Un'introduzione alla geometria algebrica.
(1a versione preliminare)

Ph. Ellia

Printed:

17-5-2005

Indice

CAPITOLO II

Insiemi algebrici proiettivi.

1. Il proiettivo: come e perché.

Consideriamo l'intersezione di una retta e di una conica (per esempio un'ellisse) nel piano. Chiaramente abbiamo al più due punti d'intersezione. Se invece consideriamo l'intersezione di una retta con una cubica, al più tre punti; di due coniche, al più quattro punti, ecc. Questo ci porta naturalmente al problema seguente: in quanti punti s'intersecano due curve algebriche piane, C, C'? Per esempio se C' è la retta $y = 0$ e se C è la curva di equazione $y - f(x) = 0$ dove f è un polinomio di grado n, allora sappiamo che:

(i) se $k = \mathbb{R}$, $\#(C \cap C') \leq n$,

(ii) se $k = \mathbb{C}$, C e C' s'intersecano in n punti, purché contati con molteplicità (teorema fondamentale dell'algebra).

Il secondo enunciato è chiaramente più soddisfacente del primo, e siamo indotti a chiederci se vale in generale.

Se $C \subseteq \mathbb{A}^2(k)$ ha equazione $f(x, y) = 0$, il grado di C ($\deg(C)$) è il grado massimo di un monomio di $f(x, y)$. La generalizzazione di (ii) è: due curve piane di gradi rispettivi d, d', s'intersecano in $d.d'$ punti, contati con molteplicità.

In tutta generalità, questo enunciato è falso. Ecco alcuni controesempi:

(1) Se k non è algebricamente chiuso può essere $C = \emptyset$. Per esempio $\mathbf{V}(X^2 + Y^2 + 1) = \emptyset$ in $\mathbb{R}^2$. Quindi, come al solito, dobbiamo assumere k algebricamente chiuso.

(2) Le due curve possono avere una componente comune, e l'intersezione sarà un insieme infinito ($C = \mathbf{V}(XY)$ e $C' = \mathbf{V}(X(Y - 1))$) hanno in comune l'asse degli y). Dobbiamo quindi assumere le due curve senza componenti comuni.

(3) Malgrado tutte queste precauzioni (k algebricamente chiuso; C, C' senza componenti comuni) l'enunciato è sempre falso: due rette parallele in $\mathbb{C}^2$ non s'intersecano! Analogamente l'iperbole $\mathbf{V}(XY - 1)$ non interseca il suo asintoto $X = 0$. È proprio per rimediare a queste situazioni che si introduce il piano proiettivo, $\mathbb{P}^2(\mathbb{C})$. Il piano proiettivo può essere visto come il piano affine completato da una "retta all'infinito". Le due rette parallele nel piano affine s'incontrano in un punto della "retta all'infinito",

l'iperbole e l'asintoto sono tangenti in un punto della "retta all'infinito". In effetti nel piano proiettivo, su un campo algebricamente chiuso, abbiamo l'enunciato ideale ("teorema di Bezout"):

Teorema 1.1: *Siano $C, C' \subseteq \mathbb{P}^2(k)$ (k algebricamente chiuso), due curve piane di gradi rispettivi d, d'. Se C e C' non hanno componenti comuni, il numero di punti di intersezione di C e C', contato con molteplicità, è uguale a $d.d'$.*

Questo risultato è fondamentale per la geometria algebrica. Si generalizza poi in varie direzioni.

La difficoltà maggiore nella dimostrazione del teorema di Bezout è di definire in modo adeguato la molteplicità d'intersezione di due curve in un punto (cosa che noi sappiamo fare solo se una delle due curve è una retta). Tanto per avere un'idea del problema il lettore potrà considerare le curve $C = \mathbf{V}((X^2+Y^2)^2+3X^2Y-Y^3)$ (trifolium), $C' = \mathbf{V}((X^2+Y^2)^3-4X^2Y^2)$ (quadrifolium), e cercare la loro molteplicità d'intersezione nell'origine ("bisogna" trovare 14).

In conclusione l'ambiente "giusto" per lavorare è lo spazio proiettivo definito su un campo algebricamente chiuso. Facciamo adesso alcuni brevi richiami sullo spazio proiettivo.

1.1. Il proiettivo. Sia E un k-spazio vettoriale di dimensione $n+1$. Su $E^* := E\backslash\{0\}$ introduciamo la relazione: $v \sim w \Leftrightarrow \exists\ \lambda \neq 0$ tale che $v = \lambda w$ (cioè v e w sono collineari). Si verifica che $\sim$ è una relazione d'equivalenza. L'insieme quoziente $E^*/\sim$ si nota $\mathbb{P}(E)$ e si chiama lo spazio proiettivo associato ad E. Lo spazio proiettivo $\mathbb{P}(E)$ si identifica con l'insieme delle rette vettoriali di E. Lo spazio proiettivo associato ad $E = k^{n+1}$, si nota $\mathbb{P}^n(k)$ (o anche $\mathbb{P}^n$) e si chiama lo spazio proiettivo standard, di dimensione n. La dimensione di $\mathbb{P}(k^{n+1})$ è n, in quanto le rette di k^{n+1} vengono contratte a punti nel proiettivo (giustificheremo comunque questo fatto più avanti). Dopo avere scelto una base possiamo identificare E a k^{n+1} e $\mathbb{P}(E)$ a $\mathbb{P}^n$.

Più precisamente, sia $B = (e_0, e_1, ..., e_n)$ una base di E; ogni $v \in E$ si scrive in modo unico $v = \lambda_0 e_0 + \lambda_1 e_1 + \ldots + \lambda_n e_n$, gli scalari λ_i sono le coordinate di v (rispetto alla base B), e scriveremo (con abuso di notazione) $v = (\lambda_0, \ldots, \lambda_n)$ (abbiamo identificato E a k^{n+1}). Se $w = (m_0, \ldots, m_n)$, la condizione $v \sim w$ (v e w entrambi non nulli) è equivalente a: $\exists\ \lambda \neq 0$ tale che $(\lambda\lambda_0, \ldots, \lambda\lambda_n) = (m_0, \ldots, m_n)$. Quindi la classe di v è individuata da una qualsiasi $n+1$-upla $(\lambda\lambda_0, \ldots, \lambda\lambda_n), \lambda \neq 0$ (cioè corrisponde alla classe di $(\lambda_0, \ldots, \lambda_n)$ in $\mathbb{P}(k^{n+1})$). Notiamo $(\lambda_0 : \lambda_1 : \ldots : \lambda_n)$ la classe di $(\lambda_0, \ldots, \lambda_n)$; abbiamo quindi: gli λ_i non sono tutti nulli ($v \neq 0$!), e $(\lambda_0 : \lambda_1 : \ldots : \lambda_n) = (m_0 : m_1 : \ldots : m_n) \Longleftrightarrow \exists\ \lambda \neq 0$ tale che $(\lambda\lambda_0, \ldots, \lambda\lambda_n) = (m_0, \ldots, m_n)$. Sia $(\lambda_0 : \lambda_1 : \ldots : \lambda_n)$ la classe di v in $\mathbb{P}(E)$, si dice che $(\lambda_0 : \lambda_1 : \ldots : \lambda_n)$ sono le coordinate omogenee del punto di $\mathbb{P}(E)$ (relativamente alla base B). Di solito nello spazio proiettivo standard si usa prendere la base canonica di k^{n+1}: $\mathbb{P}^n = \{(\lambda_0 : \ldots : \lambda_n)/$ gli λ_i non sono tutti nulli, e $(\lambda_0 : \lambda_1 : \ldots : \lambda_n) = (m_0 : m_1 : \ldots : m_n) \Leftrightarrow \exists\ \lambda \neq 0$ tale che $\lambda\lambda_i = m_i$, $\forall i\}$.

Sottospazi lineari: Con le notazioni precedenti sia $F \subseteq E$ un sottospazio vettoriale di dimensione $m+1$, $0 \leq m \leq n$. L'immagine di $F \backslash \{0\}$ in $\mathbb{P}(E)$ è, per definizione, un sottospazio lineare (o sottospazio proiettivo) di dimensione m. In effetti questa immagine si identifica con $\mathbb{P}(F)$, noteremo $\mathbb{P}(F) \subseteq \mathbb{P}(E)$; ci capiterà anche di notare con semplici lettere: V, W, ecc.. i sottospazi proiettivi di $\mathbb{P}(E)$. Se $m = 0, 1, 2, \ldots, n-1$, diremo che $\mathbb{P}(F)$ è un punto, una retta, un piano, $\ldots$, un iperpiano. Abbiamo il seguente risultato sulle incidenze di sottospazi (senza le eccezioni della geometria affine dovute al parallelismo):

Proposizione 1.2: *Siano V, W due sottospazi proiettivi di $\mathbb{P}(E)$, di dimensioni rispettivamente r, s. Se $r + s - n \geq 0$, $V \cap W$ è uno sottospazio proiettivo di dimensione $\geq r + s - n$ (in particolare $V \cap W$ è non vuoto).*

Dimostrazione. Segue dalla relazione (vettoriale) di Grassmann. $\square$

Osservazione 1.3: *In particolare due rette del piano proiettivo $\mathbb{P}^2$ s'intersecano sempre, stessa cosa per due piani in $\mathbb{P}^3$, ecc..*

Come nel caso vettoriale, l'unione di due sottospazi proiettivi, V, W di $\mathbb{P}(E)$, non è in generale un sottospazio proiettivo, ma si può considerare il sottospazio proiettivo, $< V, W >$, generato da V e W: è il più piccolo sottospazio proiettivo contenente $V \cup W$; se $V = \mathbb{P}(F)$, $W = \mathbb{P}(F')$, allora $< V, W >= \mathbb{P}(F + F')$; più generalmente si può considerare il sottospazio proiettivo generato da un sottoinsieme qualsiasi di $\mathbb{P}(E)$. Come nel caso affine diremo che $r+1$ punti, $r \leq n$, $p_0, \ldots, p_r$ di $\mathbb{P}(E)$ sono indipendenti se generano un sottospazio lineare di dimensione r: $< p_0, \ldots, p_r > \simeq \mathbb{P}^r$. Più generalmente $t+1$ punti, $p_0, \ldots, p_t$ di $\mathbb{P}^n$ sono in posizione (lineare) generale se $t = n$ e i p_i sono indipendenti, o $t > n$ e $n+1$ tra essi comunque scelti sono linearmente indipendenti (cioè non sono contenuti in un iperpiano).

1.2. Dualità. Il principio di dualità, in origine, sta tutto nell'osservazione che nelle frasi "per due punti passa una retta" e "due rette s'intersecano in un punto" le parole punto e retta possono essere scambiate (cioè sono duali), visto che nel piano proiettivo due rette s'intersecano sempre, si ottiene così una dualità perfetta tra punti e rette; ogni enunciato che coinvolge solo punti e rette ammette un enunciato duale con le parole punto e rette scambiate.

Lo spazio duale dello spazio proiettivo $\mathbb{P}(E)$ è lo spazio proiettivo $\mathbb{P}(E^\vee)$ dove $E^\vee$ (o E^*, o $Hom_k(E, k)$) indica il duale di E. Il duale di $\mathbb{P}^n$ si nota anche $\mathbb{P}^*_n$ (o $\mathbb{P}^\vee_n$) . I punti di $\mathbb{P}(E^\vee)$ sono le rette vettoriali di $E^\vee$. La dualità vettoriale ci permette di identificare una retta vettoriale di $E^\vee$ con un iperpiano vettoriale di E;

in altri termini $\mathbb{P}(E^\vee)$ si identifica con l'insieme degli iperpiani di $\mathbb{P}(E)$. Si ricorda che, più generalmente, la dualità vettoriale stabilisce una biiezione tra l'insieme dei sottospazi E di dimensione $k+1$ e l'insieme dei sottospazi di dimensione $n-k$ di E^* ($\dim E = n+1$); la biiezione è data da $V \longmapsto V^\circ$ (è biiettiva perché $V^{\circ\circ} = V$). Inoltre $V \subseteq W \Leftrightarrow W^\circ \subseteq V^\circ$ (la dualità inverte le inclusioni). In particolare il duale di $\mathbb{P}_n^\vee$ si identifica naturalmente con $\mathbb{P}^n$. Per esempio la dualità fa corrispondere (invertendo le inclusioni) un punto (risp. una retta) di $\mathbb{P}^2$ a una retta (risp. un punto) di $\mathbb{P}^2$. Quindi ogni enunciato di geometria proiettiva che riguarda solo punti e rette in $\mathbb{P}^2$ è ancora vero scambiando la parola retta con la parola punto ("principio di dualità di Poncelet").

1.3. Proiettività. Sia $f : E \to E$ un'applicazione lineare biiettiva. Siccome $f(\lambda v) = \lambda f(v)$, e siccome f è iniettiva, f induce un'applicazione $\mathbb{P}(f) : \mathbb{P}(E) \to \mathbb{P}(E)$. L'applicazione $\mathbb{P}(f)$ è biiettiva. Un'applicazione biiettiva da $\mathbb{P}(E)$ in sé stesso indotta da un endomorfismo invertibile si chiama una proiettività. Se f è un'omotetia, allora $\mathbb{P}(f)$ è l'identità, cioè il sottogruppo, $k^* \subset Gl(E)$, delle omotetie invertibili opera banalmente su $\mathbb{P}(E)$. Il gruppo quoziente $Gl(E)/k^* =: \mathbb{P}Gl(E)$ è il gruppo delle proiettività di $\mathbb{P}(E)$.

1.4. Carte affini. Consideriamo $\mathbb{P}^n$ con le coordinate omogenee standard (abbiamo scelto la base canonica in k^{n+1}). Notiamo H_0 l'iperpiano di equazione $X_0 = 0$, quindi $H_0 = \{(a_0 : \ldots : a_n) \in \mathbb{P}^n / a_0 = 0\}$; in altri termini $H_0 = \mathbb{P}(F_0)$ dove $F_0 \subseteq E$ è l'iperpiano vettoriale di equazione $X_0 = 0$. Sia $U_0 := \mathbb{P}^n \backslash H_0$. Abbiamo un'applicazione $j_0 : U_0 \to \mathbb{A}^n : (a_0 : \ldots : a_n) \longmapsto (\alpha_1, \ldots, \alpha_n)$ dove $\alpha_k = \frac{a_k}{a_0}$. Questa applicazione è biiettiva e $j_0^{-1} =: y_0 \colon \mathbb{A}^n \to U_0 : (b_1, \ldots, b_n) \longmapsto (1 : b_1 : \ldots : b_n)$. Siccome $\mathbb{P}^n = H_0 \bigsqcup U_0$ (unione disgiunta), vediamo che $\mathbb{P}^n$ è l'unione disgiunta di un proiettivo di dimensione $n-1$ ($H_0 \simeq \mathbb{P}^{n-1}$) e di uno spazio affine di dimensione n ($U_0 \simeq \mathbb{A}^n$). Per il momento questa decomposizione è soltanto insiemistica, ma vedremo che è anche algebrica, cioè j_0 e y_0 sono dei morfismi. In queste condizioni si usa dire che H_0 è l'iperpiano all'infinito. Questa terminologia si giustifica così: se partiamo da $\mathbb{A}^n$ ($\simeq U_0$), allora $\mathbb{P}^n$ si ottiene da $\mathbb{A}^n$ aggiungendo l'iperpiano H_0; i punti di $\mathbb{A}^n$ vengono chiamati punti a distanza finita mentre i punti di H_0 sono i punti all'infinito. Se invece partiamo da $\mathbb{P}^n$, possiamo ripetere quanto fatto prima con un iperpiano qualsiasi al posto di H_0 (è chiaro per gli iperpiani H_i di equazione $X_i = 0$, per gli altri cambiare base). In conclusione l'infinito non esiste nel proiettivo: l'infinito è una nozione affine!

Se $p = (a_0 : \ldots : a_n) \in \mathbb{P}^n$, esiste i tale che $a_i \neq 0$ quindi $p \in U_i$. Pertanto $\mathbb{P}^n = \bigcup_{i=0}^{n} U_i$, gli U_i sono delle carte affini di $\mathbb{P}^n$ (la terminologia proviene dalla geometria differenziale). Noteremo $j_i : U_i \to \mathbb{A}^n : p = (\ldots : x_k : \ldots) \to (\ldots, \frac{x_k}{x_i}, \ldots)$ l'applicazione analoga di j_0 ($j_i(p)$ ha n coordinate, $\frac{x_i}{x_i}$ viene omesso; le notazioni sono più pesanti e pertanto useremo più volentieri l'indice 0 (riordinando semmai gli elementi della base)). Osserviamo che sono necessari tutti gli $n+1$ U_i per ricoprire $\mathbb{P}^n$ (cfr. Esercizi).

1.5. La retta proiettiva. Abbiamo due carte affini $U_0 = \{(x_0 : x_1)/x_0 \neq 0\}$, $U_1 = \{(x_0 : x_1)/x_1 \neq 0\}$, e, per esempio, $\mathbb{P}^1 = U_1 \cup H_1$. Osserviamo che H_1 consta di un unico punto: $H_1 = \{(1 : 0)\}$. Se poniamo $\infty := (1 : 0)$ allora $\mathbb{P}^1 \setminus \{\infty\}$ si identifica con $\mathbb{A}^1$. Se $k = \mathbb{R}$ o $\mathbb{C}$, e dopo avere dato a $\mathbb{P}^n$ la topologia quoziente della topologia euclidea su $k^{n+1} \setminus \{0\}$, si ritrova che $\mathbb{P}^1$ è la compattificazione di Alexandroff di k. Se $k = \mathbb{R}$, $\mathbb{P}^1$ si identifica con una circonferenza, se $k = \mathbb{C}$, $\mathbb{P}^1$ si identifica con una sfera (pensare a $\mathbb{C}$ come al piano $\mathbb{R}^2$), la "sfera di Riemann".

Sia $f : \mathbb{P}^1 \to \mathbb{P}^1$ una proiettività, come già visto f proviene da un endomorfismo invertibile di k^2 che possiamo rappresentare sotto forma matriciale (modulo moltiplicazione dei coefficienti della matrice per uno scalare non nullo): $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Sia $p \neq \infty$ un punto di $\mathbb{P}^1$, possiamo scrivere $p = (u : 1)$ e $f(p) = (au + b : cu + d)$; se $cu + d \neq 0$ (cioè se $f(p) \neq \infty$), allora $f(p) = (\frac{au+b}{cu+d} : 1)$. Osserviamo che se $cu + d = 0$ "allora" $f(p) := \infty$. Nello stesso modo $f(\infty) = (a : c)$. Se $c \neq 0$, $(a : c) = (\frac{a}{c} : 1)$. Osserviamo che, se $c \neq 0$, $\frac{ax+b}{cx+d}$ tende a $\frac{a}{c}$ quando x tende all'infinto. Se invece $c = 0$, $(a : 0) = (1 : 0) = \infty$; e $\frac{ax+b}{d}$ tende all'infinito quando x tende all'infinito (osservare che non può essere $a = 0$ se $c = 0$). In conclusione le proiettività di $\mathbb{P}^1$ si identificano con le applicazioni: ("omografie" o "trasformazioni lineari fratte")

$f : k \cup \{\infty\} \to k \cup \{\infty\} : x \longmapsto \frac{ax+b}{cx+d}$, dove $ad - bc \neq 0$, e dove per ∞ si usano le solite regole di calcolo.

