Un'introduzione light alla geometria algebrica.

Geometria Algebrica 1 (2005-2006)

Ph. Ellia

Printed:
18-2-2006

Indice

CAPITOLO I

Insiemi algebrici affini.

1. Insiemi algebrici affini; il teorema della base.

Notazioni 1.1: *Denoteremo con* $\mathbb{A}^n(k)$ *lo spazio affine di dimensione n sul campo k. Useremo sempre il riferimento standard e si può identificare* $\mathbb{A}^n(k)$ *a* k^n.

Denoteremo con $\mathbf{S}$ *l'anello* $k[X_1, ..., X_n]$ *dei polinomi a coefficienti in k nelle variabili* $X_1, ..., X_n$*; si noterà* $P(X)$ *(o anche solo P) il polinomio* $P(X_1, ..., X_n)$*, a il punto* $(a_1, ..., a_n)$ *di* k^n *e quindi* $P(a)$ *invece di* $P(a_1, ..., a_n)$*. Finalmente* $\deg(P)$ *indicherà il grado del polinomio P (*deg = *degree mentre gr = graded, cioè graduato).*

Definizione 1.2: *Sia T un sottoinsieme di* $k[X_1, ..., X_n]$*, il luogo degli zeri di T (o la "varietà definita da T") è* $\mathbf{V}(T) := \{a \in k^n / P(a) = 0, \forall P \in T\}$.

Definizione 1.3: *Un sottoinsieme* $Z \subset k^n$ *è un sottoinsieme algebrico affine se Z è il luogo degli zeri di un sottoinsieme di* $k[X_1, ..., X_n]$*:* $\exists T \subset k[X_1, ..., X_n]$ *tale che* $Z = \mathbf{V}(T)$.

Esempio 1.4: (i) Ogni sottospazio affine, Z, di k^n è un sottoinsieme algebrico. Infatti Z è l'insieme delle soluzioni di un sistema lineare (di $r = codim(Z)$) equazioni: $L_1(X) = b_1, ..., L_r(X) = b_r$; quindi $Z = \mathbf{V}(T)$ dove $T = \{P_1, ..., P_r\}$ e dove $P_i(X_1, ..., X_n) = L_i(X_1, ..., X_n) - b_i$ sono dei polinomi di grado uno.

(ii) Sia $C \subset k^2$ la conica di equazione $P(X, Y) = aX^2 + bY^2 + cXY + dX + eY + d = 0$, allora $C = \mathbf{V}(P)$ è un insieme algebrico affine.

Un insieme algebrico affine $Z = \mathbf{V}(T)$ è dunque l'insieme delle soluzioni di un sistema (infinito) di equazioni polinomiali: $P(X) = 0, \forall P \in T$. Nel caso dei sottospazi lineari è sempre possibile ricondursi a un sistema con un numero finito di equazioni (prendendo una base dello spazio delle equazioni che definiscono Z). Grazie al "teorema della base" di Hilbert una simile riduzione è possibile per ogni sottoinsieme algebrico affine. Un primo passo verso tale riduzione è fornito dal:

Lemma 1.5: *Sia* $T \subset \mathbf{S} = k[X_1, ..., X_n]$ *un sottoinsieme e sia* $I \subset \mathbf{S}$ *l'ideale generato da T:* $I = \left\{ \sum_{finita} P_i Q_i / P_i \in T, Q_i \in \mathbf{S} \text{ qualsiasi} \right\}$. *Allora* $\mathbf{V}(T) = \mathbf{V}(I)$.

Quindi ogni insieme algebrico affine è della forma $\mathbf{V}(I)$ *per qualche ideale* $I \subset \mathbf{S}$.

DIMOSTRAZIONE. Esercizio 1.1 □

Osservazione 1.6: *La rappresentazione* $Z = \mathbf{V}(I)$ *non è unica. L'insieme algebrico* Z *può essere l'insieme degli zeri di ideali diversi.*

L'esempio più semplice è il seguente: sia $I_n \subset k[X], I_n = (X^n)$. *Allora, per ogni* $n \geq 1$, $\mathbf{V}(I_n) = \{0\}$, *ma* $I_n \neq I_m$ *se* $n \neq m$. *Questo proviene dal fatto che non stiamo considerando le molteplicità delle radici:* 0 *è radice semplice di* $X = 0$, *ma è radice con molteplicità due di* $X^2 = 0$, *ecc...*

Per tenere conto delle molteplicità si introduce la nozione di schema, che generalizza quella di insieme algebrico; lo schema definito da $X^2 = 0$ *è un "punto doppio" (cioè un punto più una direzione tangente) nella retta affine* $\mathbb{A}^1(k)$. *Comunque questa è un'altra storia...*

1.1. Il teorema della base di Hilbert. Il teorema della base di Hilbert asserisce che ogni insieme algebrico affine $Z \subset k^n$ è il luogo degli zeri di un numero finito di polinomi, cioè $Z = \mathbf{V}(P_1) \cap ... \cap \mathbf{V}(P_r)$. Si tratta quindi di un teorema di finitezza. Questo risultato introduce una classe importante di anelli: gli anelli noetheriani (in onore di Emmy Noether). Gli anelli noetheriani sono fondamentali in geometria algebrica perché permettono risultati di finitezza, compatezza.

Definizione 1.7: *Sia* A *un anello e* $T \subset A$ *un sottoinsieme.*

L'ideale generato da $T, \langle T \rangle$, *è l'insieme delle combinazioni lineari finite, a coefficienti in* A, *di elementi di* T : $\langle T \rangle := \left\{ \sum_{finita} a_i t_i / t_i \in T, a_i \in A \right\}$.

Un ideale $I \subset A$ *si dice finitamente generato, se esiste un numero finito di elementi* $g_1, ..., g_r$ *di* I *tali che* $I = \langle \{g_1, ..., g_r\} \rangle$.

In queste condizioni si dice che $(g_1, ..., g_r)$ *è un sistema di generatori dell'ideale* I *e si scrive* $I = (g_1, ..., g_r)$.

Osservazione 1.8: *Se* A *è un campo* k, *un ideale di* k *è un sotto* $k-$*spazio vettoriale; pertanto gli unici ideali di* k *sono* $\{0\}$ *e* k. *La nozione di sistema di generatori corrisponde a quella analoga per i sottospazi vettoriali.*

Definizione 1.9: *Un anello* A *è noetheriano se ogni ideale di* A *è finitamente generato.*

Questa non è la definizione usuale (cf Esercizio 1.3), ma è quella più conveniente per noi adesso.

Osservazione 1.10: *Un anello principale è noetheriano; per esempio $\mathbb{Z}$ è noetheriano.*

Se $A = k$ è un campo, k è ovviamente noetheriano; anche $k[X]$ è noetheriano, perché principale (cfr. Esercizio 1.2).

Teorema 1.11: [Teorema della base]
Sia A un anello noetheriano, allora $A[X_1, ..., X_n]$ è un anello noetheriano. In particolare se k è un campo, $k[X_1, ..., X_n]$ è noetheriano.

Il teorema della base è una conseguenza immediata del:

Teorema 1.12: *Se A è un anello noetheriano, allora anche $A[X]$ è un anello noetheriano.*

Infatti:

Dimostrazione del Teorema 1.11. Si procede per induzione su n tenendo conto che $A[X_1, ..., X_n] = B[X_n]$, dove $B = A[X_1, ..., X_{n-1}]$. □

Dimostrazione del Teorema 1.12. Se $P(X) = a_n X^n + a_{n-1}X^{n-1} + ... + a_1 X + a_0$ è un polinomio di grado n ($a_n \neq 0$), notiamo $i(P) = a_n$ il suo "coefficiente iniziale".

Sia $I \subset A[X]$, dobbiamo mostrare che I è finitamente generato.

Si scelgono induttivamente degli elementi di I con il seguente procedimento:

- $P_1(X)$ è un elemento di I con grado minimale.
- Una volta scelti $P_1(X), ..., P_t(X)$, se $(P_1, ..., P_t) = I$ allora abbiamo finito (I è finitamente generato); altrimenti se $(P_1, ..., P_t) \neq I$, scegliamo P_{t+1} in $I \backslash (P_1, ..., P_t)$, di grado minimale.

Osserviamo che se $P \in I$ e $\deg(P) < \deg(P_i)$ allora $P \in (P_1, ..., P_i)$ (infatti $P \notin (P_1, ..., P_i)$ implica $P \notin (P_1, ..., P_{i-1})$, e si ottiene una contraddizione con la scelta di P_i).

Dobbiamo mostrare che il procedimento termina dopo un numero finito di passi. Nel caso contrario otteniamo una famiglia $(P_i)_{i \in \mathbb{N}}$. Siano $b_1 = i(P_1), b_2 = i(P_2), ...$ i coefficienti iniziali dei polinomi $P_1, P_2, ...$ scelti. Sia $J \subset A$ l'ideale generato dai b_i. Siccome A è noetheriano, J è finitamente generato: $J = (g_1, ..., g_r)$. Per definizione di J ogni g_i è uguale a una somma finita della forma $\sum a_{k(i)} b_{k(i)}$. Possiamo quindi assumere $J = (b_1, ..., b_m)$.

Adesso abbiamo $b_{m+1} = \sum_{1 \leq i \leq m} c_i b_i$, e dall'osservazione precedente: $d \geq d_i, 1 \leq i \leq m$, dove $d = \deg(P_{m+1}), d_i = \deg(P_i)$. Possiamo quindi considerare il polinomio $P(X) = \sum_{1 \leq i \leq m} c_i X^{d-d_i} P_i(X)$. Osserviamo che P e P_{m+1} hanno lo stesso grado e lo stesso coefficiente iniziale. Pertanto se $Q = P_{m+1} - P$, $\deg(Q) < \deg(P_{m+1})$. Siccome Q appartiene ad I ma non appartiene a $(P_1, ..., P_m)$ (perché

$P \in (P_1, ..., P_m)$ mentre $P_{m+1} \notin (P_1, ..., P_m)$, per definizione) questo contraddice la scelta di P_{m+1}. $\square$

Esercizi.

Esercizio 1.1: *Sia $T \subset k[X_1, ..., X_n]$ un sottoinsieme qualsiasi. Dimostrare che $\mathbf{V}(T) = \mathbf{V}(I)$ dove $I \subset k[X_1, ..., X_n]$ è l'ideale generato da T.*

Esercizio 1.2: *(i) Mostrare che $k[X]$ è un anello principale. (Usare la divisione euclidea.)*
(ii) Dimostrare che $k[X, Y]$ non è un anello principale. (Dare un controesempio.)

Esercizio 1.3: *Un anello A soddisfa la condizione della catena ascendente se ogni successione crescente, $I_1 \subset I_2 \subset ... \subset I_n \subset ...$, di ideali di A è stazionaria, cioè esiste t tale che $I_m = I_t$ se $m \geq t$.*

Dimostrare che A è noetheriano se e solo se soddisfa la condizione di catena ascendente (per dimostrare: noetheriano $\Longrightarrow$ c.c.a., considerare $\cup I_i$).

Esercizio 1.4: *(i) Mostrare che l'anello $A = k[X_1, ..., X_n, ...]$ dei polinomi in un'infinità di variabili non è noetheriano. (usare l'esercizio precedente).*
(ii) Mostrare che A è integro.
(iii) Dedurre che un sottanello di un anello noetheriano non è necessariamente noetheriano. (Considerare il campo dei quozienti di A.)

Esercizio 1.5: *Dare un esempio non banale del fatto che un sottoinsieme algebrico affine $Z \subset \mathbb{A}^n$ si può rappresentare in più modi come $Z = \mathbf{V}(I)$ per certo ideale I di $\mathbf{S}$ (cfr. Osservazione 1.6).*

2. Corrispondenza tra ideali ed insiemi algebrici; il teorema degli zeri.

Introduciamo l'operazione $\mathbf{I}$, duale, in qualche modo, dell'operazione $\mathbf{V}$.

Definizione 2.1: *Sia $Z \subset k^n$ un insieme algebrico. L'ideale di Z è l'ideale di tutti i polinomi che si annullano su Z:*

$$\mathbf{I}(Z) = \{P \in k[X_1, ..., X_n] / P(x) = 0, \forall x \in Z\}.$$

Osservazione 2.2: *Per definizione $\mathbf{I}(Z)$ è il più grande ideale che definisce Z; $\mathbf{I}(Z)$ viene anche chiamato l'ideale di definizione di Z.*

Le operazioni $\mathbf{V}, \mathbf{I}$ soddisfano le seguenti proprietà:

Proposizione 2.3: *Siano I, J degli ideali di $k[X_1, ..., X_n]$ e siano Z, Y dei sottoinsiemi algebrici di k^n.*

(i) $I \subset J \Longrightarrow \mathbf{V}(J) \subset \mathbf{V}(I)$
(ii) $Z \subset Y \Longrightarrow \mathbf{I}(Y) \subset \mathbf{I}(Z)$
(iii) $\mathbf{I}(Z \cup Y) = \mathbf{I}(Z) \cap \mathbf{I}(Y)$
(iv) $I \subset \mathbf{I}(\mathbf{V}(I))$
(v) $\mathbf{V}(\mathbf{I}(Y)) = Y$
(vi) Se k è infinito, $\mathbf{I}(k^n) = \{0\}$

Dimostrazione. (i), (ii), (iii), (iv): cfr. Esercizi.

(v) Siccome Y è un sottoinsieme algebrico, $Y = \mathbf{V}(I)$ per qualche ideale I, inoltre $I \subset \mathbf{I}(Y)$ perché $\mathbf{I}(Y)$ è il più grande ideale che definisce Y. Da (i): $\mathbf{V}(\mathbf{I}(Y)) \subset \mathbf{V}(I) = Y$. Viceversa è chiaro che $Y \subset \mathbf{V}(\mathbf{I}(Y))$ perché
$\mathbf{V}(\mathbf{I}(Y)) = \big\{x \in k^n / P(x) = 0, \, \forall P \text{ tale che } P_{|Y} = 0\big\}$.

(vi) Basta mostrare che un polinomio non costante non può annullarsi su tutto k^n. Si procede per induzione su n. Il caso $n = 1$ segue dal fatto che un polinomio in una variabile, a coefficienti in k, ha al più $\deg(P)$ radici.

Sia P un polinomio non costante in n variabili. Scrivendo P secondo le potenze di X_n viene: $P = p_r(X_1, ..., X_{n-1}).X_n^r + ...$ con $r \geq 1$ e $p_r \neq 0$. Per ipotesi di induzione esistono $x_1, ..., x_{n-1}$ tali che $p_r(x_1, ..., x_{n-1}) \neq 0$. Pertanto il polinomio $P(x_1, ..., x_{n-1}, X_n) = p_r(x_1, ..., x_{n-1})X_n^r + ...$ ha grado r e ha un numero finito di radici. Quindi esiste x_n tale che $P(x_1, ..., x_n) \neq 0$. □

Osservazione 2.4: *(i) Se k è un campo finito (vi) non è verificato. Per esempio $(X - a_1).(X - a_2)...(X - a_p)$ si annulla su tutto $k = \{a_1, a_2, ..., a_p\}$.*

(ii) In generale $\mathbf{I}(\mathbf{V}(I)) \neq I$. Per esempio sia $I = (X^2) \subset k[X]$, allora $\mathbf{V}(I) = \{0\}$, e $\mathbf{I}(\mathbf{V}(I)) = (X) \neq I$.

Osservazione 2.5: *Un altro esempio, forse più "preoccupante": sia $J = (X^2+1) \subset \mathbb{R}[X]$. Allora $\mathbf{V}(J) = \emptyset$ e $\mathbf{I}(\mathbf{V}(J)) = \mathbb{R}[X]$; osserviamo che l'ideale J è massimale perché $\mathbb{R}[X]/J \simeq \mathbb{C}$).*

Dai risultati precedenti vediamo che le applicazioni:
φ: {sottoinsiemi algebrici di k^n} $\to$ {ideali di $k[X_1, ..., X_n]$}: $Z \to \mathbf{I}(Z)$
ψ: {ideali di $k[X_1, ..., X_n]$} $\to$ {sottoinsiemi algebrici di k^n}: $I \to \mathbf{V}(I)$,
non sono biiettive ($\psi \circ \varphi = Id$ mentre $\varphi \circ \psi \neq Id$).

Osserviamo che in algebra lineare le operazioni $\mathbf{V}, \mathbf{I}$ corrispondono (modulo l'identificazione in dimensione finita di uno spazio vettoriale con il suo biduale) a prendere gli ortogonali in E, E^*; l'equivalente del teorema di dualità ($V^{\circ\circ} = V$) sarebbe, nella nostra situazione: φ biiettiva e $\varphi^{-1} = \psi$. Per "recuperare" questo risultato bisogna chiaramente restringere il dominio di ψ. Per esempio se I è un ideale allora $\mathbf{V}(I) = \mathbf{V}(I^n)$ per ogni $n = 1$ (cfr. Esercizi). Per evitare questo tipo di situazioni (ed altre dello stesso genere, ma più complicate) si introduce la nozione di ideale radicale:

Definizione 2.6: *Sia A un anello e $I \subset A$ un ideale. Il radicale di $I, r(I)$ (si nota anche $\sqrt{I}$) è: $r(I) = \{x \in A / x^n \in I$, per qualche intero $n > 0$ $\}$.*

Un ideale $J \subset A$ è detto radicale se $J = r(J)$.

Si dimostra che $r(I)$ è un ideale, che un ideale primo è sempre radicale, e che, per ogni ideale $I, r(I)$ è radicale (cfr. Esercizi). Inoltre:

Lemma 2.7: *Sia $Z \subset k^n$ un insieme algebrico, allora $\mathbf{I}(Z)$ è un ideale radicale.*

DIMOSTRAZIONE. Per semplificare poniamo $\mathbf{I} = \mathbf{I}(Z)$. Abbiamo $\mathbf{I} \subset r(\mathbf{I})$ perché ogni ideale è contenuto nel suo radicale. Sia $f \in r(\mathbf{I})$, per definizione esiste m tale che $f^m \in \mathbf{I}$. Pertanto $f^m(x) = 0$ per ogni x in Z. Quindi $f^m(x) = (f(x))^m = 0$, ossia $f(x) = 0$ (k è integro) per ogni x in Z, e $f \in \mathbf{I}$. □

L'idea è di limitare le nostre considerazioni agli ideali radicali: si elimina così l'esempio dell'Osservazione 2.4. Ma questo non è sufficiente, infatti l'ideale J dell'Osservazione 2.5 è radicale (perché primo); il fatto è che $\mathbb{R}$ non essendo algebricamente chiuso, il luogo degli zeri di $X^2 + 1 = 0$ è vuoto. Il teorema seguente, ancora dovuto a Hilbert, mostra che sotto l'ipotesi che k sia algebricamente chiuso, e considerando solo ideali radicali, si ottiene una buona dualità tra $\mathbf{V}$ e $\mathbf{I}$:

Teorema 2.8: *("Nullstellensatz", teorema degli zeri)*

Se k è algebricamente chiuso e se $I \subset k[X_1, ..., X_n]$ è un ideale allora: $\mathbf{I}(\mathbf{V}(I)) = r(I)$.

DIMOSTRAZIONE. Un buon libro di algebra (cfr. Bibliografia). □

Osservazione 2.9: *L'ipotesi k algebricamente chiuso è necessaria (cfr. Osservazione 2.5).*

Corollario 2.10: *Se k è algebricamente chiuso, le applicazioni:*

φ: $\{$sottoinsiemi algebrici di $k^n\} \to \{$ideali radicali di $k[X_1, ..., X_n]\}$:
$Z \to \mathbf{I}(Z)$
ψ: $\{$ideali radicali di $k[X_1, ..., X_n]\} \to \{$sottoinsiemi algebrici di $k^n\}$:
$I \to \mathbf{V}(I)$,
sono biiettive e $\varphi^{-1} = \psi$.

DIMOSTRAZIONE. L'applicazione è ben definita (Lemma 2.7). Sappiamo già che $\psi \circ \varphi = Id$. Abbiamo $(\varphi \circ \psi)(I) = \mathbf{I}(\mathbf{V}(I))$. Dal teorema degli zeri: $\mathbf{I}(\mathbf{V}(I)) = r(I)$, siccome per ipotesi I è radicale, $\mathbf{I}(\mathbf{V}(I)) = I$, cioè $\varphi \circ \psi = Id$. □

Osservazione 2.11: *Quindi se $Z = \mathbf{V}(I)$, allora $\mathbf{I}(Z) = \mathbf{I}(\mathbf{V}(I)) = r(I)$, cioè $r(I)$ è il più grande ideale che definisce Z.*

Ecco altre notevoli conseguenze del teorema degli zeri:

Proposizione 2.12: *Sia k un campo algebricamente chiuso. Il sistema di equazioni polinomiali: $f_1(x_1, ..., x_n) = 0, ..., f_m(x_1, ..., x_n) = 0$, non ammette soluzioni in k^n se e solo se esistono dei polinomi $g_1, ..., g_m$ tali che: $1 = \sum f_i g_i$.*

DIMOSTRAZIONE. Il sistema non ha soluzioni se e solo se $\mathbf{V}(I) = \emptyset$ dove $I = (f_1, ..., f_m)$. Dal teorema degli zeri $\mathbf{I}(\mathbf{V}(I)) = r(I)$. Quindi il sistema non ha soluzioni se e solo se $r(I) = \mathbf{S}$, cioè se e solo se $1 \in I$. □

Proposizione 2.13: *Sia k un campo algebricamente chiuso. L'ideale $m \subset k[X_1, ..., X_n]$ è massimale se e solo se $m = (X_1 - a_1, ..., X_n - a_n)$, per opportuni $a_1, ..., a_n$ in k.*

DIMOSTRAZIONE. È chiaro che un ideale del tipo $(X_1 - a_1, ..., X_n - a_n)$ è massimale perché $\mathbf{S}/(X_1 - a_1, .., X_n - a_n) \simeq k$ (l'applicazione $\mathbf{S} \to \mathbf{S}/(X_1 - a_1, .., X_n - a_n)$ si identifica con la valutazione dei polinomi nel punto $a = (a_1, ..., a_n)$).

Viceversa sia m un ideale massimale di $\mathbf{S}$ e sia $Z = \mathbf{V}(m)$. Dal teorema degli zeri, $\mathbf{I}(Z) = r(m)$, inoltre $r(m) = m$ (perché m è primo, Esercizio 2.2), quindi $\mathbf{I}(Z) \neq \mathbf{S}$, e Z è non vuoto. Sia a un punto di Z allora $m = \mathbf{I}(Z) \subset \mathbf{I}(\{a\}) = (X_1 - a_1, ..., X_n - a_n)$ (cfr. Proposizione 2.3, (ii)), per massimalità: $m = (X_1 - a_1, ..., X_n - a_n)$. □

Osservazione 2.14: *(i) La proposizione precedente è nota anche come il "teorema degli zeri debole" ("weak Nullstellensatz").*

(ii) La proposizione si può riformulare nel modo seguente: se k è algebricamente chiuso, l'applicazione $a = (a_1, ..., a_n) \to m = (X_1 - a_1, ..., X_n - a_n)$ è una biiezione tra l'insieme dei punti di k^n e l'insieme degli ideali massimali di $k[X_1, ..., X_n]$.

Se $Z \subset k^n$ è un insieme algebrico l'insieme dei punti di Z è in biiezione con l'insieme degli ideali massimali di $\mathbf{S}$ contenenti $\mathbf{I}(Z)$, questo si può riformulare più precisamente cogliendo l'occasione per introdurre un nuovo oggetto importante:

Definizione 2.15: *Sia $Z \subset k^n$ un insieme algebrico. L'anello delle coordinate di Z è l'anello quoziente $A(Z) := k[X_1, ..., X_n]/\mathbf{I}(Z)$.*

Osservazione 2.16: *Osservare che $A(Z)$ è una k-algebra cioè è un anello e un k -spazio vettoriale e queste due strutture sono compatibili tra di loro; per questo $A(Z)$ viene anche chiamata "algebra affine di Z".*

Corollario 2.17: *Sia $Z \subset k^n$ un insieme algebrico. L'insieme dei punti di Z è in biiezione con l'insieme degli ideali massimali di $A(Z)$ (cioè con gli ideali massimali di $\mathbf{S}$ contenenti $\mathbf{I}(Z)$).*

DIMOSTRAZIONE. Segue dal fatto che gli ideali di $A(Z)$ corrispondono agli ideali di $\mathbf{S}$ contenenti $\mathbf{I}(Z)$. □

La corrispondenza tra punti e ideali massimali è fondamentale in geometria algebrica. (adeguatamente generalizzata porta poi alla nozione di schema, la quale permette di usare il linguaggio della geometria non solo su un campo k (algebricamente chiuso) ma su un anello A qualsiasi, per esempio $A = \mathbb{Z}, \mathbb{Q}, ...$).

Per potere sfruttare il teorema degli zeri (e per semplificarci inizialmente la vita) facciamo la:

Convenzione sul campo *D'ora in poi, il campo k sarà sempre supposto algebricamente chiuso.*

Esercizi.

Esercizio 2.1: *Dimostrare i punti (i), ...,(iv) della Proposizione 2.3.*

(2) Sia $Z = \mathbf{V}(I)$ *e* $Y = \mathbf{V}(J)$. *Mostrare che* $\mathbf{V}(I) \cap \mathbf{V}(J) = \mathbf{V}(I + J)$. *Dedurne che* $\mathbf{I}(Z \cap Y) = r(I + J)$ *(qualsiasi siano gli ideali* I, J *che definiscono* Z, Y*). In particolare:* $\mathbf{I}(Z \cap Y) = r(\mathbf{I}(Z) + \mathbf{I}(Y))$.

(3) Sia Z *la parabola di equazione* $y = x^2$ *e sia* Y *l'asse* $y = 0$ *(quindi* $\mathbf{I}(Z) = (y - x^2)$, $\mathbf{I}(Y) = (y)$*). Mostrare che* $\mathbf{I}(Z \cap Y) = (x, y)$ *(la somma di due ideali radicali non è necessariamente radicale).*

(4) $\mathbf{V}(I^n) = \mathbf{V}(I)$ *per ogni* $n \geq 1$. *(attenzione:* I^n *è l'ideale generato da tutti i prodotti* $f_1 f_2 ... f_n$ *con* $f_i \in I$*)*

Esercizio 2.2: *Sia* A *un anello e* $I \subset A$ *un ideale.*

(i) Mostrare che $r(I)$ *è un ideale, e che* $r(r(I)) = r(I)$ *(cioè* $r(I)$ *è radicale).*

(ii) Mostrare che un ideale primo è radicale. Più generalmente se $\mathfrak{p}$ *è un ideale primo, allora* $r(\mathfrak{p}^m) = \mathfrak{p}$.

(iii) Dare un esempio di un ideale radicale che non sia primo.

Esercizio 2.3: *Sia* A *un anello e* $I \subset A$ *un ideale. Scopo dell'esercizio è di dimostrare che* $r(I)$ *è l'intersezione di tutti gli ideali primi che contengono* I.

(i) Un elemento $x \in A$ *è nilpotente se* $x^m = 0$ *per qualche* $m > 0$. *Sia* $\mathcal{N}$ *l'insieme degli elementi nilpotenti di* A. *Dimostrare che* $\mathcal{N}$ *è un ideale di* A *(usare la formula del binomio), e che l'anello quoziente* $A/\mathcal{N}$ *non possiede elementi nilpotenti non nulli (*$\mathcal{N}$ *si chiama il nilradicale di* A*).*

(ii) Mostriamo che il nilradicale è uguale all'intersezione di tutti gli ideali primi di A. *Sia* $\widetilde{\mathcal{N}}$ *l'intersezione di tutti gli ideali primi di* A. *Verificare che* $\mathcal{N} \subset \widetilde{\mathcal{N}}$.

(iii) Sia $f \notin \mathcal{N}$ *e mostriamo che* $f \notin \widetilde{\mathcal{N}}$. *Sia* S *l'insieme degli ideali* J *tali che:* $m > 0 \Longrightarrow f^m \notin J$. *L'insieme* S *è non vuoto (*$0 \in S$*), e il lemma di Zorn dice che* S *ammette un elemento massimale per l'inclusione. Sia* $\mathfrak{p}$ *un elemento massimale. Mostriamo che* $\mathfrak{p}$ *è primo. Se* $x, y \notin \mathfrak{p}$, *gli ideali* $\mathfrak{p} + (x)$, $\mathfrak{p} + (y)$ *non appartengono a* S *(perché?). Quindi* $f^m \in \mathfrak{p} + (x)$, $f^t \in \mathfrak{p} + (y)$. *Dedurne che* $\mathfrak{p} + (xy) \notin S$ *(mostrare* $f^{m+t} \in \mathfrak{p} + (xy)$*). Concludere che* $xy \notin \mathfrak{p}$, *e che* $\mathfrak{p}$ *è primo. Questo completa la dimostrazione dell'uguaglianza:* $\mathcal{N} = \widetilde{\mathcal{N}}$.

(iv) Dedurre da quanto precede che $r(I)$ *è l'intersezione degli ideali primi che contengono* I *(considerare* A/I*).*

Esercizio 2.4: *Sia* $Z \subset k^n$ *un insieme algebrico. Mostrare che la* k*-algebra* $A(Z)$ *è ridotta, cioè non contiene elementi nilpotenti non nulli (cfr. Esercizio 2.3 per la definizione di elemento nilpotente di un anello).*

Esercizio 2.5: *Sia* $X \subset k^n$ *un insieme algebrico e* p *un punto di* k^n, $p \notin X$. *Dimostrare che esiste* $P \in k[X_1, ..., X_n]$ *tale che* $P(p) = 1$ *e* $P_{|X} = 0$.

3. Topologia di Zariski.

Su $\mathbb{R}^n$ (o $\mathbb{C}^n$) abbiamo la topologia euclidea (detta anche topologia usuale o trascendente) usata in geometria differenziale o in geometria analitica; questa topologia non è definita algebricamente. Se k è un campo qualsiasi non c'è, a priori, una topologia su k^n che generalizzi la topologia euclidea. Siamo dunque alla ricerca di una topologia. Vediamo a quali condizioni dovrebbe soddisfare una topologia sensata nell'ambito della geometria algebrica. Intanto, anche se non abbiamo ancora definito i morfismi tra insiemi algebrici ("applicazioni algebriche"), vogliamo senz'altro che una funzione polinomiale $P : k^n \to k : (x_1, ..., x_n) \to P(x_1, ..., x_n)$ sia un morfismo, e quindi un'applicazione continua per la nostra topologia. Pertanto $P^{-1}(0) = \mathbf{V}(P)$ dovrà essere un chiuso (ammesso che $\{0\} \subset k$ sia chiuso). Segue pertanto (dal teorema della base, Sezione 1) che ogni insieme algebrico $Z \subset k^n$ dovrà essere un chiuso. La proposizione seguente mostra che questa richiesta è sufficiente per definire una topologia su k^n:

Proposizione 3.1: *(i) k^n e l'insieme vuoto sono dei sottoinsiemi algebrici di k^n.*

(ii) Un'intersezione qualsiasi di sottoinsiemi algebrici di k^n è un sottoinsieme algebrico di k^n.

(iii) Un'unione finita di sottoinsiemi algebrici di k^n è un sottoinsieme algebrico di k^n.

Dimostrazione. (i) k^n è il luogo degli zeri del polinomio nullo mentre $\emptyset = \mathbf{V}(1)$.

(ii) Siano $Z_i \subset k^n, Z_i = \mathbf{V}(I_i)$. Allora $\cap Zi = \mathbf{V}(\Sigma I_i)$ dove ΣI_i è l'ideale generato da $\cup I_i$ (N.B. in generale $\cup I_i$ non è un ideale!).

