-1}]$ è un UFD, applicando di nuovo il lemma di Gauss si trova che $\mathbb{K}[x_1, \ldots, x_n]$ è un UFD. □

La proposizione seguente sottolinea come la nozione di irriducibilità dipenda intrinsecamente dal campo scelto.

Proposizione 2.12. *Dato*

$$f(x) := x^4 + 1 \in \mathbb{K}[x],$$

si ha che:

- *Se* $\mathbb{K} = \mathbb{Q}$ *allora* f *è irriducibile.*
- *Se* $\mathbb{K} = \mathbb{R}, \mathbb{K} = \mathbb{C}$ *oppure se* $\mathbb{K}$ *è un campo finito — i.e.* $\mathbb{K} \cong \mathbb{F}_{p^n}$ *per qualche primo* p *e intero non negativo* n *— allora* f *è riducibile.*

Dimostrazione. E' chiaro che $f(x)$ è riducibile sul campo dei numeri complessi perchè, per il teorema fondamentale dell'algebra, il campo dei numeri complessi è algebricamente chiuso. In particolare la sua fattorizzazione legge

$$f(x) = \prod_{k=1}^{4} (x - e^{i(2k-1)\frac{\pi}{4}}) \in \mathbb{C}[x]$$

sul campo dei numeri complessi mentre

$$f(x) = \left(x^2 + \sqrt{2}\,x + 1\right)\left(x^2 - \sqrt{2}\,x + 1\right) \in \mathbb{R}[x]$$

dimostra la riducibilità sul campo dei numeri reali. In generale ogni polinomio di grado tre o superiore è riducibile sul campo dei numeri reali.

Dimostriamo che è irriducibile sul campo dei numeri razionali. Sia per assurdo $f = g_1 \cdot g_2$ una fattorizzazione in $\mathbb{Q}[x]$, ove quindi sia g_1 che g_2 sono irriducibili. I polinomi g_i non possono avere grado zero altrimenti sarebbero invertibili perché $\mathbb{Q}$ é un campo e non possono avere grado uno perché le radici di f come abbiamo visto sopra sono tutte complesse non reali, e quindi non razionali. Quindi entrambi i polinomi g_i devono avere grado due. Allora per il lemma di Gauss, dato che $\mathbb{R}[x]$ è un UFD, i polinomi g_i devono essere i due fattori che appaiono nella fattorizzazione reale sopra, che però non appartengono a $\mathbb{Q}[x]$.

Dimostriamo ora che f è riducibile su ogni campo finito. Se $char(\mathbb{K}) = 2$ allora

$$(x^4 + 1) = (x^2 + 1)^2 = (x + 1)^4 \in \mathbb{K}[x].$$

Per la dimostrazione nel caso in cui la caratteristica del campo sia diversa da due ci avvarremo del seguente lemma.

Lemma 2.13. *Siano* $a, b \in \mathbb{K}$ *due elementi di un campo finito, e sia* $char(\mathbb{K}) \neq 2$*. Se nè* a *nè* b *è il quadrato di un qualche elemento di* $\mathbb{K}$ *allora* $ab = k^2$ *per un qualche* $k \in \mathbb{K}$*.*

Dimostrazione. Si consideri l'omomorfismo dei gruppi moltiplicativi

$$\begin{aligned} \delta : \ \mathbb{K}^\times &\to \mathbb{K}^\times \\ a &\mapsto a^2. \end{aligned}$$

Chiaramente $ker(\delta) = \{1, -1\}$ e

$$|\delta(\mathbb{K}^\times)| = |\mathbb{K}^\times / ker(\delta)| = \frac{|\mathbb{K}^\times|}{|\{-1, 1\}|} = \frac{|\mathbb{K}^\times|}{2}$$

Perciò l'immagine $\delta(\mathbb{K}^\times) \subset \mathbb{K}^\times$ è di indice due e in quanto tale è normale in $\mathbb{K}^\times$. Quindi abbiamo che

$$\mathbb{K}^\times / \delta(\mathbb{K}^\times) = \{e, x\} \cong \mathbb{Z}/2\mathbb{Z}$$

dove e è l'elemento neutro e $x^2 = e$. Basta osservare che e rappresenta gli elementi nell'immagine del morphismo δ, ovvero i quadrati di $\mathbb{K}^\times$. Se a e b non sono quadrati, allora $[a]_{\delta(\mathbb{K}^\times)} = [b]_{\delta(\mathbb{K}^\times)} = x$, perciò

$$[a \cdot b]_{\delta(\mathbb{K}^\times)} = [a]_{\delta(\mathbb{K}^\times)} \cdot [b]_{\delta(\mathbb{K}^\times)} = x \cdot x = e,$$

quindi ab è un quadrato. Questo conclude la dimostrazione del lemma. □

Si consideri ora l'insieme

$$S := \{-2, -1, 2\}$$

Se S non contenesse nessun quadrato, allora -2 e -1 non sarebbero quadrati, quindi per il lemma precendente $(-2) \cdot (-1) = 2$ sarebbe un quadrato, ma $2 \in S$, contraddicendo l'ipotesi. Quindi esiste almeno un quadrato in S. Dimostriamo ora che qualunque elemento in S sia quadrato dà una fattorizzazione di f in $\mathbb{K}[x]$.

- Se $-2 = a^2$ per $a \in \mathbb{K}$ allora $f(x) = (x^2 - ax - 1)(x^2 + ax - 1)$,
- Se $-1 = a^2$ per $a \in \mathbb{K}$ allora $f(x) = (x^2 - a)(x^2 + a)$,
- Se $2 = a^2$ per $a \in \mathbb{K}$ allora $f(x) = (x^2 - ax + 1)(x^2 + ax + 1)$.

Questo conclude la dimostrazione della proposizione. □

Osservazione 2.14. Se $\mathbb{K} = \overline{\mathbb{K}}$ è un campo algebricamente chiuso, allora $\mathbb{K}$ è infinito. Infatti, se per assurdo $\mathbb{K}$ fosse finito, avremmo $\mathbb{K} = \{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ per qualche $m \in \mathbb{N}_{>0}$. Si consideri

$$f(x) := (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_m) + 1 \in \mathbb{K}[x].$$

Allora $f(a) = 1 \neq 0$ per ogni elemento a del campo. Si ottine un polinomio di grado positivo senza radici in $\mathbb{K}$, il che è assurdo.

2.3.1 Polinomi omogenei

Definizione 2.15. Dato $F \in \mathbb{K}[x_0, \ldots, x_n]$ di grado $d \geq 1$, esso si può decomporre nella forma

$$F = F_d + F_{d-1} + F_{d-2} + \cdots + F_1 + F_0,$$

dove F_i è la somma di tutti i monomi di grado i, con $0 \leq i \leq d$, che compaiono in F con un coefficiente non nullo. I termini F_i si dicono *termini omogenei* di F.
Un polinomio F di grado d si dice *omogeneo* se

$$F = F_d,$$

cioè F non contiene monomi di grado strettamente minore di del suo grado. Ogni F_i è quindi un polinomio omogeneo di grado i.

Esempio 2.16. La decomposizione in termini omogenei di

$$F = x_0^4 - 2x_0x_1x_2 + x_1^2x_2 - x_2^3 + x_0x_1 + 8x_2^2 - 3x_0 + 5x_1 + 7x_2 - 1$$

è data da

$$F = F_4 + F_3 + F_2 + F_1 + F_0\,,$$

dove

$$\begin{aligned} F_4 &= x_0^4, \\ F_3 &= -2x_0x_1x_2 + x_1^2x_2 - x_2^3, \\ F_2 &= x_0x_1 + 8x_2^2, \\ F_1 &= -3x_0 + 5x_1 + 7x_2, \\ F_0 &= -1. \end{aligned}$$

Esempio 2.17. I seguenti sono polinomi omogenei:

$$x_0 + x_1 + 2x_2, \quad x_0^2 - 8x_0x_1 + 25x_0x_2 - 13x_1^2 + 11x_2^2,$$
$$x_0^3x_1x_2 - 2x_0x_1^2x_2^2 - 7x_1^5 + 3x_1x_2^4\,.$$

Definizione 2.18. Indicheremo con

$$\mathbb{K}[x_0, \ldots, x_n]_d$$

l'insieme dei polinomi omogenei di grado $d \geq 0$, unito il polinomio nullo. Si ha, in particolare

$$\mathbb{K}[x_0, \ldots, x_n]_0 = \mathbb{K}, \quad \mathbb{K}[x_0, \ldots, x_n]_1 = \{a_0 x_0 + \cdots + a_n x_n \mid a_i \in \mathbb{K}\}.$$

L'insieme $\mathbb{K}[x_0, \ldots, x_n]_d$ risulta un $\mathbb{K}$-spazio vettoriale di dimensione finita

$$\dim \mathbb{K}[x_0, \ldots, x_n]_d = \binom{n+d}{d},$$

e una sua base è data da tutti i monomi monici di grado d:

$$x_0^{i_0} x_1^{i_1} \cdots x_n^{i_n}, \quad i_j \in \{0, \ldots, d\}, \quad \sum_{j=0}^{n} i_j = d.$$

Osservazione 2.19. Il fatto che i monomi monici di grado d in $n+1$ variabili siano esattamente in numero $\binom{n+d}{d}$ si può dimostrare con l'argomento combinatorico detto *stars and bars*: ogni monomio si ottiene distribuendo i_0 simboli 'stelle' consecutivi (*star*) all'esponente della prima variabile, poi passando all'esponente della seconda variabile, etc. Il passaggio da un esponente al successivo viene indicato con il simbolo di una barra (*bar*). Ora diventa chiaro che su una stringa di $n+d$ simboli, l'operazione di scegliere d stelle (forzando quindi i rimanenti n simboli ad essere barre) definisce univocamente un monomio e questo processo è biiettivo. Per concludere basta osservare che ci sono $\binom{n+d}{d}$ scelte di d simboli in una stringa di $n+d$ simboli.

Lemma 2.20. *Un polinomio $F \in \mathbb{K}[x_0, \ldots, x_n]$ di grado $d \geq 1$ è omogeneo se e solo se vale l'identità di polinomi*

$$F(tx_0, \ldots, tx_n) = t^d \, F(x_0, \ldots, x_n) \quad \text{in } \mathbb{K}[x_0, \ldots, x_n, t]. \tag{2.1}$$

Dimostrazione. Per semplicità consideriamo il caso $n = 2$. Se F è omogeneo si scrive nella forma

$$F = \sum_{i_0+i_1+i_2=d} a_{i_0 i_1 i_2} x_0^{i_0} x_1^{i_1} x_2^{i_2},$$

con $0 \leq i_j \leq d$ per ogni $j = 0, 1, 2$. Se valutiamo F in (tx_0, tx_1, tx_2) otteniamo

$$\begin{aligned} F(tx_0, tx_1, tx_2) &= \sum_{i_0+i_1+i_2=d} a_{i_0 i_1 i_2} t^{i_0} x_0^{i_0} t^{i_1} x_1^{i_1} t^{i_2} x_2^{i_2} = \\ &= \sum_{i_0+i_1+i_2=d} a_{i_0 i_1 i_2} t^{i_0+i_1+i_2} x_0^{i_0} x_1^{i_1} x_2^{i_2} = t^d \left(\sum_{i_0+i_1+i_2=d} a_{i_0 i_1 i_2} x_0^{i_0} x_1^{i_1} x_2^{i_2} \right). \end{aligned}$$

Viceversa, sia $F \in \mathbb{K}[x_0, x_1, x_2]$ un polinomio arbitrario e supponiamo che valga l'identità (2.1). Scriviamo la decomposizione in termini omogenei:

$$F = F_d + F_{d-1} + \cdots + F_1 + F_0 \,.$$

Si ha

$$F(tx_0, tx_1, tx_2) = F_d(tx_0, tx_1, tx_2) + F_{d-1}(tx_0, tx_1, tx_2) + \cdots \\ \cdots + F_1(tx_0, tx_1, tx_2) + F_0(tx_0, tx_1, tx_2) \,.$$

Essendo ogni F_i omogeneo di grado i, per l'implicazione appena dimostrata, abbiamo

$$F(tx_0, tx_1, tx_2) = t^d F_d(x_0, x_1, x_2) + \cdots + tF_1(x_0, x_1, x_2) + F_0(x_0, x_1, x_2) \,. \tag{2.2}$$

D'altra parte, per la (2.1) possiamo anche scrivere

$$F(tx_0, tx_1, tx_2) = t^d \big(F_d(x_0, x_1, x_2) + F_{d-1}(x_0, x_1, x_2) + \cdots + F_1(x_0, x_1, x_2) + F_0(x_0, x_1, x_2)\big) =$$

$$= t^d F_d(x_0, x_1, x_2) + t^d F_{d-1}(x_0, x_1, x_2) + \cdots + t^d F_1(x_0, x_1, x_2) + t^d F_0(x_0, x_1, x_2). \tag{2.3}$$

I membri destri delle (2.2) e (2.3) devono coincidere come polinomi in x_0, x_1, x_2, t, quindi necessariamente $F_i = 0$ per ogni $0 \leq i \leq d-1$. □

2.3.2 Radici di polinomi omogenei e loro molteplicità

Definizione 2.21. Sia $G \in \mathbb{K}[\lambda, \mu]$ un polinomio omogeneo. Una *radice* di G è una coppia omogenea $(a : b) \in \mathbb{P}^1_{\mathbb{K}}$ tale che

$$G(a, b) = 0 \,.$$

Lemma 2.22 (Teorema di Ruffini omogeneo)**.** *Un punto $(b : c) \in \mathbb{P}^1_{\mathbb{K}}$ è una radice omogenea di un polinomio omogeneo $G \in \mathbb{K}[\lambda, \mu]_d$ per $d \geq 1$, se e solo se $c\lambda - b\mu$ divide G, ovvero*

$$G = (c\lambda - b\mu) \cdot G_1 \,,$$

con $G_1 \in \mathbb{K}[\lambda, \mu]_{d-1}$.

Dimostrazione. Supponiamo che $(b : c) \in \mathbb{P}^1_{\mathbb{K}}$ sia una radice di G; senza perdita di generalità possiamo supporre $b \neq 0$ (altrimenti si ripete il ragionamento che segue per c). Si ha $(b : c) = (1 : c/b)$ e

$$0 = G(1, c/b) = aG(c/b),$$

cioè c/b è una radice del polinomio deomogeneizzato $aG(t) = G(1,t)$. Per il Teorema di Ruffini, il polinomio $aG(t)$ è divisibile per $t - c/b$:

$$aG(t) = (t - c/b)g_1(t)\,.$$

Si ha quindi, per un opportuno esponente $r \geq 0$,

$$\begin{aligned} G(\lambda,\mu) &= \lambda^r h(aG) = \lambda^r h((t-c/b)g_1(t)) \\ &= \lambda^r(\mu - c/b\lambda)h(g_1(t))) \\ &= \lambda^r(c\lambda - b\mu)h(-b\cdot g_1(t))\,, \end{aligned}$$

che dimostra la tesi.

Viceversa, se $G = (c\lambda - b\mu)\cdot G_1$, la coppia omogenea $(b:c)$ annulla G. □

Definizione 2.23. Sia $(b:c) \in \mathbb{P}^1_{\mathbb{K}}$ una radice omogenea di un polinomio omogeneo $G \in \mathbb{K}[\lambda,\mu]_d$. La *molteplicità* (algebrica) m di $(b:c)$ è la molteplicità del fattore $(c\lambda - b\mu)$ come divisore di $G(\lambda,\mu)$; si ha, quindi:

$$G(\lambda,\mu) = (c\lambda - b\mu)^m \cdot G_1(\lambda,\mu)\,, \qquad G_1(b,c) \neq 0\,.$$

Lemma 2.24. *Sia $\mathbb{K} = \overline{\mathbb{K}}$ un campo algebricamente chiuso. Allora ogni polinomio omogeneo $G \in \mathbb{K}[\lambda,\mu]$ di grado $d \geq 1$ ammette esattamente d radici contate con le rispettive molteplicità:*

$$G(\lambda,\mu) = (c_1\lambda - b_1\mu)^{m_1}\cdots(c_r\lambda - b_r\mu)^{m_r}\,, \qquad \sum_{i=1}^{r} m_i = d\,. \tag{2.4}$$

Dimostrazione. Il risultato è una conseguenza diretta del Teorema Fondamentale dell'Algebra. Infatti, sia $G \in \mathbb{K}[\lambda,\mu]_d$, supponiamo che non sia costante nell'indeterminata μ (per ipotesi non può essere costante in entrambe le variabili) e consideriamo il deomogeneizzato rispetto a λ:

$$g(t) := aG(t) = G(1,t) = a_\delta t^\delta + a_{\delta-1}t^{\delta-1} + \cdots + a_1 t + a_0\,,$$

dove $\delta \leq d$. Siccome μ è presente in G, abbiamo che $\deg(g) \geq 1$, e per il Teorema Fondamentale dell'Algebra possiamo fattorizzare g nel prodotto di fattori lineari:

$$g(t) = a_\delta\cdot(t-\alpha_1)^{m_1}\cdot(t-\alpha_2)^{m_2}\cdots(t-\alpha_r)^{m_s}\,, \quad \sum_{i=1}^{s} m_i = \deg(g)\,.$$

Omogeneizzando $g(t)$ troviamo

$$G(\lambda,\mu) = \lambda^{d-\deg(g)}\cdot a\cdot(\mu-\alpha_1\lambda)^{m_1}\cdot(\mu-\alpha_2\lambda)^{m_2}\cdots(\mu-\alpha_r\lambda)^{m_s}\,,$$

che è un'espressione del tipo (2.4), dopo aver riscalato le variabili in modo da ottenere un polinomio senza ulteriori costanti moltiplicative. □

2.3.3 Il teorema di Vieta

Concludiamo con utile risultato che permette di passare dalla forma fattorizzata $f(x) = c \cdot \prod_{n=1}^{d}(x - \alpha_n)$ di un polinomio completamente riducibile nella sua forma standard $f(x) = \sum_{n=0}^{d} a_n x^n \in \mathbb{K}[x]$.

Definizione 2.25. Siano $x_1, \dots, x_n$ variabili su un campo $\mathbb{K}$. Il *polinomio elementare simmetrico e_i di grado omogeneo $i > 1$* è definito come

$$e_i(x_1, \dots, x_n) := \sum_{1 \le x_{j_1} < \dots x_{j_i} \le n} x_{j_1} x_{j_2} \cdots x_{j_i} \in \mathbb{K}[x], \qquad i > 1, \tag{2.5}$$

e per convenzione si definisce $e_0(x_1, \dots, x_n) = 1$.

Esempio 2.26. Alcuni polinomi elementari simmetrici leggono:

$$\begin{aligned}
e_0(x_1, \dots, x_n) &= 1, \\
e_1(x_1, \dots, x_n) &= x_1 + x_2 + \cdots + x_n, \\
e_2(x_1, \dots, x_n) &= x_1x_2 + x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \dots x_{n-1}x_n, \\
&\dots \\
e_n(x_1, \dots, x_n) &= x_1x_2 \cdots x_n, \\
e_{n+1}(x_1, \dots, x_n) &= 0, \\
e_{n+2}(x_1, \dots, x_n) &= 0, \\
&\dots
\end{aligned}$$

Teorema 2.27 (Vieta, 1579). *Sia $\mathbb{K} = \overline{\mathbb{K}}$ è un campo algebricamente chiuso e sia*

$$f(x) = \sum_{n=0}^{d} a_n x^n \in \mathbb{K}[x]$$

un polinomio di grado d nella sua forma standard. Sia

$$f(x) = c \cdot \prod_{n=1}^{d}(x - \alpha_n) \in \mathbb{K}[x]$$

la sua fattorizzazione sul campo $\mathbb{K}$ e si considerino i coefficienti a_n come funzioni delle radici α_i del polinomio. Si ha che

$$a_n(\alpha_1, \dots, \alpha_n) = a_d(-1)^{d-n} \cdot e_{d-n}(\alpha_1, \dots, \alpha_n). \tag{2.6}$$

In altre parole l'n-esimo coefficiente del polinomio è, a meno di costante, l'n-esimo polinomio simmetrico elementare valutato nelle radici del polinomio stesso.

Dimostrazione. La dimostrazione è per espansione del prodotto della fattorizzazione. □

Esempio 2.28. Sia

$$f(x) = 5(x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \in \mathbb{Q}[x].$$

Espandendo il prodotto troviamo:

$$\begin{aligned} f(x) &= 5x^3 + (-5)\left(\alpha_1 + \alpha_2 + \alpha_3\right)x^2 + 5(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3)x^1 + (-5)\alpha_1\alpha_2\alpha_3 \\ &= 5e_0x^3 - 5e_1x^2 + 5e_2x^1 - 5e_3 \in \mathbb{Q}[x]. \end{aligned}$$

dove i polinomi elementari e_i si intendono valutati nelle radici α_j.

3 Ipersuperfici algebriche: affini e proiettive

Introduciamo in questa sezione ipersuperfici nel caso affine e nel caso proiettivo. Le ipersuperfici in uno spazio n-dimensionale sono date dal luogo degli zeri di un polinomio, se il polinomio non è banale sono quindi oggetti $(n-1)$-dimensionali.

Nel caso del piano, affine o proiettivo rispettivamente, ovvero per $n = 2$, le ipersuperfici sono oggetti 1-dimensionali, e vengono quindi chiamate curve.

3.1 Il caso affine

Introduciamo ipersuperfici e curve nel caso affine.

3.1.1 Curve affini

Definizione 3.1. Dato un polinomio $f \in \mathbb{K}[x_1, \ldots, x_n]$ e un punto $P = (p_1, \ldots, p_n) \in \mathbb{A}^n_{\mathbb{K}}$, si indica con $f(P)$ la valutazione di f nelle coordinate di P, i.e. l'elemento $f(p_1, \ldots, p_n) \in \mathbb{K}$.

Indicheremo, inoltre, con $Z(f)$ il *luogo degli zeri di* f, cioè

$$Z(f) = \{P \in \mathbb{A}^n_{\mathbb{K}} \mid f(P) = 0\}.$$

Definizione 3.2. Una *curva algebrica piana affine* C è una coppia

$$C = \big(Z(f), f\big),$$

con $f \in \mathbb{K}[x, y]$ polinomio non costante (quindi di grado ≥ 1). Il luogo $Z(f)$ è chiamato *supporto di* C. L'equazione $f(x, y) = 0$ si dirà *equazione della curva* C. Il *grado* di C è per definizione il grado del polinomio f.

Osservazione 3.3. Due polinomi diversi possono definire curve con lo stesso supporto, come ad esempio nel caso di

$$f(x,y) = x - y \quad \text{e} \quad g(x,y) = (x-y)^2 .$$

Nel primo caso la curva è chiamata retta, nel secondo caso "retta doppia". Le rette doppie possono essere considerate come coniche piane "doppiamente degeneri", per cui vogliamo tenere traccia del fatto che sono determinate da un'equazione di secondo grado.

Esempio 3.4.

- Le rette affini sono curve algebriche di grado 1:

$$L = \big(Z(ax+by+c), ax+by+c\big),$$

  con $a, b, c \in \mathbb{K}$.

- Le coniche affini sono curve piane algebriche di grado 2:

$$C = \big(Z(a_0x^2 + a_1xy + a_2y^2 + b_0x + b_1y + c), a_0x^2 + a_1xy + a_2y^2 + b_0x + b_1y + c\big).$$

Definizione 3.5. Se $f(x,y) = f_1(x,y)^{\mu_1} \cdot f_2(x,y)^{\mu_2} \cdots f_r(x,y)^{\mu_r}$ per polinomi $f_i(x,y)$ di grado almeno uno irriducibili, allora le curve piane

$$C_i = (Z(f_i), f_i), \qquad i = 1, \ldots, r$$

si chiamano *componenti irriducibili (ridotte)* di C, di molteplicità $\mu_i \geq 0$.

Osservazione 3.6. Se $f = f_1 \cdots f_r$, allora $Z(f) = Z(f_1) \cup \cdots \cup Z(f_r)$.

Definizione 3.7.

- La curva $\big(Z(f), f\big)$ si dice *curva irriducibile* (risp. *riducibile*) sul campo $\mathbb{K}$ se e soltanto se $f(x,y)$ ha un'unica componente irriducibile (ha più di una componente irriducibile oppure non ne ha nessuna) sul campo $\mathbb{K}$.
- La curva $\big(Z(f), f\big)$ si dice *curva ridotta* (risp. *non ridotta*) sul campo $\mathbb{K}$ se e soltanto se $f(x,y)$ è un polinomio ridotto (non ridotto) sul campo $\mathbb{K}$.
- La curva $\big(Z(f), f\big)$ si dice *curva integrale* (risp. *non integrale*) sul campo $\mathbb{K}$ se e soltanto se $f(x,y)$ è un polinomio irriducibile (non irriducibile) sul campo $\mathbb{K}$.

Si noti che una curva irriducibile non è necessariamente ridotta così come una curva ridotta non è necessariamente irriducibile. Invece una curva è integrale se e soltanto se è sia ridotta che irriducibile.

Esempio 3.8.

- Sia $f = y^2 - x(x-1)(x-2)$. La curva $\big(Z(f), f\big)$ è una *cubica liscia* irriducibile.
- Sia $f = y^2 - x^3$. La curva $\big(Z(f), f\big)$ è una *cubica cuspidata* irriducibile.
- Sia $f = x(x-1)(x-2)$. La curva $\big(Z(f), f\big)$ è una *cubica riducibile ridotta*.
- Sia $f = xy^2$. La curva $\big(Z(f), f\big)$ è una *cubica riducibile non ridotta*, perché y è un polinomio di grado almeno uno e $y^2|f$.
- Sia $f = x^2$. La curva $\big(Z(f), f\big)$, detta *la retta doppia*, è una conica degenere, che è *irriducibile e non ridotta* (esempio principe di oggetto non ridotto). Nello stesso modo per $f = x^3$ si ha la cubica degenere detta retta tripla, irriducibile e non ridotta.

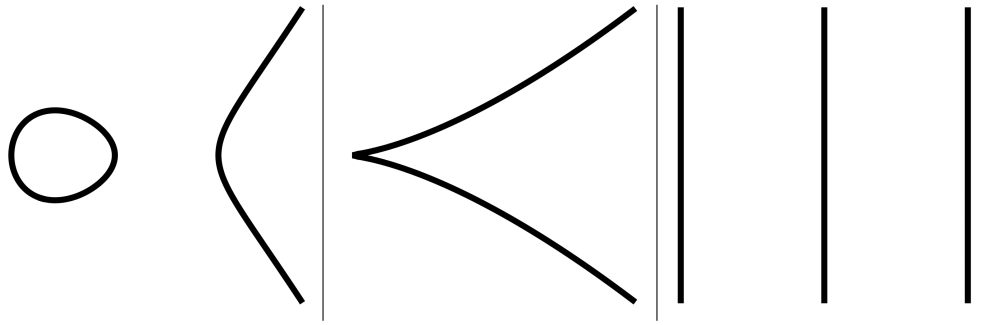


Figura 3.1: Da sinistra verso destra: 1. Una cubica piana liscia. 2. Una curva piana singolare (i.e. non liscia) cuspidata irriducibile ridotta. 3. Una cubica completamente riducibile ridotta.

3.1.2 Ipersuperfici affini

In modo perfettamente analogo a quello delle curve piane per $n = 2$ si possono definire le ipersuperfici affini per n un arbitrario numero intero positivo.

Definizione 3.9. Una *ipersuperficie algebrica affine* X è una coppia

$$X = \big(Z(f), f\big)\,,$$

con $f \in \mathbb{K}[x_1, \ldots, x_n]$ polinomio non costante (quindi di grado $d \geq 1$). Il luogo $Z(f) \subset \mathbb{A}^n_{\mathbb{K}}$ è chiamato *supporto di* C. L'equazione $f(x_1, \ldots, x_n) = 0$ si dirà *equazione della curva* C. Il *grado* di C è per definizione il grado del polinomio f.

Definizione 3.10 (Vocabolario ed esempi)**.**

- Se $n = 1$, un'ipersuperficie sarà data da un insieme finito di punti.

- Se $n = 2$, abbiamo visto che un'ipersuperficie si dice *curva*.
- Se $n = 3$, un'ipersuperficie si dice *superficie*.
- Se $d = 1$, un'ipersuperficie sarà data da un singolo punto per $n = 1$, da una *retta* per $n = 2$, da un *piano* per $n = 3$.
- Se $d = 2$, un'ipersuperficie sarà data da al più due punti per $n = 1$, da una *curva conica* per $n = 2$, da una *superficie quadrica* per $n = 3$.
- Se $d = 3$, un'ipersuperficie sarà data da al più tre punti per $n = 1$, da una *curva cubica* per $n = 2$, da una *superficie cubica* per $n = 3$.
- Se $d = 4$, un'ipersuperficie sarà data da al più quattro punti per $n = 1$, da una *curva quartica* per $n = 2$, da una *superficie quartica* per $n = 3$.

3.1.3 Comportamento sotto affinità

Consideriamo un'affinità $\alpha\colon \mathbb{A}^2_{\mathbb{K}} \to \mathbb{A}^2_{\mathbb{K}}$. Se $(x_1, y_1) = \alpha\big((x, y)\big)$, possiamo scrivere delle equazioni del tipo

$$\begin{cases} x_1 = ax + by + c\,, \\ y_1 = dx + ey + h\,, \end{cases}$$

con $\det \begin{pmatrix} a & b \\ d & e \end{pmatrix} \neq 0$. Data una curva $\big(Z(f), f\big)$, si ha

$$P_1 \in \alpha(Z(f)) \iff \alpha^{-1}(P_1) \in Z(f) \iff f\big(\alpha^{-1}(P_1)\big) = 0\,.$$

Se fissiamo una rappresentazione per α^{-1}:

$$\begin{cases} x = a_1x_1 + b_1y_1 + c_1\,, \\ y = d_1x_1 + e_1y_1 + h_1\,, \end{cases}$$

otteniamo la condizione

$$f(a_1x_1 + b_1y_1 + c_1, d_1x_1 + e_1y_1 + h_1) = 0\,.$$

Ponendo $f_1(x_1, y_1) := f(a_1x_1 + b_1y_1 + c_1, d_1x_1 + e_1y_1 + h_1)$, si ha quindi

$$\alpha\big(Z(f)\big) = Z(f_1)\,.$$

Definizione 3.11. Diremo che la curva algebrica $\big(Z(f_1), f_1\big)$ è immagine della curva $\big(Z(f), f\big)$ nell'affinità α. Due curve affini si dicono *affinemente equivalenti* se una è immagine dell'altra tramite un'affinità.