1.6. Birapporto di quattro punti della retta proiettiva. Avendo scelto una base $(e_0, \dots, e_n)$ di V ogni punto $p \in \mathbb{P}(V)$ corrisponde a delle coordinate omogenee $(a_0 : \dots : a_n)$ ($p =< v >$ e $v = a_i e_i$). Siano $p_i \in \mathbb{P}(V)$ i punti corrispondenti agli $e_i : p_i =< e_i >$. Allora $p_i =< b_i e_i >$ ($b_i \neq 0$), e $(b_0 e_0, \dots, b_n e_n)$ è una base di V, rispetto a questa base le coordinate omogenee di p sono $(\frac{a_0}{b_0} : \dots : \frac{a_n}{b_n})$; ci sono quindi tanti sistemi di coordinate omogenee corrispondenti ai punti p_i. Osserviamo che un sistema di coordinate omogenee corrisponde a una classe di proporzionalità di basi (le basi (e_i), (u_i) sono proporzionali se esiste $\lambda \neq 0$ tale che $e_i = \lambda u_i$, $\forall i$). I punti p_i non determinano univocamente un sistema di coordinate omogenee. Per fissare un sistema di coordinate omogenee corrispondente ai p_i bisogna introdurre un ulteriore punto: sia p tale che gli $n + 2$ punti $p_0, \dots, p_n, p$ siano in posizione generale (cioè $n + 1$ tra di loro non sono mai contenuti in un iperpiano). Allora esiste un unico sistema di coordinate omogenee corrispondente ai p_i (cioè $p_i = (0 : \dots : 1 : \dots : 0)$), tale che in quel sistema, le coordinate di p siano $(1 : \dots : 1)$. Infatti sia $p =< v >$ e $v = g_i e_i$, siccome i punti $p_0, \dots, p_n, p$ sono in posizione generale: $g_i \neq 0$, $\forall i$. Quindi $(g_0 e_0, \dots, g_n e_n)$ è una base di V e rispetto a questa base le coordinate omogenee di p sono $(1 : \dots : 1)$. Viceversa se p ha coordinate $(1 : \ldots : 1)$ rispetto alla base $(b_i e_i)$ allora $\lambda v = b_i e_i$, per qualche $\lambda \neq 0$; segue che $b_i = \lambda g_i$, e le basi $(b_i e_i)$, $(g_i e_i)$ sono proporzionali. In conclusione $n+2$ punti $p_0, \ldots, p_n, p$ di $\mathbb{P}^n$, in posizione generale, determinano un unico sistema di coordinate omogenee, in questo sistema $p_i = (0 : \ldots : 1 : \ldots : 0)$ (1 al posto i), $p = (1 : \ldots : 1)$; i punti p_i sono i punti fondamentali del sistema, p è il punto unità.

La maggiore (e forse unica?) applicazione di tutto questo risiede nella nozione di birapporto di quattro punti di $\mathbb{P}^1$. Per maggiori dettagli su quanto segue consultare un buon testo di geometria proiettiva (per esempio [**?**] §3, no 27). Siano $p_i \in \mathbb{P}^1$, $1 = i = 4$, con p_1, p_2, p_3 distinti (non si richiede niente su p_4). Siano $(x_0 : x_1)$ le coordinate omogenee di p_4 nel sistema avente p_1, p_2 come punti fondamentali, e p_3 come punto unità. Il birapporto dei p_i, $\beta(p_1, p_2, p_3, p_4)$, è per definizione: $\beta(p_1, p_2, p_3, p_4) := \frac{x_1}{x_0}$. Il birapporto è un elemento di $k \cup \{\infty\}$ (cioè di $\mathbb{P}^1$!). Osservare che $\beta(p_1, p_2, p_3, p_4) = 0, \infty, 1$ a secondo che $p_4 = p_1, p_2, p_3$. Osservare anche che il birapporto dei p_i dipende dall'ordine nel quale si considerano i punti: $\beta(p_1, p_2, p_3, p_4) \neq \beta(p_2, p_1, p_3, p_4)$ in generale. Abbiamo:

Teorema 1.4: *Siano p_1, p_2, p_3, p_4 (risp. q_1, q_2, q_3, q_4) dei punti di $\mathbb{P}^1$, con p_1, p_2, p_3 (risp. q_1, q_2, q_3) distinti. Esiste una proiettività $f : \mathbb{P}^1 \to \mathbb{P}^1$ tale che $f(p_i) = q_i$, $1 = i = 4$, se e solo se $\beta(p_1, p_2, p_3, p_4) = \beta(q_1, q_2, q_3, q_4)$.*

Abbiamo detto che il birapporto dipende dall'ordine sui p_i, se i quattro punti sono distinti il birapporto di una loro permutazione qualsiasi è definito; ci sono $4! = 24$ modi di ordinare i p_i, queste 24 permutazioni danno luogo a solo 6 birapporti: se $\beta = \beta(p_1, p_2, p_3, p_4)$, i 6 birapporti possibili sono $\beta, \frac{1}{\beta}, 1-\beta, \frac{1}{1-\beta}, \frac{(\beta-1)}{\beta}, \frac{\beta}{\beta-1}$.

Poniamo $j(\beta) = \frac{(\beta^2-\beta+1)^3}{\beta^2(\beta-1)^2}$, funzione razionale definita per $\beta \neq 0, 1$. Si verifica che $j(\beta) = j(\beta')$ $(\beta, \beta' \neq 0, 1)$ se e solo se $\beta' \in \{\beta, \frac{1}{\beta}, 1-\beta, \frac{1}{1-\beta}, \frac{(\beta-1)}{\beta}, \frac{\beta}{\beta-1}\}$. Segue che se β è il birapporto di quattro punti distinti, p_i, di $\mathbb{P}^1$ presi in un certo ordine, allora $j(\beta)$ non dipende dall'ordine considerato; $j(\beta) = j(p_1, \ldots, p_4)$ è il modulo della quaterna $(p_1, \ldots, p_4)$. Da quanto detto finora segue il:

Teorema 1.5: *Due quaterne (non ordinate) di punti distinti di $\mathbb{P}^1$, $\{p_1, \ldots, p_4\}$, $\{q_1, \ldots, q_4\}$ sono proiettivamente equivalenti (cioè esiste una proiettività f tale che $\{f(p_1), \ldots, f(p_4)\} = \{f(q_1), \ldots, f(q_4)\}$) se e solo se $j(p_1, \ldots, p_4) = j(q_1, \ldots, q_4)$.*

Il problema di ottenere delle condizioni esplicite affinché due sottoinsiemi di $t > n+3$ punti di $\mathbb{P}^n$ siano proiettivamente equivalenti è tuttora aperto.

Il birapporto e la funzione $j(\beta)$ sono ingredienti essenziali nella classificazione delle curve ellittiche (cubiche piane liscie).

1.7. Il piano proiettivo. Una retta, R, di $\mathbb{P}^2$ è il proiettivo associato a un iperpiano vettoriale di k^3, quindi $R = \{(x : y : z)/ax + by + cz = 0\}$, dove $ax+by+cz = 0$ è un'equazione cartesiana dell'iperpiano vettoriale. Consideriamo la carta affine U_0 e la corrispondente retta all'infinito R_∞; l'equazione di R_∞ è $x = 0$. Supponiamo $R \neq R_\infty$. Tramite la biiezione $j_0 : U_0 \to \mathbb{A}^2$, un punto $(x : y : z)$ di $R \cap U_0$ viene mandato nel punto (u, v) con $u = \frac{y}{x}$, $v = \frac{z}{x}$, che verifica l'equazione $bu + cv + a = 0$. Quindi $j_0(R \cap U_0)$ è la retta affine, r, di equazione $bu + cv + a = 0$. D'altra parte $R \cap R_\infty = (0 : -c : b)$, e $(-c, b)$ è proprio il vettore direttore della retta r. Viceversa una retta $r' \subseteq \mathbb{A}^2$ parallela a r ha un'equazione del tipo $bu + cv + a' = 0$, e $y_0(r') = R' \cap U_0$ dove $R' \subseteq \mathbb{P}^2$ è la retta di equazione $a'x + by + cz = 0$. Si ha $R' \cap R_\infty = R \cap R_\infty$: tutte le rette affini parallele a r danno luogo a rette proiettive che intersecano la retta all'infinito nello stesso punto che corrisponde alla direzione di queste rette. Le rette di $\mathbb{P}^2$ diverse da R_∞ corrispondono alle rette affini di $\mathbb{A}^2$, ogni retta proiettiva ha in più un punto all'infinito che corrisponde alla direzione della retta affine.

1.8. Coniche. Sia $C = \{p = (x : y : z) \in \mathbb{P}^2 / xy - z^2 = 0\}$; osserviamo che C è ben definita perché se $p = (x' : y' : z')$ allora $x' = \lambda x$, $y' = \lambda y$, $z' = \lambda z$ per qualche $\lambda \neq 0$, e $x'y' - z'^2 = 0$. La traccia di C nella carta affine U_0 fornisce la parabola di equazione $y = x^2$ (più precisamente, con le notazioni precedenti $u = v^2$). Osserviamo che C interseca la retta all'infinito in un unico punto: $C \cap R_\infty = (0 : 1 : 0)$ (in effetti C è tangente a R_∞).

In modo analogo la traccia di C nella carta affine U_2 fornisce l'iperbole di equazione $uv = 1$ ($u = \frac{x}{z}$, $v = \frac{y}{z}$). L'intersezione di C con la corrispondente retta all'infinito $z = 0$, è uguale a $\{(0 : 1 : 0), (1 : 0 : 0)\}$, questi due punti corrispondono alle direzioni asintotiche dell'iperbole $uv = 1$, cioè $u = 0$, e $v = 0$.

Per completare il quadro prendiamo come retta all'infinito la retta di equazione $x + y = 0$. Per vederci chiaro facciamo un cambiamento di variabili (cioè una proiettività): $X = x$, $Y = z$, $Z = x + y$. L'equazione di C diventa $X^2 + Y^2 - XZ = 0$; nella carta affine corrispondente ($Z \neq 0$), C fornisce l'ellisse di equazione $u^2 + v^2 - u = 0$ ($u = \frac{X}{Z}$, $v = \frac{Y}{Z}$), in effetti questa è una circonferenza: $u^2 + v^2 - u = (u - \frac{1}{2})^2 + v^2 - \frac{1}{4}$. L'intersezione di C con la retta all'infinito $Z = 0$ è data da $X^2 + Y^2 = 0$; è vuota se $k = \mathbb{R}$, uguale a $\{(\pm i : 1 : 0)\}$ se $K = \mathbb{C}$; $(\pm i : 1 : 0)$ sono i punti ciclici all'infinito, ne riparliamo fra poco.

La morale di questo giochetto è che la distinzione tra iperbole, parabola, ellisse è una nozione affine che si traduce proiettivamente nel fatto che la conica interseca in due, uno o zero punti la retta all'infinito ($k = \mathbb{R}$). Nel piano proiettivo (k algebricamente chiuso) tutte le coniche non degeneri sono proiettivamente equivalenti: sostanzialmente c'è un'unica conica non degenere. (D'altra parte su un campo algebricamente chiuso l'unico invariante della classificazione delle forme quadratiche è il rango)

Concludiamo questo piccolo ripasso con un altro giochetto. Abbiamo motivato l'introduzione del proiettivo col fine di ottenere il teorema di Bezout secondo il quale, in particolare, due coniche s'incontrano in quattro punti, contati con molteplicità. Consideriamo due circonferenze C, C' in $\mathbb{R}^2$. Ebbene queste due circonferenze si intersecano in al più due punti. Per vederlo fate un disegno; se non siete convinti, procediamo così: una circonferenza è il luogo dei punti, p, la cui distanza da un punto O è costante, uguale a r: $C = \{p/\ d(O,p) = r\}$. Quindi C ha un'equazione del tipo $(x-a)^2 + (y-b)^2 = r^2$ ($O = (a,b)$), ossia sviluppando: $x^2 + y^2 + ax + bx + d = 0$ (i). Nello stesso modo C' ha un'equazione della forma: $x^2 + y^2 + a'x + b'x + d' = 0$ (ii). Da (i) - (ii) viene: $x(a-a') + y(b-b') + d - d' = 0$ (iii). La relazione (iii) permette di esprimere un'incognita in funzione dell'altra, per esempio, se $a \neq a'$: $x = \frac{[y(b-b\prime)+d-d\prime]}{a'-a}$ (iv). Inserendo in (i) otteniamo un'equazione, (v), di secondo grado in y. Questa equazione ha al più due radici, y_1, y_2. Usando (iv) si ricavano i valori corrispondenti di x, da cui i due punti, (x_1, y_1), (x_2, y_2), dell'intersezione $C \cap C'$. L'equazione di secondo grado (v) potrebbe non avere soluzioni in $\mathbb{R}$ (in questo caso $C \cap C' = \emptyset$), ma sappiamo già che per avere un buon teorema di Bezout bisogna lavorare su un campo algebricamente chiuso, perciò consideriamo (v) come un'equazione a coefficienti in $\mathbb{C}$. In questo caso (v) ha sempre due soluzioni, in generale queste soluzioni saranno distinte e i corrispondenti punti avrano molteplicità uno nell'intersezione. Ma allora ci mancano due punti, dove sono finiti? Guardiamo nel proiettivo; questo torna a omogeneizzare l'equazione (i) introducendo una terza variabile: $x^2 + y^2 + axz + byz + dz^2 = 0$ (ponendo $z = 1$ si ritrova l'equazione (i)). L'intersezione con la retta all'infinito $z = 0$ è data da: $x^2 + y^2 = 0$, cioè dai due punti $(\pm i : 1 : 0)$. Quindi tutte le circonferenze incontrano la retta all'infinito nei due punti ciclici $(\pm i : 1 : 0)$, e quindi, in $\mathbb{P}^2(\mathbb{C})$, $\#(C \cap C') = 4$, come si voleva dimostrare!

Esercizi.

Esercizio 1.1: *Chiamiamo carta affine di* $\mathbb{P}^n$ *ogni sottoinsieme* $V \subseteq \mathbb{P}^n$ *che è il complementare di un iperpiano* H. *Dimostrare che non si può ricoprire* $\mathbb{P}^n$ *con meno di* $n+1$ *carte affini. Se* $V_i = \mathbb{P}^n \backslash H_i$, $0 \leq i \leq n$, *a quale condizione devono soddisfare gli iperpiani* H_i *affinché i* V_i *ricoprano* $\mathbb{P}^n$*?*

Esercizio 1.2: *Sia* $k = \mathbb{F}_p$ *il campo con* p *elementi (*p *un numero primo). Calcolare la cardinalità di* $\mathbb{P}^n(k)$.

Esercizio 1.3: (i) *Dimostrare, usando la dualità, che due rette di* $\mathbb{P}^2$ *s'intersecano sempre (considerare l'enunciato duale di "per due punti passa sempre una retta").*
(ii) *Qual è la configurazione duale di tre punti di* $\mathbb{P}^2$ *non allineati (risp. allineati) in* $\mathbb{P}_2^*$*? E quella duale di tre piani in* $\mathbb{P}^3$ *con una retta in comune?*

Esercizio 1.4: (i) *Dimostrare che l'insieme delle rette di* $\mathbb{P}^2$ *che passano per un punto ha una struttura naturale di spazio proiettivo (*$\simeq \mathbb{P}^1$*); un tale insieme di rette si chiama un fascio di rette.*

(ii) *Sia* $E \subset \mathbb{P}^n$ *un sottospazio lineare di dimensione* s. *Sia* $r = n - s - 1$. *Mostrare che esiste un sottospazio lineare* $F \subset \mathbb{P}^n$ *tale che* $E \cap F = \emptyset$.

(iii) *Sia* V *un sottospazio lineare di codimensione* $r+1$ *di* $\mathbb{P}^n$. *Dimostrare che l'insieme degli iperpiani di* $\mathbb{P}^n$ *contenenti* V *ha una struttura di spazio proiettivo di cui si determinerà la dimensione.*

Esercizio 1.5: *Siano* $R, L \subset \mathbb{P}^3$ *due rette sghembe (i.e.* $R \cap L = \emptyset$*) e sia* p *un punto non appartenente a* $R \cup L$. *Dimostrare che esiste una, ed un'unica, retta passante per* p *e incidente sia a* R *che a* L.

Siano adesso L, L', L'' *tre rette di* $\mathbb{P}^3$, *due a due sghembe. Per ogni punto* $p \in L''$, *esiste una retta,* D_p, *tale che* $p \in D_p, D_p \cap L' \neq \emptyset, D_p \cap L \neq \emptyset$. *Mostrare che* $D_p \cap D_q = \emptyset$, *se* $p \neq q$. *(In particolare prese* D_p, D_q, D_t *si può ripetere il procedimento "nell'altro verso", ottenendo delle rette* $L_m, m \in D_p$*).*

$(Q := \bigcup_{p \in L''} D_p$ *è una superficie quadrica liscia di* $\mathbb{P}^3$.$)$

Esercizio 1.6: *(Proiezione da un punto). Sia* $a \in \mathbb{P}^n$, $a = (1 : 0 : \ldots : 0)$ *e* H *l'iperpiano di equazione* $x_0 = 0$ *("il corrispondente iperpiano all'infinito"). La proiezione dal punto* a *sull'iperpiano* H *è l'applicazione* $\pi : \mathbb{P}^n \backslash \{a\} \to H \simeq \mathbb{P}^{n-1}$, *definita da* $\pi(p) = q$ *dove* q *è il punto d'intersezione della retta* $< a, p >$ *con l'iperpiano* H.
(i) *È possibile estendere* π *(in modo ragionevole) ad un'applicazione definita su tutto* $\mathbb{P}^n$*?*
(ii) *Consideriamo la carta affine* U_n*;* π *induce un'applicazione* $U_n \to H \cap U_n$. *Dare delle equazioni di questa applicazione.*

(iii) Sia $\lambda \neq 0$, *e* $\alpha_\lambda : \mathbb{P}^n \to \mathbb{P}^n : (x_0 : \ldots : x_n) \longmapsto (\lambda x_0 : \ldots : \lambda x_n)$. *Mostrare che* α_λ *è un automorfismo di* $\mathbb{P}^n$. *Descrivere* α_λ *nella carta affine* U_n. *Osservare che* π *è il limite di* α_λ *quando* $\lambda \to 0$.

2. Insiemi algebrici proiettivi.

Come al solito assumiamo il campo k algebricamente chiuso, e notiamo $\mathbb{P}^n$ invece di $\mathbb{P}^n(k)$.

Adesso cerchiamo di ripetere nel proiettivo tutto quello che abbiamo fatto nello spazio affine, molti risultati seguono direttamente dal caso affine ma ci sono alcune differenze sostanziali che cercheremo di mettere in evidenza.

La prima differenza è che un polinomio $P \in k[X_0, ..., X_n]$ non determina una funzione $\mathbb{P}^n \to k$. Infatti se $z \in \mathbb{P}^n$, $P(z)$ dipende dalle coordinate omogenee scelte per z. Per esempio ($n = 1$), sia $P = X_0^2 - X_1 + 1$, $z = (1 : 2)$, allora $P(1, 2) = 0$; però abbiamo anche $z = (2 : 4)$, ma $P(2, 4) = 1$.