(iii) Se $Z = \mathbf{V}(I), Y = \mathbf{V}(J)$ allora $Z \cup Y = \mathbf{V}(IJ)$ (cfr. Esercizio 3.1). □

Definizione 3.2: *La proposizione precedente mostra che i sottoinsiemi algebrici di k^n sono i chiusi di una topologia su k^n. Questa topologia è chiamata la topologia di Zariski (in onore di Oscar Zariski). Se $Z \subset k^n$ è un insieme algebrico, la topologia di Zariski su Z è la topologia indotta dalla topologia di Zariski su k^n.*

La topologia di Zariski è molto diversa dalla topologia usuale: gli aperti sono molto grandi e i chiusi molto piccoli.

Esempio 3.3: (1) Sia $Z \subset k$ un insieme algebrico (k algebricamente chiuso). Siccome $k[X]$ è un anello principale, $\mathbf{I}(Z)$ è generato da un unico elemento: $\mathbf{I}(Z) = (P(X))$. Se Z è non vuoto e $Z \neq k, Z$ consta di un numero finito di punti (le radici di P). In conclusione i chiusi della retta affine $\mathbb{A}^1(k)$ per la topologia di Zariski sono: $\mathbb{A}^1(k)$, il vuoto e gli insiemi finiti. In particolare due aperti non vuoti hanno sempre un'intersezione non vuota (quindi la topologia non è di Hausdorff), e $\mathbb{A}^1(k)$ è compatto (cf Proposizione 3.7).

Esempio 3.4: Insiemisticamente $k^2 = k \times k$ però la topologia di Zariski su k^2 non è la topologia prodotto delle topologie di Zariski su k (cf Esercizio 3.2).

Definizione 3.5: *Un aperto standard di k^n per la topologia di Zariski è un aperto della forma $k^n \backslash \mathbf{V}(P)$ dove $P \in k[X_1, ..., X_n]$. Si nota $D(P)$ l'aperto standard definito da P.*

Gli aperti standard sono i complementari delle ipersuperfici (insiemi algebrici definiti da un'unica equazione).

Proposizione 3.6: *Ogni aperto di k^n per la topologia di Zariski è un'unione finita di aperti standard. Gli aperti standard formano una base della topologia di Zariski.*

DIMOSTRAZIONE. Segue dal fatto che, per il teorema della base, ogni insieme algebrico è un'intersezione finita di ipersuperfici. □

Proposizione 3.7: *(i) Lo spazio affine $\mathbb{A}^n(k)$ è compatto per la topologia di Zariski (cioè da ogni ricoprimento aperto si può estrarre un sotto ricoprimento finito).*

(ii) Un insieme algebrico $Z \subset k^n$ è compatto per la topologia di Zariski.

DIMOSTRAZIONE. (i) Possiamo limitarci a ricoprimenti con aperti standard: $k^n = \bigcup_{i \in I} D(P_i)$. Si ha allora $\bigcap_{i \in I} \mathbf{V}(P_i) = \emptyset$, cioè $\mathbf{V}(J) = \emptyset$ dove J è l'ideale generato dai P_i. Dal teorema della base J è generato da un numero finito di elementi che possiamo scegliere tra i P_i: $J = (P_1, ..., P_m)$. Si conclude perché $k^n = D(P_1) \cup ... \cup D(P_m)$.

(ii) Segue dal fatto che ogni chiuso di uno spazio topologico compatto è compatto per la topologia indotta. □

Osservazione 3.8: *Vediamo come il fatto di lavorare su un anello noetheriano (il campo k) si traduce in proprietà di compatezza (finitezza).*

Definizione 3.9: *Uno spazio topologico X è irriducibile se per ogni coppia, (U, V), di aperti non vuoti di X si ha $U \cap V \neq \emptyset$.*

Osservazione 3.10: *Uno spazio topologico non irriducibile è detto riducibile. L'insieme vuoto è (per convenzione) riducibile.*

Proposizione 3.11: *Sia X uno spazio topologico. Sono equivalenti:*

(i) X è irriducibile.

(ii) Se F, F' sono due chiusi di X tali che $X = F \cup F'$ allora $X = F$ o $X = F'$.

(iii) Ogni aperto non vuoto di X è denso in X.

DIMOSTRAZIONE. cfr. Esercizi. □

3.1. Insiemi irriducibili. Cerchiamo adesso una traduzione algebrica del fatto che un insieme algebrico Z di k^n è irriducibile, cioè lo spazio topologico Z (con la topologia di Zariski) è irriducibile.

Proposizione 3.12: *Sia $Z \subset k^n$ un insieme algebrico. Sono equivalenti:*
(i) Z è irriducibile.
(ii) $\mathbf{I}(Z)$ è un ideale primo.
(iii) $A(Z)$ è un anello integro.

DIMOSTRAZIONE. (i) $\Longrightarrow$ (ii) Per contrapposizione: se $\mathbf{I}(Z)$ non è primo esistono $P, F \notin \mathbf{I}(Z)$ tali che $PF \in \mathbf{I}(Z)$. Pertanto $Z \subset \mathbf{V}(PF) = \mathbf{V}(P) \cup \mathbf{V}(F)$, e $Z = Z' \cup Z''$ dove $Z' = Z \cap \mathbf{V}(P)$, $Z'' = Z \cap \mathbf{V}(F)$. Siccome $P, F \notin \mathbf{I}(Z)$, Z', Z'' sono chiusi propri di Z. Pertanto Z è riducibile.

(ii) $\Longrightarrow$ (i) Per contrapposizione: se Z è riducibile, Z si scrive come l'unione di due chiusi propri: $Z = Z_1 \cup Z_2$. Siccome $Z_i \neq Z$, $\mathbf{I}(Z)$ è strettamente contenuto in $\mathbf{I}(Z_i)$. Possiamo quindi trovare $f_i \in \mathbf{I}(Z_i) \backslash \mathbf{I}(Z)$. Abbiamo $f_1 f_2 \in \mathbf{I}(Z_1) \cap \mathbf{I}(Z_2) = \mathbf{I}(Z_1 \cup Z_2) = \mathbf{I}(Z)$, quindi $\mathbf{I}(Z)$ non è primo.

(ii) $\Longleftrightarrow$ (iii) È chiaro. □

Corollario 3.13: *Lo spazio affine $\mathbb{A}^n(k)$ è irriducibile.*

DIMOSTRAZIONE. Infatti $\mathbf{I}(k^n) = \{0\}$ è primo in $\mathbf{S}$. □

Osservazione 3.14: *Si ricorda che per convenzione k è algebricamente chiuso (quindi infinito). In effetti il corollario precedente è valido sotto l'ipotesi k infinito, ma non è valido se k è un campo finito (in questo caso k^n è unione di un numero finito di punti che sono chiusi). Il fatto è che se k è infinito si può identificare un polinomio con la sua funzione polinomiale, mentre questo non è più vero se k è finito.*

Proposizione 3.15: *(prolungamento delle identità algebriche) Sia $Z \subset k^n$ un insieme algebrico e siano P, Q due elementi di $k[X_1, ..., X_n]$. Se $P(x) = Q(x), \forall x \in k^n \backslash Z$, allora $P = Q$.*

DIMOSTRAZIONE. Basta dimostrare che se un polinomio, P, si annulla su $k^n \backslash Z$ allora è identicamente nullo. Si ha $U \subset \mathbf{V}(P)$ dove U è l'aperto $k^n \backslash Z$, quindi $\overline{U} \subset \overline{\mathbf{V}(P)} = \mathbf{V}(P)$ (perché $\mathbf{V}(P)$ è chiuso); ma per la Proposizione 3.11, (iii), e il Corollario 3.13, $\overline{U} = k^n$, quindi $\mathbf{V}(P) = k^n$. □

Osservazione 3.16: *La proposizione precedente è valida sotto l'ipotesi più debole che k sia infinito (per es. $k = \mathbb{R}$).*

3.2. Decomposizione in componenti irriducibili. Sia $Y \subset \mathbb{A}^n$ un sottoinsieme algebrico. In generale Y non è irriducibile, e quindi può essere scritto nella

forma $Y = Y_1 \cup Y_2$ dove Y_i sono due sottoinsiemi algebrici. Se Y_j non è irriducibile, possiamo sciverlo a sua volta come unione di due sottoinsiemi algebrici, ecc... Siccome $k[X_1, ..., X_n]$ è noetheriano (cfr. Teorema 1.11) questo procedimento ha una fine e riusciamo a scrivere Y come un'unione finita di insiemi algebrici irriducibili; inoltre questa scrittura è unica.

Definizione 3.17: *Un insieme algebrico $Y \subset k^n$ ammette una decomposizione in componenti irriducibili se $Y = Y_1 \cup ... \cup Y_r$, dove gli Y_i sono degli insiemi algebrici irriducibili tali che Y_i non è contenuto in Y_j se $i \neq j$.*

Lemma 3.18: *Sia A un anello. Sono equivalenti:*

(i) A è noetheriano.

(ii) ogni insieme non vuoto, $\mathcal{F}$, di ideali di A ha un elemento massimale per l'inclusione (i.e. esiste $I \in \mathcal{F}$ tale che $J \in \mathcal{F}$ e $I \subset J$ implica $J = I$).

(iii) ogni successione crescente $I_1 \subset I_2 \subset ... \subset I_n \subset ...$ di ideali di A è stazionaria (i.e. esiste m tale che $I_n = I_m$ per ogni $n \geq m$).

Dimostrazione. (i) $\Longrightarrow$ (ii) Per l'assioma della scelta possiamo costruire un'applicazione $f : \mathcal{P}(\mathcal{F}) \to \mathcal{F} : S \to I_S$, tale che $I_S \in S$ (qui $\mathcal{P}(\mathcal{F})$ è l'insieme delle parti di $\mathcal{F}$). Sia $I_0 = f(\mathcal{F})$ l'ideale corrispondente a $\mathcal{F}$, e $S_1 = \{J \in \mathcal{F} / I_0 \subset J, I_0 \neq J\}$. Se S_1 è vuoto abbiamo finito, I_0 è massimale per l'inclusione in $\mathcal{F}$. Se S_1 non è vuoto sia $I_1 = f(S_1)$. Definiamo $S_2 = \{J \in \mathcal{F} / I_1 \subset J, I_1 \neq J\}$. Se S_2 è vuoto, I_1 è massimale per l'inclusione in $\mathcal{F}$. Vediamo quindi che basta mostrare che per qualche n, S_n è vuoto. Supponiamo per assurdo S_n non vuoto , per ogni n. Osserviamo che per costruzione $I_p \in S_p = \{J \in \mathcal{F} / I_{p-1} \subset J, I_{p-1} \neq J\}$; quindi $I_{p-1} \subset I_p$. Sia $I = \bigcup_{n \geq 0} I_n$, I è un ideale di A. Siccome A è noetheriano, I è finitamente generato: $I = (f_1, ..., f_r), f_i \in I_{n_i}$. Sia $m = \max\{n_i\}, 1 \leq i \leq r$. Allora $f_i \in I_m, 1 \leq i \leq r$, e questo implica $I = I_m$, assurdo.

(ii) $\Longrightarrow$ (iii) L'insieme $\{I_n\}$ possiede un elemento massimale per l'inclusione, diciamo I_m. Segue che $I_n = I_m$, per ogni $n \geq m$.

(iii) $\Longrightarrow$ (i) Sia $I \neq \{0\}$ un ideale di A, e sia x un elemento non nullo di I. Poniamo $I_1 = (x)$. Se $I_1 \neq I$ sia $x_2 \in I \backslash I_1$, e poniamo $I_2 = (x, x_2)$. Abbiamo $I_1 \subset I_2$. Procedendo in questo modo otteniamo una catena ascendente di ideali: $I_1 \subset I_2 \subset ... \subset I_n \subset ...$, da (iii) questa catena è stazionaria: $I_n = I_m$ se $n \geq m$. Quindi $I = I_m = (x, x_2, ..., x_m)$ è finitamente generato. □

Osservazione 3.19: *L'equivalenza tra (i) e (iii) si può dimostrare direttamente senza passare da (ii), cfr. Esercizio 1.3.*

Corollario 3.20: *Sia T un insieme non vuoto di sottoinsiemi algebrici di $\mathbb{A}^n$. Allora T possiede un elemento minimale per l'inclusione.*

DIMOSTRAZIONE. Usando la corrispondenza tra sottoinsiemi algebrici e ideali (radicali) di $k[X_1, ..., X_n]$, corrispondenza che inverte le inclusioni, il corollario discende dal lemma precedente, visto che $k[X_1, ..., X_n]$ è noetheriano. □

Proposizione 3.21: *Ogni sottoinsieme algebrico non vuoto di $\mathbb{A}^n$ ammette una, ed un'unica, decomposizione in componenti irriducibili.*

DIMOSTRAZIONE. Sia Y un sottoinsieme algebrico non vuoto di $\mathbb{A}^n$. Per prima cosa mostriamo l'esistenza di una decomposizione in componenti irriducibili, poi mostreremo l'unicità. Sia T l'insieme dei sottoinsiemi algebrici non vuoti che non ammettono una decomposizione in componenti irriducibili. Se T è non vuoto, dal corollario precedente, T ammette un elemento minimale, X. Per definizione di T, X non è irriducibile, quindi possiamo scrivere $X = X' \cup X''$ dove X', X'' sono insiemi algebrici strettamente contenuti in X. Per minimalità di X, X' e X'' ammettono una decomposizione in componenti irriducibili: $X' = \cup Z'_i, X'' = \cup Z''_j$. Segue che $X = (\cup Z'_i) \cup (\cup Z''_j)$ è una decomposizione di X in componenti irriducibili; assurdo.

Quindi ogni sottoinsieme algebrico, Y, ammette una decomposizione in componenti irriducibili: $Y = \cup Y_i$. Scartando semmai alcuni degli Y_i possiamo supporre Y_i non contenuto in Y_j se $i \neq j$. Mostriamo l'unicità di una tale decomposizione. Supponiamo di avere due tali decomposizioni: $Y = \bigcup_{1 \leq i \leq r} Y_i = \bigcup_{1 \leq j \leq t} Z_j$. Abbiamo $Y_1 = \cup (Z_j \cap Y_1)$. Ma Y_1 è irriducibile quindi $Y_1 \subset Z_m$ per qualche m. Riordinando gli indici possiamo supporre $m = 1$. Nello stesso modo $Z_1 \subset Y_s$. Segue che $Y_1 \subset Y_s$, quindi $s = 1$ e $Y_1 = Z_1$. Sia Y' la chiusura di $Y \backslash Y_1$; Y' è un sottoinsieme algebrico e $Y' = \bigcup_{2 \leq i \leq r} Y_i = \bigcup_{2 \leq j \leq t} Z_j$. Si conclude per induzione su r. □

Gli insiemi algebrici irriducibili sono quindi gli "atomi" degli insiemi algebrici, questo giustifica la seguente:

Definizione 3.22: *Una varietà algebrica affine $Z \subset k^n$ è un insieme algebrico irriducibile. Una varietà quasi-affine è un aperto non vuoto di una varietà affine.*

Notazioni 3.23: *Certi autori chiamano "varietà" quello che noi chiamiamo "insieme algebrico" e "varietà irriducibile" quello che noi chiamiamo "varietà"; questa terminologia che è quella più diffusa, è anche più comoda; la adotteremo anche noi più avanti, ma per il momento per distinguere bene le nozioni, seguiteremo ad usare la terminologia introdotta nella definizione precedente.*

Lemma 3.24: *Sia $P \in k[X_1, ..., X_n]$ un polinomio non costante e sia $P = P_1^{r_1} ... P_t^{r_t}$ la sua decomposizione in fattori irriducibili. La decomposizione in componenti irriducibili di $T = \mathbf{V}(P)$ è data da: $T = \mathbf{V}(P_1) \cup ... \cup \mathbf{V}(P_t)$, inoltre $\mathbf{I}(T) = (Q)$ dove Q è il polinomio $P_1 ... P_t$.*

DIMOSTRAZIONE. E' chiaro che $T = \mathbf{V}(P_1) \cup ... \cup \mathbf{V}(P_t)$. Ogni $\mathbf{V}(P_i)$ è irriducibile perché P_i lo è (cioè l'ideale (P_i) è primo). Inoltre $\mathbf{V}(P_i)$ non è contenuto in nessun $\mathbf{V}(P_j), j \neq i$, perché P_j è irriducibile. Quindi (per unicità) questa è la decomposizione in componenti irriducibili. Inoltre abbiamo: $\mathbf{I}(\bigcup_i \mathbf{V}(P_i)) = \bigcap_i \mathbf{I}(\mathbf{V}(P_i))$. Siccome (P_i) è un ideale primo, $\mathbf{I}(\mathbf{V}(P_i)) = (P_i)$. Finalmente $\bigcap_i (P_i) = (P_1...P_t)$ perché, essendo i P_i primi, ogni polinomio divisibile per ogni P_i, è divisibile per il prodotto $P_1...P_t$. □

Osservazione 3.25: *Segue dal lemma precedente che esiste una corrispondenza biiunivoca tra le ipersuperfici irriducibili di $\mathbb{A}^n$ e i polinomi irriducibili di $k[X_1, ..., X_n]$ (modulo identificare P e λP, $\lambda \neq 0$, $\lambda \in k$).*

Per concludere osserviamo un'ulteriore conseguenza del teorema degli zeri:

Proposizione 3.26: *Sia $P \in k[X_1, ..., X_n]$ un polinomio non costante (e k algebricamente chiuso). Se $n \geq 2$ allora $\mathbf{V}(P)$ è un insieme infinito.*

DIMOSTRAZIONE. Sia $P = P_1^{a_1}...P_r^{a_r}$ la decomposizione in fattori irriducibili. Ogni P_i è irriducibile, e $\mathbf{V}(P_i) \subset \mathbf{V}(P)$. Quindi basta mostrare che $\mathbf{V}(Q)$ è un insieme infinito se Q è irriducibile. Se $\mathbf{V}(Q)$ non è infinito, è un insieme finito di punti, e essendo irriducibile, $\mathbf{V}(Q)$ è un punto. Pertanto $\mathbf{I}(\mathbf{V}(Q)) = (Q)$ è un ideale massimale: $(Q) = (X_1 - a_1, ..., X_n - a_n)$ ("teorema degli zeri debole", cfr. Sezione 2). Se $n \geq 2$ questo è assurdo ($X_1 - a_1$ e $X_2 - a_2$ non hanno fattori in comune). □

Osservazione 3.27: *Ancora una volta, l'ipotesi k algebricamenete chiuso è essenziale.*

Esercizi.

Esercizio 3.1: *(i) Scrivere i dettagli della dimostrazione della Proposizione 3.1.*

(ii) Se $Z = \mathbf{V}(I), Y = \mathbf{V}(J)$, mostrare che $Z \cup Y = \mathbf{V}(I \cap J)$.

(iii) Mostrare che $\mathbf{I}(Z \cup Y) = \sqrt{I} \cap \sqrt{J}$.

(iv) Mostrare che $Z \cup Y = \mathbf{V}(IJ)$. Dimostrare che $IJ \subset I \cap J$ e dare un esempio per mostrare che l'inclusione può essere stretta.

(v) Concludere che: $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J} = \sqrt{IJ}$.

Esercizio 3.2: *Un spazio topologico X è di Hausdorff se presi due punti $x \neq y$ di X, esistono degli aperti, U, V tali che: $x \in U$, $y \in V$ e $U \cap V = \emptyset$.*
(i) Mostrare che uno spazio topologico X è di Hausdorff se e solo se la diagonale $\Delta \subset X \times X$ ($\Delta = \{(x, x) |\ x \in X\}$) è chiusa nella topologia prodotto su $X \times X$.
(ii) Mostrare che la diagonale $\Delta \subset \mathbb{A}^2 \simeq k \times k$ è chiusa per la topologia di Zariski. Dedurne che la topologia di Zariski su $\mathbb{A}^2$ non è la topologia prodotto di $\mathbb{A}^1$.

Esercizio 3.3: *(i) Dimostrare la Proposizione 3.11.*

(ii) Sia X uno spazio topologico irriducibile e $U \subset X$ un aperto non vuoto. Dimostrare che U è irriducibile.

(iii) Sia X uno spazio topologico e $Y \subset X$; allora: Y irriducibile $\Longrightarrow \overline{Y}$ irriducibile ($\overline{Y}$ è la chiusura di Y in X).

(iv) Siano X, Y degli spazi topologici, $Z \subset X$ e $f : X \to Y$ un'applicazione continua. Allora: Z irriducibile $\Longrightarrow f(Z)$ irriducibile.

(v) Quali sono i sottospazi irriducibili di $\mathbb{R}$ con la topologia usuale?

Esercizio 3.4: *Sia $M_n(k)$ l'insieme delle matrici $n \times n$ a coefficienti in k. Identificando $M_n(k)$ con k^{n^2} mostrare che $R_{n-1} = \{A \in M_n(k) / rango(A) < n\}$ è un insieme algebrico.*

Usare il prolungamento delle identità algebriche (Proposizione 3.15) per dimostrare che se A e B sono due matrici quadrate allora AB e BA hanno lo stesso polinomio caratteristico (assumere prima B invertibile e usare $AB = B^{-1}(BA)B$).

Esercizio 3.5: *Sia $P(X, Y) = Y^2 + X^2(X-1)^2 \in \mathbb{R}[X, Y]$.*

(i) Dimostrare che l'ideale (P) è primo (mostrare che $P(X, Y)$ è irriducibile considerandolo come un polinomio in Y).

(ii) Determinare $\mathbf{V}(P), \mathbf{I}(\mathbf{V}(P))$. Dire se $\mathbf{V}(P)$ è irriducibile, infinito.

Esercizio 3.6: *(i) Determinare la decomposizione in componenti irriducibili di $C \subset \mathbb{A}^2(k)$ (k algebricamente chiuso), $C = \mathbf{V}(XY)$.*

(ii) Stessa domanda per $Y \subset \mathbb{A}^2(k), Y = \mathbf{V}(I)$ dove $I = (X(X-1), Y(X-1), Y(Y-1), X(Y-1))$ (osservare che $I = J.J'$ dove $J = (X, Y), J' = (X-1, Y-1)$).

Esercizio 3.7: *Sia $X \subset k^n$ un insieme algebrico.*

Mostrare: $\dim_k A(X) < \infty \Leftrightarrow X$ *è un insieme finito. Inoltre se* X *è finito* $\#(X) = \dim_k A(X)$.

(hint: Se $\dim_k A(X)$ *è finita,* $1, x_i, x_i^2, ..., x_i^s, ..$ *sono linearmente dipendenti (*x_i *è la classe di* X_i *mod* $\mathbf{I}(X)$*). Viceversa se* $X = \{p_1, ..., p_r\}$*, prendere dei polinomi* $P_i, 1 \leq i \leq r$*, tali che* $P_i(p_j) = \delta_{ij}$ *(cfr. Esercizio 2.5), e mostrare che* $\left\{\overline{P_i}\right\}$ *è una base di* $A(X)$*).*

4. Morfismi ed applicazioni razionali

Come già osservato (topologia di Zariski) vogliamo senz'altro che le funzioni polinomiali $k^n \to k$ siano dei morfismi, sembra quindi naturale dire che $f : Z \to \mathbb{A}^m$ è un morfismo se $f = (f_1, ..., f_m)$ dove $f_i : Z \to k$ è (la restrizione di) un'applicazione polinomiale.

Questo naturalmente è corretto ma non è un buon punto di vista. Infatti se f è una funzione $\mathcal{C}^k$ su una varietà X e se $f(x) \neq 0$, allora $1/f$ è ancora una funzione $\mathcal{C}^k$ in un intorno di x. Questo fatto è molto importante perchè permette di mostrare che l'anello dei germi in x di funzioni $\mathcal{C}^k$ è un anello locale (cf Esercizio 4.4). Adesso se P è un polinomio e se $P(x) \neq 0$, allora $1/P$ non è una funzione polinomiale in un intorno di x (invece è una funzione razionale definita in un intorno di x). Vediamo quindi che abbiamo bisogno di una definizione locale che faccia intervenire le funzioni razionali. Le funzioni razionali hanno però vari inconvenienti: non sono delle vere funzioni (non sono definite dappertutto) e non hanno un'espressione unica. Questo complica la trattazione dei morfismi in geometria algebrica e giustifica l'uso dei sistemi lineari (che vedremo più avanti). L'uso delle funzioni razionali permette di definire la nozione di equivalenza birazionale, nozione propria alla geometria algebrica, che non ha equivalenti, per esempio, in geometria differenziale.

4.1. Funzioni regolari e morfismi.

Definizione 4.1: *Sia $Z \subset \mathbb{A}^n$ un insieme algebrico. Una funzione regolare $f : Z \to k$ è un'applicazione polinomiale; cioè esiste un polinomio $P \in k[X_1, ..., X_n]$ tale che $f(x) = P(x), \forall x \in Z$.*

Osservazione 4.2: *Sia $\mathcal{O}(Z)$ l'insieme delle funzioni regolari su Z. Abbiamo $\mathcal{O}(Z) \simeq A(Z)$ perchè due polinomi, P, Q definiscono la stessa funzione regolare su Z se e solo se $P - Q \in \mathbf{I}(Z)$.*
Ovviamente una funzione regolare è continua per la topologia di Zariski.

Adesso che abbiamo definito la nozione di funzione regolare, possiamo passare a quella di morfismo:

Definizione 4.3: *Siano $X \subset \mathbb{A}^n$, $Y \subset \mathbb{A}^m$ due insiemi algebrici. Un'applicazione $f : X \to Y$ è un morfismo se $f = (f_1, ..., f_m)$ dove le f_i sono delle funzioni regolari.*

Osservazione 4.4: *Un morfismo è un'applicazione continua. Una funzione regolare è un morfismo.*
La composizione di due morfismi (quando definita) è un morfismo.

Definizione 4.5: *Siano X, Y degli insiemi algebrici. Un morfismo $f : X \to Y$ è un isomorfismo se esiste un morfismo $g : Y \to X$ tale che: $f \circ g = 1_Y$, $g \circ f = 1_X$.*

Attenzione! Un morfismo biiettivo non è necessariamente un isomorfismo! (Cf Esercizio 4.7.)

Osservazione 4.6: *Sia $f : X \to Y$ un morfismo tra insiemi algebrici. Se $\phi : Y \to k$ è una funzione regolare, allora $\phi \circ f : X \to k$ è una funzione regolare su X. Questo definisce un'applicazione: $f^* : A(Y) \to A(X)$. Si verifica (cf Esercizio 4.1) che f^* è un morfismo di k-algebre e che f è un isomorfismo se e solo se anche f^* lo è.*

In particolare, e questo può anche sembrare sorprendente, la k-algebra $A(Z)$ non dipende dall'immersione $i : Z \hookrightarrow \mathbb{A}^n$ (se $j : Z \hookrightarrow \mathbb{A}^m$ è un'altra immersione, $A(i(Z)) \simeq A(j(Z))$).

Si ricorda (Esercizio 2.4) che la k-algebra di un insieme algebrico è ridotta (cioè non contiene elementi nilpotenti).

Viceversa ogni k-algebra, ridotta e finitamente generata è la k-algebra di un insieme algebrico. Infatti sia $A = k[x_1, ..., x_n]$ una tale k-algebra. Allora $A \simeq k[X_1, ..., X_n]/I$ ($x_i = X_i$ (mod I)). Sia $Z = \mathbf{V}(I)$, per concludere che $A \simeq A(Z)$, basta mostrare che I è radicale (questo implica $I = \mathbf{I}(Z)$). Sia $f \in r(I)$, allora $f^m \in I$ per qualche m. Prendendo l'immagine in A: $\overline{f}^m = 0$. Siccome A non ha elementi nilpotenti, $\overline{f} = 0$, cioè $f \in I$ e I è radicale.

Abbiamo quindi una corrispondenza perfetta (in realtà un'equivalenza di categorie) tra:

- *le k-algebre ridotte di tipo finito*
- *i k-insiemi algebrici affini.*

4.2. Funzioni razionali. D'ora in poi considereremo solo varietà affini, cioè insiemi algebrici irriducibili.

Se $Z \subset \mathbb{A}^n$ è una varietà affine, allora $A(Z)$ è un anello integro e possiamo quindi considerare il suo campo dei quozienti, che denoteremo con $K(Z)$. Vediamo che:

$$K(Z) = \{\frac{P}{Q} |\ P, Q \in \mathbf{S}, Q \notin \mathbf{I}(Z) \text{ e dove } \frac{P}{Q} = \frac{R}{T} \text{ se } PT - QR \in \mathbf{I}(Z)\}$$

Definizione 4.7: *Una funzione razionale su Z è un elemento di $K(Z)$.*

Modulo tutte le identificazioni necessarie, una funzione razionale su Z è la restrizione a Z di una funzione razionale su $\mathbb{A}^n$.

Osservazione 4.8: Attenzione! *Sia $Z = \mathbf{V}(x^2 + y^2 - 1) \subset \mathbb{A}^2$ e consideriamo le funzioni razionali $f = \frac{1-y}{x}$, $g = \frac{x}{1+y}$. Siccome $(1-y)(1+y)-x^2 = 1-y^2-x^2 \in \mathbf{I}(Z)$, f e g rappresentano la stessa funzione razionale su Z. Osservare che f non è definita nel punto $(0, 1)$ mentre g, invece, è definita in quel punto.*

Definizione 4.9: *Una funzione razionale, f, è definita (si dice anche* regolare*) nel punto $x \in Z$ se può essere scritta nella forma $f = \frac{P}{Q}$ con $Q(x) \neq 0$.*

L'insieme dei punti in cui una funzione razionale, f, è definita è un aperto non vuoto. Che sia non vuoto risulta immediatamente dal fatto che presa una rappresentazione qualsiasi $f = \frac{P}{Q}$, siccome $Q \notin \mathbf{I}(Z)$, esiste $x \in Z$ con $Q(x) \neq 0$. Adesso siano $f = \frac{P_i}{Q_i}, i \in I$ tutte le rappresentazioni di f. La funzione $f = \frac{P_i}{Q_i}$ è definita su l'aperto $U_i = Z \setminus \mathbf{V}(Q_i)$; quindi f è definita sull'aperto $U = \cup_{i \in I} U_i$ (l'aperto U è il *dominio di definizione* di f).

Una funzione razionale $f \in K(Z)$ definisce un'applicazione da un aperto non vuoto di Z (il suo dominio di definizione) in k, è uso indicare questa applicazione nel modo seguente: $f : Z - - > k$ (il dominio viene sottinteso e la freccia spezzata indica che f non è necessariamente definita su tutto Z).

Finalmente osserviamo che una funzione razionale è completamente determinata da una sua rappresentazione, in altre parole se due funzioni razionali coincidono su un aperto, allora sono uguali. Basta vedere che se $f = \frac{P}{Q}$ si annulla sull'aperto U allora f è la funzione nulla. Infatti, se V è l'aperto $Z \setminus \mathbf{V}(Q)$, allora $W = U \cap V$ è un aperto non vuoto di Z (perchè Z è irriducibile) e P è identicamente nullo su W, quindi (cf Proposizione 3.15) $P = 0$ e $f = 0$ in $K(Z)$.
Si può anche ragionare così: siccome $K(Z)$ è un campo, per mostrare che $f = 0$ basta mostrare che non è invertibile. Se $fg = 1$, allora si ottiene una contraddizione guardando all'aperto (non vuoto) $V = U \cap U_f \cap U_g$ (U_f, risp. U_g, è il dominio di definizione di f, risp. g).