Vogliamo ora capire se un'affinità conserva il grado. A questo scopo consideriamo ogni monomio che appare in f:

$$f = \cdots + qx^k y^h + \cdots$$
$$f_1 = \cdots + q(a_1x_1 + b_1y_1 + c_1)^k(d_1x_1 + e_1y_1 + h_1)^h + \cdots$$

quindi il grado non può aumentare: $\deg(f) \geq \deg(f_1)$. Applicando poi l'affinità inversa, troviamo che vale anche $\deg(f_1) \geq \deg(f)$.

Riassumendo si ottiene la seguente proposizione.

Proposizione 3.12. *Sia $\alpha\colon \mathbb{A}^2_{\mathbb{K}} \to \mathbb{A}^2_{\mathbb{K}}$ un'affinità. Allora α manda curve algebriche in curve algebriche dello stesso grado.*

3.2 Il caso proiettivo

Introduciamo ipersuperfici e curve nel caso proiettivo.

3.2.1 Curve proiettive

Consideriamo ora il piano proiettivo standard $\mathbb{P}^2_{\mathbb{K}}$ con il riferimento proiettivo standard. Vorremmo definire le curve algebriche piane proiettive in modo analogo al caso affine, cioè come luoghi di zeri di opportuni polinomi. Ricordiamo che le tre coordinate omogenee di un punto proiettivo sono definite a meno di un fattore di proporzionalità, quindi, in generale, dato un polinomio arbitrario in tre indeterminate, il suo logo di zeri *non è ben definito*; ciò succede, ad esempio, nel caso:

$$f(x_0, x_1, x_2) = x_0 - x_1x_2\,.$$

Abbiamo che $P = (1:1:1) = (2:2:2)$, e $f(1,1,1) = 0$, mentre $f(2,2,2) = -2$.

Vedremo che se ci restringiamo all'insieme dei *polinomi omogenei*, il luogo degli zeri risulta ben definito.

Definizione 3.13. Una *curva piana algebrica proiettiva* è una coppia

$$C = \big(Z_P(F), F\big), \quad Z_P(F) \subset \mathbb{P}^2_{\mathbb{K}}$$

dove $F \in \mathbb{K}[x_0, x_1, x_2]_d$ è un polinomio omogeneo di grado $d \geq 1$. Il *grado* di C è per definizione il grado del polinomio F:

$$\deg(C) := \deg(F).$$

3.2.2 Ipersuperfici proiettive

Lemma 3.14. *Se $F \in \mathbb{K}[x_0, \dots, x_n]_d$, è ben definito il suo* luogo degli zeri proiettivi

$$Z_P(F) = \{(q_0 : \cdots : q_n) \in \mathbb{P}^n_{\mathbb{K}} \mid F(q_0, \dots, q_n) = 0\},$$

cioè l'annullamento non dipende dalla scelta delle coordinate omogenee.

Dimostrazione. Consideriamo un'altra tupla di coordinate omogenee $(\lambda q_0 : \cdots : \lambda q_n)$, con $\lambda \neq 0$, per lo stesso punto. Per la (2.1) si ha

$$F(\lambda q_0, \dots, \lambda q_n) = \lambda^d F(q_0, \dots, q_n) = 0 \iff F(q_0, \dots, q_n) = 0\,.$$

□

Osservazione 3.15. La "P" nella notazione $Z_P(F)$ indica che consideriamo gli zeri proiettivi. Dato un polinomio omogeneo F possiamo considerare anche l'insieme degli zeri affini $Z(F) \subset \mathbb{A}^{n+1}$; l'identità (2.1) ci dice che se un punto $Q = (q_0, \dots, q_n) \in \mathbb{A}^{n+1}$ annulla F, allora anche ogni $(n+1)$-upla proporzionale lo annulla; quindi se $F \in \mathbb{K}[x_0, \dots, x_n]_d$

$$Q \in Z(F) \iff \overline{OQ} \subset Z(F),$$

dove $\overline{OQ}$ indica la retta affine per l'origine O e per Q. In altre parole, $Z(F)$ è un *cono di vertice l'origine O*.

Definizione 3.16. Una *ipersuperficie algebrica proiettiva* è una coppia

$$\mathcal{X} = \big(Z_P(F), F\big), \quad Z_P(F) \subset \mathbb{P}^n_{\mathbb{K}}\,,$$

dove $F \in \mathbb{K}[x_0, \dots, x_n]_d$ con $d \geq 1$. Il *grado* di $\mathcal{X}$ è per definizione il grado del polinomio F:

$$\deg(\mathcal{X}) := \deg(F)\,.$$

3.2.3 Lo spazio affine nello spazio proiettivo

Ricordiamo che è possibile immergere iniettivamente il piano affine nel piano proiettivo tramite la mappa

$$j_0 \colon \mathbb{A}^2_{\mathbb{K}} \to \mathbb{P}^2_{\mathbb{K}}, \quad j_0\big((q_1, q_2)\big) := (1 : q_1 : q_2)\,.$$

Questa mappa non è suriettiva, e la sua immagine risulta essere

$$j_0(\mathbb{A}^2_{\mathbb{K}}) = \mathbb{P}^2_{\mathbb{K}} \setminus Z_P(x_0) =: U_0.$$

La retta $Z_P(x_0)$ è chiamata *retta all'infinito*. L'applicazione j_0 risulta, invece, iniettiva in quanto se restringiamo il codominio a U_0, essa ammette inversa, e precisamente la mappa

$$\varphi_0 \colon U_0 \to \mathbb{A}^2_{\mathbb{K}}, \quad \varphi_0(q_0 : q_1 : q_2) = \left(\frac{q_1}{q_0}, \frac{q_2}{q_0}\right).$$

Nel caso

$$\mathbb{K} = \mathbb{R},$$

un modello di $\mathbb{P}^2_{\mathbb{R}}$ è dato dal quoziente della sfera $S^2 \subset \mathbb{R}^3$ rispetto alla mappa antipodale, che identifica un punto $(q_0, q_1, q_2) \in S^2$ con il suo antipodale $(-q_0, -q_1, -q_2)$:

$$(q_0, q_1, q_2) \sim (r_0, r_1, r_2)$$
$$\iff$$
$$(r_0, r_1, r_2) = (q_0, q_1, q_2) \ \vee \ (r_0, r_1, r_2) = (-q_0, -q_1, -q_2).$$

La retta all'infinito può essere identificata con il quoziente del cerchio di raggio massimo

$$S^2 \cap Z(x_0),$$

e il piano affine con l'interno della semisfera superiore (o inferiore). Se muniamo $\mathbb{R}^3$ della topologia euclidea e $\mathbb{P}^2_{\mathbb{R}} = S^2/\sim$ della topologia quoziente, si ha che $\mathbb{P}^2_{\mathbb{R}}$ è compatto. Possiamo interpretare quindi $\mathbb{P}^2_{\mathbb{R}}$ come una *compattificazione* di $\mathbb{A}^2_{\mathbb{R}}$. La costruzione si può generalizzare facilmente e definire un'immersione

$$j_0 \colon \mathbb{A}^n_{\mathbb{K}} \to \mathbb{P}^n_{\mathbb{K}}.$$

3.2.4 Omogeneizzazione e deomogeneizzazione

Vedremo ora che data una curva piana affine $\big(Z(f), f\big)$ è sempre possibile trovare una curva proiettiva la cui restrizione a U_0 risulti uguale a $j_0\big(Z(f)\big)$; inoltre, data una curva piana proiettiva $\big(Z_P(F), F\big)$, la sua restrizione $Z_P(F) \cap U_0$ è sempre immagine di una curva algebrica piana affine. Per fare ciò abbiamo bisogno delle seguenti nozioni.

Definizione 3.17. L'operazione di *omogeneizzazione* di un polinomio è definita come

$$h \colon \mathbb{K}[x, y] \to \mathbb{K}[x_0, x_1, x_2], \quad (hf)(x_0, x_1, x_2) := x_0^{\deg(f)} \, f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right).$$

Osserviamo che la mappa h associa a un polinomio in due indeterminate arbitrario un polinomio omogeneo in tre indeterminate, dello stesso grado.

Esempio 3.18. Se $f(x,y) = xy - 1$, si ha $(hf)(x_0, x_1, x_2) = x_0^2 \left(\frac{x_1}{x_0}\frac{x_2}{x_0} - 1\right) = x_1x_2 - x_0^2$.

Definizione 3.19. L'operazione di *deomogeneizzazione rispetto a* x_0 è definita da:

$$a\colon \mathbb{K}[x_0, x_1, x_2] \to \mathbb{K}[x, y], \quad (aF)(x, y) := F(1, x, y).$$

Osserviamo che questa mappa è definita anche per polinomi non omogenei.

Esempio 3.20. Per $F = x_1x_2 - x_0$, si ha $aF = xy - 1$. In questo caso $\deg(F) = \deg(aF)$. Per $G = x_0x_1x_2 - x_0x_1^2 + x_0^3$, si ha $aG = xy - y^2 + 1$; in questo caso $\deg(G) = 3 \neq 2 = \deg(aG)$.

La deomogeneizzazione quindi non mantiene sempre il grado, ma vale il seguente.

Lemma 3.21. *Dati due polinomi $f \in \mathbb{K}[x, y]$ e $F \in \mathbb{K}[x_0, x_1, x_2]$, valgono le seguenti*

1. $a(hf) = f$;
2. *esiste $k \geq 0$ tale che $x_0^k \cdot h(aF) = F$.*

Proposizione 3.22.

1. *Sia $C = \big(Z(f), f\big)$ una curva piana affine. Allora vale*

$$j_0\big(Z(f)\big) = Z_P(hf) \cap U_0\,.$$

2. *Sia $C = (Z_P(F), F)$ una curva piana proiettiva. Allora vale*

$$\varphi_0\big(Z_P(F) \cap U_0\big) = Z(aF)\,.$$

Dimostrazione.

1. Osserviamo che

$$\begin{aligned} Q \in j_0(Z(f)) &\iff Q = j_0(q_1, q_2) = (1 : q_1 : q_2) \text{ e } (q_1, q_2) \in Z(f) \\ &\iff Q = (1 : q_1 : q_2) \text{ e } f(q_1, q_2) = 0. \end{aligned}$$

   Notiamo ora che $(hf)(Q) = (hf)(1, q_1, q_2) = 1^{\deg(f)} f\left(\frac{q_1}{1}, \frac{q_2}{1}\right) = f(q_1, q_2)$, quindi l'ultima condizione è equivalente a $Q \in U_0$ e $(hf)(Q) = 0$.

2. La verifica è simile al punto precedente ed è lasciata per esercizio. □

La proposizione appena vista motiva la seguente definizione:

Definizione 3.23. Sia $C = \big(Z(f), f\big)$ una curva piana affine. La sua *chiusura proiettiva* è la curva piana proiettiva

$$\bar{C} = (Z_P(hf), hf)\,.$$

Osservazione 3.24. Ricordiamo che quanto fatto per l'indeterminata x_0 può essere ripetuto analogamente per le altre indeterminate. Infatti, ponendo

$$U_1 := \mathbb{P}^2 \setminus Z_P(x_1)\,, \quad U_2 := \mathbb{P}^2 \setminus Z_P(x_2)\,,$$

si possono considerare le immersioni

$$j_1 \colon \mathbb{A}^2 \to \mathbb{P}^2, \quad j_1(q_1, q_2) = (q_1 : 1 : q_2),$$

e

$$j_2 \colon \mathbb{A}^2 \to \mathbb{P}^2, \quad j_1(q_1, q_2) = (q_1 : q_2 : 1),$$

e si ha $j_1(\mathbb{A}^2) = U_1$ e $j_2(\mathbb{A}^2) = U_2$. E' possibile, inoltre, definire delle omogeneizzazioni e deomogeneizzazioni rispetto alle indeterminate x_1 e x_2 in modo perfettamente analogo a prima, e ottenere degli enunciati simili alla Proposizione 3.22.

Osservazione 3.25. In modo perfettamente analogo possiamo deomogeneizzare e omogeneizzare polinomi in n indeterminate. I corrispondenti luoghi degli zeri hanno un'interpretazione analoga al caso di 3 indeterminate: il luogo $Z(aF) \subset \mathbb{A}^n$ corrisponde a $\varphi_0(Z_P(F) \cap U_0)$ e $j_0(Z(f)) = Z_P(hf) \cap U_0$.

3.3 Esercizi

1. Si dimostri che i polinomi $y - x^2 \in \mathbb{C}[x, y]$ e $x^2 + y^2 - 1 \in \mathbb{C}[x, y]$ sono irriducibili.
2. Si dimostri che un campo algebricamente chiuso ha infiniti elementi.
3. Si dimostri che una curva piana algebrica nel piano affine complesso $\mathbb{A}^2_{\mathbb{C}}$ ha infiniti punti. Questo è vero anche sul campo dei numeri reali $\mathbb{R}$?
4. Si dimostri che ogni affinità conserva il numero di fattori irriducibili di un polinomio $f(x, y)$.

5. Si dimostri che ogni affinità conserva la molteplicità di ogni fattore irriducibile di un polinomio $f(x, y)$.
6. Si determini una base del $\mathbb{K}$-sottospazio vettoriale $\mathbb{K}[x_0, x_1, x_2]_d$ dei polinomi omogenei di grado d con l'aggiunta del polinomio nullo, e si calcoli la sua dimensione.
7. Si verifichi che se $F(x_0, x_1, x_2) \in \mathbb{K}[x_0, x_1, x_2]_d$ è un polinomio omogeneo non nullo, allora
$$G(\lambda, \mu) := F(\lambda a_0 + \mu b_0, \lambda a_1 + \mu b_1, \lambda a_2 + \mu b_2)$$
dove $A = (a_0 : a_1 : a_2)$ e $B = (b_0 : b_1 : b_2)$ sono due punti distinti di $\mathbb{P}^2_{\mathbb{K}}$, è un polinomio omogeneo di grado d in $\mathbb{K}[\lambda, \mu]$.
8. Sia $r \subset \mathbb{A}^2_{\mathbb{K}}$ una retta affine di equazioni parametriche
$$\begin{cases} x = lt + q_1 \,, \\ y = mt + q_2 \,. \end{cases}$$
Si dimostri che la sua chiusura proiettiva è la retta proiettiva descritta da equazioni parametriche
$$\begin{cases} x_0 = \mu \\ x_1 = l\lambda + q_1\mu \,, \\ x_2 = m\lambda + q_2\mu \,. \end{cases}$$
9. Si consideri la curva piana affine di equazione
$$x^4 + y^4 - y(x^2 + y^2) = 0 \,.$$

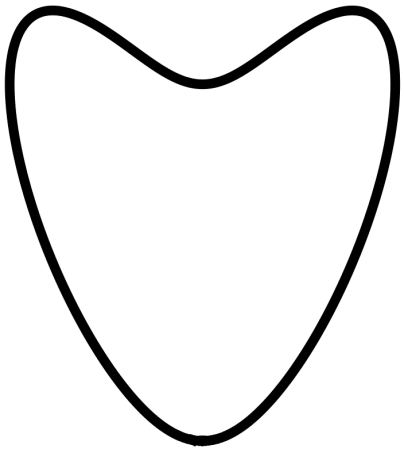


Figura 3.2: Luogo degli zeri reali del polinomio $x^4 + y^4 - y(x^2 + y^2)$.

a) Si trovi la chiusura proiettiva della curva e i suoi eventuali punti impropri;

b) si dica se la curva è irriducibile o meno.

10. Nel piano proiettivo complesso, si consideri la chiusura proiettiva $\bar{C}$ della curva affine di equazione:

$$(x-1)(x^2+y^2)-x=0\,.$$

Si determinino i punti impropri di $\bar{C}$.

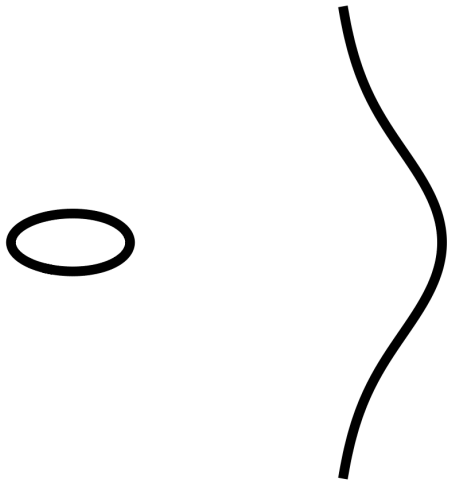


Figura 3.3: Luogo degli zeri reali del polinomio $(x-1)(x^2+y^2)-x$.

4 Intersezioni tra rette e curve piane

Il prossimo obiettivo è quello di studiare intersezioni tra curve algebriche, di dare la nozione di molteplicità di un punto e di molteplicità di intersezione in un punto. Per fare ciò sfrutteremo la nozione di molteplicità algebrica della radice di un polinomio in una variabile.

Iniziamo con un caso semplice: lo studio dell'intersezione tra una curva algebrica piana e una retta. Consideriamo il caso proiettivo, su un campo algebricamente chiuso, che risulta più semplice e presenta un comportamento costante; vedremo, infatti, che ogni curva algebrica piana proiettiva di grado $d \geq 1$ interseca una retta, non contenuta nel supporto della curva, in esattamente d punti, a patto di pesare ogni punto dell'intersezione con una opportuna molteplicità. Utilizzeremo i risultati della decomposizione dei polinomi omogenei studiati nella sezione 2.3

4.1 Il caso affine

I punti di intersezione tra una retta affine e una curva algebrica affine possono essere determinati per sostituzione, esprimendo la retta con equazioni parametriche e sostituendo alle indeterminate dell'equazione della curva le espressioni parametriche.

Osservazione 4.1. Sia $\big(Z(f), f\big)$ una curva piana affine, e sia $\ell \subset \mathbb{A}^2$ una retta affine con equazioni parametriche

$$\begin{cases} x = lt + q_1\,, \\ y = mt + q_2\,. \end{cases} \tag{4.1}$$

Sia $T \in \ell$ un punto corrispondente al valore $t = t_0$:

$$T = (lt_0 + q_1, mt_0 + q_2)\,.$$

Allora $T \in Z(f)$ se e solo se t_0 è radice del polinomio

$$g(t) := f(lt + q_1, mt + q_2)\,,$$

ovvero se e solo se $(t - t_0)$ divide g.

Osservazione 4.2. Osserviamo che il polinomio $g(t) := f(lt + q_1, mt + q_2)$ ha grado

$$\deg(g) \leq \deg(f)\,,$$

e potrebbe avere grado strettamente minore del grado di f, in particolare potrebbe essere una costante non nulla, nel qual caso g non ammette alcuna radice, e la curva $Z(f)$ e la retta ℓ hanno intersezione vuota. Ciò accade, ad esempio, nel caso delle due rette parallele $r = Z(y - 1)$ e $l = Z(y - 2)$: delle equazioni parametriche per ℓ sono

$$\begin{cases} x = t \\ y = 2, \end{cases}$$

e si ha $g(t) = 2 - 1 = 1$, oppure nel caso dell'iperbole $\big(Z(xy - 1), xy - 1\big)$ e l'asintoto $\ell = Z(x)$: delle equazioni parametriche per l sono

$$\begin{cases} x = 0 \\ y = t, \end{cases}$$

e si ha $g(t) = f(0, t) = -1$, che non ha radici.
Se intersechiamo, invece, l'iperbole $\big(Z(xy - 1), xy - 1\big)$ con la bisettrice $\ell = Z(x - y)$, che ha equazioni parametriche

$$\begin{cases} x = t \\ y = t, \end{cases}$$

e si ha $g(t) = f(t, t) = t^2 - 1$; abbiamo $\deg(g) = \deg(f)$, e ci sono due punti di intersezione, corrispondenti alle radici $t = 1$ e $t = -1$.
Infine, se intersechiamo l'iperbole $\big(Z(xy - 1), xy - 1\big)$ con la retta verticale $\ell = Z(x - 1)$, che ha equazioni parametriche

$$\begin{cases} x = 1 \\ y = t, \end{cases}$$

si ha $g(t) = f(1, t) = t - 1$; si ha $1 = \deg(g) < \deg(f) = 2$, l'unica radice di g è $t = 1$, e corrispondentemente abbiamo un unico punto di intersezione.

Definizione 4.3. Sia $\big(Z(f), f\big)$ una curva piana affine, e sia $\ell \subset \mathbb{A}^2$ una retta affine con equazioni parametriche (4.1). Supponiamo che

- $\ell \not\subset Z(f)$, e che
- $\ell \cap Z(f) \neq \emptyset$.

Sia $T \in \ell \cap Z(f)$ un punto nell'intersezione, corrispondente al valore $t = t_0$.
La *molteplicità di intersezione tra* $\big(Z(f), f\big)$ *ed* ℓ *in* T

$$I_T(f, \ell)$$

è la molteplicità della radice t_0 per il polinomio $g(t) := f(lt + q_1, mt + q_2)$.
Se $\ell \subset Z(f)$, poniamo per convenzione

$$I_T(f, \ell) = \infty$$

per ogni $T \in \ell$.

Esempio 4.4. La molteplicità di intersezione tra la parabola $\big(Z(y - x^2), y - x^2\big)$ e la retta $y = 0$ nell'origine $(0, 0)$ si determina come segue: delle equazioni parametriche per $y = 0$ sono

$$\begin{cases} x = t \\ y = 0; \end{cases}$$

Il polinomio $g(t) = f(t, 0) = 0 - t^2$ ha $t = 0$ come radice di molteplicità algebrica 2, quindi $I_{(0,0)}(f, y) = 2$.

Dalle definizioni segue immediatamente il seguente risultato.

Proposizione 4.5. *Sia* $\big(Z(f), f\big)$ *una curva piana affine, e sia* $\ell \subset \mathbb{A}^2$ *una retta affine non contenuta nella curva:* $\ell \not\subset Z(f)$. *Allora si ha*

$$\sum_{T \in Z(f) \cap \ell} I_T(f, \ell) \leq d.$$

4.2 Il caso proiettivo

Il caso proiettivo è analogo a quello affine.

Osservazione 4.6. Sia $\big(Z(F), F\big)$ una curva piana proiettiva, e sia $L \subset \mathbb{P}^2$ una retta proiettiva di equazioni parametriche

$$\begin{cases} x_0 = p_0\lambda + q_0\mu \\ x_1 = p_1\lambda + q_1\mu \\ x_2 = p_2\lambda + q_2\mu, \end{cases} \tag{4.2}$$

dove $P = (p_0 : p_1 : p_2) \in L$ e $Q = (q_0 : q_1 : q_2) \in L$ sono due punti distinti, e $(\lambda : \mu) \in \mathbb{P}^1$ è una coppia omogenea di parametri.

Sia $T \in L$ un punto corrispondente alla coppia $(\bar{\lambda} : \bar{\mu})$:

$$T = (p_0\bar{\lambda} + q_0\bar{\mu} : p_1\bar{\lambda} + q_1\bar{\mu} : p_2\bar{\lambda} + q_2\bar{\mu}) \in \mathbb{P}^2.$$

Allora $T \in Z_P(F)$ se e solo se $(\bar{\lambda} : \bar{\mu})$ è radice del polinomio

$$G(\lambda, \mu) := F(p_0\lambda + q_0\mu, p_1\lambda + q_1\mu, p_2\lambda + q_2\mu),$$

ovvero se e solo se $(\bar{\mu}\,\lambda - \bar{\lambda}\,\mu)$ divide $G(\lambda, \mu)$.

Osservazione 4.7. Diversamente dal caso affine, per il grado del polinomio $G(\lambda, \mu) := F(p_0\lambda + q_0\mu, p_1\lambda + q_1\mu, p_2\lambda + q_2\mu)$ ci sono solo due casi:

1. $G(\lambda, \mu) \equiv 0$ è il polinomio nullo; in questo caso la retta L risulta contenuta in $Z(F)$;
2. $G(\lambda, \mu)$ non è il polinomio nullo; in questo caso è omogeneo di grado esattamente $d = \deg(F)$ (esercizio).

Definizione 4.8. Sia $\big(Z_P(F), F\big)$ una curva piana proiettiva, e sia $L \subset \mathbb{P}^2$ una retta proiettiva con equazioni parametriche (4.2). Sia $T \in L \cap Z(F)$ un punto nell'intersezione, corrispondente alla coppia omogenea $(\bar{\lambda} : \bar{\mu})$.

La *molteplicità di intersezione tra* $(Z(F), F)$ *ed* L *in* T

$$I_T(F, L)$$

è la molteplicità della radice $(\bar{\lambda} : \bar{\mu})$ per il polinomio

$$G(\lambda, \mu) := F(p_0\lambda + q_0\mu, p_1\lambda + q_1\mu, p_2\lambda + q_2\mu)$$

Proposizione 4.9. *Sia* $\mathbb{K} = \overline{\mathbb{K}}$ *un campo algebricamente chiuso. Sia* $\big(Z_P(F), F\big)$ *una curva piana proiettiva in* $\mathbb{P}^2_{\mathbb{K}}$ *di grado* $\deg(F) = d$*, e sia* $L \subset \mathbb{P}^2_{\mathbb{K}}$ *una retta proiettiva non contenuta nella curva:* $L \not\subset Z_P(F)$*. Allora si ha*

$$\sum_{T \in Z(F) \cap L} I_T(F, L) = d\,.$$

Dimostrazione. Per l'Osservazione 4.7, siccome $L \not\subset Z_P(F)$, il polinomio $G(\lambda, \mu)$ ottenuto valutando F nelle equazioni parametriche di L non è identicamente nullo ed ha grado d. Per il Lemma 2.24 esso ha esattamente d radici, contate con le rispettive molteplicità; ognuna di esse determina un punto di intersezione con la stessa molteplicità, per definizione. □

Diamo, infine, la seguente definizione.

Definizione 4.10. Sia $\big(Z_P(F), F\big)$ una curva piana proiettiva in $\mathbb{P}^2_{\mathbb{K}}$ di grado $\deg(F) = d$, e sia $L \subset \mathbb{P}^2_{\mathbb{K}}$ una retta proiettiva non contenuta nella curva: $L \not\subset Z_P(F)$. Diremo che $\big(Z_P(F), F\big)$ ed L si intersecano *trasversalmente* in $T \in Z_P(F) \cap L$ se

$$I_T(F, L) = 1\,.$$

4.3 Esercizi

1. a) Siano $f, g \in \mathbb{K}[x, y]$. Si dimostri che i polinomi omogeneizzati verificano

$$h(f \cdot g) = hf \cdot hg\,.$$

   b) Siano $F, G \in \mathbb{K}[x_0, x_1, x_2]$ due polinomi omogenei. Si dimostri che i deomogeneizzati verificano

$$a(F \cdot G) = aF \cdot aG\,.$$

2. Sia $\varphi\colon \mathbb{P}^2 \to \mathbb{P}^2$. Si dimostri che se F è un polinomio omogeneo di grado $d \geq 1$, allora $\varphi(Z_P(F))$ è il luogo degli zeri di un polinomio dello stesso grado d.

   Si verifichi, inoltre, che φ mantiene il numero e i gradi delle componenti irriducibili di $Z_P(F)$.
3. Sia $F \in \mathbb{K}[x_0, x_1, x_2]_d$ e sia $G(\lambda, \mu) := F(p_0\lambda + q_0\mu, p_1\lambda + q_1\mu, p_2\lambda + q_2\mu) \in \mathbb{K}[\lambda, \mu]$. Si dimostri che se $G(\lambda, \mu)$ non è il polinomio nullo, allora è omogeneo di grado esattamente $d = \deg(F)$.

5 Singolarità di curve piane

5.1 Definizione geometrica di punto singolare

Definizione 5.1. Sia $\big(Z(f), f\big)$ una curva affine, rispettivamente $\big(Z_P(F), F\big)$ una curva proiettiva. Un punto $Q \in Z(f)$, rispettivamente $Q \in Z_P(F)$, si dice *singolare* se per ogni retta $L \ni Q$ si ha

$$I_Q(f, L) \geq 2, \quad \text{risp. } I_Q(F, L) \geq 2\,.$$

Un punto $Q \in Z(f)$, rispettivamente $Q \in Z_P(F)$, si dice *non singolare* o *liscio* altrimenti.

Definizione 5.2. Diremo anche che Q è un *punto di molteplicità* m per C se per ogni retta $L \ni Q$ si ha

$$I_Q(Z_P(F), L) \geq m$$

ed esiste almeno una retta $\overline{L}$ tale che

$$I_Q(Z_P(F), \overline{L}) = m\,.$$

Se $m \geq 2$, diremo anche che Q è un *punto m-plo*. In particolare, si dirà:

- Q *doppio* se $m = 2$;
- Q *triplo* se $m = 3$.

Osservazione 5.3. Nel caso affine, un punto $Q \in Z(f) \subseteq \mathbb{A}^2_{\mathbb{C}}$ si dice *singolare* se $j_0(Q)$ è singolare per $Z_P(hf)$.

Esempio 5.4. Cubica nodata affine e proiettiva.

Osservazione 5.5. Se $f(x, y)$, rispettivamente $F(x_0, x_1, x_2)$, è *non ridotto*, cioè ammette un fattore multiplo:

$$h^m \mid f, \quad H^m \mid F, \quad m \geq 2\,,$$

allora $Z(h) \subset Z(f)$, ovvero $Z_P(H) \subset Z_P(F)$ e ogni punto di $Z(h)$, rispettivamente di $Z_P(F)$, è singolare per $Z(f)$ ovvero $Z_P(F)$. Infatti, si verifica facilmente che per ogni $Q \in Z(h)$ e ogni retta $L \ni Q$, la radice di $g(t)$ corrispondente a Q ha molteplicità algebrica $\geq m$ (analogamente per $Z_P(H)$).

