Elementi a caso di geometria algebrica

De Donato Paolo

Indice

Capitolo 1

Prerequisiti

1.1 Elementi di algebra commutativa

Da adesso in poi, se non diversamente specificato, ogni anello e sottoanello che considereremo sarà commutativo e dotato di unità.

Un anello A (commutativo con unità) è un *dominio di integrità* se e solo se per ogni $a, b \in A$ si ha

$$ab = 0 \Leftrightarrow a = 0 \text{ oppure } b = 0$$

in un dominio di identità vale la legge di cancellazione del prodotto, ovvero se $ac = bc$ e $c \neq 0$ allora $a = b$. Se A è un dominio di integrità possiamo definire il relativo *campo delle frazioni* come

$$\tilde{A} = \left\{ \frac{x}{y} \;\middle|\; x \in A, y \in A \setminus \{0\} \right\}$$

esso è chiaramente un campo (come lo è $\mathbb{Q}$ per $\mathbb{Z}$) ed è il più piccolo campo contenente A come sottoanello. Se $B[x_1, x_2, \ldots, x_n]$ anello dei polinomi è un dominio di integrità allora il relativo campo delle frazioni verrà indicato come $B(x_1, x_2, \ldots, x_n)$.

Sia A anello, diremo che un suo sottoinsieme $I \leq A$ è un *ideale* se e solo se

- per ogni $f, g \in I$ si ha $f - g \in I$;
- per ogni $f \in I$ e per ogni $g \in A$ si ha $fg \in I$.

dalla definizione segue immediatamente che $I = A \Leftrightarrow 1 \in I$.

Se U è un sottoinsieme di A allora indicheremo con $\langle U \rangle$ l'ideale generato da U. Non è difficile dimostrare che

$$\langle U \rangle = \{a_1 u_1 + a_2 u_2 + \cdots + a_n u_n \mid n \in \mathbb{N}, a_i \in A, u_i \in U\}$$

Un ideale I è *principale* se e solo se $I = \langle a \rangle$ per un certo $a \in I$, mentre un anello A è a ideali principali se e solo se tutti i suoi ideali non banali (diversi da $\{0\}$ e da A) sono principali. In un anello A ad ideali principali diremo che, presi $a, b, c \in A$, c è un *massimo comune divisore* di a e di b se e solo se

$$\langle c \rangle = \langle a, b \rangle$$

mentre è un *minimo comune multiplo* se e solo se $\langle c \rangle = \langle a \rangle \cap \langle b \rangle$.

Lemma 1.1.1 (Krull)**.** *In ogni anello esistono ideali massimali.*

Ricordiamo inoltre che se A è a fattorizzazione unica anche il relativo anello dei polinomi $A[x_1, x_2, \ldots, x_n]$ lo è. Anche se A è un dominio di integrità segue che $A[x_1, x_2, \ldots, x_n]$ lo è, in tal caso avremo perciò che

$$\deg(fg) = \deg f + \deg g$$

Se A è un anello ad ideali principali non è detto che anche $A[x]$ lo sia. Se però A è un *campo* allora $A[x]$ è a ideali principali. Questo risultato è valido solo per polinomi in una variabile, difatti l'ideale $\langle x, y \rangle$ in $\mathbb{C}[x, y]$ non è principale.

Proposizione 1.1.2. *Sia A anello e I un suo ideale, allora*

$$I \text{ primo} \Leftrightarrow \frac{A}{I} \text{ dominio di integrità}$$
$$I \text{ massimale} \Leftrightarrow \frac{A}{I} \text{ campo}$$

si ricorda che queste proprietà valgono solo se A è commutativo e unitario.

Sia A anello e $B \leq A$ sottoanello, allora per ogni $a_1, a_2, \ldots, a_n \in A$ poniamo

$$B[a_1, a_2, \ldots, a_n] = \{q(a_1, \ldots, a_n) \mid q \in B[x_1, x_2, \ldots, x_n]\}$$

mentre se A e B sono anche *campi* allora possiamo definire anche

$$B(a_1, a_2, \ldots, a_n) = \left\{ \frac{p(a_1, \ldots, a_n)}{q(a_1, \ldots, a_n)} \;\middle|\; p, q \in B[x_1, x_2, \ldots, x_n], q(a) \neq 0 \right\}$$

Ancora diciamo che A è *B-finitamente generato* se e solo se esistono elementi $a_1, \ldots, a_n \in A$ tali che

$$A = \left\{ \sum_{i=1}^{n} b_i a_i \;\middle|\; b_i \in B \right\}$$

e quindi A, se visto come B-modulo, possiede una base finita.

Proposizione 1.1.3. *Siano $C \leq B \leq A$ con A dominio di integrità. Se A è B-finitamente generato e B è C-finitamente generato allora A è C-finitamente generato.*

Dimostrazione. Se A è generato da $a_1, \ldots, a_s$ e B è generato da $b_1, \ldots, b_t$ allora

$$A = \left\{ \sum_{i=1}^{s} x_i a_i \;\middle|\; x_i \in B \right\} = \left\{ \sum_{i=1}^{s} \left(\sum_{j=1}^{t} c_{ij} b_j \right) a_i \;\middle|\; c_{ij} \in C \right\}$$
$$= \left\{ \sum_{i=1}^{s} \sum_{j=1}^{t} c_{ij} b_j a_i \;\middle|\; c_{ij} \in C \right\}$$

e quindi A è C-generato da tutte le coppie $a_i b_j$. ∎

Un elemento $a \in A$ è *integrale* rispetto a B se e solo se esiste $p \in B[x]$ *monico* tale che $p(a) = 0$ mentre diciamo che l'anello A è integro su B se e solo se è composto da elementi integri. Se A e $B \leq A$ sono campi allora diremo rispettivamente che $a \in A$ è *algebrico* su B e A è un'*estensione algebrica* su B. In tal caso inoltre il polinomio può non essere monico. Un ben noto risultato, che qui non dimostreremo, che riguarda il campo dei numeri complessi afferma che

Teorema 1.1.4. *Ogni estensione algebrica di $\mathbb{C}$ coincide con $\mathbb{C}$, ovvero gli zeri dei polinomi a coefficienti in $\mathbb{C}$ rispetto a qualunque campo che lo contiene sono ancora elementi di $\mathbb{C}$.*

Teorema 1.1.5. *Sia A un campo, $B \leq A$ un suo sottocampo ed $a \in A$. Possiamo allora considerare la seguente applicazione*

$$f : p \in B[x] \to p(a) \in B[a]$$

Dunque valgono le seguenti asserzioni:

- *Se a non è algebrico su B allora $B[a] \cong B[x]$;*
- *Se a è algebrico allora $B[a]$ è un campo.*

Dimostrazione. La funzione f è chiaramente un epimorfismo. Se a non è algebrico allora f deve essere iniettiva altrimenti l'ideale $I = \ker f$ è non banale e principale poiché $B[x]$ è a ideali principali essendo B campo. Per la legge di annullamento del prodotto I è un ideale primo ed essendo $B[x]$ ad ideali principali si può dimostrare che I è anche massimale. Dunque per la suriettività di f avremo che $B[a]$ è un campo. ∎

Osservazione. Se A è un campo ma B ne è solamente un sottoanello allora il risultato precedente può non essere verificato. Per esempio prendendo $A = \mathbb{Q}$ e $B = \mathbb{Z}$ allora l'elemento $a = 1/2$ non è integrale su $\mathbb{Z}$ anche se il polinomio $2x - 1 \in \mathbb{Z}[x]$ si annulla in esso.

Teorema 1.1.6. *Consideriamo i campi E, F, G, se F è un'estensione algebrica di E e G è un'estensione algebrica di F allora G è un'estensione algebrica di E.*

Capitolo 2

Varietà algebriche

2.1 Insiemi algebrici affini

Definizione 2.1.1. Lo spazio affine n-dimensionale sul campo $\mathbb{C}$ è

$$\mathbb{A}^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbb{C}, 1 \leq i \leq n\}$$

Osservazione. Naturalmente è $\mathbb{A}^n \cong \mathbb{C}^n$. Useremo tuttavia la notazione $\mathbb{C}^n$ per indicare l'insieme $\mathbb{C}^n$ dotato della struttura naturale di spazio vettoriale, mentre con il simbolo $\mathbb{A}^n$ indicheremo l'insieme $\mathbb{C}^n$ con la struttura dei *punti* $\mathbb{C}^n$.

Indicheremo con $\mathbb{C}[x_1, x_2, \ldots, x_n]$ l'insieme di tutti i polinomi in n variabili con coefficienti in $\mathbb{C}$.

Definizione 2.1.2. Un insieme $I \subseteq \mathbb{A}^n$ è un *insieme algebrico affine* se e solo se esiste $S \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$ tale che

$$I = \{p \in \mathbb{A}^n \mid f(p) = 0 \ \forall f \in S\} = \mathcal{V}(S)$$

Proposizione 2.1.3. *Gli insiemi algebrici affini su $\mathbb{A}^n$ sono i chiusi di una topologia su $\mathbb{A}^n$, ovvero*

1. *L'unione di un numero finito di insiemi algebrici è un insieme algebrico;*
2. *L'intersezione di una famiglia di insiemi algebrici è un insieme algebrico;*
3. *Gli insiemi $\emptyset$ e $\mathbb{A}^n$ sono algebrici.*

Dimostrazione. Dimostriamo i vari punti

1. Presi $S, T \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$ possiamo definire il *prodotto* di S e T come
$$S \cdot T = \{f(x_1, \ldots x_n)g(x_1, \ldots, x_n) \mid f \in S, g \in T\}$$
allora avremo chiaramente che $\mathcal{V}(S \cdot T) = \mathcal{V}(T) \cup \mathcal{V}(T)$.

2. Se prendiamo una famiglia $\{S_i\}_{i\in I} \subseteq \mathbb{C}[x_1, x_2, \ldots, x_n]$ allora avremo sicuramente che
$$\mathcal{V}\left(\bigcup_{i\in I} S_i\right) = \bigcap_{i\in I} \mathcal{V}(S_i)$$
3. Chiaramente $\emptyset = \mathcal{V}(\{1\})$ e $\mathbb{A}^n = \mathcal{V}(\{0\})$

■

Questa topologia è detta *topologia di Zariski* e sarà fondamentale in tutti i risultati che dimostreremo. Osserviamo che tutti gli aperti di $\mathbb{A}^n$ sono densi in quanto l'unico polinomio che ha come zeri tutto lo spazio $\mathbb{A}^n$ è ovviamente il polinomio nullo.

Osserviamo inoltre che per ogni $S, T \subseteq \mathbb{C}[x_1, \ldots, x_n]$ abbiamo che
$$S \subseteq T \Rightarrow \mathcal{V}(T) \subseteq \mathcal{V}(T)$$

Definizione 2.1.4. Un sottoinsieme non vuoto I di $\mathbb{C}[x_1, \ldots, x_n]$ è un *ideale* se e solo se

- Per ogni $f, g \in I$ si ha $f - g \in I$;
- Per ogni $f \in I$ e $g \in \mathbb{C}[x_1, \ldots, x_n]$ si ha $fg \in I$.

Un ideale I di $\mathbb{C}[x_1, \ldots, x_n]$ si dice *primo* se e solo se per ogni $f, g \in \mathbb{C}[x_1, \ldots, x_n]$ tale che $ab \in I$ si ha $f \in I$ oppure $g \in I$.

Non è difficile dimostrare che se $S \subseteq \mathbb{C}[x_1, \ldots, x_n]$ è un generico insieme non vuoto allora il più piccolo ideale I contenente S, detto *ideale generato*, è uguale a
$$\left\{ \sum_{i=1}^{l} g_i f_i \;\middle|\; l \in \mathbb{N}, f_i \in S, g_i \in \mathbb{C}[x_1, \ldots, x_n] \right\} = \langle S \rangle$$
e quindi si dimostra facilmente il seguente risultato

Proposizione 2.1.5. *Sia $S \subseteq \mathbb{C}[x_1, \ldots, x_n]$ allora*
$$\mathcal{V}(S) = \mathcal{V}(\langle S \rangle)$$

Osservazione. Esistono chiaramente ideali distinti che generano gli stessi insiemi algebrici affini, basti pensare ad esempio x ed x^2.

Definizione 2.1.6. Sia $X \subseteq \mathbb{A}^n$ sottoinsieme non vuoto, allora definiamo
$$\mathcal{I}(X) = \{f \in \mathbb{C}[x_1, \ldots, x_n] \mid f(p) = 0 \ \forall p \in X\}$$
si verifica immediatamente che
$$X \subseteq Y \Rightarrow \mathcal{I}(Y) \subseteq \mathcal{I}(X)$$

Proposizione 2.1.7. *Siano $X \subseteq \mathbb{A}^n$ e $S \subseteq \mathbb{C}[x_1, \ldots, x_n]$ non vuoti, allora*

$$S \subseteq \mathcal{I}[\mathcal{V}(S)]$$
$$X \subseteq \mathcal{V}[\mathcal{I}(X)]$$

Dimostrazione. Dimostriamo solo la prima inclusione, in quanto la seconda si dimostra in maniera del tutto analoga.

$$f \in S \Rightarrow \mathcal{V}(S) \subseteq \mathcal{V}(\{f\}) \Rightarrow f \in \mathcal{I}[\mathcal{V}(\{f\})] \subseteq \mathcal{I}[\mathcal{V}(S)]$$

■

Proposizione 2.1.8. *Se $X \subseteq \mathbb{A}^n$ allora $\mathcal{I}(X)$ è un ideale di $\mathbb{C}[x_1, \ldots, x_n]$.*

Dimostrazione. Segue immediatamente dalla definizione. ■

Ricapitolando l'applicazione $\mathcal{V}$ manda insiemi di $\mathbb{C}[x_1, \ldots, x_n]$ in insiemi algebrici affini mentre $\mathcal{I}$ manda insiemi di $\mathbb{A}^n$ in ideali. Questo ci suggerisce una correlazione tra ideali e insiemi algebrici affini e che tra i due vi sia una corrispondenza biunivoca.

Per dimostrare l'esistenza di tale corrispondenza dobbiamo procedere per gradi, dimostrando ogni volta un risultato parziale.

Definizione 2.1.9. Un anello A si dice *nöetheriano* se e solo se per ogni ideale $I \leq A$ esiste $L \subseteq I$ finito tale che $I = \langle L \rangle$.

Teorema 2.1.10 (base di Hilbert)**.** *L'anello $\mathbb{C}[x_1, \ldots, x_n]$ è nöetheriano.*

Dimostrazione. Dimostreremo una versione più forte, ovvero che se A è un anello nöetheriano allora anche $A[x]$ è nöetheriano, difatti $\mathbb{C}$ essendo un campo ha come unico ideale l'intero spazio che è generato da 1 e quindi la tesi segue immediatamente per induzione osservando che

$$\mathbb{C}[x_1, \ldots, x_{n-1}, x_n] = (\mathbb{C}[x_1, \ldots, x_{n-1}])[x_n]$$

Sia A anello nöetheriano e $J(I) \subseteq A$ l'insieme di tutti i coefficienti direttori dei polinomi non nulli dell'ideale $I \subseteq A[x]$ (ricordiamo che per un polinomio non nullo $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0$ con $a_m \neq 0$ il suo coefficiente direttore è il coefficiente a_m). L'insieme $J(I)$ è un ideale di A in quanto per ogni coppia di polinomi $f, g \in I$ di grado d e d' rispettivamente avremo che

$$f(x)x^{d'} - g(x)x^d \in I$$

e quindi anche la differenza dei loro coefficienti direttori sta in $J(I)$. Per ipotesi $J(I)$ è finitamente generato dunque esisteranno $f_1, f_2, \ldots, f_l \in I$ i cui coefficienti direttori generano $J(I)$. Posto

$$N = \max_i (\deg f_i)$$

e quindi per ogni intero $0 \leq m \leq N$ indicheremo con $J_m \subseteq J(I) = J$ l'ideale generato da tutti i coefficienti direttori dei polinomi non nulli di I con grado minore o uguale a m.