Proposizione 4.10: *Una funzione razionale $f \in K(Z)$ definita in ogni punto della varietà affine Z è una funzione regolare.*

Dimostrazione. Per ipotesi, per ogni $x \in Z$, $\exists Q_x$, con $Q_x(x) \neq 0$ tale che $f = \frac{P_x}{Q_x}$. Sia I l'ideale generato dai Q_x; I è finitamente generato e possiamo assumere $I = (Q_{x_1}, ..., Q_{x_m})$. Chiaramente $\mathbf{V}(I) \cap Z = \emptyset$. Abbiamo $\mathbf{V}(I) \cap \mathbf{V}(\mathbf{I}(Z)) = \mathbf{V}(I + \mathbf{I}(Z)) = \emptyset$, segue che $1 \in I + \mathbf{I}(Z)$. Quindi $1 = \sum_1^m H_i Q_{x_i} \pmod{\mathbf{I}(Z)}$. Moltiplicando per f: $f = \sum_1^m H_i Q_{x_i} f = \sum_1^m H_i Q_{x_i} (\frac{P_{x_i}}{Q_{x_i}}) \pmod{\mathbf{I}(Z)}$, finalmente $f = \sum_1^m H_i P_{x_i} \pmod{\mathbf{I}(Z)}$ è una funzione regolare (polinomiale) su Z. □

4.3. Funzioni regolari e morfismi (take two). Le definizioni di funzione regolare e morfismo date nella Sezione 4.1 non sono ottimali perchè sono definizioni *globali* mentre è preferibile avere delle definizioni *locali*. Inoltre, contrariamente a quanto avviene in topologia o geometria differenziale, se $f : X \to k$ è una funzione regolare con $f(x) \neq 0$, allora, con la Definizione 4.3, $1/f$ non è un morfismo in un intorno di x ($1/f$ non è una funzione polinomiale, ma una funzione razionale), questo è una catastrofe! (i germi di morfismi in x non formano più un anello

locale!). Per rimediare basta dare una definizione locale che tenga in considerazione le funzioni razionali.

Definizione 4.11: *Sia $Y \subset \mathbb{A}^n$ una varietà affine o quasi-affine. Un'applicazione $f : Y \to k$ è regolare in $y \in Y$ se esiste un aperto U_y di Y contenente y e dei polinomi P_y, Q_y con $Q_y(x) \neq 0, \forall x \in U_y$, tali che $f = \frac{P_y}{Q_y}$ su U_y. L'applicazione f è regolare se è regolare in ogni punto di Y. Si nota $\mathcal{O}(Y)$ l'anello delle funzioni regolari su Y.*

Proposizione 4.12: *Sia $Y \subset k^n$ una varietà quasi-affine.*

(i) Se $f \in \mathcal{O}(Y)$, f è continua per la topologia di Zariski.

(ii) Sianof, $g \in \mathcal{O}(Y)$, se f e g coincidono su un aperto non vuoto di Y allora coincidono su tutto Y.

(iii) $\mathcal{O}(Y)$ è un anello integro.

La dimostrazione del punto (i) usa il seguente:

Lemma 4.13: *Sia X uno spazio topologico. Un sottinsieme Z di X è chiuso in X se e solo se esiste un ricoprimento aperto di X, $X = \bigcup_{i \in I} U_i$, tale che $Z \cap U_i$ sia chiuso in U_i per ogni i.*

Dimostrazione. ($\Longrightarrow$) è chiaro (prendere il ricoprimento banale).

($\Longleftarrow$) Mostriamo che $X \backslash Z$ è aperto: $(X \backslash Z) \cap U_i = U_i \backslash (Z \cap U_i)$ è aperto in U_i, quindi in X (perchè U_i è aperto). Se $x \in X \backslash Z$, esiste j tale che $x \in U_j$, e $(X \backslash Z) \cap U_j$ è un intorno aperto (in X) di x contenuto in $X \backslash Z$; quindi $X \backslash Z$ è aperto □

Dimostrazione della Proposizione 4.12. (i) Per provare che f è continua, basta mostrare che la contr'immagine di un chiuso è un chiuso. Siccome i chiusi non banali di $\mathbb{A}^1$ sono unioni finite di punti, basta mostrare che la contr'immagine di un punto a di $\mathbb{A}^1$ è un chiuso di Y. Per definizione, per ogni y in Y esiste un aperto U_y e una funzione razionale definita su U_y, P/Q, tale che $f = P/Q$ su U_y. Gli U_y formano un ricoprimento aperto di Y, e per il lemma precedente basta mostrare che $f^{-1}(a) \cap U_y$ è chiuso in U_y per ogni y. Abbiamo $f^{-1}(a) \cap U_y = \{x \in U_y / P(x)/Q(x) = a\} = \{x \in U_y / P(x) - aQ(x) = 0\} = \mathbf{V}(R) \cap U_y$ dove $R = P - aQ$, quindi $f^{-1}(a) \cap U_y$ è chiuso in U_y.

(ii) Sia $Z = \{x \in Y / f(x) = g(x)\}$. Allora Z è chiuso in Y perchè $Z = (f - g)^{-1}(0)$. Se Z contiene un aperto non vuoto U allora $\overline{U} \subset Z$. Ma $\overline{U} = Y$ perchè Y è uno spazio topologico irriducibile (cf Esercizio 3.3) e quindi $Z = Y$.

(iii) Sia $f \in \mathcal{O}(Y), f \neq 0$. Osserviamo che $D(f) := \{x \in Y / f(x) \neq 0\}$ è un aperto non vuoto di Y (perchè $f^{-1}(0)$ è chiuso per (i)). Se $f \neq 0$ e $g \neq 0$, gli aperti $D(f)$ e $D(g)$ hanno un'intersezione non vuota (perchè Y è irriducibile), quindi $fg \neq 0$. □

Lemma 4.14: *Se Y è una varietà affine, $\mathcal{O}(Y) \simeq A(Y)$ (cioè ogni funzione regolare secondo la Definizione 4.11 è polinomiale).*

DIMOSTRAZIONE. E' chiaro che una funzione polinomiale è regolare. Viceversa se f è regolare, allora tenuto conto che una funzione regolare è completamente determinata dai suoi valori su un aperto, la conclusione segue dalla Proposizione 4.10. □

Sia $P \in \mathbf{S} = k[X_1, ..., X_n]$, $U = \mathbb{A}^n \setminus \mathbf{V}(P)$ è una varietà quasi affine. Per ogni $Q \in \mathbf{S}$, $\frac{Q}{P}$ è una funzione regolare su U.

Arriviamo adesso alla nozione giusta di morfismo:

Definizione 4.15: *Siano X, Y delle varietà quasi-affini. Un'applicazione $\phi : X \to Y$ è un morfismo se:*

- *ϕ è continua*
- *Per ogni aperto $U \subset Y$ ed ogni funzione regolare $f : U \to k$, $f \circ \phi : \phi^{-1}(U) \to k$ è una funzione regolare.*

Naturalmente una funzione regolare è un morfismo, la composizione di due morfismi è un morfismo ed abbiamo la nozione di isomorfismo esattamente come nella Definizione 4.5. Inoltre se X è una varietà affine, un morfismo $f : X \to \mathbb{A}^m$ è dato da funzioni polinomiali. Infatti se y_i indica la funzione i-esima coordinata, y_i è regolare e quindi anche $f_i = f \circ y_i$ lo è, si conclude con il Lemma 4.14.
Finalmente, possiamo estendere la definizione ad un insieme algebrico qualsiasi: $f : X \to \mathbb{A}^m$ è un morfismo se e solo se per ogni componente irriducibile, X_i di X, $f|X_i$ è un morfismo.

4.4. Applicazioni razionali.

Definizione 4.16: *Sia Z una varietà affine. Un'applicazione razionale $f : Z - - > \mathbb{A}^m$ è data da m funzioni razionali, f_i: $f = (f_1, ..., f_m)$. L'applicazione f è definita (si dice anche* regolare*) in x se tutte le f_i lo sono, quindi il dominio di definizione di f è: $U = \cap U_i$ dove U_i è il dominio di definizione di f_i. L'immagine di f è: $f(Z) = \{f(x) |\ x \in Z$ e f è definita in $x\}$.*

Un'applicazione razionale dalla varietà affine Z nell'insieme algebrico $Y \subset \mathbb{A}^m$ è un'applicazione razionale $f : Z - - > \mathbb{A}^m$ tale che $f(Z) \subset Y$.

Si osserverà che, con le notazioni precedenti, $f : U \to \mathbb{A}^m$ è un morfismo.

Proposizione 4.17: *Sia Z una varietà affine, $f = (f_1, ..., f_m) : Z - - > \mathbb{A}^m$ un'applicazione razionale e $Y \subset \mathbb{A}^m$ un insieme algebrico. Si ha $f(Z) \subset Y$ se e solo se $\forall P \in \mathbf{I}(Y)$, $P(f_1, ..., f_m) = 0$ in $K(Z)$.*

DIMOSTRAZIONE. Se $f(Z) \subset Y$, per ogni $P \in \mathbf{I}(Y)$, $P \circ f$ è una funzione razionale su Z che si annulla su un aperto non vuoto, quindi (cf la discussione dopo

la Definizione 4.9) $P \circ f = 0$ in $K(Z)$.
Viceversa supponiamo $P \circ f = 0$ in $K(Z)$, $\forall P \in \mathbf{I}(Y)$. Se $x \in Z$ e se f è definita in x allora $P(f(x)) = 0$, $\forall P \in \mathbf{I}(Y)$. Quindi $f(x) \in Y$. □

Se $f : X - - > Y$ e $g : Y - - > Z$ sono due applicazioni razionali tra varietà affini, non è sempre possibile comporle (la composta è definitra se $f^{-1}(V) \neq \emptyset$ dove V è il dominio di definizione di g). Per superare questo inconveniente si introduce la nozione di applicazione dominante.

4.5. Applicazioni razionali dominanti.

Definizione 4.18: *Sia Z una varietà affine. Un'applicazione razionale $f : Z - - > Y$ (Y insieme algebrico) è dominante se $f(Z)$ è denso in Y.*

Osservazione 4.19: *Siccome un'applicazione razionale è continua laddove è definita (perchè è un morfismo laddove è definita), $f(Z)$ è irriducibile e quindi $Y = \overline{f(Z)}$ è irriducibile (cioè anche Y è una varietà affine). Questo accorgimento è uno strumento molto utile nella pratica per dimostrare che un insieme algebrico è irriducibile.*
Siccome un morfismo è in particolare un'applicazione razionale, si ha anche la nozione di morfismo dominante. Un morfismo dominante è un morfismo "quasi" suriettivo. Esistono però dei morfismi dominanti che non sono suriettivi. Per esempio sia $Z = \mathbf{V}(xy - 1) \subset \mathbb{A}^2$ e sia $p : Z \to k$ la proiezione sull'asse delle x, p è dominante ma non suriettivo (l'immagine è $k \setminus \{0\}$).
Se $f : X - - > Y$ e $g : Y - - > Z$ sono due applicazioni razionali dominanti, allora la composta $g \circ f : X - - > Z$ esiste sempre.

Si ricorda che se k è un sottocampo sia di K che di K' una k-estensione $j : K \hookrightarrow K'$, è un morfismo non nullo di campi (quindi iniettivo) tale che $j|k = Id$.

Proposizione 4.20: *Siano X, Y due varietà affini.*
(i) Un'applicazione razionale dominante $f : X - - > Y$ induce una k-estensione: $f^* : K(Y) \hookrightarrow K(X)$.
(ii) Più generalmente esiste una biiezione naturale tra l'insieme delle applicazioni razionali da X in Y e l'insieme delle k-estensioni di campi $K(Y) \hookrightarrow K(X)$.

Dimostrazione. (i) Sia $\phi : Y \to k$ una funzione regolare, allora $f^*(\phi) := f \circ \phi$ è una funzione razionale su X. Se $f \circ \phi = 0$ allora $\mathbf{V}(\phi)$ contiene $f(X)$, siccome $f(X)$ è denso ϕ è identicamente nulla. Questo dimostra che il morfismo d'anelli: $A(Y) \to K(X) : \phi \to f^*(\phi)$ è iniettivo. Questo morfismo si estende al campo dei quozienti di $A(Y)$ e fornisce un morfismo iniettivo di campi: $f^* : K(Y) \hookrightarrow K(X)$.

(ii) Viceversa sia $j : K(Y) \hookrightarrow K(X)$ una k-estensione. Consideriamo Y immersa in $\mathbb{A}^n$. Abbiamo $A(Y) \simeq k[t_1, ..., t_n]$ (t_i = classe di T_i mod $\mathbf{I}(Y)$); possiamo

assumere $t_i \neq 0$ (perchè?). Siccome $A(Y) \subset K(Y)$, gli elementi $j(t_i) = f_i$ sono elementi non nulli di $K(X)$ e definiscono un'applicazione razionale $f : X - - > \mathbb{A}^n : x \to (f_1(x), ..., f_n(x))$. L'immagine di f è contenuta in Y. Per questo basta mostrare che per ogni $P \in \mathbf{I}(Y)$, $P \circ f = 0$ in $K(X)$ (Proposizione 4.17). Ma questo è chiaro perchè essendo $\overline{P} = 0$ ($\overline{P}$ è l'immagine di P in $A(Y)$), $j(\overline{P}) = P \circ f = 0$. Adesso f è dominante perchè altrimenti $\overline{f(X)}$ sarebbe un chiuso proprio di Y: $\mathbf{V}(I) \cap Y$ e un elemento di I fornisce una funzione regolare ϕ con $f^*(\phi) = 0$: assurdo. Si lascia al lettore il compito di verificare che i due procedimenti sono inversi l'uno dell'altro. □

In realtà si può dimostrare di più: esiste un'equivalenza di categoria tra le estensioni di k di tipo finito e le applicazioni razionali dominanti tra varietà affini. Per questo bisogna mostrare che $K(Y)$ è un'estensione finita di k e che ogni estensione finita di k può essere realizzata come il campo delle funzioni razionali di una qualche varietà affine.

Per concludere introduciamo una nozione peculiare alla geometria algebrica: l'equivalenza birazionale.

Definizione 4.21: *Un'applicazione birazionale $\varphi : X - - > Y$, tra due varietà affini, è un'applicazione razionale che ammette un'applicazione razionale inversa; cioè esiste un'applicazione razionale dominante $\psi : Y - - > X$ tale che $\varphi \circ \psi = Id_Y$, $\psi \circ \varphi = Id_X$ (quando definite). In queste condizioni si dice che X e Y sono birazionalmente equivalenti.*

Proposizione 4.22: *Siano X, Y delle varietà affini. Sono equivalenti:*

(i) X e Y sono birazionalmente equivalenti,

(ii) Esistono degli aperti non vuoti $U \subset X$, $V \subset Y$ tali che U e V siano isomorfi,

(iii) $K(X)$ è isomorfo a $K(Y)$ come k-algebra.

Dimostrazione. (i) $\Longrightarrow$ (ii) Se φ (risp. ψ) è definita su U' (risp. V'), allora $\psi \circ \varphi$ è definita su $\varphi^{-1}(V')$, e $\varphi \circ \psi$ su $\psi^{-1}(U')$. Si verifica che gli aperti $U = \varphi^{-1}(\psi^{-1}(U'))$, $V = \psi^{-1}(\varphi^{-1}(V'))$ sono isomorfi.

(ii) $\Longrightarrow$ (iii) (Per la definizione di $K(U)$ vedere l'Esercizio 4.6.) Segue dal fatto che $K(X) \simeq K(U)$ (idem per Y e V).

(iii) $\Longrightarrow$ (i) Segue dalla Proposizione 4.20. □

Definizione 4.23: *Una varietà, X, si dice razionale se è birazionalmente equivalente a uno spazio affine $\mathbb{A}^n$.*

Osservazione 4.24: *Due varietà birazionalmente equivalenti non sono necessariamente isomorfe. Per esempio la cuspide razionale è birazionale, ma non isomorfa, a $\mathbb{A}^1$ (cfr. Esercizio 4.7).*

La geometria birazionale, cioè lo studio delle varietà algebriche modulo equivalenza birazionale, è propria alla geometria algebrica (non ha equivalenti in topologia, geometria differenziale).

Esercizi.

Esercizio 4.1: *Dimostrare che un morfismo $f : X \to Y$ di $k-$insiemi algebrici è un isomorfismo se e solo se il (co)-morfismo $f^* : A(Y) \to A(X)$ è un isomorfismo.*

In particolare due insiemi algebrici affini sono isomorfi se e solo se $A(X) \simeq A(Y)$ come $k-$algebre. Quindi l'algebra affine $A(X)$ è un invariante intrinseco di X (non dipende dall'immersione di X in uno spazio affine, cosa a priori non evidente).

Esercizio 4.2: *Sia p un punto di $\mathbb{A}^1$. Mostrare che $\mathbb{A}^1$ non è isomorfo a $\mathbb{A}^1 \setminus \{p\}$.*

Esercizio 4.3: *Un anello A con un unico ideale massimale $\mathfrak{m}$ è chiamato anello locale, il campo quoziente $k = A/\mathfrak{m}$ è chiamato il campo residuo di A.*

(i) Sia A un anello e $\mathfrak{m} \neq (1)$ un ideale tale che ogni elemento di $A \setminus \mathfrak{m}$ sia invertibile in A. Mostrare che A è locale d'ideale massimale $\mathfrak{m}$.

(ii) Sia A un anello e $\mathfrak{m}$ un ideale massimale tale che ogni elemento di $1 + \mathfrak{m} = \{1 + x / x \in \mathfrak{m}\}$ sia invertibile. Dimostrare che A è locale (usare (i)).

Esercizio 4.4: *Sia G l'insieme delle coppie (U, f) dove $U \subset \mathbb{R}^n$ è un aperto (per la topologia usuale) contenente l'origine $O = (0, \ldots, 0)$ e dove $f : U \to \mathbb{R}$ è di classe $\mathcal{C}^k$. Su G si introduce la relazione: $(U, f) \sim (V, g) \iff$ esiste un aperto non vuoto, W, $O \in W \subset V \cap U$ tale $f|W = g|W$.*

(i) Dimostrare che $\sim$ è una relazione d'equivalenza. Si noterà $< U, f >$ (o anche f_O) la classe di (U, f); $< U, f >$ è un germe di funzione $\mathcal{C}^k$ nell'origine.

(ii) Sia $\mathcal{C}^k_O$ l'insieme quoziente $G/\sim$. Definire una struttura naturale di anello su $\mathcal{C}^k_O$.

(iii) Il valore del germe $< U, f >$ nell'origine è il numero reale $f(O)$. Dimostrare che questo valore è ben definito e che $v : \mathcal{C}^k_O \to \mathbb{R} :< U, f > \to f(O)$ è un morfismo di anelli. Dedurne che $\mathcal{C}^k_O$ è un anello locale (hint: indovinare l'ideale massimale e usare Esercizio 4.3).

(iv) Sia $Y \subset \mathbb{A}^n$ una varietà affine e $x \in Y$ un punto di Y. Ripetere i punti (i), (ii), (iii) prendendo per G l'insieme delle coppie (U, f) dove U è un aperto contenente x e dove $f : U \to k$ è una funzione regolare. L'insieme dei germi di funzioni regolari in x si nota $\mathcal{O}_{Y,x}$. Verificare che $\mathcal{O}_{Y,x}$ è un anello locale.

Esercizio 4.5: *Sia A un anello commutativo. Un sottinsieme S di A è una parte moltiplicativa se $1 \in S$ e se S è chiuso rispetto alla moltiplicazione (se $s, t \in S$ allora $st \in S$).*
(i) Sia S una parte moltiplicativa di A. Su $A \times S$ si definisce la relazione: $(a, s) \sim (b, t) \Leftrightarrow \exists v \in S$ tale che: $(at - bs)v = 0$. Mostrare che $\sim$ è una relazione di equivalenza. Si nota $S^{-1}A$ l'insieme quoziente e si nota $\frac{a}{s}$ la classe di (a, s).
(ii) Si pone $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$, $\frac{a}{s} . \frac{b}{t} = \frac{ab}{st}$. Mostrare che queste operazioni sono ben

definite e che definiscono una struttura d'anello su $S^{-1}A$ ($S^{-1}A$ è il localizzato di A rispetto ad S). Mostrare che $A \to S^{-1}A : a \to \frac{a}{1}$ è un morfismo d'anelli (attenzione: questo morfismo può non essere iniettivo).
(iii) Se A è integro e $S = A \setminus \{0\}$, $S^{-1}A$ è il campo dei quozienti di A.
(iv) Sia A qualsiasi (non necessariamente integro). Se $f \in A$, allora $S = \{f^n\}$ è una parte moltiplicativa. In questo caso $S^{-1}A$ si nota A_f. Se $\mathfrak{p} \subset A$ è un ideale primo, allora $S = A \setminus \mathfrak{p}$ è una parte moltiplicativa. In questo caso si nota $S^{-1}A = A_{\mathfrak{p}}$. Mostrare che $A_{\mathfrak{p}}$ è un anello locale (indovinare l'ideale massimale ed usare l'Esercizio 4.3).
(v) Sia $Y \subset \mathbb{A}^n$ una varietà affine e sia $x \in A$. Mostrare che $\mathcal{O}_{Y,x} \simeq A(Y)_{\mathfrak{m}}$ dove $\mathfrak{m} \subset A(Y)$ è l'ideale massimale corrispondente al punto x.

Esercizio 4.6: *(i) Sia $Y \subset \mathbb{A}^n$ una varietà affine e sia $U \subset Y$ un aperto non vuoto. Si considera l'insieme delle coppie $G_U = \{(V, g)/V$ è un aperto di U, g è regolare su $V\}$. Su G_U si definisce la relazione: $(V, g) \sim (W, f)$ se esiste un aperto non vuoto $T \subset V \cap W$ tale che $g|T = f|T$. Mostrare che $\sim$ è una relazione d'equivalenza. Si nota $K(U)$ l'insieme quoziente.*
(ii) Mostrare che $K(U)$ è un campo isomorfo a $K(Y)$ e che $K(U)$ è isomorfo al campo dei quozienti di $\mathcal{O}(U)$. (N.B. Prendendo $U = Y$ si ha una definizione alternativa di $K(Y)$.)

Esercizio 4.7: *("La cubica cuspidale") Sia $C = \mathbf{V}(Y^2 - X^3) \subset \mathbb{A}^2$.*

(i) Sia $\varphi : \mathbb{A}^1 \to C : t \to (t^2, t^3)$. Mostrare che φ è un morfismo biiettivo e bicontinuo.

(ii) Mostrare che C è irriducibile.

(iii) Mostrare che φ^* (e quindi φ) non è un isomorfismo (cfr. Esercizio 4.1).

(iv) Rappresentare graficamente la curva C ($k = \mathbb{R}$) e, guardando il grafico, spiegare (iii) (e il titolo dell'esercizio).

Esercizio 4.8: *Sia $C \subset \mathbb{A}^2$ la circonferenza di equazione $x^2 + y^2 = 1$. Mostrare che C è razionale (proiettare C dal punto $(0, 1)$ sull'asse degli x).*
È C isomorfa a $\mathbb{A}^1$?

Esercizio 4.9: *Sia $C \subset \mathbb{A}^2$ la curva piana di equazione $y^2 = x^2 + x^3$ ("cubica nodale").*

(i) Disegnare il grafico (reale) di C.

(ii) Mostrare che C è irriducibile.

(iii) Determinare l'intersezione di C con una retta passante per l'origine.

(iv) Mostrare che C è razionale (usare (ii) e parametrizzare C con il fascio di rette per l'origine).

(v) E' C isomorfa a $\mathbb{A}^1$?

Esercizio 4.10: *Sia* $S = \mathbf{V}(x^3 + y^3 + z^3 - 1) \subset \mathbb{A}^3$. *Si assumerà* $ch(k) \neq 3$.
(i) Mostrare che S *contiene due rette sghembe.*
(ii) Mostrare che S *è razionale.*

5. Dimensione.

Intuitivamente la dimensione di una figura geometrica è il numero di gradi di libertà di un punto della figura. In altri termini se Y è una sottovarietà irriducible propria di X, allora deve essere $dimY < dimX$ (come per gli spazi vettoriali). La topologia di Zariski è particolarmente adatta per formalizzare questa osservazione.

Definizione 5.1: *Sia X uno spazio topologico. La dimensione di X è:*

$\dim X := \sup\{n \in \mathbb{N}/$*esiste una catena $Z_0 \subset Z_1 \subset ... \subset Z_n$ di sottoinsiemi distinti di X chiusi e irriducibili $\}$; si ricorda che l'insieme vuoto non è considerato irriducibile.*

Osservazione 5.2: *Questa definizione presenta qualche interesse solo per topologie tipo la topologia di Zariski: con questa definizione ogni spazio topologico di Hausdorff ha dimensione zero (cfr. Esercizi).*

Definizione 5.3: *La dimensione di un insieme algebrico, $Y \subset \mathbb{A}^n$, è la sua dimensione come spazio topologico (Y munito della topologia indotta dalla topologia di Zariski su $\mathbb{A}^n$).*

Esempio 5.4: (i) Se $X = \{x\}$ è ridotto ad un punto allora $\dim X = 0$.

(ii) La dimensione di $\mathbb{A}^1$ è uno. Infatti gli unici chiusi irriducibili di $\mathbb{A}^1$ sono $\mathbb{A}^1$ e i sottoinsiemi costituiti da un solo punto.

(ii) Abbiamo $\dim(\mathbb{A}^n) \geq n$ (prendere una catena di sottospazi lineari), ma siamo già in difficoltà per dimostrare l'uguaglianza. Per questo cerchiamo adesso di tradurre questa nozione topologica in termini algebrici.

Definizione 5.5: *Sia A un anello e $\mathfrak{p} \subset A$ un ideale primo. L'altezza di $\mathfrak{p}$ ("height" in inglese) è: $h(\mathfrak{p}) := \sup\{n \in \mathbb{N}/$ esiste una catena $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset ... \subset \mathfrak{p}_n = \mathfrak{p}$ di ideali primi distinti$\}$. La dimensione (di Krull) dell'anello A è:* $\dim A := \sup\{h(\mathfrak{p})$ */ $\mathfrak{p} \subset A$ è un ideale primo$\}$.*

Proposizione 5.6: *Sia $Y \subset \mathbb{A}^n$ una varietà affine. Allora* $\dim Y = \dim A(Y)$.

Osservazione 5.7: *Nella proposizione precedente,* $\dim Y$ *è la dimensione dello spazio topologico Y mentre* $\dim A(Y)$ *è la dimensione (di Krull) dell'anello $A(Y)$.*

Per dimostrare la Proposizione precedente useremo il seguente:

Lemma 5.8: *Siano R un anello, $I \subset R$ un ideale e $\pi : R \to R/I$ l'applicazione naturale di passaggio al quoziente. Poniamo $\mathcal{J} = \{J \subset R, J$ è un ideale contenente $I\}, \mathcal{J}' = \{J' \subset R/I, J'$è un ideale$\}$, e consideriamo $\mathcal{J}$ e $\mathcal{J}'$ ordinati (dall'inclusione).*

(i) l'applicazione $\varphi : \mathcal{J} \to \mathcal{J}' : J \to \pi(J)$ è una biiezione di insiemi ordinati. L'applicazione $\Phi : \mathcal{J}' \to \mathcal{J} : J' \to \pi^{-1}(J')$ è l'applicazione inversa di φ. Abbiamo quindi una corrispondenza biiunivoca tra l'insieme degli ideali di R/I e l'insieme degli ideali di R contenenti I.

(ii) con le notazioni precedenti, J' è radicale (risp. primo, massimale) se e solo se J lo è.

DIMOSTRAZIONE. Si verifica facilmente che $\pi(J)$ e $\pi^{-1}(J')$ sono degli ideali e che $\varphi \circ \Phi = Id$, $\Phi \circ \varphi = Id$.

Se $I \subset J$ abbiamo un'applicazione naturale (suriettiva) $R/I \to R/J$ il cui nucleo è J/I; da questa inclusione di J/I in R/I vediamo che l'ideale $\pi(J)$ di R/I si identifica con J/I. In particolare $(R/I)/\pi(J) \cong R/J$. Da questo risulta: J primo (risp. massimale) $\iff \pi(J)$ primo (risp. massimale).

Supponiamo J radicale e mostriamo $J' = \pi(J)$ radicale. Sia $\pi(f)^n \in J' = \pi(J)$; abbiamo $\pi(f)^n = \pi(f^n) = \pi(x)$, $x \in J$. Quindi $\pi(f^n - x) = 0$ ossia $f^n - x \in I \subset J$, da cui $f^n \in J$. Siccome J è radicale questo implica $f \in J$, quindi $\pi(f) \in J'$, e J' è radicale. Viceversa supponiamo J' radicale e mostriamo che $J = \pi^{-1}(J')$ è radicale. Sia $x^n \in J$, allora $\pi(x^n) = \pi(x)^n \in J'$. Siccome J' è radicale, questo implica $\pi(x) \in J'$, e quindi $x \in J$. □

Corollario 5.9: *Sia $Y \subset \mathbb{A}^n$ un insieme algebrico. Sia $\mathcal{H} = \{Z/Z \subset Y, Z$ é un insieme algebrico$\}$ e $\mathcal{I} = \{J' \subset A(Y); J'$ è un ideale radicale$\}$. Notiamo*

$\pi : k[X_1, ..., X_n] \to A(Y)$ la proiezione naturale.

(i) l'applicazione $\varphi : \mathcal{H} \to \mathcal{I} : Z \to \pi(\mathbf{I}(Z))$ è biiettiva.

(ii) L'applicazione $\varphi^{-1} : \mathcal{I} \to \mathcal{H}$ è definita da $\varphi^{-1}(J') = \mathbf{V}(\pi^{-1}(J'))$. Inoltre Z è irriducibile (risp. Z è un punto) se e solo se J' è primo (risp. massimale).

Questo corollario stabilisce quindi una corrispondenza biiunivoca tra i sottoinsiemi algebrici di Y e gli ideali radicali di $A(Y)$; le sottovarietà di Y corrispondono agli ideali primi di $A(Y)$ (cioè gli ideali primi di $k[X_1, ..., X_n]$ contenenti $\mathbf{I}(Y)$).

DIMOSTRAZIONE DELLA PROPOSIZIONE 5.6. Segue immediatamente dalle definizioni e dal corollario precedente. □

Se Y è un insieme algebrico qualsiasi (non necessariamente irriducibile) abbiamo:

Lemma 5.10: *Sia $Y \subset \mathbb{A}^n$ un insieme algebrico e $Y = Y_1 \cup ... \cup Y_k$ la sua decomposizione in componenti irriducibili. La dimensione di Y è:* $\dim Y = \max_{1 \le i \le k}\{\dim Y_i\}$.

DIMOSTRAZIONE. È chiaro che $\max\{\dim Y_i\} \le \dim Y$ (cfr. Esercizi). Viceversa supponiamo $\dim Y > n = \max\{\dim Y_i\}$, allora esiste una catena $Z_0 \subset Z_1 \subset ... \subset Z_{n+1}$ di chiusi irriducibili distinti di Y. Abbiamo $Z_{n+1} = \bigcup_i (Y_i \cap Z_{n+1})$, ma

$Y_i \cap Z_{n+1}$ è chiuso e Z_{n+1} è irriducibile, quindi $Z_{n+1} \subset Y_j$ per qualche j, contro l'ipotesi $\dim Y_j \leq n$. □

La traduzione algebrica non migliora molto la situazione e abbiamo ancora difficoltà per calcolare $\dim \mathbb{A}^n$. Il prossimo risultato risolve questo problema:

Teorema 5.11: *Sia A una k-algebra integra di tipo finito. Sia K il campo dei quozienti di A. La dimensione di Krull di A,* $\dim A$*, è uguale al grado di trascendenza di K su k:* $\dim A = tr.degK/k$.

DIMOSTRAZIONE. Un buon testo di algebra. □

Per capire bene questo enunciato facciamo adesso alcuni brevi richiami.

Osservazione 5.12: Estensioni trascendenti: *Sia $k \subset K$ un'estensione di campi. Gli elementi di un sottoinsieme $A \subset K$ sono algebricamente indipendenti su k se per ogni sottoinsieme finito $\{x_1, ..., x_r\} \subset A$, e $\forall P \in k[X_1, ..., X_r] : P(x_1, ..., x_r) = 0 \Longrightarrow P = 0$ (è l'analogo dell'indipendenza lineare negli spazi vettoriali).*

Per esempio se $A = \{x\}$, x è algebricamente indipendente $\Longleftrightarrow$ x è trascendente su k.