5.2 Polinomi derivati e polinomi di Taylor

In questa sezione vedremo delle nozioni di calcolo differenziale per polinomi a coefficienti in un dominio d'integrità D qualunque; non utilizzeremo tecniche metriche, e non parleremo di limiti di rapporti incrementali. Utilizzeremo, invece, le proprietà della derivazione di monomi conosciute nel caso di coefficienti reali per dare delle definizioni di tipo generale.

Infine, nel caso in cui $D \supseteq \mathbb{Q}$, illustreremo delle formule di Taylor per polinomi in una indeterminata e più indeterminate, perfettamente analoghe al caso reale. Vedremo che è possibile introdurre anche delle versioni omogenee di tali formule.

Definizione 5.6. Sia D un dominio d'integrità e sia $f \in D[t]$, con

$$f = a_m t^m + a_{m-1} t^{m-1} + \cdots + a_1 t + a_0.$$

Il *polinomio derivato* f' di f è per definizione

$$f'(t) := m\ a_m t^{m-1} + (m-1)\ a_{m-1} t^{m-2} + \cdots + a_1\,,$$

dove si intende $m\ a_m = a_m + \cdots + a_m$, la somma di m termini uguali ad a_m, ed analogamente per gli altri coefficienti.

Lemma 5.7. *La derivazione di polinomi soddisfa la* regola di Leibnitz*:*

$$(f_1(t) \cdot f_2(t))' = f_1'(t) \cdot f_2(t) + f_1(t) \cdot f_2'(t)\,.$$

Dimostrazione. Si faccia la verifica per esercizio. □

Vediamo ora la formula di Taylor per polinomi, che vale per coefficienti in un qualsiasi campo. Ricordiamo che lo spazio dei polinomi di grado $\leq d$ in una indeterminata ha dimensione:

$$\dim \mathbb{K}[t]_{\leq d} = d + 1,$$

e una base (base standard) è data da

$$\{t^d, t^{d-1}, \dots, t, 1\}.$$

Vediamo però può essere comodo considerare una base diversa.

Lemma 5.8. *Sia $\mathbb{K} \supseteq \mathbb{Q}$ un campo. Allora per ogni $b \in \mathbb{K}$, l'insieme*

$$\{(t-b)^d, (t-b)^{d-1}, \dots, t-b, 1\}$$

è una base di $\mathbb{K}[t]_{\leq d}$.

Dimostrazione. Mostriamo che i polinomi sono linearmente indipendenti; lo facciamo per induzione su d. Se $d = 0$, una combinazione lineare nulla del polinomio costante 1 è $c_0 \cdot 1 = 0$, da cui otteniamo direttamente che $c_0 = 0$. Supponiamo ora $d \geq 1$ e consideriamo una combinazione lineare che dia il polinomio nullo:

$$c_d(t-b)^d + c_{d-1}(t-b)^{d-1} + \cdots + c_1(t-b) + c_0 = 0, \tag{5.1}$$

cioè il polinomio con tutti i coefficienti dei monomi t^i nulli. Per il principio di identità dei polinomi, anche l'espressione sinistra deve avere questa proprietà. Osserviamo che il coefficiente di t^d è c_d, quindi otteniamo $c_d = 0$ e la (5.1) diventa

$$c_{d-1}(t-b)^{d-1} + \cdots + c_1(t-b) + c_0 = 0,$$

e per ipotesi induttiva anche i coefficienti $c_{d-1} = c_{d-2} = \cdots = c_0 = 0$.
Essendo i polinomi $(t-b)^i$ esattamente in numero di $d+1 = \dim \mathbb{K}[t]$ e linearmente indipendenti, formano una base. □

Come conseguenza abbiamo che ogni polinomio $g(t) \in \mathbb{K}[t]$ può essere scritto in modo unico come combinazione lineare della base $(t-b)^i$:

$$g(t) = b_d(t-b)^d + b_{d-1}(t-b)^{d-1} + \cdots + b_1(t-b) + b_0.$$

I coefficienti b_i sono determinati dal seguente risultato.

Teorema 5.9 (Formula di Taylor per polinomi in una indeterminata)**.** *Sia $D \supseteq \mathbb{Q}$ un dominio d'integrità contenente i numeri razionali. Dato $g \in D[t]$ di grado $d \geq 1$, vale l'identità*

$$g(t) = \sum_{i=0}^{d} \frac{g^{(i)}(b)}{i!}(t-b)^i, \tag{5.2}$$

dove $g^{(i)}(b)$ denota la derivata i-esima valutata in b.

Dimostrazione. Scriviamo $g(t) = b_d(t-b)^d + b_{d-1}(t-b)^{d-1} + \cdots + b_1(t-b) + b_0$. Osserviamo che

$$g(b) = b_0.$$

Inoltre, se deriviamo, otteniamo:

$$g'(t) = d\, b_d(t-b)^{d-1} + (d-1)\, b_{d-1}(t-b)^{d-2} + \cdots + b_1,$$

da cui

$$g'(b) = b_1.$$

Derivando ancora, al passo i otteniamo

$$\begin{aligned} g^{(i)}(t) = d(d-1)\cdots(d-i+1)\, b_d(t-b)^{d-i} + \\ + (d-1)\cdots(d-2+1)\, b_{d-1}(t-b)^{d-i-1} + \cdots + i(i-1)\cdots 2\, b_i, \end{aligned}$$

da cui

$$g^{(i)}(b) = i!\, b_i.$$

□

Passiamo ora ai polinomi in più indeterminate.

Definizione 5.10. Sia $\mathbb{K}$ un campo e sia $f \in \mathbb{K}[x_1, \ldots, x_n]$. Se pensiamo $\mathbb{K}[x_1, \ldots, x_n] = \mathbb{K}[x_1, \ldots, \hat{x}_i, \ldots, x_n][x_i]$, ponendo $D = \mathbb{K}[x_1, \ldots, \hat{x}_i, \ldots, x_n]$, definiamo $\partial_{x_i} g$ la *derivata parziale di f rispetto a x_i* come il polinomio derivato di $f \in D[x_i]$.

Analogamente si possono definire le derivate parziali di ordine superiore.

Teorema 5.11 (Formula di Taylor omogenea)**.** *Sia $\mathbb{K} \supseteq \mathbb{Q}$ un campo. Se $G(\lambda, \mu) \in \mathbb{K}[\lambda, \mu]_d$ è un polinomio omogeneo, allora vale la formula*

$$G(\lambda, \mu) = \sum_{i=0}^{d} \frac{\partial_{\mu^i} G(\lambda, 0)}{i!} \mu^i. \tag{5.3}$$

Dimostrazione. Si tratta della formula di Taylor per $G \in \mathbb{K}[\lambda][\mu] = D[\mu]$ espressa in $b = 0$. □

Definizione 5.12. Dato $f \in \mathbb{K}[x_1, \ldots, x_n]$, definiamo il suo *gradiente* come il vettore colonna

$$\nabla f = \begin{pmatrix} \partial_{x_1} f \\ \partial_{x_2} f \\ \vdots \\ \partial_{x_n} f \end{pmatrix}.$$

Osservazione 5.13. Dalla definizione si può verificare che anche per i polinomi a coefficienti in un campo arbitrario vale il *Teorema di Schwarz*, cioè le derivate parziali sono invariate se si permuta l'ordine di derivazione.

Osservazione 5.14. E' facile verificare che se $F \in \mathbb{K}[x_1, \dots, x_n]_d$ è un polinomio omogeneo, anche tutte le sue derivate parziali sono polinomi omogenei, se non identicamente nulli. Inoltre, la derivazione rispetto a una indeterminata abbassa il grado di 1.

Proposizione 5.15 (Derivazione di composizione di polinomi)**.** *Se* $g \in \mathbb{K}[x_1, x_2, \dots, x_n]$, *e* $x_1(t), \dots, x_n(t) \in \mathbb{K}[t]$, *si ha*

$$\begin{aligned} f\big(x_1(t), x_2(t), \dots, x_n(t)\big)' &= \partial_{x_1} f \, x_1(t)' + \partial_{x_2} f \, x_2(t)' + \cdots + \partial_{x_n} f \, x_n(t)' \\ &= \begin{pmatrix} x_1(t)' & x_2(t)' & \cdots & x_n(t)' \end{pmatrix} \cdot \nabla f. \end{aligned}$$

Dimostrazione. Esercizio. □

Teorema 5.16 (Formula di Eulero)**.** *Sia* $F \in \mathbb{K}[x_0, x_1, \dots, x_n]_d$ *omogeneo di grado* $d \geq 1$, *Allora vale l'identità*

$$(\deg F) \cdot F = \sum_{i=0}^{n} x_i \partial_{x_i} F = \begin{pmatrix} x_0 & x_1 & \dots & x_n \end{pmatrix} \cdot \nabla F.$$

Dimostrazione. Ricordiamo che per il Lemma 2.20 F è omogeneo di grado d se e solo se

$$F(tx_0, tx_1, \dots, tx_n) = t^d \, F(x_0, x_1, \dots, x_n)$$

come polinomi in $\mathbb{K}[x_0, x_1, \dots, x_n, t]$. Derivando rispetto a t i due membri otteniamo

$$\begin{pmatrix} x_0 & x_1 & \cdots & x_n \end{pmatrix} \cdot \nabla F = d \, t^{d-1} \, F(x_0, x_1, \dots, x_n) \, .$$

Infine, valutando l'ultima uguaglianza in $t = 1$ troviamo la tesi. □

Teorema 5.17 (Formula di Taylor per polinomi in due indeterminate)**.** *Sia* $\mathbb{K} \supseteq \mathbb{Q}$ *un campo contenente i numeri razionali, sia* $g \in \mathbb{K}[x, y]$ *e siano* $a, b \in \mathbb{K}$ *arbitrari.*

Allora l'espansione di Taylor di $g(x,y)$ nel punto (a,b) legge:

$$\begin{aligned}
g(x,y) &= \sum_{n=0}^{\infty} \frac{1}{n!} \left((x-a)\partial_x + (y-b)\partial_y\right)^n . g(x,y)\Big|_{(x,y)=(a,b)} \\
&= \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{i=0}^{n} \binom{n}{i} (\partial_x^i \partial_y^{n-i} g)(a,b)\,(x-a)^i (y-b)^{n-i} \\
&= g(a,b) + (\partial_x g)(a,b)(x-a) + (\partial_y g)(a,b)(y-b) \\
&\quad + \frac{1}{2}\Big[(\partial_{xx} g)(a,b)(x-a)^2 + 2(\partial_{xy} g)(a,b)(x-a)(y-b) \\
&\qquad + (\partial_{yy} g)(a,b)(y-b)^2\Big] \\
&\quad + \frac{1}{3!}[(\partial_{xxx} g)(a,b)(x-a)^3 + 3(\partial_{xxy} g)(a,b)(x-a)^2(y-b) \\
&\qquad + 3(\partial_{xyy} g)(a,b)(x-a)(y-b)^2 + (\partial_{yyy} g)(a,b)(y-b)^3] + \dots
\end{aligned}$$

Dimostrazione. La dimostrazione si basa sul fatto che l'insieme di tutti i prodotti di potenze dei binomi $(x-a)$ e $(y-b)$ è una base dello spazio vettoriale $\mathbb{K}[x,y]$. □

Naturalmente nella somma su n i termini con $n > \deg(g)$ contribuiscono zero e quindi si possono eliminare, rendendo la somma finita. Generalizzando, per polinomi in più indeterminate vale la seguente formula di Taylor.

Corollario 5.18. *Sia $\mathbb{K} \supseteq \mathbb{Q}$, sia $g \in \mathbb{K}[x_1,\dots,x_k]$ e sia $\vec{a} := (a_1,\dots,a_k)$ un punto di $\mathbb{K}^k$. Allora l'espansione di Taylor di g nel punto $\vec{a}$ legge:*

$$g(x_1,\dots,x_k) = \left[\sum_{n=0}^{\deg(g)} \frac{1}{n!} \left(\sum_{i=1}^{k} (x_i - a_i)\partial_{x_i}\right)^n . g(x_1,\dots,x_k)\right]\Big|_{(x_1,\dots,x_k)=(a_1,\dots,a_k)}$$

5.2.1 Caratterizzazione differenziale dei punti singolari

Vediamo ora come le formule di Taylor ci permettono di caratterizzare i punti singolari.

Iniziamo con il caso proiettivo, e consideriamo le curve di $\mathbb{P}^2$ per semplicità. Dato $Q = (q_0 : q_1 : q_2) \in Z_P(F)$ e $A = (a_0 : a_1 : a_2) \neq Q$, le coordinate omogenee del generico punto della retta $\overline{QA}$ si scrivono nella forma $(\lambda q_0 + \mu a_0 : \lambda q_1 + \mu a_1 : \lambda q_2 + \mu a_2)$, e poniamo

$$G(\lambda,\mu) := F(\lambda q_0 + \mu a_0 : \lambda q_1 + \mu a_1 : \lambda q_2 + \mu a_2).$$

Ricordiamo che la molteplicità del punto Q è per definizione la molteplicità della radice $(1:0)$, ovvero la molteplicità del fattore μ per $G(\lambda,\mu)$. Usando (5.3), scriviamo la formula di Taylor per $G(\lambda,\mu)$ nel punto Q, quindi per $\mu = 0$:

$$\begin{aligned} G(\lambda,\mu) &= \sum_{i=0}^{d} \frac{\partial_{\mu^i} G(\lambda,0)}{i!}\mu^i \\ &= F(\lambda Q) + (\partial_{x_0}F(\lambda Q)\,a_0 + \partial_{x_1}F(\lambda Q)\,a_1 + \partial_{x_2}F(\lambda Q)\,a_2)\,\mu \\ &+ \frac{1}{2}\left(\sum_{i,j=0}^{2} \partial_{x_i x_j}F(\lambda Q)\,a_i\,a_j\right)\mu^2 \\ &+ \dots \\ &+ \frac{1}{m!}\left(\sum_{i_1,\dots,i_m=0}^{2} \partial_{x_{i_1}\dots x_{i_m}}F(\lambda Q)\,a_{i_1}\cdots a_{i_m}\right)\mu^m \\ &+ \dots \end{aligned}$$

ovvero

$$\begin{aligned} G(\lambda,\mu) &= F(Q)\,\lambda^d + (\partial_{x_0}F(Q)\,a_0 + \partial_{x_1}F(Q)\,a_1 + \partial_{x_2}F(Q)\,a_2)\,\lambda^{d-1}\mu \\ &+ \frac{1}{2}\left(\sum_{i,j=0}^{2} \partial_{x_i x_j}F(Q)\,a_i\,a_j\right)\lambda^{d-2}\mu^2 \\ &+ \dots \\ &+ \frac{1}{m!}\left(\sum_{i_1,\dots,i_m=0}^{2} \partial_{x_{i_1}\dots x_{i_m}}F(Q)\,a_{i_1}\cdots a_{i_m}\right)\lambda^{d-m}\mu^m \\ &+ \dots \end{aligned}$$

Quindi Q è singolare di molteplicità m se e solo se $G(\lambda,\mu)$ è divisibile per μ^m e non è divisibile per μ^{m+1}, e dalla formula di Taylor vediamo che ciò succede se e solo se tutte le derivate parziali k-esime di F con $k \leq m-1$ si annullano in Q, ed esiste almeno una derivata parziale m-esima di F che non si annulla in Q. Infatti, il coefficiente $\left(\sum_{i_1,\dots,i_k=0}^{2} \partial_{x_{i_1}\dots x_{i_k}}F(Q)\,a_{i_1}\cdots a_{i_k}\right)$ è nullo per il generico punto $A = (a_0 : a_1 : a_2) \in \mathbb{P}^2 \setminus \{Q\}$ se è solo se il polinomio

$$\sum_{i_1,\dots,i_k=0}^{2} \partial_{x_{i_1}\dots x_{i_k}}F(Q)\,x_{i_1}\cdots x_{i_k} = 0$$

è identicamente nullo (se non lo fosse, il suo luogo di zeri sarebbe una curva, e non tutto il piano proiettivo meno un punto).

Abbiamo così anticipato una parte della dimostrazione del seguente risultato:

Proposizione 5.19. *Un punto $Q \in Z_P(F)$ è singolare di molteplicità $m \geq 2$ se e solo se tutte le derivate parziali $(m-1)$-esime di F si annullano in Q, ed esiste almeno una derivata parziale m esima di F che non si annulla in Q.*

Dimostrazione. Ci basta verificare che se Q annulla tutte le derivate parziali $(m-1)$-esime di F, allora annulla anche tutte le derivate parziali k-esime per ogni $k \leq m-1$. Questo segue immediatamente dalle formule di Eulero iterate:

$$(d-1)\,\partial_{x_i} F = \begin{pmatrix} x_0 & x_1 & x_2 \end{pmatrix} \cdot \nabla(\partial_{x_i} F),$$
$$(d-k)\,\partial_{x_{i_1}\ldots x_{i_k}} F = \begin{pmatrix} x_0 & x_1 & x_2 \end{pmatrix} \cdot \nabla(\partial_{x_{i_1}\ldots x_{i_k}} F).$$

□

Vediamo, infine, il criterio differenziabile per le singolarità di curve affine. Siccome le molteplicità di intersezione tra curve e rette vengono mantenute identificando l'aperto U_0 con $\mathbb{A}^2$, omogeneizzando troviamo:

$$m_q(Z(f)) = m \iff m_{j_0(q)}(Z_P(hf)) = m\,.$$

Avendo $F(x_0, x_1, x_2) = hf(x_0, x_1, x_2) = x_0^{\deg(f)} f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right)$, si ottiene

$$\partial_{x_1} F(1, q_1, q_2) = \partial_x f(q_1, q_2), \quad \partial_{x_2} F(1, q_1, q_2) = \partial_y f(q_1, q_2)\,.$$

Infine, usando la formula di Eulero, si trova che $q \in Z(f)$ è singolare se e solo se

$$\partial_x f(q) = 0 = \partial_y f(q)\,.$$

5.2.2 Retta tangente e cono tangente

Definizione 5.20. Se $Q \in Z_P(F) \subset \mathbb{P}^2$ è non singolare, allora la retta di equazione

$$\begin{pmatrix} x_0 & x_1 & x_2 \end{pmatrix} \cdot \nabla F(Q) = 0, \quad \text{ovvero } \partial_{x_0} F(Q) x_0 + \partial_{x_1} F(Q) x_1 + \partial_{x_2}(Q) x_2 = 0$$

si chiama *retta tangente a $Z_P(F)$ in Q*, e si indica con $\tau_Q(Z_P(F))$.

Per trovare l'equazione della retta tangente nel caso affine è sufficiente deomogeneizzare l'equazione omogenea ed usare la formula di Eulero.

Definizione 5.21. Se $q = (q_1, q_2) \in Z(f) \subset \mathbb{A}^2$ è non singolare, allora la retta di equazione

$$\begin{pmatrix} x - q_1 & y - q_2 \end{pmatrix} \cdot \nabla f(q) = 0, \quad \text{ovvero} \quad \partial_x f(q)(x - q_1) + \partial_y f(q)(y - q_2) = 0$$

si chiama *retta tangente affine a* $Z(f)$ *in* q, e si indica con $t_q(Z(f))$.

Definizione 5.22. Se Q è singolare per $Z_P(F)$ di molteplicità $m \geq 2$, allora la curva di equazione

$$\sum_{i_1,\dots,i_m=0}^{2} \partial_{x_{i_1}\dots x_{i_m}} F(Q)\, x_{i_1} \cdots x_{i_m} = 0 \tag{5.4}$$

si chiama *cono tangente proiettivo a* $Z_P(F)$ *in* Q.

Osservazione 5.23. È possibile dimostrare che (5.4) è unione di m rette passanti per Q, non necessariamente tutte distinte. Ogni tale retta si chiama *tangente principale in* Q.

5.2.3 Molteplicità dell'origine per curve affini

Nel caso in cui una curva affine $Z(f) \subset \mathbb{A}^2$ passi per l'origine $(0,0)$, la verifica della molteplicità di $(0,0)$ e le equazioni delle tangenti principali sono particolarmente semplici.

Ricordiamo che la formula di Taylor per un polinomio f di grado d legge:

$$f(x,y) = \sum_{n=0}^{d} \frac{1}{n!} \sum_{i=0}^{n} \binom{n}{i} (\partial_x^i \partial_y^{n-i} f)(a,b)\, (x-a)^i (y-b)^{n-i}$$

Chiaramente se $(a,b) = (0,0)$ e se $f(0,0) = 0$, il polinomio f non ha termine noto. Espansa nell'origine la formula sopra quindi legge:

$$f(x,y) = \sum_{n=1}^{d} \frac{1}{n!} \sum_{i=0}^{n} \binom{n}{i} (\partial_x^i \partial_y^{n-i} f)(0,0)\, x^i y^{n-i}$$

Inoltre le sue componenti omogenee sono esattamente indicizzate da n:

$$f(tx,ty) = \sum_{n=0}^{d} \frac{t^n}{n!} \sum_{i=0}^{n} \binom{n}{i} (\partial_x^i \partial_y^{n-i} f)(0,0)\, x^i y^{n-i} = \sum_{n=1}^{d} t^n f_n(x,y).$$

Ne segue che la componente omogenea di grado n in f è data da

$$f_n(x,y) = \frac{1}{n!} \sum_{i=0}^{n} \binom{n}{i} (\partial_x^i \partial_y^{n-i} f)(0,0)\, x^i y^{n-i}, \qquad n = 1, \dots, d.$$

La generica retta per $(0,0)$ e per il punto $(a,b) \neq (0,0)$ ha equazioni parametriche

$$\begin{cases} x = at \\ y = bt \end{cases}$$

Inoltre si ha

$$\begin{aligned} f(at,bt) &= f_1(at,bt) + f_2(at,bt) + \cdots + f_d(at,bt) \\ &= t\, f_1(a,b) + t^2 f_2(a,b) + \cdots + t^d f_d(a,b)\,. \end{aligned}$$

Siamo ora pronti per studiare la molteplicità del punto $(0,0)$ per la curva $Z(f)$ in termini di molteplicità della radice del polinomio di Taylor nella variabile omogenea t.

In altre parole il punto $(0,0)$ ha molteplicità m per la curva $Z(f)$ se e soltanto se il punto $(0,0)$ è una radice di molteplicità m per $g(t) := f(at,bt) \in \mathbb{K}[t]$, e questo accade se e soltanto se

$$f_1(a,b) = f_2(a,b) = \cdots = f_{m-1}(a,b) = 0, \qquad f_m(a,b) \neq 0.$$

Siccome abbiamo parametrizzato una retta generica passante per il punto (a,b) e per l'origine, allora le condizioni sulle componenti omogenee f_n devono valere per ogni punto $(a,b) \in \mathbb{K}^2 \setminus \{(0,0)\}$. D'altra parte però anche la valutazione dei f_n per $n = 1,\ldots,d$ nell'origine deve ritornare il valore zero perchè f_n è omogeneo di grado positivo.

Riassumendo, abbiamo ottenuto il seguente risultato.

Lemma 5.24. *L'origine ha molteplicità m per la curva $Z(f)$ se e soltanto se*

$$f_1 \equiv f_2 \equiv \cdots = f_{m-1} \equiv 0, \qquad f_m \not\equiv 0.$$

Otteniamo inoltre il seguente lemma.

Lemma 5.25. *Se l'origine è singolare di molteplicità m (i.e. $m \geq 2$) per $Z(f)$, l'equazione del cono tangente è data da $f_m = 0$. Se l'origine è non singolare, un'equazione della retta tangente affine nell'origine è data da $f_1 = 0$.*

Dimostrazione. La dimostrazione segue dalle definizioni e dall'espansione di Taylor di f. Infatti, se l'origine è singolare di molteplicità m abbiamo che $f_n \equiv 0$ per ogni

$n = 0, \dots, m-1$ mentre f_m non è identicamente nullo, quindi l'equazione $f_m = 0$ determina la curva piana di grado m data dall'equazione

$$\sum_{i=0}^{m} \left(\frac{\partial_x^i}{i!} \frac{\partial_y^{m-i}}{(m-i)!} f \right) (x,y)\, x^i y^{m-i} = 0,$$

che è esattamente l'equazione del cono tangente per la definizione in 5.4. I fattoriali sono dovuti alla desimmetrizzazione della formula. Se l'origine è un punto liscio allora si osservi che

$$f_1 = 0 \iff (\partial_x f)(x,y) + (\partial_y f)(x,y) = 0 \iff ({}^t\nabla f).(x,y) = 0$$

ovvero $f_1 = 0$ determina l'equazione della retta tangente. □

5.3 Luogo singolare di curve ridotte

Concludiamo il capitolo con un importante teorema sulla finitezza dei punti singolari per curve ridotte.

Teorema 5.26. *Sia $\mathbb{K} = \overline{\mathbb{K}}$ un campo algebricamente chiuso e sia $F \in \mathbb{K}[x_0, x_1, x_2]_{d>0}$. Allora sia ha che*

$$|\operatorname{Sing}(Z_P(F))| < \infty \iff Z_P(F) \text{ è ridotta } .$$

Dimostrazione. Dimostriamo separatamente entrambe le implicazioni.
$\Leftarrow$). Supponiamo che $Z_P(F)$ sia una curva non ridotta. Sia $F = F_1^{m_1} \cdots F_r^{m_r}$ la sua scomposizione in componenti irriducibili. Per ipotesi esiste almeno un $m_i \geq 2$. Allora $Z(F_i^{m_i}) \subset Z(F)$ e $\operatorname{Sing}(Z(F_i^{m_i})) \subset \operatorname{Sing}(Z(F))$, quindi $|\operatorname{Sing}(Z(F_i^{m_i}))| < |\operatorname{Sing}(Z(F))|$. Per ipotesi ogni punto di $Z(F_i^{m_i})$ è singolare, $\deg(F_i) \geq 1$, e il campo $\mathbb{K}$ è algebricamente chiuso e quindi infinito, perciò $\operatorname{Sing}(Z(F_i^{m_i})) = Z(F_i^{m_i})$ è un insieme infinito. Ne segue che $|\operatorname{Sing}(Z(F_i^{m_i}))| = \infty$.
$\Rightarrow$). Supponiamo che $Z_P(F)$ sia una curva ridotta. Sia $F = F_1 \cdots F_r$ la sua scomposizione in componenti irriducibili. Allora per la regola di Leibnitz si ha che

$$\partial_{x_k} F = \sum_{i=1}^{r} F_1 \cdots F_{i-1} (\partial_{x_k} F_i) F_{i+1} \cdots F_r, \qquad k = 0, 1, 2. \tag{5.5}$$

Questo implica la seguente scomposizione

$$\operatorname{Sing}(Z_P(F)) = \bigcup_{i=1}^{r} Z_P(F_i) \cup \bigcup_{1 \leq i < j \leq r} (Z_P(F_i) \cap Z_P(F_j)). \tag{5.6}$$

Si ha che $|\mathrm{Sing}(Z_P(F_i) \cap Z_P(F_j))| < \infty$ per la proposizione 6.17 che vedremo nella prossima unità grazie ai risultanti di Sylvester. Ne segue che $|\mathrm{Sing}(Z_P(F))| < \infty$ se e solo se $|Z_P(F_i)| < \infty$ per ogni $i = 1, \ldots, r$. In altre parole, per dimostrare l'enunciato è sufficiente dimostrarlo per curve irriducibili ridotte, i.e. per curve $Z_P(F)$ integrali, e quindi per polinomi F irriducibili.

Sia F irriducibile. Il luogo singolare $\mathrm{Sing}(Z_P(F))$ è determinato dall'intersezione del luogo degli zeri di F e delle sue derivate parziali. Si noti che le tre derivate possono essere nulle. Se F ha grado zero è una costante e non ci sono punti singolari. Assumendo F di grado positivo, si distinguono tre casi distinti:

1. Due derivate parziali si annullano. Senza perdita di generalità possiamo assumere che $\partial_0 F \not\equiv 0$, mentre $\partial_1 F \equiv \partial_2 F \equiv 0$. Dunque $F(x_0, x_1, x_2) = F(x_0) = c \cdot x_0^d$ per qualche costante $c \in \mathbb{K}^\times$. Per ipotesi F irriducibile quindi $d = 1$, ovvero $Z_P(F)$ è una retta per cui $|\mathrm{Sing}(Z_P(F))| = |\emptyset| = 0 < \infty$.
2. Una derivata parziale si annulla. Senza perdita di generalità possiamo assumere che $\partial_0 F, \partial_1 F \not\equiv 0$, mentre $\partial_2 F \equiv 0$. Dunque $F(x_0, x_1, x_2) = F(x_0, x_1)$, e per ipotesi il campo è algebricamente chiuso dunque il polinomio spezza in fattori lineari di molteplicità uno $F(x_0, x_1) = \prod_{i=1}^{d} (\lambda_i x_0 - \mu_i x_1)$ per costanti $\lambda_i, \mu_i \in \mathbb{K}$ non entrambe nulle, $i = 1, \ldots, d$, e fattori distinti. Per ipotesi F irriducibile quindi $d = 1$, ovvero $Z_P(F)$ è di nuovo una retta per cui $|\mathrm{Sing}(Z_P(F))| = |\emptyset| = 0 < \infty$.
3. Nessuna derivata parziale si annulla. Si noti che le derivate parziali potrebbero condividere componenti irriducibili comuni. Si distinguono quindi tre sottocasi:
   a) Tutte e tre le derivate parziali hanno un fattore irriducibile in comune. Allora
   $$\partial_k F = H \cdot H_k, \quad k = 0, 1, 2, \quad \exists H \in \mathbb{K}[x_0, x_1, x_2]_{d \geq e > 0}$$
   E' sufficiente utilizzare la relazione di Eulero per raggiungere una contraddizione. Infatti:
   $$d \cdot F = \sum_{k=0}^{2} x_k \partial_k F = H \cdot \left(\sum_{k=0}^{2} x_k H_k \right),$$
   contraddicendo l'ipotesi di irriducibilità.
   b) Due derivate parziali hanno un fattore irriducibile in comune. Allora senza perdita di generalità possiamo assumere
   $$\partial_k F = H \cdot H_k, \quad k = 0, 1, \quad \exists H \in \mathbb{K}[x_0, x_1, x_2]_{d \geq e > 0}$$

Allora

$$\mathrm{Sing}(Z_P(F)) = (Z_P(H) \cap Z_P(\partial_2 F)) \cup (Z_P(H_0) \cap Z_P(H_1) \cap Z_P(\partial_2 F)) =: T_1 \cup T_2$$

Ancora una volta per la proposizione 6.17, sia T_1 and T_2 sono insiemi finiti, da cui la tesi.

c) Rimane il caso in cui le derivate parziali a due a due non hanno componenti irriducibili in comune, dunque

$$\mathrm{Sing}(Z_P(F)) := Z_P(F) \cap Z_P(\partial_0 F) \cap Z_P(\partial_1 F) \cap Z_P(\partial_2 F) \subseteq Z_P(\partial_0 F) \cap Z_P(\partial_1 F).$$

Sempre per la proposizione 6.17 il termine di destra ha cardinalità finita. Questo conclude la dimostrazione.

