Un'introduzione alla geometria algebrica. (2a versione preliminare)

Ph. Ellia

Printed:
September-2005

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 $r = \text{codim}(Z)$) 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}. □

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 $\mathbb{I}$, 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:*

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

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

Le operazioni $\mathbf{V}, \mathbb{I}$ 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) $Z \subset Y \Longrightarrow \mathbb{I}(Y) \subset \mathbb{I}(Z)$

(iii) $\mathbb{I}(Z \cup Y) = \mathbb{I}(Z) \cap \mathbb{I}(Y)$

(iv) $I \subset \mathbb{I}(\mathbf{V}(I))$

(v) $\mathbf{V}(\mathbb{I}(Y)) = Y$

(vi) Se k è infinito, $\mathbb{I}(k^n) = \{0\}$

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

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

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

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 $k[X_1, ..., X_n]$}: $Z \to \mathbb{I}(Z)$
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 $\mathbf{V}, \mathbb{I}$ 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 $\mathbb{I}(Z)$ è un ideale radicale.*

Dimostrazione. Per semplificare poniamo $\mathbb{I} = \mathbb{I}(Z)$. Abbiamo $\mathbb{I} \subset r(\mathbb{I})$ perché ogni ideale è contenuto nel suo radicale. Sia $f \in r(\mathbb{I})$, per definizione esiste m tale che $f^m \in \mathbb{I}$. 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 $f \in \mathbb{I}$. □

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 $\mathbb{I}$:

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: $\mathbb{I}(\mathbf{V}(I)) = r(I)$.

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 $k[X_1, ..., X_n]\}$:
$Z \to \mathbb{I}(Z)$
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 $(\varphi \circ \psi)(I) = \mathbb{I}(\mathbf{V}(I))$. Dal teorema degli zeri: $\mathbb{I}(\mathbf{V}(I)) = r(I)$, siccome per ipotesi I è radicale, $\mathbb{I}(\mathbf{V}(I)) = I$, cioè $\varphi \circ \psi = Id$. □

Osservazione 2.11: *Quindi se $Z = \mathbf{V}(I)$, allora $\mathbb{I}(Z) = \mathbb{I}(\mathbf{V}(I)) = r(I)$, 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 $\mathbb{I}(\mathbf{V}(I)) = r(I)$. 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, $\mathbb{I}(Z) = r(m)$, inoltre $r(m) = m$ (perché m è primo, Esercizio 2.2), quindi $\mathbb{I}(Z) \neq \mathbf{S}$, e Z è non vuoto. Sia a un punto di Z allora $m = \mathbb{I}(Z) \subset \mathbb{I}(\{a\}) = (X_1 - a_1, ..., X_n - a_n)$ (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 $\mathbb{I}(Z)$, 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 $A(Z) := k[X_1, ..., X_n]/\mathbb{I}(Z)$.*

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 $\mathbb{I}(Z)$).*

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

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 $\mathbb{I}(Z \cap Y) = r(I + J)$ (qualsiasi siano gli ideali I, J che definiscono Z, Y). In particolare: $\mathbb{I}(Z \cap Y) = r(\mathbb{I}(Z) + \mathbb{I}(Y))$.

(3) Sia Z la parabola di equazione $y = x^2$ e sia Y l'asse $y = 0$ (quindi $\mathbb{I}(Z) = (y - x^2)$, $\mathbb{I}(Y) = (y)$). Mostrare che $\mathbb{I}(Z \cap Y) = (x, y)$ (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, $\mathbb{I}(Z)$ è generato da un unico elemento: $\mathbb{I}(Z) = (P(X))$. 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) $\mathbb{I}(Z)$ è un ideale primo.
(iii) $A(Z)$ è un anello integro.

DIMOSTRAZIONE. (i) $\Longrightarrow$ (ii) Per contrapposizione: se $\mathbb{I}(Z)$ non è primo esistono $P, F \notin \mathbb{I}(Z)$ tali che $PF \in \mathbb{I}(Z)$. 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 $P, F \notin \mathbb{I}(Z)$, 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 $Z_i \neq Z$, $\mathbb{I}(Z)$ è strettamente contenuto in $\mathbb{I}(Z_i)$. Possiamo quindi trovare $f_i \in \mathbb{I}(Z_i) \backslash \mathbb{I}(Z)$. Abbiamo $f_1 f_2 \in \mathbb{I}(Z_1) \cap \mathbb{I}(Z_2) = \mathbb{I}(Z_1 \cup Z_2) = \mathbb{I}(Z)$, quindi $\mathbb{I}(Z)$ non è primo.

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

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

DIMOSTRAZIONE. Infatti $\mathbb{I}(k^n) = \{0\}$ 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 $\mathbb{I}(T) = (Q)$ 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: $\mathbb{I}(\bigcup_i \mathbf{V}(P_i)) = \bigcap_i \mathbb{I}(\mathbf{V}(P_i))$. Siccome (P_i) è un ideale primo, $\mathbb{I}(\mathbf{V}(P_i)) = (P_i)$. 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 $\mathbb{I}(\mathbf{V}(Q)) = (Q)$ 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 $\mathbb{I}(Z \cup Y) = \sqrt{I} \cap \sqrt{J}$.