Un sottoinsieme $A \subset K$ *genera algebricamente* K su k se l'estensione $k(A) \subset K$ è algebrica . Si ricorda che l'estensione $k(A) \subset K$ è algebrica se ogni elemento di K è radice di un polinomio a coefficienti in $k(A)$.

Finalmente $A \subset K$ è una base di trascendenza di K su k se A genera algebricamente K su k e se gli elementi di A sono algebricamente indipendenti su k.

Si dimostra che esiste sempre una base di trascendenza e che due basi di trascendenza hanno la stessa cardinalità, questa cardinalità è il grado di trascendenza di K su k, lo si nota $tr.degK/k$.

Esempio 5.13: (i) L'esempio standard: sia $K = k(X_1, ..., X_n)$ il campo delle funzioni razionali a coefficienti in k, nelle variabili (indeterminate) $X_1, ..., X_n$. Allora $A = \{X_1, ..., X_n\}$ è una base di trascendenza di K su k e $tr.degK/k = n$.

(ii) Sia $C = \mathbf{V}(F) \subset \mathbb{A}^2$, dove $F(X, Y)$ è un polinomio irriducibile. Notiamo x, y le classi di X, Y mod $(F) = \mathbf{I}(C)$. Abbiamo $A(C) = k[x, y]$ e $K(C) = k(x, y)$. Se F ha grado uno (cioè se $deg_X(F) = deg_Y(F) = 1$) allora C è una retta e $C \simeq \mathbb{A}^1$ ha dimensione uno. Possiamo quindi assumere $deg_X(F) > 1$.

Mostriamo che x è trascendente su k. Infatti, siccome k è algebricamente chiuso, basta fare vedere $x \notin k$. Abbiamo $x \in k \Longleftrightarrow X - \lambda \in (F) \Longleftrightarrow F|X - \lambda$, ma questo è assurdo per ragioni di grado.

Adesso mostriamo che y è algebrico su $k(x)$. Se $F(X,Y) = \Sigma a_{ij}X_iY_j$, abbiamo $\Sigma a_{ij}x_iy_j = 0$ in $A(C)$ e y è radice del polinomio $\Sigma a_{ij}x_iT_j \in k(x)[T]$. Pertanto $k(x,y) = k(x)[y]$ e $\{x\}$ è una base di trascendenza di $K(C)$ su k. Quindi $tr.degK(C)/k = 1$ e $\dim C = 1$ (C è una curva!).

Possiamo riassumere questi esempi nella seguente:

Proposizione 5.14: *(i) Lo spazio affine $\mathbb{A}^n$ ha dimensione n. In particolare la dimensione di un insieme algebrico affine è finita.*

(ii) Sia $C = \mathbf{V}(F) \subset \mathbb{A}^2$ con F polinomio irriducibile, allora $\dim C = 1$.

DIMOSTRAZIONE. (i) Segue dal Teorema 5.11 e dall' Esempio 5.13 (i) in quanto $K(\mathbb{A}^n) = k(X_1, ..., X_n)$.

(ii) Segue dal Teorema 5.11 e dall' Esempio 5.13 (ii) se $\deg_X(F) > 1$, per il caso generale cfr. Esercizi. □

5.1. Ipersuperfici. Impegnandosi un po' in algebra commutativa, si ottiene la generalizzazione naturale del Proposizione 5.14 (ii):

Proposizione 5.15: *Sia $X \subset \mathbb{A}^n$ una varietà affine, allora* $\dim X = n-1 \iff X = \mathbf{V}(f)$ *dove $f \in k[X_1, ..., X_n]$ è un polinomio non costante irriducibile.*

Questo risultato è essenzialmente una traduzione del teorema dell'ideale principale ("Hauptidealsatz") di Krull:

Teorema 5.16: *Sia A un anello noetheriano e $f \in A$ un elemento non invertibile e non divisore dello zero. Allora ogni ideale primo minimale (per l'inclusione) contenente f ha altezza uno.*

DIMOSTRAZIONE. Un buon testo di algebra. □

Useremo anche:

Proposizione 5.17: *(i) Un anello è fattoriale (u.f.d.) se e solo se ogni ideale primo di altezza uno è principale.*

(ii) Sia A una k-algebra integra, di tipo finito e $I \subset A$ un ideale primo. Se $\dim A = n$ *esiste una catena massimale di primi passante per I: $(0) = \mathfrak{p}_0 \subset \mathfrak{p}_1 \subset ... \subset \mathfrak{p}_{n-r} = I \subset ... \subset \mathfrak{p}_n$. In particolare: $h(I) + \dim(A/I) = \dim A$.*

DIMOSTRAZIONE. Un buon testo di algebra. □

Osservazione 5.18: *L'altezza gioca il ruolo di codimensione: se $A = \mathbf{S}, h(I) =$* $\dim \mathbb{A}^n - \dim X =: codimX$, *dove $X = \mathbf{V}(I)$.*

DIMOSTRAZIONE DELLA PROPOSIZIONE 5.15. (i) Se $X = \mathbf{V}(f)$ allora $\mathbf{I}(X) = (f)$ è primo, e (cfr. Teorema 5.16) ha altezza uno, segue (Proposizione 5.17 (ii)) che $\dim X = n - 1$.

(ii) Se $\dim X = n-1$ allora $\mathbf{I}(X)$ è primo di altezza uno. Siccome $\mathbf{S}$ è fattoriale, $\mathbf{I}(X)$ è principale (Proposizione 5.17 (i)) quindi $\mathbf{I}(X) = (f)$ e f è necessariamente irriducibile. □

5.2. Dimensione degli aperti. Sembra intuitivamente chiaro che se U è un aperto non vuoto di una varietà affine X allora $\dim U = \dim X$. Per arrivare a questo risultato ci servono alcuni preliminari (che saranno utili anche nel seguito).

Lemma 5.19: *Sia $f \in k[X_1, ..., X_n]$ un polinomio non costante. L'aperto $D(f)$ di $\mathbb{A}^n$ è isomorfo all'ipersuperficie $Y = \mathbf{V}(X_{n+1}f - 1)$ di $\mathbb{A}^{n+1}$.*

DIMOSTRAZIONE. Consideriamo φ: $Y \to \mathbb{A}^n : (x_1, ..., x_n, x_{n+1}) \to (x_1, ..., x_n)$, è un morfismo la cui immagine è contenuta in $D(f)$. Osserviamo che $1/f \in \mathcal{O}(D(f))$. Pertanto l'applicazione

φ^{-1}: $D(f) \to Y : (a_1, ..., a_n) \to (a_1, ..., a_n, \frac{1}{f(a_1,...,a_n)})$, è un morfismo. □

Osservazione 5.20: *Risulta dalla Proposizione 5.15 che $\dim D(f) = n$.*

Definizione 5.21: *Sia X una varietà quasi-affine, un aperto affine di X è un aperto di X isomorfo a una varietà affine.*

Abbiamo appena visto che, sorprendentemente (cf Esercizio 5.6), gli aperti standard, $D(f)$, di $\mathbb{A}^n$ sono degli aperti affini. In particolare la topologia di $\mathbb{A}^n$ ha una base di aperti affini (cfr. Sezione 3); questo vale per ogni varietà quasi-affine:

Proposizione 5.22: *Sia $X \subset \mathbb{A}^n$ una varietà quasi-affine. La topologia di X ha una base di aperti affini.*

DIMOSTRAZIONE. Considerando semmai la chiusura di X possiamo assumere che X è una varietà affine. Sia $U \subset X$ un aperto non vuoto. Abbiamo $U = V \cap X$ dove V è un aperto di $\mathbb{A}^n$. Siccome gli aperti standard sono una base della topologia, $V = D(f_1) \cup ... \cup D(f_m)$. Quindi: $U = D_X(f_1) \cup ... \cup D_X(f_m)$, dove $D_X(f) = D(f) \cap X$. Basta mostrare che $D_X(f)$ è una varietà affine. Siccome $D_X(f)$ è un aperto non vuoto di X, $D_X(f)$ è irriducibile (cf Esercizio 3.3). Adesso $D_X(f)$ è chiuso in $D(f)$ e se $f : D(f) \to Y$ è l'isomorfismo di $D(f)$ con la varietà affine Y, $f(D_X(f))$ è chiuso in Y e quindi è una varietà affine. □

Osservazione 5.23: *Non tutti gli aperti di una varietà quasi-affine sono affini (cfr. Esercizio 5.5).*

Proposizione 5.24: *Sia U un aperto non vuoto della varietà affine X, allora* $\dim U = \dim X$.

DIMOSTRAZIONE. Dalla Proposizione precedente segue che U contiene un aperto affine: $D_X(f) \subset U \subset X$. Basta mostrare $\dim D_X(f) = \dim X$. Abbiamo$K(D_X(f)) = K(X)$. La dimensione della varietà affine $D_X(f)$ è $tr.degK(D_X(f))/k$ (giustificare!), quindi $\dim X = \dim D_X(f)$. □

Esercizi.

Esercizio 5.1: *Dimostrare che, con la Definizione 5.1, ogni spazio topologico di Hausdorff ha dimensione zero.*

Esercizio 5.2: *Sia X uno spazio topologico e $Y \subset X$ un sottospazio. Mostrare che* $\dim Y \leq \dim X$. *Inoltre se X è irriducibile, di dimensione finita, e se Y è chiuso, $Y \neq X$, allora* $\dim Y < \dim X$. *In particolare se X è una varietà affine e $Y \subset X$ è un sottoinsieme algebrico, allora:* $\dim X = \dim Y \Longrightarrow X = Y$.

Esercizio 5.3: *(i) Due spazi topologici omeomorfi hanno la stessa dimensione.*

(ii) Dimostrare che una varietà affine X ha dimensione zero se e solo se è ridotta a un punto (mostrare che $\mathbf{I}(X)$ è massimale, N.B. $A(X)$ è integro, quindi (0) è un ideale primo).

Esercizio 5.4: *Sia X una varietà affine. Per dimostrare che un aperto non vuoto, $U \subset X$, ha dimensione $dim(X)$, si potrebbe ragionare cosí: abbiamo il campo, $K(U)$, delle funzioni razionali su U e $K(U) \simeq K(X)$ (cf Esercizio 4.6), in particolare $K(U)$ è il campo dei quozienti della k-algebra $\mathcal{O}(U)$. Adesso: $dim(U) = tr.deg(K(U)/k) = tr.deg(K(X)/k) = dim(X)$. Cosa c'è che non va in questo ragionamento?*

Esercizio 5.5: *Si lavora sul campo dei numeri complessi ($k = \mathbb{C}$). Una varietà algebrica, X, è in particolare una varietà analitica, X_{an}. Si ammetterà il fatto seguente: se X e Y sono isomorfe allora X_{an} e Y_{an} sono isomorfe (cfr. "GAGA", di J.P. Serre).*

(i) Sia $U = \mathbb{A}^2 \setminus \{(0,0)\}$. Mostrare che $\mathcal{O}(U) = k[X,Y]$.

(ii) Dedurre da (i) che U non è un aperto affine di $\mathbb{A}^2$. (hint: altrimenti U sarebbe isomorfo a $\mathbb{A}^2$ (cfr. Esercizio 4.1), quindi (per "GAGA") U sarebbe analiticamente isomorfo a $\mathbb{C}^2$; ma questo è assurdo perché, per la topologia usuale, U non è omeomorfo a $\mathbb{C}^2$ (perché?))

(iii) Adesso, sempre usando (i), mostrare che $\mathbb{A}^2$ e U non sono isomorfi, qualsiasi sia k (algebricamente chiuso, come sempre).

Esercizio 5.6: *Sia $X \subset \mathbb{A}^n$ una varietà affine. Sia $U \neq X$ un aperto affine, U è chiuso in X? (e in $\mathbb{A}^n$?).*

6. Spazio tangente di Zariski.

Sia $f : \mathbb{R} \to \mathbb{R} : x \to \ y = f(x)$ una funzione differenziabile. La derivata $f'(x_0)$ nel punto x_0 dà la pendenza della tangente alla curva C di equazione $y = f(x)$ nel punto $P_0 = (x_0, f(x_0))$. Si ha $f'(x0) = \lim_{x\to x_0} \frac{(f(x_0)-f(x))}{x_0-x}$, cioè $f'(x_0)$ è il limite, quando P tende a P_0, delle pendenze delle rette $[P_0, P]$, $P \in C$, quindi la tangente è il limite delle rette ("corde") $[P_0, P]$ quando P tende a P_0 sulla curva C.

Ripetiamo adesso questo procedimento per una curva algebrica. Sia, per esempio, $C \subset \mathbb{R}^2$ la circonferenza di centro $P = (1, 0)$ e di raggio 1: $C = \{(x, y)/x^2 - 2x + y^2 = 0\}$. Sia R una retta passante per l'origine, di equazione $ax + by = 0$, $(a, b) \neq (0, 0)$. Per calcolare $C \cap R$ possiamo procedere nel modo seguente (se $a \neq 0$): abbiamo $x = -by/a$, dall'equazione di R; inserendo nell'equazione di C ricaviamo: $y[(a^2 + b^2)y + 2ba]/a^2 = 0$. Quindi $C \cap R = \{O, P_R\}$ dove O è l'origine e dove $P_R = (2b^2/(a^2 + b^2), -2ab/(a^2 + b^2))$. Se $b \neq 0$ (cioè se R non è verticale) $O \neq P_R$. Se facciamo tendere, sulla circonferenza, il punto P_R verso O (cioè $b \to 0$), l'equazione della retta R tende a: $x = 0$. Notiamo L la retta di equazione $x = 0$. L'intersezione $C \cap L$ è data da: $x = 0$ e $x^2 - 2x + y^2 = 0$, inserendo la prima equazione nella seconda: $y^2 = 0$, di cui 0 è radice con molteplicità due. Quindi $C \cap L = \{O\}$, ma algebricamente O deve essere contato "con molteplicità due" nell'intersezione, ossia la retta L è tangente a C in O.

Più generalmente se C è una curva piana di equazione $f(x, y) = 0$ e se $P \in C, P = (x_0, y_0)$, una retta R, di equazione $y = ax + b$, passante per P sarà tangente a C in P se la molteplicità d'intersezione di R e C in P sarà ≥ 2, cioè se x_0 è radice con molteplicità > 1 di $j(x) = f(x, ax + b) = 0$. Questa definizione si estende al caso di una varietà affine $Y \subset \mathbb{A}^n$, $P \in Y$. Lo spazio tangente di Zariski a Y in P è il sottospazio affine (passante per P) generato dalle rette tangenti a Y in P.

6.1. Molteplicità d'intersezione di un insieme algebrico affine e di una retta in un punto. Sia $Y \subset \mathbb{A}^n$ un insieme algebrico affine, $a \in Y$ un punto di Y e $R \subset \mathbb{A}^n$ una retta passante per a. Sia q un altro punto di R di modo che $R = \{(1 - t)a + tq/t \in k\}$ $(R = a+ < q - a >)$. Sia $\mathbf{I}(Y) = (P_1, ..., P_m)$. L'intersezione $Y \cap R$ è data dai valori di t soluzioni del sistema:

$P_1((1 - t)a + tq) := p_1(t) = 0$

.....

$P_m((1 - t)a + tq) := p_m(t) = 0$

Osservazione 6.1: *I polinomi $p_i(t)$, $1 \leq i \leq m$, sono tutti identicamente nulli se e solo se R è contenuta in Y, d'ora in poi si assumerà R non contenuto in Y.*

Siccome, per ipotesi, k è algebricamente chiuso ogni $p_i(t)$ si scrive: $p_i(t) = \beta_i \prod_j (t - \alpha_j)^{m_j}$. Il massimo comun divisore (M.C.D.) dei $p_i(t)$ è dato dalle radici comuni, con molteplicità: $p(t) = \beta\Pi(t - \alpha_r)^{m_r}$. Quindi, insiemisticamente, $Y \cap R$

$= \{(1-\alpha_r)a + \alpha_r q\}$. Tra questi punti, per ipotesi, c'è il punto a. Possiamo quindi supporre $\alpha_1 = 0$.

Definizione 6.2: *Con le notazioni precedenti la molteplicità d'intersezione di Y e R nel punto a è: $i(Y, R; a) := m_1$ (cioè la molteplicità della radice $t = 0$ nell'equazione $p(t) = 0$).*

Osservazione 6.3: *(i) Per completezza si pone $i(Y, R; a) = +\infty$ se $R \subset Y$.*

(ii) La definizione di $i(Y, R; a)$ non dipende dalle scelte fatte (parametrizzazione della retta R (i polinomi p_i dipendono dal punto q), scelta dei generatori P_i di $\mathbf{I}(Y)$).

Se $\mathbf{I}(Y) = (Q_1, ..., Q_p)$ allora $Q_i = \Sigma U_j P_j$, e con notazioni naturali, $p(t)|q_i(t), \forall t$. Quindi $q(t)$, il M.C.D. dei Q_i, è un multiplo di $p(t)$. Nello stesso modo: $q(t)|p(t)$, pertanto p e q differiscono per un fattore costante.

Se si prende un altro punto di R: $q' = (1-\lambda)a + \lambda q, (\lambda \neq 0)$, ci si riconduce a considerare $p'(t) = p(\lambda t) = c\lambda^d \Pi(t - \alpha_i/\lambda)^{m_r}$, la molteplicità della radice $t = 0$ in $p\prime(t) = 0$ è sempre m_1.

(iii) <u>Attenzione</u>: È essenziale prendere $\mathbf{I}(Y)$ e non un ideale J tale che $\mathbf{V}(J) = Y$.

Esempio 6.4: Sia Y in $\mathbb{A}^2$ la retta di equazione $x = 0$, quindi $\mathbf{I}(Y) = (x)$. Sia R la retta $y = 0$ e $a = (0, 0)$ l'origine. Abbiamo $i(Y, R; a) = 1$. D'altra parte $Y = \mathbf{V}(J)$ dove $J = (x^n)$, ripetiamo il procedimento con questo ideale J al posto di $\mathbf{I}(Y)$. Abbiamo $R = \{(t, 0)/t \in k\}$, $p(t) = t^n$, e $t = 0$ è radice con molteplicità n di $p(t)$; si avrebbe $i(Y, R; a) = n$.

Definizione 6.5: *Sia $Y \subset \mathbb{A}^n$ un insieme algebrico affine e sia $a \in Y$. Una retta R passante per a è tangente a Y in a se $i(Y, R; a) \geq 2$.*

Esempio 6.6: (i) Sia $C \subset \mathbb{A}^2$ la conica di equazione $y = x^2$, $a = (0, 0)$ e R la retta per l'origine e per il punto $q = (\alpha, \beta)$, $q \neq a$. Si ha $R = \{(t\alpha, t\beta)/t \in k\}$, inserendo nell'equazione di C:$p(t) = t(\beta - t\alpha^2)$. Vediamo che $t = 0$ è radice semplice tranne se $b = 0$ cioè se R è la tangente a C in a.

(ii) Più generalmente sia C la curva piana di equazione $y - f(x) = 0$ dove f è un polinomio con $f(0) = 0$. Se R è una retta passante per l'origine O, allora $i(C, R; O) = 1$ tranne se R è la retta di equazione $y = f'(0).x$ (Esercizio).

Esempio 6.7: (iii) Sia $C \subset \mathbb{A}^2$ la cubica cuspidale di equazione $y^2 = x^3$, $a = (0, 0)$ e R la retta per l'origine e per il punto $q = (\alpha, \beta)$, $q \neq a$. Questa volta $p(t) = t^2(\beta^2 - t\alpha^3)$, $t = 0$ è radice doppia se $\beta \neq 0$ e, addiritura, radice tripla se $\beta = 0$! Ogni retta per l'origine è tangente a C nell'origine; questo proviene dal fatto che, come vedremo, l'origine è un punto "singolare" di C.

Definizione 6.8: *Sia $Y \subset \mathbb{A}^n$ un insieme algebrico affine, e sia $a \in Y$. Lo spazio tangente ("immerso") di Zariski a Y nel punto a è: $T_aY = \{y \in \mathbb{A}^n / \text{esiste una retta tangente a } Y \text{ in } a \text{ passante per } y\}$. In altri termini T_aY è l'unione delle rette tangenti a Y in a.*

Osservazione 6.9: *Se X è una varietà quasi-affine e se $a \in X$, allora X è un aperto di una varietà affine X' (la chiusura di X), si pone $T_aX = T_aX'$.*

Adesso cerchiamo una descrizione più comoda dello spazio tangente di Zariski. Sia $Y \subset \mathbb{A}^n$ e supponiamo, per iniziare, che l'origine $O = (0, ..., 0) \in Y$ e cerchiamo di descrivere T_OY. Se $Q \in k[X_1, ..., X_n]$ possiamo scrivere Q come una somma di polinomi omogenei: $Q = a_0 + Q_1 + ... + Q_r$, dove $a_0 = Q(O)$ e dove Q_i è omogeneo di grado i. Il termine lineare è dato da: $Q_1(X_1, ..., X_n) = \sum_1^n \frac{\partial Q}{\partial x_i}(O)X_i$. Se $Q \in \mathbf{I}(Y)$, $a_0 = 0$.

Sia $R = \{tq = (tq_1, ..., tq_n) | \ t \in k\}$ una retta per l'origine ($q \in R, q \neq O$). Se $Q \in \mathbf{I}(Y)$, abbiamo: $Q(tq) = Q(tq_1, ..., tq_n) = Q_1(tq_1, ..., tq_n) + ... + Q_r(tq_1, ..., tq_n)$. Siccome Q_i è omogeneo di grado i: $Q_i(tq_1, ..., tq_n) = t^i Q_i(q_1, ..., q_n)$. Quindi vediamo che: $Q(tq) = tQ_1(q) + t^2(G(tq))$ e $t = 0$ è radice con molteplicità almeno due di $Q(tq) = 0$ se e solo se: $Q_1(q) = \sum_1^n \frac{\partial Q}{\partial x_i}(O)q_i = 0$.

Se $\mathbf{I}(Y) = (P_1, ..., P_m)$, la matrice jacobiana di $P_1, ..., P_m$ nel punto $a \in Y$, $J(P_1, ..., P_m)(a)$ è la matrice:

$$J(P_1, ..., P_m)(a) = \begin{pmatrix} \frac{\partial P_1}{\partial x_1}(a) & \cdots & \frac{\partial P_1}{\partial x_n}(a) \\ \vdots & & \vdots \\ \frac{\partial P_m}{\partial x_1}(a) & \cdots & \frac{\partial P_m}{\partial x_n}(a) \end{pmatrix}$$

Per quanto detto prima, T_OY è il sotto spazio vettoriale $Ker(J(P_1, ..., P_m)(O))$ di $\mathbb{A}^n$.

Passiamo adesso al caso generale. Sia $a \neq O$ un punto qualsiasi di Y. Ci riportiamo al caso precedente con una traslazione, ossia con il cambio di variabili: $X - a = T$. Abbiamo: $Q(T) = Q(a) + Q_1(T) + ... + Q_r(T)$ ossia: $Q(X - a) = Q(a) + Q_1(X - a) + ... + Q_r(X - a)$ (non è alro che lo sviluppo di Taylor). Per $X = (1 - t)a + tq$, viene: $Q(t(q - a)) = tQ_1(q - a) + t^2(...)$ ($Q(a) = 0$ se $Q \in \mathbf{I}(Y)$). Quindi $t = 0$ è radice di molteplicità almeno due se e solo se: $Q_1(q - a) = \sum_1^n \frac{\partial Q}{\partial x_i}(a)(q_i - a_i) = 0$.

Vediamo quindi che T_aY è l'insieme delle soluzioni del sistema lineare (nelle incognite q_i):

$$\sum_1^n \frac{\partial P_i}{\partial x_i}(a)(q_i - a_i) = 0 \ 1 \leq i \leq m \ (*)$$

Ovviamente a è soluzione del sistema, quindi T_aY è il sottospazio affine $a + V$ dove $V = Ker(J(P_1, ..., P_m)(a))$ è l'insieme delle soluzioni del sistema lineare omogeneo associato. Abbiamo dimostrato:

Proposizione 6.10: *Sia $Y \subset \mathbb{A}^n$ un insieme algebrico affine, $a \in Y$, e $\mathbf{I}(Y) = (P_1, ..., P_m)$. Lo spazio tangente ("immerso") di Zariski è il sottospazio affine di $\mathbb{A}^n$ passante per a: $T_aY = a + Ker(J(P_1, ..., P_m)(a))$; in particolare $dim(T_aY) = n - r$, dove $r = rango(J(P_1, ..., P_m)(a))$.*

Definizione 6.11: *Con le notazioni precedenti lo spazio vettoriale $V = \{v / J(P_1, ..., P_m)(a).^t v = 0\}$ (ossia V è la direzione, o giacitura dello spazio affine T_aY) si chiama lo spazio tangente (vettoriale) di Zariski di Y in a, e si nota TY_a.*

Esempio 6.12: Sia Y la varietà $\mathbf{V}(F) \subset \mathbb{A}^n$. Se $a \in Y$, $T_aY = \{x \in \mathbb{A}^n / d_aF(x - a) = 0\}$. Se esiste j tale che $\frac{\partial F}{\partial x_j}(a) \neq 0$, T_aY è l'iperpiano di equazione $\Sigma \frac{\partial F}{\partial x_i}(a).Xi + b = 0$ dove $b = -\Sigma \frac{\partial F}{\partial x_i}(a).a_i$. Altrimenti, se tutte le derivate parziali di F sono nulle in $a, T_aY = \mathbb{A}^n$. Abbiamo $\dim Y = n-1$, quindi nel primo caso $\dim(T_aY) = \dim Y$, nel secondo caso $\dim(T_aY) > \dim Y$.

Se Y è abbastanza "regolare" in a, lo spazio tangente T_aX dovrebbe fornire una buona approssimazione di Y in a, in particolare si dovrebbe avere $\dim T_aY = \dim Y$ (per esempio si vede facilmente che $T_a\mathbb{A}^n \simeq \mathbb{A}^n$, per ogni $a \in \mathbb{A}^n$), questo giustifica la seguente:

Definizione 6.13: *Sia $Y \subset \mathbb{A}^n$ una varietà affine, $a \in Y$. Il punto a è un punto nonsingolare (o liscio, o regolare) di Y se $\dim T_aY = \dim Y$; altrimenti a è un punto singolare (o singolarità) di Y. La varietà Y è nonsingolare (o liscia) se ogni punto di Y è un punto nonsingolare di Y.*

Scopo di quanto segue è di dimostrare il seguente:

Teorema 6.14: *Sia $Y \subset \mathbb{A}^n$ una varietà quasi-affine, l'insieme dei punti nonsingolari di Y contiene un aperto non vuoto.*

Vedremo poi che l'insieme dei punti regolari di Y è un aperto non vuoto di Y. Il teorema risulta dai seguenti fatti:

Proposizione 6.15: *Sia $f : X \to Y$ un isomorfismo tra due varietà quasi-affini, allora: X è liscia in $x \iff Y$ è liscia in $f(x)$.*

Teorema 6.16: *Ogni varietà affine Y è birazionalmente equivalente ad un' ipersuperficie di $\mathbb{A}^{n+1}$ ($n = \dim Y$).*

Dimostrazione del Teorema 6.14. Facciamo prima il caso in cui $Y = \mathbf{V}(F)$ è un'ipersuperficie di $\mathbb{A}^n$ (F polinomio non costante e irriducibile). Abbiamo già visto che $y \in Y$ è un punto singolare se e solo se tutte le derivate parziali $F_i'(y) := \frac{\partial F}{\partial x_i}(y)$ sono nulle, pertanto l'insieme dei punti singolari è chiuso in

Y. Se ogni punto di y è singolare, le derivate parziali si annullano su Y, cioè $F_i' \in \mathbf{I}(Y) = (F)$, ossia $F|F_i'$. Se X_i compare in F, $\deg_{X_i}(F_i') < \deg_{X_i}(F)$, e quindi l'unica possibilità è $F_i' = 0$. Se la caratteristica di k è zero e se tutte le derivate parziali di F sono nulle, allora necessariamente F è costante, e abbiamo la contraddizione cercata. Se la caratteristica è positiva, diciamo $ch(k) = p$, $F_i' = 0$ implica che F è un polinomio in x_i^p. Siccome questo è vero per ogni i, prendendo delle radici $p-$esime dei coefficienti di F (possiamo farlo perché k è algebricamente chiuso), abbiamo $F = R^p$, contro l'ipotesi F irriducibile. Questo dimostra il teorema nel caso delle ipersuperfici.

Se Y è una varietà affine qualsiasi, dal Teorema 6.16 segue che esiste un'ipersuperficie $Z \subset \mathbb{A}^n$, degli aperti non vuoti $U \subset Y$, $V \subset Z$, e un isomorfismo $f : U \to V$. Dalla prima parte della dimostrazione l'insieme dei punti lisci di Z è un aperto non vuoto, W, di Z. Siccome Z è irriducibile $V \cap W$ è un aperto non vuoto. Segue dalla Proposizione 6.15 che ogni punto dell'aperto $f^{-1}(V \cap W)$ è un punto liscio di Y. □

Dimostrazione del Teorema 6.16. La dimostrazione utilizza risultati della teoria dei campi, rimandiamo ad un buon testo di algebra per la dimostrazione di questi risultati. Siccome $\dim Y = n$, $K(Y)$ è un'estensione algebrica finita di $k(t_1, ..., t_n)$ (i t_i formano una base di trascendenza), inoltre siccome k è algebricamente chiuso (quindi in particolare perfetto), $K(Y)$ è un'estensione separabile di $k(t_1, ..., t_n)$ (questo è comunque automatico se $ch(k) = 0$). Per il teorema dell'elemento primitivo esiste $t \in K(Y)$ tale che $K(Y) \simeq k(t_1, ..., t_n, t)$. L'elemento t è algebrico su $k(t_1, ..., t_n)$ e quindi verifica un'equazione, che prendiamo minimale, $P(t) = 0$ dove P è un polinomio a coefficienti in $k(t_1, ..., t_n)$. Riducendo allo stesso denominatore otteniamo $f(t_1, ..., t_n, t) = 0$ con f polinomio a coefficienti in k; inoltre, per minimalità di P, f è irriducibile. Sia $Z \subset \mathbb{A}^{n+1}$ l'ipersuperficie di equazione $f = 0$; si ha $K(Z) \simeq K(Y)$ (cfr. Esempio 5.13), e quindi (cfr. Proposizione 4.22) Y e Z sono birazionalmente equivalenti. □

Rimandiamo la dimostrazione della Proposizione 6.15 (ma cfr. Esercizi) a quando avremo una descrizione più intrinseca dello spazio tangente.

Osserviamo che se $y \in Y$ è un punto singolare di Y, allora finora sappiamo soltanto che $\dim T_y Y \neq \dim Y$, a priori potrebbe anche essere $\dim T_y Y < \dim Y$; vediamo adesso che questo caso non si presenta.

Lemma 6.17: *Sia $Y \subset \mathbb{A}^n$ una varietà affine. Per ogni $t \in \mathbb{N}$ sia $Y_t := \{a \in Y / \dim T_a Y \geq t\}$. Allora Y_t è Zariski chiuso in Y.*

Dimostrazione. Sia $\mathbf{I}(Y) = (P_1, ..., P_m)$, e notiamo $J(a)$ la matrice jacobiana dei P_i nel punto a. Dalla Proposizione 6.10: $\dim T_a Y = t \iff \text{rango}(J(a) = n - t \iff$ tutti i minori di ordine $n - t + 1$ di $J(a)$ sono nulli. Quindi Y_t è

l'intersezione di Y con il chiuso $\mathbf{V}(\Delta_1, ..., \Delta_i, ...)$ dove i Δ_i sono i minori di ordine $n - t + 1$ della matrice jacobiana $J(P_1, ..., P_m)$. □

Corollario 6.18: *Sia Y una varietà quasi-affine, allora per ogni y in Y:* $\dim T_y Y \geq \dim Y$. *In particolare $Sing(Y)$, l'insieme dei punti singolari di Y, è un chiuso proprio di Y, e $y \in Sing(Y)$ se e solo se* $\dim T_y Y > \dim Y$.