□

5.4 Esercizi

1. Si dimostri che nel caso affine un punto $Q \in Z(f) \subseteq \mathbb{A}^2_{\mathbb{C}}$ è singolare se e solo se $j_0(Q)$ è singolare per $Z_P(hf) \subset \mathbb{P}^2_{\mathbb{C}}$.
2. Si consideri la curva affine di equazione

$$x^5 - x^2 + x - 1 - y(x^4 - 2x^2 - x + 1) = 0\,.$$

Si determini un'equazione della sua chiusura proiettiva e le coordinate di eventuali punti singolari.

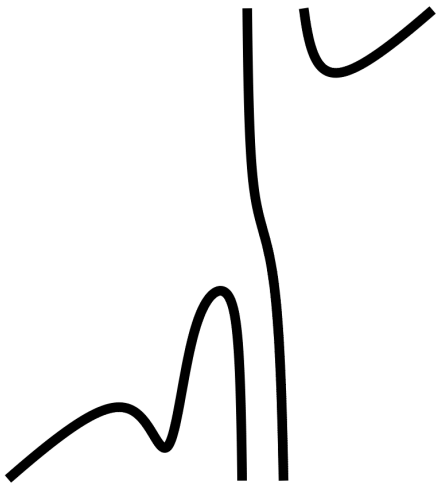


Figura 5.1: Luogo degli zeri reali del polinomio $x^5 - x^2 + x - 1 - y(x^4 - 2x^2 - x + 1)$.

6 Il risultante di Sylvester

Vogliamo ora capire come determinare punti di intersezione tra due curve algebriche, e generalizzare la nozione di molteplicità di intersezione in punto, vista nel caso retta-curva, al caso curva-curva. Vedremo che sotto opportune ipotesi riusciremo a ricondurci al problema delle radici comuni tra due polinomi f e g in una indeterminata.

Vediamo intanto dei risultati preliminari.

6.1 Lemma di Bézout

Supponiamo che $f, g \in A[t]$ abbiano un fattore comune h con $\deg(h) \geq 1$, quindi

$$f = h \cdot u\,, \quad g = h \cdot v\,,$$

dove

$$\deg(u) < \deg(f)\,, \quad \deg(v) < \deg(g)\,.$$

Allora vale l'uguaglianza di polinomi

$$f \cdot v = g \cdot u\,,$$

ovvero

$$f \cdot v - g \cdot u = 0\,.$$

Il risultato seguente ci assicura che l'ultima relazione è anche sufficiente affinché due polinomi abbiano un fattore comune.

Lemma 6.1 (Lemma di Bézout)**.** *Sia A un UFD. Due polinomi $f, g \in A[t]$ hanno un fattore comune non costante se e solo se esistono due polinomi $u, v \in A[t]$ con* $\deg(u) < \deg(f)$ *e* $\deg(v) < \deg(g)$ *tali che*

$$f \cdot v - g \cdot u = 0\,. \tag{6.1}$$

Dimostrazione. Essendo A, e quindi anche $A[t]$ per il lemma di Gauss 2.10, un UFD, a meno di permutazioni e moltiplicazione per elementi invertibili abbiamo delle fattorizzazioni uniche del tipo

$$f = f_1^{m_1} \cdots f_r^{m_r}\,, \quad v = v_1^{h_1} \cdots v_s^{h_s}\,, \quad g = g_1^{n_1} \cdots g_k^{n_k}\,, \quad u = u_1^{p_1} \cdots u_l^{p_l}\,,$$

dove i fattori f_i, v_j, g_q, u_t sono tutti irriducibili. Per la 6.1 possiamo scrivere

$$f_1^{m_1} \cdots f_r^{m_r} \cdot v_1^{h_1} \cdots v_s^{h_s} = g_1^{n_1} \cdots g_k^{n_k} \cdot u_1^{p_1} \cdots u_l^{p_l}\,.$$

Siccome $\deg(u) < \deg(f)$, i fattori irriducibili di u non possono esaurire tutti i fattori di f, quindi esiste almeno un fattore irriducibile g_q che divide f. □

Vediamo ora con un esempio come possiamo utilizzare computazionalmente il Lemma di Bézout per cercare eventuali fattori comuni di due due polinomi.

Esempio 6.2. Sia D un UFD e dominio di integrità tale che $D \supseteq \mathbb{Q}$. Consideriamo un generico polinomio $f \in D[t]$ di grado 3:

$$f(t) = a_3 t^3 + a_2 t^2 + a_1 t + a_0\,, \quad a_3 \neq 0\,,$$

e sia $g \in D[t]$ di grado 2:

$$g(t) = b_2 t^2 + b_1 t + b_0\,, \quad b_2 \neq 0\,.$$

Ci chiediamo quando esistono due polinomi u di grado $\deg(u) < \deg(f) = 3$ e v di grado $\deg(v) < 2$ tali che valga (6.1). Cerchiamo quindi dei coefficienti $\alpha, \beta, \gamma, \delta, \epsilon$ con

$$u(t) = \gamma t^2 + \delta t + \epsilon\,, \quad v(t) = \alpha t + \beta\,,$$

che verifichino

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

Sviluppando i prodotti otteniamo un polinomio di quarto grado, che deve essere nullo; ciò succede se e solo se tutti i suoi coefficienti sono nulli. Otteniamo così le seguenti 5 equazioni:

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

Si tratta di un sistema lineare omogeneo di 5 equazioni delle 5 indeterminate $\alpha, \beta, \gamma, \delta, \epsilon$. Dalla teoria dei sistemi lineari omogenei sappiamo che tale sistema ammette soluzioni $(\alpha, \beta, \gamma, \delta, \epsilon) \neq (0,0,0,0,0)$ non nulle se e solo se il determinante della matrice dei coefficienti è nullo, quindi

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

Questa condizione è equivalente all'annullamento del determinante della matrice trasposta della matrice dei coefficienti, in cui moltiplichiamo le righe relative ai b_i per (-1):

$$\det \begin{pmatrix} a_3 & a_2 & a_1 & a_0 & 0 \\ 0 & a_3 & a_2 & a_1 & a_0 \\ b_2 & b_1 & b_0 & 0 & 0 \\ 0 & b_2 & b_1 & b_0 & 0 \\ 0 & 0 & b_2 & b_1 & b_0 \end{pmatrix} = 0\,. \tag{6.2}$$

Per gradi arbitrari vale un risultato perfettamente analogo. La matrice (6.2) è, in generale, del tipo seguente.

Definizione 6.3. Dati due polinomi $f, g \in D[t]$:

$$f = a_n t^n + \cdots + a_1 t + a_0\,,$$
$$g = b_m t^m + \cdots + b_1 t + b_0\,,$$

la *matrice di Sylvester* $\mathrm{Syl}(f,g)$ di f e g è la seguente matrice quadrata di tipo $(n+$

$m) \times (n+m)$:

$$\left(\begin{array}{cccccccccc}
a_n & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 & 0 & 0 & \cdots & 0 \\
0 & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 & 0 & \cdots & 0 \\
0 & 0 & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 & 0 \\
0 & 0 & 0 & \cdots & 0 & a_n & a_{n-1} & a_{n-2} & \cdots & a_0 \\
\hline
b_m & b_{m-1} & b_{m-2} & \cdots & b_0 & 0 & 0 & 0 & \cdots & 0 \\
0 & b_m & b_{m-1} & b_{m-2} & \cdots & b_0 & 0 & 0 & \cdots & 0 \\
0 & 0 & b_m & b_{m-1} & b_{m-2} & \cdots & b_0 & 0 & \cdots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & \cdots & 0 & b_m & b_{m-1} & b_{m-2} & \cdots & b_0 & 0 \\
0 & 0 & 0 & \cdots & 0 & b_m & b_{m-1} & b_{m-2} & \cdots & b_0
\end{array}\right).$$

Il suo determinante si dice *risultante di Sylvester* $R(f,g)$ *di* f *e* g.

Teorema 6.4. *Sia D un dominio d'integrità e UFD, e siano $f, g \in D[t]$ due polinomi non nulli; allora f e g hanno un fattore comune se e solo se*

$$R(f,g) = 0\,.$$

Osservazione 6.5. Notiamo che le soluzioni non nulle del sistema lineare omogeneo corrispondono sempre a polinomi v e u che sono *entrambi* non nulli; infatti, se per assurdo si avesse $v = 0$ e $u \neq 0$, dalla $f \cdot v = g \cdot u$ si otterrebbe $g \cdot u = 0$; essendo D un dominio di integrità, anche $D[t]$ è dominio di integrità, quindi si avrebbe $g = 0$.

Proposizione 6.6. *Sia $\mathbb{K} = \overline{\mathbb{K}}$ un campo algebricamente chiuso e siano $f, g \in \mathbb{K}[t]$. Allora $R(f,g) = 0$ se e solo se f e g hanno una radice comune.*

Dimostrazione. Ricordiamo che ogni campo è un dominio d'integrità e UFD, quindi si applica il teorema precendente. Se $R(f,g) = 0$, i polinomi f e g hanno almeno un fattore irriducibile comune; ma su un campo algebricamente chiuso, gli unici polinomi irriducibili sono i polinomi lineari, quindi f e g hanno una radice comune. Viceversa, se f e g hanno una radice comune α, il polinomio $(t-\alpha)$ divide entrambi, quindi hanno un fattore comune, e $R(f,g) = 0$. □

6.2 Discriminante

Vedremo ora che, nel caso particolare in cui $g(t)$ sia il polinomio derivato di $f(t)$, il risultante ci fornisce una generalizzazione della nota nozione di *discriminante* di un polinomio di secondo grado.

Proposizione 6.7. *Sia D un dominio d'integrità e UFD. Sia $f \in D[t]$ e sia $\alpha \in D$. Allora:*

$$\alpha \text{ è radice multipla per } f \iff \alpha \text{ è radice di } f \text{ e } f'$$

Dimostrazione. Sia α una radice di f:

$$f(\alpha) = 0.$$

Se $m \geq 1$ è la molteplicità algebrica di α, per il Teorema di Ruffini possiamo scrivere

$$f(t) = (t-\alpha)^m \cdot h(t),$$

dove $h(\alpha) \neq 0$. Per la regola di Leibnitz si ha:

$$f'(t) = m(t-\alpha)^{m-1} \cdot h(t) + (t-\alpha)^m \cdot h'(t).$$

In particolare, osserviamo che

$$m \geq 2 \iff f'(t) = (t-\alpha)^{m-1} \cdot (m\, h(t) + (t-\alpha) \cdot h'(t)),$$

con $(t-\alpha)^{m-1}$ di grado $m-1 \geq 1$, quindi se e solo se $(t-\alpha)$ divide $f'(t)$. □

Definizione 6.8. Dato $f \in D[t]$, il suo *discriminante* $\Delta(f)$ è per definizione il risultante di Sylvester di f ed f':

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

Dalla Proposizione 6.7 otteniamo immediatamente il seguente corollario.

Corollario 6.9. *Un polinomio $f \in D[t]$ ha una radice multipla se e solo se $\Delta(f) = 0$.*

Esempio 6.10 (Discriminante per polinomi di secondo grado)**.** Consideriamo f un generico polinomio di secondo grado in $D[t]$ e il suo polinomio derivato f':

$$f(x) = ax^2 + bx + c$$
$$f'(x) = 2ax + b$$

Possiamo considerare il risultante di f e f':

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

Siccome stiamo supponendo f di secondo grado, abbiamo $a \neq 0$. Quindi otteniamo:

$$R(f,f') = 0 \iff b^2 - 4ac = 0\,.$$

Cioè ritroviamo il classico risultato che f ha una radice doppia se e solo se $\Delta(f) = 0$, dove $\Delta(f) = b^2 - 4ac$.

Esempio 6.11 (Discriminante per polinomi di terzo grado)**.** Consideriamo un generico polinomio monico $f \in D[t]$

$$f = t^3 + a_1t^2 + a_2t + a_3\,.$$

Osserviamo che, con un cambio variabile, esso può essere ricondotto alla forma di *Tschirnhaus*:

$$f = x^3 + ax + b\,.$$

Infatti, con l'affinità $t \mapsto t - \frac{a_1}{3}$ si riesce a eliminare il termine a_1. Consideriamo la sua derivata:

$$f' = 3x^2 + a$$

Quindi il risultante sarà della forma

$$R(f,f') = \det \begin{pmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{pmatrix}$$
$$= b(b(-27)) + a((-a)9a - a(-3a)) - a(-2a)$$
$$= -(4a^3 + 27b^2)\,.$$

6.3 Risultante di polinomi in più indeterminate

Possiamo generalizzare le nozioni viste al caso di polinomi $f, g \in \mathbb{K}[x_1, \ldots, x_n]$, quindi pensando $D = \mathbb{K}[x_1, \ldots, x_{n-1}]$ e $f, g \in D[x_n]$. In questo caso scriviamo:

$$F = A_r x_n^r + A_{r-1} x_n^{r-1} + \cdots + A_1 x_n + A_0\,,$$
$$G = B_s x_n^s + B_{s-1} x_n^{s-1} + \cdots + B_1 x_n + B_0\,,$$

con $A_i, B_j \in \mathbb{K}[x_1, \cdots, x_{n-1}]$, e $\deg_{x_n}(f) = r$ e $deg_{x_n}(f) = s$.

Definizione 6.12. Il *risultante di f e g rispetto a x_n* è il polinomio $R_n := R_{x_n}(f, g) \in \mathbb{K}[x_1, \ldots, x_{n-1}]$, dato da:

$$R_n(f,g) = \det \left(\begin{array}{ccccccccccc} A_r & A_{r-1} & A_{r-2} & \cdots & A_0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & A_r & A_{r-1} & A_{r-2} & \cdots & A_0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & A_r & A_{r-1} & A_{r-2} & \cdots & A_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & A_r & A_{r-1} & A_{r-2} & \cdots & A_0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & A_r & A_{r-1} & A_{r-2} & \cdots & A_0 \\ \hline B_s & B_{s-1} & B_{s-2} & \cdots & B_0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & B_s & B_{s-1} & B_{s-2} & \cdots & B_0 & 0 & 0 & \cdots & 0 \\ 0 & 0 & B_s & B_{s-1} & B_{s-2} & \cdots & B_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & B_s & B_{s-1} & B_{s-2} & \cdots & B_0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & B_s & B_{s-1} & B_{s-2} & \cdots & B_0 \end{array}\right)$$

Passiamo ora al caso $f, g \in \mathbb{K}[x, y]$ e vediamo che proprietà geometriche possiamo dedurre dal valore del risultante.

Osservazione 6.13. Per il risultante $R_y(f, g) = R(x)$ rispetto a y abbiamo i seguenti casi:

1. $R(x) = 0$ è il polinomio nullo: per i risultati visti, $f(x, y)$ e $g(x, y)$ hanno un fattore comune $h(x, y)$, di grado non nullo nella y, quindi le curve $Z(f)$ e $Z(g)$ hanno una componente comune $Z(h)$;
2. $R(x) = c \neq 0$ è una costante non nulla: per ogni $\overline{x} \in \mathbb{K}$, i polinomi $f(\overline{x}, y)$ e $g(\overline{x}, y)$ non hanno fattori comuni, e quindi nemmeno radici comuni, quindi $Z(f) \cap Z(f) = \emptyset$;

3. $R(x)$ è un polinomio non nullo di grado ≥ 1 in x: se $R(x)$ ha radici nel campo, sia $\overline{x}$ una radice; quindi $R(\overline{x}) = 0$, da cui se $f(\overline{x}, y)$ e $g(\overline{x}, y)$ sono entrambi polinomi non costanti, hanno un fattore comune, che risulta un polinomio non costante in y. Se tale polinomio ha una radice $\overline{y}$, allora otteniamo

$$f(\overline{x}, \overline{y}) = 0 = g(\overline{x}, \overline{y}),$$

cioè $(\overline{x}, \overline{y}) \in Z(f) \cap Z(g)$.

In questo caso, inoltre, vediamo che $Z(f) \cap Z(g)$ consiste al più di un numero finito di punti.

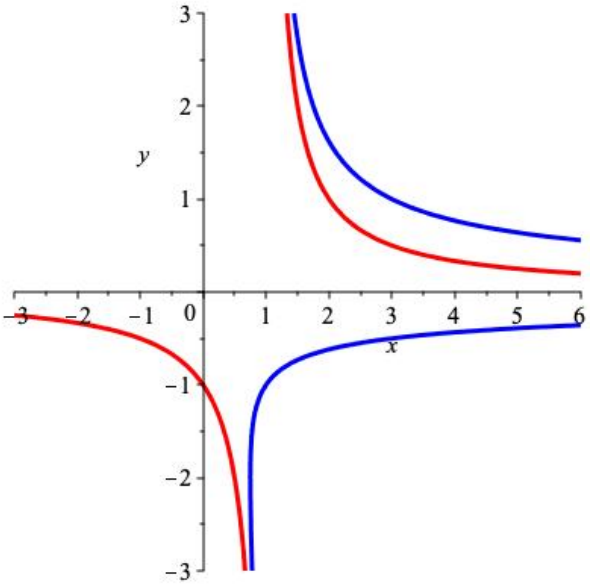
Esempio 6.14. Notiamo che anche se $R(x)$ è un polinomio non nullo di grado ≥ 1 in x, le curve $Z(f)$ e $Z(g)$ potrebbero non avere punti di intersezione, ciò succede, ad esempio, per i polinomi

$$f(x, y) = (1 - x)y^2 + y + 1, \quad g(x, y) = (1 - x)y + 1.$$

Abbiamo:

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

L'unica radice di $R(x)$ è 1; se valutiamo $f(1, y) = y + 1$, $g(1, y) = 1$, quindi non ci sono zeri comuni e le due curve affini non si intersecano.



6.4 Risultante di polinomi omogenei

Proposizione 6.15. *Siano $F \in \mathbb{K}[x_0, x_1, \dots, x_n]_r$ e $G \in \mathbb{K}[x_0, x_1, \dots, x_n]_s$ due polinomi omogenei non costanti, con $\deg_{x_n}(F) = r$ e $\deg_{x_n}(G) = s$. Allora una delle due è verificata:*

- *$R_{x_n}(F, G) = 0$ è il polinomio nullo, oppure*
- *$R_{x_n}(F, G)$ è un polinomio omogeneo di grado rs.*

Dimostrazione. Per semplicità consideriamo il caso $n = 2$; il caso generale è analogo. In questo caso scriviamo:

$$F = A_r x_2^r + A_{r-1} x_2^{r-1} + \cdots + A_1 x_2 + A_0, \quad G = B_s x_2^s + B_{s-1} x_2^{s-1} + \cdots + B_1 x_2 + B_0,$$

con $A_i \in \mathbb{K}[x_0, x_1]_{r-i}$ e $B_j \in \mathbb{K}[x_0, x_1]_{s-j}$ polinomi omogenei; siccome $\deg_{x_2}(F) = r$ e $\deg_{x_2}(G) = s$, i due coefficienti A_r e B_s sono due costanti non nulle. Supponiamo che $R_{x_2}(F, G) \neq 0$.

Per dimostrare l'omogeneità utilizziamo il criterio del Lemma 2.20, poniamo

$$R(x_0, x_1) := R_{x_2}(F, G)$$

e determiniamo $R(tx_0, tx_1)$. Useremo un trucco basato sulla multilinearità del determinante: consideriamo la matrice di Sylvester di F e G valutata in tx_0 e tx_1 e moltiplichiamo ogni riga i esima per t^i, per ogni $1 \leq i \leq s$; poi ogni riga $s + j$-esima è moltiplicata per t^j per ogni $1 \leq j \leq r$.

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

Per la multilinearità del determinante sulle righe, il determinante

$$\delta = \det\left(M(F,G)(tx_0,tx_1) \cdot^t (\cdot t, \cdot t^2, \cdots, \cdot t^s, \cdot t, \cdot t^2, \cdots, \cdot t^r)\right)$$

della matrice che stiamo considerando è uguale a

$$\delta = t^{\frac{s(s+1)}{2}} \cdot t^{\frac{r(r+1)}{2}} \cdot R(tx_0, tx_1);$$

Usando ora l'omogeneità dei coefficienti A_i e B_j possiamo scrivere $A_i(tx_0, tx_1) = t^{r-i} A_i(x_0, x_1)$ e $B_j(tx_0, tx_1) = t^{s-j} B_j(x_0, x_1)$, e svolgendo i prodotti troviamo la matri-

ce

$$\begin{pmatrix} tA_r & t^2A_{r-1} & \cdots & t^{r+1}A_0 & 0 & 0 & 0 & \cdots & 0 \\ 0 & t^2A_r & t^3A_{r-1} & \cdots & t^{r+2}A_0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & t^sA_r & t^{s+1}A_{r-1} & t^{s+2}A_{r-2} & \cdots & t^{r+s}A_0 \\ tB_s & t^2B_{s-1} & \cdots & \cdots & 0 & 0 & 0 & \cdots & 0 \\ 0 & t^2B_s & t^3B_{s-1} & \cdots & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 0 & 0 & t^rB_s & \cdots & t^{r+s}B_0 \end{pmatrix}$$

Osserviamo che anche le colonne risultano multipli di opportune potenze di t, da cui troviamo

$$\delta = t^{\frac{(r+s)(r+s+1)}{2}} \cdot R(x_0, x_1)\,,$$

e semplificando otteniamo

$$R(tx_0, tx_1) = t^{rs}R(x_0, x_1)\,.$$

□

Osservazione 6.16. Le condizioni $\deg_{x_2}(F) = r$ e $\deg_{x_2}(G) = s$ corrispondono a $A_r \neq 0$ e $B_s \neq 0$; osservando che

$$A_r = F(0,0,1)\,, \quad B_s = G(0,0,1)\,,$$

tali condizioni corrispondono geometricamente alle richieste

$$(0:0:1) \notin Z_P(F) \quad \text{e} \quad (0:0:1) \notin Z_P(G)\,.$$

Proposizione 6.17. *Siano $F \in \mathbb{K}[x_0, x_1, \ldots, x_n]_r$ e $G \in \mathbb{K}[x_0, x_1, \ldots, x_n]_s$ due polinomi omogenei non costanti, con $\deg_{x_n}(F) = r \geq 1$ e $\deg_{x_n}(G) = s \geq 1$, e supponiamo che F e G non abbiano componenti comuni. Allora $Z_P(F) \cap Z_P(G)$ è costituito da un numero finito di punti.*

Dimostrazione. Per l'ipotesi che F e G non abbiano componenti comuni, possiamo affermare che $R_{x_2}(F, G) = R(x_0, x_1)$ è un polinomio non nullo.

Osserviamo ora che se un punto $(c_0 : c_1 : c_2) \in Z_P(F) \cap Z_P(G)$, allora $(c_0 : c_1)$ è una radice di $R(x_0, x_1)$. Infatti, se $(c_0 : c_1 : c_2) \in Z_P(F) \cap Z_P(G)$, i polinomi $F(c_0, c_1, x_2)$ e $G(c_0, c_1, x_2)$ hanno c_2 come radice comune, quindi il risultante valutato in $(c_0 : c_1)$ è nullo; inoltre, siccome $(0:0:1) \notin Z_P(F)$ e $(0:0:1) \notin Z_P(G)$, si ha $(c_0 : c_1) \neq (0:0)$.

Infine, essendo $R(x_0, x_1)$ un polinomio non nullo, ha al più un numero finito di radici. Infine, per ogni radice $(c_0 : c_1)$ di $R(x_0, x_1)$ abbiamo al più un numero finito di scalari c_2 tali che $(c_0 : c_1 : c_2) \in Z_P(F) \cap Z_P(G)$; se così non fosse, i polinomi $F(c_0, c_1, x_2)$ e $G(c_0, c_1, x_2)$ avrebbero infinite radici in comune, quindi sarebbero entrambi identicamente nulli, cioè l'indeterminata x_2 non sarebbe presente né in F né in G, contraddicendo l'ipotesi $\deg_{x_2}(F) = r \geq 1$ e $\deg_{x_2}(G) = s \geq 1$. □

Corollario 6.18 (Lemma di Study)**.** *Siano $F \in \mathbb{K}[x_0, x_1, x_2]_r$ e $G \in \mathbb{K}[x_0, x_1, x_2]_s$ due polinomi omogenei non costanti, e supponiamo che $Z_P(F) \cap Z_P(G)$ contenga infiniti punti. Allora F e G hanno un fattore non costante comune.*

In particolare, se G è irriducibile e $Z_P(F) \cap Z_P(G)$ contiene infiniti punti, allora G divide F.

7 Teorema di Bézout

Possiamo ora affrontare il problema di determinare il numero di intersezioni tra due curve algebriche. Come nel caso retta-curva, vedremo che nel proiettivo è possibile dare una formula esatta per il numero totale di intersezioni, contate con delle opportune molteplicità.

Iniziamo con la seguente definizione.

Definizione 7.1. Siano $F \in \mathbb{K}[x_0, x_1, x_2]_r$ e $G \in \mathbb{K}[x_0, x_1, x_2]_s$ due polinomi omogenei non costanti e senza fattori comuni. Diremo che $Z_P(F) \subset \mathbb{P}^2$ e $Z_P(G) \subset \mathbb{P}^2$ sono in *posizione ammissibile rispetto a* $E_2 = (0 : 0 : 1)$ se valgono le seguenti:

- $E_2 \notin Z_P(F)$ e $E_2 \notin Z_P(G)$ (equivalentemente $\deg_{x_2}(F) = r$ e $\deg_{x_2}(G) = s$);
- per ogni coppia di punti $Q_1, Q_2 \in Z_P(F) \cap Z_P(G)$, la retta $\overline{Q_1Q_2} \not\ni E_2$ (equivalentemente, l'equazione di $\overline{Q_1Q_2}$ contiene l'indeterminata x_2).

Proposizione 7.2. *Sia* $\mathbb{K} = \overline{\mathbb{K}}$ *un campo algebricamente chiuso. Siano* $F \in \mathbb{K}[x_0, x_1, x_2]_r$ *e* $G \in \mathbb{K}[x_0, x_1, x_2]_s$ *due polinomi omogenei non costanti e senza fattori comuni, tali che* $Z_P(F) \subset \mathbb{P}^2$ *e* $Z_P(G) \subset \mathbb{P}^2$ *sono in posizione ammissibile rispetto a* $E_2 = (0 : 0 : 1)$. *Allora c'è una biiezione tra i punti di* $Z_P(F) \cap Z_P(G)$ *e le radici del risultante* $R_{x_2}(F, G) = R(x_0, x_1)$*:*

$$\{Q \mid Q \in Z_P(F) \cap Z_P(G)\} \longleftrightarrow \{(q_0 : q_1) \mid R(q_0, q_1) = 0\}\,.$$

Dimostrazione. Siccome F e G non hanno fattori comuni, il risultante $R_{x_2}(F, G) = R(x_0, x_1)$ è un polinomio non nullo, omogeneo di grado rs.

Abbiamo visto nella sezione precedente che se $Q = (q_0 : q_1 : q_2) \in Z_P(F) \cap Z_P(G)$, allora $(q_0 : q_1)$ è radice di $R(x_0, x_1)$. Questa mappa è iniettiva; infatti, se $Q, Q' \in Z_P(F) \cap Z_P(G)$, con $Q = (q_0 : q_1 : q_2)$ e $Q' = (q_0' : q_1' : q_2')$ verificassero $(q_0 : q_1) = (q_0' : q_1')$, i due punti giacerebbero sulla retta di equazione

$$q_1x_0 - q_0x_1 = 0\,.$$

Tale retta passa per E_2, quindi questo contraddice l'ipotesi che le due curve siano in posizione ammissibile rispetto a E_2.

Infine, la mappa è suriettiva: se $R(q_0, q_1) = 0$, allora $F(q_0, q_1, x_2)$ e $G(q_0, q_1, x_2)$ ammettono una radice comune q_2, quindi il punto $(q_0 : q_1 : q_2) \in Z_P(F) \cap Z_P(G)$. □

7.1 Teoremi di Bézout

Teorema 7.3 (Forma debole del Teorema di Bézout)**.** *Sia* $\mathbb{K}$ *un campo algebricamente chiuso. Siano* $F, G \in K[x_0, x_1, x_2]$ *omogenei di gradi* r, s *rispettivamente. Se* $Z_P(F) \cap Z_P(G)$ *contiene* $rs + 1$ *punti, allora* F *e* G *hanno un fattore irriducibile comune.*

Dimostrazione. Supponiamo per assurdo che $Z_P(F)$ e $Z_P(G)$ siano senza componenti comuni. Osserviamo che, a meno di proiettività di $\mathbb{P}^2_{\mathbb{K}}$, possiamo supporre che $Z_P(F)$ e $Z_P(G)$ siano in posizione ammissibile rispetto a E_2. Infatti, se non lo sono, possiamo scegliere un punto che non stia né su $Z_P(F)$, né su $Z_P(G)$, né su alcuna retta congiungente coppie di punti nell'intersezione delle due curve (esercizio). Per la Proposizione 6.17, il numero di tali rette è finito.