Ricordiamo che un polinomio $P(X_0, \dots, X_n) = \Sigma a_{i_0 \dots i_n} X_0^{i_0} \dots X_n^{i_n}$, è omogeneo di grado d se tutti i suoi monomi hanno grado d: $a_{i_0 \dots i_n} \neq 0 \Longrightarrow i_0 + \dots + i_n = d$. Inoltre ogni polinomio $P \in k[X_0, \dots, X_n]$ si scrive, in modo unico, nella forma $P = P_d + P_{d-1} + \dots + P_0$ dove P_i è omogeneo di grado i. Osserviamo che se P è omogeneo di grado d allora $P(\lambda a_0, \dots, \lambda a_n) = \lambda^d P(a_0, \dots, a_n)$, e quindi, anche se P non definisce una funzione su $\mathbb{P}^n$, ha senso dire che P si annulla o meno nel punto z di $\mathbb{P}^n$:

Definizione 2.1: *Il punto $z \in \mathbb{P}^n$ è uno zero del polinomio omogeneo $P \in k[X_0, \dots, X_n]$ se $P(z_0, \dots, z_n) = 0$ dove $(z_0 : \dots : z_n)$ è un rappresentante qualsiasi di z.*

Osservazione 2.2: *Se P è un polinomio qualsiasi e se $z \in \mathbb{P}^n$, diciamo che z è uno zero di P se $P(z_0, \dots, z_n) = 0$ per <u>ogni</u> rappresentante di z. Abbiamo $P = P_d + P_{d-1} + \dots + P_0$, dove P_i è omogeneo di grado i. Un rappresentante qualsiasi di z è della forma $(\lambda z_0 : \dots : \lambda z_n)$, abbiamo $P(\lambda z_0, \dots, \lambda z_n) = \sum_{j=0}^{d} P_j(\lambda z_0, \dots, \lambda z_n) = \sum_{j=0}^{d} \lambda^j P_j(z_0, \dots, z_n)$, quindi $P(\lambda z_0, \dots, \lambda z_n) = 0$, $\forall \lambda$ se e solo se $P_j(z_0, \dots, z_n) = 0$, $\forall j$ (considerare il polinomio in λ). Questo ci conduce ad introdurre la nozione di ideale omogeneo.*

Definizione 2.3: *Un ideale $I \subseteq k[X_0, \dots, X_n]$ è omogeneo se può essere generato da polinomi omogenei.*

Un'altra caratterizzazione degli ideali omogenei:

Lemma 2.4: *Un ideale $I \subseteq k[X_0, \dots, X_n]$ è omogeneo se e solo se: per ogni polinomio P si ha: $P \in I \Leftrightarrow P_i \in I$, $\forall i$, dove $P = \sum_{i=0}^{d} P_i$ è la decomposizione di P in elementi omogenei.*

Dimostrazione. ($\Longrightarrow$)Supponiamo I omogeneo e sia $P = \sum_{i=0}^{d} P_i$ con P_i omogeneo di grado i. Se ogni P_i appartiene a I allora chiaramente $P \in I$. Viceversa supponiamo $P \in I$. Allora $P = \Sigma f_j q_j$ dove gli f_j sono dei generatori omogenei di I. Sia $q_j = \sum_k q_k^{(j)}$, $q_k^{(j)}$ omogenei di grado k. Abbiamo $P = \sum_{i=0}^{d} P_i = \sum_{j,k=0} f_j q_k^{(j)}$, confrontando i gradi vediamo che $P_i \in I$, $\forall i$.

($\Longleftarrow$) Sia $I = (f_1, \dots, f_r)$, $f_i = \sum_k f_{i,k}$, $f_{i,k}$ omogeneo di grado k. Allora I è generato dai polinomi omogenei $f_{i,k}$. $\square$

Inoltre abbiamo:

Lemma 2.5: *Siano I, J degli ideali omogenei di $k[X_0, \dots, X_n]$ allora $I + J$, $I.J$, $I \cap J$, $\sqrt{I}$, sono degli ideali omogenei.*

Dimostrazione. Lasciata al lettore. $\square$

Definizione 2.6: *Sia $I = (f_1, \dots, f_r)$ un ideale omogeneo, con f_i polinomi omogenei. Il luogo degli zeri di I è: $\mathbf{V}(I) = \{z \in \mathbb{P}^n / \ f_i(z) = 0, \forall i\}$.*

Osservazione 2.7: *Equivalentemente $\mathbf{V}(I) = \{z \in \mathbb{P}^n / \ P(z) = 0, \forall P \in I\}$, purché $P(z) = 0$ sia interpretato come nell'Osservazione 2.2.*

Definizione 2.8: *Un sottoinsieme $X \subseteq \mathbb{P}^n$ è un sottoinsieme algebrico (proiettivo) se esiste un ideale omogeneo $I \subseteq k[X_0, \dots, X_n]$ tale che $X = \mathbf{V}(I)$.*

Esempio 2.9:
- (i) Sia $F \in k[X_0, \dots, X_n]$ un polinomio omogeneo e $I = (F)$ l'ideale generato da F, $X = \mathbf{V}(I)$ è l'ipersuperficie di $\mathbb{P}^n$ di equazione $F = 0$. Se $n = 2$, X è una curva piana.
- (ii) Sia $\mathfrak{m} = (X_0, \dots, X_n) \subseteq k[X_0, \dots, X_n]$ l'ideale massimale dei polinomi senza termine costante; è un ideale omogeneo e $\mathbf{V}(\mathfrak{m}) = \emptyset$, infatti ogni punto di $\mathbb{P}^n$ ha almeno una coordinata X_i non nulla. D'altra parte $\mathfrak{m}$ definisce l'origine di k^{n+1} ma $\mathbb{P}^n$ è il quoziente di $k^{n+1} \backslash \{0\}$ per la relazione $\sim$ di proporzionalità. Abbiamo quindi due ideali che definiscono il vuoto: (1) e l'ideale massimale $\mathfrak{m}$ che viene chiamato, appunto, l'ideale irrilevante . Questa è una differenza con la situazione affine, e dovremo scartare $\mathfrak{m}$ per avere una buona corrispondenza tra ideali (radicali) e sottoinsiemi algebrici proiettivi.
- (iii) Sia $z = (a'_0 : \dots : a'_n) \in \mathbb{P}^n$, uno degli a'_i è non nullo, per esempio $a'_0 \neq 0$, dividendo per a'_0 abbiamo $z = (1 : a_1 : \dots : a_n)$ e $\{z\} = \mathbf{V}(X_1 - a_1 X_0, \dots, X_n - a_n X_0)$, quindi un punto di $\mathbb{P}^n$ è un insieme algebrico. Osservare che l'ideale $(X_1 - a_1 X_0, \dots, X_n - a_n X_0)$ non è massimale (perché nell'affine k^{n+1} questo ideale definisce la retta corrispondente a z; tranne l'ideale irrilevante $\mathfrak{m}$, gli ideali massimali di $k[X_0, \dots, X_n]$ non sono omogenei, cfr. I, Sezione 2).

Definizione 2.10: *Sia $X \subseteq \mathbb{P}^n$ un insieme algebrico, l'ideale di X, $\mathbf{I}(X)$, è l'ideale generato da tutti i polinomi omogenei che si annullano su X.*

Osservazione 2.11: *(i) In altri termini $\mathbf{I}(X) = \{P \in k[X_0, \dots, X_n] / \ P(z) = 0$, $\forall z \in X$, dove la relazione $P(z) = 0$ va intesa nel senso dell'Osservazione 2.2$\}$.*

(ii) Chiaramente $\mathbf{I}(X)$ è il più grande ideale che definisce X e si verifica facilmente che $\mathbf{I}(X)$ è radicale.

Passiamo adesso alla corrispondenza tra ideali e sottoinsiemi algebrici. Per questo ci riporteremo allo spazio affine $\mathbb{A}^{n+1}$. Per distinguere dal caso proiettivo, indicheremo con $\mathbf{V}_a(I)$, (risp. $\mathbf{I}_a(Y)$) il luogo degli zeri in $\mathbb{A}^{n+1}$ dell'ideale I (risp. l'ideale del sottoinsieme algebrico Y di $\mathbb{A}^{n+1}$).

Definizione 2.12: *Sia $X \subseteq \mathbb{P}^n$ un sottoinsieme algebrico. Il cono affine di X, $C(X)$, è definito da $C(X) = \{(x_0, \dots, x_n) \in \mathbb{A}^{n+1} \ / \ (x_0, \dots, x_n) = (0, \dots, 0)$ o $[x_0 : \dots : x_n] \in X\}$.*

Osservazione 2.13: *Sia $p : k^{n+1} \backslash \{0\} \to \mathbb{P}^n$ la proiezione canonica, allora $C(X) = \overline{p^{-1}(X)}$ ($C(X)$ è la chiusura in k^{n+1} di $p^{-1}(X)$). Come sottoinsieme di k^{n+1}, $C(X)$ è proprio un cono di vertice l'origine, infatti se $p \in C(X)$ allora tutta la retta passante per p e per l'origine è contenuta in $C(X)$.*

Lemma 2.14: *Sia $X \subseteq \mathbb{P}^n$ un sottoinsieme algebrico non vuoto. Il cono affine di X è un sottoinsieme algebrico di $\mathbb{A}^{n+1}$ e $\mathbf{I}_a(C(X)) = \mathbf{I}(X)$.*

DIMOSTRAZIONE. Infatti se $P \in \mathbf{I}_a(C(X))$ e $z \in X$, allora P si annulla sulla retta vettoriale di $\mathbb{A}^{n+1}$ corrispondente a z, quindi $P \in \mathbf{I}(X)$. Viceversa sia $Q \in \mathbf{I}(X)$, $Q = Q_m + \dots + Q_r$, Q_i omogeneo di grado i. Siccome $\mathbf{I}(X)$ è un ideale omogeneo, ogni Q_i appartiene a $\mathbf{I}(X)$. Inoltre X essendo non vuoto, $\mathbf{I}(X)$ non contiene costanti, ossia $\deg(Q_i) \geq 1$. Finalmente siccome ogni polinomio omogeneo di grado almeno uno, P, verifica $P(0, \dots, 0) = 0$, dalla definizione di $C(X)$ segue che $Q \in \mathbf{I}_a(C(X))$. □

Usando il teorema degli zeri otteniamo il teorema degli zeri omogeneo:

Proposizione 2.15: *Sia $I \subseteq k[X_0, \dots, X_n]$ un ideale omogeneo.*

- *(i) $\mathbf{V}(I) \subseteq \mathbb{P}^n$ è vuoto se e solo se $(X_0, \dots, X_n)^N \subseteq I$ per qualche $N \geq 1$ (i.e. I contiene tutti i polinomi omogenei di grado $\geq N$);*
- *(ii) se $\mathbf{V}(I) \neq \emptyset$, allora $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.*

DIMOSTRAZIONE. (i) È chiaro che $\mathbf{V}(I) = \emptyset$ se e solo se $\mathbf{V}_a(I) \subseteq \{(0, \dots, 0)\}$. Dal Teorema degli zeri $\mathbf{I}_a(\mathbf{V}_a(I)) = \sqrt{I}$. Dall'inclusione $\mathbf{V}_a(I) \subseteq \{(0, \dots, 0)\}$, risulta $(X_0, \dots, X_n) \subseteq \sqrt{I}$. Quindi per ogni i esiste n_i tale che $X_i^{n_i} \in I$. Se $m = \max\{n_i\}$, allora per ogni i, $X_i^k \in I$, se $k \geq m$. Pertanto si vede che se N è abbastanza grande (se $m = 2$, $N = (n+1)m$ va bene), $(X_0, \dots, X_n)^N \subseteq I$.

(ii) Abbiamo $\mathbf{I}(\mathbf{V}(I)) = \mathbf{I}_a(C(X))$ dove $X = \mathbf{V}(I)$ (cfr. Lemma 2.14). Siccome $C(X) = \mathbf{V}_a(I)$, $\mathbf{I}(\mathbf{V}(I)) = \mathbf{I}_a(\mathbf{V}_a(I))$. Dal Teorema degli zeri: $\mathbf{I}_a(\mathbf{V}_a(I)) = \sqrt{I}$, e quindi $\mathbf{I}(\mathbf{V}(I)) = \sqrt{I}$.

□

Abbiamo quindi due ideali radicali che definiscono il vuoto: (1) e l'ideale irrilevante $\mathfrak{m}$. Per avere una buona corrispondenza scarteremo l'ideale $\mathfrak{m}$.

Proposizione 2.16: *Sia φ così definita:*

$\varphi : \{$*sottoinsiemi algebrici di* $\mathbb{P}^n\} \to \{$*ideali omogenei radicali di* $k[X_0, ..., X_n]$ *diversi da* $\mathfrak{m}\} : X \to \mathbf{I}(X)$

(i) φ è biiettiva e $\varphi^{-1} = \psi$ dove

$\psi : \{$*ideali omogenei radicali di* $k[X_0, ..., X_n]$ *diversi da* $\mathfrak{m}\} \to \{$*sottoinsiemi algebrici di* $\mathbb{P}^n\} : J \to \mathbf{V}(J)$

(ii) φ e φ^{-1} invertono le inclusioni.

Dimostrazione. Esercizio. □

Passiamo adesso alla topologia di Zariski:

Lemma 2.17: *L'unione di due sottoinsiemi algebrici è un sottoinsieme algebrico. L'intersezione di ogni famiglia di sottoinsiemi algebrici è un sottoinsieme algebrico. L'insieme vuoto e $\mathbb{P}^n$ sono dei sottoinsiemi algebrici.*

Dimostrazione. È simile a quella del caso affine. □

Definizione 2.18: *Dal lemma precedente segue che i sottoinsiemi algebrici sono i chiusi di una topologia su $\mathbb{P}^n$. Questa topologia è la topologia di Zariski su $\mathbb{P}^n$.*

Osservazione 2.19: *Adesso che $\mathbb{P}^n$ ha una struttura di spazio topologico abbiamo, come nel caso affine, le nozioni di sottoinsieme algebrico irriducibile e di dimensione ("topologica").*

Definizione 2.20: *Una varietà proiettiva è un sottoinsieme algebrico irriducibile (per la topologia indotta dalla topologia di Zariski) di $\mathbb{P}^n$. Una varietà quasi-proiettiva è un aperto di una varietà proiettiva.*

Per riconoscere algebricamente le varietà proiettive abbiamo:

Lemma 2.21: *Un sottoinsieme algebrico $X \subseteq \mathbb{P}^n$ è irriducibile se e solo se $\mathbf{I}(X)$ è un ideale primo.*

Dimostrazione. Modulo il lemma seguente, è simile a quella del caso affine. □

Lemma 2.22: *Sia $I \subseteq k[X_0, \ldots, X_n]$ un ideale omogeneo. L'ideale I è primo se e solo se: $\forall P, Q$ omogenei, $PQ \in I \Rightarrow P \in I$ o $Q \in I$.*

Dimostrazione. Supponiamo I omogeneo tale che per ogni coppia di elementi omogenei (P, Q), $PQ \in I$ implica $P \in I$ o $Q \in I$, e mostriamo che I è primo. Sia $GH \in I$. Consideriamo le decomposizioni di G, H in elementi omogenei: $G = G_m + \ldots + G_0$, $H = H_t + \ldots + H_0$, $(\deg(G_i) = \deg(H_i) = i)$. Abbiamo $GH = \Sigma F_i$ con $F_i = \Sigma G_{i-k}.H_k$. Siccome I è omogeneo, $F_i \in I$ per ogni i. In particolare $G_m H_t \in I$ quindi $G_m \in I$ o $H_t \in I$. Se entrambi sono in I, ci riduciamo a considerare $G - G_m$, $H - H_t$ al posto di G, H. Supponiamo quindi $G_m \in I$ e $H_t \notin I$. Con questa ipotesi mostriamo, per induzione, che $G_i \in I$ per ogni i (quindi $G \in I$). Supponiamo di avere dimostrato che $G_m, \ldots, G_r$ sono in I. Abbiamo $F_{r-1+t} = G_{r-1}H_t + (G_r H_{t-1} + G_{r+1}H_{t-2} + \ldots) = G_{r-1}H_t + Q$ con $Q \in I$. Quindi $G_{r-1}H_t \in I$ e l'ipotesi implica $G_{r-1} \in I$. □

Finalmente, come nel caso affine, si dimostra:

Proposizione 2.23: *Ogni sottoinsieme algebrico non vuoto, X, di $\mathbb{P}^n$ ammette una ed un'unica decomposizione in componenti irriducibili: $X = X_1 \cup \ldots \cup X_r$, X_i irriducibili, con $X_i \neq X_j$ se $i \neq j$.*

Esercizi.

Esercizio 2.1: *Dimostrare il Lemma 2.5.*

3. Carte affini.

Iniziamo col definire la nozione di funzione regolare nel caso proiettivo. Ricordiamo che $f : \mathbb{A}^n \to k$ è regolare in x se, in un intorno di x, f è una funzione razionale, definita sull'intorno: $f = \frac{P}{Q}, Q(x) \neq 0$. Nel caso proiettivo questa definizione non si estende perché una funzione razionale, come un polinomio, non definisce in generale un'applicazione da $\mathbb{P}^n$ in k. C'è però un'eccezione: una funzione razionale $f = \frac{P}{Q}$ con P e Q omogenei e dello stesso grado definisce un'applicazione $\mathbb{P}^n \to k$ perché, se $d = \deg(P) = \deg(Q)$: $\frac{P(\lambda x_0,\dots,\lambda x_n)}{Q(\lambda x_0,\dots,\lambda x_n)} = \frac{\lambda^d P(x_0,\dots,x_n)}{\lambda^d Q(x_0,\dots,x_n)} = \frac{P(x_0,\dots,x_n)}{Q(x_0,\dots,x_n)}$. Questa osservazione ci porta alla seguente definizione: una funzione razionale, f, su $\mathbb{P}^n$ è un quoziente di due polinomi omogenei dello stesso grado; se $f = \frac{P}{Q}$, f è definita (o regolare) nei punti $z \in \mathbb{P}^n$ tali che $Q(z) \neq 0$. Per arrivare a questa definizione si può procedere diversamente: $\mathbb{P}^n$ è ricoperto dagli $U_i = \{(x_0 : \dots : x_n)/x_i \neq 0\}$, dove ogni U_i è in biiezione con $\mathbb{A}^n$. Come in geometria differenziale potremmo definire la struttura di varietà su $\mathbb{P}^n$ incollando le varie carte U_i, in particolare f è regolare in $x = (x_0 : \dots : x_n)$, $x_0 \neq 0$, se $f \circ y_0$ è regolare in $u = j_0(x)$, dove $y_0^{-1} = j_0 : U_0 \to \mathbb{A}^n : (x_0 : \dots : x_n) \longmapsto (u_1, \dots, u_n)$ con $u_i = \frac{x_i}{x_0}$. Se $f \circ y_0$ è regolare in un intorno di u allora $f \circ y_0(u) = \frac{p(u)}{q(u)}$. Scriviamo p e q come somme di polinomi omogenei: $p = p_d + \dots + p_i + \dots + p_0$, $q = q_r + ... + q_i + \dots + q_0$, p_i e q_i omogenei di grado i. Abbiamo:
$p_i(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}) = \frac{1}{x_0^i} p_i(x_1, \dots, x_n)$, quindi

$$p(\frac{x_1}{x_0}, \dots, \frac{x_n}{x_0}) = \frac{p_d(x_1, ..., x_n) + ... + x_0^{d-i} p_i(x_1, ..., x_n) + ... + x_0^d p_0}{x_0^d}$$

.

Poniamo $p^*(x_0, \dots, x_n) := p_d(x_1, \dots, x_n) + \dots + x_0^{d-i} p_i(x_1, \dots, x_n) + \dots + x_0^d p_0$, è un polinomio omogeneo di grado $d = \deg(p)$ (è l'omogeneizzato di p). Procedendo in modo analogo con q, abbiamo: $p(u)/q(u) = \frac{x_0^r p^*(x)}{x_0^d q^*(x)}$, cioè un quoziente di due polinomi omogenei dello stesso grado in $x_0, \dots, x_n$.