Sempre per ipotesi esisteranno $f_{m,1}, f_{m,2}, \ldots, f_{m,l_m} \in I$ i cui coefficienti direttori generano J_m, ponendo per comodità $f_{N,j} = f_j$. Definiamo infine $I' \subseteq I$ l'ideale generato dagli $f_{m,j}$ dimostreremo ora che $I' = I$ e quindi I è finitamente generato. Se per assurdo $I' \subset I$ potremmo sempre prendere $g \in I \setminus I'$ di grado minimo.

Ci sono due scenari possibili

- $g = c$ costante, in questo caso possiamo identificare i polinomi con i propri coefficienti direttori e quindi $g \in I'$.
- $\deg g > N$ il coefficiente direttore appartiene all'ideale J, quindi esisteranno dei coefficienti $\alpha_i \in A$ e degli interi $n_i \in \mathbb{N}_0$ tali che il polinomio
$$q(x) = \sum_{i=1}^{l} \alpha_i f_i(x) x^{n_i}$$
abbia lo stesso grado di g e lo stesso coefficiente direttore, dunque $\deg(g - q) < \deg g$ e per minimalità $g - q, q \in I'$ e quindi $g \in I'$.
- $\deg g = m \leq N$ con $m > 0$, si procede in maniera del tutto analoga sostituendo J con J_m e considerando i polinomi $f_{m,j}$ in quanto avranno sicuramente grado minore di g.

In tutti e tre i casi otteniamo un assurdo, dunque $I = I'$. ■

Per comodità indicheremo con $\langle S \rangle$ l'ideale generato da un sottoinsieme S di un anello.

Definizione 2.1.11. Preso un generico ideale I di un anello commutativo A definiamo il suo *radicale* come

$$\sqrt{I} = \{x \in A \mid \exists r \in \mathbb{N} \text{ tale che } x^r \in I\}$$

chiaramente $I \subseteq \sqrt{I}$, dimostriamo che è anch'esso un ideale di A. Prendiamo innanzitutto $x \in \sqrt{I}$ e $a \in A$, esisterà $r \in \mathbb{N}$ tale che

$$x^r \in I \Rightarrow (ax)^r = a^r x^r \in I \Rightarrow ax \in \sqrt{I}$$

sfruttando la commutatività di A. Ora poiché $(-x)^2 = x^2$ avremo che $x \in \sqrt{I} \Leftrightarrow -x \in \sqrt{I}$, se ora prendiamo $x, y \in \sqrt{I}$ con $r, s \in \mathbb{N}$ tali che $x^r, y^s \in I$ allora sempre sfruttando la commutatività della moltiplicazione in A

$$(x + y)^{r+s} = \sum_{i+j=r+s} \frac{(s+t)!}{i!j!} x^i y^j$$

che appartiene ad I in quanto per ogni addendo della somma al secondo membro avremo $i \geq r$ oppure $j \geq s$.

Prendiamo ora $I \subseteq \mathbb{C}[x_1, \ldots, x_n]$ ideale, dalla definizione segue immediatamente dalla legge di annullamento del prodotto che

$$\mathcal{V}(I) = \mathcal{V}\left(\sqrt{I}\right) \tag{2.1}$$

e quindi $\sqrt{I} \subseteq \mathcal{I}[\mathcal{V}(I)]$.

Teorema degli zeri di Hilbert. *Per ogni I ideale di $\mathbb{C}[x_1, \ldots, x_n]$ avremo che*

$$\mathcal{I}[\mathcal{V}(I)] = \sqrt{I}$$

Dimostriamo innanzitutto che il teorema degli zeri di Hilbert discende dal seguente risultato

Teorema debole degli zeri di Hilbert. *Se I è un ideale proprio di $\mathbb{C}[x_1, \ldots, x_n]$ allora $\mathcal{V}(I) \neq \emptyset$.*

Dal teorema della base di Hilbert avremo che $I = \langle f_1, f_2, \ldots, f_l \rangle \subset \mathbb{C}[x_1, \ldots, x_n] \subseteq \mathbb{C}[x_1, \ldots, x_n, x_{n+1}]$ e scegliamo $g \in \mathcal{I}[\mathcal{V}(I)]$ *non nullo.* Allora poniamo

$$J = \langle f_1, f_2, \ldots, f_l, x_{n+1}g - 1 \rangle$$

ideale di $\mathbb{C}[x_1, \ldots, x_n, x_{n+1}]$, mostriamo che $\mathcal{V}(J) = \emptyset$.

Se infatti per assurdo esistesse $p = (p_1, p_2, \ldots, p_{n+1}) \in \mathbb{A}^{n+1}$ tale che $p \in \mathcal{V}(J)$ allora $f_i(p_1, p_2, \ldots, p_n) = 0$ per ogni i e quindi $g(p_1, p_2, \ldots, p_n) = 0$ il che è assurdo in quanto $p_{n+1}g(p_1, p_2, \ldots, p_n) = 1$.

Dal teorema debole degli zeri di Hilbert allora $J = \mathbb{C}[x_1, x_2, \ldots, x_{n+1}]$ e in particolare $1 \in J$, esisteranno allora dei polinomi q_j in $n+1$ variabili tali che

$$\sum_{i=1}^{l} f_i q_i + (x_{n+1}g - 1)\, q_{l+1} = 1 \tag{2.2}$$

e prendiamo $N = \max_{1 \leq j \leq l+1} \deg_{x_{n+1}} q_j$ dove gli q_j sono visti come polinomi in x_{n+1}.

per ogni $p \in \mathbb{A}^n$ tale che $g(p) \neq 0$ possiamo porre $x_{n+1} = 1/g(p)$ nella (2.2) per ottenere

$$g^{N+1}(p) = \sum_{i=1}^{l} c_i(p) f_i(p) \tag{2.3}$$

dove $c_i(x)$ è un polinomio in n variabili tale che

$$c_i(p) = \begin{cases} g^{N+1}(p) q_i\left(p, \frac{1}{g(p)}\right) & \text{se } g(p) \neq 0 \\ 0 & \text{se } g(p) = 0 \end{cases}$$

ma allora la (2.3) è verificata anche se $g(p) = 0$ e quindi $g^{N+1} \in I \Rightarrow g \in \sqrt{I}$ e il teorema degli zeri di Hilbert è dimostrato.

Proposizione 2.1.12. *Per ogni ideale I di A si ha* $\sqrt{\sqrt{I}} = \sqrt{I}$.

quindi l'estrazione del radicale è un'operazione idempotente.

Definizione 2.1.13. Diciamo che un ideale I è *radicale* se e solo se $I = \sqrt{I}$.

Dal teorema degli zeri, dalla proposizione 2.1.12 e dalla (2.1) si dimostra immediatamente che le due applicazioni

$$X \text{ sottoinsieme algebrico affine di } \mathbb{A}^n \to \mathcal{I}(X) \text{ ideale radicale}$$
$$I \text{ ideale radicale} \to \mathcal{V}(I) \text{ sottoinsieme algebrico affine di } \mathbb{A}^n$$

sono biunivoche e sono l'una l'inversa dell'altra.

2.2 Il teorema debole degli zeri di Hilbert

In questa sezione ci concentreremo esclusivamente sulla dimostrazione del teorema debole degli zeri di Hilbert che procederà per gradi. Per la decrescenza di $\mathcal{V}$ e dal lemma di Krull basta verificare il teorema debole degli zeri di Hilbert nel caso in cui I sia un ideale proprio massimale.

Non è difficile verificare che le seguenti asserzioni sono tra loro equivalenti

- I ideale massimale di $\mathbb{C}[x_1, \ldots, x_n]$;
- $\mathbb{C}[x_1, \ldots, x_n]/I$ è un campo e possiede un sottocampo isomorfo a $\mathbb{C}$;
- esiste un campo L e un epimorfismo $\varphi : \mathbb{C}[x_1, \ldots, x_n] \to L$ tale che $\ker \varphi = I$ ed $I \cap \mathbb{C} = \{0\}$.

l'ultimo punto in particolare è piuttosto interessante in quanto ci permette di lavorare sugli omomorfismi.

Lemma 2.2.1. *Sia A dominio di integrità, B sottoanello e $\alpha \in A$. Allora sono equivalenti le seguenti affermazioni:*

1. *α è integrale su B;*
2. *$B[\alpha]$ è B-finitamente generato;*
3. *Esiste C sottoanello di A B-finitamente generato contenente $B[\alpha]$.*

Dimostrazione. Sia α integrale su B, allora esiste un polinomio monico $f \in B[x]$ di grado $d \geq 1$ tale che $f(\alpha) = 0$. Se per assurdo $B[\alpha]$ non fosse generato dagli α^n per $n < d$ allora esisterà un polinomio $g \in B[x]$ di grado maggiore o uguale a d per cui $g(\alpha) \neq h(\alpha)$ per ogni $h \in B[x]$ con $\deg h < d$. Possiamo prendere $\deg g = m$ il più piccolo possibile, mentre indicheremo con a il suo parametro direttore.

Ma allora

$$\deg\left(g(x) - af(x)x^{m-d}\right) < m$$

e quindi esisterà un $h \in B[x]$ di grado strettamente minore di d per cui

$$h(\alpha) = g(\alpha) - af(\alpha)\alpha^{m-d} = g(\alpha)$$

il che è assurdo, quindi $B[\alpha] = \{h(\alpha) \mid h \in B[x], \deg h < d\}$ e quindi è generato da un numero finito di α^n.

Il terzo punto discende immediatamente dal secondo prendendo $C = B[\alpha]$, dimostriamo che il terzo implica il primo. Sia C un sottoanello di A contenente $B[\alpha]$ che come B-modulo è generato da un numero finito di elementi $c_1, c_2, \ldots, c_l \in C$.

In particolare $\alpha \in C$ e quindi esistono $b_{ij} \in B$, dove $1 \leq i, j \leq l$, tali che

$$\alpha c_i = \sum_{j=1}^{l} b_{ij}c_j \Rightarrow \sum_{j=1}^{l} (\delta_{ij}\alpha - b_{ij})\, c_j = 0 \Rightarrow (\alpha I - B)\, C = 0$$

dove I è la matrice $l \times l$ identica, $B = \{b_{ij}\}$ e C è il vettore colonna di componenti c_j non nulle. Poiché il teorema di Cramer si può estendere ai B-moduli con B dominio di integrità avremo che

$$0 = \det(\alpha I - B) = f(\alpha) \text{ con } f \in B[x] \text{ monico e } \deg f \leq l$$

e quindi α è integrale. ■

Proposizione 2.2.2. *Gli elementi di A che sono integrabili su B formano un sottoanello di A.*

Dimostrazione. Prendiamo α e β integrabili su B, chiaramente $B[\alpha - \beta]$ e $B[\alpha\beta]$ sono sottoanelli di $B[\alpha, \beta]$, ma $B[\alpha, \beta] = (B[\alpha])[\beta]$ che per l'integrabilità di β è $B[\alpha]$-finitamente generato, mentre $B[\alpha]$ è B-finitamente generato.

Per la proposizione 1.1.3 $B[\alpha, \beta]$ è B-finitamente generato e per il terzo punto della proposizione 2.2.1 $\alpha - \beta$ e $\alpha\beta$ sono integrabili. ■

Teorema 2.2.3. *Preso L campo e $K \leq L$, se esistono $\alpha_1, \alpha_2, \ldots, \alpha_l \in L$ tali che $L = K[\alpha_1, \ldots, \alpha_l]$ allora L è un'estensione algebrica di K.*

Dimostrazione. Utilizzeremo l'induzione su l.

Se $l = 1$ allora α_1 può essere algebrico o meno. Nel primo caso dalla proposizione di prima tutti gli elementi di L sarebbero algebrici su K e quindi ne è un'estensione algebrica, altrimenti l'epimorfismo

$$f \in K[x] \to f(\alpha_1) \in K[\alpha_1]$$

è biettivo, quindi $K[\alpha_1]$ non è un campo (i polinomi non costanti non possiedono inverso) in contraddizione con la nostra ipotesi.

Supponiamo il teorema verificato per $l-1$ e sia $L = K[\alpha_1, \ldots, \alpha_l]$. Indichiamo con K' il sottocampo di L generato da K e da α_l allora avremo che

$$L = (K[\alpha_l])\,[\alpha_1, \ldots, \alpha_{l-1}] = K'[\alpha_1, \ldots, \alpha_{l-1}]$$

e quindi L è un'estensione algebrica di K', in particolare α_i è algebrico su K'.

Se α_l fosse algebrico su K allora $K' = K[\alpha_l]$ e dal lemma 2.2.1 per ogni $a \in L$ l'anello $K'[a]$ è K'-finitamente generato. Ma $K'[a] \supseteq K[a]$ e K' è K-finitamente generato dunque a è algebrico su K, perciò L è un'estensione algebrica di K.

Supponiamo adesso che α_l non è algebrico su K, esisteranno dunque alcuni polinomi $p_{i,j}, q_{i,j} \in K[x]$ per ogni $1 \leq i \leq l-1$ tali che $p_{i,0} = q_{i,0} = 1$ e

$$\sum_{j=0}^{n_i} \frac{p_{i,j}(\alpha_l)}{q_{i,j}(\alpha_l)} \alpha_i^{n_i - j} = 0$$

Prendiamo ora

$$C = \operatorname*{lcm}_{i,j} q_{i,j}$$
$$c = C(\alpha_l) \in K[\alpha_l]$$

e quindi avremo un $P_i \in K[x]$ tale che

$$P_i(c\alpha_i) = (c\alpha_i)^{n_i} + \sum_{j=1}^{n_i} p_{i,j}(\alpha_l) \frac{c^j}{q_{i,j}(\alpha_l)} (c\alpha_i)^{n_i - j} = 0$$

e quindi $c\alpha_i$ è integrale su $K[\alpha_l]$ (non è un campo) per ogni i, quindi essendo $L = K[\alpha_l][\alpha_1, \ldots, \alpha_{l-1}]$ avremo che per ogni $a \in L$ esiste un intero N per cui $c^N a$ è integrabile su $K[\alpha_l]$.

Se ora prendessimo $p \in K[\alpha_l]$ con $\gcd(p, c) = 1$ (è sempre possibile trovarlo in quanto $K[\alpha_l]$ è isomorfo a $K[x]$) allora sia

$$a = \frac{1}{p} \in L$$

esisterebbe $N \in \mathbb{N}$ tale che c^N/p è integrale su $K[\alpha_l]$. Ma allora esisterebbero dei coefficienti $b_i \in K[\alpha_l]$ per cui

$$\left(\frac{c^N}{p}\right)^m + \sum_{i=0}^{m-1} b_i \left(\frac{c^N}{p}\right)^i = 0 \Rightarrow c^{mN} = -p \left(\sum_{i=0}^{m-1} b_i c^{iN} p^{m-1-i}\right)$$

e quindi p divide c^{mN} in $K[\alpha_l]$ il che è assurdo.

La contraddizione nasce dall'aver supposto che α_l non sia algebrico su K, dunque L è un'estensione algebrica di K e il teorema è così dimostrato. ■

Siamo adesso in grado di dimostrare il teorema debole degli zeri di Hilbert, per farlo procederemo per passi. Innanzitutto possiamo considerare un qualunque ideale massimale I di $\mathbb{C}[x_1, \ldots, x_n]$ e poniamo

$$K = \frac{\mathbb{C}[x_1, \ldots, x_n]}{I}$$

Esisterà dunque un epimorfismo $\varphi : \mathbb{C}[x_1, \ldots, x_n] \to L$ tale che $\ker \varphi = I$ e φ è iniettivo su $\mathbb{C}$, quindi possiamo supporre che $\mathbb{C} \leq L$ e φ è l'identità su $\mathbb{C}$. Posto inoltre $\alpha_i = \varphi(x_i)$ allora $L = \mathbb{C}[\alpha_1, \ldots, \alpha_n]$ e dai teoremi 2.2.3 e 1.1.4 avremo che $L = \mathbb{C}$.