Dimostrazione. Sia $\dim Y = n$, con le notazioni del lemma precedente, il chiuso Y_n contiene un aperto di punti nonsingolari di Y, quindi $Y_n = Y$. □

Esercizi.

Esercizio 6.1: *Sia C la curva piana di equazione $y - f(x) = 0$ dove f è un polinomio con $f(0) = 0$. Se R è una retta passante per l'origine O, allora $i(C, R; O) = 1$ tranne se R è la retta di equazione $y = f\prime(0)x$.*

Esercizio 6.2: *Sia $C \subset \mathbb{A}^3$ una curva liscia, irriducibile (cioè una varietà affine di dimensione uno, nonsingolare) tale che $\mathbf{I}(C) = (f, g)$. Dimostrare che in ogni punto $x \in C$ la tangente a C, T_xX, è l'intersezione dei piani tangenti T_xF, T_xG, dove F (risp. G) è la superficie di equazione $f = 0$ (risp. $g = 0$). In particolare F e G sono liscie e trasversali (i.e. i piani tangenti sono distinti) in ogni punto di C.*

N.B.: *Una curva, C, dello spazio $\mathbb{A}^3$ si dice* intersezione completa *se $\mathbf{I}(C)$ può essere generato da due (= codim$C$) equazioni; invece la curva si dice* insiemisticamente intersezione completa *se esiste un ideale J generato da due equazioni, tale che $\mathbf{V}(J) = C$. Esistono curve (lisce, irriducibili) non intersezioni complete, ma secondo un risultato di Ferrand-Szpiro (1975) ogni curva liscia, irriducibile di $\mathbb{A}^3$ è insiemisticamente intersezione completa.*

Esercizio 6.3: *Sia $C \subset \mathbb{A}^2(k)$ con k di caratteristica due, la conica di equazione $y = x^2$. Mostrare che tutte le tangenti a C sono parallele (questo fenomeno non può accadere in caratteristica zero).*

Esercizio 6.4: *Siano $X \subset \mathbb{A}^n, Y \subset \mathbb{A}^m$ delle varietà affini, e $f : X \to Y$ un morfismo. Per $x \in X$ si definisce (come in geometria differenziale) un'applicazione lineare $d_xf : TX_x \to TY_y$, $(y = f(x))$; d_xf è la derivata (o applicazione lineare tangente) di f in x.*

Sappiamo che f è la restrizione a X di un'applicazione polinomiale (sempre notata f) $k^n \to k^m : x = (x_1, ..., x_n) \to (f_1(x), ..., f_m(x))$. Per ogni $a \in \mathbb{A}^n$ possiamo considerare la matrice jacobiana $J_a(f)$; se $v = (v_1, ..., v_n) \in T\mathbb{A}^n_a$ (spazio tangente vettoriale) poniamo $d_af(v) = J_a(f).{}^tv$, questo definisce un'applicazione lineare $d_af : T\mathbb{A}^n_a \to T\mathbb{A}^m_b, (b = f(a))$.

Se $x \in X$, consideriamo la restrizione di d_xf a TX_x, e mostriamo che questo definisce un'applicazione lineare $d_xf : TX_x \to TY_y, (y = f(x))$.

Sia $\mathbf{I}(X) = (f_1, ..., f_r), \mathbf{I}(Y) = (g_1, ..., g_t)$. Per ogni $i, g_i \circ f$ è una funzione regolare su $\mathbb{A}^n$ che si annulla su X, quindi $g_i \circ f \in \mathbf{I}(X)$, ossia $g_i \circ f = \Sigma P_j f_j$, derivando: $d_{f(x)}g_i \circ d_xf = \Sigma P_j(x).d_xf_j + d_xP_j.f_j(x)$. Se $x \in X, f_j(x) = 0$ per ogni j; se $v \in TX_x, d_xf_j(v) = 0$ per ogni j.

(i) Concludere che $d_xf(TX_x) \subset TY_y$.

(ii) Siano $f : X \to Y, g : Y \to Z$ dei morfismi di varietà affini, $y = f(x)$, $z = g(y)$. Verificare che $d_x(g \circ f) = d_yg \circ d_xf$. Concludere che se $f : X \to Y$ è un isomorfismo di varietà affini allora: $x \in X$ è un punto nonsingolare $\iff f(x) \in Y$ è nonsingolare. Basta questo per dimostrare la Proposizione 6.15?

Esercizio 6.5: *Lo spazio tangente di Zariski è un primo invariante utile per la classificazione. Se Y è una varietà affine con $\dim(T_yY) = p$, per qualche $y \in Y$, allora Y non è isomorfa a nessuna sottovarietà di $\mathbb{A}^n, n < p$. Perché? In particolare $\mathbb{A}^n \simeq \mathbb{A}^m \Longleftrightarrow n = m$.*

Esercizio 6.6: *Sia $X \subset \mathbb{A}^n$ una varietà affine, $x \in X$, e $I = (f_1, ..., f_r)$ un ideale tale che $X = \mathbf{V}(I)$. Dimostrare che se il rango della jacobiana $J(f_1, .., f_r)(x)$ è uguale a $n - \dim X$ allora x è un punto nonsingolare di X. Cosa si può dire invece se il rango è $< n - \dim X$?*

Esercizio 6.7: *Sia $X \subset \mathbb{A}^n$ un'ipersuperficie riducibile e sia $X = X_1 \cup ... \cup X_r$ la sua decomposizione in componenti irriducibili. Mostrare che se $x \in X_i \cap X_j$ allora x è un punto singolare di X.*

Esercizio 6.8: *("La cubica gobba") Sia $\varphi : k \to k^3 : t \to (t, t^2, t^3)$. Si pone $C = Im(\varphi)$.*

(i) Mostrare che $C = \mathbf{V}(I)$ dove $I = (Y - X^2, Z - X^3)$.

(ii) Si ammetterà che l'ideale I è primo (potete provare a dimostrarlo, per esempio mostrando che $k[X, Y, Z]/I \simeq k[T]$). Dedurne che $\mathbf{I}(C) = I$.

(iii) Mostrare che C è nonsingolare col criterio jacobiano.

(iv) Mostrare che C è isomorfa a $\mathbb{A}^1$ (quindi C è razionale).

(v) Mostrare che C non è contenuta in nessun piano di $\mathbb{A}^3$ e che un piano generico di $\mathbb{A}^3$ interseca C in tre punti distinti. Mostrare che C non ha trisecanti (rette che la incontrano in (almeno) tre punti).

(vi) Mostrare che C è intersezione completa (cfr. Esercizio 6.2).*

Esercizio 6.9: *Sia Y uno spazio topologico. Un'applicazione $f : Y \to \mathbb{Z}$ è semicontinua superiormente se per ogni $y \in Y$ esiste un intorno aperto, U, di y in Y tale che per ogni $y' \in U$, $f(y') \leq f(y)$.*

Sia $Y \subset \mathbb{A}^n$ una varietà affine. Dimostrare che l'applicazione $f : Y \to \mathbb{Z} : a \to \dim T_aY$ è semicontinua superiormente.

CAPITOLO II

Insiemi algebrici proiettivi

1. Il proiettivo: come e perchè.

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, purchè contati con molteplicità (teorema fondamentale dell'algebra).

Il secondo enunciato è chiaramente più soddisfacente del primo, e siamo condotti 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 $V(X^2 + Y^2 + 1) = \emptyset$ 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 ($C = V(XY)$ e $C' = V(X(Y - 1))$) 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 $V(XY - 1)$ non interseca il suo asintoto $X = 0$. E' 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 $C = V((X^2+Y^2)^2 + 3X^2Y - Y^3)$ (trifolium), $C' = V((X^2+Y^2)^3 - 4X^2Y^2)$ (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 $(\lambda_0 : \lambda_1 : \ldots : \lambda_n) = (m_0 : m_1 : \ldots : m_n) \iff \exists\ \lambda \neq 0$ 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, ..., 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. □

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 $\mathbb{P}(E^\checkmark)$ dove $E^\checkmark$ (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 $\mathbb{P}^\checkmark_n$) . I punti di $\mathbb{P}(E^\checkmark)$ sono le rette vettoriali di $E^\checkmark$. La dualità vettoriale ci permette di identificare una retta vettoriale di $E^\checkmark$ con un iperpiano vettoriale di E;

in altri termini $\mathbb{P}(E^\checkmark)$ 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^* ($dimE = n+1$); la biiezione è data da $V \longmapsto V^\circ$ (è biiettiva perchè $V^{\circ\circ} = V$). Inoltre $V \subseteq W \Leftrightarrow W^\circ \subseteq V^\circ$ (la dualità inverte le inclusioni). In particolare il duale di $\mathbb{P}^\checkmark_n$ 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 se 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 $j_0^{-1} =: y_0 : \mathbb{A}^n \to U_0 : (b_1, \ldots, b_n) \longmapsto (1 : b_1 : \ldots : b_n)$. 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 $\mathbb{P}^1 \backslash \{\infty\}$ 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 $k^{n+1}\backslash\{0\}$, 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 $(e_0, \ldots, e_n)$ di V ogni punto $p \in \mathbb{P}(V)$ corrisponde a delle coordinate omogenee $(a_0 : \ldots : a_n)$ ($p =< v >$ 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 $(b_0 e_0, \ldots, b_n e_n)$ è una base di V, rispetto a questa base le coordinate omogenee di p sono $(\frac{a_0}{b_0} : \ldots : \frac{a_n}{b_n})$; 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 $p_0, \ldots, p_n, p$ siano in posizione generale (cioè non $n+1$ tra di loro sono contenuti in un iperpiano). Allora esiste un unico sistema di coordinate omogenee corrispondente ai p_i (cioè $p_i = (0 : \ldots : 1 : \ldots : 0)$), tale che in quel sistema, le coordinate di p siano $(1 : \ldots : 1)$. Infatti sia $p =< v >$ e $v = g_i e_i$, siccome i punti $p_0, \ldots, p_n, p$ sono in posizione generale: $g_i \neq 0$, $\forall i$. Quindi $(g_0 e_0, \ldots, g_n e_n)$ è una base di V e rispetto a questa base le coordinate omogenee di p sono $(1 : \ldots : 1)$. Viceversa se p ha coordinate $(1 : \ldots : 1)$ rispetto alla

base (b_ie_i) allora $\lambda v = b_ie_i$, per qualche $\lambda \neq 0$; segue che $b_i = \lambda g_i$, e le basi (b_ie_i), (g_ie_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 [**S**] §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 affinchè 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 perchè 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 $a \neq a'$: $x = \frac{[y(b-b')+d-d']}{a'-a}$ (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 sarano 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 affinchè 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 $H = \{X_0 = 0\}$ ("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) *E' 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 $P(X_0, \ldots, X_n) = \Sigma a_{i_0 \ldots i_n} X_0^{i_0} ... X_n^{i_n}$, è omogeneo di grado d se tutti i suoi monomi hanno grado d: $a_{i_0 \ldots i_n} \neq 0 \Longrightarrow i_0 + \ldots + i_n = d$. Inoltre ogni polinomio $P \in k[X_0, \ldots, X_n]$ si scrive, in modo unico, nella forma $P = P_d + P_{d-1} + \ldots + P_0$ dove P_i è omogeneo di grado i. Osserviamo che se P è omogeneo di grado d allora $P(\lambda a_0, \ldots, \lambda a_n) = \lambda^d P(a_0, \ldots, a_n)$, 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 $P \in k[X_0, \ldots, X_n]$ se $P(z_0, \ldots, z_n) = 0$ dove $(z_0 : \ldots : z_n)$ 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 $P(z_0, \ldots, z_n) = 0$ per ogni rappresentante di z. Abbiamo $P = P_d + P_{d-1} + \ldots + P_0$, dove P_i è omogeneo di grado i. Un rappresentante qualsiasi di z è della forma $(\lambda z_0 : \ldots : \lambda z_n)$, abbiamo $P(\lambda z_0, \ldots, \lambda z_n) = \sum_{j=0}^{d} P_j(\lambda z_0, \ldots, \lambda z_n) = \sum_{j=0}^{d} \lambda^j P_j(z_0, \ldots, z_n)$, quindi $P(\lambda z_0, \ldots, \lambda z_n) = 0$, $\forall \lambda$ se e solo se $P_j(z_0, \ldots, z_n) = 0$, $\forall j$ (considerare il polinomio in λ). Questo ci conduce ad introdurre la nozione di ideale omogeneo.*

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

Un'altra caratterizzazione degli ideali omogenei:

Lemma 2.4: *Un ideale $I \subseteq k[X_0, \ldots, X_n]$ 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 $I = (f_1, \ldots, f_r)$, $f_i = \sum_k f_{i,k}$, $f_{i,k}$ omogeneo di grado k. Allora I è generato dai polinomi omogenei $f_{i,k}$ □

Inoltre abbiamo:

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

DIMOSTRAZIONE. Lasciata al lettore □

Definizione 2.6: *Sia $I = (f_1, \ldots, f_r)$ 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* $\mathbf{V}(I) = \{z \in \mathbb{P}^n / \ P(z) = 0, \forall P \in I\}$, *purchè $P(z) = 0$ sia interpretato come nell'osservazione 2.2.*

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

Esempio 2.9:

(*i*) Sia $F \in k[X_0, \ldots, X_n]$ 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 $\mathfrak{m} = (X_0, \ldots, X_n) \subseteq k[X_0, \ldots, X_n]$ 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 sottinsiemi algebrici proiettivi.

(*iii*) Sia $z = (a_0' : \ldots : a_n') \in \mathbb{P}^n$, uno degli a_i' è non nullo, per esempio $a_0' \neq 0$, dividendo per a_0' abbiamo $z = (1 : a_1 : \ldots : a_n)$ e $\{z\} = \mathbf{V}(X_1 - a_1 X_0, \ldots, X_n - a_n X_0)$, quindi un punto di $\mathbb{P}^n$ è un insieme algebrico. Osservare che l'ideale $(X_1 - a_1 X_0, \ldots, X_n - a_n X_0)$ non è massimale (perchè nell'affine k^{n+1} questo ideale definisce la retta corrispondente a z; tranne l'ideale irrilevante $\mathfrak{m}$, gli ideali massimali di $k[X_0, \ldots, X_n]$ non sono omogenei, cfr I.§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* $\mathbf{I}(X) = \{P \in k[X_0, \ldots, X_n] / \ P(z) = 0, \forall z \in X$, *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 sottinsiemi 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 sottinsieme 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 $C(X) = \{(x_0, \ldots, x_n) \in A^{n+1} \ / \ (x_0, \ldots, x_n) = (0, \ldots, 0)$ o $[x_0 : \ldots : x_n] \in X\}$.*

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 sottinsieme 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 sottinsieme algebrico non vuoto. Il cono affine di X è un sottinsieme 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 $Q \in \mathbf{I}(X)$, $Q = Q_m + \ldots + Q_r$, 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 $P(0, \ldots, 0) = 0$, 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 $I \subseteq k[X_0, \ldots, X_n]$ un ideale omogeneo.*

(*i*) *$\mathbf{V}(I) \subseteq \mathbb{P}^n$ è vuoto se e solo se $(X_0, \ldots, X_n)^N \subseteq I$ 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*) E' chiaro che $\mathbf{V}(I) = \emptyset$ se e solo se $\mathbf{V}_a(I) \subseteq \{(0, \ldots, 0)\}$. Dal Teorema degli zeri $\mathbf{I}_a(\mathbf{V}_a(I)) = \sqrt{I}$. Dall'inclusione $\mathbf{V}_a(I) \subseteq \{(0, \ldots, 0)\}$, risulta $(X_0, \ldots, X_n) \subseteq \sqrt{I}$. 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), $(X_0, \ldots, X_n)^N \subseteq I$.

(*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*:

$\varphi : \{$*sottinsiemi 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* $\mathfrak{m}\} \to \{$*sottinsiemi 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 sottinsiemi algebrici è un sottinsieme algebrico. L'intersezione di ogni famiglia di sottinsiemi algebrici è un sottinsieme algebrico. L'insieme vuoto e $\mathbb{P}^n$ sono dei sottinsiemi algebrici.*

Dimostrazione. E' simile a quella del caso affine □

Definizione 2.18: *Dal lemma precedente segue che i sottinsiemi 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 sottinsieme algebrico irriducibile e di dimensione ("topologica").*

Definizione 2.20: *Una varietà proiettiva è un sottinsieme 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 sottinsieme 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 sottinsieme 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 perchè 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 $\mathbb{P}^n \to k$ perchè, se $d = deg(P) = deg(Q)$: $\frac{P(\lambda x_0,\ldots,\lambda x_n)}{Q(\lambda x_0,\ldots,\lambda x_n)} = \frac{\lambda^d P(x_0,\ldots,x_n)}{\lambda^d Q(x_0,\ldots,x_n)} = \frac{P(x_0,\ldots,x_n)}{Q(x_0,\ldots,x_n)}$. 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 $U_i = \{(x_0 : \ldots : x_n)/x_i \neq 0\}$, 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 $x = (x_0 : \ldots : x_n)$, $x_0 \neq 0$, se $f \circ y_0$ è regolare in $u = j_0(x)$, dove $y_0^{-1} = j_0 : U_0 \to \mathbb{A}^n : (x_0 : \ldots : x_n) \longmapsto (u_1, \ldots, u_n)$ 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: $p = p_d + \ldots + p_i + \ldots + p_0$, $q = q_r + ... + q_i + \ldots + q_0$, p_i e q_i omogenei di grado i. Abbiamo:

$p_i(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) = \frac{1}{x_0^i} p_i(x_1, \ldots, x_n)$, quindi

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

.

Poniamo $p^*(x_0, \ldots, x_n) := p_d(x_1, \ldots, x_n) + \ldots + x_0^{d-i} p_i(x_1, \ldots, x_n) + \ldots + x_0^d p_0$, 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 $x_0, \ldots, x_n$.

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 uniformizzare 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 (perchè 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 $f_0(u) = \sum_{0 \le i \le d} a_i u^i$, cioè $f_0(\frac{x_1}{x_0}) = \sum_{0 \le i \le d} a_i (\frac{x_1}{x_0})^i = (\sum_{0 \le i \le d} a_i x_1^i . x_0^{d-i})/x_0^d$. Nello stesso modo $f_1(v) = \sum_{0 \le j \le r} b_j v^j$, ossia $f_1(\frac{x_0}{x_1}) = (\sum_{0 \le j \le r} b_j x_0^j . x_1^{r-j})/x_1^r$. In un punto $(x_0 : x_1)$ di $U_0 \cap U_1$ si deve avere:
$(\sum_{0 \le i \le d} a_i x_1^i . x_0^{d-i})/x_0^d = (\sum_{0 \le j \le r} b_j x_0^j . x_1^{r-j})/x_1^r$, *cioè* $P(x_0, x_1) = \sum_{0 \le i \le d} a_i x_1^{i+r} . x_0^{d-i} - \sum_{0 \le j \le r} b_j x_0^{j+d} . x_1^{r-j} = 0$. *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 $x_0^{d+r-i} x_1^i$, $0 \le i \le d + r$) di P sono nulli. Gli a_i sono coefficienti di monomi nei quali x_0 compare con una potenza $\le d$, mentre i b_j sono coefficienti di monomi nei quali x_0 compare con una potenza $\ge d$. 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 $f(t_1, \ldots, t_n) \in k[t_1, \ldots, t_n]$ un polinomio in n variabili. Sia $f = f_d + \ldots + f_i + \ldots + f_0$ 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:*

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

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

Osservazione 3.8: *Le proprietà seguenti sono di facile verifca (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, $0 \leq i \leq n$, l'applicazione*

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

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 $\mathbb{I}(X) = (f_1, \ldots, f_r)$ l'ideale di X, allora $X' := \mathbf{V}(f_1^*, \ldots, f_r^*)$ 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 $x = (x_0 : \ldots : x_n) \in \mathbb{P}^n$: $f^*(x_0 : \ldots : x_n) = 0 \Leftrightarrow f^*(1 : \frac{x_1}{x_0} : \ldots : \frac{x_n}{x_0}) = 0$, ma $f_*(1 : \frac{x_1}{x_0} : \ldots : \frac{x_n}{x_0}) = f(\varphi(x))$. 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 $\mathbb{I}(Y') = (F_1, \ldots, F_t)$, sia $Z \subseteq \mathbb{A}^n$ il chiuso $Z = \mathbf{V}(F_{1*}, \ldots, F_{t*})$. Basta mostrare $\varphi(Y) = Z$; come prima, questo segue da: $F(x) = 0 \Leftrightarrow F_*(\varphi(x)) = 0$.

Rimane da vedere cheφ 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 $\square$

Osservazione 3.10: (*i*) *Segue che per ogni* i, j *l'applicazione:* $\varphi_j \circ \psi_i$*:* $\varphi_i(U_{ij}) \to \varphi_j(U_{ij})$ *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 $S = k[X_0, \ldots, X_n]$ e 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 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 3.6).*

4. Curve algebriche piane: generalità.

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

Possiamo considerare lo spazio proiettivo $\mathbb{P}(S_d)$ associato allo spazio vettoriale S_d. Un elemento di $\mathbb{P}(S_d)$ è una classe d'equivalenza costituita da tutti i multtipli 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 $\mathbb{P}(S_d)$ 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 sottinsieme 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.*
Benchè 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 sottinsieme 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 sottinsieme 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 $\mathbf{V}(F)\cap U_x,\dots,\mathbf{V}(F)\cap U_z$, 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 $F(x,y,z)=\Sigma a_{ijk}x^iy^jz^k$ 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 $C_x=\{(u,v)A^2/F_*(u,v)=0\}$, 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 sottinsieme 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:

$F(\lambda p + \mu q) = L_1^{\alpha_1}(\lambda, \mu) \dots L_r^{\alpha_r}(\lambda, \mu)$, $\alpha_1 + \ldots + \alpha_r = d$, $L_i(\lambda, \mu) = a_i\lambda + b_i\mu$. Pertanto $X \cap R$ è dato da il 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 $(1 : 0)$ (perchè $p \in X \cap R$), 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:*

$d.F(X_0,...,X_n) = \sum_{i=0}^{n} X_i.\frac{\partial F}{\partial x_i}(X_0,...,X_n)$

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: $\Sigma X_i \frac{\partial F}{\partial X_i}(\lambda X_0,\ldots,\lambda X_n) = d\lambda^{d-1}.F(X_0,\ldots,X_n)$. 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:

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

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 perchè $F(p) = 0$

(*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 le osservazioni 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 in 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: $f(tq, tq') = t^n f_n(Q) + \ldots + t^i f_i(Q) + \ldots + t f_1(Q)$. 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 (perchè 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 $(1-l)T(p)+lT(q) = (1-l)(N(p)+f)+l(N(q)+f) = (1-l)(N(p)+l(N(q)+f = N((1-l)p+lq)+f$ (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: $l_i(x, y) = 0$ $\square$

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 $F(X,Y,Z) = X^3 - X^2Z + Y^2Z$, 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 2: 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 perchè, 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 Es. 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. Il teorema di Bezout.

Scopo di questo paragrafo è di illustrare (senza dimostrazioni) il teorema di Bezout. Sia $C \subset \mathbb{P}^2$ una curva e sia R una retta non componente di C, abbiamo definito, $i(C, R; p)$, la molteplicità d'intersezione di C e R nel punto p, e abbiamo visto la versione "debole" del teorema di Bezout: se d è il grado di C, allora: $d = i(C, R; p)$. Se C e X sono due curve qualsiasi di $\mathbb{P}^2$, e se $p \in \mathbb{P}^2$, si definisce il numero d'intersezione (o molteplicità d'intersezione) di C e X in p: $i(C, X; p)$ (se X è una retta si ritrova la definizione precedente), e si ha:

Teorema 7.1 (Teorema di Bezout)**:** *Siano C, X due curve di $\mathbb{P}^2$, di gradi d, m, senza componenti comuni. Allora:* $\sum_{p \in C \cap X} i(C, X; p) = d.m.$

Osservazione 7.2:
(*i*) *In questo enunciato il termine curva va inteso nel senso della Sezione 4.*
(*ii*) *Il numero d'intersezione verifica*
(*a*) *$i(C, X; p)$ è un numero positivo tranne se C e X hanno una componente comune che passa per p, in tal caso $i(C, X; p) = \infty$.*
(*b*) *$i(C, X; p) = 0 \Leftrightarrow p \notin X \cap C$.*
(*iii*) *In particolare due curve di $\mathbb{P}^2$ s'intersecano sempre.*

7.1. Il numero d'intersezione di due curve piane. Facciamo un passo indietro:
Sia $T \subseteq \mathbb{A}^2$ un sottoinsieme algebrico. Abbiamo visto: $A(T)$ è una k-algebra finita $\Leftrightarrow T$ è un insieme finito. Inoltre se T è finito, $dim_k A(T) = \#(T)$.
Sia $I \subseteq S = k[X, Y]$ un ideale tale che $\sqrt{I} = \mathbb{I}(T)$ (cioè $\mathbf{V}(I) = T$). Cosa possiamo dire di $\frac{S}{I}$? è ancora una k-algebra finita? e se sì, qual'è la sua dimensione? Facciamo un pò di esempi:

Esempio 7.3:
(*i*) Sia $T = \{(0, 0)\}$. Quindi $\mathbb{I}(T) = (X, Y)$, $A(T) \simeq k$ ha dimensione uno come k-spazio vettoriale. Sia $I = (X^2, Y)$. Abbiamo chiaramente $\mathbf{V}(I) = T$.
La k-algebra $\frac{S}{I}$ ha dimensione due su k: Siano x, y le classi di X, Y modulo I, allora 1 e x formano una base del k-spazio vettoriale $\frac{S}{I}$. Più precisamente: $\frac{S}{I} \simeq k[e]$, dove $k[e]$ $(e^2 = 0)$, è "l'algebra dei numeri duali". Infatti $\frac{k[X,Y]}{(X^2,Y)} \simeq \frac{k[X]}{(X^2)} \simeq k[e] = \{a + be / \ a, b \in k, e^2 = 0\}$. Osservare che se $f(X) \in k[X]$, allora la classe di f modulo X^2 è $f(0) + f'(0)e$ $(e = x)$.
In particolare:
la k-algebra$\frac{S}{I}$ è un anello locale il cui ideale massimale è nilpotente:

Osservazione 7.4: *l'anello $k[e]$ è locale: l'ideale (e) è massimale ($\frac{k[e]}{(e)} \simeq k$), e ogni elemento non appartenente a (e) è invertibile:* $(a+be).(\frac{1}{a} - \frac{b}{a^2}e) = 1 - \frac{be}{a} + \frac{be}{a} - \frac{b^2e^2}{a^2} =$

1, perchè $e^2 = 0$. L'ideale massimale $\mathfrak{m} = (e)$ di $k[e]$ verifica $\mathfrak{m}^2 = 0$, quindi è nilpotente.
Legame col teorema di Bezout: Cerchiamo l'intersezione della conica, C, di equazione $Y = X^2$ con la retta, R, di equazione $Y = 0$. L'intersezione si riduce ad un unico punto (l'origine), ma R e C sono tangenti nell'origine ($i(C, R; O) = 2$), "infatti" l'ideale "intersezione" $J := \mathbf{I}(C) + \mathbf{I}(R) = (Y - X^2, Y) = (X^2, Y)$, verifica: $\frac{S}{J}$ è una k-algebra finita di dimensione due.

Esempio 7.5: (1)

(*ii*) L'ideale $I = (X^n, Y)$ verifica $\mathbf{V}(I) = \{O\}$, e $\frac{S}{I}$ è una k-algebra finita di dimensione n. Si ha pure che $\frac{S}{I}$ è un anello locale il cui ideale massimale è nilpotente ($\mathfrak{m}^n = 0$). L'ideale I è l'ideale "intersezione" (somma) della curva $Y - X^n = 0$ con la retta $Y = 0$.

Per riassumere, in questi due esempi abbiamo un ideale I tale che $V(I) = \{O\}$, e $\frac{S}{I}$ è una k-algebra finita e un anello locale il cui ideale massimale è nilpotente; inoltre se scriviamo $I = (f, g)$, $dim_k \frac{S}{I}$ è la molteplicità d'intersezione in O delle curve di equazioni $f = 0$, $g = 0$.

Cerchiamo di generalizzare: siano $C, C' \subseteq \mathbb{A}^2$ due curve di equazioni rispettivamente $f = 0$, $g = 0$, senza componenti comuni. Sia $I = (f, g)$. L'insieme $X := C \cap C' = V(I)$ è finito (eventualmente vuoto), supponiamo $X = \{p_1, \ldots, p_r\}$; vogliamo ripetere in ogni punto p_i quello che abbiamo fatto prima.

Per questo introduciamo l'anello locale $\mathcal{O}_i = \mathcal{O}_{A^2, p_i}$, dei germi in p_i di funzioni regolari su $\mathbb{A}^2$. Abbiamo un morfismo $\varphi_i : S \to \mathcal{O}_i$, se $h \in S$, $\varphi_i(h)$ è il germe in p_i di h ($= \frac{h}{1}$). Sia $I.\mathcal{O}_i$ l'ideale di $\mathcal{O}_i$ generato dall'immagine di I, cioè $I.\mathcal{O}_i$ è l'insieme dei germi $\frac{h}{q}$ dove $h \in I$. L'anello quoziente $\frac{\mathcal{O}_i}{I.\mathcal{O}_i}$ è ancora un anello locale (l'ideale massimale è quello di $\mathcal{O}_i$ *mod* $I.\mathcal{O}_i$. Osservare che se $p_i \notin \mathbf{V}(I)$ allora $I.\mathcal{O}_i$ contiene un elemento invertibile e $\frac{\mathcal{O}_i}{I.\mathcal{O}_i} = 0$). Tutto questo si può fare algebricamente (con la localizzazione), e per un ideale I qualsiasi. Abbiamo quindi associato ad ogni punto p_i di $\mathbf{V}(I)$ un anello locale (in p_i) dipendente da I ($\frac{\mathcal{O}_i}{I.\mathcal{O}_i}$ è l'anello locale in p_i dello "schema" definito da I). Questo anello locale ha una struttura di k-spazio vettoriale (considerare i germi di funzioni costanti), e per concludere ci basterebbe avere: se $\mathbf{V}(I)$ è un insieme finito, allora $dim_k \frac{\mathcal{O}_i}{I.\mathcal{O}_I} < \infty$; se questo fosse vero si potrebbe definire $i(C, C'; p_i) := dim_k \frac{\mathcal{O}_i}{I.\mathcal{O}_i}$. In effetti è proprio così e per vederlo si usa:

Proposizione 7.6: *Sia $(A, \mathfrak{m}, k)$ una k-algebra locale, noetheriana, con k algebricamente chiuso. Il k-spazio vettoriale A è di dimensione finita se e solo se $\mathfrak{m}$ è nilpotente.*

Per la dimostrazione si rimanda a un buon testo di algebra. Spieghiamo invece perchè la condizione che, per ogni i, l'ideale massimale di $\frac{\mathcal{O}_i}{I.\mathcal{O}_i}$ sia nilpotente assicura

che $\mathbf{V}(I)$ sia un insieme finito. Supponiamo che p_i sia l'origine. L'ideale massimale dell'origine è generato da x, y ("parametri locali"), dire che l'ideale massimale di $\frac{\mathcal{O}_i}{I.\mathcal{O}_i}$ è nilpotente significa: $\exists\ n$ tale che $x^n \in I.\mathcal{O}_i$, $\exists\ m$ tale che $y^m \in I.\mathcal{O}_i$, cioè esistono dei polinomi P, Q con $P(p_i).Q(p_i) \neq 0$ tali che $x^n P \in I$, $y^m Q \in I$. Se p è un punto "vicino" (pensare alla topologia usuale su $\mathbb{C}$) a p_i si avrà ancora $P(p).Q(p) \neq 0$, inoltre una delle due coordinate di p sarà non nulla, diciamo $x(p) \neq 0$. Quindi $x^n P$ non si annulla in p, e quindi $p \in \mathbf{V}(I)$; cioè ogni punto di $\mathbf{V}(I)$ è isolato, pertanto $\mathbf{V}(I)$ è finito.