Definizione 3.1: *Sia $Y \subseteq \mathbb{P}^n$ una varietà quasi-proiettiva. Un'applicazione $f : Y \to k$ è regolare in $y \in Y$ se esiste un intorno aperto $U \subseteq Y$ di y, e due polinomi omogenei dello stesso grado P, Q con Q che non si annulla su U, tali che $f = \frac{P}{Q}$ su U. La funzione f è regolare su Y se è regolare in ogni punto di Y.*

Osservazione 3.2: *Come nel caso affine si dimostra che una funzione regolare è continua e che se due funzioni regolari coincidono su un aperto non vuoto della varietà Y, allora coincidono su tutto Y.*

Adesso cerchiamo di uniformare le definizioni date finora.

Definizione 3.3: *Una varietà (algebrica, su k) è una varietà affine, quasi-affine, proiettiva o quasi-proiettiva. Se X e Y sono due varietà, un morfismo $\varphi : X \to Y$ è* *un'applicazione continua tale che per ogni aperto $V \subseteq Y$ e per ogni funzione regolare $f : V \to k$, la funzione $f \circ \varphi : \varphi^{-1}(V) \to k$ sia regolare.*

Osservazione 3.4: *La definizione di varietà algebrica data qui sopra non è quella più generale (le nostre varietà sono immerse in $\mathbb{A}^n$ o $\mathbb{P}^n$, la definizione di funzione regolare, e quindi di morfismo, usa questa immersione). Comunque sia la definizione precedente introduce quello che sarà per noi la categoria delle varietà algebriche su k (perché ovviamente la composizione di due morfismi è un morfismo). In particolare abbiamo la nozione di isomorfismo: è un morfismo biiettivo,f, tale che anche f^{-1} sia un morfismo. Osservare che esistono dei morfismi biiettivi, bicontinui che non sono degli isomorfismi.*

Osservazione 3.5: *Se, come già detto, definiamo una funzione razionale su $\mathbb{P}^n$ come un quoziente di polinomi omogeni dello stesso grado allora abbiamo una definizione uniforme di funzione regolare su una varietà $X \subseteq E$ ($E = \mathbb{A}^n$ o $\mathbb{P}^n$): $f : X \to k$ è regolare in $x \in X$ se in un intorno U di x in X coincide con una funzione razionale su E, definita (cioè regolare) su U. In altri termini una funzione è regolare in x (cioè è localmente in x un morfismo in k) se è una funzione razionale su X, regolare (cioè definita) in x; una tale funzione si esprime come la restrizione di una funzione razionale $\frac{P}{Q}$ su E, ma questa rappresentazione non è unica ($\frac{P}{Q} = \frac{R}{S}$ se $PS - QR \in \mathbb{I}(X)$). Come vedremo, un morfismo $X \to Y$ tra due varietà è un'applicazione razionale regolare (definita) su tutto X.*

Osservazione 3.6: *La grossa differenza tra il caso affine e il caso proiettivo risiede nel fatto che su una varietà proiettiva, ogni funzione regolare (su tutta la varietà) è costante.*

Nel caso di $\mathbb{P}^1$ questo si può vedere così: darsi una funzione regolare $f : \mathbb{P}^1 \to k$ consiste nel darsi una funzione regolare $f_0 : U_0 \to k$, e una funzione regolare $f_1 : U_1 \to k$ tali che $f_0 = f_1$ su $U_0 \cap U_1$. Una funzione regolare $U_0 \simeq \mathbb{A}^1 \to k$ è una funzione polinomiale $f_0(u) = \sum\limits_{0\leq i\leq d} a_i u^i$, cioè $f_0(\frac{x_1}{x_0}) = \sum\limits_{0\leq i\leq d} a_i(\frac{x_1}{x_0})^i$ $= (\sum\limits_{0\leq i\leq d} a_i x_1^i.x_0^{d-i})/x_0^d$. Nello stesso modo $f_1(v) = \sum\limits_{0\leq j\leq r} b_j v^j$, ossia $f_1(\frac{x_0}{x_1}) =$ $(\sum\limits_{0\leq j\leq r} b_j x_0^j.x_1^{r-j})/x_1^r$. In un punto $(x_0 : x_1)$ di $U_0 \cap U_1$ si deve avere:
$(\sum\limits_{0\leq i\leq d} a_i x_1^i.x_0^{d-i})/x_0^d = (\sum\limits_{0\leq j\leq r} b_j x_0^j.x_1^{r-j})/x_1^r$, cioè $P(x_0, x_1) = \sum\limits_{0\leq i\leq d} a_i x_1^{i+r}.x_0^{d-i} -$ $\sum\limits_{0\leq j\leq r} b_j x_0^{j+d}.x_1^{r-j} = 0$. Il polinomio $P(x_0, x_1)$ è omogeneo di grado $d + r$ e ha un'infinità di radici (in $\mathbb{P}^1$), questo implica (Esercizio) che $P(x_0, x_1) = 0$, quindi i coefficienti (rispetto alla base $x_0^{d+r-i}x_1^i$, $0 \leq i \leq d + r$) di P sono nulli. Gli a_i sono coefficienti di monomi nei quali x_0 compare con una potenza $\leq d$, mentre i b_j sono coefficienti di monomi nei quali x_0 compare con una potenza $\geq d$. Pertanto $a_0 = b_0$, $a_i = b_j = 0$ se $i > 0$, $j > 0$, e f è la funzione costante uguale a a_0.

Per completare il quadro, e per vedere che possiamo sempre prendere $E = \mathbb{P}^n$ qui sopra, mostriamo che $\varphi_0 : U_0 \to \mathbb{A}^n$ è un isomorfismo di varietà. Per questo ci servono alcuni preliminari sulla (de)omogeneizzazione dei polinomi:

Definizione 3.7: *Sia $f(t_1,\dots,t_n) \in k[t_1,\dots,t_n]$ un polinomio in n variabili. Sia $f = f_d+\dots+f_i+\dots+f_0$ la decomposizione di f come somma di polinomi omogenei (f_i omogeneo di grado i). L'omogeneizzato di f (rispetto alla variabile X_0), è il polinomio in $n+1$ variabili:*

$$f^*(X_0,X_1,\dots,X_n) := f_d(X_1,\dots,X_n) + \dots + X_0^i f_i(X_1,\dots,Xn) + \dots + X_0^d f_0.$$

Sia $F(X_0,X_1,\dots,X_n) \in k[X_0,X_1,\dots,X_n]$ un polinomio omogeneo in $n+1$ variabili. Il deomogeneizzato di F (rispetto alla variabile X_0), è il polinomio in n variabili: $F_*(t_1,\dots,t_n) := F(1,t_1,\dots,t_n)$.

Osservazione 3.8: *Le proprietà seguenti sono di facile verifica (Esercizi):*
$(f^*)_* = f$; $X_0^t(F_*)^* = F$ dove t è la più grande potenza di X_0 che divide F,
$(fg)^* = f^*g^*$, $(FG)_* = F_*G_*$.

Proposizione 3.9: *Per ogni i, $0 \le i \le n$, l'applicazione*

$$\varphi_i : U_i \to \mathbb{A}^n : (\dots : x_k : \dots) \to (\dots, \frac{x_k}{x_i}, \dots)$$

è un isomorfismo di varietà.

Dimostrazione. Possiamo assumere $i = 0$, e scrivere φ invece di φ_0. Sappiamo già che φ è biiettiva e che $\varphi^{-1} = \psi$. Mostriamo che φ è un omeomorfismo.

- (i) Continuità di φ: sia $X \subseteq \mathbb{A}^n$ un chiuso. Sia $\mathbb{I}(X) = (f_1,\dots,f_r)$ l'ideale di X, allora $X' := \mathbf{V}(f_1^*,\dots,f_r^*)$ è un chiuso di $\mathbb{P}^n$. Basta mostrare che $\varphi^{-1}(X) = X' \cap U_0$ (✠) per avere che $\varphi^{-1}(X)$ è chiuso in U_0. Se $x = (x_0 : \dots : x_n) \in \mathbb{P}^n$: $f^*(x_0 : \dots : x_n) = 0 \Leftrightarrow f^*(1 : \frac{x_1}{x_0} : \dots : \frac{x_n}{x_0}) = 0$, ma $f_*(1 : \frac{x_1}{x_0} : \dots : \frac{x_n}{x_0}) = f(\varphi(x))$. Usando questa osservazione, (✠) segue immediatamente.
- (ii) φ è chiusa (continuità di ψ): sia $Y \subseteq U_0$ un chiuso, quindi $Y = U_0 \cap Y'$ dove $Y' \subseteq \mathbb{P}^n$ è chiuso. Se $\mathbb{I}(Y') = (F_1,\dots,F_t)$, sia $Z \subseteq \mathbb{A}^n$ il chiuso $Z = \mathbf{V}(F_{1*},\dots,F_{t*})$. Basta mostrare $\varphi(Y) = Z$; come prima, questo segue da: $F(x) = 0 \Leftrightarrow F_*(\varphi(x)) = 0$.

Rimane da vedere che φ e ψ trasformano funzioni regolari in funzioni regolari. Sia f una funzione regolare in un intorno di $t \in \mathbb{A}^n$, quindi $f = \frac{p}{q}$ su un intorno, V, di $t = \varphi(x)$. Allora, come già visto, $(f \circ \varphi)(x) = \frac{x_0^r p^*(x)}{x_0^d q^*(x)}$ ($r = \deg(q)$, $d = \deg(p)$) su $\varphi^{-1}(V)$; quindi φ trasforma funzioni regolari in funzioni regolari. Sia adesso g regolare in un intorno di $x \in U_0$, allora $g = \frac{P}{Q}$ in un intorno A di x, e $(g\circ\psi)(u) = \frac{P_*(u)}{Q_*(u)}$ su $\psi^{-1}(A)$; quindi anche ψ trasforma funzioni regolari in funzioni regolari. □

Osservazione 3.10: (*i*) *Segue che per ogni* i, j *l'applicazione:* $\varphi_j \circ \psi_i \colon \varphi_i(U_{ij}) \to \varphi_j(U_{ij})$ *dove* $U_{ij} := U_i \cap U_j$, *è un isomorfismo.*

(*ii*) *Grazie alla Proposizione precedente, per studiare questioni locali ci possiamo ricondurre a lavorare nell'affine.*

Esercizi.

Esercizio 3.1: *Dimostrare l'Osservazione 3.8.*

Esercizio 3.2: *Sia* $\mathbf{S} = k[X_0, \ldots, X_n]$ *e* $\mathbf{S}_d$ *il sottospazio vettoriale dei polinomi omogenei di grado* d *nelle variabili* $X_0, \ldots, X_n$*. Dimostrare che la dimensione del* k*-spazio vettoriale* $\mathbf{S}_d$ *è* $\binom{n+d}{n}$ *(coefficiente binomiale).*

Esercizio 3.3: (i) *Sia* $P \in k[X_0, X_1]$ *un polinomio omogeneo di grado* d*.*
Dimostrare che P *si scrive come un prodotto di* d *forme lineari:*
$P(X_0, X_1) = \prod_i L_i(X_0, X_1)$*, dove gli* L_i *sono dei polinomi omogenei di grado uno (se il coefficiente di* X_0^d *è non nullo, considerare* P_**, il deomogeneizzato rispetto a* X_0*; si ricorda che* k *è algebricamente chiuso). La fattorizzazione di* P *come prodotto di forme lineari è unica modulo costanti.*
(ii) *Un punto* $z \in \mathbb{P}^1$ *è "radice" del polinomio omogeneo* $P(X_0, X_1)$ *se* $P(z) = 0$*. Dimostrare che un polinomio omogeneo di grado* d *ammette* d *radici , contate con molteplicità. (usare* (i)*)*

Esercizio 3.4: *Dimostrare che ogni funzione regolare* $f : \mathbb{P}^n \to k$ *è costante. (induzione su* n*, usando Osservazione 3.6)*

4. Curve algebriche piane: generalità.

Sia $\mathbf{S} = k[X, Y, Z]$e $\mathbf{S}_d := k[X, Y, Z]_d$, lo spazio vettoriale dei polinomi omogenei di grado d nelle tre variabili X, Y, Z. Si verifica che $\mathbf{S}_d$ è un k-spazio vettoriale di dimensione $\frac{(d+2)(d+1)}{2}$ (cfr. Esercizi).

Possiamo considerare lo spazio proiettivo $\mathbb{P}(\mathbf{S}_d)$ associato allo spazio vettoriale $\mathbf{S}_d$. Un elemento di $\mathbb{P}(\mathbf{S}_d)$ è una classe d'equivalenza costituita da tutti i multipli non nulli di un polinomio omogeneo di grado d, $\overline{F} := \{\lambda F(X, Y, Z)/\ \lambda \in k^*\}$. Chiaramente i luoghi degli zeri $\mathbf{V}(F) \subset \mathbb{P}^2$ e $\mathbf{V}(\lambda F) \subset \mathbb{P}^2$ sono uguali.

Definizione 4.1: *Una curva algebrica piana proiettiva, C, è un elemento di $\mathbb{P}(\mathbf{S}_d)$ per qualche $d \geq 1$. Se $F(X, Y, Z)$ è un rappresentante di C si dice che $F(X, Y, Z) = 0$ è un'equazione di C (o per abuso di linguaggio, l'equazione di C). Il grado di C è il grado del polinomio $F(X, Y, Z)$. Il sottoinsieme algebrico $\mathbf{V}(F) \subset \mathbb{P}^2$ si chiama il supporto di C.*

Osservazione 4.2: *Due curve algebriche distinte, C, C', possono avere lo stesso supporto: per esempio C di equazione $X = 0$ e C' di equazione $X^2 = 0$ hanno lo stesso supporto, ma sono curve diverse (hanno gradi diversi). Quindi il luogo geometrico individuato dal supporto non è sufficiente per determinare una curva: bisogna considerare l'equazione algebrica. Questa definizione di curva è diversa da quella data in precedenza (insieme algebrico di dimensione uno), ed è quella che si avvicina di più al concetto di schema.*
Benché una curva non sia un luogo di punti ma una classe di equivalenza di polinomi, ci capiterà di scrivere: " Sia $C \subseteq \mathbb{P}^2$ una curva ", si terrà comunque sempre presente la differenza tra supporto ed equazione.

Definizione 4.3: *Una curva C di equazione $F = 0$ si dice irriducibile se il polinomio F è irriducibile.*

Osservazione 4.4: *C'è una corrispondenza biunivoca tra curve irriducibili e sottovarietà di dimensione uno di $\mathbb{P}^2$.*
Una curva irriducibile è completamente determinata dal suo supporto (questo giustifica l'abuso di linguaggio precedente).
Se C è riducibile (i.e. non irriducibile) sia $F = \prod_i F_i^{a_i}$ una decomposizione in fattori irriducibili del polinomio F. Abbiamo $\mathbf{V}(F) = \mathbf{V}(F_1) \cup \ldots \cup \mathbf{V}(F_r)$: è la decomposizione in componenti irriducibili del sottoinsieme algebrico $\mathbf{V}(F)$.

Definizione 4.5: *Nella situazione precedente, se $a_i \geq 2$, la curva C_i di equazione $F_i = 0$ è una componente multipla (di molteplicità a_i) di C. Se invece ogni a_i è uguale a uno, si dice che C è ridotta (o priva di componenti multiple).*

4.1. Curve affini. In modo analogo a quanto fatto nel caso proiettivo si definisce la nozione di curva affine piana:

Definizione 4.6: *Una curva algebrica, affine, piana è una classe di proporzionalità di polinomi non costanti di* $k[X, Y]$. *Se* $f(X, Y) = 0$ *è un rappresentante della curva si dice che* $f(X, Y) = 0$ *è un'equazione (o l'equazione) della curva. Il sottoinsieme algebrico* $\mathbf{V}(f) \subset \mathbb{A}^2$ *è il supporto della curva; il grado della curva è il grado di* f.

4.2. Il passaggio affine-proiettivo (andata-ritorno). Sia $C \subseteq \mathbb{P}^2$ una curva piana proiettiva di equazione $F(X, Y, Z) = 0$. Il piano proiettivo è ricoperto dagli aperti affini $U_x = \{(x : y : z)/\ x \neq 0\}$, $U_y = \{(x : y : z)/\ y \neq 0\}$, $U_z = \{(x : y : z)/\ z \neq 0\}$. Ognuno di questi aperti è in biiezione (in effetti isomorfo) con il piano $\mathbb{A}^2$; per esempio:

$\varphi_x : U_x \to \mathbb{A}^2 : (x : y : z) \longmapsto (\frac{y}{x}, \frac{z}{x})$;

$\varphi_x^{-1} : \mathbb{A}^2 \to U_x : (u, v) \longmapsto (1 : u : v)$.

Un buon modo per studiare $\mathbf{V}(F)$ consiste nel considerare le intersezioni $\mathbf{V}(F) \cap U_x, \ldots, \mathbf{V}(F) \cap U_z$, come sottoinsiemi di $\mathbb{A}^2$. Cerchiamo quindi di determinare $C_x := \varphi_x(\mathbf{V}(F) \cap U_x) \subset \mathbb{A}^2$.

Un punto $(x_0 : y_0 : z_0)$ di $\mathbb{P}^2$ appartiene a $\mathbf{V}(F) \cap U_x$ se:

(i) $x_0 \neq 0$;

(ii) $F(x_0, y_0, z_0) = 0$.

Abbiamo $F(x, y, z) = \Sigma a_{ijk} x^i y^j z^k$ con $i + j + k = d$ (F è omogeneo di grado d).

Siccome $x_0 \neq 0$ possiamo scrivere:

$F(x_0, y_0, z_0) = \Sigma a_{ijk} (\frac{y_0}{x_0})^j (\frac{z_0}{x_0})^k x_0^i x_0^{j+k} = x_0^d (\Sigma a_{ijk} (\frac{y_0}{x_0})^j (\frac{z_0}{x_0})^k) = x_0^d . F(1, \frac{y_0}{x_0}, \frac{z_0}{x_0})$.

Siccome $x_0 \neq 0$, vediamo che: $F(x_0, y_0, z_0) = 0 \Leftrightarrow F(1, \frac{y_0}{x_0}, \frac{z_0}{x_0}) = 0$. In conclusione:

Lemma 4.7: *Se* $C_x := \varphi_x(\mathbf{V}(F) \cap U_x) \subset \mathbb{A}^2$, *allora* $C_x = \{(u, v) \in \mathbb{A}^2 / F_*(u, v) = 0\}$, *dove* F_* *indica il deomogeneizzato di* F *rispetto alla variabile* x.