Per la Proposizione 7.2, c'è una biiezione tra i punti di $Z_P(F) \cap Z_P(G)$ e le radici di $R(x_0, x_1)$; queste ultime sono al più rs, quindi troviamo un assurdo. □

7.1.1 Molteplicità di intersezione curva-curva

La Proposizione 7.2 ci permette anche di dare la definizione di molteplicità di intersezione tra due curve in un punto; infatti, se due curve sono in posizione ammissibile rispetto a E_2, a ogni punto di intersezione possiamo associare la molteplicità algebrica della corrispondente radice del risultante.

Definizione 7.4. Sia $\mathbb{K} = \overline{\mathbb{K}}$ un campo algebricamente chiuso. Siano $F \in \mathbb{K}[x_0, x_1, x_2]_r$ e $G \in \mathbb{K}[x_0, x_1, x_2]_s$ due polinomi omogenei non costanti e senza fattori comuni, tali che $Z_P(F) \subset \mathbb{P}^2$ e $Z_P(G) \subset \mathbb{P}^2$ sono in posizione ammissibile rispetto a $E_2 = (0 : 0 : 1)$, e sia $Q = (q_0 : q_1 : q_2) \in Z_P(F) \cap Z_P(G)$. La *molteplicità di intersezione* $I_Q(F, G)$ *tra* $Z_P(F)$ *e* $Z_P(G)$ *in* Q è la molteplicità algebrica della radice $(q_0 : q_1)$ di $R_{x_2}(F, G)$:

$$I_Q(F, G) = m, \quad \text{dove} \quad R_{x_2}(F, G) = (c_1 x_0 - c_0 x_1)^m \cdot H(x_0, x_1), \quad H(c_0, c_1) \neq 0\,.$$

Osservazione 7.5. È possibile dimostrare, usando tecniche locali di algebra commutativa, che la definizione è ben posta, e non dipende dalla scelta delle coordinate.

Teorema 7.6 (Forma forte del teorema di Bézout per curve algebriche)**.** *Sia* $\mathbb{K} = \overline{\mathbb{K}}$ *un campo algebricamente chiuso. Siano* $F, G \in K[x_0, x_1, x_2]$ *omogenei di gradi* r, s *rispettivamente e senza fattori comuni. Allora si ha*

$$\sum_{Q \in Z(F) \cap Z(G)} I_Q(F, G) = rs\,.$$

Dimostrazione. Come già osservato, a meno di proiettività possiamo supporre che $Z_P(F)$ e $Z_P(G)$ siano in posizione ammissibile.

L'enunciato segue immediatamente dal fatto che $R_{x_2}(F, G)$ è omogeneo di grado di rs, dalla Proposizione 7.2 e dalla definizione di molteplicità di intersezione. □

Come conseguenza otteniamo il seguente risultato, generalizzazione del fatto che due rette proiettive sullo stesso piano si intersecano sempre.

Corollario 7.7. *Su un campo algebricamente chiuso* $\mathbb{K} = \overline{\mathbb{K}}$*, due curve nello stesso piano proiettivo si intersecano.*

Finiamo questa sezione con una stima sulla molteplicità di intersezione in punti singolari.

Proposizione 7.8. *Siano* $Z_P(F) \subset \mathbb{P}^2$ *e* $Z_P(G) \subset \mathbb{P}^2$ *due curve piane senza componenti comuni, e sia* $Q \in Z_P(F) \cap Z_P(G)$ *un punto di molteplicità* m *per* $Z_P(F)$ *e di molteplicità* n *per* $Z_P(G)$*. Allora si ha*

$$I_Q(F, G) \geq mn\,.$$

Dimostrazione. A meno di proiettività, possiamo supporre che le due curve siano in posizione ammissibile rispetto a E_2 e che si abbia

$$Q = (1 : 0 : 0) \in U_0 \cong \mathbb{A}^2\,;$$

le molteplicità dei punti e le molteplicità di intersezione, infatti, sono mantenute per proiettività.

Possiamo quindi restringerci a $U_0 \cong \mathbb{A}^2$ e lavorare nell'affine; ricordiamo che $Z_P(F) \cap U_0$ e $Z_P(G) \cap U_0$ corrispondono alle curve affine determinate dalle equazioni deomogeneizzate. Scriviamo

$$aF = f(x,y) = f_r(x)y^r + f_{r-1}y^{r-1} + \cdots + f_1(x) + f_0(x)\,, \tag{7.1}$$

$$aG = g(x,y) = g_s(x)y^s + g_{s-1}y^{s-1} + \cdots + g_1(x)y + g_0(x)\,. \tag{7.2}$$

Le coordinate affini di Q sono $(0,0)$, quindi è l'origine; ricordiamo che la molteplicità dell'origine è m per una curva affine, se e solo se la sua equazione non contiene monomi di grado $\geq m-1$ e ne contiene almeno uno di grado m. Affinché ciò sia verificato dal polinomio (7.1), si deve avere

$$x^m \mid f_0(x),\ x^{m-1} \mid f_1(x),\ \ldots\ x \mid f_{m-1}(x)\,,$$

quindi possiamo scrivere

$$f_0(x) = x^m a_0(x),\ f_1(x) = x^{m-1}a_1(x),\ \ldots\ f_{m-1}(x) = xa_{m-1}(x)\,.$$

Analogamente, l'origine $(0,0)$ ha molteplicità n per $Z(g)$ se e solo se

$$x^n \mid g_0(x),\ x^{n-1} \mid g_1(x),\ \ldots\ x \mid g_{n-1}(x)\,,$$

quindi possiamo scrivere

$$g_0(x) = x^n b_0(x),\ g_1(x) = x^{n-1}b_1(x),\ \ldots\ f_{n-1}(x) = xb_{n-1}(x)\,.$$

La matrice di Sylvester di f e g avrà quindi la forma

$$\begin{pmatrix}
f_r(x) & f_{r-1}(x) & \cdots & x^{m-1}a_1(x) & x^m a_0(x) & 0 & \cdots & 0 \\
0 & f_r(x) & f_{r-1}(x) & \cdots & x^{m-1}a_1(x) & x^m a_0(x) & 0 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
g_s(x) & g_{s-1}(x) & \cdots & x^{n-1}b_1(x) & x^n b_0(x) & 0 & \cdots & 0 \\
0 & g_s(x) & g_{s-1}(x) & \cdots & x^{n-1}b_1(x) & x^n b_0(x) & 0 & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots
\end{pmatrix}.$$

Vogliamo capire la molteplicità della radice $x = 0$ per il risultante.

Usiamo nuovamente il trucco di moltiplicare le righe della matrice per opportune potenze di x, e precisamente: per $i = r-m, \ldots, r$, moltiplichiamo la riga i-esima per x^i; analogamente, per $j = (r+s)-n, \ldots, (r+s)$, moltiplichiamo la riga j-esima per x^j. Sfruttando l'omogeneità del determinante troviamo che x^{mn} divide il risultante. □

7.1.2 Stima sul numero di punti singolari di curve ridotte

Una conseguenza del Teorema di Bézout riguarda la seguente stima sulle singolarità di una curva piana ridotta.

Teorema 7.9. *Sia $Z_P(F)$ una curva ridotta e siano $P_1, \dots, P_s$ i suoi punti singolari, di molteplicità rispettive $m_1, \dots, m_s \geq 2$. Allora si ha*

$$\sum_{i=1}^{s} m_i(m_i - 1) \leq d(d-1)\,. \tag{7.3}$$

In particolare vale $s \leq \frac{d(d-1)}{2}$.

Dimostrazione. Abbiamo visto che le proiettività mantengono tutti i punti singolari e le loro molteplicità. A meno di proiettività possiamo supporre che $Z_P(F)$ sia in posizione ammissibile rispetto a $E_2 = (0:0:1)$. Possiamo quindi scrivere F come

$$F = A_d x_2^d + A_{d-1} x_2^{d-1} + \cdots + A_1 x_2 + A_0,$$

con $A_d \neq 0$. Abbiamo

$$\partial_2 F = d\ A_d x_2^{d-1} + \cdots + A_1,$$

quindi anche $\partial_2 F$ è in posizione ammissibile rispetto a E_2.

Osserviamo ora che F e $\partial_2 F$ non possono avere componenti comuni. Infatti, se per assurdo esistesse H, in cui compare x_2, tale che $F = HF_1$ e $\partial_2 F = HG$, si avrebbe che H^2 divide F ed F non sarebbe ridotto. Infine, se $H = H(x_0, x_1)$, la curva $Z_P(F)$ non sarebbe in posizione ammissibile rispetto a E_2.

Per il Teorema di Bézout si ha

$$\sum_{Q \in Z_P(F) \cap Z_P(\partial_2 F)} I_Q(F, \partial_2 F) \leq d(d-1).$$

Osserviamo ora che se P_i è un punto singolare per $Z_P(F)$ di molteplicità $m_i \geq 2$, cioè annulla tutte le derivate parziali di ordine $\leq m_i - 1$, allora P_i è un punto di molteplicità $m_i - 1$ per $Z_P(\partial_2 F)$ (perché annulla tutte le derivate parziali di ordine $\leq m_i - 2$ di $\partial_2 F$).

Quindi si ha

$$\sum_{i=1}^{s} m_i(m_i-1) \leq \sum_{i=1}^{s} I_{P_i}(F, \partial_2 F) \leq \sum_{Q \in Z_P(F) \cap Z_P(\partial_2 F)} I_Q(F, \partial_2 F),$$

da cui la tesi. □

Osservazione 7.10. La stima è ottimale ed è realizzata, ad esempio, da un'unione di d rette generali, cioè tali che per ogni punto di intersezione passino esattamente due rette. I punti singolari, in questo caso, sono tutti doppi e ce ne sono $\frac{d(d-1)}{2}$.

8 Sistemi lineari di ipersuperfici proiettive

Vorremmo ora studiare famiglie di ipersuperfici proiettive, partendo dalle tipologie più semplici, i sistemi lineari, cioè quelle che corrispondono a opportuni sottospazi proiettivi lineari. Le nozioni che vedremo sono generalizzazioni di fasci e reti di rette, e di fasci e reti di coniche piane.

Iniziamo osservando che una scelta naturale per il ruolo di insieme parametrizzante le ipersuperfici proiettive $(Z_P(F), F)$ di un certo grado $d \geq 1$ è il proiettivizzato dello spazio vettoriale dei polinomi omogenei di grado d:

$$\mathbb{P}(\mathbb{K}[x_0, \ldots, x_n]_d)\,.$$

Infatti, se $(Z_P(F), F)$ è ridotta, dal Lemma di Study otteniamo che $(Z_P(G), G)$ verifica $Z_P(F) = Z_P(G)$ se e solo se i polinomi F e G sono proporzionali. Lo spazio proiettivo $\mathbb{P}(\mathbb{K}[x_0, \ldots, x_n]_d)$ parametrizza, quindi, tutti i supporti di ipersuperfici ridotte, e include anche, in modo naturale, tutte i casi limite di ipersuperfici ridotte, cioè le ipersuperfici con componenti multiple.

Ricordiamo, infine, che la dimensione vettoriale

$$\dim \mathbb{K}[x_0, \ldots, x_n]_d = \binom{n+d}{n}\,,$$

quindi $\dim \mathbb{P}(\mathbb{K}[x_0, \ldots, x_n]_d) = \binom{n+d}{n} - 1 =: N(d, n)$.

In particolare, gli iperpiani proiettivi sono identificati con lo spazio $\mathbb{P}(\mathbb{K}[x_0, \ldots, x_n]_1)$ di dimensione $N(1, n) = n$, e infatti lo spazio delle classi di proporzionalità dei polinomi lineari omogenei è isomorfo allo spazio duale $(\mathbb{P}^n)^\vee$. Lo spazio delle coniche piane si identifica con $\mathbb{P}(\mathbb{K}[x_0, x_1, x_2]_2)$ di dimensione $N(2, 2) = 5$. Infine, lo spazio delle curve proiettive piane ha dimensione

$$N(d, 2) = \frac{(d+2)(d+1)}{2} - 1 = \frac{d(d+3)}{2}\,.$$

8.1 Sistemi lineari: prime definizioni

Definizione 8.1. Un sistema lineare Λ di dimensione $q \geq 0$ di ipersuperfici proiettive di grado $d \geq 1$ è un sottospazio proiettivo $\Lambda \subseteq \mathbb{P}(\mathbb{K}[x_0, \ldots, x_n]_d)$ di dimensione q, quindi il proiettivizzato di un sottospazio vettoriale di $\mathbb{K}[x_0, \ldots, x_n]_d$ di dimensione $q+1$:

$$\Lambda = \mathbb{P}(U)\,, \quad U \subseteq \mathbb{K}[x_0, \ldots, x_n]_d\,, \quad \dim U = q+1 \geq 1\,.$$

Definizione 8.2. Se $q = 0$, allora Λ è un *punto*. Se $q = 1$, allora Λ si dice *fascio* (in inglese *pencil*). Se $q = 2$, allora Λ si dice *rete* (in inglese *net*). Se $q = 3$, allora Λ si dice *tessuto* (in inglese *web*).

Osservazione 8.3. È possibile capire di che tipo sono gli elementi di Λ studiando la posizione di quest'ultimo in $\mathbb{P}(\mathbb{K}[x_0, \ldots, x_n]_d)$ rispetto a certi luoghi geometrici particolari.

Esercizi 1. Consideriamo lo spazio delle coniche piane $\mathbb{P}(\mathbb{K}[x_0, x_1, x_2]_2) = \mathbb{P}^5$. Un luogo speciale è, ad esempio, quello corrispondente alle coniche degeneri.

Ricordiamo che una conica proiettiva piana è riducibile se e solo se la matrice simmetrica associata alla suo polinomio quadratico è degenere, cioè ha determinante nullo. Più precisamente, se l'equazione della conica è

$$F(x_0, x_1, x_2) = a_{00}x_0^2 + 2a_{01}x_0x_1 + a_{11}x_1^2 + 2a_{02}x_0x_2 + a_{11}x_1^2 + 2a_{12}x_1x_2 + a_{22}x_2^2 = 0\,.$$

consideriamo la matrice

$$A = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{01} & a_{11} & a_{12} \\ a_{02} & a_{12} & a_{22} \end{pmatrix}\,.$$

La conica $Z_P(F)$ è degenere se e solo se

$$\det(A) = \sum_{\sigma \in S_3} (-1)^{\mathrm{sgn}(\sigma)} a_{0\sigma(0)}\, a_{1\sigma(1)}\, a_{2\sigma(2)} = 0\,. \tag{8.1}$$

L'ultima espressione è un polinomio omogeneo di terzo grado nelle coordinate omogenee della classe di proporzionalità $[F]$:

$$[F] = (a_{00} : 2a_{01} : 2a_{02} : a_{11} : 2a_{12} : a_{22})\,.$$

Da ciò segue che il luogo $\Sigma \subset \mathbb{P}^5$ corrispondente alle coniche degeneri è una ipersuperficie cubica, di equazione (8.1). Non è difficile verificare, inoltre, che la (8.1), e quindi Σ, è irriducibile.

Consideriamo ora un fascio di coniche $\Lambda \subset \mathbb{P}(\mathbb{K}[x_0, x_1, x_2]_2) = \mathbb{P}^5$, quindi una retta proiettiva. Determinare le coniche degeneri di Λ corrisponde alla determinazione dei punti di intersezione $\Lambda \cap \Sigma$.

In modo analogo al caso delle intersezioni retta - curva in $\mathbb{P}^2$, è possibile verificare che abbiamo due casi:

1. $\Lambda \subset \Sigma$, nel qual caso tutte le coniche del fascio sono degeneri;
2. $\Lambda \not\subset \Sigma$, e si ha
$$\sum_{Q \in \Lambda \cap \Sigma} I_Q(\Lambda, \Sigma) = 3\,.$$
In Λ possiamo avere, quindi, 3 coniche degeneri distinte (fascio generale), 2 coniche degeneri (fascio tangente, fascio bitangente o fascio osculatore), oppure 1 conica degenere (fascio iperosculatore).

Consideriamo ora la seguente questione: come assegnare un sistema lineare Λ? Essendo $\Lambda = \mathbb{P}(U)$ con U sottospazio vettoriale, dall'Algebra Lineare sappiamo che U si può determinare sia assegnando un insieme di generatori, che possiamo supporre linearmente indipendenti, sia con delle equazioni cartesiane.

Se fissiamo U scegliendone dei generatori linearmente indipendenti (quindi una base di U), avremo
$$U = \mathrm{Span}(F_0, \dots, F_q)\,,$$
con $F_i \in \mathbb{K}[x_0, \dots, x_n]_d$, il generico elemento $F \in U$ si scrive in modo unico
$$F = \lambda_0 F_0 + \lambda_1 F_1 + \cdots + \lambda_q F_q\,.$$

Se scegliamo, invece, di determinare $U \subset \mathbb{K}[x_0, \dots, x_n]_d$ con delle equazioni cartesiane, ricordiamo che un sottospazio vettoriale di dimensione $\dim U = q+1$ può sempre essere interpretato con il sottospazio delle soluzioni di un sistema lineare omogeneo di $\dim \mathbb{K}[x_0, \dots, x_n]_d - (q+1) = \binom{n+d}{n} - (q+1)$ equazioni in $\dim \mathbb{K}[x_0, \dots, x_n]_d = \binom{n+d}{n}$ indeterminate.

Infine, per costruzione degli spazi proiettivi, le stesse equazioni determinano $\Lambda = \mathbb{P}(U)$.

8.2 Condizioni lineari sui polinomi

Definizione 8.4. Una equazione lineare omogenea con indeterminate i coefficienti di un generico polinomio omogeneo di $\mathbb{K}[x_0, \dots, x_n]_d$ viene chiamata *condizione lineare* sui polinomi omogenei di grado d.

D'ora in poi useremo la seguente notazione per i coefficienti del generico polinomio $F \in \mathbb{K}[x_0, \dots, x_n]_d$:

$$F(x_0, \dots, x_n) = \sum_{i_0+\cdots+i_n=d} w_{i_0 \dots i_n} x_0^{i_0} \dots x_n^{i_n}.$$

Esercizi 2. Vediamo degli esempi di condizioni lineari:

- **passaggio per un punto**: sia $A = (a_0 : \cdots : a_n) \in \mathbb{P}^n$ un punto arbitrario, e consideriamo tutte le ipersuperfici di grado d passanti per A; la condizione si esprime richiedendo che valga

  $$\sum_{i_0+\cdots+i_n=d} w_{i_0 \dots i_n} a_0^{i_0} \dots a_n^{i_n} = 0.$$

  Questa è una condizione lineare nelle incognite $w_{i_0 \dots i_n}$.

  Infine, il sistema lineare Λ_A delle ipersuperfici di grado d passanti per A ha codimensione 1, quindi è un iperpiano proiettivo.
- **singolarità in un punto**: sia $Q = (q_0 : \cdots : q_n) \in \mathbb{P}^n$ un punto arbitrario, e consideriamo tutte le ipersuperfici di grado d che hanno Q come punto singolare.

  La condizione si esprime imponendo

  $$\nabla F(q_0, \dots, q_n) = 0,$$

  che corrisponde a $n+1$ condizioni del tipo

  $$\partial_j F(q_0, \dots, q_n) = 0. \tag{8.2}$$

  Essendo

  $$\partial_j F = \sum_{i_0+\cdots+i_n=d} w_{i_0 \dots i_n} x_0^{i_0} \dots i_j x_j^{i_j - 1} \dots x_n^{i_n},$$

  le condizioni (8.2) sono lineari nei coefficienti di F. Non è difficile verificare che sono linearmente indipendenti, quindi la codimensione del sistema lineare corrispondente è $n+1$.

Nel caso proiettivo, al contrario di quello affine, non è necessario imporre la condizione ulteriore che le curve passino per Q, i.e. la condizione $F(Q) = 0$. Infatti dalla relazione di Eulero si ha che

$$F = \sum_{j=0}^{n} \left(\frac{x_j}{d}\right) \partial_j F$$

quindi da $(\partial_j F)(Q) = 0,\ j = 0, \dots, n$, ne segue anche che $F(Q) = 0$.

- **passaggio per un punto e tangente assegnata**: sia $Q = (q_0 : q_1 : q_2) \in \mathbb{P}^2$ un punto arbitrario e sia $L \ni Q$ una retta proiettiva piana passante per Q.

  Vogliamo determinare il luogo delle curve passanti per Q e aventi Q come punto singolare, oppure L come retta tangente alla curva in Q.

  La condizione di passaggio per Q si esprime con la condizione lineare

  $$F(Q) = 0\,. \tag{8.3}$$

  Supponiamo per il momento che Q sia liscio per $Z_P(F)$; la retta L coincide con la retta tangente $\tau_Q Z_P(F)$ se e solo se, scelto un punto $R = (r_0 : r_1 : r_2) \in L$, con $Q \neq R$, si ha $R \in \tau_Q Z_P(F)$. Ricordiamo che una equazione cartesiana della retta tangente è data da $\nabla F(Q) \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = 0$, quindi R scelto come punto di L appartiene alla tangente $\tau_Q Z_P(F)$ se e solo se

  $$\nabla F(Q) \cdot \begin{pmatrix} r_0 \\ r_1 \\ r_2 \end{pmatrix} = 0. \tag{8.4}$$

  Osserviamo che la condizione (8.4) è lineare nei coefficienti di F, e che è automaticamente soddisfatta se Q è un punto singolare per $Z_P(F)$.

  Concludiamo, quindi, che il luogo cercato è un sistema lineare di codimensione 2, determinato dalle due equazioni lineari (8.3) e (8.4), e che tale sistema lineare contiene il sottosistema lineare di tutte le curve singolari in Q (che ha codimensione 3 per il punto precedente).

Osservazione 8.5. Consideriamo ora r punti $Q_1, \dots, Q_r \in \mathbb{P}^n$; il passaggio per ciascuno di essi è una condizione lineare sulle ipersuperfici proiettive di grado d. Vogliamo

determinare la dimensione del sistema lineare delle ipersuperfici passanti per tutti gli r punti (tali ipersuperfici si chiamano *interpolanti* per gli r punti); in altre parole, vogliamo capire se le r condizioni di passaggio sono indipendenti oppure no.

Le condizioni di passaggio per r punti di $\mathbb{P}^n$ sono dipendenti se e solo se una equazione si può scrivere come combinazione lineare delle altre, ovvero se e solo se tale equazione è automaticamente soddisfatta dai coefficienti di tutti i polinomi che soddisfano le altre $r-1$ equazioni. In altre parole, ciò vale se e solo se tra gli r punti ce ne sono $r-1$ per cui ogni ipersuperficie che passa per gli $r-1$ punti passa automaticamente anche per l'r-esimo.

La discussione appena fatta ha come conseguenza il seguente risultato.

Proposizione 8.6. *Il passaggio per r punti $Q_1, \dots, Q_r$ di $\mathbb{P}^n$ corrisponde a r condizioni lineari indipendenti se e solo se*

$$\forall Q_i \in \{Q_1, \dots, Q_r\},\ \exists F \in \mathbb{K}[x_0, \dots, x_n]_d \ :\ F(Q_j) = 0,\ j \neq i,\ F(Q_i) \neq 0.$$

Definizione 8.7. Dati r punti in $\mathbb{P}^n$, se il passaggio per essi corrisponde ad r condizioni indipendenti per le ipersuperfici di grado d, allora si dicono in *posizione generale rispetto alle ipersuperfici di grado d*.

Esempio 8.8. Scrivere tutte le possibili configurazioni di 4 punti nel piano e le condizioni imposte alle coniche.

Da questo punto in poi considereremo solo sistemi lineari di curve proiettive piane.

Definizione 8.9. Sia Λ un sistema lineare di curve piane. Il *luogo base* di Λ è per definizione

$$\mathrm{Bs}(\Lambda) := \{Q \in \mathbb{P}^2 \ :\ F(Q) = 0,\ \forall [F] \in \Lambda\}.$$

Osservazione 8.10. Se $\Lambda = \mathbb{P}(\mathrm{Span}(F_0, \dots, F_q))$, allora $Q \in \mathrm{Bs}(\Lambda)$ se e solo se $Q \in Z_P(F_0) \cap \dots \cap Z_P(F_q)$.

Infatti, sia $[F] \in \Lambda$; si ha $F = \lambda_0 F_0 + \dots + \lambda_q F_q$. Se $F_0(Q) = \dots = F_q(Q) = 0$, allora $F(Q) = \lambda_0 F_0(Q) + \dots + \lambda_q F_q(Q)$, perché la valutazione di un polinomio nelle coordinate di un punto è un omomorfismo di anelli. Quindi $F(Q) = 0$.

Se, viceversa, $F(Q) = 0$ per ogni $[F] \in \Lambda$, questo vale in particolare per $F_0, \dots, F_q$.

Esempio 8.11. Luoghi base di fasci di coniche.

Esempio 8.12. Consideriamo due cubiche piane che si intersecano in 9 punti distinti; il sistema lineare Λ delle cubiche passanti per tali punti è almeno un fascio, generato dalle due cubiche, e quindi deve avere dimensione almeno uno, data dal parametro libero proiettivo del fascio. Questa scelta ci fornisce quindi 9 punti che non sono in posizione generale rispetto alle cubiche, perché si ha

$$\dim \Lambda \geq 1 > N(3,2) - 9 = \binom{3+2}{3} - 1 - 9 = 0.$$

8.3 Teorema di Castelnuovo ed Esagramma Mistico di Pascal

Teorema 8.13 (Teorema di Guido Castelnuovo (Venezia 1865 – Roma 1952))**.** *Siano $Q_1, \ldots, Q_r \in \mathbb{P}^2$ punti distinti. Allora, per ogni $d \geq r-1$, essi sono in posizione generale rispetto alla curve di grado d.*

Dimostrazione. Fissiamo $d \geq 1$, e dimostriamo l'enunciato per induzione su r con $r \leq d+1$.

Se $r = 1$, la tesi è vera.

Supponiamo la tesi vera per $r-1$; ogni sottoinsieme $\{Q_{i_1}, \ldots, Q_{i_{r-1}}\}$ di $r-1$ punti di $\{Q_1, \ldots, Q_r\}$ impone condizioni indipendenti alle curve di grado d (infatti $r-1 < r \leq d+1$). Sia

$$\Lambda_{i_1,\ldots,i_{r-1}} = \{[F] \ : \ \{Q_{i_1}, \ldots, Q_{i_{r-1}}\} \subset Z_P(F)\},$$

e sia

$$\Lambda_r = \{[F] \ : \ \{Q_1, \ldots, Q_r\} \subset Z_P(F)\}.$$

Per ipotesi induttiva abbiamo

$$\dim \Lambda_{i_1,\ldots,i_{r-1}} = N(d,2) - (r-1).$$

Quindi avremo $\dim \Lambda_r = N(d,2) - r$ se e solo se $\Lambda_{i_1,\ldots,i_{r-1}} \supsetneq \Lambda_r$.

Un elemento $[F] \in \Lambda_{i_1,\ldots,i_{r-1}} \setminus \Lambda_r$ è, ad esempio, il polinomio corrispondente alla curva riducibile data da $r-1$ rette passanti per gli $r-1$ punti e non passanti per l'r-esimo, unita con una curva di grado $d-(r-1) \geq 0$ non passante per l'r-esimo punto. □

Osservazione 8.14. Osserviamo che la limitazione $d \geq r-1$ è ottimale: infatti, dal Teorema di Bézout si deduce facilmente che r punti allineati impongono condizioni dipendenti alla curve di grado $d = r-2$.

Vediamo ora un altro risultato sulla geometria dei punti del piano proiettivo, che ci permetterà poi di dimostrare un famoso Teorema di Pascal.

Teorema 8.15. *Siano $F, G \in \mathbb{K}[x_0, x_1, x_2]_d$ due polinomi tali che $Z_P(F) \cap Z_P(G)$ consista esattamente di d^2 punti distinti.*
Se esiste $n < d$ tale che nd di questi punti giacciano su un curva irriducibile di grado n, allora i rimanenti $d^2 - nd = d(d-n)$ punti giacciono su una curva di grado $d - n$.

Dimostrazione. Consideriamo il fascio $\Lambda = \mathbb{P}(\mathrm{Span}(F, G))$ e sia $H \in \mathbb{K}[x_0, x_1, x_2]_n$ un polinomio irriducibile tale che $Z_P(H)$ contiene nd punti. Su $Z_P(H)$ scegliamo un ulteriore punto Q, diverso dai precedenti. Siccome $\dim \Lambda = 1$, esiste almeno una curva $Z_P(M)$ di Λ passante per Q.
Per costruzione $Z_P(H) \cap Z_P(M)$ contiene $nd + 1 > \deg H \cdot \deg M$ punti, quindi per il Teorema di Bézout le due curve hanno una componente comune. Essendo H irriducibile, ne deduciamo che $Z_P(H) \subset Z_P(M)$ e che

$$M = H \cdot H_1 \,,$$

con $H_1 \in \mathbb{K}[x_0, x_1, x_2]_{n-d}$. Siccome $\mathrm{Bs}\,\Lambda$ consiste di d^2 punti distinti per ipotesi, si ha che $Z_P(H_1) \cap Z_P(F)$ consiste di $d(d-n)$ punti base del fascio. □

Come conseguenza abbiamo il seguente notevole risultato, scoperto nel 1639 dall'allora sedicenne matematico e filosofo francese Blaise Pascal (1623-1662):

Teorema 8.16 (Teorema dell'Esagramma Mistico di Pascal)**.** *Si considerino nel piano proiettivo una conica e un esagono i cui vertici giacciono sulla conica. Allora le tre coppie di rette che individuano lati opposti dell'esagono si incontrano in tre punti che giacciono su una retta, detta la "retta di Pascal" dell'esagono.*

Dimostrazione. Un esagono inscritto a una conica è determinato da una 6-upla $\{P_1, \ldots, P_6\}$ di punti ordinati sulla conica. I punti di intersezione delle rette relative a lati opposti sono:

$$A = \overline{P_1P_2} \cap \overline{P_4P_5}, \quad B = \overline{P_2P_3} \cap \overline{P_5P_6}, \quad C = \overline{P_3P_4} \cap \overline{P_6P_1}.$$

Consideriamo le seguenti cubiche riducibili:

$$\overline{P_1P_2} \cup \overline{P_3P_4} \cup \overline{P_5P_6}, \quad \overline{P_2P_3} \cup \overline{P_4P_5} \cup \overline{P_6P_1}.$$

Esse si incontrano nei punti $P_1, \dots, P_6, A, B, C$, cioè $9 = 3 \cdot 3$ punti distinti. Per costruzione i primi $6 = 2 \cdot 3$ punti giacciono su una conica, quindi i rimanenti $9 - 6 = 3$ punti giacciono su una curva di grado $3 - 2 = 1$. □

Osservazione 8.17. In particolare, se due coppie di lati opposti sono parallele, esse si intersecano sulla retta all'infinito, e quindi anche la terza coppia di lati opposti è parallela.