Dopo questa giustificazione enunciamo il risultato principale:

Proposizione 7.7: *Sia $I \subseteq k[X_1, ..., X_n]$ un ideale.*
(i) L'insieme algebrico $\mathbf{V}(I)$ è finito se e solo se $dim_k \frac{S}{I}$ è finita.
(ii) Supponiamo $\mathbf{V}(I) = \{p_1, \ldots, p_r\}$ e poniamo $\mathcal{O}_i = \mathcal{O}_{A^n, p_i}$. Allora $\frac{S}{I}$ è isomorfo a $\bigoplus_{1 \leq i \leq r} \frac{\mathcal{O}_i}{I.\mathcal{O}_i}$ (prodotto diretto degli anelli locali $\frac{\mathcal{O}_i}{I.\mathcal{O}_i}$). In particolare $dim_k \frac{S}{I} = \sum dim_k(\frac{\mathcal{O}_i}{I.\mathcal{O}_i})$.

Definizione 7.8: *Siano $C, X \subseteq \mathbb{A}^2$ due curve di equazioni rispettivamente $f = 0$, $g = 0$, senza componenti comuni. Se $p \in C \cap X$, la molteplicità d'intersezione di C e X in p è: $i(C, X; p) = dim_k \frac{\mathcal{O}_p}{(f,g).\mathcal{O}_p}$.*

Osservazione 7.9: *Segue dalla Prop. 7.7 che $i(C, X; p) = dim_k(\frac{k[X,Y]}{(f,g)})$; attenzione però, potrebbe essere $C \cap X = \emptyset$! per superare questo inconveniente si passa al proiettivo.*

Definizione 7.10: *Siano C e X due curve di $\mathbb{P}^2$ senza componenti comuni. Se $p \in C \cap X$, la molteplicità d'intersezione di C e X in p è la molteplicità d'intersezione delle corrispondenti curve affini in una carta affine contenente p.*

Osservazione 7.11:
- *(i) Si verifica che $i(C, X; p)$ non dipende dalla carta scelta.*
- *(ii) Per dimostrare Bezout si prende una carta affine contenente tutti i punti di $C \cap X$ e si dimostra che $dim_k(\frac{k[X,Y]}{(F*, G*)}) = d.m$ dove $F = 0$, $G = 0$ sono le equazioni di C, X ($d = deg(F)$, $m = deg(G)$).*
- *(iii) Il calcolo del numero d'intersezione $i(C, X; p)$ può risultare piuttosto difficile, specialmente se le curve sono singolari in p. Ci limiteremo ad osservare la seguente:*

Proposizione 7.12: *Siano C, X due curve di $\mathbb{P}^2$ senza componenti comuni. Se $p \in C \cap X$ e se p è un punto singolare di una delle due curve, allora:*

$$i(C, X; p) \geq 2$$

.

DIMOSTRAZIONE. Basta fare il caso affine. Possiamo assumere $p = (0,0)$ e X singolare in p. Se f è l'equazione di X, dire che X è singolare in p è equivalente a: $f \in (x,y)^2$. Sia g l'equazione di C, abbiamo $g \in (x,y)^k$, per qualche $k \geq 1$. Possiamo assumere $x \notin (f,g)$ (il termine lineare di g non può, da solo, generare (x,y)). Mostriamo che 1 e x sono linearmente indipendenti in $\frac{\mathcal{O}_p}{(f,g).\mathcal{O}_p}$. Sappiamo che x è nilpotente: $x^m = 0$, $x^{m-1} \neq 0$. Se $\alpha 1 + \mu x = 0$, allora $x^{m-1}(\alpha + \mu x) = 0 = \alpha x^{m-1}$, se $\alpha \neq 0$, α è invertibile, quindi l'unica possibilità è $\alpha = 0$. Pertanto $i(C,X;p) = dim_k(\frac{\mathcal{O}_p}{(f,g).\mathcal{O}_p}) \geq 2$ □

Concludiamo con un'applicazione (importante) riguardante le intersezioni complete.

Definizione 7.13: *Sia $Z \subseteq \mathbb{P}^2$ un insieme finito; Z è intersezione completa delle due curve F_a, F_b se $\mathbf{I}(Z) = (F_a, F_b)$.*

Osservazione 7.14:
(*i*) *Se $\mathbf{I}(Z) = (F_a, F_b)$ si dice che Z è un'intersezione completa di tipo (a,b). Se G è l'equazione di una curva di grado m contenente Z, allora $G = PF_a + RF_b$, per opportuni polinomi omogenei di grado $m-a$,$m-b$ ($degF_a = a$, $degF_b = b$).*
(*ii*) *Sia $Z = \{p_1, \ldots, p_d\}$ un insieme di d punti (nb: con questo si intende (ovviamente) che i p_i sono distinti: $p_i \neq p_j$ se $i \neq j$). Se $\mathbf{I}(Z) = (F_a, F_b)$ allora $F_a \cap F_b = Z$, e le due curve F_a, F_b sono trasversali (cioè sono lisce e hanno tangenti diverse) in ogni p_i; in particolare $d = ab$, vediamo adesso che vale anche il viceversa:*

Proposizione 7.15: *Sia $Z \subseteq \mathbb{P}^2$ un insieme di d punti ("distinti"), e siano F_a, F_b due curve (di gradi a, b) senza componenti comuni. Si assume$Z \subseteq F_a \cap F_b$. Allora Z è intersezione completa di F_a e F_b se e solo se $d = ab$.*

DIMOSTRAZIONE.
(*i*) Supponiamo $\mathbf{I}(Z) = (F_a, F_b)$, e prendiamo una carta affine (possiamo assumere che sia la carta $x_0 \neq 0$) contenente tutti i punti di Z; sia $\mathbb{I}(Z)^*$ l'ideale di $k[X,Y]$ ($X = \frac{x_1}{x_0}$, $Y = \frac{x_2}{x_o}$) generato dai deomogeneizzati dei generatori di $\mathbb{I}(Z)$. Abbiamo che $\mathbb{I}(Z)^*$ è l'ideale di tutti i polinomi che si annullano su Z (cf Es.). Dal teorema di Bezout: $dim_k(\frac{k[X,Y]}{(f_a,f_b)} = ab$, d'altra parte $dim_k(\frac{k[X,Y]}{(f_a,f_b)}) = dim_k(\frac{k[X,Y]}{\mathbb{I}(Z)^*}) = dim_k A(Z) = d$. Quindi $d = ab$.
(*ii*) Supponiamo $d = ab$ e $Z \subseteq F_a \cap F_b$. Poniamo $\mathbb{I} = (F_a, F_b)$; chiaramente $I \subset \mathbb{I}(Z)$. Prendiamo una carta affine (possiamo assumere che sia la carta $x_0 \neq 0$) contenente tutti i punti di $F_a \cap F_b$. L'inclusione $I_* \subseteq I(Z)_*$ induce una suriezione $\frac{R}{I_*} \to \frac{R}{\mathbb{I}(Z)_*}$ ($R = k[X,Y]$, $I_* = (f_a, f_b)$); inoltre $ab = dim_k(\frac{R}{I_*})$ per il teorema di Bezout, e $dim_k(\frac{R}{\mathbb{I}(Z)_*}) = d$, quindi $\frac{R}{I_*} \simeq \frac{R}{\mathbb{I}(Z)_*}$ (sono k-spazi vettoriali di dimensione finita), ossia $I_* = \mathbb{I}(Z)_*$.

Mostriamo adesso che questo implica, visto la scelta della carta affine, $I = \mathbb{I}(Z)$. Supponiamo $I \subset \mathbb{I}(Z)$, $I \neq BbbI(Z)$ e sia G un polinomio di grado minimo appartenente a $\mathbb{I}(Z)\backslash I$.
x_0 non divide G: se $G = x_0 G\prime$ allora $G\prime \in \mathbb{I}(Z)$ perchè x_0 non si annulla in nessun punto di Z. Se $G\prime \in I$ allora anche $G \in I$, quindi $G\prime \in \mathbb{I}(Z)\backslash I$. Questo è assurdo perchè $deg(G\prime) < deg(G)$.
Abbiamo $G_* \in \mathbb{I}(Z)_* = I_*$, quindi $G_* = hf_a + gf_b$. Pertanto $(G_*)^* = (hf_a + gf_b)^*$. Osserviamo che l'omogeneizzato di una somma, $r + s$, non è sempre la somma degli omogeneizzati (r^* e s^* potrebbero non avere lo stesso grado), in generale si avrà: $(r+s)^* = r^* + x_0^d s^*$, dove $d = deg(r^*) - deg(s^*)$; invece $(rs)^* = r^* s^*$. Detto ciò, segue che $(G_*)^* = x_0^d h^* F_a + g^* F_b$ (possiamo assumere che x_* non divida F_a e F_b). Siccome x_0 non divide G, $G = (G_*)^*$, e $G \in I$

□

Esercizi.

Esercizio 7.1: *Se X è una retta verificare che la definizione di $i(C, X; p)$ data in questo paragrafo è equivalente a quella data nella versione "debole" di Bezout.*

Esercizio 7.2: *(i) Se C e X sono trasversali in p allora $i(C, X; p) = 1$.*
(ii) Se C e X sono lisce e tangenti in p (cioè hanno la stessa tangente in p), allora $i(C, X; p) = 2$

Esercizio 7.3: *(i) Sia $C \subseteq \mathbb{P}^2$ una curva liscia. Dimostrare che C è irriducibile.*
(ii) Mostrare che per ogni $n \geq 1$, il polinomio $F_n(X, Y, Z) = X^n + Y^n - Z^n$ è irriducibile.

Esercizio 7.4: *Sia $C \subseteq \mathbb{P}^2$ una curva liscia di grado d. Calcolare (in funzione di d) il grado della curva duale $C^* \subseteq \mathbb{P}_2$.*

Esercizio 7.5: *Sia $X = \{p_1, \ldots, p_d\} \subseteq \mathbb{P}^2$. Si assume $X \subseteq U_0$. Mostrare che $\mathbb{I}(X)^* \subseteq k[X, Y]$ è l'ideale di tutti i polinomi che si annullano su $X \cap A^2 \simeq U_0$.*

Esercizio 7.6: *Non tutti gli insiemi di punti (distinti, come sempre) di $\mathbb{P}^2$ sono intersezione completa di due curve (potete giustificare questa affermazione?), ma "quasi" tutti sono insiemisticamente intersezione completa, cioè esistono due curve C, $C\prime$ tali che $C \cap C\prime = X$ (come insiemi, senza contare le molteplicità); in altri termini $\sqrt{(F, F')} = \mathbb{I}(X)$, dove F, $F\prime$ sono le equazioni di C, $C\prime$.*
(i) (formula di interpolazione di Lagrange) Siano $a_1, \ldots, a_n$ n elementi distinti del campo k. Allora $\forall\ (b_1, \ldots, b_n) \in k^n$, esiste un unico polinomio di grado $\leq n - 1$, $P(X) \in k[X]$, tale che $P(a_i) = b_i$, $1 \leq i \leq n$.

(ii) Sia $Q(X) \in k[X]$ un polinomio di grado m e consideriamo in $\mathbb{A}^2$ la curva di equazione $Y = Q(X)$. Dimostrare che la chiusura proiettiva di questa curva, $C \subseteq \mathbb{P}^2$, ha un punto di molteplicità $m - 1$ sulla retta all'infinito $Z = 0$. Determinare (in $\mathbb{P}^2$) l'intersezione della curva $Y = Q(X)$ con una retta "verticale" $X = \lambda$, $\lambda \in k$ (si può dedurre la prima parte da quest'ultima).
(iii) Sia $X = \{p_1, \ldots, p_r\} \subseteq \mathbb{P}^2$ un insieme di punti distinti in posizione lineare generale (cioè X non contiene tre punti allineati). Dimostrare che X è insiemisticamente intersezione completa (hint: assumere $p_1 = (0 : 1 : 0)$ e usare $(i), (ii)$).

Esercizio 7.7: *Sia $V \subset \mathbb{P}^4$ un'ipersuperficie liscia. Se V contiene un piano allora V è un iperpiano.*

(Questo è un caso particolare del teorema di Severi-Lefschetz che afferma che se $X \subset \mathbb{P}^n$ è una varietà proiettiva di dimensione ≥ 3, intersezione completa, allora ogni sottovarietà di X di codimensione uno localmente definita da un'equazione ("divisore (di Cartier)") è intersezione completa di X con un'ipersuperficie di $\mathbb{P}^n$.)

8. 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 8.1: *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 8.2: *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 $F_0, F_1, \ldots, F_r$ 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 cosi un 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 8.3: *Le curve di grado n che passano per un punto p formano un sistema lineare, e 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 $\geq N_n - \sum_{i=1}^{d} \frac{r_i(r_i+1)}{2}$. In particolare se $N_n - \sum_{i=1}^{d} \frac{r_i(r_i+1)}{2} \geq 0$ 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 8.4: *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 $\geq N_n - \sum_{i=1}^{d} \frac{r_i(r_i+1)}{2}$. In particolare se $N_n - \sum_{i=1}^{d} \frac{r_i(r_i+1)}{2} \geq 0$ 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 8.5: Per due punti passa sempre una retta, per 5 punti passa sempre una conica, per 9 punti passa sempre una cubica, ecc...

Osservazione 8.6: *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 8.7: *I punti $p_1, \dots, p_d$ impogono condizioni indipendenti alle curve di grado n se* $\dim \delta_n(p_1, \dots, p_d) = \max\{N_n - d, -1\}$ *(con la convenzione* $\dim \emptyset = -1$*).*

Esempio 8.8: (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 8.9: *("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 $p_1, \dots, p_d$ 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 (perchè 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 8.10: *Sia $X \subseteq \mathbb{P}^2$, $X = \{p_1, \dots, p_d\}$ 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 Es. 8.1).

Lemma 8.11: *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 8.12: *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 8.10. 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 8.13: *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 $n \geq 1$ (cf Esercizi); un tale insieme di punti si dice di* rango massimo.

8.1. 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) $r_X(n)$: $\mathbf{S}_n \to k^d$: $F \longmapsto (F_*(P_1), \ldots, F_*(P_d))$.

Lemma 8.14: *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. E' chiaro che $r_X(n)$ è k-lineare (perchè $(\lambda F + \mu G)_* = \lambda F_* + \mu G_*$), inoltre $r_X(n)(F) = 0$ se e solo se $F \in \mathbf{I}(X)_n$; si conclude perchè, per definizione, $A(X)_n = \frac{\mathbf{S}_n}{\mathbf{I}(X)_n}$ □

Osservazione 8.15: *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 8.16: *L'applicazione $h_X : \mathbb{N} \to \mathbb{N} : n \longmapsto \dim(Imr_X(n)) = \dim(A(X)_n)$ si chiama funzione di Hilbert dell'insieme di punti X.*

Osservazione 8.17:

(*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, $\delta_n(P_1, \ldots, P_d)$, delle curve di grado n che passano per $X = \{P_1, \ldots, P_d\}$ non è altro che $\mathbb{P}(\mathbf{I}(X)_n) \subseteq \mathbb{P}(\mathbf{S}_n)$, $h_X(n)$ è la codimensione di $\delta_n(P_1, \ldots, P_d)$ in $\mathbb{P}(\mathbf{S}_n)$ (cioè il numero di condizioni imposte dai punti $P_1, \ldots, P_d$ 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:*

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

(1) *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 8.18: *Sia* $X \subseteq \mathbb{P}^2$, $X = \{P_1, \ldots, P_d\}$, *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*) E' una semplice traduzione.

(*ii*) Anche questa è una traduzione ma diamo una dimostrazione in questo contesto: se $r_X(n)$ è suriettiva $(0, \ldots, 1, \ldots, 0)$ (1 al posto i, 0 altrimenti) appartiene a $\mathrm{Im}(r_X(n))$ per ogni i, quindi esiste F_i tale che $r_X(F_i) = (0, \ldots, 1, \ldots, 0)$: 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 $(0, \ldots, a_i, \ldots, 0) \in \mathrm{Im}(r_X(n))$, 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 8.19: *Ci sono quindi un numero finito di casi da considerare per determinare la funzione di Hilbert di un insieme di punti.*

8.2. 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 8.20: *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 nè 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 $R \cap X = \{P_2, P_3\}$ perchè X non contiene tre punti allineati. I cinque punti $P_4, \dots, P_8$ sono contenuti in una conica, C. Abbiamo $C \cap X = \{P_4, \dots, P_8\}$ perchè X non contiene sei punti su una conica. La cubica $C \cup R$ passa per $X\backslash\{P_1\}$ e non contiene P_1. E' 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 (perchè non contengono 4 punti allineati). Pertanto $\dim(\mathbf{I}(X'))_3 = 1$, cioè X' impone condizioni indipendenti alle cubiche, quindi (cf Cor. 8.10) anche X impone condizioni indipendenti alle cubiche.

(iii) 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

□

Proposizione 8.21: *("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 $X = \{P_1, \ldots, P_8\}$. 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 $F(P_9) = \lambda F_3(P_9) + \mu F_3'(P_9) = 0$ □

Osservazione 8.22: *Ogni insieme "generico", $X \subset \mathbb{P}^2$, di otto punti verifica* $\dim(\mathbf{I}(X)_3) = 2$ *e quindi il sistema lineare $\delta_3(P_1, \ldots, P_8)$ 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 8.23: *Con le notazioni precedenti: P, Q, R sono allineati se e solo se $v_1, \ldots, v_6$ sono su una conica.*

DIMOSTRAZIONE. Da ognuno dei punti P, Q, R escono due rette della figura, scegliendo opportunatamente una retta per ogni punto realizziamo i nove punti $v_1, \ldots, v_6, P, Q, R$ come l'intersezione completa di due cubiche:
$C \cap C' = \{v_1, \ldots, v_6, P, Q, R\}$, 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 $v_1, \ldots, v_5$ (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 Prop. 8.21, $K \cap L$ contiene anche v_6, questo implica $v_6 \in K$ (perchè $v_6 \notin L$?).

(*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 $R \in L$ (perchè $R \notin K$?)

□

Esercizi.

Esercizio 8.1: *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 8.2: *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 8.3: *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 8.4: *L'anello $S = k[X_0, \ldots, X_n]$ è un anello graduato: $S = \bigoplus_{i \geq 0} S_i$ dove S_i è l'insieme dei polinomi omogenei di grado i. Un S-modulo graduato è un S-modulo, M, tale che $M = \bigoplus M_t$, dove M_t è un gruppo abeliano e dove $S_i M_t \subseteq M_{t+i}$, per ogni i, t. In particolare ogni M_t è un S_0-modulo, cioè un k-spazio vettoriale. Se $M = \bigoplus M_t$, $N = \bigoplus N_t$ sono due S-moduli graduati, un morfismo di grado p, $j : M \to N$, è un morfismo 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 S in se stesso: $S \to S : F \longmapsto PF$. Per fare diventare questo morfismo di grado zero s'introduce l'S-modulo graduato $S(-p)$ definito da $S(-p)_t = S_{t-p}$; come S-modulo $S(-p)$ è isomorfo a S, è cambiata solo la graduazione. La moltiplicazione per P induce adesso un morfismo di grado zero $S(-p) \to S$.*

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 S-moduli graduati (con morfismi di grado zero):

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

dove l'applicazione $S(-a-b) \to S(-a) \oplus S(-b)$ è data da $F \longmapsto (F_b F, F_a F)$, e dove l'applicazione $S(-a) \oplus S(-b) \longmapsto \mathbf{I}(X)$ 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 8.5: *Sia $d = 6$. Determinare tutte le possibili funzioni di Hilbert di un insieme di d punti distinti di $\mathbb{P}^2$.*

Esercizio 8.6: *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; $H(d)$ paramettrizza i sottinsiemi 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 8.7: *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 (sugg: 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 (perchè 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 8.8: *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 $j : \mathbb{P}^2 \to \mathbb{P}(S_2^*) : x \longmapsto H_x$, dove H_x è l'iperpiano di 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 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 $a_0^2X^2 + a_1^2Y^2 + \ldots +$ $a_1a_2YZ = 0$ (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 $\mathbb{P}^5$.

CAPITOLO III

Cubiche piane, curve ellittiche: geometria e aritmetica.

1. Legge di gruppo sulle cubiche piane lisce.

Sia $C \subset \mathbb{P}^2$ una cubica liscia. Se R è una retta di $\mathbb{P}^2$, dalla versione debole del teorema di Bezout segue che R interseca C in tre punti contati con molteplicità. Abbiamo quindi le seguenti possibilità:
(1) $C \cap R$ consta di tre punti, cioè R è trasversale a C in ogni punto di $C \cap R$:

Questo è il caso generico.
(2) R è tangente a C e $C \cap R$ consta di due punti:

(3) R è una tangente di flesso: $C \cap R$ consta di un unico punto, p, R è la tangente a C in p, e $i(C, R; p) = 3$. In questa situazione si dice che p è un *flesso* di C. Questa è la situazione più speciale.

Il terzo punto: Se a, b sono due punti di C notiamo $[ab]$ il terzo punto di $C \cap R$ dove R è la retta passante per a e b: $C \cap R = \{a, b, [ab]\}$. Osservare che se R è tangente a C in a (risp. b) allora $[ab] = a$ (risp. b). In particolare se $a = b$, $[aa]$ è il terzo punto di $C \cap R$ dove R è la tangente a C in a (abusando le notazioni: $C \cap R = \{2a, [aa]\}$. Il punto a è un punto di flesso se e solo se $[aa] = a$. Adesso fissiamo un punto $O \in C$ e definiamo una legge di composizione interna ("addizione") su C:

Definizione 1.1: *Siano p, q due punti di C, allora $p + q := [O, [pq]]$, cioè $p + q$ è il terzo di $C \cap R$ dove R è la retta generata da O e $[pq]$: $C \cap R = \{O, [pq], p + q\}$.*

Questo definisce una legge di composizione interna: $C \times C \to C : (p, q) \to p+q$. Vogliamo mostrare che $(C, +)$ è un gruppo abeliano.

Lemma 1.2: *Con le notazioni precedenti abbiamo: (i) Per ogni $(p, q) \in C^2$, $p+q = q + p$*
(ii) Per ogni $p \in C$, $p + O = O + p = O$
(iii) Per ogni $p \in C$, esiste $-p \in C$ tale che $p + (-p) = (-p) + p = O$.

DIMOSTRAZIONE. (i) , (ii): chiaro.
(iii) Sia $O' := [OO]$ (O' è il terzo punto di $T \cap C$ dove T è la tangente a C in O). Per ogni punto p poniamo $-p := [pO']$. Si verifica facilmente che $-p$ è il simmetrico di p. □

Rimane quindi da mostrare che $+$ è associativa: questa è la parte difficile. Si tratta qundi di mostrare che $(a+b)+c = a+(b+c)$, per ogni terna (a,b,c) di punti di C. Calcoliamo $(a+b)+c$:

Abbiamo $s' = (a+b)+c$. Se calcoliamo $t' = (b+c)+a(= a+(b+c))$, nello stesso modo (scambiando a,b con b,c) otteniamo dei punti q, q', t, t' (corrispondenti a r, r', s, s'). In ognuna di queste due costruzioni compaiono quattro rette, e possiamo riassumere la situazione nel modo seguente:

$$\begin{array}{cccc} L_1 & L_2 & L_3 & L_4 \\ abr & cr's & r'Or & Os's \end{array}$$

L_1 è la retta passante per a, b e r, ecc (cf figura).
In modo analogo nella seconda costruzione avremo quattro rette D_i con i relativi punti $D_i \cap C$:

$$\begin{array}{cccc} D_1 & D_2 & D_3 & D_4 \\ bcq & aq't & q'Oq & Ot't \end{array}$$

Vogliamo dimostrare che $t' = s'$, per questo basta fare vedere che $s = t$. Sia $F = L_1 \cup L_2 \cup D_3$, e $G = D_1 \cup D_2 \cup L_3$. Abbiamo:
$F \cap C = \{a, b, c, r, r', q', O, q, s\}$
$G \cap C = \{a, b, c, r, r', q', O, q, t\}$.
Supponiamo i punti distinti. Gli otto punti a, b, c, r, r', q', O, q, sono otto dei nove punti dell'intersezione completa delle due cubiche F, C. Per la Proposizione 13 del 3, ogni cubica passante per questi otto punti deve passare anche per il punto s. In particolare G deve passare per s. Questo implica $s = t$. Abbiamo dimostrato l'associatività se tutti i punti a, b, c, r, r', q', O, q sono distinti. Come concludere in generale? Ci accontenteremo di alcuni cenni:
(1) Con la nozione di schema si può dimostrare Prop. 13 del 3 senza assumere i punti distinti, si può allora ripetere il ragionamento precedente in tutta generalità (teoria della "liaison").
(2) I seguenti due fatti sono intuitivamente chiari, anche se un pò noiosi da dimostrare:
(i) L'addizione $j : C \times C \to C : (a,b) \to a+b$ è un'applicazione continua
(ii) $\forall (a,b,c) \in C^3$, $\exists (a',b',c') \in C^3$ arbitrariamente vicino a (a,b,c) tale che i nove punti $a', b', c', O, r', r, q', q, s'$ siano distinti.
Consideriamo $f = j \circ (j \times id) : C \times C \times C \to C \times C \to C : (a,b,c) \to (a+b,c) \to (a+b)+c$,
$g = j \circ (id \times j) : C \times C \times C \to C \times C \to C : (a,b,c) \to (a,b+c) \to a+(b+c)$, Da

(i) segue che f, g sono due applicazioni continue. Sia $U = \{(a, b, c) \in C^3 \mid$ i nove punti corrispondenti siano distinti$\}$. Per (ii), U è denso in C^3. Le applicazioni continue f, g coincidono sull'aperto denso U, e quindi coincidono dappertutto. Infatti, se $k = \mathbb{C}$, (i) e (ii) sono veri con la topologia trascendente (usuale), e possiamo applicare il seguente risultato:

" Siano X, Y due spazi topologici, con Y di Hausdorff, $f, g : X \to Y$ due applicazioni continue. Se esiste un aperto denso, U, di X tale che: $f(x) = g(x), \forall x \in U$, allora $f = g$."

Dimostrazione. Sia $E = \{x \in X \mid f(x) = g(x)\}$. Allora E è chiuso in X. Infatti consideriamo $\varphi : X \to Y \times Y : x \to (f(x), g(x))$. L'applicazione φ è continua (per la topologia prodotto su $Y \times Y$). Sia $D = \{(y, y') \in Y^2$
$: y = y'\}$ la diagonale di Y. Siccome Y è di Hausdorff, D è un chiuso di $Y \times Y$ (per la topologia prodotto). Abbiamo $E = \varphi^{-1}(D)$. Quindi E è chiuso in X. D'altra parte $U \subset E$, quindi $X = \overline{U} = E$; pertanto $E = X$. □

Nel caso generale (k qualsiasi, topologia di Zariski) si può ragionare in modo analogo perchè φ è continua e perchè $D \subset C \times C$ è chiusa (per la topologia di Zariski su $C \times C$); infatti: (a) $C \times C$ è chiuso in $\mathbb{P}^2 \times \mathbb{P}^2$, (b) la diagionale di $\mathbb{P}^2 \times \mathbb{P}^2$ è chiusa in $\mathbb{P}^2 \times \mathbb{P}^2$ (esercizio). Vedremo queste cose più dettagliatamente quando parleremo di varietà prodotto (**??**).
Cogliamo l'occasione per osservare il fatto seguente: anche se la topologia su $Y \times Y$ non è la topologia prodotto, il fatto che la diagonale sia chiusa in $Y \times Y$, ci permette di ragionare come nel caso Hausdorff. Questo introduce la nozione di varietà algebrica separata: "una varietà algebrica Y è separata se la diagonale di $Y \times Y$ è chiusa in $Y \times Y$ (qui $Y \times Y$ è il prodotto nella categoria delle varietà algebriche)."

(3) Data un'equazione di $C \subset \mathbb{P}^2$ possiamo ricavare un'espressione analitica ("equazioni") dell'addizione, e verificare, analiticamente, che si tratta effettivamente di una legge di gruppo. Riprenderemo questo punto di vista più avanti. Comunque sia, abbiamo una struttura di gruppo abeliano sulla cubica liscia $C \subset \mathbb{P}^2$. Questa legge di gruppo ha una proprietà notevole: è algebrica. Ossia i morfismi:
$C \times C \to C : (a, b) \to a + b$
$C \to C : a \to -a$
sono dei morfismi di varietà algebriche. Questa affermazione è ragionevole in quanto questi morfismi sono definiti da costruzioni algebro-geometriche (cf dimostrazione del lemma 8, 2).

Definizione 1.3: *Un gruppo algebrico è un insieme algebrico, G, munito di una struttura di gruppo tale che $GxG \to G : (x, y) \to xy$, $G \to G : x \to x^{-1}$ siano dei*

morfismi algebrici.
Una varietà abeliana è una varietà proiettiva con una struttura di gruppo algebrico.

Osservazione 1.4: *(i) La definizione di gruppo algebrico è simile a quella di gruppo topologico, con una differenza però: la topologia su $G\times G$ non è la topologia prodotto; un gruppo algebrico non è un gruppo topologico (tranne in dimensione zero). Infatti un gruppo topologico è T2 mentre un gruppo algebrico non lo è.*
(ii) Si dimostra che la struttura di gruppo di una variet abeliana è sempre commutativa.
(iii) Un gruppo algebrico si dice affine (o lineare) se G è un sottoinsieme algebrico affine.
(iv) Un gruppo algebrico è sempre nonsingolare ($Sing(G)$ è un chiuso proprio, quindi esiste un punto liscio $x \in G$, se $y \in G$ sia $z := x^{-1}y$ allora $y = t_z(x)$ dove $t_z : G \to G$ è la traslazione utouz. Siccome t_z è chiaramente un isomorfismo e siccome x è liscio, anche y è liscio).
(v) Una varietà abeliana di dimensione uno si dice anche curva ellittica. Quindi ogni cubica liscia è una curva ellittica. Si dimostra che se X è una curva ellittica allora esiste $f : X \to \mathbb{P}^2$ tale che $f(X)$ sia una cubica liscia, con f un isomorfismo.

Scelta dell'origine.

Concludiamo questo paragrafo con alcune osservazioni sulla scelta dell'origine O per la struttura di gruppo su una cubica piana liscia. Supponiamo che O sia un punto di flesso di C (la tangente a C in O incontra C in "tre" volte O). Mostriamo che in questo caso le costruzioni geometriche sono semplificate.

Intanto $O' = [OO] = O$, pertanto $-a = [O'a] = [Oa]$.
Abbiamo poi:

Lemma 1.5: *(i) Se O è un punto di flesso allora per ogni $(p, q, r) \in C^3 : p+q+r = O$ se e solo se p, q, r sono allineati.*
(ii) p è un punto di flesso se e solo se $3p = O$
(iii) Se p e q sono due flessi allora il "terzo" punto $r := [pq]$ è anch'esso un flesso.

Dimostrazione. Esercizio. □

Usando il teorema di Bezout si può dimostrare che una cubica liscia ammette sempre almeno un flesso.