Osservazione 4.8: *(i) Sarebbe più preciso scrivere* $F_{*,X}$, *ma il contesto indicherà sempre chiaramente la variabile rispetto alla quale si deomogeneizza.*

(ii) Si sarebbe tentati di dire che $\varphi_x(\mathbf{V}(F) \cap U_x)$ *è la curva affine di equazione* $F_*(u, v) = 0$. *Questo è inesatto in quanto può succedere che il polinomio* $F_*(u, v)$ *sia costante (e quindi non è l'equazione di una curva). Questo succede se e solo se* $F(X, Y, Z) = X^n$ *(i.e. il supporto di* C *coincide con la retta "all'infinito").*

(iii) Il grado di F_* *può essere diverso dal grado di* F. *Questo succede se e solo se* $X | F(X, Y, Z)$. *Più precisamente se* $X^r | F$ *e* X^{r+1} *non divide* F *allora* $\deg(F_*) + r = \deg(F)$. *Per esempio se* $F(X, Y, Z) = X^2(Y + Z)$ *allora* $F_*(u, v) = u + v$. *A parte inconvenienti di questo tipo si osserverà che il passaggio da* C *a* C_x *conserva non solo il supporto ma anche le molteplicità.*

In conclusione il passaggio da F a F_* (dalla curva $C \subseteq \mathbb{P}^2$ alla curva $C_x \subseteq \mathbb{A}^2$) ci fa "perdere":

- *i punti dell'intersezione $C \cap L$ (L è la retta all'infinito, $X = 0$).*
- *un'eventuale componente irriducibile (con eventuale molteplicità) avente per supporto la retta L.*

La curva C_x é la parte affine di C (relativamente a U_x). Considerando tutte le parti affini C_x, C_y, C_z vediamo tutta la curva, pezzo per pezzo. Questo è molto utile per considerazioni locali.

Sia adesso $X \subseteq \mathbb{A}^2$ una curva di equazione $f(u,v) = 0$. Possiamo immergere $\mathbb{A}^2$ in $\mathbb{P}^2$ tramite $\varphi_x^{-1} : \mathbb{A}^2 \to \mathbb{P}^2 : (u,v) \longmapsto (1 : u : v)$ e quindi considerare la chiusura (nella topologia di Zariski) di $\varphi_x^{-1}(X) \subset \mathbb{P}^2$: otteniamo così un sottoinsieme algebrico Y di $\mathbb{P}^2$. Cerchiamo di individuare Y. Un punto $(x_0 : y_0 : z_0)$ appartiene a $\varphi_x^{-1}(X)$ se e solo se:

(i) $x_0 \neq 0$;
(ii) $f(\frac{y_0}{x_0}, \frac{z_0}{x_0}) = 0$.

Sia f^* l'omogeneizzato di f. Siccome $x_0^n\, f(\frac{y_0}{x_0}, \frac{z_0}{x_0}) = f^*(x_0, y_0, z_0)$, vediamo (usando (i)) che $(x_0 : y_0 : z_0) \in \varphi_x^{-1}(X)$ se e solo se $f^*(x_0, y_0, z_0) = 0$. Concludiamo che Y è il supporto della curva algebrica di equazione $f^*(x,y,z) = 0$.

Definizione 4.9: *Con le notazioni precedenti la curva $C \subseteq \mathbb{P}^2$ di equazione $f^* = 0$ si chiama la chiusura proiettiva della curva $X \subseteq \mathbb{A}^2$.*

Osservazione 4.10: *Visto che $(f^*)_* = f$, la parte affine (rispetto a U_x) della curva C è la curva iniziale $X \subseteq \mathbb{A}^2$.*

4.3. Molteplicità d'intersezione con una retta in un punto. Sia $C \subseteq \mathbb{A}^2$ una curva di equazione $f(x,y) = 0$. Se $p \in C$ e se L è una retta passante per p vogliamo definire la molteplicità d'intersezione della curva C e della retta L nel punto p. Per questo procediamo come nel caso delle varietà ma prendendo come ideale di C l'ideale (f). Quindi se $L = \{(1-t)p + tq\}$, $i(C, L; p)$ è la molteplicità della radice $t = 0$ nell'equazione $f((1-t)p + tq) = 0$. Per esempio se C ha equazione $x^2 = 0$ e se L è la retta $y = 0$ allora $i(C, L; O) = 2$ (dove O indica l'origine). Osservare che il risultato trovato tiene conto dell'equazione algebrica e non del supporto della curva.

Sia adesso $X \subseteq \mathbb{P}^2$ la curva di equazione $F(X,Y,Z) = 0$, $p \in X$, e R una retta di $\mathbb{P}^2$, di equazione $G(X,Y,Z) = 0$, passante per p. Per definire la molteplicità d'intersezione di X e R nel punto p possiamo procedere in vari modi. Per esempio osservando che si tratta di una questione locale, possiamo prendere una carta affine contenente p e ricondurci a calcolare $i(C, L; p)$ dove C è la curva di equazione

$F_* = 0$, L la retta di equazione $G_* = 0$. Dopo avere dimostrato che il numero trovato non dipende dalle scelte fatte (carta affine) si pone $i(X, R; p) = i(C, L; p)$.

Altrimenti si può procedere direttamente nel proiettivo. Sia q un altro punto della retta R; quindi $R = \{\lambda p + \mu q / \ (\lambda : \mu) \in \mathbb{P}^1\}$. Consideriamo $F(\lambda p + \mu q) := F(\lambda p_1 + \mu q_1, \lambda p_2 + \mu q_2, \lambda p_3 + \mu q_3)$, dove $p = (p_1 : p_2 : p_3)$, $q = (q_1 : q_2 : q_3)$. Il polinomio $F(\lambda p + \mu q)$ è omogeneo nelle variabili λ, μ di grado $d = \deg(F)$ (R non contenuta in X). Quindi questo polinomio si decompone in un prodotto di d (contate con molteplicità) forme lineari:

$F(\lambda p + \mu q) = L_1^{\alpha_1}(\lambda, \mu) \dots L_r^{\alpha_r}(\lambda, \mu)$, $\alpha_1 + \dots + \alpha_r = d$, $L_i(\lambda, \mu) = a_i \lambda + b_i \mu$. Pertanto $X \cap R$ è dato dal luogo degli zeri in $\mathbb{P}^1$ (con coordinate $(\lambda : \mu)$) di $F(\lambda p + \mu q)$, cioè dai punti $(-b_i : a_i)$, $i = 1, \dots, r$. Tra questi c'è il punto $(1 : 0)$ (perché $p \in X \cap R$), e possiamo assumere $(-b_1 : a_1) = (1 : 0)$. Si pone allora $i(X, R; p) := \alpha_1$. Rimane da verificare che questa definizione non dipende dalla scelta del punto q; questo si fa nel solito modo.

Il lettore si convincerà da solo che i due procedimenti sono equivalenti.
D'ora in poi considereremo il caso affine come un caso particolare ("locale") del caso proiettivo.
Come prima applicazione abbiamo una versione "debole" del teorema di Bezout:

Proposizione 4.11: *Sia $X \subseteq \mathbb{P}^2$ una curva di grado d e sia $R \subseteq \mathbb{P}^2$ una retta non contenuta in X. Allora X e R s'intersecano in d punti contati con molteplicità. Più precisamente:* $\sum_{p \in X \cap R} i(X, R; p) = d$.

DIMOSTRAZIONE. Con le notazioni precedenti il polinomio $F(\lambda p + \mu q)$ ha d radici ("in $\mathbb{P}^1$") contate con molteplicità. □

Osservazione 4.12: *Otteniamo un'interpretazione geometrica del grado di una curva: è il numero di punti (contati con molteplicità) in cui una retta generica incontra la curva.*

4.4. Spazio tangente di Zariski.

Sia $p \in C \subseteq \mathbb{P}^2$, e sia R una retta per p.

Definizione 4.13: *La retta R è tangente a C in p se $i(C, R; p) = 2$.*
Lo spazio tangente ("immerso") di Zariski a C nel punto p è: $T_pC = \{q \in \mathbb{P}^2 / \ \exists\ L$ tangente a C in p tale $q \in L\}$ = unione delle rette tangenti a C in p.

Osservazione 4.14:
- (i) *Lo spazio tangente ("immerso") di Zariski a C nel punto p è un sottospazio lineare di $\mathbb{P}^2$, cioè una retta passante per p ("la tangente") o tutto $\mathbb{P}^2$.*
- (ii) *Nel caso affine la definizione è analoga a quella per le varietà ma usando l'equazione della curva. Se $C \subseteq \mathbb{A}^2$ di equazione $f(x, y) = 0$ allora T_pC è il*

sottospazio affine passante per p *di direzione* $\{(x,y)/\ (\frac{\partial f}{\partial x}(p), \frac{\partial f}{\partial y}(p)).\begin{pmatrix} x \\ y \end{pmatrix} = 0\}$. *In particolare ci sono solo due possibilità:*

(a) $(\frac{\partial f}{\partial x}(p), \frac{\partial f}{\partial y}(p)) \neq (0,0)$ *e* T_pC *è la retta di equazione:*

$$(x-x_0)\frac{\partial f}{\partial x}(p) + (y-y_0)\frac{\partial f}{\partial y}(p) = 0 \ (p = (x_0, y_0));$$

(b) $(\frac{\partial f}{\partial x}(p), \frac{\partial f}{\partial y}(p)) = (0,0)$ *e* $T_pC = \mathbb{A}^2$.

Nel caso (a) p *è un punto liscio della curva, nel caso* (b) p *è un punto singolare di* C.

(iii) *Sia* C *una curva riducibile, di equazione* $f = gh$. *Siano* C', C'' *le curve di equazioni* $g = 0$, $h = 0$. *Se* $p \in C' \cap C''$ *allora* p *è un punto singolare di* C.

(iv) *Sia* C *una curva non ridotta, di equazione* $f^n = 0$. *Allora, contrariamente a quanto avviene per le varietà ogni punto di* C *è singolare!*

Sia $C \subseteq \mathbb{P}^2$, $p \in C$. Per determinare lo spazio tangente di Zariski a C in p possiamo prendere una carta affine contenente p, calcolare nell'affine e poi omogeneizzare lo spazio tangente trovato. Per esempio sia C di equazione $X^2 - Y^2 + Z^2 = 0$, e $p = (1:1:0)$. Prendiamo la carta affine U_x, dobbiamo calcolare lo spazio tangente alla curva di equazione $f(y,z) = 1 - y^2 + z^2 = 0$ nel punto $(1,0)$. Troviamo che la curva ha una tangente di equazione $y = 1$. Omogeneizzando viene che la curva C è liscia in p, e la tangente in p è la retta di equazione $Y = X$.

C'è però un modo più veloce di procedere usando la relazione di Eulero per i polinomi omogenei:

Lemma 4.15: *Sia* $F(X_0, \ldots, X_n)$ *un polinomio omogeneo di grado* d. *Allora:*
$d.F(X_0, ..., X_n) = \sum\limits_{i=0}^{n} X_i.\frac{\partial F}{\partial x_i}(X_0, ..., X_n)$.

Dimostrazione. Siccome F è omogeneo di grado d, $F(\lambda X_0, \ldots, \lambda X_n) = \lambda^d.F(X_0, \ldots, X_n)$. Derivando rispetto a λ viene: $\sum\limits_{i=0}^{n} X_i \frac{\partial F}{\partial X_i}(\lambda X_0, \ldots, \lambda X_n) = d\lambda^{d-1}.F(X_0, \ldots, X_n)$. Ponendo $\lambda = 1$ si ottiene l'asserto. □

Tornando alle curve piane proiettive:

Lemma 4.16: *Sia* $C \subseteq \mathbb{P}^2$ *una curva di equazione* $F(X_0, X_1, X_2) = 0$ *e sia* p *un punto di* C*:*

(i) p *è un punto liscio di* C *se e solo se una delle derivate parziali* $\frac{\partial F}{\partial x_i}(p)$ *è non nulla;*

(ii) *Se* p *è un punto liscio di* C, *la tangente a* C *in* p *è la retta di equazione:*

$$\sum_{i=0}^{2} X_i \frac{\partial F}{\partial X_i}(p) = 0.$$

DIMOSTRAZIONE. (*i*) Sia $p = (p_0 : p_1 : p_2)$, supponiamo $p_i \neq 0$ e guardiamo nella carta affine U_i. Notiamo p' il punto di coordinate $(..\frac{p_j}{p_i}...)$ immagine di p nell'affine, e poniamo $x_j := \frac{X_j}{X_i}$ $(j \neq i)$. L'osservazione di base è che se F_* indica il deomogeneizzato di F rispetto a X_i, allora:

$$p_i^{d-1} \frac{\partial F_*}{\partial X_j}(p') = \frac{\partial F}{\partial X_j}(p)$$

Per vederlo, per linearità della derivata, basta verificarlo su un monomio $X^i Y^j Z^t$. Se p è non singolare, esiste j tale che $\frac{\partial F_*}{\partial X_j}(p') \neq 0$ $(j \neq i)$, e quindi anche $\frac{\partial F}{\partial X_j}(p) \neq 0$. Viceversa supponiamo che esista j tale che $\frac{\partial F}{\partial X_j}(p) \neq 0$. Se $j \neq i$, come prima siamo a posto. Se $\frac{\partial F}{\partial X_i}(p)$ è l'unica derivata non nulla, dalla relazione di Eulero viene: $p_i \frac{\partial F}{\partial X_i}(p) = d.F(p)$, ma questo è assurdo perché $F(p) = 0$.

(*ii*) Se p è un punto nonsingolare di C, la sua tangente è l'omogeneizzata della retta affine di equazione $(x_j - p_j)\frac{\partial F_*}{\partial x_j}(p') + (x_t - p_t)\frac{\partial F_*}{\partial x_j}(p') = 0$; ossia $x_j \frac{\partial F_*}{\partial x_j}(p') + x_t \frac{\partial F_*}{\partial x_t}(p') = p_j \frac{\partial F_*}{\partial x_j}(p') + p_t \frac{\partial F_*}{\partial x_t}(p')$. Omogeneizzando viene: $X_j \frac{\partial F}{\partial X_j}(p) + X_t \frac{\partial F}{\partial X_t}(p) = X_i(p_j \frac{\partial F}{\partial X_j}(p) + p_t \frac{\partial F}{\partial X_t}(p))$. Moltiplicando per p_i^{d-1} e usando la relazione di Eulero al secondo membro si ottiene il risultato cercato.

□

Osservazione 4.17: *Lo stesso ragionamento funziona con più variabili, cioè per ipersuperfici di equazione* $F(X_0, \ldots, X_n) = 0$ *in* $\mathbb{P}^n$.

Esercizi.

Esercizio 4.1: *Dimostrare l'Osservazione 4.14.*

Esercizio 4.2: *Per ogni* $n \geq 1$ *esiste una curva liscia di grado* n *in* $\mathbb{P}^2$.

Esercizio 4.3: *Sia* $C \subseteq \mathbb{P}^2$ *la curva di equazione* $Y^2Z - X^3 + XZ^2 = 0$. *Determinare la tangente,* R*, a* C *nel punto* $p = (0 : 1 : 0)$. *Calcolare la molteplicità d'intersezione* $i(C, R; p)$.

Esercizio 4.4: *Sia* $C \subseteq \mathbb{P}^2$ *una curva liscia. Per ogni* $p \in C$ *sia* T_pC *la tangente a* C *in* p. *Definiamo un'applicazione* $f : C \to C \subseteq \mathbb{P}_2 : p \longmapsto T_pC$. *Si ammetterà che l'immagine,* C^**, di* C *è una curva algebrica (lo potreste giustificare, anche molto vagamente?). La curva* C^* *si chiama la curva "duale" di* C.
Sia $X \subseteq \mathbb{P}^2$ *la conica di equazione* $Y^2 - XZ = 0$. *Dimostrare che* X *è liscia e determinare la curva duale* X^*.

Esercizio 4.5: *(i) Mostrare che la superficie* $Q \subset \mathbb{P}^3$ *di equazione* $xz - yt = 0$ *è non singolare.*

(ii) Descrivere il piano tangente a Q *in un suo punto* p.

(iii) Determinare il luogo singolare della superficie $Q' \subset \mathbb{P}^3$*, di equazione* $x^2 + y^2 - z^2 = 0$. *Determinare lo spazio tangente a* Q' *nel punto* $(1 : 0 : 1 : 1)$. *Più generalmente descrivere lo spazio tangente a* Q' *in un suo punto* p.

5. Singolarità delle curve piane.

In questo paragrafo ci proponiamo di studiare la struttura locale delle curve piane.
Trattandosi appunto di questioni locali lavoreremo soprattutto nell'affine.

Definizione 5.1: *Sia C una curva piana (affine o proiettiva) e sia p un punto del piano. La molteplicità, $m_p(C)$, di C in p (o di p per C) è:*

$$m_p(C) := \min_{p\in L}\{i(C,L;p)\}.$$

Osservazione 5.2: (*i*) *Se $p \notin C$, si pone $m_p(C) = 0$. Se $p \in C$, allora p è un punto nonsingolare di C se e solo se $m_p(C) = 1$. Intuitivamente $m_p(C)$ misura "quante" volte la curva C passa per il punto p. Questo però va preso con le dovute cautele: consideriamo la cuspide di equazione $y^2 = x^3$, se p è l'origine allora $m_p(C) = 2$ (e C passa solo una volta per l'origine).*

(*ii*) *Si ha $0 \leq m_p(C) \leq \deg(C)$.*

(*iii*) *Se $m_p(C) = 2$, p si dice punto doppio (per C); se $m_p(C) = 3$, p si dice punto triplo (per C), ecc (un punto liscio, cioè con $m_p(C) = 1$ si dice anche punto semplice).*

Come calcolare la molteplicità di una curva in un punto? Facciamo prima un caso particolare:

Sia $C \subseteq \mathbb{A}^2$ la curva di equazione $f(x, y) = 0$ con $f(0, 0) = 0$, e cerchiamo di calcolare $m_O(C)$ dove $O = (0, 0)$. Decomponiamo f come somma di polinomi omogenei:

$f(x, y) = f_n(x, y)+f_{n-1}(x, y)+\ldots+f_1(x, y)$, dove $f_i(x, y)$ è omogeneo di grado i nelle variabili x, y.

Lemma 5.3: *Con le notazioni precedenti $m_O(C) = m \Leftrightarrow f_1 = \ldots = f_{m-1} = 0$, e $f_m \neq 0$.*

Dimostrazione. Sia $Q = (q, q') \neq O$ un punto qualsiasi, e L la retta $[O, Q]$. Abbiamo $L = \{(tq, tq')/\ t \in k\}$. Siccome f_i è omogeneo di grado i, $f_i(tq, tq') = t^i f_i(q, q')$, pertanto: $f(tq, tq') = t^n f_n(Q)+\ldots+t^i f_i(Q)+\ldots+tf_1(Q)$. Per definizione $m_O(C) = m$ se:

(*i*) $t = 0$ è radice con molteplicità $\geq m$ di $f(tQ) = 0$, per ogni Q;

(*ii*) esiste almeno un Q tale che $t = 0$ sia radice con molteplicità m di $f(tQ) = 0$.