Osservazione 8.18. Dati sei punti non ordinati su una conica, essi possono essere congiunti per formare un esagono in 60 modi distinti, e di conseguenza esistono 60 rette di Pascal; l'insieme di tali rette è detto l'Esagramma Mistico relativo ai 6 punti, e per tale motivo il teorema di Pascal è anche detto teorema dell'Esagramma Mistico.

Il teorema di Pascal può essere visto come una generalizzazione del classico teorema di Pappo: infatti, quest'ultimo si ottiene nel caso limite in cui la conica degenera nell'unione di due rette. Si noti inoltre che è possibile dare un enunciato del teorema di Pascal anche nel piano affine, trattando opportunamente i casi in cui una o più coppie di rette diventino parallele; ad esempio, se due coppie di lati opposti definiscono rette parallele, allora lo stesso vale per tutte e tre le coppie di lati opposti, e non esiste nessuna retta di Pascal affine (in tal caso la retta di Pascal è la retta all'infinito).

Concludiamo questa sezione ponendoci la seguente domanda: qual è il numero massimo di punti del piano proiettivo che impongono condizioni indipendenti alla curve di grado d? Ecco la risposta:

Proposizione 8.19. *Per ogni $d \geq 1$, esistono $N(d, 2) = \frac{d(d+3)}{2}$ punti in posizione generale rispetto alle curve di grado d.*

Dimostrazione. Scegliamo $d + 1$ punti su una retta L_1; poi fissiamo d punti su una altra retta L_2, di cui nessuno appartenente a L_1; proseguiamo in questo modo, fissando $d + 2 - i$ punti su una retta L_i, per ogni $1 \leq i \leq d$, in modo che le rette L_i siano tutte distinte, e nessuno dei punti scelti coincida con $L_i \cap L_j$ per qualche j.

Abbiamo ottenuto complessivamente $(d + 1) + d + \cdots + 2 = \frac{(d+1)(d+2)}{2} - 1 = N(d, 2)$ punti. Affermiamo che questi punti appartengono a una unica curva di grado d, e precisamente l'unione delle d rette che abbiamo fissato: $L_1 \cup L_2 \cup \cdots \cup L_d$.

Infatti, se esistesse un'altra curva $Z_P(F)$ di grado d passante per tutti i punti, essa intersecherebbe la retta L_1 in $d + 1$ punti, e per il Teorema di Bézout dovrebbe contenere tutta L_1; la curva residua, di grado $d - 1$ intersecherebbe L_2 in d punti, quindi

conterrebbe L_2. Procedendo in questo modo vediamo che $Z_P(F)$ deve coincidere di fatto con l'unione delle d rette.

Ne segue che il sistema lineare Λ delle curve di grado d passanti per questi $N(d,2)$ punti ha dimensione

$$\dim \Lambda = 0\,,$$

quindi il numero di condizioni indipendenti è

$$c = \dim \mathbb{P}(\mathbb{K}[x_0, x_1, x_2]_d) - \dim \Lambda = N(d,2) - 0 = N(d,2).$$

□

Corollario 8.20. *Per ogni $d \geq 1$, esistono $N(d,2)+1$ punti del piano proiettivo, che non giacciono su nessuna curva piana di grado d.*

Dimostrazione. Basta scegliere $N(d,2)$ punti che giacciono su una unica curva di grado d, e scegliere l'ulteriore punto fuori da tale curva. □

Osservazione 8.21. Ricordiamo che il numero di condizioni indipendenti relative a imporre che un punto sia singolare è uguale a $n+1$, quindi è uguale a 3 nel piano proiettivo. L'analoga questione su quale sia il numero massimo di condizioni indipendenti imposte da un insieme di punti singolari è estremamente complessa ed è stata determinata dai matematici J. Alexander e A. Hirschowitz nel 1995.

Teorema 8.22 (Teorema di Alexander - Hirschowitz)**.** *Siano $P_1, \ldots, P_r \in \mathbb{P}^2$ in posizione generale rispetto alle curve di grado d.*

Allora il numero di condizioni imposte dall'avere singolarità in $P_1, \ldots, P_r$ è il massimo possibile, e cioè

$$\min\{3r, N(d,2)+1\},$$

ad eccezione dei casi $(r,d) = (2,2)$ e $(r,d) = (5,4)$.

Osservazione 8.23. Nel caso $(r,d) = (2,2)$ si ha

$$\min\{3r, N(d,2)+1\} = 6,$$

quindi non dovrebbero esistere coniche con due punti singolari, mentre invece la retta doppia passante per i due punti c'è.

Nel caso $(r, d) = (5, 4)$ si ha

$$\min\{3r, N(d, 2) + 1\} = 15,$$

quindi non dovrebbero esistere quartiche con cinque punti singolari, mentre invece la conica doppia passante per i cinque punti c'è.

8.4 Curve polari

Tra i sistemi lineari più significativo c'è il sistema lineare polare, generato dalle derivate parziali di un polinomio omogeneo, che ha delle proprietà geometriche particolari.

Definizione 8.24. Sia $F \in \mathbb{K}[x_0, x_1, x_2]_d$ con $d \geq 2$ un polinomio omogeneo. Il *sistema lineare polare* associato a F è

$$\Sigma_F := \mathbb{P}(\mathrm{Span}(\partial_0 F, \partial_1 F, \partial_2 F)).$$

Dato un punto $R = (r_0 : r_1 : r_2) \in \mathbb{P}^2$, la *curva polare* di F rispetto a R è la curva piana di equazione

$$r_0\partial_0 F + r_1\partial_1 F + r_2\partial_2 F = 0\,.$$

Il polinomio $\mathrm{Pol}_R F = r_0\partial_0 F + r_1\partial_1 F + r_2\partial_2 F = \nabla F \cdot \begin{pmatrix} r_0 \\ r_1 \\ r_2 \end{pmatrix} \in \Sigma_F$ è, in generale, un polinomio non nullo di grado $d - 1$.

Se F è sufficientemente generale, il sistema polare è una rete, cioè le tre derivate parziali sono linearmente indipendenti. Infatti, vale il seguente risultato, che non dimostriamo.

Proposizione 8.25. *Un polinomio $F \in \mathbb{K}[x_0, x_1, x_2]_d$ ha le derivate parziali linearmente dipendenti se e solo se $Z_P(F)$ è un'unione di d curve passanti per un punto comune a tutte (d rette concorrenti in un punto).*

Vediamo ora una proprietà molto utile.

Proposizione 8.26. *Sia $R \notin Z_P(F)$. Allora*

$$Z_P(F) \cap Z_P\big(\mathrm{Pol}_R(F)\big) = \mathrm{Sing}Z_P(F) \cup \{Q \,:\, \overline{QR} = \tau_Q Z_P(F)\},$$

ovvero la curva polare rispetto a R interseca $Z_P(F)$ nei suoi eventuali punti singolari e nei punti di tangenza delle tangenti alla curva uscenti da R.

Dimostrazione. Sia $Q \in Z_P(F) \cap Z_P(\mathrm{Pol}_R(F))$, quindi Q verifica

$$F(Q) = 0, \quad \nabla F(Q) \cdot \begin{pmatrix} r_0 \\ r_1 \\ r_2 \end{pmatrix} = 0\,.$$

Si hanno due casi: $\nabla F(Q) = 0$, e allora Q è un punto singolare, oppure Q è un punto liscio, e la relazione $\nabla F(Q) \cdot \begin{pmatrix} r_0 \\ r_1 \\ r_2 \end{pmatrix} = 0$ ci dice che R appartiene alla retta tangente a $Z_P(F)$ in Q. □

Corollario 8.27. *Data una curva irriducibile $Z_P(F)$ di grado d, che non sia un'unione di d rette concorrenti, per un punto $R \in \mathbb{P}^2 \setminus Z_P(F)$ il numero n di rette tangenti uscenti da R è limitato da*

$$n \leq d(d-1)\,.$$

Dimostrazione. Siccome la curva non è un'unione di d rette concorrenti, la curva polare rispetto a R ha grado $d-1$; inoltre, $Z_P(F)$ è irriducibile, quindi non ha componenti comuni con $Z_R(\mathrm{Pol}_P(F))$. Per il Teorema di Bézout, il numero di punti nell'intersezione è limitato dal prodotto dei gradi. □

Come conseguenza abbiamo il risultato seguente:

Proposizione 8.28 (Teorema di Bertini)**.** *Sia $Z_P(F)$ una curva irriducibile e ridotta, e sia $R \in \mathbb{P}^2 \setminus Z_P(F)$.*
Allora la generica retta per R interseca $Z_P(F)$ in d punti distinti.

Dimostrazione. Sia $L \ni R$. Per il Teorema di Bézout abbiamo

$$\sum_{Q \in L \cap Z_P(F)} I_Q(L, Z_P(F)) = d.$$

Osserviamo ora che un punto Q soddisfa $I_Q(L, Z_P(F)) \geq 2$ se e solo se Q è singolare, oppure L è tangente alla curva in Q. Ma abbiamo visto che il numero di punti singolari di una curva ridotta è finito, e anche i punti di tangenza delle tangenti uscenti da R sono finiti. Segue che solo un numero finito di rette per R ha tra i punti di intersezione qualche Q con $I_Q(L, Z_P(F)) \geq 2$. □

8.5 Esercizi

1. Sia $\mathbb{K}$ un campo algebricamente chiuso (basta che sia infinito) e siano $Z_P(F) \subset \mathbb{P}^2_{\mathbb{K}}$ e $Z_P(G) \subset \mathbb{P}^2_{\mathbb{K}}$ due curve proiettive senza componenti comuni. Si dimostri che esiste sempre un proiettività di $\mathbb{P}^2_{\mathbb{K}}$ che manda le due curve in una coppia di curve in posizione ammissibile rispetto a E_2.
2. Sia $Z_P(F) \subset \mathbb{P}^n_{\mathbb{C}}$ una ipersuperficie proiettiva, e sia $\varphi : \mathbb{P}^n_{\mathbb{C}} \to \mathbb{P}^n_{\mathbb{C}}$ una proiettività determinata da una matrice invertibile A. Si dimostri che se un punto $Q \in Z_P(F)$ è singolare, allora $\varphi(Q)$ è singolare per la ipersuperficie immagine $\varphi(Z_P(F))$.
3. Usando l'esercizio precedente, si dimostri che la condizione sulle ipersuperfici di grado d in $\mathbb{P}^n_{\mathbb{C}}$ di avere un punto singolare assegnato corrisponde a $n+1$ condizioni lineari linearmente indipendenti sui coefficienti del generico polinomio.
4. Si determinino esplicitamente le condizioni sui coefficienti dei polinomi $F \in \mathbb{C}[x_0, x_1, x_2]_3$ di avere:
   - tangente $x_1 = 0$ in $(1 : 0 : 1)$;
   - tangente $x_1 - x_2 = 0$ in $(1 : 1 : 1)$;
   - una singolarità nel punto $(1 : 0 : 0)$.

   Se ne deduca la dimensione del sistema lineare corrispondente. Ci sono curve irriducibili in tale sistema lineare?
5. Si dimostri che fissati cinque punti arbitrari su una conica piana irriducibile, il passaggio per essi impone cinque condizioni linearmente indipendenti ai polinomi omogenei di grado 2 in tre indeterminate.
6. Si determini una condizione lineare sui polinomi omogenei di grado 2 in 3 indeterminate x_0, x_1, x_2 che non corrisponde al passaggio per alcun punto di $\mathbb{P}^2$.
7. Si dimostri che se r punti del piano non sono allineati, allora impongono r condizioni indipendenti alle curve piane di grado $d = r - 2$.
8. Si dimostri che 9 punti del piano proiettivo, ottenuti come intersezione di due cubiche piane irriducibili, impongono esattamente 8 condizioni lineari indipendenti alle cubiche. Suggerimento: si dimostri che comunque scelti 7 punti, esiste una cubica passante per i 7 punti e non passante per i rimanenti due.

9. Si consideri la cubica proiettiva piana C di equazione

$$x_1^3 + x_0 x_1^2 - x_0 x_2^2 = 0.$$

Usando la nozione di curva polare, si determinino tutte le tangenti a punti non singolari di C uscenti dal punto $(0 : 1 : 0)$. Si determini, inoltre, una retta passante per $(0 : 1 : 0)$ che interseca C in tre punti distinti.

9 Singolarità di curve irriducibili e razionalità

9.1 Stima sul numero di punti singolari di curve irriducibili

Vediamo ora come con l'uso di opportuni sistemi lineari possiamo migliorare la stima sui punti singolari di una curva irriducibile.

Teorema 9.1. *Sia F un polinomio irriducibile di grado $d \geq 2$ e siano $P_1, \dots, P_s$ i punti singolari di $Z_P(F)$ di rispettive molteplicità $m_1, \dots, m_s$.*

Allora si ha

$$\sum_{i=1}^{s} m_i(m_i - 1) \leq (d-1)(d-2)\,. \tag{9.1}$$

Dimostrazione. Per la dimostrazione useremo il *metodo delle curve aggiunte* di grado $d-1$; consideriamo il sistema lineare

$$\begin{aligned}\Lambda &:= \{\text{curve di grado } d-1 \text{ aventi } P_i \text{ con molteplicità} \geq m_i - 1,\ \forall i = 1, \dots, s\} \\ &= \{[F] \in \mathbb{P}^{N(d-1,2)} \ :\ F(P_i) = 0,\ m_{P_i}(F) \geq m_i - 1\}.\end{aligned}$$

Osserviamo che $\Lambda \neq \emptyset$, in quanto si ha $[\partial_{x_i} F] \in \Lambda$ per $i = 0, 1, 2$.

Vogliamo ora valutare la codimensione di Λ, cioè il numero di condizioni lineari indipendenti imposte ai polinomi di grado $d-1$. Per definizione di molteplicità di un punto, si ha che $[G] \in \Lambda$ se e solo se tutte le derivate parziali $(m_i - 2)$-esime di G si annullano in P_i per ogni $i = 1, \dots, s$. Inoltre, è facile verificare che il numero di derivate parziali di ordine $m_i - 2$ coincide con il numero di monomi monici di grado $m_i - 2$, ed è quindi uguale a

$$\binom{2 + (m_i - 2)}{2} = \binom{m_i}{2} = \frac{m_i(m_i - 1)}{2}\,.$$

Quindi il numero di condizioni lineari indipendenti è $\leq \sum_{i=1}^{s} \frac{m_i(m_i-1)}{2}$, da cui otteniamo

$$\dim \Lambda \geq N(d-1,2) - \sum_{i=1}^{s} \frac{m_i(m_i-1)}{2}\,.$$

Osserviamo ora che essendo F irriducibile, in particolare è anche ridotto, quindi possiamo usare la maggiorazione data in (7.3):

$$\sum_{i=1}^{s} \frac{m_i(m_i-1)}{2} \leq \frac{d(d-1)}{2}.$$

Si ottiene

$$\dim \Lambda \geq N(d-1,2) - \frac{d(d-1)}{2} = \frac{(d-1)(d+2)}{2} - \frac{d(d-1)}{2} = d-1.$$

Siccome stiamo supponendo che sia $d \geq 2$, abbiamo che $\dim \Lambda \geq N(d-1,2) - \sum_{i=1}^{s} \frac{m_i(m_i-1)}{2} \geq 1$. Poniamo

$$t := N(d-1,2) - \sum_{i=1}^{s} \frac{m_i(m_i-1)}{2}, \tag{9.2}$$

e fissiamo ulteriori t punti $Q_1, \ldots, Q_t \in Z_P(F)$, tutti diversi dai P_i. Dalla $\dim \Lambda \geq t$ deduciamo che possiamo imporre alle curve di Λ il passaggio per $Q_1, \ldots, Q_t$ e troviamo un sottosistema lineare non vuoto $\Lambda' \subset \Lambda$ di dimensione $\dim \Lambda' \geq 0$. Possiamo quindi scegliere una classe di polinomio

$$[G] \in \Lambda';$$

per costruzione abbiamo

$$Z_P(F) \cap Z_P(G) \supseteq \{P_1, \ldots, P_s, Q_1, \ldots, Q_t\}.$$

Inoltre, essendo F irriducibile di grado d e G di grado $d-1 < d$, certamente F e G sono privi di fattori comuni, quindi per il Teorema di Bézout si ha

$$d(d-1) = \sum_{R \in Z_P(F) \cap Z_P(G)} I_R(F,G) \geq \sum_{i=1}^{s} I_{P_i}(F,G) + \sum_{j=1}^{t} I_{Q_j}(F,G) \geq \sum_{i=1}^{s} m_i(m_i-1) + t.$$

Usando l'espressione (9.2) otteniamo

$$\sum_{i=1}^{s} m_i(m_i-1) + N(d-1,2) - \sum_{i=1}^{s} \frac{m_i(m_i-1)}{2} \leq d(d-1)\,,$$

da cui

$$\sum_{i=1}^{s} \frac{m_i(m_i-1)}{2} \leq d(d-1) - N(d-1,2) = d(d-1) - \frac{(d-1)(d+2)}{2} = \frac{(d-1)(d-2)}{2},$$

che dà la tesi. □

Osservazione 9.2. La stima (9.1) è ottimale, ed è soddisfatta, ad esempio, dalle curve di equazione

$$F_d + x_0 F_{d-1} = 0\,,$$

dove $F_d = F_d(x_1, x_2)$ e $F_{d-1} = F_{d-1}(x_1, x_2)$ sono due polinomi omogenei di gradi d e $d-1$, senza fattori comuni. La curva risulta irriducibile e con un unico punto singolare, in $(1:0:0)$, di molteplicità $d-1$. Si ha $s = 1$ e $m_1 = d-1$.

9.2 Genere geometrico e curve razionali

Definizione 9.3. Un punto singolare Q di molteplicità $m \geq 2$ di una curva ridotta $Z_P(F)$ si dice *singolarità ordinaria* se il cono tangente consiste di m rette tangenti distinte, e *cuspide ordinaria* se il cono tangente consiste di un'unica tangente L e si ha

$$I_Q(F, L) = m + 1\,.$$

Definizione 9.4. Sia $Z_P(F)$ una curva irriducibile e ridotta, con singolarità ordinarie e/o cuspidi ordinarie. Il *genere geometrico* di $Z_P(F)$ è

$$g = g(F) := \binom{d-1}{2} - \sum_{i=1}^{s} \binom{m_i}{2} \geq 0. \tag{9.3}$$

In particolare:

- se $Z_P(F)$ è liscia (i.e. $s = 0$), si ha $g = \binom{d-1}{2}$.
- se $g = 0$, la curva si dice *razionale*.

Osservazione 9.5. La definizione di genere geometrico implica direttamente che per $d = 1$ e per $d = 2$ la curva è sempre liscia e razionale, mentre per $d > 2$ una curva razionale non può essere liscia.

Definizione 9.6. Una *parametrizzazione razionale* di una curva piana proiettiva è una mappa polinomiale

$$\varphi\colon \mathbb{P}^1 \setminus \Sigma \to Z_P(F),$$

con Σ insieme finito di punti, eventualmente vuoto, e φ genericamente iniettiva, ovvero non iniettiva in al più un numero finito di punti, e data da componenti del tipo

$$\varphi(t_0 : t_1) = \big(F_0(t_0, t_1) : F_1(t_0, t_1) : F_2(t_0, t_1)\big),$$

con F_i omogenei e tutti dello stesso grado.

Esempio 9.7. Si verifichi che una mappa

$$\varphi(t_0 : t_1) = \big(F_0(t_0, t_1) : F_1(t_0, t_1) : F_2(t_0, t_1)\big),$$

con F_i omogenei e tutti dello stesso grado è ben definita su $\mathbb{P}^1 \setminus \Sigma$.

Osservazione 9.8. Vediamo come possiamo caratterizzare la restrizione di una mappa razionale $\varphi\colon \mathbb{P}^1 \setminus \Sigma \to Z_P(F)$ a un aperto affine. Per semplicità consideriamo $U_0 = \{(t_0 : t_1) \mid t_0 \neq 0\} \subset \mathbb{P}^1$ e sia $V_0 = \{(x_0 : x_1 : x_2) \mid x_0 \neq 0\} \subset \mathbb{P}^2$. Osserviamo che possiamo scrivere le coordinate omogenee dei punti di U_0 nella forma $(1 : t) \in U_0$. Si ha quindi

$$\varphi(U_0 \setminus \Sigma) \cap V_0 = \{(F_0(1, t) : F_1(1, t) : F_2(1, t)) \mid F_0(1, t) \neq 0\} \subset Z_P(F) \cap V_0.$$

Ricordiamo ora che U_0 è in biiezione con $\mathbb{A}^1$ e che V_0 è in biiezione con $\mathbb{A}^2$ tramite le immersioni di tipo j_0. Troviamo quindi un diagramma commutativo

$$\begin{array}{rccc} \varphi\colon & U_0 \setminus \Sigma & \to & Z_P(F) \cap V_0 \\ & \uparrow j_0 & & \uparrow j_0 \\ \psi\colon & \mathbb{A}^1 \setminus \Sigma' & \to & Z(aF) \subset \mathbb{A}^2, \end{array}$$

dove $\Sigma' = j_0^{-1}(\Sigma)$ e $\psi(t)$ è data da:

$$\psi(t) = \left(\frac{F_1(1, t)}{F_0(1, t)}, \frac{F_2(1, t)}{F_0(1, t)}\right) = \left(\frac{aF_1(t)}{aF_0(t)}, \frac{aF_2(t)}{aF_0(t)}\right) = \left(\frac{f_1(t)}{f_0(t)}, \frac{f_2(t)}{f_0(t)}\right).$$

Quindi, la restrizione di una mappa razionale proiettiva è una applicazione razionale tra spazi affini, le cui componenti sono quozienti di polinomi in una indeterminata.

Viceversa, osserviamo che data una applicazione razionale $\psi\colon \mathbb{A}^1 \setminus \Sigma' \to Z(f) \subset \mathbb{A}^2$, dove Σ' è un insieme finito, eventualmente vuoto, essa si può sempre estendere a una mappa razionale proiettiva.

Esempio 9.9. Consideriamo la conica liscia data dal cerchio piano

$$C = Z(x^2 + y^2 - 1) \subset \mathbb{A}^2$$

e la parametrizzazione indotta dal fascio di rette passanti per il punto $P = (1, 0)$ come in figura 9.1:

$$\begin{cases} x^2 + y^2 - 1 = 0 \\ (x - 1) + ty = 0. \end{cases}$$

Sostituendo $x = 1 - ty$ nella prima equazione troviamo

$$0 = (1-ty)^2 + y^2 - 1 = (t^2+1)y^2 - 2ty = y \cdot ((t^2+1)y - 2t)\,.$$

La radice $y = 0$ corrisponde al punto di intersezione $(1,0)$, che è comune a tutte la rette, mentre la radice $y = \frac{2t}{t^2+1}$ rappresenta la seconda coordinata del punto variabile di intersezione tra la generica retta del fascio e il cerchio.

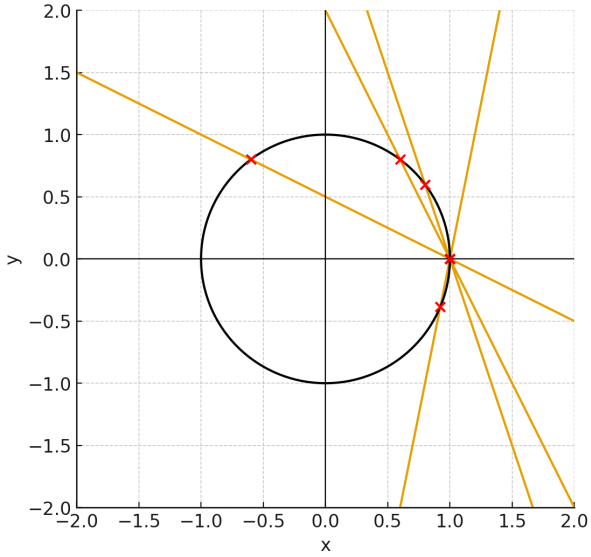


Figura 9.1: Un fascio di rette passanti per $P = (1,0)$ e le sue intersezioni con il cerchio unitario permettono di dare una parametrizzazione razionale.

Otteniamo quindi la parametrizzazione

$$\psi\colon \mathbb{A}^1 \setminus \{i,-i\} \to C, \quad \psi(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right).$$

se $\bar{C} = Z_P(x_1^2 + x_2^2 - x_0^2)$ è la chiusura proiettiva di C, allora una parametrizzazione razionale di $\bar{C}$ è data da

$$\varphi\colon \mathbb{P}^1 \to \bar{C},\ \varphi(t_0 : t_1) = (t_0^2 + t_1^2 : t_0^2 - t_1^2 : 2t_0t_1).$$

Esempio 9.10. Consideriamo la quartica affine

$$C = Z\big(xy(y-x)(y-2x) + (y+3x)(y+x)(y+2x)\big) \subset \mathbb{A}^2$$

e la parametrizzazione

$$\psi\colon \mathbb{A}^1 \setminus \{0,1,2\} \to C,\ \psi(t) = \left(\frac{(t+1)(t+2)(t+3)}{t(t-1)(t-2)}, \frac{(t+1)(t+2)(t+3)}{(t-1)(t-2)}\right),$$

se $\overline{C} = Z_P(x_1x_2(x_2-x_1)(x_2-2x_1)+(x_2+3x_1)(x_2+x_1)(x_2+2x_1)x_0)$ è la chiusura proiettiva di C, allora una parametrizzazione razionale di $\overline{C}$ è data da

$$\varphi\colon \mathbb{P}^1 \to \overline{C},$$

$$\varphi(t_0:t_1) = \Big(t_0t_1(t_1-t_0)(t_1-2t_0) : t_0(t_1+t_0)(t_1+2t_0)(t_1+3t_0) : t_1(t_1+t_0)(t_1+2t_0)(t_1+3t_0)\Big).$$

Teorema 9.11. *Se $Z_P(F)$ è una curva irriducibile razionale, allora ammette una parametrizzazione razionale.*

Dimostrazione. Fissiamo $2d-3$ punti nonsingolari $Q_1,\dots,Q_{2d-3} \in Z_P(F)\cap U_0$ e siano $P_1,\dots,P_s$ i punti singolari di $Z_P(F)$. A meno di proiettività (esercizio) possiamo supporre che:

- $Z_P(F)$ e i punti $P_1,\dots,P_s,Q_1,\dots,Q_{2d-3}$ siano in posizione ammissibile sia rispetto a $E_2=(0:0:1)$ che rispetto a $E_1=(0:1:0)$;
- Sing $Z_P(F) \subset U_0 = \mathbb{P}^2 \setminus Z_P(x_0)$.

Consideriamo il sistema lineare delle aggiunte di grado $d-1$ e passanti per i punti $Q_1,\dots,Q_{2d-3}$:

$$\Lambda_{d-1} := \{\text{curve di grado } d-1, \text{ aventi } P_i \text{ di molteplicità } \geq m_i-1, \text{ e passanti per } Q_1,\dots,Q_{2d-3}\}.$$

Vogliamo dare una stima della dimensione di Λ_{d-1}. Ricordiamo che un punto ha molteplicità $\geq m_i-1$ se e solo se annulla tutte le derivate parziali di ordine m_i-2. Inoltre, osserviamo che il numero di tali derivate parziale corrisponde al numero di monomi di grado m_i-2 nelle indeterminate x_0,x_1,x_2, ed è quindi uguale a $\binom{m_i-2+2}{2}$. L'annullamento di ogni derivata parziale è una condizione lineare sui coefficienti dei polinomi di grado $d-1$; non sappiamo se le l'insieme di condizioni lineari sia linearmente indipendente; in ogni caso, possiamo dire che il numero di condizioni lineari imposte è maggiorato da

$$\sum_{i=1}^{s}\binom{m_i}{2} + (2d-3).$$

Quindi abbiamo

$$\begin{aligned}\dim \Lambda_{d-1} &\geq N(d-1,2) - \sum_{i=1}^{s}\binom{m_i}{2} - (2d-3)\\ &= N(d-1,2) - \sum_{i=1}^{s}\frac{m_i(m_i-1)}{2} - (2d-3). \quad (9.4)\end{aligned}$$

Ricordiamo che ora per ipotesi vale

$$\sum_{i=1}^{s} \frac{m_i(m_i-1)}{2} = \frac{(d-1)(d-2)}{2};$$

sostituendo tale espressione nella (9.4), troviamo

$$\dim \Lambda_{d-1} \geq 1.$$

Affermiamo che vale $\dim \Lambda_{d-1} = 1$.

Supponiamo per assurdo che sia $\dim \Lambda_{d-1} \geq 2$. Allora possiamo imporre alle curve di Λ_{d-1} il passaggio per ulteriori 2 punti nonsingolari di $Z_P(F)$, che chiamiamo S_1 e S_2; sia $[D] \in \Lambda_{d-1}$ un tale elemento. Essendo F irriducibile, sicuramente D e F sono privi di fattori comuni. Possiamo quindi applicare il Teorema di Bézout e troviamo

$$\begin{aligned} d(d-1) &= \sum_{Q \in Z_P(F) \cap Z_P(D)} I_Q(F,D) \\ &\geq \sum_{P_i \in \mathrm{Sing} Z_P(F)} I_{P_i}(F,D) + \sum_{j=1}^{2d-3} I_{Q_j}(F,D) + I_{S_1}(F,D) + I_{S_2}(F,D) \\ &\geq \sum_{i=1}^{s} m_i(m_i-1) + (2d-3) + 2 \\ &= (d-1)(d-2) + (2d-3) + 2 = d(d-1) + 1\,, \end{aligned}$$

e abbiamo un assurdo.