(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 $\mathbf{V}(P), \mathbb{I}(\mathbf{V}(P))$. 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* $\mathbb{I}(X)$*). 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 $P - Q \in \mathbb{I}(Z)$.*
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 $I = \mathbb{I}(Z)$). 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:

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

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 $(1-y)(1+y)-x^2 = 1-y^2-x^2 \in \mathbb{I}(Z)$, 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 $Q \notin \mathbb{I}(Z)$, 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 $\mathbf{V}(I) \cap \mathbf{V}(\mathbb{I}(Z)) = \mathbf{V}(I + \mathbb{I}(Z)) = \emptyset$, segue che $1 \in I + \mathbb{I}(Z)$. Quindi $1 = \sum_1^m H_i Q_{x_i} \pmod{\mathbb{I}(Z)}$. Moltiplicando per f: $f = \sum_1^m H_i Q_{x_i} f = \sum_1^m H_i Q_{x_i} (\frac{P_{x_i}}{Q_{x_i}}) \pmod{\mathbb{I}(Z)}$, finalmente $f = \sum_1^m H_i P_{x_i} \pmod{\mathbb{I}(Z)}$ 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 $\forall P \in \mathbb{I}(Y)$, $P(f_1, ..., f_m) = 0$ in $K(Z)$.*

DIMOSTRAZIONE. Se $f(Z) \subset Y$, per ogni $P \in \mathbb{I}(Y)$, $P \circ f$ 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 $K(Z)$, $\forall P \in \mathbb{I}(Y)$. Se $x \in Z$ e se f è definita in x allora $P(f(x)) = 0$, $\forall P \in \mathbb{I}(Y)$. 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 $\mathbb{I}(Y)$); 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 $P \in \mathbb{I}(Y)$, $P \circ f = 0$ 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 $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$, $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$. 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: $ht(\mathfrak{p}) := \sup\{n \in \mathbb{N}/$ 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:* $\dim A := \sup\{ht(\mathfrak{p})$ */ $\mathfrak{p} \subset A$ 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 $\varphi : \mathcal{H} \to \mathcal{I} : Z \to \pi(\mathbb{I}(Z))$ 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 $\mathbb{I}(Y)$).

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:* $\dim Y = \max_{1 \leq i \leq k}\{\dim Y_i\}$.

DIMOSTRAZIONE. È chiaro che $\max\{\dim Y_i\} \leq \dim Y$ (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 $(F) = \mathbb{I}(C)$. 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 $F(X, Y) = \Sigma a_{ij} X_i Y_j$, abbiamo $\Sigma a_{ij} x_i y_j = 0$ in $A(C)$ e y è radice del polinomio $\Sigma a_{ij} x_i T_j \in k(x)[T]$. 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: $ht(I) + \dim(A/I) = \dim A$.*

DIMOSTRAZIONE. Un buon testo di algebra. □

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

DIMOSTRAZIONE DELLA PROPOSIZIONE 5.15. (i) Se $X = \mathbf{V}(f)$ allora $\mathbb{I}(X) = (f)$ 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 $\mathbb{I}(X)$ è primo di altezza uno. Siccome $\mathbf{S}$ è fattoriale, $\mathbb{I}(X)$ è principale (Proposizione 5.17 (i)) quindi $\mathbb{I}(X) = (f)$ 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 $\mathbb{I}(X)$ 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 $\mathbb{I}(Y) = (P_1, ..., P_m)$. 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 $\mathbb{I}(Y)$).

Se $\mathbb{I}(Y) = (Q_1, ..., Q_p)$ 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 $\mathbb{I}(Y)$ 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 $\mathbb{I}(Y) = (x)$. 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 $\mathbb{I}(Y)$. 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 $Q \in \mathbb{I}(Y)$, $a_0 = 0$.

Sia $R = \{tq = (tq_1, ..., tq_n) |\ t \in k\}$ una retta per l'origine ($q \in R, q \neq O$). Se $Q \in \mathbb{I}(Y)$, 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: $Q_i(tq_1, ..., tq_n) = t^iQ_i(q_1, ..., q_n)$. 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 $\mathbb{I}(Y) = (P_1, ..., P_m)$, 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 $Q \in \mathbb{I}(Y)$). 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 $\mathbb{I}(Y) = (P_1, ..., P_m)$. 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 $F_i' \in \mathbb{I}(Y) = (F)$, 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 $\mathbb{I}(Y) = (P_1, ..., P_m)$, 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 $\mathbb{I}(C) = (f, g)$. 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 $\mathbb{I}(C)$ 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 $\mathbb{I}(X) = (f_1, ..., f_r), \mathbb{I}(Y) = (g_1, ..., g_t)$. Per ogni $i, g_i \circ f$ è una funzione regolare su $\mathbb{A}^n$ che si annulla su X, quindi $g_i \circ f \in \mathbb{I}(X)$, 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 $\mathbb{I}(C) = I$.

(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.

Bibliografia

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

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

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

[Sh] Shafarevich, I. *Basic algebraic geometry, vol. 1 (Second Edition, translated by M. Reid.)*. Springer (1994)