La condizione (*i*) è equivalente a: $f_1(Q) = \ldots = f_{m-1}(Q) = 0$, $\forall Q$. Siccome k è infinito (perché algebricamente chiuso) questo implica $f_1 = \ldots = f_{m-1} = 0$. La condizione (*ii*) è equivalente a: $\exists\ Q_0$ tale che $f_m(Q_0) \neq 0$, cioè $f_m \neq 0$. □

Osservazione 5.4: *E' sempre possibile ricondursi a questa situazione con un cambiamento di variabili (cioè un'affinità): sia* $p \in C$*,* $p = (a, b)$*, e sia* $T : \mathbb{A}^2 \to \mathbb{A}^2$ *un'affinità che manda p nell'origine:* $T(q) = N(q) + t$*, dove N è la parte lineare e dove t è la traslazione. Sia D la curva di equazione* $g(x, y) := (f \circ T^{-1})(x, y) = 0$*. Abbiamo:* $T(q) = D \Leftrightarrow q \in C$*; per questo motivo D si nota anche* $T(C)$*. In particolare* $T(p) = O = D$*. Adesso basta mostrare che, per un punto p e un'affinità qualsiasi:* $i(C, L; p) = i(T(C), T(L); T(p))$*. Se* $L = [p, q]$*,* $T(L) = [T(p), T(q)]$*, e i punti di* $T(L)$ *sono della forma* $(1-l)T(p)+lT(q) = (1-l)(N(p)+t)+l(N(q)+t) = (1-l)N(p)+l(N(q)+t = N((1-l)p+lq)+t$ *(N è lineare)* $= T((1-l)p+lq)$*. Per definizione* $i(T(C), T(L); T(p))$ *è la molteplicità della radice* $l = 0$ *nell'equazione:* $(f \circ T^{-1})((1-l)T(p) + lT(q)) = (f \circ T^{-1})(T((1-l)p + lq)) = f((1-l)p + lq)$*, e questo non è altro che* $i(C, L; p)$*.*

Definizione 5.5: *Sia C una curva piana e* $p \in C$*. Una retta L passante per p è una tangente principale a C in p se* $i(C, L; p) > m_p(C)$*.*

Osservazione 5.6: *Se p è un punto liscio di C, c'è un'unica tangente principale a C in p: è la solita tangente.*

L'insieme delle tangenti principali in $p \in C$ si chiama il **cono tangente a** C **in** p.

Proposizione 5.7: *Ci sono al più* $m_p(C)$ *tangenti principali a C in p.*

DIMOSTRAZIONE. Possiamo assumere la curva C affine e $p = O$, l'origine. Sia $m = m_O(C)$, e $f(x, y) = f_n(x, y) + \ldots + f_m(x, y)$ l'equazione di C. Riprendendo le notazioni della dimostrazione del lemma precedente abbiamo che $i(C, L; O) > m \Leftrightarrow f_m(Q) = 0$, dove $L = [O, Q]$. Osserviamo che se Q' è un altro punto di L allora $Q' = \lambda Q$ per qualche $\lambda \in k$, e $f_m(Q') = \lambda^m f_m(Q)$. Quindi le rette, L, per O tali che $i(C, L; O) > m$ corrispondono agli zeri di f_m in $\mathbb{P}^1 : \mathbf{V}(f_m) \subseteq \mathbb{P}^1$. In altri termini, siccome f_m è un polinomio omogeneo di grado m nelle due variabili x, y, si fattorizza in un prodotto di termini lineari: $f_m = l_1^{a_1} \ldots l_r^{a_r}$, $a_1 + \ldots + a_r = m$, e dove $l_i(x, y) = a_i x + b_i y$. Le tangenti principali sono le rette di equazione: $l_i(x, y) = 0$. □

Osservazione 5.8: *Quanto precede ci permette di analizzare facilmente, localmente nell'origine, la curva* $C \subset \mathbb{A}^2$*, di equazione* $f(x, y) = f_n(x, y) + f_{n-1}(x, y) + \ldots + f_1(x, y)$ *(*f_i *omogeneo di grado i). Se* $f_1 \neq 0$*, l'origine O è un punto liscio e la tangente a C in O è la retta di equazione* $f_1(x, y) = 0$*. Se* $f_1 = 0$*, O è un punto singolare; se* f_m *è la componente omogenea non nulla di grado più basso allora* $m_O(C) = m$*, le tangenti principali sono le rette di equazioni* $l_i(x, y) = 0$ *dove* $f_m = l_1^{a_1} \ldots l_r^{a_r}$*,* $a_1 + \ldots + a_r = m$*.*

Definizione 5.9: *Sia $p \in C$ un punto di molteplicità $m > 1$. Il punto p è una singolarità ordinaria se C ha m tangenti principali distinte nel punto p. Un nodo è un punto doppio ordinario.*

Esempio 5.10:

(i) La curva di equazione $y^2 - x^2 - x^3 = 0$ ha una singolarità nell'origine (non c'è il termine lineare). La singolarità è un punto doppio (c'è il termine quadratico). Le tangenti principali sono date dal termine di grado due: $y^2 - x^2 = (y-x)(y+x)$, quindi l'origine è un nodo (punto doppio ordinario).

(ii) La curva di equazione $y^2 - x^3 = 0$ ha un punto doppio nell'origine. Le tangenti principali sono date da: $y^2 = 0$; c'è un'unica tangente principale, T, di equazione $y = 0$. Si ha $i(C, T; O) = 3$, questa singolarità è una cuspide ordinaria.

(iii) La curva di equazione $x^2 - x^4 - y^4 = 0$. L'origine è un punto doppio, le tangenti principali sono date da $x^2 = 0$; quindi c'è un'unica tangente principale, T, di equazione $x = 0$. Questa volta $i(C, T; O) = 4$; questa singolarità è un tacnodo.

Osservazione 5.11: *Si osserverà che "non tutti i punti doppi sono uguali".*

Per trattare il caso generale, cioè $p \in C$, $p = (a, b)$, ci si riconduce al caso precedente. Sia $T : \mathbb{A}^2 \to \mathbb{A}^2$ la traslazione che manda p nell'origine: $T(x, y) = (x - a, y - b)$. Consideriamo la curva $D = T(C)$, di equazione $g(x, y) := (f \circ T^{-1})(x, y) = 0$ $(g(x, y) = f(x - a, y - b))$. Abbiamo: $T(q) = D \Leftrightarrow q \in C$; per questo motivo D si nota anche $T(C)$. In particolare $T(p) = O = D$. Da quanto precede le tangenti principali in O sono date dalla decomposizione di $g_m(x, y)$. Siccome $g \circ T = f$, le tangenti principali a C in p sono date dalla fattorizzazione di $g_m(x - a, y - b) = 0$.

In caratteristica zero abbiamo poi un criterio differenziale per calcolare la molteplicità di C in un punto p. Innanzitutto ricordiamo che per i polinomi vale, con una dimostrazione formale lo sviluppo di Taylor in un punto. In una variabile abbiamo: $f(x) = f(a) + f'(a) + \frac{1}{2!}f''(a)(x-a)^2 + \ldots + \frac{1}{d!}f^{(d)}(a)(x-a)^d + \ldots$ In particolare: $d!a_d = f^{(d)}(a)$ (dove $f(x) = \sum\limits_{i \geq 0} a_i x^i$). Osservare che se $p = ch(k)$ divide $d!$ allora $f^{(d)}(a) = 0$ mentre a_d non è necessariamente nullo. In più variabili lo sviluppo di Taylor è: $F(X) = F(a) + DF(a).(X-a). + \frac{1}{2!}D^2F(a).(X-a)^2 + \ldots + \frac{1}{d!}D^dF(a).(X-a)^d + \ldots$, dove $X = (x_1, \ldots, x_n)$, $a = (a_1, \ldots, a_n)$, $DF(a).(X-a) = \Sigma \frac{\partial F}{\partial x_i}(a).(x_i - a_i)$, e dove $D^rF(a).(X-a)^r$ indica la potenza simbolica $(\Sigma \frac{\partial F}{\partial x_i}(a).(x_i - a_i))^r$.

Per esempio se $n = 2$: $((\frac{\partial f}{\partial x}(a).(x - a_1) + \frac{\partial f}{\partial y}(a).(y - a_2))^r =$
$= \sum\limits_{i=0}^{r} \binom{r}{i} \frac{\partial^i f}{\partial x^i}(a).(x - a_1)^i \frac{\partial^{r-i} f}{\partial y^{r-i}}(a).(y - a_2)^{r-i}$

$$= \sum_{i=0}^{r} \binom{r}{i} \frac{\partial^r}{\partial x^i \partial y^{r-i}}(a).(x-a_1)^i (y-a_2)^{r-i}.$$

Lemma 5.12: *Si assume $ch(k) = 0$.*

(*i*) *Sia $C \subseteq \mathbb{A}^2$ una curva di equazione $f(x, y) = 0$, e sia $p \in C$. Il punto p è un punto di molteplicità m di C se e solo se tutte le derivate parziali di f di ordine $< m$ sono nulle in p, e se esiste una derivata parziale di f di ordine m non nulla in p.*

(*ii*) *Sia $C \subseteq \mathbb{P}^2$ una curva di equazione $F(X, Y, Z) = 0$, e sia $p \in C$. Il punto p è un punto di molteplicità m di C se e solo se tutte le derivate parziali di ordine $m-1$ di F sono nulle in p, e se esiste una derivata parziale di ordine m di F non nulla in p.*

Dimostrazione. (*i*) Si usa lo sviluppo di Taylor osservando che la parte omogenea di grado d è $\frac{1}{d!}D^d f(a).(X-a)^d$.

(*ii*) Si ragiona come prima tenendo conto del fatto che, se F è omogeneo e se le derivate parziali di ordine $m-1$ di F sono nulle in p, allora, per la relazione di Eulero, tutte le derivate parziali di ordine $< m$ di F sono nulle in p.

□

Esempio 5.13: Sia $C \subseteq \mathbb{P}^2$ la curva di equazione $F(X, Y, Z) = 0$ dove $F(X, Y, Z) = X^3 - X^2 Z + Y^2 Z$, e sia $p = (0 : 0 : 1) \in C$. Le derivate parziali sono: $F_X = 3X^2 - 2XZ$, $F_Y = 2YZ$, $F_Z = -X^2 + Y^2$. Tutte le derivate parziali del primo ordine sono nulle in p. La derivata parziale seconda $F_Y^2 = 2Z$ non è nulla in p, quindi p è un punto doppio.

6. Curve di grado basso.

Usando quanto fatto finora cerchiamo di classificare le curve di grado basso in $\mathbb{P}^2$.

Ogni curva di grado 1 è una retta, e tutto è chiaro: ogni retta è nonsingolare, razionale ($\simeq \mathbb{P}^1$) e due rette qualsiasi sono proiettivamente equivalenti.

Curve di grado due: una curva riducibile di grado due non può essere altro che l'unione di due rette (distinte o no).

Lemma 6.1: *Una conica (= curva di grado due), $C \subseteq \mathbb{P}^2$, irriducibile è liscia e razionale.*

Dimostrazione. (*i*) Supponiamo che $p \in C$ sia un punto singolare. Per definizione, se L è una retta passante per p, $i(C, L; p) \geq 2$. Sia $q \neq p$ un altro punto di C e sia R la retta passante per p e q. Siccome $i(C, R; p) \geq 2$

e $i(C, R; q) \geq 1$, abbiamo $\sum_{x \in C \cap R} i(C, R; x) > \deg(C)$, questo contraddice la versione debole del teorema di Bezout in quanto C ed R non hanno componenti comuni perché, per ipotesi, C è irriducibile.

(ii) Fissiamo un punto $p \in C$ e una retta D non passante per p. Proiettiamo la conica C dal punto p sulla retta D: $\pi : C \to D : q \longmapsto \pi(q)$ dove $\pi(q)$ è il punto d'intersezione della retta $[p, q]$ con D (se $q = p$ si prende la tangente a C in p per $[q, p]$). L'applicazione π è chiaramente biiettiva, e il lettore si convincerà da solo che π è un isomorfismo. (altrimenti adotterà il principio secondo il quale ogni applicazione definita da costruzioni algebro-geometriche, cioè che si possono esprimere con equazioni algebriche, è un morfismo).

□

Dalla teoria delle forme quadratiche risulta (se $ch(k) \neq 2$), che ogni conica C di $\mathbb{P}^2$ è proiettivamente equivalente ad una delle seguenti coniche:
coniche di rango uno: $X^2 = 0$ ("retta doppia");
coniche di rango due: $X^2 + Y^2 = 0$ ("coppia di rette");
coniche di rango tre: $X^2 + Y^2 + Z^2 = 0$ ("conica irriducibile").

Curve di grado tre: per le curve di grado tre la situazione è già molto più complessa. Le cubiche riducibili sono unioni di curve di grado < 3. Per le cubiche irriducibili abbiamo:

Lemma 6.2: *Sia $C \subseteq \mathbb{P}^2$ una cubica irriducibile.*

(i) *C ha al più un punto singolare (che può essere solo un punto doppio);*
(ii) *Se C è singolare allora C è razionale.*

Dimostrazione. (i) Si ragiona come nella dimostrazione del lemma precedente. Se $p \neq q$ sono due punti singolari di C allora $i(C, L; p) \geq 2$ (risp.$i(C, L; q) \geq 2$), per ogni retta L per p (risp. q). Considerando la retta $R = [p, q]$ si ottiene una contraddizione con la versione debole del teorema di Bezout. Nello stesso modo si dimostra che ogni punto ha molteplicità al più due.

(ii) Sia p l'unico punto singolare di C. Osserviamo che se L è una retta passante per p che non è una tangente principale, allora $i(C, L; p) = 2$. Quindi L incontra C in un ulteriore punto q, $q \neq p$. Siano $L_1, \ldots, L_n$ le tangenti principali a C in p (sono al più due). Sia F il fascio di rette per p. Abbiamo un'applicazione: $\pi : C \backslash \{p\} \to F \backslash \{L_1, \ldots, L_n\} : q \longmapsto [p, q]$. Come nella dimostrazione del lemma precedente si vede che π stabilisce un isomorfismo tra un aperto di C e un aperto di $F \simeq \mathbb{P}^1$, quindi C è razionale.

□

Osservazione 6.3: *Il punto singolare di una cubica piana irriducibile può essere un nodo (punto doppio ordinario):* $Y^2 = X^2 + X^3$*, o una cuspide ordinaria:* $Y^2 = X^3$*. Si può dimostrare che due cubiche irriducibili singolari sono proiettivamente equivalenti se e solo se hanno una singolarità della stessa natura (cioè hanno entrambe un nodo o hanno entrambe una cuspide).*

La classificazione delle cubiche lisce è un problema affascinante sul quale torneremo.

Esercizi.

Esercizio 6.1: *Sia* $C \subseteq \mathbb{P}^2$ *la curva di equazione* $F(X,Y,Z) = (X^2+Y^2)^3 - 4X^2Y^2Z^2$, *e sia* $p \in C$, $p = (0:0:1)$. *Determinare* $m_p(C)$ *e le tangenti principali.*

Esercizio 6.2: *Un punto liscio* p, $p \in C$, *di una curva piana* C *è un punto di flesso se* $i(C, T_p; p) \geq 3$, *dove* T_p *è la tangente a* C *in* p.

(i) Una conica irriducibile non ha flessi.

(ii) Un flesso si dice di specie k (≥ 1) *se* $i(C, T_p; p) = k+2$, *se* $k = 1$ *il flesso si dice ordinario. Mostrare che la curva di equazione* $y - x^{k+2} = 0$ *ha un flesso di specie* k *nell'origine.*

Esercizio 6.3: *Sia* $C \subseteq \mathbb{P}^2$ *una curva di grado* n. *Se* C *ha un punto di molteplicità* n *allora* C *è l'unione di* n *rette (distinte o no) passanti per quel punto.*
Se C *è irriducibile e ha un punto di molteplicità* $n-1$ *allora quel punto è l'unica singolarità di* C, *e* C *è razionale (considerare il fascio di rette per il punto singolare).*

Esercizio 6.4: *Le considerazioni svolte per le curve piane (molteplicità d'inter--sezione con una retta, punti singolari) si estendono al caso delle ipersuperfici di* $\mathbb{P}^n$.
Sia $S \subseteq \mathbb{P}^n$ *un ipersuperficie, e* $p \in Sing(S)$ *un punto singolare di* S. *Sia* H *un iperpiano passante per* p. *Mostrare che l'ipersuperficie* $S \cap H$ *di* $H \simeq \mathbb{P}^{n-1}$ *è singolare in* p *(hint: se* $S = \mathbf{V}(F)$, *assumere* H *di equazione* $x_0 = 0$ *e scrivere* F *come un polinomio in* x_0*).*

Esercizio 6.5: *("Superficie cubica rigata di prima specie") Sia* $S \subseteq \mathbb{P}^3$ *la superficie di equazione* $xy^2 - z^2t = 0$.

(i) Sia R *la retta di equazioni* $y = z = 0$. *Dimostrare che* $Sing(S) = R$ *e che ogni punto di* R *è un punto di molteplicità due per* S *("*S *è una superficie cubica con retta doppia").*

(ii) Sia H *un piano per* R, *descrivere la curva* $S \cap H$. *Dedurre che se* $p \in S \backslash R$ *esiste una, ed un'unica retta,* L_p, *contenuta in* S, *passante per* p, *e che incontra* R *(considerare il piano* $[p, R]$*) ("*S *è una superficie rigata").*

(iii) La retta D *di equazioni* $x = t = 0$ *è contenuta in* S *e non incontra* R. *Determinare per ogni punto* p, $p \in D$, *la curva* $T_pS \cap S$ *(si può usare Esercizio 6.4).*

(iv) Si pone $q_1 = (0:0:0:1)$, $q_2 = (1:0:0:0)$ *(le coordinate di* $\mathbb{P}^3$ *sono* $(x:y:z:t)$*). Se* $q \neq q_i$, $1 \leq i \leq 2$, *è un punto di* R, *mostrare che esistono due rette* R'_q, R''_q, *contenute in* S, *passanti per* q, *e che si appoggiano su* D. *E se* $q = q_i$*?*

(v) Determinare tutte le rette contenute in S.

7. Punti nel piano e sistemi lineari di curve piane.

Dati d punti del piano, è possibile trovare una curva di grado n passante per questi d punti? Ovviamente la risposta dipende dagli interi d, n e dalla posizione (”geometria”) dei punti. Un classico risultato in merito è la formula di interpolazione di Lagrange. Scopo di questo paragrafo è di dare alcuni risultati generali su questo problema (per punti in $\mathbb{P}^2$), e di introdurre la nozione di sistema lineare.

Sia $\mathbf{S} = k[X, Y, Z]$, allora, $\mathbf{S}_n$, l'insieme dei polinomi omogenei di grado n, è un k-spazio vettoriale di dimensione $\frac{(n+2)(n+1)}{2}$. Pertanto l'insieme, $\mathbb{P}(\mathbf{S}_n)$ delle curve piane di grado n di $\mathbb{P}^2$ è uno spazio proiettivo di dimensione $N_n := \frac{(n+2)(n+1)}{2} - 1$.

Definizione 7.1: *Un sistema lineare di curve piane di grado n è un sottospazio lineare di $\mathbb{P}(\mathbf{S}_n)$. La dimensione (proiettiva) del sistema lineare è la dimensione del sottospazio lineare di $\mathbb{P}(\mathbf{S}_n)$.*

Osservazione 7.2: *Sia $\Delta \subseteq \mathbb{P}(\mathbf{S}_n)$ un sistema lineare allora $\Delta = \mathbb{P}(V)$ dove $V \subseteq \mathbf{S}_n$ è un sottospazio vettoriale. La dimensione (proiettiva) del sistema lineare è $\dim \Delta$, la dimensione (vettoriale) del sistema lineare è $\dim V = \dim \Delta + 1$. Nel linguaggio classico si usa esclusivamente la dimensione proiettiva, e per indicare che un sistema lineare Δ ha dimensione (proiettiva) r si dice che Δ è ∞^r (”infinito alla r”). Un sistema lineare ∞^1 si chiama ”fascio” (pencil in inglese, pinceau in francese). Darsi un sistema lineare ∞^r di curve di grado n è equivalente a darsi un sottospazio vettoriale di dimensione $r + 1$ di $\mathbf{S}_n$, se $F_0, F_1, \dots, F_r$ è una base di tale sottospazio ogni curva del sistema avrà un'equazione del tipo $\lambda_0 F_0 + \ldots + \lambda_r F_r$.*

Un punto $p \in \mathbb{P}^2$ è un punto base del sistema lineare Δ se ogni curva di Δ passa per p. Il luogo base di Δ è l'insieme dei punti base; il luogo base è un sottoinsieme algebrico, se contiene una curva, questa curva viene chiamata la curva fissa di Δ.