Quindi $\alpha_i \in \mathbb{C}$ e inoltre $x_i - \alpha_i \in I$ per ogni i, possiamo quindi considerare l'ideale

$$I' = \langle x_i - \alpha_i | 1 \leq i \leq n \rangle \leq I$$

ora ogni polinomio di $\mathbb{C}[x_1, \ldots, x_n]$ può essere riscritto in funzione degli $x_i - \alpha_i$ al posto degli x_i senza cambiare di grado, quindi $\mathbb{C}[x_1, \ldots, x_n]/I' = \mathbb{C}$ campo dunque I' è massimale. Abbiamo così dimostrato che $I' = I$ e quindi

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathcal{V}(I) \neq \emptyset$$

Corollario 2.2.4. *Gli ideali massimali sono radicali.*

Dimostrazione. Sia I un ideale massimale, allora $I \leq \sqrt{I}$ e $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$. Se per assurdo fosse $\sqrt{I} = \mathbb{C}[x_1, \ldots, x_n]$ allora $\mathcal{V}(\sqrt{I}) = \emptyset \neq \mathcal{V}(I)$ per il teorema debole degli zeri di Hilbert, quindi per massimalità $I = \sqrt{I}$. ■

Corollario 2.2.5. *L'applicazione*

$$F : (p_1, \ldots, p_n) \to \langle x_1 - p_1, \ldots, x_n - p_n \rangle$$

tra punti di $\mathbb{A}^n$ e ideali massimali di $\mathbb{C}[x_1, \ldots, x_n]$ è biunivoca.

Dimostrazione. Dalla dimostrazione del teorema debole degli zeri di Hilbert ne abbiamo verificato la suriettività. Siano ora $p = (p_1, \ldots, p_n), q = (q_1, \ldots, q_n) \in \mathbb{A}^n$ con $p_n \neq q_n$, possiamo quindi costruire il polinomio

$$f(x) = \sum_{i=1}^{n-1} (x_i - p_i)(x_i - q_i) + (x_n - p_n)$$

chiaramente $f \in F(p)$ ma $f(q) \neq 0$ e quindi $F(p) \neq F(q)$. ■

Quindi possiamo identificare $\mathbb{A}^n$ direttamente con l'insieme degli ideali massimali di $\mathbb{C}[x_1, \ldots, x_n]$. Per questo motivo non abbiamo specificato fin dall'inizio $\mathbb{C}^n$ in quanto anche prendendo un qualunque altro campo la struttura rimane invariata.

Corollario 2.2.6. *Lo spazio $\mathbb{A}^n$ con la topologia di Zariski è compatto.*

Dimostrazione. La compattezza di $\mathbb{A}^n$ equivale a dimostrare che per ogni famiglia di chiusi $\{C_i\}_{i\in I}$ tali che $\bigcap_{i\in I} C_i = \emptyset$ esistono $C_{i_1}, C_{i_2}, \dots C_{i_m}$ tali che

$$C_{i_1} \cap C_{i_2} \cap \cdots \cap C_{i_m} = \emptyset$$

Presi $L_i \subseteq \mathbb{C}[x_1, \dots, x_n]$ tali che $C_i = \mathcal{V}(L_i)$ dal teorema debole degli zeri di Hilbert l'ideale $\langle L_i | i \in I\rangle$ coincide con $\mathbb{C}[x_1, \dots, x_n]$ e in particolare contiene l'unità. Esisteranno allora $f_{n_i} \in L_{n_i}$ e $g_i \in \mathbb{C}[x_1, \dots, x_n]$ per $1 \leq i \leq m$ tali che

$$1 = \sum_{i=1}^{m} g_i f_{n_i}$$

e quindi $\mathcal{V}(L_{n_1}, \dots, L_{n_m}) = \emptyset$. ■

2.3 Insiemi proiettivi

Definizione 2.3.1. Lo spazio proiettivo di dimensione n sul campo $\mathbb{C}$ è il seguente insieme

$$\mathbb{P}^n\mathbb{C} = \frac{\mathbb{A}^{n+1} \setminus \{0\}}{\sim}$$

dove $\sim$ è la relazione di equivalenza su $\mathbb{A}^{n+1}$ definita come

$$x \sim y \Leftrightarrow \exists \lambda \in \mathbb{C} \setminus \{0\} : x = \lambda y$$

gli elementi di $\mathbb{P}^n\mathbb{C}$ verranno indicati con le parentesi quadre $[x_0, x_1, \dots, x_n]$ per ricordarci che non sono punti ma classi di equivalenza.

Rivedere meglio dopo l'esame

A causa di questa relazione di equivalenza non possiamo valutare un polinomio arbitrario in $n+1$ variabili non può essere sempre valutato sui punti dello spazio proiettivo. Per poter definire un insieme algebrico proiettivo avremmo bisogno di particolari polinomi, detti *omogenei*. Un polinomio $p \in \mathbb{C}[x_0, x_1, \dots, x_n]$ è omogeneo se e solo se per ogni $x \in \mathbb{A}^{n+1}$ e per ogni $\lambda \in \mathbb{C}$ si ha

$$p(\lambda x) = \lambda^{\deg p} p(x) \tag{2.4}$$

Chiaramente nemmeno per i polinomi omogenei avrebbe senso valutarli sui punti proiettivi a meno che $k = 0$, ciononostante se un rappresentante di un punto proiettivo $x \in \mathbb{P}^n\mathbb{C}$ annulla un polinomio omogeneo allora tutti i suoi rappresentanti lo annullano, e quindi ha senso dire che $x \in \mathbb{P}^n\mathbb{C}$ *annulla* il polinomio omogeneo $p \in \mathbb{C}[x_0, x_1, \dots, x_n]$.

Proposizione 2.3.2. *Se $p \in \mathbb{C}[x_0, x_1, \dots, x_n]$ è un polinomio generico allora per ogni $k \in \mathbb{N}_0$ esiste un unico r_k polinomio nullo oppure omogeneo di grado k tale che*

$$p = \sum_{k=0}^{\deg p} r_k(x)$$

e questi r_k sono dette componenti omogenee *di p.*

La somma di due polinomi omogenei è omogeneo se e solo se hanno lo stesso grado, mentre il prodotto di polinomi omogenei è sempre omogeneo, quindi non formano un sottoanello dei polinomi e non possiamo definire un ideale composto esclusivamente da polinomi omogenei. Ciononostante introdurremo la seguente definizione di ideale omogeneo che risulta molto maneggevole per i nostri scopi.

Definizione 2.3.3. Diremo quindi che un ideale $I \leq \mathbb{C}[x_0, x_1, \ldots, x_n]$ è *omogeneo* se e solo se è generato da polinomi omogenei.

Da questa semplice definizione possiamo dimostrare questo notevole risultato di equivalenza

Lemma 2.3.4. *Un ideale $I \leq \mathbb{C}[x_0, x_1, \ldots, x_n]$ è omogeneo se e solo se le componenti omogenee di ogni elemento p di I appartengono esse stesse a I.*

Dimostrazione. Sia I un ideale omogeneo, dalla definizione per ogni $p \in I$ esisteranno dei polinomi omogenei $p_k \in I$ e $a_k \in \mathbb{C}[x_0, x_1, \ldots, x_n]$ tali che

$$p = \sum_{k=1}^{n} a_k p_k$$

Ora per quanto detto all'inizio possiamo scrivere $a_k = \sum_{j=0}^{m_k} r_{kj}$ dove r_{kj} o è nullo oppure è un polinomio omogeneo di grado j e inoltre $r_{kj}p_k \in I$ per ogni j, k dalla definizione di ideale. Infine avremo che

$$p = \sum_{k=1}^{n} \sum_{j=0}^{m_k} r_{kj} p_k \tag{2.5}$$

Riordinando e raggruppando gli addendi della (2.5) otterremo una decomposizione di p con polinomi omogenei che a loro volta saranno somme di polinomi omogenei di I e quindi anche le componenti omogenee di p appartengono a I. ■

Esempio 1. L'ideale in $\mathbb{C}[x]$

$$\langle x - 1 \rangle$$

non è chiaramente omogeneo e gli unici polinomi omogenei che contiene sono quelli costanti. In particolare l'elemento $x-1$ può chiaramente essere scritto come somma di x e -1 entrambi omogenei, ma x non appartiene ad I.

Dal lemma precedente possiamo dimostrare molti risultati, tra i quali abbiamo

Proposizione 2.3.5. *Valgono le seguenti affermazioni:*

1. *Siano I, J ideali omogenei allora $I + J$ e $I \cap J$ sono ancora ideali omogenei;*

2. *Se I è omogeneo allora $\sqrt{I}$ è omogeneo;*

3. *Sia I omogeneo, allora I è primo se e solo se per ogni coppia f, g di polinomi omogenei con $fg \in I$ avremo che $f \in I$ oppure $g \in I$*

Dimostrazione. Dimostriamo i vari casi

1. Dalla definizione segue immediatamente che $I + J$ è omogeneo, mentre lavorando sulle componenti omogenee si dimostra facilmente che $I \cap J$ è omogeneo.

2. Per assurdo $\sqrt{I}$ non è omogeneo, quindi possiamo prendere $p \in \sqrt{I}$ di grado minimo le cui componenti omogenee non appartengono ad $\sqrt{I}$, ovvero la componente p_k di grado $k = \deg p$ non appartiene a $\sqrt{I}$ mentre quelle più piccole sì.

   Esisterà un $n \in \mathbb{N}$ tale che $p^n \in I$ e quindi p_k^n, che è anche la componente omogenea di grado nk di p^n, apparterrà a I dunque $p_k \in \sqrt{I}$ assurdo.

3. Dimostriamo che I è primo se soddisfa l'asserto. Per assurdo esistono due polinomi f e g tali che $fg \in I$ ma né f né g appartengono a I, dunque se indichiamo con f_i, g_j le componenti omogenee di f e g di grado i e j rispettivamente potremmo considerare $f_i, g_j \notin I$ con indici i più grandi possibili.

   Ora la componente di grado $i + j$ di fg è pari a

   $$\sum_{i'+j'=i+j} f_{i'} g_{i'} \in I$$

   se $i' > i$ allora per massimalità $f_{i'} \in I \Rightarrow f_{i'} g_{j'} \in I$ e analogamente per $j' > j$, quindi si ha $f_i g_j \in I$. Ma per ipotesi avremmo che $f_i \in I$ oppure $g_j \in I$ ottenendo una contraddizione, quindi I è un ideale primo.

■

Prendiamo ora un polinomio generico $f \in \mathbb{C}[x_0, x_1, \ldots, x_n]$ e $[x] \in \mathbb{P}^n\mathbb{C}$, diremo che $[x]$ *annulla* il polinomio generico f se e solo se un suo rappresentante (e quindi tutti) $x \in \mathbb{A}^{n+1}$ annulla tutte le componenti omogenee di f. Si osserva anche che se un punto proiettivo annulla un polinomio allora tutti i suoi rappresentanti annulleranno il polinomio nel senso usuale. Vale anche il viceversa, ovvero se tutti i rappresentanti di un punto omogeneo annullano un polinomio allora il punto lo annulla secondo la definizione appena introdotta.

Come per gli insiemi affini se F è un insieme di polinomi definiamo l'insieme

$$\mathcal{V}(F) = \{x \in \mathbb{P}^n\mathbb{C} \mid x \text{ annulla } f \quad \forall f \in F\}$$

e per quanto detto prima esisterà sempre un ideale *omogeneo* I tale che $\mathcal{V}(F) = \mathcal{V}(I)$. Ancora se $X \subseteq \mathbb{P}^n\mathbb{C}$ l'insieme

$$\mathcal{I}(X) = \langle f \in \mathbb{C}[x_0, x_1, \ldots, x_n] | f \text{ si annulla in } x \quad \forall x \in X \rangle$$

è un ideale omogeneo. Quindi possiamo ricostruire tutti i risultati sugli insiemi affini anche nello spazio proiettivo.

Grazie al lemma 2.3.4 possiamo riscrivere il teorema della base di Hilbert nella seguente forma:

Teorema 2.3.6. *Gli ideali omogenei di* $\mathbb{C}[x_0, x_1, \ldots, x_n]$ *sono generati da un numero finito di polinomi omogenei.*

e i teoremi degli zeri di Hilbert in versione omogenea (senza dimostrazione)

Teorema 2.3.7. *Sia* I *ideale omogeneo massimale proprio dell'anello dei polinomi, allora*

$$\mathcal{V}(I) = \emptyset \Leftrightarrow I = \langle x_0, x_1, \ldots, x_n \rangle$$

Teorema 2.3.8. *Per ogni* I *ideale omogeneo di* $\mathbb{C}[x_0, x_1, \ldots, x_n]$ *avremo che*

$$\mathcal{I}[\mathcal{V}(I)] = \sqrt{I}$$

Dimostrazione. Indichiamo con X' l'insieme dei punti in $\mathbb{A}^{n+1}$ che annullano tutti i polinomi di I. Poiché I è un ideale omogeneo allora un punto $x \in \mathbb{A}^{n+1}$ annulla tutti i polinomi dell'ideale I se e solo se x ne annulla le componenti omogenee, ovvero $[x] \in \mathcal{V}(I)$. Quindi avremo che

$$\mathcal{I}[\mathcal{V}(I)] = \mathcal{I}(X' \setminus \{0\}) = \sqrt{I}$$

e il teorema è dimostrato. ■

che determina una corrispondenza biunivoca tra ideali radicali omogenei di $\mathbb{C}[x_0, x_1, \ldots, x_n]$ e insiemi proiettivi algebrici.

2.4 Varietà algebriche

Definizione 2.4.1. Uno spazio topologico X è *riducibile* se e solo se esistono due sottoinsiemi chiusi X_1, X_2 diversi da X tali che $X = X_1 \cup X_2$. Uno spazio non riducibile è detto *irriducibile*.

Chiaramente gli spazi irriducibili sono connessi, mentre $\mathbb{R}$ è uno spazio connesso ma non irriducibile con la topologia usuale.

Proposizione 2.4.2. *Uno spazio topologico* X *è irriducibile se e solo se tutti gli aperti non vuoti sono densi. Inoltre se* X *è irriducibile allora tutti gli aperti di* X *sono irriducibili nella topologia indotta.*

Dimostrazione. La tesi segue immediatamente osservando che $C \subseteq X$ è chiuso se e solo se $X \setminus C$ è aperto e inoltre

$$X \setminus (C \cup D) = (X \setminus C) \cap (X \setminus D)$$

quindi gli aperti non vuoti hanno sempre intersezione non nulla. ■

Proposizione 2.4.3. *Lo spazio $\mathbb{A}^n$ con la topologia di Zariski è irriducibile.*

Dimostrazione. Presi due insiemi $I, J \subseteq \mathbb{C}[x_1, \ldots, x_n]$ tali che $\mathbb{A}^n = \mathcal{V}(I) \cup \mathcal{V}(J) = \mathcal{V}(IJ)$. Quindi almeno uno tra I e J deve contenere solamente il polinomio nullo 0. ■

Osservazione. Questo risultato ci chiarisce il motivo per cui introduciamo il concetto di irriducibilità in geometria algebrica: una curva irriducibile sarà formata da una sola componente, mentre curve riducibili saranno l'unione di più curve semplici.

Proposizione 2.4.4. *Sia X spazio topologico e $Y \subseteq X$ irriducibile, allora $\overline{Y}$ è irriducibile.*

Dimostrazione. Siano X_1, X_2 chiusi in X tali che $Y \subseteq \overline{Y} \subseteq X_1 \cup X_2$, per l'irriducibilità di Y avremo ad esempio che $Y \subseteq X_1 \Rightarrow \overline{Y} \subseteq X_1$ e quindi anche $\overline{Y}$ è irriducibile. ■

Definizione 2.4.5. Un qualunque insieme algebrico affine irriducibile di $\mathbb{A}^n$ rispetto alla topologia di Zariski è detto *varietà affine*. Sottoinsiemi aperti di varietà affini sono detti *varietà quasi-affini*.

Se $X \subseteq \mathbb{A}^n$ è una varietà affine allora definiamo le *sottovarietà affini* di X tutte le varietà affini di $\mathbb{A}^n$ contenute in X.

Proposizione 2.4.6. *Sia $X \subseteq \mathbb{A}^n$ insieme algebrico affine, allora X è una varietà se e solo se $I = \mathcal{I}(X)$ è un ideale primo.*

Dimostrazione. Sia X irriducibile con la topologia di Zariski, prendiamo $f, g \in \mathbb{C}[x_1, \ldots, x_n]$ tali che $fg \in I$ e quindi $X \subseteq \mathcal{V}(fg) = \mathcal{V}(f) \cup \mathcal{V}(g)$ e quindi avremo o $f \in I$ oppure $g \in I$.