Il sistema lineare Λ_{d-1} è quindi un fascio, e possiamo esprimerlo nella forma

$$\Lambda_{d-1} = \mathbb{P}\big(\mathrm{Span}(G_0, G_1)\big).$$

Osserviamo che, per costruzione, per ogni $[G] \in \Lambda_{d-1}$, si ha

$$Z_P(G) \cap Z_P(F) \supseteq \{P_1, \ldots, P_s, Q_i, \ldots, Q_{2d-3}\},$$

e inoltre

$$\begin{aligned} d(d-1) \geq \sum_{Q \in Z_P(F) \cap Z_P(G)} I_Q(F,G) &\geq \sum_{P_i \in \mathrm{Sing} Z_P(F)} I_{P_i}(F,G) + \sum_{j=1}^{2d-3} I_{Q_j}(F,G) \\ &\geq \sum_{i=1}^{s} m_i(m_i-1) + (2d-3) = d(d-1) - 1. \end{aligned}$$

Notiamo che di fatto l'ultima diseguaglianza è un'uguaglianza, e che al variare di $[G]$ nel fascio Λ_{d-1}, si ottiene un unico punto variabile; infatti, per ogni punto $Q \in Z_P(F)$

con $Q \neq P_i$, $Q \neq Q_j$, esiste sempre una curva del fascio passante per Q. L'idea è che esprimendo le coordinate di questo punto variabile troveremo una parametrizzazione della curva.

Per trovare le coordinate del punto variabile di intersezione, ci restringiamo a un aperto affine, per semplicità.

Consideriamo quindi

$$Z_P(F) \cap Z_P(t_0 G_0 + t_1 G_1) \cap U_0;$$

così facendo escludiamo i punti impropri di $Z_P(F)$, che sono in numero finito perché F è irriducibile. Questo insieme è in biiezione con

$$Z(aF) \cap Z(t_0\, aG_0 + t_1\, aG_1) \subset \mathbb{A}^2.$$

Inoltre, possiamo supporre $t_0 \neq 0$; così facendo escludiamo il punto $Z(aF) \cap Z(aG_1)$. Nell'intersezione $Z(aF) \cap Z(aG_0 + t\, aG_1)$ son quindi esclusi al più un numero finito di punti rispetto a $Z_P(F) \cap Z_P(t_0 G_0 + t_1 G_1)$.

Se ora consideriamo i due risultanti

$$R_y(aF, aG_0 + t\, aG_1) =: R_1(x,t), \quad R_x(aF, aG_0 + t\, aG_1) =: R_2(x,t),$$

i loro zeri corrispondono, rispettivamente, alle prime e seconde coordinate dei punti di intersezione in $aF \cap aG_0 + taG_1$; essendo $d(d-1) - 1$ di questi fissi, avremo che solo uno zero dei due risultanti dipenderà da t.

Più precisamente: se

$$R_1(x,t) = b_M(t) x_M + b_{M-1} x^{M-1} + \cdots + b_1(t) x + b_0(t), \tag{9.5}$$

dove $M = d(d-1)$, se $P_i = (1 : \alpha_i : \beta_i) \in U_0$ e $Q_j = (1 : \gamma_j : \delta_j) \in U_0$, per costruzione abbiamo che ogni α_i è radice di molteplicità $m_i(m_i - 1)$ e ogni γ_j è radice di molteplicità 1; inoltre, come osservato, c'è una ulteriore radice $\Phi(t)$ che dipende da t. Possiamo quindi scrivere

$$R_1(x,t) = b_M(t) \cdot \Pi_{i=1}^{s} (x - \alpha_i)^{m_i(m_i-1)} \cdot \Pi_{j=1}^{2d-3} (x - \gamma_j) \cdot (x - \Phi(t)).$$

Notiamo che il coefficiente di x^{M-1} risulta essere

$$-b_M(t) \left(\sum_{i=1}^{s} m_i(m_i-1)\alpha_i + \sum_{j=1}^{2d-3} \gamma_j + \Phi(t) \right).$$

Dalla (9.5) otteniamo quindi

$$-\frac{b_{M-1}(t)}{b_M(t)} - \left(\sum_{i=1}^{s} m_i(m_i-1)\alpha_i + \sum_{j=1}^{2d-3} \gamma_j \right) = \Phi(t),$$

da cui vediamo che $\Phi(t)$ è un quoziente di polinomi in t.

Analogamente si può verificare che la radice variabile $\Psi(t)$ di $R_2(t)$ è un quoziente di opportuni polinomi.

Abbiamo così ottenuto una mappa

$$\varphi \colon \mathbb{A}^1 \setminus \Sigma \to Z(aF) \subset \mathbb{A}^2, \quad \varphi(t) = (\Phi(t), \Psi(t)).$$

Infine, non è difficile verificare che è iniettiva, escludendo al più un insieme finito di punti (esercizio). □

Esempio 9.12. Nel caso $d = 3$ razionale si ha

$$\sum_{i=1}^{s} \binom{m_i}{2} = 1$$

Essendo $m_i \geq 2$ per ogni $i = 1, \ldots, s$, vediamo che l'unica possibilità è

$$s = 1, \quad m_1 = 2\,,$$

cioè la curva C ha un unico punto singolare P_1, che è doppio.

Inoltre, questo caso $d - 1 = 2$ e il sistema lineare Λ_2 delle aggiunte di grado 2 consiste delle coniche passanti per P_1 con molteplicità $\geq m_1 - 1 = 1$, e passanti per ulteriori $2d - 3 = 6 - 3 = 3$ punti semplici Q_1, Q_2, Q_3 della curva. In definitiva Λ_2 è dato dalle coniche passanti per 4 punti. Siccome C è irriducibile, comunque scegliamo i punti Q_j, i 4 punti P_1, Q_1, Q_2, Q_3 non sono allineati (esercizio), mentre possiamo eventualmente scegliere Q_1, Q_2, Q_3 allineati (e eventualmente anche non distinti). In ogni caso Λ_2 è un fascio di coniche. La generica conica del fascio interseca C in P_1 con molteplicità $\geq m_1(m_1 - 1) = 2$, e nei Q_j la molteplicità di intersezione è 1. Per il Teorema di Bézout c'è un sesto punto nell'intersezione, e al variare della conica nel fascio, descrive (quasi) tutti i punti di C.

Vediamo un esempio numerico: se C è la cubica cuspidata $Z_P(x_0x_2^2 - x_1^3)$, con cuspide il punto $P_1 = (1 : 0 : 0)$; scegliamo come ulteriori punti i punti intersezione con la retta $x_0 - x_1 = 0$ quindi i punti

$$Q_1 = (0 : 0 : 1), \quad Q_2 = (1 : 1 : 1), \quad Q_3 = (1 : 1 : -1).$$

Il fascio Λ_2 è un fascio degenere; infatti, per il Teorema di Bézout, tutte le sue coniche contengono la componente fissa $Z_P(x_0 - x_1)$, e hanno una retta variabile $t_0x_1 + t_1x_2$ e appartenente al fascio di rette passanti per P_1. Quindi

$$\Lambda_2 = \{[(x_0 - x_1)(t_0x_1 + t_1x_2)]\}.$$

Essendo $Z_P(x_0 - x_1)$ contenuta nel luogo base del fascio, il punto variabile si trova sulla retta $t_0x_1 + t_1x_2$. Tale punto in questo caso si può determinare direttamente per sostituzione:

$$\begin{cases} x_0x_2^2 - x_1^3 = 0 \\ t_0x_1 + t_1x_2 = 0 \end{cases} \iff x_1 = 0 \vee (x_0 : x_1 : x_2) = (t_1^3 : t_0^2t_1 : t_0^3).$$

Osserviamo che in questo caso la parametrizzazione è definita su tutto $\mathbb{P}^1$:

$$\varphi\colon \mathbb{P}^1 \to Z_P(x_0x_2^2 - x_1^3), \quad \varphi(t_0 : t_1) = (t_1^3 : t_0^2t_1 : t_0^3).$$

Esempio 9.13. Si noti che un punto doppio $m_i = 2$ contribuisce il valore 1 alla somma, un punto triplo $m_i = 3$ ha un contributo pari a 3 e un punto quadruplo ha un contributo pari a 6. Sia $\mathbf{m} = (m_1, \ldots, m_s)$ il vettore delle molteplicità.

Nel caso $d = 4$ razionale si ha $\sum_{i=1}^{s} \binom{m_i}{2} = \binom{3}{2} = 3$, ci sono quindi le seguenti possibilità:

- $\mathbf{m} = (3)$
- $\mathbf{m} = (2, 2, 2)$

Nel caso $d = 5$ razionale si ha $\sum_{i=1}^{s} \binom{m_i}{2} = \binom{4}{2} = 6$, ci sono quindi le seguenti possibilità:

- $\mathbf{m} = (4)$
- $\mathbf{m} = (3, 3)$
- $\mathbf{m} = (3, 2, 2, 2)$
- $\mathbf{m} = (2, 2, 2, 2, 2, 2)$.

9.2.1 La formula di Kontsevich

Immaginiamo di voler contare curve algebriche piane razionali di un certo grado fissato, e singolarità il più generiche possibili, i.e. nodi ordinari, in particolare di molteplicità minima, uguale a due. Ognuno di questi nodi singolari come abbiamo

visto corrisponde ad una condizione di codimensione uguale a tre se considerato in un dato punto fissato. Se invece la richiesta viene fatta senza specificare il punto del piano dove la singolarità viene imposta, la codimensione è uguale a $3 - \dim(\mathbb{P}^2) = 3 - 2 = 1$. Singolarità meno generiche, come ad esempio cuspidi ordinarie, hanno comunque molteplicità due ma codimensione più alta, e non vengono quindi contate.

Ora se la curva di grado fissato d è razionale dobbiamo avere che

$$\sum_{i=1}^{s} \binom{m_i}{2} = \binom{d-1}{2}.$$

Siccome vogliamo le molteplicità delle singolarità più basse possibili allora

$$\binom{d-1}{2} = \sum_{i=1}^{s} \binom{m_i}{2} = \sum_{i=1}^{s} 1 = s$$

perciò avremo esattamente codimensione pari ad uno per ognuno degli s punti, ovvero codimensione $\binom{d-1}{2}$. Se vogliamo costruire un problema enumerativo, ovvero la cui risposta sia un numero, dobbiamo costruire un insieme di curve finito, cioè di dimensione zero. La dimensione del luogo di curve Λ descritto finora ammonta a

$$\dim(\Lambda) = N(d,2) - \binom{d-1}{2} = \frac{d(d+3)}{2} - \frac{(d-1)(d-2)}{2} = 3d - 1.$$

Definiamo quindi Λ come il luogo di curve di grado d, razionali, che passino per $3d-1$ punti in posizione generale.

Teorema 9.14 (Kontsevich, 1995)**.** *Sia N_d il numbero di curve algebriche piane razionali passanti per $3d-1$ punti di $\mathbb{P}^2$ in posizione generale rispetto al grado d. Allora $\{N_d\}_{d\in\mathbb{Z}_{\geq 1}}$ è univocamente determinato da*

$$N_d = \sum_{\substack{a,b\geq 1 \\ a+b=d}} aN_a \cdot bN_b \left[\binom{3d-4}{3a-2} ab - \binom{3d-4}{3a-3} b^2 \right], \qquad N_1 = 1. \tag{9.6}$$

Il dato iniziale $N_1 = 1$ è equivalente al fatto che per due punti passi una ed una sola retta, dato che ogni curva di grado uno è razionale.

Illustriamo come utilizzare la formula.

Esempio 9.15. Per $d = 2$ si ha soltanto il caso $(a,b) = (1,1)$, che corrisponde al contributo

$$(a,b)=(1,1): \qquad 1N_1 \cdot 1N_1 \cdot \left[\binom{6-4}{3-2} - \binom{6-4}{3-3}\right] = 1 \tag{9.7}$$

In conclusione $N_2 = 1$, confermando che per cinque punti in posizione generale passa una ed una sola conica (la razionalità è di nuovo superflua nell'enunciato dato che tutte le coniche sono razionali).

Per $d = 3$ si hanno i seguenti contributi:

$$(a,b)=(1,2): \qquad 1N_1 \cdot 2N_2 \cdot \left[\binom{9-4}{3-2}2 - \binom{9-4}{3-3}2^2\right] = 12 \tag{9.8}$$

$$(a,b)=(2,1): \qquad 2N_2 \cdot 1N_1 \cdot \left[\binom{9-4}{6-2}2 - \binom{9-4}{6-3}\right] = 0 \tag{9.9}$$

In conclusione $N_3 = 12$: per 8 punti in posizione generale passano 12 cubiche razionali, tutte quindi necessariamente singolari.

Per $d = 4$ si hanno i seguenti contributi:

$$(a,b)=(1,3): \qquad 1N_1 \cdot 3N_3 \cdot \left[\binom{8}{1}3 - \binom{8}{0}9\right] = 36 \cdot 15 \tag{9.10}$$

$$(a,b)=(2,2): \qquad 2N_2 \cdot 2N_2 \cdot \left[\binom{8}{4}4 - \binom{8}{3}4\right] = 16 \cdot 14 \tag{9.11}$$

$$(a,b)=(3,1): \qquad 1N_1 \cdot 3N_3 \cdot \left[\binom{8}{7}3 - \binom{8}{6}\right] = 36 \cdot (-4) \tag{9.12}$$

In conclusione $N_4 = 620$: per 11 punti in posizione generale passano 620 quartiche razionali, tutte quindi necessariamente singolari. Questo risultato era stato precedentemente ottenuto dal matematico danese Zeuthen (1873), utilizzando metodi di geometria classica.

Per $d = 5$ si hanno i seguenti contributi:

$$(a,b)=(1,4): \qquad 1N_1 \cdot 4N_4 \cdot \left[\binom{11}{1}4 - \binom{11}{0}16\right] = 69.440 \tag{9.13}$$

$$(a,b)=(2,3): \qquad 2N_2 \cdot 3N_3 \cdot \left[\binom{11}{4}6 - \binom{11}{3}9\right] = 35.640 \tag{9.14}$$

$$(a,b)=(3,2): \qquad 3N_3 \cdot 2N_2 \cdot \left[\binom{11}{7}6 - \binom{11}{6}4\right] = 9.504 \tag{9.15}$$

$$(a,b)=(4,1): \qquad 4N_4 \cdot 1N_1 \cdot \left[\binom{11}{10}4 - \binom{11}{9}\right] = -27.280 \tag{9.16}$$

In conclusione $N_5 = 87.304$: per 14 punti in posizione generale passano 87.304 quintiche razionali, tutte quindi necessariamente singolari. Questo risultato è stato ottenuto dal matematico brasiliano Vainsencher (1993) poco prima della scoperta della formula di Kontsevich.

9.3 Esercizi

1. Sia $Z_P(F) \subset \mathbb{P}^2_{\mathbb{K}}$ una curva proiettiva di grado $d \geq 3$, e siano $P_1, \ldots, P_s$ i suoi punti singolari, con le rispettive molteplicità m_i per $i = 1, \ldots, s$. Si dimostri che il sistema lineare Λ delle curve aggiunte di grado $d-2$, cioè delle curve di grado $d-2$ aventi i punti $P_1, \ldots, P_s$ come punti di molteplicità $m_i - 1$, per $i = 1, \ldots, s$, e passante per ulteriori $d-3$ punti di $Z_P(F)$, verifica

$$\dim \Lambda = 1\,.$$

2. Sia $\Gamma \subset \mathbb{P}^2_{\mathbb{K}}$ una conica degenere, unione di due rette distinte:

$$\Gamma = L_1 \cup L_2,$$

e sia $Q \in L_1 \setminus L_2$ un punto non singolare. Si dimostri che la retta tangente proiettiva $\tau_Q\Gamma$ verifica

$$\tau_Q\Gamma = L_1.$$

3. Polinomi di Čebyšev: sono i polinomi così definiti

$$T_n(x) = \sum_{h=0,\, h \text{ pari}}^{n} \binom{n}{h} (x^2-1)^{h/2} x^{n-h} \in \mathbb{R}[x].$$

Siano ora $m, n \in \mathbb{N}$ coprimi e si considerino le curve affini di equazione

$$T_n(x) - T_m(y) = 0.$$

Usando la regola di Cartesio per polinomi reali, si verifichi per alcuni valori bassi di m e n che tali curve hanno la proprietà di avere esattamente $\frac{(m-1)(n-1)}{2}$ punti singolari doppi ordinari, tutti reali e concentrati in un quadrato.

4. **Cissoide di Diocle**: data una circonferenza di diametro a del piano euclideo usuale, un suo punto O e la tangente t nel punto diametralmente opposto. Per

ogni retta r per O, siano O e R le intersezioni con il cerchio, e T l'intersezione con t. Sia P il punto di r tale che $d(O,P) = d(R,T)$.

Mostrare che il luogo descritto da tali punti P è una curva algebrica che in un opportuno riferimento ha equazioni cartesiane

$$(x^2 + y^2)x - ay^2 = 0\,.$$

Si dimostri che la chiusura proiettiva di tale curva è razionale, e se ne trovi una parametrizzazione con l'uso di un programma di calcolo simbolico.

5. **Sezioni spiriche o toriche di Perseo**. Studiare le sezioni "laterali" piane di un toro immerso nello spazio euclideo usuale. Partendo dalla seguente rappresentazione cartesiana del toro in $\mathbb{A}^3_{\mathbb{R}}$:

$$(x^2 + y^2 + z^2 - R^2 - r^2)^2 - 4R^2(r^2 - x^2),$$

dove $0 < r < R$, e usando i piani $z = c$, mostrare che si tratta di curve di grado 4 e prevederne l'aspetto grafico.

6. Si verifichi che la cubica cuspidata proiettiva di equazione $x_0x_2^2 - x_1^3 = 0$ contiene un unico flesso.

   Si verifichi che la cubica nodata $x_0x_1x_2 - x_1^3 - x_2^3 = 0$ contiene tre flessi che risultano allineati.

7. **Curve iperellittiche**: Si dicono curve iperellittiche le curve proiettive di grado $d \geq 3$ che in una opportuna scelta di un riferimento si scrivono nella forma

$$x_0^{d-2}x_2^2 - p(x_0, x_1) = 0$$

dove $p(x_0, x_1) \in \mathbb{K}[x_0, x_1]_d$ è un polinomio omogeneo di grado d, ovvero nella forma affine

$$y^2 - p(x) = 0,$$

con $p(x)$ polinomio di grado $d \geq 3$.

Si preveda la traccia reale della curva. Si dimostri che l'unico punto improprio delle curve iperellittiche è singolare se e solo se $d > 3$, e che in ogni caso ha come unica tangente la retta impropria.

Infine, si dimostri che la curva iperellittica affine $y^2 - p(x) = 0$ ha punti singolari se e solo se il polinomio $p(x)$ ha radici multiple, e si faccia qualche esempio.

8. Sia C la curva proiettiva di $\mathbb{P}^2_{\mathbb{C}}$ di equazione

$$F(x_0, x_1, x_2) = x_0x_2^2 - x_1^3 + x_0x_1^2 + 5x_0^2x_1 - 5x_0^3 = 0$$

e sia $Q = (0 : 1 : 0)$. Si verifichi che C è non singolare e si determinino i punti $P \in C$ tali che la tangente a C in P passi per il punto Q.

9. Si consideri la curva C di $\mathbb{A}^2_{\mathbb{C}}$ di equazione

$$f(x, y) = x - xy^2 + 1 = 0\,.$$

a) Si determinino i punti singolari e gli asintoti di C.

b) Si determinino i punti di flesso della chiusura proiettiva di C, verificando che sono allineati, e si calcoli l'equazione di una retta che li contiene.

10. Al variare dei parametri $a, b \in \mathbb{C}$, si consideri la curva affine $C_{a,b}$ di equazione

$$f(x, y) = x^3 - 2ay^2 + bxy^2 = 0\,.$$

a) Si determinino i valori di a, b per cui la retta all'infinito e è tangente alla chiusura proiettiva $\bar{C}_{a,b}$ di $C_{a,b}$ e per ciascuno di tali valori si dica se $C_{a,b}$ è singolare nel punto di tangenza.

b) Si determinino, se esistono, $a, b \in \mathbb{C}$ tali che $C_{a,b}$ passi per il punto $(1, 2)$ con tangente $x - y + 1 = 0$.

11. Sia C una quartica irriducibile di $\mathbb{P}^2_{\mathbb{C}}$ avente 3 cuspidi. Si dimostri che le tre tangenti principali a C nei punti cuspidali appartengono a un fascio di rette.

12. Si implementi la formula di Kontsevich per curve algebriche piane razionali nel linguaggio di programmazione preferito (e.g. Sagemath, Python, ...) e si calcoli N_d per d più grande possibile.

10 Curva hessiana e punti di flesso

Vogliamo ora introdurre la nozione di punto di flesso; l'idea è di generalizzare i punti di flesso per grafici di funzioni di una variabile reale, nonché i punti di flesso di curve reali piane differenziabili, cioè punti con curvatura nulla.

L'esempio più semplice di punto di flesso è l'origine $(0,0) \in \mathbb{A}^2_{\mathbb{R}}$ per la curva piana di equazione

$$y - x^3 = 0\,.$$

Questa curva è grafico della funzione $f : \mathbb{R} \to \mathbb{R}$ data da $f(x) = x^3$.

Vediamo come possiamo studiare il punto di flesso da un punto di vista algebrico. Il punto $(0,0)$ è un punto non singolare per $Z(y - x^3)$; inoltre, la tangente in tale punto è la retta affine $y = 0$. Vediamo la molteplicità di intersezione tra la curva e la tangente:

$$\begin{cases} y - x^3 = 0 \\ y = 0 \end{cases} \iff x^3 = 0,$$

quindi la radice $x = 0$ è tripla; in altre parole, la retta tangente, che ha, per definizione, in generale molteplicità di intersezione ≥ 2 nel punto di tangenza, in questo caso interseca con una molteplicità maggiore. Questa semplice osservazione è il nostro punto di partenza.

Definizione 10.1. Un punto $q \in Z(f) \subset \mathbb{A}^2$, ovvero $Q \in Z_P(F) \subset \mathbb{P}^2$, si dice *punto di flesso* se

- q, ovvero Q, è un punto non singolare;
- $I_q(f, t_q(Z(f))) \geq 3$, ovvero $I_Q(F, \tau_Q(Z_P(F))) \geq 3$.

Esempio 10.2.

1. Se il grado $d = 1$, la curva $Z_P(F) = L$ è una retta; ogni $Q \in L$ è nonsingolare, e per ogni $Q \in L$ si ha $\tau_Q(L) = L$. Ricordiamo che per convenzione abbiamo

$$I_Q(L, \tau_Q L) = +\infty,$$

quindi ogni $Q \in L$ è un punto di flesso.

2. Sia $Z_P(F)$ una conica irriducibile e ridotta (i.e. integrale). Per il Teorema di Bézout, la molteplicità di intersezione totale tra una retta arbitraria e $Z_P(F)$ è 2; in particolare, per ogni $Q \in Z_P(F)$ si ha $I_Q(F, \tau_Q(Z_P(F))) = 2$, quindi le coniche integrali non hanno punti di flesso.

10.1 Curva hessiana e flessi

Vediamo ora una tecnica per determinare i punti di flesso di una curva proiettiva.

Definizione 10.3. Data $Z_P(F) \subset \mathbb{P}^2$, di grado $d \geq 2$. La *matrice hessiana* di F in $Q \in Z_P(F)$ è la matrice simmetrica delle derivate parziali seconde:

$$M_F(Q) = \begin{pmatrix} \partial_{x_0x_0}F(Q) & \partial_{x_0x_1}F(Q) & \partial_{x_0x_2}F(Q) \\ \partial_{x_0x_1}F(Q) & \partial_{x_1x_1}F(Q) & \partial_{x_1x_2}F(Q) \\ \partial_{x_0x_2}F(Q) & \partial_{x_1x_2}F(Q) & \partial_{x_2x_2}F(Q) \end{pmatrix}. \tag{10.1}$$

L'*hessiano* o *determinante hessiano* di F in Q è il determinante della matrice hessiana $H_F(Q) := \det M_F(Q)$.

Analogamente, la *matrice hessiana* di F (non valutata) è la matrice delle derivate parziali seconde $M_F = (\partial_{x_{i-1}}\partial x_{j-1})_{1\leq i,j\leq 3}$. Le sue entrate sono polinomi omogenei di grado $d-2 \geq 0$. L'*hessiano* è il polinomio $H_F = \det M_F$; se non è il polinomio nullo, è un polinomio omogeneo di grado $3(d-2)$.

Definizione 10.4. Sia $Z_P(F)$ una curva di grado $d \geq 3$ e supponiamo che l'hessiano H_F non sia il polinomio identicamente nullo. La *curva hessiana* è la curva proiettiva

$$Z_P(H_F) \subset \mathbb{P}^2.$$

Definizione 10.5. Sia $Z_P(F)$ una curva di grado $d \geq 3$. La *conica osculatrice* $\Gamma_F(Q)$ a $Z_P(F)$ in un punto nonsingolare $Q \in Z_P(F)$ è la conica proiettiva di equazione

$$\begin{pmatrix} x_0 & x_1 & x_2 \end{pmatrix} M_F(Q) \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}. \tag{10.2}$$

Osservazione 10.6. Si ha $Q \in \Gamma_F(Q)$. Infatti per l'identità di Eulero si ha che se $Q \in Z_P(F)$ liscio allora

$$\begin{aligned}
(\Gamma_F(Q))(Q) &= \begin{pmatrix} q_0 & q_1 & q_2 \end{pmatrix} M_F(Q) \begin{pmatrix} q_0 \\ q_1 \\ q_2 \end{pmatrix} \\
&= \sum_{i,j=0}^{2} \partial_{x_i x_j} F(Q) q_i q_j \\
&= \left(\sum_{j=0}^{2} \partial_{x_0 x_j} F(Q) q_j \right) q_0 + \cdots + \left(\sum_{j=0}^{2} \partial_{x_2 x_j} F(Q) q_j \right) q_2 \\
&= (d-1)\partial_{x_0} F(Q) q_0 + \cdots + (d-1)\partial_{x_2} F(Q) q_2 \\
&= (d-1) \sum_{j=0}^{2} \partial_{x_j} F(Q) q_j \\
&= (d-1) d \; F(Q) = 0.
\end{aligned}$$

Osservazione 10.7. Nel caso reale $\mathbb{K} = \mathbb{R}$, si può verificare che $Z(aF)$ e $\Gamma_F(Q) \cap U_0$ hanno la stessa curvatura in Q.

Proposizione 10.8. *Sia $Z_P(F)$ una curva di grado $d \geq 3$. Un punto non singolare $Q \in Z_P(F)$ è un punto di flesso se e solo se $\Gamma_F(Q)$ è degenere.*

Inoltre, in questo caso, una delle componenti di $\Gamma_F(Q)$ è la retta tangente $\tau_Q(Z_P(F))$.

Dimostrazione. Supponiamo che $Q = (q_0 : q_1 : q_2) \in Z_P(F)$ sia un punto di flesso e sia $R = (r_0 : r_1 : r_2) \in \tau_Q(Z_P(F))$ un punto della retta tangente con $R \neq Q$; allora il generico punto di $\tau_Q(Z_P(F))$ si può esprimere come $\lambda Q + \mu R$. Usiamo ora la formula di Taylor omogenea:

$$\begin{aligned}
G(\lambda, \mu) = F(\lambda Q + \mu R) = F(Q)\lambda^d + (\sum_{i=0}^{2} \partial_{x_i} F(Q) r_i) \lambda^{d-1} \mu \\
+ \left(\frac{1}{2} \sum_{i,j=0}^{2} \partial_{x_i x_j} F(Q) r_i r_j \right) \lambda^{d-2} \mu^2 + \ldots \quad (10.3)
\end{aligned}$$

Siccome $Q \in Z_P(F)$, il primo termine $F(Q) = 0$. Inoltre, la retta tangente $\tau_Q(F)$ ha equazione ${}^t\nabla F(Q) \cdot \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} = 0$, e avendo $R \in \tau_Q(F)$, anche il secondo termine si

annulla. Infine, siccome Q è un punto di flesso, si ha $I_Q(F, \tau_Q(F)) \geq 3$, cioè la coppia $(\bar{\lambda} : \bar{\mu}) = (1 : 0)$ è una radice di $G(\lambda, \mu)$ di molteplicità almeno 3; questa condizione è verificata se e solo se $\sum_{i,j=0}^{2} \partial_{x_i x_j} F(Q) r_i r_j = 0$, cioè $R \in \Gamma_F(Q)$. Siccome questo deve valere per ogni punto $R \in \tau_Q(F)$ con $R \neq Q$, otteniamo che la retta tangente $\tau_Q(F) \subseteq \Gamma_F(Q)$. In particolare, la conica osculatrice $\Gamma_F(Q)$ è degenere.

Viceversa, supponiamo che Q sia non singolare e che $\Gamma_F(Q)$ sia degenere. Se dimostriamo che $\tau_Q(Z_P(F)) \subseteq \Gamma_F(Q)$, dalla (10.3) si avrà che $I_Q(F, \tau_Q(Z_P(F)) \geq 3$, e quindi che Q è un flesso.