Conica osculatrice ad una curva piana in un punto liscio:

In quanto segue, per maggiore tranquilità, si assumerà il campo di caratteristica zero.
Sia $C \subset \mathbb{P}^2$ una curva (di grado $d > 1$), di equazione $F(X_0, X_1, X_2) = 0$, $p \in C$ un punto liscio di C, e T la tangente a C in p. Il punto p è un punto di flesso se $i(C, T; p) > 2$.
Sia $q \in T, q \neq p$, abbiamo: $F(p + \lambda q) = F(p) + DF(p).(\lambda q) + \frac{1}{2}D^2F(p).(\lambda q)^2 + \cdots$
Tenuto conto che $p \in C$ e $q \in T$, questa espressione si riduce a:
$F(p+\lambda q) = \lambda^2[\sum_{ij} F_{ij}(p)q_iq_j] + \lambda^3[\cdots]$, dove F_{ij} indica la derivata parziale seconda rispetto a X_i e X_j. Abbiamo quindi:

Lemma 1.6: *Con le notazioni precedenti:*
p è un punto di flesso se e solo se $i(C, T; p) > 2$, cioè se e solo se $\sum_{ij} F_{ij}(p)q_iq_j = 0$ per ogni punto $q \in T$.

Definizione 1.7: *La conica, Γ_p, di equazione $\sum_{ij} F_{ij}(p)X_iX_j = 0$, è la conica osculatrice a C in p.*

Osservazione 1.8: *Possiamo riformulare il Lemma 1.6 nel modo seguente: p è un punto di flesso se e solo se la tangente T è una componente della conica osculatrice Γ_p.*

Proposizione 1.9: *Con le notazioni precedenti:*
(i) $p \in \Gamma_p$ e p è un punto liscio di Γ_p.
(ii) La tangente a Γ_p in p è T.
(iii) p è un punto di flesso di C se e solo se Γ_p è degenere.

Dimostrazione. Abbiamo $\sum_{ij} F_{ij}(p)p_jr_i = (\sum_j F_{0j}(p)p_j)r_0 + (\sum_j F_{1j}(p)p_j)r_1 + (\sum_j F_{2j}(p)p_j)r_2$. Usando la relazione di Eulero: $\sum_{ij} F_{ij}(p)p_jr_i = (d-1).[F_0(p)r_0 + F_1(p)r_1 + F_2(p)r_2]$. In particolare:

$$(*) \quad \sum_{ij} F_{ij}(p)p_jr_i = 0 \Leftrightarrow (r_0 : r_1 : r_2) \in T$$

Da $(*)$ segue immediatamente che $p \in \Gamma_p$. Dire che p è un punto singolare della conica Γ_p è equivalente a dire che la retta vettoriale $< p >$ di k^3 è nell'ortogonale $(k^3)^\perp$ (ortogonalità per la forma bilineare simmetrica associata alla matrice $A = (F_{ij}(p))$); cioè che $\sum_{ij} F_{ij}(p)p_jr_i = 0$, per ogni $(r_0 : r_1 : r_2)$, mentre da $(*)$ segue che questo è verificato solo se $(r_0 : r_1 : r_2) \in T$. Questo dimostra (i).
(ii) Se p è un punto liscio della conica $\sum_{ij} a_{ij}X_iX_j = 0$, la tangente alla conica in

p ha equazione $\sum_{ij} a_{ij}p_iX_j = 0$ (Esercizio).
(iii) Se p è un flesso di C allora T è una componente di Γ_p (Osservazione 1.8), e quindi Γ_p è degenere. Viceversa se Γ_p è degenere, da (i) segue che Γ_p è l'unione di due rette distinte: $\Gamma_p = R \cup D$, e, diciamo, $p \in R \setminus (R \cap D)$ (perchè p è un punto liscio di Γ_p). Da (ii) segue che $T = R$, e quindi (Osservazione 1.8) p è un flesso di C. □

Curva Hessiana e flessi:

Manteniamo le notazioni precedenti. Sia $H(F)$ la matrice simmetrica, tre per tre, a coefficienti le derivate parziali seconde di F: $H(F) = (F_{ij}(x))$. Il determinante di $H(F)$ è un polinomio omogeneo di grado $3(d-2)$.

Definizione 1.10: *La curva $H(C) \subset \mathbb{P}^2$, di equazione $det(H(F)) = 0$, si chiama la curva Hessiana di C.*

Teorema 1.11: *Sia $C \subset \mathbb{P}^2$ una curva. I flessi di C sono esattamente i punti lisci di C che appartengono a $C \cap H(C)$.*

Dimostrazione. Sia $p \in C$ un punto nonsingolare. Abbiamo visto (Proposizione 1.9,(iii)): p è un flesso se e solo se Γ_p è degenere. Ma Γ_p è degenere se e solo se $|F_{ij}(p)| = 0$, cioè $p \in H(C)$. □

Corollario 1.12: *Ogni curva liscia $C \subset \mathbb{P}^2$ di grado $d \geq 3$ ammette almeno un flesso.*

Dimostrazione. Basta mostrare $C \cap H(C) \neq \emptyset$. Se C e $H(C)$ hanno una componente in comune, questa componente è C. Se C e $H(C)$ non hanno componenti comuni, dal teorema di Bezout, C e $H(C)$ si intersecano in $3d(d-2) > 0$ punti contati con molteplicità. □

Osservazione 1.13: *(i) Una curva di grado 2 non ha flessi.*
(ii) Dalla dimostrazione precedente risulta che se C è una cubica liscia allora $C = H(C)$ o C ha al più 9 flessi. Vedremo in effetti che ogni cubica liscia ha esattamente 9 flessi (cfr anche Es.3).
(iii) In realtà il Corollario 1.12 si può dimostrare senza il teorema di Bezout: basta sapere che due curve di $\mathbb{P}^2$ s'intersecano sempre. Il teorema di Bezout permette di stimare il numero di flessi.

Esercizi.

Esercizio 1.1: *Dimostrare il Lemma 1.5.*

Esercizio 1.2: *Sia $K \subset \mathbb{P}^2$ la conica di equazione $F(x_0, x_1, x_2) = a_{00}x_0^2 + a_{11}x_1^2 + a_{22}x_2^2 + 2a_{01}x_0x_1 + 2a_{02}x_0x_2 + 2a_{12}x_1x_2 = 0$. Si assume $ch(k) \neq 2$.*
Sia M la matrice simmetrica tre per tre: $M = (a_{ij})$, di modo che $F(x_0, x_1, x_2) = {}^tX.M.X$, dove ${}^tX = (x_0, x_1, x_2)$. Siano inoltre R_0, R_1, R_2 le righe della matrice M.
(i) Osservare che $F_i(x_0, x_1, x_2) = 2.(R_i|X)$ (F_i è la derivata parziale rispetto a x_i, $(\cdot|\cdot)$ è il prodotto scalare). Concludere che se p è un punto liscio di K, la tangente a K in p ha equazione $\sum_{ij} a_{ij}p_ix_j = 0$.
(ii) La conica K è non singolare se e solo se $det(M) \neq 0$ (cioè la forma bilineare simmetrica su k^3 di matrice M è non degenere).
(iii) Sia $f : k^3 \times k^3 \to k$ la forma bilineare simmetrica tale che $mat_B(f) = M$ (B la base canonica). Si assume $det(M) \neq 0$. Sia v un vettore non isotropo ($f(v, v) \neq 0$) allora $< v >^\perp$ ha dimensione due. Quindi $< v >^\perp$ corrisponde in $\mathbb{P}^2$ a una retta, R. La retta R interseca K in due punti, a_1, a_2. Mostrare che $a_1 \neq a_2$ e che la tangente a K in a_1 (risp. a_2) passa per il punto $p = \mathbb{P}(< v >)$. La retta R è la polare *del punto p rispetto alla conica K.*
Cosa succede se $p \in K$? (cioè se v è isotropo)
(iv) Dimostrare che K^* (la curva duale) è una conica liscia, e che $K^{**} = K$.

Esercizio 1.3: *Sia $C \subset \mathbb{P}^2(\mathbb{C})$ una curva piana irriducibile di grado > 1. Mostrare che C ha un numero finito di flessi. (hint: ci si riconduce al caso affine, se $p(x_0, y_0) = 0$ e $p_y(x_0, y_0) \neq 0$, dal teorema delle funzioni implicite, esistono degli intorni aperti (nella topologia trascendente) U, V di x_0, y_0 in $\mathbb{C}$, e una funzione olomorfa $f : U \to V$ tale che per $(x, y) \in U \times V : y = f(x) \Leftrightarrow p(x, y) = 0$. Quindi, localmente nella topologia usuale, C è data dal grafico di f. Osservare che un punto $(x, f(x))$ è di flesso per C se e solo se $f"(x) = 0$ e concludere)(hint^2: dualità).*

2. Classificazione delle cubiche piane nonsingolari.

Forme di Weierstrass e di Legendre:

Teorema 2.1: *Sia k un campo algebricamente chiuso, con $ch(k) \neq 2$. Sia $C \subset \mathbb{P}^2$ una cubica (non necessariamente liscia). Si suppone che C ammette un flesso. Allora C è proiettivamente equivalente ad una cubica di equazione $Y^2Z - F(X,Z) = 0$, dove F è un polinomio omogeneo di grado tre.*

Dimostrazione. Per ipotesi C ammette un flesso, p. Con una proiettività possiamo trasformare il punto p nel punto $(0:1:0)$ e $T_p(C)$ nella retta $Z = 0$. L'equazione di C è del tipo $a_0X^3 + X^2(a_1Y + a_2Z) + X(a_3Y^2 + a_4YZ + a_5Z^2) + a_6Y^3 + a_7Y^2Z + a_8YZ^2 + a_9Z^3$. Nell'aperto affine $U_y \simeq \mathbb{A}^2$, C è data da $f(x,z) = a_0x^3 + x^2(a_1 + a_2z) + x(a_3 + a_4z + a_5z^2) + a6 + a_7z + a_8z^2 + a_9z^3 = a_6 + (a_7z + a_3x) + (a_1x^2 + a_4xz + a_8z^2) + (a_0x^3 + a_2x^2z + a_5xz^2 + a_9z^3)$. Poichè $p \in C$, $f(0,0) = 0$ ossia $a_6 = 0$. Inoltre siccome $T_p(C) = \{Z = 0\}$, la tangente nell'origine di $\mathbb{A}^2$ ha equazione $z = 0$, quindi $a_3 = 0$ (e $a_7 \neq 0$ perchè p è un punto nonsingolare di C). Finalmente p essendo un flesso la tangente nell'origine ha conttato ≥ 3 con la curva, ossia $a_1 = 0$. Quindi l'equazione diventa: $f(x,y) = a_7z + a_4xz + a_8z^2 + A"(x,z)$. Siccome $a_7 \neq 0$, dividendo per a_7, possiamo ricondurci ad un'equazione del tipo: $f(x,y) = z + sxz + tz^2 + A'(x,z)$. L'equazione omogenea della nostra curva $C \subset \mathbb{P}^2$ è del tipo:

$$Y^2Z + sXYZ + tYZ^2 + A'(X,Z) = Z(Y^2 + sXY + tYZ) + A'(X,Z) \quad (*)$$

Siccome $ch(k) \neq 2$, possiamo ridurre la forma quadratica $Y^2 + sXY + tYZ$ col metodo di Gauss:

$$Y^2 + sXY + tYZ = Y(Y + sX + tZ) = (Y + \frac{s}{2}X + \frac{t}{2}Z)^2 - (\frac{s}{2}X + \frac{t}{2}Z)^2$$

Quindi ponendo $Y' = Y + \frac{s}{2}X + \frac{t}{2}Z$, l'equazione $(*)$ diventa:

$$F(X,Y',Z) = ZY'^2 - Z(\frac{s}{2}X + \frac{t}{2}Z)^2 + A'(X,Z)$$

ossia: $F(X,Y',Z) = ZY'^2 + A(X,Z)$ con $A(X,Z)$ omogeneo di grado tre. □

Osservazione 2.2: *Nel teorema precedente non si assume C nonsingolare.*

Corollario 2.3: *Si assume $ch(k) \neq 2,3$ (e k algebricamente chiuso, come sempre). Sia $C \subset \mathbb{P}^2$ una cubica nonsingolare.*
(i) C è proiettivamente equivalente ad una curva di equazione $Y^2Z = X(X - Z)(X - \lambda Z)$, con $\lambda \neq 0, 1$ (forma di Legendre).
(ii) C è proiettivamente equivalente ad una curva di equazione: $Y^2Z = X^3 + aXZ^2 + bZ^3$, con $4a^3 + 27b^2 \neq 0$ (forma di Weierstrass).

DIMOSTRAZIONE. Siccome C è nonsingolare, C ammette almeno un flesso (Corollario 1.12), pertanto dal teorema precedente C è proiettivamente equivalente a una curva di equazione $Y^2Z - F(X,Z) = 0$.
(i) Nell'aperto affine U_Z, C è data dall'equazione $y^2 - F(x,1) = y^2 - (ax^3 + bx^2 + gx + d) = 0$. Abbiamo $a \neq 0$ (altrimenti $Z|Y^2Z - F(X,Z)$ e C sarebbe riducibile, quindi singolare cfr II.3, Es.3). Il polinomio $f(x) = F(x,1)$ ha tutte le sue radici in k e queste radici sono distinte. Infatti se ξ è radice multipla di f allora $(x-\xi)^2|f(x)$, e il punto di $\mathbb{A}^2$ di coordinate $(\xi,0)$ è un punto singolare di C, ma questo è escluso per ipotesi. Sia quindi $f(x) = a(x-r_1)(x-r_2)(x-r_3)$, con $r_i \neq r_j$ se $i \neq j$. Poniamo $x = (r_2 - r_1)x' + r_1$, $y = [a(r_2 - r_3)^3]^{1/2}.y'$. Con questo cambiamento di variabili l'equazione diventa: $y'^2 = x'(x'-1)(x'-\lambda)$ con $\lambda = (r_3 - r_1)/(r_2 - r_1)$. In forma omogenea: $Y^2Z' = X'(X' - Z')(X' - \lambda Z')$. Finalmente $\lambda \neq 0$ (perchè $r_3 \neq r_1$), e $\lambda \neq 1$ (perchè $r_2 \neq r_3$).
(ii) Come prima consideriamo l'equazione affine $y^2 = ax^3 + bx^2 + gx + d$. Abbiamo già osservato che $a \neq 0$. Dividendo per a: $y'^2 = (y/\sqrt{a})^2 = x^3 + bx^2 + cx + d$. Si tratta adesso di fare sparire il termine in x^2 per "completamento del cubo": questo è possibile perchè $ch(k) \neq 3$. Infatti ponendo $x = (x' - b)/3$, l'equazione diventa: $y'^2 = (x'-b)^3/27 + b(x'-b)^2/9 + c(x'-b)/3 + d$, ossia: $27y'^2 = x'^3 - 3bx'^2 + 3b^2x' - b^3 + 3b(x'^2 + b^2 - 2bx') + 9c(x'-b) + 27d$, cioè un'espressione della forma: $y'^2 = x'^3/27 + x'A'/3 + B = (x'/3)^3 + A(x'/3) + B$. Ponendo $x" = x'/3$ si arriva alla forma cercata. Come prima si vede che il polinomio $\varphi(x) = x^3 + Ax + B$ ha radici distinte (altrimenti C sarebbe singolare). Questo è equivalente a $Disc(\varphi) \neq 0$, dove il discriminante $Disc(\varphi)$ è il risultante di φ e φ' (cf Es.1). Si verifica che $Disc(\varphi) = -4A^3 - 27B^2$. □

Lemma 2.4: *Sia $C \subset \mathbb{P}^2$ una cubica liscia e $p \in C$ un punto di flesso. Ci sono esttamente quattro tangenti a C passanti per p.*

DIMOSTRAZIONE. Con una proiettivit possiamo trasformare C in una curva di equazione $F(X,Y,Z) = 0$ dove $F(X,Y,Z) = Y^2Z - X(X-Z)(X-\lambda Z)$, $\lambda \neq 0, 1$, e p nel punto $(0:1:0)$. Le tangenti a C passanti per p sono le quattro rette: $Z = 0$, $X = 0$, $X = Z$, $X = \lambda Z$. Infatti la tangente a C in un punto q ha equazione $F_X(q).X + F_Y(q).Y + F_Z(q).Z = 0$, questa retta passa per p se e solo se $F_Y(q) = 0$; se $q = (x:y:z)$, questo è equivalente a $yz = 0$. Se $y = 0$, deve essere $x(x-z)(x-\lambda z) = 0$ (perchè $q \in C$), e quindi q è uno dei tre punti $p_1 = (0:0:1)$, $p_2 = (1:0:1)$, $p_3 = (l:0:1)$. Se $z = 0$, inserendo nell'equazione di C, si ricava $x = 0$, cioè $q = p$. Si verifica poi che le tangenti nei punti p_i trovati sono quelle annunciate, e che passano per p. □

Manteniamo le notazioni della dimostrazione precedente: C è una cubica liscia di equazione $Y^2Z = X(X-Z)(X-\lambda Z)$, $p = (0:1:0)$. Il lemma precedente fornisce quattro tangenti a C che passano per il punto p. Queste quattro rette danno

quattro punti nel $\mathbb{P}^1$ isomorfo al fascio di rette passanti per p (in altri termini sia L una retta non passante per p allora le quattro tangenti intersecano L in quattro punti distinti). Questi quattro punti di $\mathbb{P}^1$ hanno un modulo (cf I.9, Teo.3), questo modulo è uguale a $j(\lambda) = (\lambda^2 - \lambda + 1)/\lambda^2(\lambda - 1)^2$ (prendere per L la retta $Y = 0$); diciamo che questo modulo è il modulo delle quattro tangenti passanti per il flesso p.

Lemma 2.5: *Sia $C \subset \mathbb{P}^2$ una cubica liscia. Il modulo delle quattro tangenti passanti per un flesso di C non dipende dal flesso.*

DIMOSTRAZIONE. Siano p, p' due flessi di C. Con una proiettività possiamo mandare p' su p. La proiettività induce una proiettività tra il fascio di rette per p' e il fascio di rette per p, in questa proiettività le quattro tangenti si corrispondono (per esempio perchè una proiettivit di $\mathbb{P}^2$ conserva la molteplicità d'intersezione di due curve); si conclude con I.9, Teo.3. □

Quindi il modulo delle quattro tangenti per un flesso della cubica C non dipende dal flesso scelto, ma solo dalla curva.

Definizione 2.6: *Il modulo, $j(C)$, di una cubica liscia, C, di $\mathbb{P}^2$ è il modulo delle sue quattro tangenti passanti per un suo punto di flesso.*

Teorema 2.7: *(i) Due cubiche lisce di $\mathbb{P}^2$ sono proiettivamente equivalenti se e solo se hanno lo stesso modulo.*
(ii) L'insieme delle cubiche lisce di $\mathbb{P}^2$ modulo equivalenza proiettiva è in biiezione con il campo k.

DIMOSTRAZIONE. (i) Se due cubiche sono proiettivamente equivalenti allora hanno lo stesso modulo (perchè una proiettivit conserva la molteplicità d'intersezione in un punto, quindi trasforma flessi in flessi e tangenti in tangenti). Viceversa se C e C' hanno lo stesso modulo allora C è proiettivamente equivalente a una curva di equazione $Y^2Z = X(X - Z)(X - \lambda Z)$ mentre C' è proiettivamente equivalente a una curva di equazione $Y^2Z = X(X - Z)(X - \lambda' Z)$ con $\lambda' \in \{\lambda, 1/\lambda, 1 - \lambda, 1/(1 - \lambda), (\lambda - 1)/\lambda, \lambda/(\lambda - 1)\}$, $\lambda, \lambda' \neq 0, 1$. Si tratta in ogni caso di trovare una proiettività che trasforma un'equazione nell'altra. Per esempio ponendo $x = \lambda x'$, $y = \lambda^{3/2} y'$ nella prima equazione (in affine) si ricava $y'^2 = x'(x' - 1)(x' - 1/\lambda)$; invece se $x = 1 - x'$, $y = iy'$ (i radice quadrata di -1), si ottiene $y'^2 = x'(x' - 1)(x' - (1 - \lambda))$. Si conclude combinando queste proiettività.
(ii) Basta mostrare che per ogni $j \in k$ esiste una cubica liscia C con $j(C) = j$. Siccome k è algebricamente chiuso, l'equazione $jX^2(X - 1)^2 - (X^2 - X + 1)^3 = 0$ ammette una soluzione, $\lambda \in k$. Necessariamente $\lambda \neq 0, 1$. La cubica di equazione $y^2 = x(x - 1)(x - \lambda)$ è non singolare e ha modulo j. □

Osservazione 2.8: *Il Teorema 2.7 risolve il problema della classificazione proiettiva delle cubiche lisce di* $\mathbb{P}^2$*:* $\{$*cubiche lisce*$\}/$*equivalenza proiettiva* $\simeq k$*, tramite* $[C] \to j(C)$*. Si può (con il teorema di Riemann-Roch) dimostrare un risultato più forte: due cubiche lisce sono isomorfe se e solo se hanno lo stesso modulo, cioè:* $\{$*cubiche lisce*$\}/$*isomorfismo* $\simeq k$*; osservare che* k *è una variet algebrica.*

Esercizi.

Esercizio 2.1: *Il problema iniziale è il seguente: determinare quando due polinomi* $F(X), G(X) \in k[X]$ *hanno una radice comune. Chiaramente l'approccio brutale consiste nel calcolare le radici di* F *e* G*, e confrontarle. Questo procedimento è generalmente impraticabile.*

Osserviamo invece che F *e* G *hanno un fattore comune se e solo se esiste un polinomio,* H*, di grado* $f+g-1$ *(*$f := deg(F)$*,* $g := deg(G)$*), divisibile per* F *e per* G*. Infatti se* $H = F.F' = G.G'$*, e se* F *e* G *non hanno radici comuni, tutte le radici di* F *(nella chiusura algebrica di* k*) sono radici di* G'*, ma questo è impossibile perchè* $deg(G') = f-1$*. Viceversa se* $F = R.F'$*,* $G = R.G'$*, allora* $H = R.F'.G'$ *è un polinomio di grado* $\leq f+g-1$ *divisibile per* F *e per* G*.*
Sia $V_F := \{P \in k[X]_{\leq f+g-1} \mid F|P\}$*, il* k*-spazio vettoriale dei polinomi di grado* $\leq f+g-1$ *divisibili per* F*. Chiaramente* V_F *è l'insieme dei multipli di* F*, di grado* $\leq f+g-1$*, quindi una base di* V_F *è* $F, XF, X^2F, \cdots, X^{g-1}F$*. Nello stesso modo* $V_G =< G, XG, \cdots, X^{f-1}G >$*. Dire che esiste* H *di grado* $\leq f+g-1$ *divisibile per* F *e per* G *è equivalente a dire che i sottospazi* V_F *e* V_G *non sono in somma diretta, cioè che* $F, XF, \cdots, X^{g-1}F, G, XG, \cdots, X^{f-1}G$ *sono linearmente dipendenti. Scrivendo questi vettori nella base* $1, X, \cdots, X^{f+g-1}$ *di* $k[X]_{\leq f+g-1}$*, concludiamo che* $F(X) = a_0 + a_1X + \cdots + a_fX^f$ *e* $G(X) = b_0 + b_1X + \cdots + b_gX^g$ *hanno una radice comune se e solo se* $R(F,G) = 0$*, dove* $R(F,G)$ *è il determinante della seguente matrice:*

$$\begin{pmatrix} a_0 & \cdots & a_f & 0 & 0 & \cdots & 0 \\ 0 & a_0 & \cdots & a_f & 0 & \cdots & 0 \\ & & \ddots & & \ddots & & \\ 0 & \cdots & 0 & a_0 & & \cdots & a_f \\ b_0 & \cdots & b_g & 0 & 0 & \cdots & 0 \\ 0 & b_0 & \cdots & b_g & 0 & \cdots & 0 \\ & & \ddots & & \ddots & & \\ 0 & \cdots & 0 & b_0 & & \cdots & b_g \end{pmatrix}$$

Il determinante $(f+g)\times(f+g)$*,* $R(F,G)$ *esprime che i* $(f+g)$ *vettori* $F, XF, \cdots, X^{g-1}F, G, XG, \cdots, X^{f-1}G$ *dello spazio, di dimensione* $f+g$*,* $k[X]_{\leq f+g-1}$*, sono linearmente dipendenti. Il determinante* $R(F,G)$ *è il* risultante *dei polinomi* F *e* G*.*
In conclusione F *e* G *hanno una radice comune se e solo se il loro risultante* $R(F,G)$ *è nullo. Osserviamo che* $R(F,G)$ *coinvolge solo i coefficienti dei polinomi* F, G*; abbiamo eliminato la variabile* X*. ("Teoria dell'eliminazione".)*
Il discriminante *di un polinomio* $P(X)$ *è il risultante* $R(P,P')$*.*
Per ritrovare un vecchio compagno di giochi, calcolare il discriminante di $aX^2 + bX + c$*.*

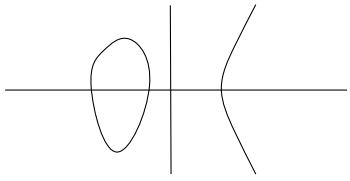
3. Formule esplicite per l'addizione su una cubica liscia.

Sia $C \subset \mathbb{P}^2(\mathbb{C})$ una cubica in forma di Weierstrass: $Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$ (cfr II. 6). Il punto $p = (0 : 1 : 0)$ è un punto di flesso di C (in particolare nonsingolare) quindi $C \cap T_pC = \{p\}$ (con molteplicità tre), dove T_pC è la retta $Z = 0$. Nella carta affine $U_Z \simeq \mathbb{C}^2$ la curva è data da $y^2 = x^3 + ax^2 + bx + c$. Siamo interessati in cubiche lisce, abbiamo:

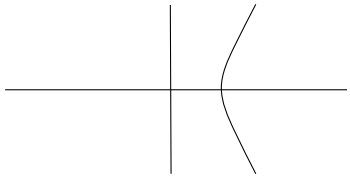
Lemma 3.1: *Con le notazioni precedenti, la cubica C è liscia se e solo se $D \neq 0$ dove $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27b^2$.*

Osservazione 3.2: *Il numero D è il discriminante del polinomio $f(x) = x^3 + ax^2 + bx + c$; la condizione $D \neq 0$ equivale a dire che $f(x) = 0$ ha tre radici distinte. Se $a = 0$, l'espressione di D è più simpatica: $D = -4b^3 - 27b^2$.*

L'intersezione della curva affine $y^2 = f(x) := x^3 + ax^2 + bx + c$ con la retta all'infinito consta, come abbiamo visto, dell'unico punto p (che corrisponde alle direzioni verticali). Quindi i punti di C sono i punti a distanza finita e il punto all'infinito O, cioè: $\{(x, y) \in \mathbb{C}^2 \mid y^2 = f(x)\} \cup \{O\}$. In quanto segue si cercherà di esplicitare la struttura di gruppo su C con origine $p = O$. Se a, b, c sono reali la parte reale di C è del tipo:



($f(x) = 0$ ha tre radici reali).



($f(x) = 0$ ha una radice reale).

Se $P \in \mathbb{C}^2$ è un punto del piano noteremo $(x(P), y(P))$ le sue coordinate (o anche (x, y) se non c'è rischio di confusione). Cerchiamo di stabilire delle formule per le coordinate di $P + Q$, $-P$, $2P = P + P$, dove P, Q sono punti di C.
Il simmetrico: Sia $P \neq O$ un punto di C. Siccome O è un punto di flesso, $-P$ è il terzo punto di $R \cap C$ dove R è la retta generata da P e O. La retta R è la retta verticale passante per P, ossia la retta di equazione affine $x = x(P)$. Siccome C è simmetrica rispetto all'asse delle x:

Lemma 3.3: *Sia $P = (x(P), y(P))$ un punto di C ($P \neq O$). Allora $-P = (x(P), -y(P))$.*

Somma di due punti distinti: Siano $P = (x_1, y_1)$, $P' = (x_2, y_2)$ due punti distinti di C. Se $[PP'] = (x_3, y_3)$ allora $P + P'$ è il terzo punto di $R \cap C$ dove R è la retta generata da O e $[PP']$; quindi $P + P' = (x3, -y3)$. Sia $y = \lambda x + \nu$ l'equazione della retta, D, per P e P' (se la retta è verticale $P = -P'$ e $P + P' = O$). Abbiamo $\lambda(x_1 - x_2) = y_1 - y_2$, cioè: $\lambda = (y_1 - y_2)/(x_1 - x_2)$ (se $x_1 = x_2$ allora $P = \pm P'$). Il punto $[PP']$ è il terzo punto di $D \cap C$, questa intersezione è data da:
$y^2 = (\lambda x + \nu)^2 = x^3 + ax^2 + bx + c$, cioè: $x^3 + x^2(a - \lambda^2) + x(b - 2\nu) + c - \nu^2 = 0$.
Questa equazione è verificata da $P, P', [PP']$, quindi:
$x^3 + x^2(a - \lambda^2) + x(b - 2\nu) + c - \nu^2 = (x - x_1)(x - x_2)(x - x_3)$.
Identificando i coefficienti di x^2 abbiamo: $x_3 = \lambda^2 - a - x_1 - x_2$; e poi $y_3 = \lambda x_3 + \nu$, dove $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$. Riassumendo:

Lemma 3.4: *Siano $P = (x_1, y_1)$, $P' = (x_2, y_2)$ due punti a distanza finita di C. Se $P \neq P'$, le coordinate (x, y) di $P + P'$ sono:*
$x = \lambda^2 - a - x_1 - x_2$
$y = -\lambda x - \nu$
dove $\lambda = (y_1 - y_2)/(x_1 - x_2)$, $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$.

Formula di duplicazione: Consideriamo adesso il caso $P = P'$, vogliamo quindi calcolare le coordinate di $2P = P + P$ in funzione delle coordinate (x_1, y_1) di P. Si procede come prima ma con la tangente in P al posto della retta $< P, P' >$. L'equazione della tangente è: $-(x - x_1)f'(x_1) + (y - y_1)2y_1 = 0$. La tangente è verticale se e solo se $2P = O$. Se $y_1 \neq 0$ la tangente ha equazione $y = \lambda x + \nu$ con $\lambda = f'(x_1)/2y_1 = (3x_1^2 + 2ax_1 + b)/2y_1$, ragionando come prima viene $x(2P) = \lambda^2 - a - 2x_1$, e riducendo allo stesso denominatore:

Lemma 3.5: *Sia $P = (x, y)$ un punto di C a distanza finita. Se $y \neq 0$ allora:*

$$x(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4x^3 + 4ax^2 + 4bx + 4c} = \frac{f'(x)^2}{4f(x)} - a - 2x \quad (*)$$

Se $y = 0$, allora $2P = O$.

Osservazione 3.6: *(i) La formula $(*)$ del Lemma 3.5 si chiama formula di duplicazione; si può ottenere una formula analoga per $y(2P)$.*
(ii) Si possono usare le formule dei lemmi precedenti per una dimostrazione alternativa del fatto che l'addizione definisce una struttura di gruppo abeliano su C (e che questa struttura è algebrica, cioè che C è una variet abeliana).

Esercizi.

Esercizio 3.1: *Sia C la curva di equazione $y^2 = x^3 + 17$.*
(i) Verificare che C è nonsingolare.
(ii) Verificare che $P_1 = (-1, 4)$, $P_2 = (2, 5)$ appartengono a C, e che $P_1 + P_2 = (-8/9, -109/27)$, $2P_1 = (137/64, -2651/512)$.
(iii) Siano $P_3 = (-2, 3)$, $P_4 = (4, 9)$, $P_5 = (8, 23)$. Verificare che questi punti sono su C, e calcolare $P_6 = -P_3 + 2P_2$, $P_7 = 3P_3 - P_2$.
(iv) I punti $P_1, \cdots, P_7$ hanno tutti coordinate intere. Si può dimostrare che ci sono esattamente 8 punti su C con coordinate intere. Sapreste trovare l'ultimo? (fatevi aiutare da un computer, e anche così, se non viene, non insistete troppo...)