Viceversa sia I ideale primo e prendiamo S_1, S_2 ideali di $\mathbb{C}[x_1, \ldots, x_n]$ tali che $X \subseteq \mathcal{V}(S_1) \cup \mathcal{V}(S_2) = \mathcal{V}(S_1 S_2)$, se $X \nsubseteq \mathcal{V}(S_i)$ allora esisterebbero $f_i \in S_i$ per $i = 1, 2$ che non si annullerebbero su tutti i punti di X, ma invece $f_1 f_2 \in I$ generando così un assurdo. ■

Definizione 2.4.7. Se X è un insieme affine definiamo l'*anello delle coordinate affini* di X come

$$\mathbb{C}[X] = \frac{\mathbb{C}[x_1, \ldots, x_n]}{\mathcal{I}(X)}$$

in particolare identifica i polinomi che assumono gli stessi valori su X.

Per quanto detto precedentemente se X è una varietà allora $\mathcal{I}(X)$ è primo e quindi $\mathbb{C}[X]$ è un dominio di integrità e quindi soddisfa ancora buona parte delle proprietà dei polinomi usuali. Prendiamo adesso la varietà affine $X = \{p\}$ composta da un singolo punto $p \in \mathbb{A}^n$. Allora $\mathcal{I}(X) = \langle x_1 - p_1, x_2 - p_2, \ldots, x_n - p_n \rangle$ e per ogni coppia di polinomi f e g abbiamo

$$f + \mathcal{I}(X) = g + \mathcal{I}(X) \Leftrightarrow f(p) = g(p)$$

e quindi l'elemento $f + \mathcal{I}(X) = \mathbb{C}[\{p\}]$ corrisponde esattamente alla valutazione del polinomio f nel punto p.

Quindi gli elementi di $\mathbb{C}[X]$ possono essere visti anche come le valutazioni dei polinomi in $\mathbb{C}[x_1, \ldots, x_n]$ sulla varietà X. D'altronde se $Y \subseteq X$ sono due varietà affini possiamo vedere l'applicazione

$$f + \mathcal{I}(X) \in \mathbb{C}[X] \to f + \mathcal{I}(Y) \in \mathbb{C}[Y]$$

come la valutazione di un polinomio su X sulla varietà Y. In particolare l'inclusione di varietà e un morfismo come vedremo più avanti.

Sull'anello delle coordinate affini di una varietà algebrica valgono risultati analoghi dimostrati in $\mathbb{A}^n$, in particolare otteniamo la seguente formulazione del teorema debole degli zeri di Hilbert

Teorema 2.4.8. *Sia X varietà affine e $I \subseteq \mathbb{C}[X]$ ideale i cui elementi non si annullano in alcun punto di X. Allora $I = \mathbb{C}[X]$.*

Dimostrazione. Identifichiamo I con l'ideale di $\mathbb{C}[x_1, \ldots, x_n]$ formato da tutti i rappresentanti degli elementi di I e $J = \mathcal{I}(X)$. Allora $\mathcal{V}(I \cup J) = \emptyset$ e dal teorema debole degli zeri di Hilbert esistono $p_1, \ldots, p_r \in I$, $p_{r+1}, \ldots, p_s \in J$ e $a_1, \ldots, a_s \in \mathbb{C}[x_1, \ldots, x_n]$ tali che

$$1 = \sum_{i=1}^{r} a_i p_i + \sum_{j=r+1}^{s} a_j p_j$$

ma allora

$$1 + J = \sum_{i=1}^{r} (a_i + J)(p_i + J) \in \mathbb{C}[X]$$

e quindi $1 \in I \subseteq \mathbb{C}[X]$. ■

La dimostrazione del seguente risultato non è nel programma

Teorema 2.4.9. *Gli insiemi chiusi di $\mathbb{A}^n$ sono unione finita di chiusi irriducibili.*

Dimostrazione. Un ideale K è primo se e solo se per ogni coppia di ideali $I, J \supseteq K$ tali che $I \cap J = K$ si ha $I = K$ oppure $J = K$. Quindi dobbiamo dimostrare che per ogni ideale proprio I di $\mathbb{C}[x_1, \ldots, x_n]$ esistono degli ideali

primi $I_1, I_2, \ldots, I_n$ contenenti I tali che $I = I_1 \cap I_2 \cap \cdots \cap I_n$ per dimostrare il teorema.

Indichiamo con $\mathcal{G}$ la classe degli ideali propri che non soddisfano tale proprietà e per assurdo è non vuota. Allora sfruttando il teorema della base di Hilbert e il lemma di Zorn la classe $\mathcal{G}$ possiede un qualche elemento massimale I'.

Ora I' non è nemmeno primo, dunque esisteranno J_1, J_2 contenenti propriamente I' tali che $J_1 \cap J_2 = I'$. Nessuno di questi due ideali coincide con l'intero spazio e per la massimalità di $\mathcal{G}$ saranno prodotto di ideali primi che conterranno I' raggiungendo così un assurdo. ■

Varietà su $\mathbb{A}^2$

Consideriamo un qualunque polinomio in due variabili $f \in \mathbb{C}[x, y]$, possiamo considerare l'ideale principale $\langle f \rangle$ i cui elementi si annullano negli zeri di f, e quindi possiamo associare ad ogni *curva algebrica piana* di equazione $f(x, y) = 0$ un ideale.

Possiamo scomporre f nei suoi fattori irriducibili

$$f(x, y) = f_1^{n_1}(x, y) f_2^{n_2}(x, y) \cdots f_k^{n_k}(x, y)$$

per la fattorizzazione unica dei polinomi avremo che se $n_i = 1$ per ogni i allora l'ideale è radicale e la relativa curva algebrica piana è detta *ridotta*. In particolare una curva algebrica piana è una varietà algebrica se e solo se f è irriducibile.

Enunciamo il seguente lemma senza però dimostrarlo

Lemma 2.4.10 (Gauss)**.** *Definiamo il campo*

$$\mathbb{C}(x) = \left\{ \frac{p(x)}{q(x)} \;\middle|\; p \in \mathbb{C}[x], q \in \mathbb{C}[x] \setminus \{0\} \right\}$$

allora ogni polinomio irriducibile in $\mathbb{C}[x, y] = \mathbb{C}[x][y]$ *è irriducibile anche in* $\mathbb{C}(x)[y]$.

Lemma 2.4.11. *Se* $f, g \in \mathbb{C}[x, y]$ *non hanno fattori comuni allora* $\mathcal{V}(f) \cap \mathcal{V}(g)$ *è formato da un numero finito di punti.*

Dimostrazione. I polinomi f e g possono essere scomposti in fattori irriducibili univocamente su $\mathbb{C}[x, y] = \mathbb{C}[x][y]$ quindi dal lemma di Gauss non hanno fattori in comune nemmeno in $\mathbb{C}(x)[y]$. Poiché $\mathbb{C}(x)$ è un campo il relativo spazio dei polinomi è a ideali principali e quindi $\langle f, g \rangle = \mathbb{C}(x)[y]$ e quindi esisteranno $r, s \in \mathbb{C}(x)[y]$ tali che $1 = r(x, y) f(x, y) + s(x, y) g(x, y)$.

Facendo il minimo comune multiplo degli elementi frazionari esisterà $d \in \mathbb{C}[x]$ ed $r', s' \in \mathbb{C}[x, y]$ tali che

$$d(x) = r'(x, y) f(x, y) + s'(x, y) g(x, y)$$

e quindi $(x_0, y_0) \in \mathcal{V}(f, g) \Rightarrow x_0 \in \mathcal{V}(d)$ e d, avendo una sola variabile, ha solamente un numero finito di zeri.

Procedendo in maniera del tutto analoga con la variabile y otterremo che anche le y_0 devono essere in numero finito e quindi si ha la tesi. ■

Varietà proiettive

Tutti i ragionamenti per le varietà affini possono essere estesi anche alle varietà proiettive, in particolare la proposizione 2.4.6 si può dimostrare ragionando esclusivamente sui polinomi e sugli ideali omogenei grazie alla proposizione 2.3.5. In particolare definiamo l'anello delle coordinate omogenee di $X \subseteq \mathbb{P}^n\mathbb{C}$ come

$$\mathbb{C}[X] = \frac{\mathbb{C}[x_0, x_1, \ldots, x_n]}{\mathcal{I}(X)}$$

Ora per ogni $0 \leq i \leq n$ l'insieme $U_i = \{x \in \mathbb{P}^n\mathbb{C} \mid x_i \neq 0\}$ è aperto nella topologia di Zariski e l'applicazione

$$\hat{x}_i : [x_0, x_1, \ldots, x_n] \in U_i \to \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right) \in \mathbb{A}^n$$

è ben definita ed è un omeomorfismo tramite il quale possiamo costruire l'applicazione F_i che ad ogni polinomio $f \in \mathbb{C}[x_1, \ldots, x_n]$ associa il polinomio omogeneo

$$x_i^{\deg f} f\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \ldots, \frac{x_n}{x_i}\right)$$

Quindi ogni varietà proiettiva X può essere ricoperta da insiemi aperti $X \cap U_i$ che a loro volta sono omeomorfi a varietà affini e omogeneizzando le coordinate (proiettare $\mathbb{A}^{n+1}$ su $\mathbb{P}^n\mathbb{C}$) ogni varietà affine diventa omeomorfa a qualche aperto della relativa varietà proiettiva.

2.5 Prodotto di varietà

In questa sezione vogliamo dimostrare che prodotti di varietà algebriche sono ancora varietà algebriche. Il caso affine risulta molto più semplice del caso proiettivo in quanto il prodotto di due spazi proiettivi non è uno spazio proiettivo.

Prendiamo $m, n \in \mathbb{N}$ e poniamo $\mathbb{A}^{m+n} = \mathbb{A}^m \times \mathbb{A}^n$, siamo inoltre $X \subseteq \mathbb{A}^m$ e $Y \subseteq \mathbb{A}^n$ varietà affini, se $I \subseteq \mathbb{C}[x_1, \ldots, x_m]$ e $J \subseteq \mathbb{C}[y_1, \ldots, y_m]$ sono gli ideali generatori di X e Y rispettivamente allora $X \times Y$ è generato dall'ideale

$$\langle f(x_1, \ldots, x_m), g(y_1, \ldots, y_n) | f \in I, g \in J \rangle$$

come è facilmente verificabile, quindi $X \times Y$ è chiuso in $\mathbb{A}^{m+n}$.

Osservazione. Benché il prodotto di chiusi sia ancora chiuso la topologia di Zariski su $\mathbb{A}^{m+n}$ non è la topologia prodotto. Se prendiamo ad esempio $m = n = 1$ e per assurdo la topologia di Zariski di $\mathbb{A}^2$ fosse la topologia prodotto allora, poiché la retta $x = y$ è chiusa in $\mathbb{A}^2$ avremo che $\mathbb{A}^1$ è uno spazio di Hausdorff. Ma nella topologia di Zariski di $\mathbb{A}^1$ i chiusi sono tutti e i soli insiemi finiti e quindi si ha una contraddizione.

In particolare abbiamo dimostrato che per ogni $x \in \mathbb{A}^m, y \in \mathbb{A}^n$ le applicazioni

$$p_1 : x' \in \mathbb{A}^m \to (x', y) \in \mathbb{A}^{m+n}$$
$$p_2 : y' \in \mathbb{A}^n \to (x, y') \in \mathbb{A}^{m+n}$$

sono degli omomorfismi in quanto biettive, continue e chiuse. Possiamo quindi dimostrare il seguente risultato di irriducibilità dal quale segue immediatamente che il prodotto di varietà affini è una varietà affine.

Lemma 2.5.1. *Siano X e Y sono spazi topologici irriducibili e Z spazio topologico generico per cui esiste un'applicazione $p : X \times Y \to Z$ biettiva. Posto $p_y(x) = q_x(y) = p(x, y)$ se le seguenti affermazioni sono verificate per ogni $x \in X$, $y \in Y$*

- *I sottoinsiemi $q_x(Y)$ e $p_y(X)$ sono chiusi in Z;*
- *Le proiezioni $p_y : X \to p_y(X)$, $q_x : Y \to q(Y)$ sono omeomorfismi.*

allora Z è uno spazio topologico irriducibile.

Dimostrazione. Poniamo $Z = Z_1 \cup Z_2$ con Z_i chiusi, avremo che $Z_i \cap p_y(X)$ è omeomorfo ad un chiuso di X per ogni $y \in Y$ e quindi per l'irriducibilità avremo che $p_y(X)$ è contenuto o in Z_1 o in Z_2.

Poniamo ora per $i = 1, 2$

$$Y_i = \{y \in Y \mid p_y(X) \subseteq Z_i\}$$

da cui si ha chiaramente che $Y = Y_1 \cup Y_2$ ma soprattutto

$$Y_i = \bigcap_{x \in X} q_x^{-1}(Z_i)$$

e quindi è chiuso. Per l'irriducibilità di Y possiamo porre $Y = Y_1$ e quindi $Z = p(X \times Y) = Z_1$. ∎

Passando alle varietà proiettive la difficoltà maggiore è il prodotto di spazi proiettivi non è affatto uno spazio proiettivo, come è facile da dimostrare. Per poter dare una definizione di spazio proiettivo prodotto bisogna

fare qualche passaggio supplementare, innanzitutto definiamo la seguente funzione

$$F : (x_0, x_1, \dots, x_m) \times (y_0, y_1, \dots, y_n) \in \mathbb{A}^{m+1} \times \mathbb{A}^{n+1} \\ \to (\dots, x_i y_j, \dots) \in \mathbb{A}^{(m+1)(n+1)}$$

dove al secondo membro si ottiene un vettore con tutti i prodotti delle coordinate di x e di y (non importa l'ordine). Per esempio se $m = n = 1$ allora avremo che

$$F\left[(x_0, x_1), (y_0, y_1)\right] = (x_0y_0, x_0y_1, x_1y_0, x_iy_1) \in \mathbb{A}^4$$

Innanzitutto osserviamo che se $x \neq 0$ e $y \neq 0$ allora $F(x, y) \neq 0$ e per ogni $\lambda, \mu \in \mathbb{R} \setminus \{0\}$

$$F(\lambda x, \mu y) = \lambda\mu F(x, y)$$

e quindi possiamo riscrivere F come una funzione che va da $\mathbb{P}^m\mathbb{C} \times \mathbb{P}^n\mathbb{C}$ in $\mathbb{P}^{mn+m+n}\mathbb{C}$.

Proposizione 2.5.2. *Sia F la funzione definita come sopra tra spazi proiettivi. Allora F è iniettiva e la sua immagine è un chiuso di $\mathbb{P}^{mn+m+n}\mathbb{C}$.*

Dimostrazione. Siano $x, x' \in \mathbb{A}^{m+1}$ e $y, y' \in \mathbb{A}^{n+1}$ tali che $F([x], [y]) = F([x'], [y'])$. Supponiamo inoltre che $x_i \neq 0$ e $y_j \neq 0$ allora esiste $\lambda \neq 0$ tale che per ogni indice j'

$$x_i y_{j'} = \lambda x'_i y'_{j'} \Rightarrow y_{j'} = \left(\lambda \frac{x'_i}{x_i}\right) y'_{j'}$$

e quindi $[y] = [y']$, mentre lavorando su j si dimostra che $[x] = [x']$.