Ricordiamo ora la retta tangente in un punto non singolare Q di una conica di equazione

$$\begin{pmatrix} x_0 & x_1 & x_2 \end{pmatrix} A \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}$$

ha equazione

$$\begin{pmatrix} q_0 & q_1 & q_2 \end{pmatrix} A \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}.$$

Quindi, se Q è non singolare per $\Gamma_F(Q)$, la retta $\tau_Q \Gamma_F(Q)$ ha equazione

$$\begin{pmatrix} q_0 & q_1 & q_2 \end{pmatrix} M_F(Q) \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix}.$$

Usando l'identità di Eulero otteniamo:

$$\begin{aligned}
\begin{pmatrix} q_0 & q_1 & q_2 \end{pmatrix} M_F(Q) \begin{pmatrix} x_0 \\ x_1 \\ x_2 \end{pmatrix} &= \sum_{i,j=0}^{2} \partial_{x_i x_j} F(Q) q_i x_j \\
&= \left(\sum_{j=0}^{2} \partial_{x_0 x_j} F(Q) q_j \right) x_0 + \left(\sum_{j=0}^{2} \partial_{x_1 x_j} F(Q) q_j \right) x_1 + \left(\sum_{j=0}^{2} \partial_{x_2 x_j} F(Q) q_j \right) x_2 \\
&= (d-1)\partial_{x_0} F(Q) x_0 + (d-1)\partial_{x_1} F(Q) x_1 + (d-1)\partial_{x_2} F(Q) x_2 \\
&= (d-1) \sum_{j=0}^{2} \partial_{x_j} F(Q) x_j,
\end{aligned}$$

che è anche l'equazione della retta tangente $\tau_Q(Z_P(F))$. Infine, una conica degenere contiene tutte le sue rette tangenti.

Se Q è invece singolare per $\Gamma_F(Q)$, allora sia $R = (r_0 : r_1 : r_2) \in \tau_Q(Z_P(F))$. Si ha

$$0 = (d-1)\left(\sum_{j=0}^{2} \partial_{x_j} F(Q) r_j\right) = \sum_{i,j=0}^{2} \partial_{x_i x_j} F(Q) q_i r_j,$$

quindi $Q \in \tau_R \Gamma_F(Q)$; ma per un conica degenere con punto singolare Q, la retta tangente $\tau_R \Gamma_F(Q)$ è semplicemente la retta QR, che nel nostro caso coincide con $\tau_Q(Z_P(F))$, ed è una componente di $\Gamma_F(Q)$. □

Teorema 10.9. *Sia F un polinomio omogeneo di grado $d \geq 3$, non necessariamente irriducibile né ridotto. Allora si ha*

$$Z_P(F) \cap Z_P(H_F) = \mathrm{Sing} Z_P(F) \cup \{\textit{flessi di } Z_P(F)\}. \tag{10.4}$$

Dimostrazione. Supponiamo che $Q \in \mathrm{Sing} Z_P(F)$, quindi $\nabla F(Q) = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$. Conseguentemente abbiamo

$$\begin{aligned}
0 &= (d-1)\partial_{x_0} F(Q) = q_0 \partial_{x_0 x_0} F(Q) + q_1 \partial_{x_0 x_1} F(Q) + q_2 \partial_{x_0 x_2} F(Q), \\
0 &= (d-1)\partial_{x_1} F(Q) = q_0 \partial_{x_1 x_0} F(Q) + q_1 \partial_{x_1 x_1} F(Q) + q_2 \partial_{x_1 x_2} F(Q), \\
0 &= (d-1)\partial_{x_2} F(Q) = q_0 \partial_{x_2 x_0} F(Q) + q_1 \partial_{x_2 x_1} F(Q) + q_2 \partial_{x_2 x_2} F(Q),
\end{aligned}$$

quindi $(q_0, q_1, q_2) \in \ker M_F(Q)$ ed è un vettore non nullo. Ne segue che $M_F(Q)$ è una matrice degenere, da cui otteniamo che Q annulla il determinante hessiano.

Se Q è un flesso, dalla Proposizione 10.8 sappiamo che la conica osculatrice è degenere, quindi in particolare il determinante hessiano si annulla in Q.

Viceversa, sia $Q \in Z_P(F) \cap Z_P(H_F)$. Se Q è singolare, la tesi è verificata. Se Q è non singolare, siccome annulla il determinante hessiano, la conica osculatrice $\Gamma_F(Q)$ è degenere, quindi concludiamo che Q è un flesso, sempre per la Proposizione 10.8. □

Corollario 10.10. *Su un campo algebricamente chiuso $\mathbb{K} = \bar{\mathbb{K}}$ sia $Z_P(F) \subset \mathbb{P}^2_{\mathbb{K}}$ liscia curva proiettiva di grado $d \geq 3$. Allora:*

$$1 \leq \left|\{\textit{flessi di } Z_P(F)\}\right| \leq 3d(d-2).$$

Dimostrazione. Siccome $Z_P(F) \cap Z_P(H_F) \neq \emptyset$ e $\mathrm{Sing} Z_P(F) = \emptyset$ per ipotesi di liscezza, per la proposizione precedente deve esistere almeno un punto di flesso. D'altra parte

l'Hessiano è dato dal determinante di una matrice $3x3$ nelle derivate doppie di F, che hanno quindi grado omogeneo $(d-2)$ e quindi $deg(H_F) = 3(d-2)$ mentre $deg(F) = d$. Siccome il campo è algebricamente chiuso e per liscezza non possiamo avere componenti irriducibili comuni tra $Z_P(F)$ e $Z_P(H_F)$, per il Teorema di Bézout si ha che $Z_P(F) \cap Z_P(H_F)$ consta al più di un numero di punti pari al prodotto dei gradi, ovvero $3d(d-2)$. Applicando di nuovo la proposizione precedente conclude la dimostrazione. □

Osservazione 10.11. Se due curve sono proiettivamente equivalenti, allora hanno matrici hessiane simili (esercizio).

Osservazione 10.12. Se $Z_P(F)$ è un'unione di rette tutte passante per un punto fissato S, allora il determinante hessiano è identicamente nullo. Infatti, a meno di proiettività possiamo supporre che $S = (1:0:0)$. Quindi F è del tipo

$$F = \Pi_{i=1}^{d}(\alpha_i x_1 + \beta_i x_2),$$

e la matrice hessiana ha la forma

$$\begin{pmatrix} 0 & 0 & 0 \\ 0 & \partial_{x_1x_1}F & \partial_{x_1x_2}F \\ 0 & \partial_{x_1x_2}F & \partial_{x_2x_2}F \end{pmatrix}.$$

Vale anche il viceversa del fatto appena visto:

Teorema 10.13 (Teorema di Gordan-Noether)**.** *Sia $\mathbb{K} = \bar{\mathbb{K}}$ un campo algebricamente chiuso. Una curva $Z_P(F) \subset \mathbb{P}^2$ verifica $H_F \equiv 0$ se e solo se è unione di d rette passanti per un punto S.*

Dimostrazione. Omessa. □

Osservazione 10.14. In generale, ogni cono in $\mathbb{P}^n$, cioè ogni ipersuperficie che sia unione di rette tutte passanti per un punto $S \in \mathbb{P}^n$, ha determinante hessiano identicamente nullo.

Il matematico Ludwig Otto Hesse congetturò che queste fossero tutte e solo le ipersuperfici a hessiano nullo. I matematici Gordan e Noether dimostrarono che la congettura è vera in $\mathbb{P}^2$ e $\mathbb{P}^3$, mentre non è più vera se $n \geq 4$. Un controesempio in $\mathbb{P}^4$ è dato dalla *cubica di Perazzo* di equazione

$$x_0x_3^2 + 2x_1x_3x_4 + x_2x_4^2 = 0\,.$$

Chiaramente il suo luogo degli zeri non è una unione di rette per un punto e

$$\det \begin{pmatrix} 0 & 0 & 0 & 2x_3 & 0 \\ 0 & 0 & 0 & 2x_4 & 2x_3 \\ 0 & 0 & 0 & 0 & 2x_4 \\ 2x_3 & 2x_4 & 0 & 2x_0 & 2x_1 \\ 0 & 2x_3 & 2x_4 & 2x_1 & 2x_2 \end{pmatrix} = 0,$$

come può essere notato direttamente dalla sottomatrice nulla 3×3 di una matrice 5×5: ogni permutazione nella definizione di determinante deve contenere almeno uno degli elementi della matrice 3×3 e quindi contribuisce zero alla somma.

10.2 Esercizi

1. Fascio di cubiche di Hesse.

   Si consideri il fascio

   $$\mathcal{F} := \{C_{\lambda,\mu} \mid (\lambda : \mu) \in \mathbb{P}^1_{\mathbb{C}}\},$$

   dove $C_{\lambda,\mu} \subset \mathbb{P}^2_{\mathbb{C}}$ è la cubica di equazione

   $$F_{\lambda\mu}(x_0, x_1, x_2) = \lambda(x_0^3 + x_1^3 + x_2^3) + \mu x_0 x_1 x_2 = 0.$$

   a) Si trovino i punti base di $\mathcal{F}$ e si verifichi che ciascuno di essi è non singolare per ogni $C_{\lambda,\mu}$.

   b) Si mostri che per ogni $(\lambda : \mu) \in \mathbb{P}^1_{\mathbb{C}}$, la curva Hessiana $H(C_{\lambda,\mu})$ di $C_{\lambda,\mu}$ è definita ed appartiene al fascio $\mathcal{F}$.

   c) Si consideri l'applicazione

   $$H \colon \mathcal{F} \to \mathcal{F}, \qquad C_{\lambda,\mu} \to H(C_{\lambda,\mu}).$$

   Si dimostri che H ha quattro punti fissi e che non è una proiettività.

   d) Si determinino i flessi di $C_{\lambda,\mu}$, quando $C_{\lambda,\mu}$ non è un punto fisso per H.

2. Si verifichi che la cubica di Perazzo ha determinante hessiano identicamente nullo.

3. Si calcoli il determinante hessiano della cubica piana di equazione $x_0 x_1 x_2 = 0$. Cosa notate?

11 Cubiche piane proiettive

In questo ultimo capitolo studieremo le cubiche piane proiettive irriducibili, vedremo prima la loro classificazione sia nel caso liscio che singolare, e poi la legge di gruppo algebrico che si può ad esse associare nel caso liscio.

11.1 Classificazione delle cubiche piane irriducibili

In questa sezione ci occupiamo della questione della classificazione proiettiva delle cubiche piane irriducibili nel piano proiettivo, sul campo complesso $\mathbb{C}$. Ricordiamo che nel caso delle coniche piane, la classificazione consiste in un numero finito di casi, uno per ogni valore del rango della matrice simmetrica associata alla conica.

Il caso delle cubiche singolari avremo effettivamente un caso per tipo di singolarità, mentre per le cubiche non singolari la situazione è molto diversa: si hanno infinite classi proiettive, tante quante il campo dei numeri complessi.

Definizione 11.1. Si definisca j, detta *modulo*, come la funzione razionale complessa

$$\begin{aligned} j\colon \mathbb{C} \setminus \{0,1\} &\to \mathbb{C} \\ c &\mapsto \frac{(c^2-c+1)^3}{c^2(c-1)^2} \end{aligned}$$

Sia $C \subset \mathbb{P}^2_{\mathbb{C}}$ una cubica non singolare della forma

$$x_0x_2^2 - x_1(x_1-x_0)(x_1-cx_0) = 0, \qquad y^2 = x(x-1)(x-c), \qquad c \in \mathbb{C}\setminus\{0,1\} \quad (11.1)$$

L'equazione (11.1) si chiama *forma o rappresentazione di Legendre*.

Il *modulo* o *invariante j* della curva C è definito come il numero complesso

$$j(C) := j(c) \in \mathbb{C}.$$

Proposizione 11.2. *La funzione j è suriettiva e la sua fibra è data da*

$$j^{\leftarrow}(j(c)) = \left\{c, \frac{1}{c}, 1-c, \frac{1}{1-c}, \frac{c-1}{c}, \frac{c}{c-1}\right\}, \qquad c \in \mathbb{C} \setminus \{0,1\}.$$

Dimostrazione. Fissiamo $\bar{\jmath} \in \mathbb{C}$, e consideriamo il polinomio

$$Q(x) = (x^2 - x + 1)^3 - \bar{\jmath}x^2(x-1)^2 \in \mathbb{C}[x]\,.$$

Essendo $\mathbb{C}$ algebricamente chiuso, $Q(x)$ possiede almeno una radice c; ma dire che $Q(c) = 0$ equivale a $(c^2 - c + 1)^3 - \bar{\jmath}c^2(c-1)^2 = 0$, cioè $\bar{\jmath} = j(c)$. Verifichiamo, infine, che $c \neq 0$ e $c \neq 1$; infatti si ha

$$Q(0) = 1 = Q(1)\,,$$

quindi 0 e 1 non sono mai radici di Q, i.e. j è suriettiva. Si noti che Q ha grado sei in un campo algebricamente chiuso e quindi ha sei radici contate con molteplicità. E' facile vedere che i sei valori elencati soddisfano il polinomio. □

Esempio 11.3. Genericamente la fibra di j ha cardinalità sei, ma per alcuni valori di c i valori della preimmagine possono coincidere, ad esempio $j^{\leftarrow}\left(j(\frac{1}{2})\right) = \left\{\frac{1}{2}, 1, 2\right\}$.

Siamo ora pronti per enunciare il teorema di classificazione delle cubiche irriducibili. Le cubiche riducibili sono già classificate grazie alla classificazione delle coniche.

Teorema 11.4 (Classificazione delle cubiche irriducibili piane proiettive)**.**

- ***Caso liscio**. Ogni cubica piana liscia C è proiettivamente equivalente ad una cubica in forma di Legendre*

$$x_0x_2^2 - x_1(x_1 - x_0)(x_1 - cx_0) = 0, \qquad y^2 = x(x-1)(x-c), \tag{11.2}$$

per un certo $c \in \mathbb{C} \setminus \{0,1\}$.

Quindi possiamo associare ad ogni cubica piana liscia un modulo $j(c)$ come il modulo della curva in forma di Legendre a cui è equivalente.

In aggiunta, C è proiettivamente equivalente a tutte le cubiche in forma di Legendre con parametro c' per ogni elemento nella fibra di c

$$c' \in j^{\leftarrow}(j(c))\,.$$

In altre parole, due cubiche lisce piane proiettive C e C' sono proiettivamente equivalenti se e soltanto se hanno lo stesso modulo $j(c) = j(c')$. Quindi l'insieme quoziente che

parametrizza le classi di equivalenza proiettive delle cubiche piane lisce è $(\mathbb{C} \setminus \{0,1\})/j$*, che abbiamo visto essere in biezione con* $\mathbb{C}$ *perché j è suriettiva.*

Inoltre, C possiede esattamente 9 flessi a tre a tre allineati, i.e. ogni retta che ne contiene due ne contiene un terzo.

- ***Caso nodo ordinario****. Tutte le cubiche piane nodate sono proiettivamente equivalenti. In particolare, un rappresentante di questa classe è*

$$x_0x_2^2 - x_1^2(x_1 - x_0) = 0, \qquad y^2 = x^2(x-1) \tag{11.3}$$

Inoltre, le cubiche nodate hanno tre flessi allineati.

- ***Caso cuspide ordinaria****. Tutte le cubiche piane cuspidate sono proiettivamente equivalenti. In particolare, un rappresentante di questa classe è*

$$x_0x_2^2 - x_1^3, \qquad y^2 = x^3. \tag{11.4}$$

Inoltre, le cubiche cuspidate hanno un unico punto di flesso.

Dimostrazione del caso liscio. Per ipotesi l'insieme delle singolarità è l'insieme vuoto, quindi per il teorema 10.9 esiste almeno un punto di flesso P, che possiamo mappare con una proiettività nel punto $(0:0:1)$ con tangente $x_0 = 0$. In coordinate affini nella carta affine $U_0 \cong \mathbb{A}^2_{\mathbb{C}}$ abbiamo

$$aF(x,y): \ y^2 + bxy + cy = g_1(x), \quad \deg(g_1) = 3.$$

Applicando l'affinità

$$\begin{cases} x &= X \\ y &= Y - \frac{b}{2}X - \frac{c}{2} \end{cases}$$

si ottiene

$$aF(X,Y): \ Y^2 = a(X-\alpha_1)(X-\alpha_2)(X-\alpha_3), \qquad a \neq 0, \ \ \alpha_i \text{ distinti.}$$

Infatti se a fosse nullo oppure se due radici di $alpha_i$ e $alpha_j$ fossero uguali, la curva sarebbe singolare.

Applicando una seconda affinità

$$\begin{cases} X &= (\alpha_2 - \alpha_1)X' + \alpha_1 \\ Y &= \sqrt{a(\alpha_2 - \alpha_1)^3}Y' \end{cases}$$

si ottiene

$$aF(X',Y'):\ (Y')^2 = X'(X'-1)(X'-c), \qquad c := \frac{\alpha_3-\alpha_1}{\alpha_2-\alpha_1}.$$

Si osservi che

$$\begin{cases} c=0 & \text{iff} \quad \alpha_1=\alpha_3, \\ c=1 & \text{iff} \quad \alpha_2=\alpha_3, \\ c=\infty & \text{iff} \quad \alpha_1=\alpha_2. \end{cases}$$

Questo dimostra che ogni cubica liscia è proiettivamente equivalente ad una in forma di Legendre per un certo $c \in \mathbb{C}\setminus\{0,1\}$. Dimostriamo ora che questa forma di Legendre è proiettivamente equivalente a qualsiasi altra forma di Legendre con parametro c' nella stessa fibra

$$j^{\leftarrow}(j(c)) = \left\{c, \frac{1}{c}, 1-c, \frac{1}{1-c}, \frac{c-1}{c}, \frac{c}{c-1}\right\}, \qquad c \in \mathbb{C}\setminus\{0,1\}. \tag{11.5}$$

Si osservi che se $c' = c$ non c'è nulla da dimostrare, e che è sufficiente esibire due affinità Φ e Ψ che trasformino il parametro della forma di Legendre affine come $c \mapsto \frac{1}{c}$ e $c \mapsto 1-c$, rispettivamente, in quanto gli altri valori $c' \in \{\frac{1}{1-c}, \frac{c}{c-1}, \frac{c-1}{c}\}$ si possono ottenere semplicemente componendo Φ e Ψ in modo opportuno.

Le affinità cercate sono date dalle seguenti equazioni:

$$\Phi\colon \begin{cases} x &= cX \\ y &= c^{3/2}Y \end{cases}, \qquad \Psi\colon \begin{cases} x &= -X+1 \\ y &= iY \end{cases}.$$

Questo conclude la dimostrazione del caso liscio, a parte lo studio dei flessi. Siccome le proiettività preservano le molteplicità di intersezione, preservano anche il numero di flessi e le loro posizioni relative, ovvero la proprietà di essere allineati a tre a tre. Perciò è sufficiente calcolare i flessi di una qualunque forma di Legendre e dimostrarne l'allineamento a tre a tre. Quindi basta calcolare e studiare le coordinate degli zeri del determinante della matrice Hessiana di una forma di Legendre. Lasciamo questo calcolo al lettore per esercizio. Questo conclude la dimostrazione del caso liscio. □

Dimostrazione del caso nodato. La dimostrazione del caso nodato segue la stessa idea del caso liscio. A meno di proiettività possiamo assumere che il nodo abbia coordinate proiettive $(1:0:0)$ e che le tangenti siano sugli assi x_1 e x_2, rispettivamente. Nella carta affine $U_0 \cong \mathbb{A}^2_{\mathbb{C}}$ avremo:

$$aF(x,y):\ xy + ax^3 + bx^2y + cxy^2 + dy^3 = 0.$$

Per ipotesi di irriducibilità abbiamo che $a, d \neq 0$. Omogeneizzando rispetto a x_0 troviamo:

$$F(x_0, y_0, z_0) : \; x_0 x_1 x_2 + a x_1^3 + b x_1^2 x_2 + c x_1 x_2^2 + d x_2^3 = 0.$$

La proiettività

$$T : \begin{cases} x_0 &= d^{-\frac{1}{3}} y_0 \\ x_1 &= a^{-\frac{1}{3}} y_1 \\ x_2 &= -c \cdot d^{-\frac{1}{3}} y_0 - b \cdot a^{-\frac{1}{3}} y_1 + (ad)^{\frac{1}{3}} y_2 \end{cases} .$$

porta l'equazione nella forma del rappresentante nodato scelto in equazione 11.3. Questo dimostra le prime due proposizioni dell' enunciato. Per lo studio dei flessi è sufficiente calcolare la matrice Hessiana

$$M = \begin{pmatrix} 0 & x_1 & x_1 \\ x_2 & 6x_1 & x_0 \\ x_1 & x_0 & 6x_2 \end{pmatrix}$$

e il suo determinante, l'Hessiano, che si annulla nei tre punti

$$[0 : e^{i\frac{k\pi}{3}} : 1], \qquad k = 1, 3, 5.$$

I tre flessi sono chiaramente allineati. Questo conclude la dimostrazione del caso nodato. □

Dimostrazione del caso cuspidato. La dimostrazione del caso cuspidato segue la stessa idea del caso liscio. A meno di proiettività possiamo assumere che la cuspide abbia coordinate proiettive $(1 : 0 : 0)$ e che l'unica tangente doppia sia sull'asse x_1. Nella carta affine $U_0 \cong \mathbb{A}^2_{\mathbb{C}}$ avremo:

$$aF(x, y) : \; y^2 + a x^3 + b x^2 y + c x y^2 + d y^3 = 0.$$

Per ipotesi di irriducibilità abbiamo che $a \neq 0$. Omogeneizzando rispetto a x_0 troviamo:

$$F(x_0, y_0, z_0) : \; x_0 x_2^2 + a x_1^3 + b x_1^2 x_2 + c x_1 x_2^2 + d x_2^3 = 0.$$

Le proiettività

$$T : \begin{cases} x_0 &= y_0 \\ x_1 &= y_1 - \frac{b}{3a} y_0 \\ x_2 &= y_2 + \left(\frac{b^2}{3a} - c \right) y_1 \end{cases} , \qquad S : \begin{cases} y_0 &= z_0 \\ y_1 &= -a^{-\frac{1}{3}} z_1 \\ y_2 &= z_2 - \left([y_0^3] T(F) \right) z_0 \end{cases} ,$$

portano l'equazione nella forma del rappresentante cuspidato scelto in Equation (11.4), dove $[y_0^3]$ è l'operatore che selezione il coefficiente del monomio y_0^3 nel polinomio a cui viene applicato. Questo dimostra le prime due proposizioni dell' enunciato. Si calcoli per esercizio l'unico punto che annulla il determinante della matrice Hessiana. Questo conclude la dimostrazione del caso cuspidato. □

11.2 Struttura di gruppo abeliano su cubiche non singolari

In questa sezione vediamo che una curva ellittica si può dotare di una operazione binaria in modo tale che diventi un gruppo abeliano. Questa è una caratteristica molto speciale per un oggetto geometrico e dipendende intrinsicamente dal fatto che il grado della curva sia tre, ovvero uguale al numero totale di elementi del dominio e del codominio richiesti per una operazione binaria. La liscezza e la struttura dei flessi garantiscono che le proprietà di gruppo abeliano siano soddisfatte.

Definizione 11.5. Si considerino due punti distinti A e B sulla curva ellittica $\mathscr{C}$. Per il Teorema di Bézout l'unica retta che passa per A e B interseca la curva $\mathscr{C}$ anche in un terzo punto con molteplicità, ovvero il terzo punto potrebbe coincidere con A o con B, in tal caso la retta sarebbe tangente a quel punto. Nello stesso modo, il punto A e il punto B potrebbero coincidere, nel qual caso possiamo scegliere la retta per A come la tangente alla curva $\mathscr{C}$ passante per il punto A. In ogni caso chiamiamo questo terzo punto di intersezione $R(A, B)$. Questo definisce un'operazione binaria R su $\mathscr{C}$.

$$\begin{aligned} R : \mathscr{C} \times \mathscr{C} &\to \mathscr{C} \\ (A, B) &\mapsto R(A, B) \end{aligned}$$

Chiaramente R è un'operazione commutativa perchè la retta che unisce i punti scelti non dipende dal loro ordine. Inoltre, è chiaro per la definizione di flesso e dal Teorema di Bézout che $R(A, A) = A$ se e soltanto se A è un punto di flesso per la curva ellittica $\mathscr{C}$.

Si fissi O uno dei 9 punti di flesso disponibili su $\mathscr{C}$. Si definisca l'operazione binaria $+$ su $\mathscr{C}$, come il risultato dell'operazione R tra due punti della curva, ulteriormente

applicata al flesso di riferimento O.

$$\begin{aligned} + : \mathscr{C} \times \mathscr{C} &\to \mathscr{C} \\ (A, B) &\mapsto R(R(A, B), O) \end{aligned}$$

Teorema 11.6. *La struttura algebrica $(\mathscr{C}, +, O)$ è un gruppo abeliano.*

Dimostrazione. Studiamo una alla volta le proprietà necessarie per promuovere $(\mathscr{C}, +, O)$ a gruppo abeliano.

- **Chiusura dell'operazione**. La chiusura di $+$ segue dalla chiusura di R, infatti dalla definizione
$$A + B := R(R(A, B), O)$$
l'operazione $+$ è definita in termini di due applicazioni dell'operazione R.
La struttura algebrica $(\mathscr{C}, +, O)$ è quindi promossa a magma algebrico.
- **Commutatività**. La commutatività di $+$ segue dalla commutatività di R:
$$A + B := R(R(A, B), O) = R(R(B, A), O) =: B + A.$$
La struttura algebrica $(\mathscr{C}, +, O)$ è quindi promossa a magma algebrico abeliano.
- **Associatività**. La dimostrazione dell'associatività è la parte non banale, e utilizzeremo il Teorema 8.15 con $d = 3$ ed $n = 1$.
Si osservi che è sufficiente dimostrare che per tre punti non necessariamente distinti A, B, C appartenenti alla curva ellittica $\mathscr{C}$ si abbia
$$R(A + B, C) = R(A, B + C). \tag{11.6}$$
Infatti applicando l'operazione $R(\bullet, O)$ da entrambi i lati si ottiene:
$$(A + B) + C = A + (B + C). \tag{11.7}$$
L'idea chiave ora è definire la cubica completamente riducibile D come l'unione di tre rette:
$$D := L_{A,B} \cup L_{A+B,C} \cup L_{O,B+C}$$
Dunque D interseca $\mathscr{C}$ nei seguenti nove punti:

$$\mathscr{C} \cap D := \{O, A, B, C, A+B, B+C, R(A,B), R(B,C), R(A+B,C)\}. \tag{11.8}$$

Dimostreremo l'equazione 11.6 assumendo che i nove punti in 11.8 siano distinti. Questa condizione è genericamente verificata, lasciamo al lettore la verifica nel caso degenere.

Osserviamo ora che $B, C, R(B,C)$ sono allineati. Quindi per il Teorema 8.15 con $d = 3$ e $n = 1$ dato che $|\mathscr{C} \cap D| = 9 = d^2$ e $n \cdot d = 3$ giacciono su una curva irriducibile di grado $n = 1$, ovvero una retta, allora i restanti punti

$$\mathscr{C} \cap D := \{O, A, A+B, B+C, R(A,B), R(A+B,C)\} \tag{11.9}$$

devo giacere su di una conica. D'altra parte $O, R(A,B), A+B = R(R(A,B),O)$ sono allineati, per cui la conica è necessariamente degenere e anche i restanti punti $A, B+C, R(A+B,C) \in \mathscr{C}$ sono allineati. Questo conclude la dimostrazione, perché dati i due punti $A, B+C$ su $\mathscr{C}$ esiste un unico terzo punto di intersezione con la retta $L_{A,B+C}$ su $\mathscr{C}$, e questo punto è per definizione $R(A, B+C)$. Quindi dobbiamo avere che i due punti coincidono, ovvero $R(A+B,C) = R(A,B+C)$.

La struttura algebrica $(\mathscr{C}, +, O)$ è quindi promossa a semigruppo abeliano.

- **Esistenza dell'elemento neutro**. Si noti che per un punto $A \in \mathscr{C}$ diverso dal flesso O si ha per definizione di R:

$$A + O = O + A = R(R(O,A),O) = A.$$

Per $A = O$ invece si osservi che $R(O,O) = O$ perché O è un flesso, e dunque $O + O = R(R(O,O),O) = O$.

La struttura algebrica $(\mathscr{C}, +, O)$ è quindi promossa a monoide abeliano.

- **Esistenza dell'elemento inverso**. Basta definire $-A := R(A,O)$. Allora

$$A + (-A) = R(R(A, R(A,O)),O) = R(O,O) = O.$$

La struttura algebrica $(\mathscr{C}, +, O)$ è quindi promossa a gruppo abeliano.

□

Osservazione 11.7. Per il teorema di classificazione delle cubiche piane irriducibili proiettive, caso liscio, le curve ellittiche hanno 9 flessi distinti, a tre a tre allineati. Ci sono in particolare 9 strutture di gruppo abeliano su ogni curva ellittica.

Proposizione 11.8. *Siano O e O' due flessi distinti della curva ellittica $\mathscr{C}$, e siano $(\mathscr{C}, +, O)$ e $(\mathscr{C}, +', O')$ le due strutture di gruppo abeliano associate. Allora*

$$A +' B = A + B - O'. \tag{11.10}$$

In particolare, $(\mathscr{C}, +, O)$ e $(\mathscr{C}, +', O')$ sono gruppi isomorfi, e quindi lo sono le nove strutture algebriche di gruppo su $\mathscr{C}$.

Dimostrazione. La dimostrazione è lasciata come esercizio al lettore. □

11.3 Esercizi

1. Si dimostri che ogni cubica non singolare ha nove flessi a tre a tre allineati.
2. Si dimostri che ogni cubica cuspidata ha esattamente un flesso.
3. Si dimostri che se $c = 0$ oppure $c = 1$ nell'equazione (11.1), allora la cubica è singolare.
4. Si trovino tutti i valori complessi c tali che il numero di elementi distinti della sua fibra sia strettamente minore di sei.
5. Si dimostri che le nove strutture di gruppo abeliano su una curva ellittica sono isomorfe come gruppi algebrici.
6. Si illustrino le proprietà delle operazioni R e $+$ su una cubica singolare irriducibile, e poi su una cubica riducibile.
7. Si illustrino i dettagli della dimostrazione della associatività di $+$ nel caso alcuni dei nove punti di intersezione coincidano.