4. Aritmetica sulle cubiche piane lisce.

L'aritmetica diofantea è lo studio delle soluzioni intere (razionali) di equazioni polinomiali a coefficienti interi (razionali). Il problema diofanteo più famoso è senz'altro la congettura di Fermat: "se degli interi x, y, z soddisfano $x^n + y^n = z^n$, per qualche intero $n \geq 3$, allora $xyz = 0$". Il caso $n = 2$ ("terne pitagoriche") è noto dall'antichità. La congettura di Fermat è stata dimostrata da Wiles (1995), usando, tra altre cose, tecniche molto profonde e sofisticate dell'aritmetica delle curve ellittiche. L'aritmetica delle curve ellittiche è, grosso modo, quella parte dell'aritmetica diofantea che si occupa delle equazioni $y^2 = f(x)$ dove $f(x) \in \mathbb{Q}[x]$ è un polinomio del terzo grado tale che $f(x) = 0$ abbia tre radici distinte in $\mathbb{C}$. La denominazione viene dal fatto che la curva di $\mathbb{C}^2$ di equazione $y^2 = f(x)$ è, come sappiamo, una cubica liscia, cioè una variet abeliana di dimensione uno, o ancora una curva ellittica.

In questi ultimi quaranta anni l'aritmetica diofantea ha fatto progressi enormi dovuti in gran parte all'uso sistematico di metodi geometrici. Scopo di questo paragrafo e dei successivi, è di dare una breve introduzione (senza dimostrazioni) all'aritmetica delle curve ellittiche.

Definizione 4.1: *Un punto di $\mathbb{P}^2(\mathbb{C})$ è razionale (o definito su $\mathbb{Q}$) se e solo se ammette delle coordinate razionali (cioè se e solo se ammette delle coordinate intere).*

Osservazione 4.2: *Se $p = (x : y : z)$ con $x \neq 0$, allora $p = (1 : y/x : z/x)$ e p è razionale se e solo se y/x, z/x appartengono a $\mathbb{Q}$. Per esempio $(\sqrt{2} : 0 : 1/\sqrt{2})$ è razionale (perchè uguale a $(2 : 0 : 1)$), mentre $(\sqrt{2} : 0 : 1)$ non è razionale.*

Definizione 4.3: *Una curva $C \subset \mathbb{P}^2(\mathbb{C})$ è definita su $\mathbb{Q}$ se ammette un'equazione a coefficienti razionali: $F(X, Y, Z) = 0$ con $F(X, Y, Z) \in \mathbb{Q}[X, Y, Z]$. Si nota $C(\mathbb{Q})$ l'insieme dei punti razionali (definiti su $\mathbb{Q}$) di C.*

Osservazione 4.4: *Se C è definita su $\mathbb{Q}$ può accadere che $C(\mathbb{Q})$ sia vuoto. Per esempio la cubica, E, di equazione $3X^3 + 4Y^3 + 5Z^3 = 0$ non ha punti razionali (e questo benchè l'equazione $3X^3 + 4Y^3 + 5Z^3 \equiv 0$ (mod m) abbia soluzioni non banali per ogni intero m. Questo risultato è dovuto a Selmer (1951)). Data una cubica, E, definita su $\mathbb{Q}$, non si conosce nessun algoritma in grado di decidere se $E(\mathbb{Q})$ sia o meno vuoto.*

Notazioni, convenzioni: Supporemo quindi che la nostra cubica E, definita su $\mathbb{Q}$, ha almeno un punto razionale e che questo punto è un punto di flesso. In altri termini supporemo che E è data da un'equazione in forma di Weierstrass (cfr II. 6): $y^2 = x^3 + ax^2 + bx + d$, con a, b, d in $\mathbb{Q}$. Con un cambiamento di variabili del tipo $X = d^2x$, $Y = d^3y$, d intero abbastanza grande, ci riconduciamo a un'equazione del

tipo $y^2 = x^3+ax^2+bx+c$ con a, b, c in $\mathbb{Z}$. Finalmente siccome vogliamo che la nostra cubica sia liscia assumeremo $D \neq 0$, dove $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ è il discriminante di $f(x) := x^3 + ax^2 + bx + c$. L'insieme dei punti razionali di E è costituito dal punto all'infinito, O, e dai punti razionali a distanza finita: $E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = f(x)\} \cup \{O\}$. In altri termini risolvere l'equazione diofantea $y^2 = f(x)$ è equivalente a determinare $E(\mathbb{Q})$. Analogamente determinare le soluzioni in numeri interi dell'equazione $Y^2Z = X^3 + aX^2Z + bXZ^2 + cZ^3$, si riconduce a descrivere $E(\mathbb{Q})$. D'ora in poi E denoterà una cubica di equazione $y^2 = f(x)$, $f(x) := x^3 + ax^2 + bx + c$ con a, b, c in $\mathbb{Z}$ e tale che $D \neq 0$, $D := -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$; infine: $E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = f(x)\} \cup \{O\}$. La condizione $D \neq 0$ implica che la cubica E è nonsingolare, sappiamo che $E(\mathbb{C}) = \{(x, y) \in \mathbb{C}^2 \mid y^2 = f(x)\} \cup \{O\}$ (cioè $E \subset \mathbb{P}^2(\mathbb{C})$) ha una struttura di gruppo abeliano (cfr II. 5). Chiaramente $E(\mathbb{Q}) \subset E(\mathbb{C})$, ma abbiamo qualcosa di più:

Lemma 4.5: *$E(\mathbb{Q})$ è un sottogruppo di $E(\mathbb{C})$.*

DIMOSTRAZIONE. Le formule della Sezione 3 mostrano che se $P, Q \in E(\mathbb{Q})$ allora anche $P - Q \in E(\mathbb{Q})$ (osservare che $O \in E(\mathbb{Q})$ per ipotesi). Si può anche dimostrare il lemma ricordando la definizione geometrica dell'addizione e osservando che se un polinomio del terzo grado, a coefficienti razionali, ha due radici razionali, allora anche la terza radice è razionale. □

Osservazione 4.6: *Per gli stessi motivi anche $E(\mathbb{R})$ è un sottogruppo di E e abbiamo delle inclusioni di gruppi: $O \subset E(\mathbb{Q}) \subset E(\mathbb{R}) \subset E(\mathbb{C})$. Più generalmente se F è un campo (un sottocampo di $\mathbb{C}$, un campo finito, ecc...) e se a, b, c sono in F, l'insieme, $E(F)$, dei punti F-razionali (a coordinate in F) è un gruppo (usare le formule esplicite dell'addizione).*

Il primo risultato fondamentale sul gruppo abeliano $E(\mathbb{Q})$ fu congetturato da Poincaré (1901) e dimostrato da Mordell (1923):

Teorema 4.7: *(Mordell) Il gruppo abeliano $E(\mathbb{Q})$ è finitamente generato.*

Esiste quindi un numero finito di punti di $E(\mathbb{Q})$, $P_1, ..., P_r$ tali che ogni altro punto $P \in E(\mathbb{Q})$ si scriva nella forma: $P = \sum n_iP_i$, $n_i \in \mathbb{Z}$. Osserviamo che se P e Q, sono due punti razionali di E, il terzo punto,$[PQ]$, della retta ("corda" se $P \neq Q$, tangente se $P = Q$) generata da P e Q, è un punto razionale. Il teorema afferma che applicando il procedimento delle corde e delle tangenti, in tutti i modi possibili, partendo da $P_1, ..., P_r$, si ottengono tutti i punti razionali di E.

Dal teorema di struttura dei gruppi abeliani finitamente generati risulta che $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$, dove $E(\mathbb{Q})_{tors}$ è il sottogruppo di torsione, cioè il sottogruppo degli elementi di ordine finito: $E(\mathbb{Q})_{tors} = \{P \in E(\mathbb{Q}) \mid \exists m \in N, m \neq 0,$ tale che: $m.P = P+\cdots+P = O\}$, e dove $\mathbb{Z}^r$ è la parte "libera"; l'intero r si chiama

il *rango* di $E(\mathbb{Q})$. Come vedremo i possibili gruppi di torsione sono tutti classificati; invece si sa pochissimo sul rango: data una curva ellittica non esiste nessun algoritmo in grado di calcolare il suo rango (nella pratica è molto difficile calcolare il rango di una data curva ellittica). Nel 1995 non si conosceva nessuna cubica $E(\mathbb{Q})$ con rango > 21, e il problema di sapere se il rango di una cubica razionale può essere arbitrariamente grande è tuttora (2003) aperto. La famosa congettura di Birch-Swinnerton Dyer collega il rango con altri invarianti della curva.

5. Punti di torsione.

Definizione 5.1: *Un elemento, g, di un gruppo abeliano G ha ordine m ($m \neq 0, m \in \mathbb{N}$) se $mg = g + \cdots + g = 0$, e se $ng \neq 0$ per ogni $n < m$ (si dice anche che g è di m-torsione). L'insieme degli elementi di m-torsione (con il neutro) è un sottogruppo di G. Se invece $mg \neq 0$, $\forall m$, g è di ordine infinito (non è di torsione).*

Cerchiamo adesso di determinare, usando le formule della Sezione 3, i punti di ordine due, tre di una cubica liscia $E \subset \mathbb{P}^2(\mathbb{C})$, di equazione $y^2 = f(x) = x^3 + ax^2 + bx + c$.

Punti di ordine due: Sia $P \neq O$ un punto di E tale che $2P = O$, allora $P = -P$, e questo implica (Sezione 3, Lemma 3.3): $y(P) = 0$. Quindi $x(P)$ è una delle tre radici di $f(x) = 0$. Notiamo a_1, a_2, a_3 le tre radici complesse (distinte) di $f(x) = 0$. L'insieme dei punti di ordine due di E è $E_2 := \{O, P_1, P_2, P_3\}$ dove $P_i = (a_i, 0)$, $1 \leq i \leq 3$. Ogni elemento di E_2 ha ordine due quindi E_2 è isomorfo al prodotto diretto di $\mathbb{Z}_2$ con se stesso ($\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$). In conclusione $E_2 \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$ (il gruppo $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ è noto come gruppo di Klein, o Four Group). Questa conclusione è valida perchè abbiamo considerato tutti i punti con coordinate complesse di E. Se ci limitiamo ai punti con coordinate reali ($E(\mathbb{R})$), allora: $E_2(\mathbb{R})$ = Four Group ($f(x)$ ha tre radici reali), $\mathbb{Z}_2$ ($f(x)$ ha una radice reale). Se ci limitiamo ulteriormente ai punti con coordinate razionali: $E_2(\mathbb{Q})$ = Four Group, $\mathbb{Z}_2$, o $\{O\}$.

Punti di ordine tre: Abbiamo già visto che un punto P verifica $3P = O$ se e solo se P è un flesso di E. Sia $P \neq O$ un flesso di E. Abbiamo $2P = -P$, e quindi $x(2P) = x(-P) = x(P)$ (Sezione 3). Siccome $x(2P) = \frac{f'(x)}{4f(x)} - a - 2x$, e tenuto conto che $12x + 4a = 2f"(x)$, la relazione $x(2P) = x$ è equivalente a: $\psi(x) = 2f"(x)f(x) - f'(x)^2 = 0$. Il polinomio $\psi(x)$ ha grado quattro e le sue radici sono distinte. Infatti $\psi'(x) = 12f(x)$ e una radice doppia di $\psi(x)$ sarebbe una radice doppia di f (ma le radici di f sono distinte perchè E è liscia). Siano $b_1, ..., b_4$ le radici complesse di $\psi(x) = 0$, e sia $d_i = \sqrt{f(b_i)}$, allora l'insieme dei punti P tali che $3P = O$ è $\{O, (b_1, \pm d_1), (b_2, \pm d_2), (b_3, \pm d_3), (b_4, \pm d_4)\}$.

Corollario 5.2: *Una cubica nonsingolare, $E \subset \mathbb{P}^2(\mathbb{C})$, ha nove flessi distinti.*

Per quanto riguarda i punti di ordine tre definiti su $\mathbb{R}$, $\mathbb{Q}$, si rimanda agli esercizi.

Il teorema di Lutz-Nagell:

Torniamo adesso alle cubiche lisce definite su $\mathbb{Q}$, quindi E è una cubica di equazione $y^2 = f(x) = x^3 + ax^2 + bx + c$, con a, b, c in $\mathbb{Z}$, il cui discriminante $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$, è non nullo. Siamo interessati a determinare $E(\mathbb{Q})_{tors}$. In merito, il primo risultato fondamentale è il seguente:

Teorema 5.3: *(Lutz-Nagell)*
Con le notazioni precedenti sia $P = (x(P), y(P)) \in E(\mathbb{Q})_{tors}$.
(i) $x(P)$ e $y(P)$ sono interi.
(ii) $y(P) = 0$ (e in questo caso $2P = O$), oppure $y(P)^2$ divide il discriminante D.

Osservazione 5.4: *(i) Il teorema di Lutz-Nagell dà solo condizioni necessarie (ma non sufficienti) affinchè un punto sia di torsione.*
(ii) Il teorema può fornire informazioni sul rango di $E(\mathbb{Q})$, in effetti sia $P \in E(\mathbb{Q})$ un punto con coordinate intere, se calcolando i multipli $2P, 3P, ...$ si arriva a nP le cui coordinate non sono intere, si può concludere che nP, e a fortiori P, non è di torsione. Inoltre ci si può limitare a calcolare $x(2P), x(4P), x(8P), ...$ con la formula di duplicazione (Lemma 3.5). Per esempio la curva di equazione $y^2 = x^3 + 17$ ha rango ≥ 1 (cioè vi è un'infinità di soluzioni razionali dell'equazione $y^2 = x^3 + 17$) perchè $P_1 = (-1, 4)$ verifica $x(2P1) = 137/64$ (cf Esercizio 3.1).
(iii) La dimostrazione del teorema non è eccessivamente difficile.

Il risultato definitivo sul gruppo di torsione è il seguente:

Teorema 5.5: *(Mazur, 1977)*
Sia E una cubica liscia definita su $\mathbb{Q}$.
(i) $E(\mathbb{Q})_{tors}$ è isomorfo a uno dei seguenti quindici gruppi:
$\mathbb{Z}_n$, *per* $n = 1, 2, ..., 9, 10, 12$
$\mathbb{Z}_{2n} \oplus \mathbb{Z}_2$, *per* $n = 1, 2, 3, 4$.
(ii) Ognuno di questi quindici gruppi è il gruppo di torsione di una cubica liscia definita su $\mathbb{Q}$.

Osservazione 5.6: *(i) In particolare non esiste nessuna curva con un punto di ordine 11. Se $t = \#(E(\mathbb{Q})_{tors}$ allora $1 \leq t \leq 10$ o $t = 12$, o $t = 16$. Un punto di torsione ha ordine ≤ 12.*
(ii) La dimostrazione del punto (i) del teorema è molto difficile (utilizza concetti sofisticati di geometria aritmetica).

(iii) Con i teoremi di Lutz-Nagell e Mazur si ha un algoritmo (finito) per determinare $E(\mathbb{Q})_{tors}$.
(a) si prende il discriminante D e tutti i suoi divisori (che sono in numero finito), tra questi divisori si considerano solo quelli della forma d^2.

(b) poi si sostituisce nell'equazione $y^2 = f(x)$, e si ottiene $x^3+ax^2+bx = d^2-c\,(*)$. Se un intero x verifica questa relazione allora $x|d^2 - c$, quindi basta verificare se i divisori di $d^2 - c$ soddisfano $(*)$.
(c) dopo un numero finito di operazioni abbiamo determinato i possibili punti di torsione, bisogna poi verificare che i punti ottenuti sono effettivamente di torsione (il teorema di Lutz-Nagell d delle condizioni necessarie ma non sufficienti); quindi per ogni punto P ottenuto si calcola $2P, 3P, ...$; se troviamo m tale che $mP = O$ allora P è di torsione. Per il teorema di Mazur basta provare per $m \leq 12$.

Facciamo alcuni esempi:

Esempio 5.7: $\boxed{y^2 = x^3 + 2; E(\mathbb{Q})_{tors} = \{O\}}$
Il discriminante è $D = -3^3.2^2$. Se $P = (x, y)$ è un punto di torsione allora $y = 0$ o $y^2|D$ dal teorema di Lutz-Nagell. Non ci sono punti razionali con $y = 0$. La condizione $y^2|D$ dà le seguenti possibilit: $y \in \{\pm 2, \pm 3, \pm 6, \pm 1\}$. Se $y^2 \neq 1$ si verifica facilmente che non ci sono soluzioni intere. Se $y^2 = 1$ allora $x = -1$ e abbiamo le due possibilità $P_1 = (-1, 1)$, $P_2 = (-1, -1)$. Questi punti non sono di torsione perchè la formula di duplicazione fornisce $x(2P_1) = x(2P_2) = -15/4$ che non è intero. In particolare la curva di equazione $y^2 = x^3 + 2$ ha rango ≥ 1.

Esempio 5.8: $\boxed{y^2 = x^3 + x; E(\mathbb{Q})_{tors} = \mathbb{Z}_2}$
Il discriminante è $D = -4$, quindi se $y^2|D$, allora $y^2 = 1$ o 4: non ci sono soluzioni intere corrispondenti (osservare che $x|y^2$). L'unica possibilità è $y = 0$ che dà $P = (0, 0)$ punto di 2-torsione. Pertanto $E(\mathbb{Q})_{tors} = \mathbb{Z}_2$.

Esempio 5.9: $\boxed{y^2 = x^3 + 4x; E(\mathbb{Q})_{tors} = \mathbb{Z}_4}$
Il discriminante è $D = -2^8$. Se $y = 0$ otteniamo il punto di 2-torsione $P_1 = (0, 0)$. La condizione $y^2|D$ implica $y \in \{\pm 2, \pm 4, \pm 8, \pm 16\}$, l'unico caso in cui x è intero è $y = \pm 4$ (osservare che $x|y^2$); in questo caso $\pm P = (2, \pm 4)$. Rimane da vedere se P è effettivamente di torsione. Dalla formula di duplicazione $x(2P) = 0$, quindi $2P = P_1$, e P è di 4-torsione. Concludiamo che $E(\mathbb{Q})_{tors} = \{O, P_1, \pm P\}$ è isomorfo a $\mathbb{Z}_4$ (perchè?).

Esempio 5.10: $\boxed{y^2 = x^3 + 1; E(\mathbb{Q})_{tors} = \mathbb{Z}_6}$
L'unico punto razionale con $y = 0$ è $P_1 = (0, 0)$; è un punto di 2-torsione. Il discriminante è $D = -3^3$ e la condizione $y^2|D$ implica $y = \pm 1, \pm 3$. Le soluzioni corrispondenti sono $\pm P = (0, \pm 1)$, $\pm Q = (2, \pm 3)$. Si verifica facilmente che P è un flesso (quindi è di 3-torsione). Per la formula di duplicazione $x(2Q) = 0$, quindi $2Q = \varepsilon P$, $\varepsilon \in \{-1, 1\}$, e Q è di 6-torsione. Concludiamo che $E(\mathbb{Q})_{tors} = \{O, P_1, \pm P, \pm Q\}$ è isomorfo a $\mathbb{Z}_6$ (perchè?).

Esercizi.

Esercizio 5.1: *Sia E una cubica definita su $\mathbb{Q}$. Se F è un sottocampo di $\mathbb{C}$ si indica con $E(F)_3$ il gruppo degli elementi, definiti su F, il cui ordine divide tre. Abbiamo visto che $\#(E(\mathbb{C})_3) = 9$. Mostrare che $\#(E(\mathbb{R})_3 = 3$ (sempre), e $\#(E(\mathbb{Q})_3 = 1$ o 3.*

Esercizio 5.2: *Completare la dimostrazione dell'Esempio 5.9 (idem per l'Esempio 5.10).*

6. Il teorema di Mordell.

In tutto questo paragrafo si indicherà con $E \subset \mathbb{P}^2(\mathbb{C})$ una cubica liscia di equazione (affine) $y^2 = f(x) = x^3 + ax^2 + bx + c$, con a, b, c in $\mathbb{Z}$; e con $E(\mathbb{Q})$ il gruppo abeliano dei punti razionali di E: $E(\mathbb{Q}) = \{(x, y) \in \mathbb{Q}^2 \mid y^2 = f(x)\} \cup \{O\}$. Abbiamo:

Teorema 6.1: *(Mordell)*
Con le notazioni precedenti, il gruppo $E(\mathbb{Q})$ è finitamente generato.

La dimostrazione del teorema di Mordell consta di due parti:
(I) si mostra prima che il gruppo $E(\mathbb{Q})/2.E(\mathbb{Q})$ è finito (qui $2.E(\mathbb{Q})$ è l'immagine della moltiplicazione per 2: $2.E(\mathbb{Q}) = \{P \in E(\mathbb{Q}) \mid \exists Q \in E(\mathbb{Q}) \text{ tale che } P = 2Q\}$).
(II) con un argomento di"discesa" si mostra che (I) implica il teorema.
(II) è la parte facile, mentre (I) è la parte difficile. Per quanto riguarda (I) osserviamo che, in generale, se G è un gruppo abeliano tale che $G/2G$ sia finito allora G non è necessariamente finitamente generato (per esempio $G = \mathbb{R}$). Si può dare una dimostrazione relativamente semplice di (I) nel caso in cui $f(x) = 0$ abbia tutte le sue radici in $\mathbb{Q}$ (e quindi in $\mathbb{Z}$ visto che $f(x) \in \mathbb{Z}[x]$). Nel caso generale la dimostrazione è molto più delicata (bisogna lavorare nel campo di spezzamento di f).
Il metodo della discesa ("infinita") è stato introdotto da Fermat per mostrare che certe equazioni (per es. $x^4 + y^4 = z^4$) non hanno soluzioni intere non banali. L'idea è la seguente: ogni (ipotetica) soluzione viene "misurata" con un numero intero. Poi si dimostra che se esiste una soluzione allora ne esiste una di "misura" più piccola. Siccome $\mathbb{N}$ ha un più piccolo elemento non si può "scendere" indefinitamente, e si ottiene la contraddizione cercata.

Esempio 6.2: Mostriamo che $\sqrt{2}$ è irrazionale ossia che l'equazione $x^2 = 2y^2$ non ha soluzioni in $\mathbb{N}$. Supponiamo per assurdo che $(x, y) \in \mathbb{N}^2$ sia una soluzione. Si ha $2|x$, quindi $x = 2x'$, e $4x'^2 = 2y^2$, cioè $y^2 = 2x'^2$ e (y, x') è soluzione. La soluzione (y, x') è più piccola della soluzione (x, y) perchè, per esempio, $||(y, x')||^2 = y^2 + x'^2 < ||(x, y)||^2 = y^2 + x^2$. Si arriverebbe dunque a una soluzione di norma zero, e questo è assurdo.

Per dimostrare il teorema di Mordell si cerca di usare un argomento di discesa per ricondursi a un numero finito di possibilità (i generatori). Per questo bisogna "misurare" adeguatamente i punti razionali sulla nostra curva. Questo si fa introducendo la nozione di altezza.

Definizione 6.3: *Sia $x \in \mathbb{Q}$ con $x = m/n$, $(m, n) = 1$. L'altezza di x, $H(x)$, è definita da $H(x) :=$ max $\{|m|, |n|\}$.*

Osservazione 6.4: *Si potrebbe pensare di misurare x con il valore assoluto $|x|$, però se consideriamo i numeri razionali $x = 1$, $x' = 99999/100000$, vediamo che i loro valori assoluti differiscono di poco mentre $H(x) = 1$ e $H(x') = 100000$, e questo riflette meglio il fatto che, da un punto di vista aritmetico, x' è un numero più "complicato" di 1.*

Definizione 6.5: *Sia $P \in E(\mathbb{Q})$, $P \neq O$. L'altezza di P è: $H(P) := H(x(P))$. Si definisce anche l'altezza "piccola": $h(P) = log(H(P))$. Inoltre si pone $H(O) = 1$, $h(O) = 0$.*

Il teorema di Mordell sarà conseguenza dei seguenti risultati:

Teorema 6.6: *Il gruppo $E(\mathbb{Q})/2E(\mathbb{Q})$ è finito.*

Lemma 6.7: *Per ogni M in $\mathbb{R}$, $\{P \in E(\mathbb{Q}) \mid h(P) \leq M\}$ è un insieme finito.*

Lemma 6.8: *Sia $P_0 \in E(\mathbb{Q})$. Esiste k_0 (che dipende da P_0 e da a, b, c, i coefficienti dell'equazione di E) tale che: $\forall P \in E(\mathbb{Q})$, $h(P + P_0) \leq 2h(P) + k_0$.*

Lemma 6.9: *Esiste k (che dipende solo da E) tale che: $\forall P \in E(\mathbb{Q})$, $h(2P) \geq 4h(P) - k$.*

Proposizione 6.10: *("discesa")*
Sia G un gruppo abeliano. Supponiamo che esista un'applicazione ("altezza") $h : G \to \mathbb{R}_+$ tale che:
(i) $\forall r \in \mathbb{R}_+$, $\{P \in G \mid h(P) \leq r\}$ sia finito
(ii) $\forall P_0 \in G$, esiste k_0 tale che per ogni $P \in G$: $h(P + P_0) \leq 2h(P) + k_0$.
(iii) $\exists k$ tale che per ogni $P \in G$, $h(2P) \geq 4h(P) - k$.
In queste condizioni, e se $G/2G$ è finito, G è finitamente generato.

Le dimostrazioni dei Lemma 6.7, Lemma 6.8, Lemma 6.9 sono "tecniche" ma non presentano difficoltà particolari. Ci limiteremo a dare la dimostrazione della Proposizione 6.10.

Dimostrazione della Proposizione 6.10. Per ipotesi $G/2G$ è finito: $G/2G = \{[Q1], ..., [Qn]\}$ (dove $[P]$ indica la classe di P mod. $2G$). Sia $P \in G$. Esiste i_1 tale che $[P] = [Q_{i_1}]$, pertanto $P - Q_{i_1} = 2P_1$. Nello stesso modo $[P_1] = [Q_{i_2}]$, e $P_1 - Q_{i_2} = 2P_2$. Procedendo così:

$$P - Q_{i_1} = 2P_1$$

$$P_1 - Q_{i_2} = 2P_2$$

$$\dots$$

$$P_{j-1} - Q_{i_j} = 2P_j$$

Il punto sta nel mostrare che ad un certo momento si arriverà ad un P_j tale che $h(P_j) \leq M$, dove M è una certa costante che non dipende da P (cioè che funziona per ogni $P \in G$). Infatti da (i) l'insieme dei punti di altezza al più M è finito, diciamo $\{P \mid h(P) \leq M\} = \{R_1, ..., R_t\}$. Quindi P_j è uno degli R_p, e $P_{j-1} = Q_{i_j} + 2P_j$ è combinazione lineare dei Q_i e degli R_p. Risalendo fino a P, si esprime P come combinazione lineare dei Q_i e degli R_p. Siccome questo vale per ogni P (M non dipende da P), G è finitamente generato.

Cerchiamo di determinare M. Applichiamo (ii) a $-Q_i$: $\exists k_i$ tale che "per ogni $P \in G, h(P - Q_i) \leq 2h(P) + k_i$. Sia $K := \max\{k_1, ..., k_n\}$. Abbiamo:

$$\forall i, \forall P \in G, h(P - Q_i) \leq 2h(P) + K \ (*)$$

Poniamo $M := K + k$ (dove k è la costante fornita dal punto (iii)), e mostriamo che questa costante M funziona.
Sia $P \in G$ qualsiasi, col procedimento descritto all'inizio otteniamo una serie di elementi $P_1, ..., P_{j-1}, P_j, ...$, se $h(P_{j-1}) \leq M$, abbiamo finito, supponiamo quindi $h(P_{j-1}) > M$. Da (iii): $4h(P_j) \leq h(2P_j) + k$. D'altra parte $2P_j = P_{j-1} - Q_{i_j}$, e usando $(*)$: $h(2P_j) = h(P_{j-1} - Q_{i_j}) \leq 2h(P_{j-1}) + K$. Combinando: $4h(Pj) \leq 2h(P_{j-1}) + M$, cioè: $h(P_j) \leq \frac{3}{4}h(P_{j-1}) - \frac{1}{4}(h(P_{j-1}) - M) < \frac{3}{4}h(P_{j-1})$ (perchè $h(P_{j-1}) > M$); quindi $h(P_j) < h(P_{j-1})$, l'altezza decresce strettamente, e si arriverà ad un elemento di altezza al più M. □

Per concludere questo breve tour di aritmetica segnaliamo un altro risultato fondamentale:

Teorema 6.11: *(Faltings, 1983)*
Sia $C \subset \mathbb{P}^2(\mathbb{C})$ una curva liscia di grado $d \geq 4$, definita da un'equazione a coefficienti interi. Allora C ha un numero finito di punti razionali.

Osservazione 6.12: *(i) In altri termini una curva liscia di grado almeno quattro in $\mathbb{P}^2(\mathbb{C})$, definita su $\mathbb{Q}$, ha un numero finito di punti razionali (cfr Definizione 4.3).*
(ii) Questo risultato fu congetturato da Mordell (su $\mathbb{Q}$) e sotto forma più generale (con un campo di numeri al posto di $\mathbb{Q}$) da Weil. In realtà il Teorema 6.11 è un corollario di un risultato molto più generale dimostrato da Faltings.
(iii) Segue immediatamente dal Teorema 6.11 che per ogni $n \geq 4$, l'equazione di Fermat $X^n + Y^n = Z^n$ ha al più un numero finito di soluzioni intere.

Per quanto riguarda l'insieme dei punti razionali di una curva liscia di grado d in $\mathbb{P}^2(\mathbb{C})$ definita su $\mathbb{Q}$, possiamo riassumere la situazione nel modo seguente:

Grado	Insieme punti razionali
$d = 1, 2$	vuoto o infinito
$d = 3$	gruppo abeliano finitamente generato
$d \geq 4$	finito

Una curva algebrica liscia in $\mathbb{P}^2(\mathbb{C})$ (con la topologia trascendente) è omeomorfa a una superficie reale compatta, orientabile (cioè a un toro con g buchi), quindi la classificazione topologica delle curve algebriche piane lisce dipende da un'unico invariante: il *genere* g. Si dimostra che il genere di una curva piana liscia di grado d è $(d-1)(d-2)/2$, quindi una curva di grado $d \leq 2$ ha genere zero (*curve razionali*), una curva di grado tre ha genere uno (*curve ellittiche*), una curva di grado $d \geq 4$ ha genere $g \geq 2$ (*curve di tipo generale*). Vediamo quindi che la struttura dell'insieme dei punti razionali dipende dalla topologia della curva!

Bibliografia

[A-M] Atiyah, M.F. e Macdonald, I.G. *Introduction to commutative algebra*. Addison-Wesley Publishing Company (1969)

[E] Ellia, Ph. *Appunti di Geometria I*. Pitagora Ed.

[F] Fulton W. *Algebraic curves*. Benjamin/Cummings (1969)

[F2] Fulton W. *Algebraic topology, a first course*. Springer G.T.M. 153

[G-H] Griffiths, Ph. and Harris, J. *Principles of algebraic geometry* Wiley & sons (1978)

[H] Hartshorne, R. *Algebraic Geometry*. G.T.M. **52**, Springer (1977)

[J] Jacobson, N. *Basic Algebra, I*. W.H. Freeman and Company (1974)

[L] Lang, S. *Algebra (2^{nd} edition)*. Addison-Wesley Publishing Company (1984)

[M] Matsumura, H. *Commutative Algebra (2^{nd} edition)*. Benjamin-Cummings Publishing Company (1980)

[R] Reid, M. *Undergraduate Algebraic Geometry*. London Math. Sc. (1988)

[S] Sernesi, E. *Geometria 1*. Bollati-Boringhieri

[FAC] Serre, J.P. *Faisceaux algébriques cohérents*. Ann. of Math., 61, 197-278 (1955)

[Sh] Shafarevich, I. *Basic algebraic geometry, vol. 1 (2nd ed.)*. Springer (1994)