Per dimostrare la chiusura dell'immagine possiamo indicizzare le variabili di un polinomio in $(m + 1)(n + 1)$ variabili nella forma z_{ij}. Possiamo così definire più facilmente l'omomorfismo

$$f : z_{ij} \in \mathbb{C}[z_{ij}] \to x_i y_j \in \mathbb{C}[x_0, \dots, x_m, y_0, \dots, y_m]$$

e si può verificare che $I = \ker f$ è un ideale omogeneo e possiamo porre $Z = \mathcal{V}(I) \subseteq \mathbb{P}^{mn+m+n}\mathbb{C}$. Ora per ogni coppia di indici $(i, j), (i', j')$ chiaramente avremo che

$$z_{ij}z_{i'j'} - z_{ij'}z_{i'j} \in I$$

Prendiamo ora $z \in Z$ generico, per comodità di notazione $z_{00} \neq 0$ e quindi avremo che per ogni i, j indici

$$z_{ij} = \frac{1}{z_{00}} z_{i0} z_{0j}$$

e quindi posto $x_i = z_{i0}$ e $y_j = z_{0j}$ avremo che $F(x, y) = z$ e quindi $z \in \operatorname{im} F$. Poiché $\operatorname{im} F \subseteq Z$ avremo che $\operatorname{im} F$ è chiuso e il teorema è così dimostrato. ∎

Diciamo che l'immagine di questa F è il *prodotto* degli spazi proiettivi $\mathbb{P}^m\mathbb{C}$ e $\mathbb{P}^n\mathbb{C}$. Da questo risultato segue immediatamente che $\operatorname{im} F$ soddisfa tutte le ipotesi del lemma 2.5.1 prendendo $p = F$.

Possiamo definire anche il prodotto di una varietà affine e di una proiettiva ponendo $\mathbb{A}^n \cong U_i \subseteq \mathbb{P}^n\mathbb{C}$.

2.6 Morfismi

Siano $X \subseteq \mathbb{A}^m$ e $Y \subseteq \mathbb{A}^n$ varietà affini, allora un'applicazione $\varphi : X \to Y$ è un *morfismo* se e solo se esistono $\phi_i \in \mathbb{C}[x_1, \ldots, x_m]$ per ogni $1 \leq i \leq n$ tali che

$$\varphi(x_1, \ldots, x_n) = (\phi_1(x_1, \ldots, x_n), \ldots, \phi_n(x_1, \ldots, x_n))$$

Esempio 2. Per ogni indice i possiamo definire i morfismi coordinate

$$x_i : x \in \mathbb{A}^n \to x_i \in \mathbb{A}$$

che associa ad ogni punto dell'intero spazio l'i-esima coordinata.

Osservazione. Possiamo prendere tranquillamente $\phi_i \in \mathbb{C}[X]$. Dalla definizione di coordinate affini anche se ϕ_i è una classe di equivalenza la sua valutazione nei punti di X non dipende dalla scelta del rappresentante.

Scegliere le componenti dei morfismi in $\mathbb{C}[X]$ al posto dell'intero spazio dei polinomi ci permette di "tagliare via" quelle componenti del polinomio che annullandosi su X non apportano un significativo contributo al morfismo.

Proposizione 2.6.1. *I morfismi sono applicazioni continue.*

Dimostrazione. Prendiamo I, J in modo tale che $X = \mathcal{V}(I)$ e $Y = \mathcal{V}(J)$, consideriamo adesso un qualunque ideale J' contenente J. Posto

$$I' = \{f \circ \varphi \mid f \in J'\}$$

avremo che I' è un ideale tale che

$$x \in \mathcal{V}(I') \Leftrightarrow \varphi(x) \in \mathcal{V}(J')$$

e quindi $\varphi^{-1}[\mathcal{V}(J')]$ è chiuso. ■

Un morfismo φ può essere tranquillamente esteso su tutto $\mathbb{A}^m$ e $\mathbb{A}^n$ essendo definito a partire da polinomi, in questo caso avremo che se un polinomio p si annulla su tutto Y allora $p \circ \varphi$ si annulla su tutto X. Quindi il pull-back

$$\varphi^* : f \in \mathbb{C}[Y] \to f \circ \varphi \in \mathbb{C}[X]$$

è ben definito.

Valgono chiaramente le seguenti proprietà

$$(\mathrm{id}_X)^* = \mathrm{id}_{C[X]} \qquad\qquad (f \circ g)^* = g^* \circ f^*$$

ma soprattutto abbiamo che $\psi_1 = \varphi^* x_i$ e quindi ad ogni applicazione tra spazi delle coordinate possiamo ricavarci sempre i relativi morfismi. Il pull-back permette di dimostrare il seguente

Teorema 2.6.2. *Il funtore tra la categoria delle $\mathbb{C}$-algebre finitamente generate integrali e quella delle varietà affini stabilisce un'equivalenza categoriale.*

Questa definizione risulta però troppo poco maneggevole, quindi se ne introdurrà un'altra equivalente ma che utilizza risultati di geometria commutativa.

Definizione 2.6.3. Un anello generico A è *locale* se e solo se possiede un unico ideale massimale.

Si dimostra facilmente che tutti gli elementi di un anello locale che non appartengono a tale ideale sono invertibili. Prendiamo inoltre D dominio di integrità con K come campo dei quozienti ed $S \subseteq D$ tale che

- $1 \in S$ e $0 \notin S$;
- Se $x, y \in S$ allora $xy \in S$.

allora definiamo

$$S^{-1}D = \left\{ \frac{x}{y} \in K \;\middle|\; x \in D, y \in S \right\}$$

che è chiaramente un anello contenente D.

Prendiamo adesso anche un ideale primo P di D non banale, allora $D \setminus P = P^c$ soddisfa tutte le ipotesi di S e poniamo $D_P = (P^c)^{-1} D$.

Proposizione 2.6.4. *L'anello D_P è un anello locale il cui unico ideale massimale è $P^* = \{x/y \mid x \in P, y \notin P\}$.*

Dimostrazione. Essendo P primo il suo complementare P^c soddisfa tutte le ipotesi di S. Che P^* sia un ideale di D_P è immediato da verificare, invece se $x, y \in P^c$ avremo che x/y è invertibile in D_P con inverso y/x e quindi P^* è l'unico ideale non banale di D_P. ∎

Definizione 2.6.5. Se $X \subseteq \mathbb{A}^n$ è una varietà quasi affine (aperto di una varietà affine) allora la funzione $f : X \to \mathbb{C}$ è *regolare* in $p \in X$ se e solo se esistono un aperto $U \subseteq X$ contenente p e dei polinomi $g, h \in \mathbb{C}[x_1, \ldots, x_n]$ tali che per ogni $u \in U$

$$h(u) \neq 0$$
$$f(u) = \frac{g(u)}{h(u)}$$

Una funzione è *regolare* in X se è regolare su tutti i punti.

I punti non regolari saranno detti *singolari*. Utilizzeremo la notazione (U, f) per indicare una funzione f regolare sulla varietà quasi affine U, mentre indicheremo con $\mathcal{O}(U)$ l'insieme di tutte le funzioni regolari su U.

Dalla definizione di punto regolare avremo che ogni funzione regolare in un punto sarà regolare anche in un intorno dello stesso, quindi lo spazio delle funzioni regolari in $p \in X$ coinciderebbe con

$$\bigcup_{\substack{p \in U \\ U \text{ aperto}}} \mathcal{O}(U)$$

in realtà come vedremo a breve non ci converrà considerare questo spazio direttamente in quanto vorremmo identificare le funzioni che coincidono "quasi ovunque". Dimostriamo prima il seguente risultato

Lemma 2.6.6. *Siano f e g due funzioni da X in $\mathbb{C}$ regolari rispettivamente sugli aperti U e U'. Se esiste $L \subseteq U \cap U'$ denso in X tale che $f(x) = g(x)$ per ogni $x \in L$ allora f e g coincidono su $U \cap U'$.*

Dimostrazione. Consideriamo $p, q \in \mathbb{C}[X]$ due polinomi che coincidono su un insieme denso L allora $\{x \in X \mid p(x) - q(x) = 0\}$ è chiuso e contiene L, perciò coincide con tutto X.

Prendiamo ora f regolare su U e g regolare su U' che coincidono in $L \subseteq U \cap U'$ denso in X. Prendiamo ora un $x \in U \cap U'$ generico, esisteranno dunque due aperti $x \in U_1 \subseteq U$ e $x \in U_2 \subseteq U'$ tali che $f = p/q$ su U_1 e $g = p'/q'$ su U_2. Ma $U_1 \cap U_2 \cap L \neq \emptyset$ per densità quindi

$$p(y)q'(y) = p'(y)q(y) \quad \forall y \in U_1 \cap U_2 \cap L$$

L'insieme $U_1 \cap U_2 \cap L$ è ancora denso in quanto l'intersezione finita di aperti non vuoti è diversa da $\emptyset$ e per quanto detto prima questi polinomi coincideranno su tutto X, in particolare in x. Ora poiché $q(x), q'(x) \neq 0$ possiamo dividere e $f(x) = g(x)$ ottenendo così la tesi. ■

Osservazione. I due polinomi p e q possono non coincidere su tutto lo spazio $\mathbb{A}^n$, basta per esempio prendere $X = \{(0, y) \mid y \in \mathbb{A}\}$, $p = x + y^2$, $q = x^2 + y^2$. In questo caso l'insieme in cui coincidono è comunque chiuso in $\mathbb{A}^2$ ma non contiene alcun sottoinsieme denso.

Possiamo adesso definire la seguente relazione di equivalenza tra funzioni regolari su aperti di una varietà affine X

$$(U, f) \sim (V, g) \Leftrightarrow f(x) = g(x) \quad \forall x \in U \cap V$$

in particolare per il lemma precedente soddisfa la proprietà transitiva.

Possiamo adesso definire la seguente classe di anelli sulla varietà X

$$\mathcal{O}_p(X) = \{(U, f) \mid p \in U, U \text{ aperto di } X\} / \sim$$
$$\mathcal{O}_R(X) = \{(U, f) \mid U \neq \emptyset, U \text{ aperto di } X\} / \sim$$

e definiamo su essi le usuali operazioni di somma e prodotto tra classi di equivalenza. In questo modo $\mathcal{O}_p(X)$ è un anello locale con unico ideale massimale

$$m_p = \{(U, f) \in \mathcal{O}_p(X) \mid f(p) = 0\} / \sim \tag{2.6}$$

Invece $\mathcal{O}_R(X)$ è un campo chiamato anche *campo delle funzioni razionali* di X.

Proposizione 2.6.7. *Se X è una varietà (quasi-)affine e $V \subseteq X$ un suo aperto allora $\mathcal{O}_R(X)$ e $\mathcal{O}_R(V)$ sono isomorfi.*

Dimostrazione. L'isomorfismo è determinato dall'applicazione

$$[U, f]_\sim \in \mathcal{O}_R(X) \to [U \cap V, f]_\sim \in \mathcal{O}_R(V)$$

■

Dimostriamo il seguente risultato, prima per le varietà affini e poi per quelle proiettive.

Proposizione 2.6.8. *Se X è una varietà affine e $\mathbb{C}[X]$ il suo anello delle coordinate affini. Se $M_p = \{f \in \mathbb{C}[X] \mid f(p) = 0\}$ allora abbiamo che*

1. $\mathcal{O}(X) \equiv \mathbb{C}[X]$;
2. $\mathcal{O}_p(X) \equiv C[X]_{M_p}$;
3. $\mathcal{O}_R(X) \equiv \mathbb{C}(X)$.

Si ricorda che $\mathbb{C}(X)$ è il campo dei quozienti di $\mathbb{C}[X]$ definito come $\mathbb{C}(X) = \{\frac{g}{h} \mid g, h \in \mathbb{C}[X], h \neq 0\}$.

Dimostrazione. Per ogni $h \in \mathbb{C}[X]$ consideriamo l'aperto

$$U_h = \{x \in X \mid h(x) \neq 0\}$$

Definiamo le seguenti applicazioni

$$\Psi : p \in \mathbb{C}[X] \to p \in \mathcal{O}(X)$$
$$\psi : \frac{p}{q} \in \mathbb{C}[X]_{M_p} \to \left[U_q, \frac{p}{q}\right] \in \mathcal{O}_p(X)$$
$$\psi' : \frac{p}{q} \in \mathbb{C}(X) \to \left[U_q, \frac{p}{q}\right] \in \mathcal{O}_R(X)$$

tutte le applicazioni sono iniettive mentre ψ e ψ' sono anche suriettive e Ψ è una restrizione di ψ. Inoltre $\mathcal{O}(X) \subseteq \mathcal{O}_p(X)$ per ogni p e quindi applicando ψ ad entrambi i membri

$$\mathbb{C}[X] \subseteq \mathcal{O}(X) \subseteq \bigcup_{p \in X} \mathbb{C}[X]_{M_p}$$

Ora sia $f \in \mathcal{O}(X)$, per ogni punto $p \in X$ esiste un aperto U_p contenente p e due polinomi $g_p, h_p \in \mathbb{C}[X]$ tali che h_p non si annulla mai in U_p. Dunque $h_p f = g_p$ sempre su U_p e quindi applicando il lemma 2.6.6 coincideranno su tutto X in quanto sia g_p che $h_p f$ sono funzioni regolari su tutto X

Questo significa che l'ideale generato dagli h_p al variare di $p \in X$ non si annulla mai, dal teorema debole degli zeri di Hilbert sulle varietà esistono $f_1, \ldots, f_t \in \mathbb{C}[X]$ tali che

$$\sum_{i=1}^{t} f_i h_i = 1$$

quindi

$$f = \sum_{i=1}^{t} f_i f h_i = \sum_{i=1}^{t} f_i g_i \in \mathbb{C}[X]$$

su tutto X. ■

Da ora in poi identificheremo con $\mathbb{C}(X)$ anche il campo delle funzioni razionali di X. Per quanto riguarda le varietà proiettive il lavoro è più delicato ma non eccessivamente difficile.

Definizione 2.6.9. Se $X \subseteq \mathbb{A}^n$ è una varietà quasi proiettiva (aperto di una varietà proiettiva) allora la funzione $f : X \to \mathbb{C}$ è *regolare* in $p \in X$ se e solo se esistono un aperto $U \subseteq X$ contenente p e dei polinomi omogenei $g, h \in \mathbb{C}[x_1, \ldots, x_n]$ *con lo stesso grado* tali che per ogni $u \in U$

$$h(u) \neq 0$$
$$f(u) = \frac{g(u)}{h(u)}$$

Una funzione è *regolare* in X se è regolare su tutti i punti.

Anche per le varietà proiettiva vale il lemma 2.6.6 come è facile da verificare. Definiamo l'ideale omogeneo

$$N_p = \{f \in \mathbb{C}[X] \mid f \text{ si annulla in } p\}$$

Proposizione 2.6.10. *Se X è una varietà proiettiva allora*

1. $\mathcal{O}(X) \equiv \mathbb{C}$;
2. $\mathcal{O}_p(X) \equiv \{g/h \mid g, h \text{ omogenei dello stesso grado }, h(p) \neq 0\}$;
3. $\mathcal{O}_R(X) \equiv \{g/h \mid g, h \text{ omogenei dello stesso grado }, h \neq 0\}$.

Dimostrazione. Ricordiamo che $U_i = \{x_i \neq 0\}$ e $X_i = X \cap U_i$ è isomorfo ad una varietà affine. Dato che $\mathcal{O}_p(X)$ e un anello locale se $p_i \neq 0$ possiamo spostarci ad un aperto X_i e quindi utilizzare il precedente risultato sulle varietà affini.

Se f è una funzione regolare su un aperto di $X_i \cong \mathbb{A}^n$ esistono $p, q \in \mathbb{C}[x_1, \ldots, x_n]$ tali che

$$f(x_0, x_1, \ldots, x_n) = f\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, 1, \ldots, \frac{x_n}{x_i}\right) = \frac{p\left(x_0/x_i, \ldots, x_n/x_i\right)}{q\left(x_0/x_i, \ldots, x_n/x_i\right)} = \frac{x_i^k p\left(x_0/x_i, \ldots, x_n/x_i\right)}{x_i^k q\left(x_0/x_i, \ldots, x_n/x_i\right)}$$

con $k \geq \max\{\deg p, \deg q\}$. Indicando con $\tilde{p}$ e $\tilde{q}$ i polinomi al numeratore e al denominatore saranno omogenei con lo stesso grado k e $\tilde{q}(p) \neq 0$.

La dimostrazione del terzo punto è la stessa, quindi dobbiamo verificare solamente la prima affermazione. Sempre supponendo che $p \in X_i$ per la proposizione di prima ogni funzione regolare in p coincide con $g_i/x_i^{k_i}$ su X_i, dove $g \in \mathbb{C}[x_0, x_1, \ldots, x_n]$ è un polinomio omogeneo di grado k_i.