Il modo più naturale di ottenere un sistema lineare è di imporre il passaggio per un punto.

Innanzitutto osserviamo che scegliendo come base di $\mathbf{S}_n$ i monomi $X^i Y^j Z^t$, $i + j + t = n$, possiamo associare ad ogni curva di grado n, $C \subseteq \mathbb{P}^2$, di equazione $F(X, Y, Z) = \sum a_{ijt} X^i Y^j Z^t$, delle coordinate omogenee (costruite sui coefficienti di una sua equazione): $(\ldots : a_{ijt} : \ldots)$ in $\mathbb{P}(\mathbf{S}_n)$ stabilendo cosìun isomorfismo tra $\mathbb{P}(\mathbf{S}_n)$ e $\mathbb{P}^{N_n}$.

Sia $p = (p_0 : p_1 : p_2) \in \mathbb{P}^2$. Abbiamo $p \in C \Leftrightarrow \sum a_{ijt} p_0^i p_1^j p_2^t = 0$ (✠). Siccome i termini $p_0^i p_1^j p_2^t$ sono delle costanti (p è fissato) possiamo interpretare (✠) come un'equazione lineare nelle variabili a_{ijt}, cioè (✠) è l'equazione di un iperpiano in $\mathbb{P}^{N_n}$. Abbiamo quindi:

Lemma 7.3: *Le curve di grado n che passano per un punto p formano un sistema lineare, più precisamente un iperpiano di $\mathbb{P}^{N_n}$.*

Più generalmente siano $p_1, \ldots, p_d$, d punti di $\mathbb{P}^2$, con $p_i = (\alpha_i : \beta_i : \gamma_i)$. L'insieme delle curve di grado n che passano per $p_1, \ldots, p_d$ sono date dalle soluzioni del sistema lineare omogeneo:

$$\begin{cases} \sum a_{ijt}\alpha_1^i\beta_1^j\gamma_1^t & = & 0 \\ \vdots & \vdots & \vdots \\ \sum a_{ijt}\alpha_d^i\beta_d^j\gamma_d^t & = & 0 \end{cases}$$

Si tratta quindi di un sistema lineare di d equazioni nelle incognite a_{ijt}, l'insieme delle soluzioni è un sottospazio lineare $\Delta \subseteq \mathbb{P}^{N_n}$ di dimensione $\geq N_n - d$. Possiamo vedere questo sistema più geometricamente: le curve di grado n che passano per il punto p costituiscono un iperpiano, $\delta_n(p)$, le curve che passano per $p_1, \ldots, p_d$ costituiscono il sottospazio lineare $\delta_n(p_1, \ldots, p_d) := \delta_n(p_1) \cap \ldots \cap \delta_n(p_d)$. Abbiamo $\dim(\delta_n(p_1, \ldots, p_d)) \geq N_n - d$ in base al fatto elementare seguente:

Sia $H \subseteq \mathbb{P}^n$ un iperpiano e $F \subseteq \mathbb{P}^n$ un sottospazio lineare. Ci sono due casi: $F \subseteq H$ e allora $\dim(H \cap F) = \dim F$, oppure F non è contenuto in H e $\dim(F \cap H) = \dim F - 1$.

Più generalmente il passaggio per un punto p con molteplicità almeno r corrisponde a $\frac{r(r+1)}{2}$ condizioni lineari sui coefficienti (bisogna annullare le derivate parziali di ordine $r-1$ in p ($ch(k) = 0$), e ci sono $\frac{r(r+1)}{2}$ tali derivate). Finalmente concludiamo che l'insieme delle curve di grado n che passano per i punti $p_1, \ldots, p_d$ con molteplicità almeno $r_1, \ldots, r_n$ rispettivamente è un sistema lineare $\delta_n(p_1^{r_1}, \ldots, p_d^{r_d})$ di dimensione $\geq N_n - \sum\limits_{i=1}^{d} \frac{r_i(r_i+1)}{2}$. In particolare se $N_n - \sum\limits_{i=1}^{d} \frac{r_i(r_i+1)}{2} \geq 0$ esiste sempre almeno una curva di grado n che passa per i punti $p_1, \ldots, p_d$ con almeno molteplicità $r_1, \ldots, r_d$ rispettivamente. Per riassumere:

Proposizione 7.4: *Le curve di grado n che passano per i punti p_i, con molteplicità almeno r_i, $1 \leq i \leq d$, costituiscono un sistema lineare, $\delta_n(p_1^{r_1}, \ldots, p_d^{r_d})$, di dimensione $\geq N_n - \sum\limits_{i=1}^{d} \frac{r_i(r_i+1)}{2}$. In particolare se $N_n - \sum\limits_{i=1}^{d} \frac{r_i(r_i+1)}{2} \geq 0$ esiste sempre una curva di grado n che passa per i punti p_i con molteplicità almeno r_i, $1 \leq i \leq d$.*

Esempio 7.5: Per due punti passa sempre una retta, per 5 punti passa sempre una conica, per 9 punti passa sempre una cubica, ecc...

Osservazione 7.6: *Chiaramente i punti $p_1, \ldots, p_d$ sono punti base del sistema $\delta_n(p_1^{r_1}, \ldots, p_d^{r_d})$, questi punti base vengono detti "assegnati" (con molteplicità r_i). Non sempre il luogo base coincide con il luogo base assegnato. Per esempio se $\delta = \delta_2(p_1, p_2, p_3)$ dove i p_i sono allineati su una retta R, allora il luogo base di δ è la curva fissa R.*

Torniamo al sistema lineare $\delta = \delta_n(p_1, \ldots, p_d)$ delle curve di grado n che passano per i punti p_i, $1 \leq i \leq d$. Abbiamo visto che $\dim \delta \geq N_n - d$.

Definizione 7.7: *I punti* $p_1, \ldots, p_d$ *impongono condizioni indipendenti alle curve di grado* n *se* $\dim \delta_n(p_1, \ldots, p_d) = \max\{N_n - d, -1\}$ *(con la convenzione* $\dim \emptyset = -1$*).*

Esempio 7.8: (*i*) Due punti, p_1, p_2, impogono sempre condizioni indipendenti. Infatti $\delta_n(p_1, p_2) = \delta_n(p_1) \cap \delta_n(p_2)$ è l'intersezione di due iperpiani, basta quindi verificare che $p_1 \neq p_2 \Rightarrow \delta_n(p_1) \neq \delta_n(p_2)$. Per questo basta trovare una curva di grado n che passa per p_1 ma non per p_2. Se $n = 1$ non c'è difficoltà a trovare una retta di equazione $L = 0$ tale che $L(p_1) = 0$, $L(p_2) \neq 0$. Se $n > 1$, basta considerarne L^n.

(*ii*) Tre punti non danno sempre condizioni indipendenti. Per esempio tre punti allineati non impogono condizioni indipendenti alle rette. Ma se $n = 2$, tre punti danno sempre condizioni indipendenti.

Lemma 7.9: *("Criterio di separazione") Siano* n, d *degli interi,* $n \geq 1$, $d \leq N_n + 1 = \frac{(n+1)(n+2)}{2}$. *Un insieme di* d *punti* $p_1, \ldots, p_d$ *di* $\mathbb{P}^2$ *dà delle condizioni indipendenti alle curve di grado* n *se e solo se:* $\forall i$, *esiste una curva* C_i, *di grado* n, *che passa per* P_j *se* $j \neq i$, *e che non passa per* P_i.

Dimostrazione. Sia $\delta = \bigcap_{1 \leq i \leq d} \delta_n(p_i)$. Si tratta di dimostrare: $\dim \delta = \max\{N_n - d, -1\} \Leftrightarrow \forall i$, esiste una curva, C_i, di grado n che passa per p_j se e solo se $j \neq i$. Ossia $\dim \delta = \max\{N_n - d, -1\} \Leftrightarrow \forall i$, esiste un punto, C_i, di $\mathbb{P}^{N_n}$ che appartiene a $\delta_n(p_j)$ se e solo se $j \neq i$. Supponiamo $\dim \delta = \max\{N_n - d, -1\}$ e consideriamo $\delta' = \bigcap_{j \neq i} \delta_n(p_j)$; δ' è un sottospazio lineare non vuoto (perché di dimensione $\geq N_n - (d-1)$) di $\mathbb{P}^{N_n}$. L'ipotesi $\dim \delta = \max\{N_n - d, -1\}$ implica che δ' non è contenuto in $\delta_n(p_i)$, quindi esiste un punto, C_i, appartenente a δ', che non appartiene a $\delta_n(p_i)$.
Viceversa se esiste un punto, C_i, di $\mathbb{P}^{N_n}$ che appartiene a $\delta_n(p_j)$ se e solo se $j \neq i$, allora usando il fatto elementare menzionato qui sopra, e ragionando per induzione, si vede che segando con gli iperpiani $\delta_n(p_i)$, la dimensione cala ogni volta di uno: $\dim(\delta_n(p_1) \cap \ldots \cap \delta_n(p_t)) = N_n - t$, $t \geq 1$. □

Corollario 7.10: *Sia* $X \subseteq \mathbb{P}^2$, $X = \{p_1, \ldots, p_d\}$ *un insieme di* d *punti con* $d \leq N_n + 1$, *che impone condizioni indipendenti alle curve di grado* n. *Se* $X' \subseteq X$ *allora anche* X' *impone condizioni indipendenti alle curve di grado* n.

Adesso dimostriamo che per ogni $d \geq 1$ e per ogni $n \geq 1$ esiste un insieme di d punti in $\mathbb{P}^2$ che impone condizioni indipendenti alle curve di grado n (il lettore deve convincersi che un tale enunciato necessita di una dimostrazione: il punto è che non tutti i sistemi lineari si ottengono imponendo il passaggio per dei punti, cfr. Esercizio 7.1).

Lemma 7.11: *Per ogni $n \geq 1$ esiste un insieme di $N_n + 1$ punti in $\mathbb{P}^2$ che non è contenuto in nessuna curva di grado n (e quindi impone condizioni indipendenti alle curve di grado n).*

Dimostrazione. Osserviamo che $N_n+1 = \frac{(n+2)(n+1)}{2} = (n+1)+n+\ldots+2+1$. Consideriamo un insieme, X, di N_n+1 punti $\{Pi\}$ costituito da $n+1$ sottoinsiemi due a due disgiunti: il primo sottoinsieme, $X_1 = \{P_1, \ldots, P_{n+1}\}$, consta di $n+1$ punti allineati su una retta R_1; il secondo sottoinsieme, $X_2 = \{P_{n+2}, \ldots, P_{2n+1}\}$, consta di n punti allineati su una retta $R_2 \neq R_1$; l'n-esimo sottoinsieme, X_n, consta di due punti allineati su una retta, R_n, diversa da R_i se $i < n$; e l'ultimo sottoinsieme, X_{n+1}, consta di un solo punto non appartenente a nessuna delle rette $R_1, \ldots, R_n$. Sia C una curva di grado n contenente X. Allora C interseca la retta R_1 in $n+1$ punti ($X_1 \subset C \cap R_1$). Per la versione debole del teorema di Bezout R_1 è una componente di C: $C = R_1 \cup C'$. La curva C' (di grado $n-1$) interseca la retta R_2 in n punti ($X_2 \subseteq C \cap R_2$, $R_2 \neq R_1$, e $X_1 \cap X_2 = \emptyset$). Quindi per la versione debole del teorema di Bezout $C' = R_2 \cup C''$. Procedendo così si vede che C contiene $R_1 \cup R_2 \cup \ldots \cup R_n$. Siccome C ha grado n, $C = R_1 \cup R_2 \cup \ldots \cup R_n$. Ma allora C non contiene X_{n+1}, e, a fortiori, non contiene X. □

Proposizione 7.12: *Per ogni $n \geq 1$ e per ogni $d \geq 1$ esiste un insieme di d punti che impone condizioni indipendenti alle curve di grado n.*

Dimostrazione. Se $d = N_n + 1$ l'enunciato segue dal lemma precedente. Se $d < N_n + 1$ l'enunciato segue dal lemma precedente e dal *Corollario* 7.10. Se $d > N_{n+1}$, prendiamo un insieme, X', di $N_n + 1$ punti che impogono condizioni indipendenti alle curve di grado n e lo completiamo con un insieme qualsiasi di $d - (N_n + 1)$ punti. □

Osservazione 7.13: *Si può dimostrare un risultato più forte: per ogni d, esiste un insieme di d punti che impone condizioni indipendenti alle curve di grado n, per ogni $n \geq 1$ (cfr. Esercizi); un tale insieme di punti si dice di* rango massimo.

7.1. La funzione di Hilbert di un insieme di punti. Sia $X \subseteq \mathbb{P}^2$ un insieme di d punti P_i, prendendo una retta che non interseca X otteniamo una carta affine contenente X, e quindi possiamo considerare $X \subseteq \mathbb{A}^2$. Modulo cambiamento di base, possiamo assumere che la retta all'infinito sia la retta di equazione $X_0 = 0$. Se $f(x,y) \in k[x,y]$ possiamo valutare f nei punti $P_i = (x_i, y_i)$ di X ottenendo così l'elemento $(f(P_1), \ldots, f(P_d))$ di k^d. Chiaramente la curva di equazione $f(x,y) = 0$ contiene X se e solo se $f(P_i) = 0$ per ogni i. Sia adesso $F(X_0, X_1, X_2)$ un polinomio omogeneo di grado n, e indichiamo con $F_*(x,y) = F(1,x,y)$ il suo deomogeneizzato rispetto a X_0. Da quanto precede la curva $C \subseteq \mathbb{P}^2$ di equazione $F = 0$ contiene X

se e solo se $F_*(Pi) = 0$ per ogni i. Otteniamo così un'applicazione (di restrizione) $r_X\,(n)$: $\mathbf{S}_n \to k^d$: $F \longmapsto (F_*(P_1), \dots, F_*(P_d))$.

Lemma 7.14: *Con le notazioni precedenti, l'applicazione $r_X\,(n)$ è un'applicazione k-lineare. Si ha $Ker(r_X\,(n)) = \mathbf{I}(X)_n$, e $Im(r_X(n)) \simeq A(X)_n$.*

Dimostrazione. È chiaro che $r_X\,(n)$ è k-lineare (perché $(\lambda F + \mu G)_* = \lambda F_* + \mu G_*$), inoltre $r_X\,(n)\,(F) = 0$ se e solo se $F \in \mathbf{I}(X)_n$; si conclude perché, per definizione, $A(X)_n = \frac{\mathbf{S}_n}{\mathbf{I}(X)_n}$. □

Osservazione 7.15: *La nostra definizione dell'applicazione $r_X\,(n)$ non è intrinseca (dipende dalla scelta della carta affine) ma il lemma precedente mostra che ogni carta affine contenente tutto X porterà allo stesso risultato per quanto riguarda le dimensioni del ker e dell'immagine.*

Definizione 7.16: *L'applicazione $h_X : \mathbb{N} \to \mathbb{N} : n \longmapsto \dim(Im(r_X(n))) = \dim(A(X)_n)$ si chiama funzione di Hilbert dell'insieme di punti X.*

Osservazione 7.17: *(i) Siccome $h_X\,(n) = \dim \mathbf{S}_n - \dim \mathbf{I}(X)_n$, abbiamo $\dim \mathbf{I}(X)_n = \frac{(n+2)(n+1)}{2} - h_X\,(n)$, quindi la funzione di Hilbert determina la "postulazione" di X cioè la dimensione, per ogni n, dello spazio vettoriale dei polinomi omogenei di grado n che si annullano sui punti di X; viceversa la postulazione determina la funzione di Hilbert.*
Siccome il sistema lineare, $\delta_n(P_1, \dots, P_d)$, delle curve di grado n che passano per $X = \{P_1, \dots, P_d\}$ non è altro che $\mathbb{P}(\mathbf{I}(X)_n) \subseteq \mathbb{P}(\mathbf{S}_n)$, $h_X(n)$ è la codimensione di $\delta_n(P_1, \dots, P_d)$ in $\mathbb{P}(\mathbf{S}_n)$ (cioè il numero di condizioni imposte dai punti $P_1, \dots, P_d$ alle curve di grado n).

(ii) Un'applicazione lineare $f : V \to W$ è detta di rango massimo se è iniettiva o suriettiva. Un insieme di punti, X, impone condizioni indipendenti alle curve di grado n se e solo se $r_X\,(n)$ è di rango massimo.

(iii) Poniamo $D(X)_n := Coker(r_X\,(n))$ allora abbiamo una successione esatta di k-spazi vettoriali:

$$0 \to \mathbf{I}(X)_n \overset{i_X(n)}{\to} \mathbf{S}_n \overset{r_X(n)}{\to} k^d \overset{\partial_X(n)}{\to} D(X)_n \to 0$$

(iv) Tutte le applicazioni $i_X(n)$, $r_X(n)$, $\partial_X(n)$ sono k-lineari, e dire che la successione è esatta significa che: $i_X(n)$ è iniettiva, $Im(i_X(n)) = Ker(r_X(n))$, $Im(r_X(n)) = Ker(\partial_X(n))$, $\partial_X(n)$ è suriettiva (osservare: $i_X(n)$ iniettiva $\Leftrightarrow Ker(i_X(n)) = Im(0 \to I_X(n))$; $\partial_X(n)$ suriettiva $\Leftrightarrow Im(\partial_X(n)) = Ker(D(X)_n \to 0)$, dove 0 indica un k-spazio vettoriale di dimensione zero). In una successione esatta la somma alterna delle dimensioni è uguale a zero: $d + \dim(\mathbf{I}(X)_n) = \frac{(n+2)(n+1)}{2} + \dim(D(X)_n)$; per vederlo si può spezzare la successione in due successioni esatte "corte" (cioè a tre

termini):

$$0 \to \mathbf{I}(X)_n \to \mathbf{S}_n \to A(X)_n \to 0$$

$$0 \to A(X)_n \to k^d \to D(X)_n \to 0$$

Per il teorema delle dimensioni: $\frac{(n+2)(n+1)}{2} = \dim(\mathbf{I}(X)_n) + \dim(A(X)_n)$, *e* $d = \dim(A(X)_n) + \dim(D(X)_n)$, *mettendo tutto insieme si ottiene il risultato.*
In conclusione $\mathbf{I}(X)_n$ *misura il difetto di iniettività di* $r_X(n)$, *mentre* $D(X)_n$ *misura il difetto di suriettività di* $r_X(n)$.

Un insieme di punti è di rango massimo se per ogni n, $r_X(n)$ è iniettiva o suriettiva, cioè se $\dim(\mathbf{I}(X)_n).\dim(D(X)_n) = 0$ per ogni n.

Proposizione 7.18: *Sia* $X \subseteq \mathbb{P}^2$, $X = \{P_1, \dots, P_d\}$, *un insieme di* d *punti.*

(i) X *impone condizioni indipendenti alle curve di grado* n *se e solo se* $r_X(n)$ *è di rango massimo.*
(ii) *L'applicazione* $r_X(n)$ *è suriettiva* $\Leftrightarrow$ $\forall i$ *esiste una curva di grado* n, C_i, *che passa per* P_j, $j \neq i$, *e che non passa per* P_i *("criterio di separazione").*
(iii) *Se* $r_X(n)$ *è suriettiva allora* $r_X(m)$ *è suriettiva per ogni* $m \geq n$.
(iv) $r_X(d-1)$ *è suriettiva* ($d = \deg(X)$).