Per ogni $f \in \mathcal{O}(X)$ allora $x^{k_i} f$ può essere definito su tutto X ed è un polinomio omogeneo di grado k_i in $\mathbb{C}[X]$. Fissato

$$k \geq \sum_{i=0}^{n} k_i$$

allora per ogni g polinomio omogeneo di grado k avremo che anche gf è omogeneo di grado k e quindi anche gf^2 è omogeneo di grado k, iterando il procedimento avremo che gf^t è omogeneo di grado k per ogni $t \in \mathbb{N}$.

Se indichiamo con L lo *spazio vettoriale* su $\mathbb{C}$ dei polinomi omogenei di grado k allora possiamo vedere f come un endomorfismo di L. Poiché L è finitamente generato anche lo spazio degli endomorfismi, e in particolare il sottospazio generato dagli f^i, è finitamente generato quindi esistono $a_1, a_2, \ldots, a_m \in \mathbb{C}$ tali che

$$\left(f^m + a_1 f^{m-1} + \ldots + a_{m-1} f + a_m\right) x_i^k = 0$$

per ogni x_i. Ma allora il termine all'interno della parentesi si annulla in ogni punto di $\mathbb{P}^n\mathbb{C}$ e quindi è identicamente nullo. ■

Adesso abbiamo tutto il necessario per poter definire i morfismi tra varietà algebriche.

Definizione 2.6.11. Prese due varietà algebriche/proiettive X, Y un'applicazione

$$\psi : X \to Y$$

è un *morfismo* se e solo se è continuo e per ogni aperto $V \subseteq Y$ l'applicazione

$$\psi^* : f \in \mathcal{O}(V) \to f \circ \psi \in \mathcal{O}\left(\psi^{-1}(V)\right)$$

è un morfismo di anelli. Un morfismo è un *isomorfismo* se e solo se è invertibile e anche l'inverso è un morfismo.

Questa nuova definizione è valida per tutti i tipi di varietà date finora, e per le varietà affini è del tutto equivalente alla definizione data ad inizio sezione. In particolare l'applicazione di omogenizzazione tra $\mathbb{A}^n$ e gli aperti U_i di $\mathbb{P}^n\mathbb{C}$ sono isomorfismi.

Osservazione. Se X e Y sono varietà affini e $\psi^* : \mathbb{C}[Y] \to \mathbb{C}[X]$ è suriettiva allora ψ è iniettivo. Difatti presi $x, y \in X$ distinti esisterà chiaramente un polinomio $f \in \mathbb{C}[X]$ per cui $f(x) \neq f(y)$. Ma allora per la suriettività di ψ^* esiste $g \in \mathbb{C}[Y]$ tale che $g[\psi(z)] = f(z)$ per ogni $z \in X$ quindi $\psi(x) \neq \psi(y)$.

Il viceversa non è però valido, prendiamo $X = \mathbb{A}$ e $Y = \mathcal{V}(x^2 - y^3)$ e

$$\psi : t \in X \to (t^3, t^2) \in Y$$

allora ψ è chiaramente iniettivo (esercizio, si ricordi che lavorando sui complessi non è possibile estrarre la radice quadrata) ma

$$\psi^* : f(x, y) \in \mathbb{C}[Y] \to f(t^3, t^2) \in \mathbb{C}[X]$$

non è suriettivo in quanto $p(t) = t$ non è controimmagine di alcun elemento in quanto $\mathbb{C}[X] = \mathbb{C}[x]$.

Esempio 3. Consideriamo l'applicazione $\varphi : t \in \mathbb{A} \to (t^2, t^3) \in \mathbb{A}^2$. Innanzitutto φ è un omeomorfismo con l'immagine ma $\psi^* : \mathbb{C}[t^2, t^3] \to \mathbb{C}[t]$ non è invertibile.

Finora abbiamo lavorato con le seguenti tipologie di varietà:

- affini;
- quasi affini;
- proiettive;
- quasi proiettive.

vogliamo dimostrare che localmente sono tutte equivalenti a varietà affini. Nel caso delle varietà proiettive sappiamo già che esiste sempre un ricoprimento aperto di varietà affini, quindi anche le varietà quasi proiettive saranno ricoperte da varietà quasi affini.

Con un abuso di notazione chiameremo varietà affini anche gli insiemi isomorfi alle varietà affini.

Proposizione 2.6.12. *In ogni varietà X ci sta una base per la topologia di X formata da aperti affini.*

Dimostrazione. Prendiamo un generico punto $p \in X$ e V_1 un qualunque aperto contenente p. Ma V_1 è essa stessa una varietà quindi esistono un aperto $p \in V_2 \subseteq V_1$ e una varietà quasi affine $U \subseteq \mathbb{A}^n$ isomorfa a V_2. Sia $\psi : V_2 \to U$ tale isomorfismo e $q = \psi(p)$ e indichiamo con $\overline{U}$ la chiusura di U,

allora $\overline{U}$ deve essere necessariamente una varietà affine (gli aperti non vuoti delle varietà sono densi) che possiede U come aperto. L'insieme $Z = \overline{U} \setminus U$ è chiuso e non contiene q, quindi esisterà un polinomio $f \in \mathcal{I}(Z)$ tale che $f(q) \neq 0$.

Ora posto $H = \mathcal{V}(f)$ abbiamo che $Z \subseteq H$ ma $q \notin H$, inoltre posto

$$Z_1 = \mathcal{V}(x_{n+1}f - 1) \subseteq \mathbb{A}^{n+1}$$

allora Z_1 è una varietà affine (il polinomio $x_{n+1}f - 1$ è chiaramente irriducibile essendo lineare in x_{n+1}) e la seguente applicazione è chiaramente un morfismo di varietà

$$f : (a_1, \ldots, a_n, a_{n+1}) \in Z_1 \to (a_1, \ldots, a_n) \in \mathbb{A}^n$$

e se ne restringiamo l'immagine a $\mathbb{A}^n \setminus H$ diventa un isomorfismo con inversa

$$f^{-1} : (a_1, \ldots, a_n) \in \mathbb{A}^n \setminus H \to \left(a_1, \ldots, a_n, \frac{1}{f(a_1, \ldots, a_n)}\right) \in Z_1$$

e quindi $\mathbb{A}^n \setminus H$ è una varietà affine.

Anche $U \setminus H$ è un aperto di $\overline{U}$ perciò è irriducibile, inoltre $Z = \overline{U} \setminus U$ è contenuto in H e quindi $U \setminus H = (\mathbb{A}^n \setminus H) \cap \overline{U}$ chiuso nella varietà affine $\mathbb{A}^n \setminus H$. Abbiamo così dimostrato che $U \setminus H$ è una varietà affine aperta in U.

Il morfismo ψ^{-1} dunque la manderà in un aperto contenente p e contenuto in V_2. La dimostrazione è così conclusa. ■

Quindi quando si lavora su intorni piccoli dei punti di una varietà potremo sempre supporre che sia una varietà affine.

2.7 Dimensione di una varietà affine

Prima di introdurre il concetto di dimensione di una varietà affine dimostriamo alcuni risultati di algebra commutativa relativa alle estensioni trascendenti. Preso un generico campo A contenente $\mathbb{C}$, diciamo che A è una *estensione finita* di $\mathbb{C}$ se e solo se esistono $t_1, \ldots, t_l \in A$ tali che $A = \mathbb{C}(t_1, t_2, \ldots, t_l)$. Un estensione finita A è detta *trascendente* se e solo se non è una estensione algebrica, in tal caso diciamo che un qualunque sottoinsieme finito $\{a_1, a_2, \ldots, a_n\}$ di A è *trascendente* se e solo se non esiste alcun polinomio non nullo di $\mathbb{C}[x_1, \ldots, x_n]$ che si annulli in esso.

Proposizione 2.7.1. *Sia A estensione finita di $\mathbb{C}$, $T = \{t_1, \ldots, t_n\} \subseteq A$ insieme trascendente e $a \in A \setminus \{0\}$ elemento generico. Allora*

$$T \cup \{a\} \text{ insieme trascendente } \Leftrightarrow a \text{ trascendente rispetto a } \mathbb{C}(T)$$

Dimostrazione. Se $T \cup \{a\}$ non è trascendente allora esiste un polinomio $p \in \mathbb{C}[x_1, \ldots, x_n, x_{n+1}]$ tale che $p(t_1, \ldots, t_n, a) = 0$. Ma possiamo scrivere $p(t_1, \ldots, t_n, a) = p'(a)$ con $p' \in \mathbb{C}(T)[x]$ e quest'ultimo polinomio sarà sicuramente *non nullo* essendo T trascendente su $\mathbb{C}$. Perciò a è algebrico su $\mathbb{C}(T)$.

Viceversa supponiamo che a è algebrico su $\mathbb{C}(T)$. Esisteranno allora $p_j, q_j \in \mathbb{C}[x_1, \ldots, x_n]$ tali che

$$\sum_{j=0}^{l} \frac{p_j(t_1, \ldots, t_n)}{q_j(t_1, \ldots, t_n)} a^j = 0 \tag{2.7}$$

Se ora poniamo $q(x_1, \ldots, x_n) = \prod_j q_j(x_1, \ldots, x_n)$ e lo moltiplichiamo ad entrambi i membri della (2.7) troveremo un polinomio in $\mathbb{C}[x_1, \ldots, x_n, x_{n+1}]$ non identicamente nullo, in quanto $p_l(t_1, \ldots, t_n) \neq 0$ e $q(t_1, \ldots, t_n) \neq 0$, che si annullerà in $(t_1, \ldots, t_n, a)$ e quindi $T \cup \{a\}$ non è un insieme trascendente. ■

Un insieme finito trascendente massimale è detto *base trascendente*. Dalla proposizione precedente non è difficile verificare la seguente proposizione

Proposizione 2.7.2. *Sia A una estensione finita di $\mathbb{C}$. Un insieme trascendente $T = \{t_1, t_2, \ldots, t_n\}$ è una base di A se e solo se A è una estensione algebrica finita di $\mathbb{C}(t_1, \ldots, t_n)$.*

Corollario 2.7.3. *Se A è una estensione trascendente finita di $\mathbb{C}$ allora esiste una base trascendente di A.*

Dimostrazione. Posto $A = \mathbb{C}(t_1, t_2, \ldots, t_n)$ con $t_i \in A$, allora almeno uno dei t_i deve essere trascendente rispetto a $\mathbb{C}$ altrimenti per la proposizione 2.2.2 A sarebbe una estensione algebrica di $\mathbb{C}$. Possiamo dunque sempre prendere un sottoinsieme trascendente T di $\{t_1, \ldots, t_n\}$ che sia massimale in $\{t_1, \ldots, t_n\}$.

Allora per ogni $t_i \notin T$ avremo che t_i è algebrico su $\mathbb{C}(T)$ e quindi applicando di nuovo la proposizione 2.2.2 segue che A è una estensione algebrica di $\mathbb{C}(T)$ dunque T è una base trascendente. ■

Teorema 2.7.4. *Siano A e B campi dove A è una estensione finita di B. Allora esiste un sottoinsieme di A finito trascendente e massimale, inoltre due qualunque sottoinsiemi di A finiti trascendenti e massimali possiedono lo stesso numero di elementi.*

Dimostrazione. Consideriamo ora $P = \{p_1, \ldots, p_s\}$ e $Q = \{q_1, \ldots, q_t\}$ sottoinsiemi trascendenti massimali in A con $s \leq t$, supponiamo che gli unici elementi in comune che hanno sono i primi $k \in \mathbb{N}_0$ elementi con $k < s$.

Ora se tutti i q_i fossero algebrici su $\mathbb{C}(p_1, \ldots, p_k, p_{k+2}, \ldots, p_s)$ allora $\mathbb{C}(Q)$ sarebbe un'estensione algebrica di $\mathbb{C}(P \setminus \{p_{k+1}\})$ e per il teorema 1.1.6 seguirebbe che P non sarebbe massimale.

Quindi a meno di una nuova indicizzazione supponiamo che q_{k+1} non sia algebrico su $\mathbb{C}(p_1, \ldots, p_k, p_{k+2}, \ldots, p_s)$ pur essendolo su $\mathbb{C}(P)$. Dunque esisterà $f \in \mathbb{C}[x_1, \ldots, x_{s+1}]$ tale che

$$f(p_1, \ldots, p_n, x) \neq 0 \qquad f(p_1, \ldots, p_s, q_{k+1}) = 0$$

(la prima relazione la otteniamo poiché il polinomio non nullo viene preso in $\mathbb{C}(p_1, \ldots, p_s)[x]$). Raccogliendo nella variabile x_{k+1} avremo che

$$f(x_1, \ldots, x_s, x) = \sum_{j=0}^{l} g_j(x_1, \ldots, x_k, x_{k+2}, \ldots, x_s, x) x_{k+1}^j \tag{2.8}$$

con $l = \deg_{x_{k+1}} f$ e i polinomi g_j non sono tutti nulli se visti come elementi di $\mathbb{C}(p_1, \ldots, p_k, p_{k+2}, \ldots p_s)[x]$. Poiché q_{k+1} è trascendente su $\mathbb{C}(P \setminus \{p_{k+1}\})$ allora per tali g_j

$$g_j(p_1, \ldots, p_k, p_{k+2}, \ldots, p_s, q_{k+1}) \neq 0$$

e quindi il secondo membro della (2.8) è un polinomio non nullo se visto come elemento di $\mathbb{C}(p_1, \ldots, p_k, p_{k+2}, \ldots, p_s, q_{k+1})[x_{k+1}]$ e si annulla in p_{k+1}.

Abbiamo cos' dimostrato che p_{k+1} è algebrico rispetto all'insieme

$$P' = \{p_1, \ldots, p_k, q_{k+1}, p_{k+2}, \ldots, p_s\} = \{q_1, \ldots, q_k, q_{k+1}, p_{k+2}, \ldots, p_s\}$$

in particolare P' è un insieme trascendente e $\mathbb{C}(P)$ è una estensione algebrica di $\mathbb{C}(P')$. Sempre per il teorema 1.1.6 e per la proposizione 2.7.2 P' è una base trascendente.

Ora si rifà lo stesso e identico ragionamento su q_{k+2} e p_{k+2} fino a dimostrare che l'insieme

$$\{q_1, \ldots, q_s\}$$

è una base trascendente massimale contenuta in Q e quindi $s = t$. ■

Adesso osserviamo che da quanto detto nel capitolo precedete se X è una varietà affine allora $\mathbb{C}(X)$ è un'estensione finita di $\mathbb{C}$ generata dagli elementi nella forma $z_i = x_i + \mathcal{I}(X)$ quindi possiamo applicare tutti i risultati appena ottenuti.

Diciamo quindi che X ha *dimensione* $k \in \mathbb{N}_0$ se e solo se $\mathbb{C}(X)$ possiede una base trascendente di cardinalità k, che indicheremo anche con il simbolo $\dim X$. Se $X = \mathbb{A}^n$ allora $\mathbb{C}(\mathbb{A}^n) \cong \mathbb{C}(x_1, \ldots, x_n)$ e quindi $\dim \mathbb{A}^n = n$ mentre se $\dim X = 1$ diciamo che X è una *curva*.

Esempio 4. Consideriamo in $\mathbb{A}^2$ l'insieme algebrico generato dal polinomio $xy - 1 \in \mathbb{C}[x, y]$. Poiché è irriducibile l'ideale $\mathcal{I}(X)$ è primo e quindi X è una varietà algebrica e

$$C[X] = \{p(x) + q(y) \mid p, q \in \mathbb{C}[t]\}$$

Osserviamo che x e y sono trascendenti rispetto a $\mathbb{C}$ ma $\{x, y\}$ non è trascendente in quanto il polinomio $x_1x_2 - 1$ si annulla per $x_1 = x$ e $x_2 = y$, quindi $\dim X = 1$.

Nei prossimi capitoli vedremo come una varietà algebrica può essere vista come una varietà differenziabile e ottenere in tal modo una definizione equivalente di dimensione.

2.8 Differenziazione

In questa sezione utilizzeremo un altro metodo per ricondurci alla dimensione di una varietà tramite un approccio simile alla geometria differenziale, ovvero tramite le derivazioni. Consideriamo un generico anello commutativo unitario A e il relativo anello dei polinomi $A[x_1, x_2, \ldots, x_n]$, possiamo definire la *derivata parziale* i-esima come un'applicazione

$$\partial_{x_i} : A[x_1, x_2, \ldots, x_n] \to A[x_1, x_2, \ldots, x_n]$$

tale che

- $\partial_{x_i} a = 0$ per ogni $a \in A$;
- $\partial_{x_i} x_j = 0$ se $j \neq i$ mentre $\partial_{x_i} x_1 = 1$;
- $\partial_{x_i}(f + g) = \partial_{x_i} f + \partial_{x_i} g$;
- $\partial_{x_i}(fg) = g\partial_{x_i} f + f\partial_{x_i} g$.

Chiaramente la derivazione è un'applicazione A-lineare su $A[x_1, \ldots, x_n]$ visto come un A-modulo. Possiamo generalizzare il concetto di derivazione a qualunque anello commutativo unitario, e non solo agli anelli di polinomi.

Definizione 2.8.1. Sia A un anello commutativo con unità, diciamo che un'applicazione $D : A \to A$ è una *derivazione* se e solo se per ogni $a, b \in A$ si ha

$$D(a + b) = D(a) + D(b)$$
$$D(ab) = aD(b) + D(a)b$$

Diciamo che D è *costante* su $B \leq A$ sottoanello se e solo se per ogni $b \in B$ si ha $D(b) = 0$.

Osservazione. Se A è anche un dominio di integrità possiamo considerare il suo campo dei quozienti K. Se ora D è una derivazione di K avremo per ogni $a \in A \setminus \{0\}$

$$D(1) = D\left(a \cdot \frac{1}{a}\right) = \frac{D(a)}{a} + aD\left(\frac{1}{a}\right) \Rightarrow D\left(\frac{1}{a}\right) = \frac{D(1)}{a} - \frac{D(a)}{a^2}$$

e questo significa che D è univocamente determinata dai valori assunti su A. Viceversa una derivazione definita su A si estende in maniera univoca ad una derivazione su K.

Proposizione 2.8.2. *Lo spazio delle derivazioni di $\mathbb{C}(x_1, \ldots, x_n)$ costanti su $\mathbb{C}$ è un $\mathbb{C}(x_1, \ldots, x_n)$-spazio vettoriale di dimensione n.*

Dimostrazione. Una derivazione D su $\mathbb{C}[x_1, \ldots, x_n]$ è determinata univocamente dai valori assunti negli x_i ■

Da questo punto considereremo solo le derivazioni costanti su $\mathbb{C}$. Scegliamo ora una generica varietà X (che per la proposizione 2.6.12 possiamo sempre supporre affine) e consideriamo il relativo spazio dei polinomi $\mathbb{C}[X]$. Gli elementi di tale spazio sono le classi di equivalenza $f + \mathcal{I}(X)$ con $f \in \mathbb{C}[x_1, \ldots, x_n]$, ma $\mathbb{C}[X]$ è un anello e in particolare abbiamo

$$f(x_1, \ldots, x_n) + \mathcal{I}(X) = f(x_1 + \mathcal{I}(X), \ldots, x_n + \mathcal{I}(X))$$

e dunque non è difficile verificare che ogni derivazione D di $\mathbb{C}[X]$ soddisfa la regola di derivazione di funzioni composte

$$D(f + \mathcal{I}(X)) = \sum_{i=1}^{n} [\partial_{x_i} f + \mathcal{I}(X)] D(x_i + \mathcal{I}(X))$$

e per $f \in \mathcal{I}(X)$ il primo membro si annulla.

Il fatto più interessante è però l'implicazione opposta, ovvero se definiamo D solo sugli $x_i + \mathcal{I}(X)$ in modo tale che vale la precedente uguaglianza allora potremmo estenderla a tutto $\mathbb{C}[X]$. In altre parole

Proposizione 2.8.3. *Sia D una derivazione di $\mathbb{C}[x_1, \ldots, x_n]$ con $D(x_i) = f_i \in \mathbb{C}[x_1, \ldots, x_n]$. Considerata una varietà affine $X \subseteq \mathbb{A}^n$ se vale l'implicazione*

$$f \in \mathcal{I}(X) \Rightarrow \sum_{i=1}^{n} f_i \partial_{x_i} f \in \mathcal{I}(X) \tag{2.9}$$

allora possiamo definire D su $\mathbb{C}[X]$ in modo tale che

$$D(f + \mathcal{I}(X)) = D(f) + \mathcal{I}(X)$$

Questi risultati valgono in maniera del tutto analoga anche per le varietà proiettive, difatti la derivazione standard manda polinomi omogenei in altri polinomi omogenei di un grado inferiore. Quindi assumeremo che X sia una varietà generica.

Osservazione. Non tutte le derivazioni su $\mathbb{C}[x_1, \ldots, x_n]$ si possono trasportare su $\mathbb{C}[X]$. Si prenda ad esempio la varietà $y = x^2$ e la derivazione D su $\mathbb{C}[x, y]$ tale che $D(x) = y$ e $D(y) = x$. In particolare avremo che

$$D(y - x^2) = x - 2xy = x(1 - 2y)$$

che non si annulla in X. Inoltre $y \equiv x^2$ ma $D(y) = x \not\equiv 2xy = D(x^2)$ e quindi non è ben definita sulle classi di equivalenza.

Invece ponendo $D(x) = x$ e $D(y) = 2y$ la (2.9) è verificata e determina così una derivazione su $\mathbb{C}[X]$, in particolare $D(x^2) = 2xD(x) = 2x^2 = 2y = D(y)$.

Per una varietà affine X definiamo lo *spazio tangente* TX di X come l'insieme di tutte le derivazioni di $\mathbb{C}(X)$ visto come $\mathbb{C}(X)$-spazio vettoriale. Dimostriamo che se $t_1, t_2, \ldots, t_k$ è una base trascendente di $\mathbb{C}(X)$ allora $\dim TX = k$.

Se $\mathbb{C}(X) = \mathbb{C}(t_1, t_2, \ldots, t_k)$ allora $h(t_1, \ldots, t_k) = 0 \Leftrightarrow h = 0$ per ogni $h \in \mathbb{C}[x_1, \ldots, x_k]$. Quindi vi è una corrispondenza biunivoca tra $\mathbb{C}[X]$ e $\mathbb{C}[x_1, \ldots, x_k]$ e quindi ogni derivazione su quest'ultimo spazio corrisponde ad un'unica derivazione su $\mathbb{C}(X)$ e perciò

$$\dim TX = k = \dim X$$

Supponiamo ora che $K = \mathbb{C}(X)$ è algebrico su $F = \mathbb{C}(t_1, \ldots, t_n)$, per un risultato di teoria dei campi una volta dimostrato il risultato nel caso $K = F(y)$, con y algebrico rispetto ad F, segue immediatamente il caso generale. Preso $f \in \mathbb{C}[x]$ polinomio minimo di y e D una qualunque derivazione di F vogliamo determinare in quanti modi possibili può essere ricondotta ad una derivazione di K.

Sia allora $f^D \in F[x]$ il polinomio ottenuto derivando tutti i coefficienti di f, consideriamo allora una derivazione D' di K che estende D e $D'(y) = u$, allora $D'(ay^n) = D(a)y^n + nay^{n-1}D'(y)$ e quindi

$$0 = D'\left[f(y)\right] = f^D(y) + u\partial_x f(y)$$

ma f è il polinomio minimo di y quindi $\partial_x f(y) \neq 0$ e quindi per ogni derivazione D' che estende D si avrà

$$D'(y) = -\frac{f^D(y)}{\partial_x f(y)}$$

e quindi D' è ben definita a partire da D. Questi ragionamenti sono del tutto validi anche se D' non estende alcuna derivazione di F in quanto $t_1, \ldots, t_n$ è una base trascendente anche per K

Viceversa essendo f un polinomio minimo ogni altro polinomio che annulla y è un multiplo di f, quindi la derivazione D' così definita è ben posta. Abbiamo così dimostrato il

Teorema 2.8.4. *Se X è una varietà allora*

$$\dim X = \dim TX$$

Da teorema della base di Hilbert ogni varietà X può essere scritta nella forma $X = \mathcal{V}(f_1, f_2, \ldots, f_k)$ dunque le derivazioni di $\mathbb{C}(X)$ saranno indotte esclusivamente dagli $u_i \in \mathbb{C}(X)$ che annullano la (2.9) per ogni f_k sui punti di X, determinando così un sistema lineare di k equazioni in n incognite. Ora definiamo la matrice C di k righe e n colonne con elementi $c_{ij} = \partial_{x_j} f_i \in \mathbb{C}[X]$ e sia r il suo rango, allora si avrà

$$\dim TX = n - r$$

Da un noto risultato di algebra lineare esisteranno due matrici quadrate A $k \times k$ e B $n \times n$ a coefficienti in $\mathbb{C}(X)$ invertibili tali che

$$ACB = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$$

dove I_r è la matrice identica $r \times r$. Poiché il determinante è un polinomio rispetto ai coefficienti della matrice esisterà un aperto $U \subseteq X$ tale che per ogni $p \in U$ i determinanti di $A(p)$ e $B(p)$ saranno non nulli e quindi il rango di $C(p)$ sarà r per ogni $p \in U$.

Proposizione 2.8.5. *Se X è una varietà affine di dimensione $\dim X = n - k$ allora esistono $f_1, \ldots, f_k \in \mathbb{C}[x_1, \ldots, x_n]$ tali che $X = \mathcal{V}(f_1, \ldots, f_k)$. Se è una varietà proiettiva allora i polinomi sono omogenei.*

Dimostrazione. Per tutto il ragionamento detto sopra esistono $f_1, f_2, \ldots, f_l$ con $l \geq k$ che generano X la cui matrice C ha rango esattamente k. Questo significa che $l - k$ righe della matrice possono essere espresse come combinazione lineare delle k rimanenti. Per comodità supponiamo che le ultime $l - k$ righe possono essere scritte come combinazione lineare delle prime k, allora per ogni $1 \leq m \leq n$ e per ogni $j \geq k + 1$ avremo che

$$\partial_{x_m} f_j = a_{1j} \partial_{x_m} f_1 + a_{2j} \partial_{x_m} f_2 + \ldots + a_{kj} \partial_{x_m} f_k$$

con $a_{ij} \in \mathbb{C}$. Poiché l'uguaglianza vale per ogni m esiste $c_j \in \mathbb{C}$ tale che

$$f_j + c_j = a_{1j} f_1 + a_{2j} f_2 + \ldots + a_{kj} f_k$$

Poiché c_j appartiene all'ideale che genera X allora se $c_j \neq 0$ per un certo j avremmo che $X = \mathcal{V}(c_j)$ altrimenti tutti gli $f_{k+1}, f_{k+2}, \ldots, f_l$ appartengono all'ideale generato da $f_1, \ldots, f_k$ e quindi si ha la tesi. ■

Definiamo ora le derivazioni puntuali sull'anello $\mathcal{O}_p(X)$. Diremo che un'applicazione $D : \mathcal{O}_p(X) \to \mathbb{C}$ è una *derivazione puntuale* di X in p se e solo se soddisfa le stesse proprietà delle derivazioni costanti su $\mathbb{C}$ tranne che al posto della regola di derivazione del prodotto vale la seguente

$$D(fg) = f(p)D(g) + D(f)g(p)$$

lo spazio di tutte le derivazioni puntuali in p lo indicheremo con T_pX, il quale è chiaramente uno spazio vettoriale su $\mathbb{C}$.

Ragionando esattamente come per le derivazioni usuali se $D(y_i) = a_i \in \mathbb{C}$ allora per ogni $f \in \mathbb{C}[x_1, \ldots, x_n]$

$$D[f(y_1, \ldots, y_n)] = \sum_{i=1}^{n} a_i \partial_{x_i} f(p) \tag{2.10}$$

e quindi D è una derivazione puntuale se e solo se la (2.10) si annulla per ogni $f \in \mathcal{I}(X)$. Poiché ogni derivazione su $\mathbb{C}(X)$ induce una derivazione puntuale in $\mathcal{O}_p(X)$ allora

$$\dim T_pX \geq \dim TX = \dim X \tag{2.11}$$

Definizione 2.8.6. Un punto $p \in X$ è *liscio* se e solo se vale l'uguaglianza in (2.11), altrimenti è detto *singolare*.

Ricordiamo che $M_p = \{f \in \mathbb{C}[X] \mid f(p) = 0\}$ e poniamo M_p^2 l'ideale generato da $\{fg \mid f, g \in M_p\}$, quindi

$$\frac{M_p}{M_p^2} = \left\{ \sum_{i=1}^{n} c_i(y_i - p_i) + M_p^2 \;\middle|\; c_i \in \mathbb{C} \right\}$$

e quindi può essere trattato alla stregua di uno spazio vettoriale di dimensione al più n. Inoltre poiché

$$\mathbb{C}[X] = \mathbb{C} + M_p$$

e dato che le derivazioni si annullano in M_p^2 avremo che T_pX è isomorfo allo spazio duale di M_p/M_p^2 e in particolare

$$\dim T_pX = \dim \frac{M_p}{M_p^2} \tag{2.12}$$

Lo stesso e identico ragionamento vale anche per $\mathcal{O}_p(X)$ considerando l'ideale m_p definito in (2.6). Gli elementi saranno nella forma f/g dive f, g sono polinomi con $f(p) = 0$ e $g(p) \neq 0$, chiaramente possiamo scrivere $f(x) = \sum_i c_i(x_i - p_i) + M_p^2$ e quindi

$$\begin{aligned}
\frac{f(x)}{g(x)} &= \sum_{i=1}^{n} c_i \frac{x_i - p_i}{g(x)} + m_p^2 \\
&= \sum_{i=1}^{n} \frac{c_i}{g(p)}(x_i - p_i) + \sum_{i=1}^{n} c_i \frac{[g(p) - g(x)](x_i - p_i)}{g(p)g(x)} + m_p^2 \\
&= \sum_{i=1}^{n} \frac{c_i}{g(p)}(x_i - p_i) + m_p^2
\end{aligned}$$

quindi i binomi $x_i - p_i$ generano m_p/m_p^2. Quindi possiamo procedere alla stessa maniera ottenendo così

$$\dim T_p X = \dim \frac{m_p}{m_p^2} \tag{2.13}$$

Esempio 5. Consideriamo la curva piana $y^2 - x^2(x+1) = 0$, la matrice C vale allora

$$\begin{pmatrix} 2y & -x(3x+2) \end{pmatrix}$$

e il suo rango è massimo per ogni $(x, y) \neq (0, 0)$ all'interno della curva e quindi $\dim TX = 1$. Nel punto $(0, 0)$ abbiamo chiaramente che la dimensione di $M_{(0,0)}/M_{(0,0)}^2$ vale 2 e quindi $\dim T_0 X = 2 > 1$. Se invece prendessimo $(x, y) = (-1, 0)$ allora

$$0 = y^2 - x^2(x+1) = y^2 - \left[(x+1)^3 + (x+1) - 2(x+1)^2\right] \Rightarrow x+1 \in M_{(-1,0)}^2$$

e quindi $\dim M_{(-1,0)}/M_{(-1,0)}^2 = 1$.

Chiameremo *sottovarietà chiuse* i sottoinsiemi chiusi e irriducibili di una varietà generica, allora vale il seguente risultato

Proposizione 2.8.7. *Se X è una varietà e $Y \subset X$ una sottovarietà chiusa e propria allora* $\dim Y < \dim X$.

Dimostrazione. Chiaramente avremo che $\dim Y \leq \dim X$, supponiamo che X è una varietà affine altrimenti per il risultato precedente possiamo passare ad un sottoinsieme aperto affine di X e di Y. Se $\dim X = r$ allora a meno di semplificare i denominatori gli elementi di una base trascendente di $\mathbb{C}(X)$ si trovano in $\mathbb{C}[X]$.