Dimostrazione. (i) È una semplice traduzione.
(ii) Anche questa è una traduzione ma diamo una dimostrazione in questo contesto: se $r_X(n)$ è suriettiva $(0, \dots, 1, \dots, 0)$ (1 al posto i, 0 altrimenti) appartiene a $\mathrm{Im}(r_X(n))$ per ogni i, quindi esiste F_i tale che $r_X(F_i) = (0, \dots, 1, \dots, 0)$: la curva C_i di equazione $F_i = 0$ passa per P_j se e solo se $j \neq i$. Viceversa, se per ogni i esiste C_i che passa per P_j se e solo se $j \neq i$ allora $(0, \dots, a_i, \dots, 0) \in \mathrm{Im}(r_X(n))$, con $a_i \neq 0$, per ogni i. Pertanto $\dim(r_X(n)) = d$ e $r_X(n)$ è suriettiva.
(iii) Se vale il criterio di separzione per le curve di grado n, vale a fortiori per quelle di grado $m \geq n$.
(iv) Il criterio di separazione vale sempre per le curve di grado $d-1$: prendere una retta R_j che incontra X solo in P_j, allora $C_i = \bigcup_{j \neq i} R_j$ passa per $P_j$se e solo se $j \neq i$.

□

Osservazione 7.19: *Ci sono quindi un numero finito di casi da considerare per determinare la funzione di Hilbert di un insieme di punti.*

7.2. Esempi. Concludiamo questo paragrafo con alcuni esempi che ci saranno utili anche in seguito.

Nel resto di questo paragrafo useremo spesso il teorema di Bezout (anche se non lo abbiamo dimostrato!).

Lemma 7.20: *Sia* $X = \{P_1, \dots, P_8\} \subseteq \mathbb{P}^2$ *un insieme di* 8 *punti di cui mai* 4 *sono allineati e mai* 7 *sono su una conica. Allora* $\dim(\mathbf{I}(X)_3) = 2$ *(cioè* X *impone condizioni indipendenti alle cubiche).*

Dimostrazione. (a) Iniziamo con l'assumere che X non contenga tre punti allineati né sei punti su una conica (è il caso generale). Verifichiamo il criterio di separazione: per ogni i, dobbiamo trovare una cubica passante per $X \backslash \{P_i\}$ e non contenente P_i. Supponiamo $i = 1$ (per semplificare le notazioni). Sia R la retta individuata da P_2 e P_3, allora $R \cap X = \{P_2, P_3\}$ perché X non contiene tre punti allineati. I cinque punti $P_4, \dots, P_8$ sono contenuti in una conica, C. Abbiamo $C \cap X = \{P_4, \dots, P_8\}$ perché X non contiene sei punti su una conica. La cubica $C \cup R$ passa per $X \backslash \{P_1\}$ e non contiene P_1. È chiaro che questo ragionamento vale per ogni indice i (oppure cambiare la numerazione).

(b) Supponiamo che X contenga tre punti allineati, diciamo P_1, P_2, P_3 sono allineati sulla retta R. Consideriamo un ulteriore punto, P_9, su R, e poniamo $X' = X \cup \{P_9\}$. Ogni cubica contenente X' interseca R in 4 punti e quindi contiene R (versione debole del teorema di Bezout), perciò ogni cubica contenente X' è della forma $R \cup K$ dove K è una conica contenente $P_4, \dots, P_8$. I cinque punti $P_4, \dots, P_8$ danno condizioni indipendenti alle coniche (perché non contengono 4 punti allineati). Pertanto $\dim(\mathbf{I}(X'))_3 = 1$, cioè X' impone condizioni indipendenti alle cubiche, quindi (cfr. *Corollario* 7.10) anche X impone condizioni indipendenti alle cubiche.

(b) Finalmente supponiamo che X contenga sei punti (diciamo $P_1, \dots, P_6$) su una conica, K. Si ragiona come prima considerando un ulteriore punto, P_9, su K. Se C è una cubica contenente $X' = X \cup \{P_9\}$ allora C interseca K in 7 punti, per il teorema di Bezout, $C = K \cup L$ dove L è la retta per P_7 e P_8. Quindi $\dim(\mathbf{I}(X')_3) = 1$, X' impone condizioni indipendenti alle cubiche, e quindi anche X impone condizioni indipendenti.

$\square$

Proposizione 7.21: *("Paradosso di Cramer") Sia* $X' = \{P_1, \dots, P_9\}$ *un insieme di* 9 *punti, intersezione completa di due cubiche. Se* C *è una cubica passante per* $P_1, \dots, P_8$ *allora* C *passa anche per* P_9.

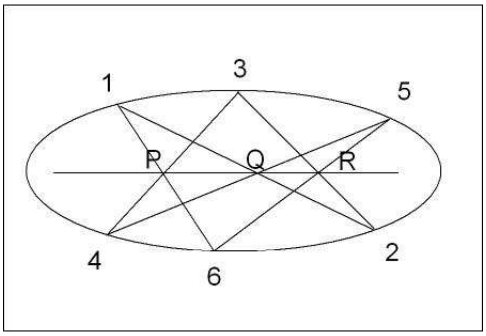
Dimostrazione. Sia $X = \{P_1, \dots, P_8\}$. Mostriamo che X soddisfa le condizioni del lemma precedente: X non contiene 4 punti allineati: infatti per ipotesi $X' = F_3 \cap F_3'$, se X, e quindi X', contenesse 4 punti allineati su una retta R, R

sarebbe una componente delle cubiche F_3, F_3', e quindi si avrebbe $R \subseteq F_3 \cap F_3'$, ma questo è assurdo. Nello stesso modo (usando il teorema di Bezout) si vede che X non contiene 7 punti su una conica. Quindi, per il lemma precedente, X impone condizioni indipendenti alle cubiche e $\dim(\mathbf{I}(X)_3) = 2$. Pertanto F_3 e F_3' formano una base di $\mathbf{I}(X)_3$, e ogni cubica contenente X è della forma $F = \lambda F_3 + \mu F_3'$. In particolare $F(P_9) = \lambda F_3(P_9) + \mu F_3'(P_9) = 0$. $\square$

Osservazione 7.22: *Ogni insieme "generico", $X \subset \mathbb{P}^2$, di otto punti verifica $\dim(\mathbf{I}(X)_3) = 2$ e quindi il sistema lineare $\delta_3(P_1, \dots, P_8)$ ha sempre un punto base non assegnato: è il nono punto dell'intersezione completa di due cubiche (linearmente indipendenti) contenenti X.*

Concludiamo con un'applicazione all'esagono "mistico" di Pascal. Siano v_1, v_2, v_3, v_4, v_5, v_6 i vertici di un esagono in $\mathbb{P}^2$. I sei lati sono: $\overline{12}$, $\overline{23}$, $\overline{34}$, $\overline{45}$, $\overline{56}$, $\overline{61}$. Prolungando i lati opposti ($\overline{12}$ e $\overline{45}$, $\overline{23}$ e $\overline{56}$, $\overline{34}$ e $\overline{61}$), si ottengono tre punti P, Q, R.

Proposizione 7.23: *Con le notazioni precedenti: P, Q, R sono allineati se e solo se $v_1, \dots, v_6$ sono su una conica.*



Dimostrazione. Da ognuno dei punti P, Q, R escono due rette della figura, scegliendo opportunamente una retta per ogni punto realizziamo i nove punti $v_1, \dots, v_6, P, Q, R$ come l'intersezione completa di due cubiche:

$$C \cap C' = \{v_1, \dots, v_6, P, Q, R\}$$

dove C è l'unione delle rette $< v_5, v_6 >$, $< v_1, v_2 >$, $< v_3, v_4 >$; mentre C' è l'unione delle tre rette $< v_2, v_3 >$, $< v_4, v_5 >$, $< v_1, v_6 >$.

(a) Sia K una conica per i 5 punti $v_1, \dots, v_5$ (5 punti sono sempre su una conica) e sia L la retta individuata da P, Q, R. La cubica $K \cup L$ contiene 8 dei 9 punti dell'intersezione completa $C \cap C'$, quindi per la *Proposizione* 7.21, $K \cap L$ contiene anche v_6, questo implica $v_6 \in K$ (perché $v_6 \notin L$?).

(*b*) Sia K la conica contenente $v_1, \ldots, v_6$ e L la retta passante per P e Q. Come prima si deduce che $K \cup L$ contiene R, questo implica $R \in L$ (perché $R \notin K$?).

$\square$

Esercizi.

Esercizio 7.1: *Sia* $\mathbb{P}^{N_n} = \mathbb{P}(\mathbf{S}_n)$ *lo spazio proiettivo delle curve piane di grado* n. *Un iperpiano di* $\mathbb{P}^{N_n}$ *corrisponde a un sistema lineare* ∞^{N_n-1} *di curve piane di grado* n. *Mostrare che se* $n \geq 2$, *in generale, questo sistema lineare non è della forma* $\delta_n(p)$ *(il sistema lineare delle curve di grado* n *che passano per il punto* p*). E se* $n = 1$*?*

Esercizio 7.2: *Sia* $X \subseteq \mathbb{P}^2$ *un insieme di* d *punti distinti, non contenente tre punti allineati. Mostrare che* $h_X(\frac{d}{2}) = d$ *se* d *è pari (risp.* $h_X(\frac{(d-1)}{2}) = d$ *se* d *è dispari).*

Esercizio 7.3: *Sia* $X \subseteq \mathbb{P}^2$ *un insieme di* d *punti distinti. Si pone* $d_n := \dim_k D(X)_n$.
(i) Dimostrare che $n \geq m \Rightarrow d_n \leq d_m$.
(ii) Si ammeterà che la funzione d_n *decresce strettamente fino a raggiungere zero:* $d_{n-1} \neq 0 \Rightarrow d_n < d_{n-1}$. *(provate a dimostrarlo). Dimostrare le seguenti affermazioni:*
(a) $h_X(d-2) \neq d \Leftrightarrow X$ *è contenuto in una retta.*
(b) Se $d \geq 5$*:* $h_X(d-3) \neq d \Leftrightarrow X$ *è contiene* $d-1$ *punti allineati ("la funzione di Hilbert riflette la geometria di* X*").*

Esercizio 7.4: *L'anello* $\mathbf{S} = k[X_0, \ldots, X_n]$ *è un anello graduato:* $\mathbf{S} = \bigoplus_{i \geq 0} \mathbf{S}_i$ *dove* $\mathbf{S}_i$ *è l'insieme dei polinomi omogenei di grado* i. *Un* $\mathbf{S}$*-modulo graduato è un* $\mathbf{S}$*-modulo,* M*, tale che* $M = \bigoplus M_t$*, dove* M_t *è un gruppo abeliano e dove* $\mathbf{S}_i M_t \subseteq M_{t+i}$*, per ogni* i*,* t*. In particolare ogni* M_t *è un* $\mathbf{S}_0$*-modulo, cioè un* k*-spazio vettoriale. Se* $M = \bigoplus M_t$*,* $N = \bigoplus N_t$ *sono due* $\mathbf{S}$*-moduli graduati, un morfismo di grado* p*,* $j : M \to N$*, è un morfismo* $\mathbf{S}$*-lineare tale che* $j(M_t) \subseteq N_{p+t}$*, per ogni* t*. Per esempio se* P *è un polinomio omogeneo fissato, di grado* p*, la moltiplicazione per* P *induce un morfismo di grado* p *di* $\mathbf{S}$ *in se stesso:* $\mathbf{S} \to \mathbf{S} : F \longmapsto PF$*. Per fare diventare questo morfismo di grado zero s'introduce l'*$\mathbf{S}$*-modulo graduato* $\mathbf{S}(-p)$ *definito da* $\mathbf{S}(-p)_t = \mathbf{S}_{t-p}$*; come* $\mathbf{S}$*-modulo* $\mathbf{S}(-p)$ *è isomorfo a* $\mathbf{S}$*, è cambiata solo la graduazione. La moltiplicazione per* P *induce adesso un morfismo di grado zero* $\mathbf{S}(-p) \to \mathbf{S}$.
Sia $X \subseteq \mathbb{P}^2$ *un insieme di punti (distinti) intersezione completa di due curve:* $\mathbf{I}(X) = (F_a, F_b)$*. Mostrare che esiste una successione esatta di* $\mathbf{S}$*-moduli graduati (con morfismi di grado zero):*

$$0 \to \mathbf{S}(-a-b) \to \mathbf{S}(-a) \oplus \mathbf{S}(-b) \to \mathbf{I}(X) \to 0$$

dove l'applicazione $\mathbf{S}(-a-b) \to \mathbf{S}(-a) \oplus \mathbf{S}(-b)$ *è data da* $F \longmapsto (F_b F, F_a F)$*, e dove l'applicazione* $\mathbf{S}(-a) \oplus \mathbf{S}(-b) \longmapsto \mathbf{I}(X)$ *è data da* $(P, Q) \longmapsto F_a P - F_b Q$.
Dedurne la funzione di Hilbert di X*; in particolare:* $h_X(m) = d \Leftrightarrow m \geq a + b - 2$.
Ritrovare (usando h_X*) il fatto che* X *ha grado* ab.

Esercizio 7.5: *Sia $d = 6$. Determinare tutte le possibili funzioni di Hilbert di un insieme di d punti distinti di $\mathbb{P}^2$.*

Esercizio 7.6: *Sia $d \geq 1$ un intero. Si ammetterà che $(\mathbb{P}^2)^d$ è una varietà algebrica irriducibile. Giustificare brevemente la seguente affermazione: $U_d := \{(P_1, \ldots, P_d)/\ P_i \neq P_j$ se $i \neq j\}$ è una varietà algebrica irriducibile (considerare le "diagonali" $D_{ij} = \{(P_1, \ldots, P_d) \in (\mathbb{P}^2)^d/\ P_i = P_j\}$). Il gruppo simmetrico σ_d agisce su U_d: se $s \in \sigma_d$, $s(P_1, \ldots, P_d) = (P_{s(1)}, \ldots, P_{s(d)})$. Si ammetterà che $U_d/\sigma_d =: H(d)$ è una varietà algebrica irriducibile; $H(d)$ parametrizza i sottoinsiemi di d punti (distinti) di $\mathbb{P}^2$.*
Si ammetterà che, per ogni $n \in N$, le applicazioni $h_0(n) : H(d) \to \mathbb{N} : X \longmapsto \dim(\mathbf{I}(X)_n)$, $h_1(n) : H(d) \to \mathbb{N} : X \longmapsto \dim D_n(X)$, sono semicontinue superiormente. ("teorema di semicontinuità della coomologia"). Dimostrare che esiste un aperto non vuoto, W_d, di $H(d)$ tale che: $X \in W_d \Rightarrow X$ è un insieme di d punti di $\mathbb{P}^2$, di rango massimo ("il generico insieme di d punti di $\mathbb{P}^2$ è di rango massimo").

Esercizio 7.7: *Sia $C \subseteq \mathbb{P}^2$ una curva irriducibile di grado d, allora C ha al più $\frac{(d-1)(d-2)}{2}$ punti singolari (hint: per assurdo, aggiungendo $d-3$ punti generici di C e considerando una curva di grado $d-2$ passante per questi $d-3$ punti e i punti singolari di C (perché esiste una tale curva?)).*
(ii) Se una curva irriducibile di grado d ha $\frac{(d-1)(d-2)}{2}$ punti singolari, allora ogni punto singolare è un punto doppio.
(iii) Qual è il numero massimo possibile di punti singolari di una curva di grado d?

Esercizio 7.8: *Sia δ_2 il sistema lineare di tutte le coniche di $\mathbb{P}^2$.*
(i) Il sistema δ_2 è senza punti base. Si considera la corrispondenza $j : \mathbb{P}^2 \to \mathbb{P}(\mathbf{S}_2^*) : x \longmapsto H_x$, dove H_x è l'iperpiano di $\mathbf{S}_2$ costituito dai polinomi omogenei di grado 2 che si annullano in x. Mostrare: j è un'applicazione $\Leftrightarrow$ δ_2 è senza punti base.
(ii) "δ_2 separa i punti": se $p \neq q$ sono due punti di $\mathbb{P}^2$ esiste $C \in \delta_2$ che passa per p ma che non passa per q. Mostrare: j è iniettiva $\Leftrightarrow$ δ_2 separa i punti.
(iii) "d_2 separa i vettori tangenti": sia $p \in \mathbb{P}^2$, e sia t una direzione tangente in p; allora esiste $C \in \delta_2$ passante per p ma non contenente t. Provate a giustificare questa affermazione: δ_2 separa i vettori tangenti $\Leftrightarrow$ la derivata del morfismo j è iniettiva in ogni punto (cioè j è un'immersione).
(iv) Sia $B = (x^2, y^2, z^2, xy, xz, yz)$ base di $\mathbf{S}_2$. Se $a = (a_0 : a_1 : a_2) \in \mathbb{P}^2$, l'iperpiano delle coniche che si annullano in a ha equazione $a_0^2 X^2 + a_1^2 Y^2 + \ldots + a_1 a_2 YZ = 0$ (dove X^2, Y^2,..., YZ è la base duale di B). Con la scelta di queste basi j si scrive:

$$j : \mathbb{P}^2 \to \mathbb{P}^5 : (x : y : z) \longmapsto (x^2 : y^2 : z^2 : xy : xz : yz)$$

Usando le carte affini verificare che j è un morfismo (assumere $x \neq 0$, allora $j(x : y : z) \in U_0 \cap \mathbb{P}^5$; scrivere j in queste carte).

(v) Da quanto precede $V = Im(j)$ *è una superficie liscia di* $\mathbb{P}^5$*, isomorfa a* $\mathbb{P}^2$ *tramite* j *(in particolare* V *è razionale). Sia* $H \subseteq \mathbb{P}^5$ *un iperpiano, mostrare che* $H \cap V$ *è l'immagine tramite* j *di una conica di* $\mathbb{P}^2$*.*
(vi) Un generico $\mathbb{P}^3$ *di* $\mathbb{P}^5$ *interseca* V *in* 4 *punti (cioè* $V \subseteq \mathbb{P}^5$ *ha grado* 4*) (hint: usare* (v)*).*
(vii) Sia $C \subseteq \mathbb{P}^2$ *una curva di grado d, allora* $j(C) \subseteq V \cap \mathbb{P}^5$ *ha grado* $2d$ *(cioè un generico iperpiano di* $\mathbb{P}^5$ *incontra* $j(C)$ *in* $2d$ *punti). In particolare* V *non contiene rette.*
(viii) Dati due punti p*,* q *(anche "infinitamente vicini") di* V *esiste una conica liscia, contenuta in* V*, passante per* p *e* q*. Più precisamente* V *è ricoperta da una famiglia di dimensione due di coniche irriducibili. (usare* (vii)*).*
(ix) Concludere "a occhio" che $Sec(V) := \{z \in \mathbb{P}^5 / \ \exists L$ *retta bisecante a* V *con* $z \in L\}$ *ha dimensione* ≤ 4*. Pertanto,* $Sec(V)$*è strettamente contenuta in* $\mathbb{P}^5$*, e la proiezione da un punto generico di* $\mathbb{P}^5$ *induce un isomorfismo tra* V *e una superficie liscia di* $\mathbb{P}^4$*.*
La superficie V *è la superficie di Veronese, si può dimostrare (Severi, 1905) che* V *è l'unica superficie liscia di* $\mathbb{P}^5$ *la cui varietà delle secanti non riempe tutto* $\mathbb{P}^5$*.*