Poiché $Y \subseteq X$ allora i $g_1, g_2, \ldots, g_r \in \mathbb{C}[Y]$ saranno immagine di certi $f_1, \ldots, f_r \in \mathbb{C}[X]$ mediante il pull-back dell'immersione, ora poiché l'inclusione è stretta esisterà un polinomio $g \in \mathbb{C}[X]$ che si annulla su Y ma non in X. Poiché $\dim X = r$ esisterà $p \in \mathbb{C}[x_1, x_2, \ldots, x_{r+1}]$ irriducibile non nullo tale che

$$p(f_1, \ldots, f_r, g) = 0$$

avendo supposto p irriducibile avremo che $p(x_1, \ldots, x_n, 0)$ non è identicamente nullo, ciononostante avremo che $p(g_1, \ldots, g_r, 0) = 0$ e quindi non esistono basi trascendenti di $\mathbb{C}(Y)$ di r elementi. ■

Corollario 2.8.8. *Se Y è il sottoinsieme delle singolarità di X allora la dimensione massima delle componenti irriducibili di Y è strettamente minore di* $\dim X$.

Corollario 2.8.9. *Una curva ha al più un numero finito di punti singolari.*

Dimostrazione. Per il teorema 2.4.9 gli insiemi algebrici sono unione finita di varietà irriducibili, e per il risultato precedente ciascuna di esse avrà dimensione 0, ovvero sono dei punti. ■

Dimensione di curve su $\mathbb{A}^2$

Concentriamoci di nuovo sulle curve piane, osserviamo che i punti singolari della curva piana ridotta $f(x,y)=0$ sono univocamente determinati dalle equazioni

$$\begin{aligned} f(x,y) &= 0 \\ \partial_x f(x,y) &= 0 \\ \partial_y f(x,y) &= 0 \end{aligned}$$

e quindi il corollario precedente discenderebbe dal lemma 2.4.11 in quanto, essendo la curva ridotta, questi polinomi non possono avere fattori comuni.

Adesso consideriamo $f \in \mathbb{C}[x,y]$ non nullo e $p=(x_0,y_0) \in \mathcal{V}(f)$, non è difficile verificare che per ogni $i \in \mathbb{N}$ esiste un unico polinomio $r_i(x,y)$ nullo oppure omogeneo di grado i, con $r_m, r_n \neq 0$ per $n \leq m$ e

$$f(x,y) = r_m(x-x_0, y-y_0) + r_{m-1}(x-x_0, y-y_0) + \cdots + r_n(x-x_0, y-y_0) \tag{2.14}$$

inoltre diremo che n è la *molteplicità* di p in $\mathcal{V}(f)$. Dalle proprietà delle componenti omogenee si verifica facilmente che la molteplicità di un prodotto di polinomi coincide con la somma delle rispettive molteplicità.

Se inoltre $f_i(x,y)$ è un polinomio omogeneo di grado i allora esiste un unico $p \in \mathbb{C}[x]$ tale che $f(x,y) = y^i p\,(x/y)$ e poiché $\mathbb{C}$ è un campo algebricamente chiuso avremo che

$$p(x) = \prod_{j=1}^{l} (a_j x + b_j)^{c_j}$$

con $\sum_j c_j = i$ e (a_j, b_j) non contemporaneamente nulli. Quindi

$$f(x-x_0, y-y_0) = \prod_{j=1}^{l} \left[a_j(x-x_0) + b_j(y-y_0)\right]^{c_j}$$

Se al posto della f mettiamo tutte le componenti connesse della (2.14) allora le rette di equazione $a_j(x-x_0)+b_j(y-y_0)=0$ sono le *rette tangenti* ad $\mathcal{V}(f)$.

2.9 Applicazioni razionali e birazionali

Nel capitolo sui morfismi abbiamo accennato alle funzioni razionali in quanto applicazioni regolari solamente su un aperto di una varietà. Come per i morfismi sono una "generalizzazione" delle funzioni regolari definiamo le applicazioni razionali come estensione delle funzioni razionali.

Definizione 2.9.1. Definiamo un'*applicazione razionale* ψ dalla varietà X alla varietà Y una qualunque applicazione $\psi : Z \to Y$ con $Z \subseteq X$ contenente almeno un aperto di X tale che per ogni $V \subseteq Z$ aperto di X la restrizione di ψ su V è un morfismo tra varietà.

L'applicazione razionale ψ è detta *dominante* se e solo se l'immagine di V mediante ψ è densa in Y per ogni $V \subseteq Z$ aperto.

Come per i morfismi usuali un'applicazione razionale dominante induce un omomorfismo di campi

$$\psi^* : f \in \mathbb{C}(Y) \to f \circ \psi \in \mathbb{C}(X)$$

la richiesta della dominanza è così motivata: per ogni $f \in \mathbb{C}(Y)$ esiste un aperto $V \subseteq Y$ su cui f è regolare. Sia U un aperto di X contenuto in Z per cui $\psi(U)$ è denso allora avrà intersezione non vuota con V e quindi $f \circ \psi$ è regolare sull'aperto $U \cap \psi^{-1}(V)$ che è ancora denso. Questo omomorfismo è anche iniettivo grazie proprio alla densità di $\psi(V)$ e al lemma 2.6.6.

Un'applicazione razionale dominante è anche *birazionale* se e solo se esiste l'inversa quasi ovunque ed è un'applicazione birazionale dominante.

Esempio 6. Prendiamo gli aperti affini $U_i = \{x_i \neq 0\}$ dello spazio proiettivo $\mathbb{P}^n\mathbb{C}$, allora l'inclusione di U_i in $\mathbb{P}^n\mathbb{C}$ è un'applicazione birazionale in quanto l'immagine è densa e possiamo prendere come inversa l'applicazione identica su U_i. In generale tutte le inclusioni di un aperto nell'intero spazio sono applicazioni birazionali.

Diremo che due varietà X e Y sono *birazionali* se e solo se esiste un'applicazione birazionale tra esse. Di particolare interesse nella geometria algebrica è la classificazione delle varietà a meno di una relazione di birazionalità in quanto sussiste il seguente risultato

Teorema 2.9.2. *Per ogni coppia di varietà X e Y si ha una corrispondenza biunivoca tra le applicazioni razionali dominanti da X in Y e i monomorfismi di $\mathbb{C}(Y)$ in $\mathbb{C}(X)$.*

Dimostrazione. Dobbiamo dimostrare solamente che ad ogni monomorfismo tra estensioni finite di $\mathbb{C}$ $f : K \to K'$ è associato un'unica applicazione razionale da X in Y con $\mathbb{C}(X) = K'$ e $\mathbb{C}(Y) = K$

Supponiamo inizialmente di aver già trovato queste due varietà. Lavorando su una base affine di Y possiamo supporlo affine e quindi, preso un generatore $y_1, \ldots, y_n$ di $\mathbb{C}[Y]$ essi genereranno anche $\mathbb{C}(Y)$ e $f(y_i)$ sono funzioni regolari sullo stesso aperto affine $U \subseteq X$. Ma allora $\mathcal{O}(U) = \mathbb{C}[U]$ e abbiamo così determinato una applicazione iniettiva

$$g : p \in \mathbb{C}[Y] \to f(p) \in \mathbb{C}[U]$$

Ma allora esiste un unico morfismo $\psi : U \to Y$ tale che $\psi^* = g$, in particolare se y_i fosse anche un generatore (di campi) di $\mathbb{C}(Y)$ allora avremo immediatamente che $\psi^* = f$.

Ci rimane dunque da dimostrare solamente che se Y è una varietà allora $\mathbb{C}(Y)$ è una estensione finita di $\mathbb{C}$ e che per ogni K estensione finita di $\mathbb{C}$ esiste una varietà Y tale che $K = \mathbb{C}(Y)$. Dato che $\mathbb{C}(Y)$ è un anello locale possiamo sempre scegliere Y affine e quindi $\mathbb{C}(Y)$ è generato dagli y_i. Viceversa siano $a_1, a_2, \ldots, a_n \in K$ un generatore di K allora posto

$$F : p \in \mathbb{C}[x_1, \ldots, x_n] \to f(p) \in \mathbb{C}[a_1, \ldots, a_n]$$

avremo che $\mathbb{C}(a_1, \ldots, a_n) = K$ e l'ideale $I = \ker F$ induce una varietà Y tale che $K = \mathbb{C}(Y)$. ■

Corollario 2.9.3. *Due varietà sono birazionali se e solo se i rispettivi campi sono isomorfi.*

Anelli a valutazione discreta

In questa sezione ci concentreremo sulle curve ($\dim X = 1$) di $\mathbb{P}^n\mathbb{C}$.

Definizione 2.9.4. Un dominio di integrità D è un *anello a valutazione discreta* se e solo se esiste $t \in D$, detto *parametro di uniformizzazione*, tale che per ogni $a \in D \setminus \{0\}$ esistono $u \in D$ invertibile e $n \in \mathbb{N}_0$, detto *ordine* di a, tali che

$$a = ut^n \tag{2.15}$$

e questa scrittura è unica. Si può estendere il concetto di ordine anche sull'anello dei quozienti di D, in questo caso avremo che $n \in \mathbb{Z}$.

Proposizione 2.9.5. *Se p è un punto liscio della curva C allora $\mathcal{O}_p(C)$ è un anello a valutazione discreta.*

Dimostrazione. Sappiamo già che $\mathcal{O}_p(C)$ è un anello locale che ha come ideale massimale m_p l'insieme di tutte le funzioni regolari in p che si annullano in esso. Dimostriamo che è un ideale principale.

Poiché C è una curva dalla (2.13) esisterà $t \in m_p \setminus m_p^2$ tale che $m_p = \mathbb{C}t + m_p^2$. Per comodità poniamo $I = \langle t \rangle$, $R = \mathcal{O}_p(C)/I$ e $M = m_p/I$ allora R è ancora locale ed M è il suo ideale massimale e inoltre

$$M^2 = M$$

Se per assurdo $M \neq \{0\}$ indicheremo con $\mathcal{N} \subseteq M$ il più piccolo generatore di M. Preso $f_1 \in \mathcal{N}$ esso sarà generato da una somma finita di prodotti di elementi di M, quindi esisteranno $f_1, f_2, \ldots, f_l \in \mathcal{N}$ e $h_1, \ldots, h_l \in M$ tali che

Esercizio: dimostrarlo

$$f_1 = \sum_{i=1}^{l} h_i f_i \Rightarrow (1-h_1)f_1 = \sum_{i=2}^{l} h_i f_i$$

Ora se $1-h_1 \in M$ avremmo $M = R$ assurdo, quindi $1-h_1$ è invertibile e così M è generato da $\mathcal{N} \setminus \{f_1\}$ in contraddizione con la minimalità. Perciò $M = \{0\}$ e $m_p = I$ quindi è un ideale principale.

Adesso prendiamo un generico $a \in \mathcal{O}_p(C)$ e dimostriamo che soddisfa la (2.15). Se a è invertibile allora si ha immediatamente la tesi, altrimenti $a \in m_p$ ed esiste $a_1 \in \mathcal{O}_p(C)$ tale che $a = ta_1$. Se a_1 è invertibile la dimostrazione è terminata altrimenti esisterà $a_2 \in \mathcal{O}_p(C)$ tale che $a_1 = ta_2$ e quindi $a = a_2 t^2$. Iterando il procedimento arriveremo ad un certo a_i invertibile allora avremo dimostrato la (2.15), altrimenti la catena di ideali

$$\langle a \rangle \leq \langle a_1 \rangle \leq \cdots \leq \langle a_l \rangle \leq \ldots$$

Essendo l'anello $\mathcal{O}_p(C)$ noetheriano per il lemma di Zorn questa catena prima o poi terminerà ovvero $\langle a_i \rangle = \langle a_{i+1} \rangle$ da un certo punto in poi, ovvero esisterà $f \in \mathcal{O}_p(C)$ tali che

$$a_i = ta_{i+1} = fta_i$$

dato che $a_i \neq 0$ e siamo in un dominio di integrità avremo che $t = f^{-1}$ il che è assurdo poiché t non è invertibile. Quindi la nostra sequenza di a_i deve terminare prima o poi.

L'unicità segue osservando che se $ut^m = vt^n$ con $m \geq n$ allora ut^{m-n} è invertibile e ciò è vero se e solo se $m = n$. ■

Adesso vogliamo determinare un procedimento per trovare da un campo K un sottoanello R a valutazione discreta. Diremo innanzitutto che una applicazione $v : K \to \mathbb{Z} \cup \{+\infty\}$ è una *valutazione* di K se e solo se

1. $v(x) = +\infty$ se e solo se $x = 0$;
2. $v(xy) = v(x) + v(y)$;
3. $v(x+y) \geq \min\{v(x), v(y)\}$.

Proposizione 2.9.6. *Se v è una valutazione di K allora*

1. $v(1) = 0$;
2. $v(-x) = v(x)$.

Dimostrazione. La prima affermazione discende immediatamente dal secondo punto. Per quanto riguarda la seconda avremo che

$$0 = v(1) = v(-1) + v(-1) \Rightarrow v(-1) = 0$$

■

In particolare il sottoinsieme

$$R = \{x \in K \mid v(x) \geq 0\}$$

è un anello locale con ideale massimale $R' = \{x \in K \mid v(x) > 0\}$. Dimostreremo ora che R è anche un anello a valutazione discreta.

Che R sia un anello discende immediatamente dalle proprietà di v, inoltre se $k = \min\{v(x) \mid x \in R\} > 1$ allora $v(x) \in k\mathbb{Z}$ per ogni $x \in K \setminus \{0\}$ e quindi a meno di effettuare una divisione potremmo supporre che esiste $t \in R$ per cui $v(t) = 1$.

Poiché siamo pur sempre in un campo K tutti e i soli elementi invertibili u di R saranno quelli per i quali $v(u) = 0$. Allora per ogni $x \in R$ l'elemento $x/t^{v(x)}$ appartiene ad R ed è invertibile e quindi

$$x = \frac{x}{t^{v(x)}} t^{v(x)}$$

Sempre poiché siamo in un campo questa scrittura è unica e la tesi è così dimostrata.

Viceversa se R è un anello a valutazione discreta esiste un'unica estensione dell'ordine degli elementi di R su K che soddisfa le stesse proprietà di v.

Proposizione 2.9.7. *Sia α un'applicazione birazionale da C a C' curve proiettive, allora α può essere estesa su tutti i punti lisci di C.*

Dimostrazione. Grazie alla proposizione 2.8.7 se α non è dominante allora esiste un aperto $U \subseteq C$ tale che $\alpha(U)$ è un insieme finito. Ancora per la continuità di α possiamo restringere ancora di più U in modo tale che sia costante su tutto U e quindi ogni sua estensione su C deve essere costante.

Possiamo allora porre α dominante e $p \in C$ liscio e indichiamo con $X \subseteq C \setminus \{p\}$ l'aperto su cui α è definito ed è un morfismo, dimostreremo che esiste $Y \subseteq C$ aperto contenente p e X e un morfismo $\psi : Y \to \mathbb{P}^n\mathbb{C}$ che coincide con α su X.

Preso $U = \{[x] \in \mathbb{P}^n\mathbb{C} \mid x_i \neq 0 \quad \forall i\}$ allora possiamo supporre senza perdere in generalità che

$$\alpha(X) \cap U \neq \emptyset$$

altrimenti, per l'irriducibilità di X, $\alpha(X)$ sarebbe interamente contenuto in uno degli iperpiani $\{x_i = 0\}$ quindi possiamo ridurre la dimensione dello spazio proiettivo contenente $\alpha(X)$ fino a quando non sarà più possibile.

Le applicazioni x_i/x_j sono sempre regolari in U e quindi il pull-back $f_{ij} = \alpha^*(x_i/x_j)$ è definito sull'aperto denso $X \cap \alpha^{-1}(U)$ dunque $f_{ij} \in \mathbb{C}(X) = \mathbb{C}(C)$. Presa v la valutazione di $\mathcal{O}_p(C)$ che può essere estesa al suo campo dei quozienti $\mathbb{C}(C)$ (p è liscio) e $n_i = v(f_{i0})$ allora

$$n_i - n_j = v\left(\frac{f_{i0}}{f_{j0}}\right) = v(f_{ij})$$

e prendiamo h in modo tale che n_h sia il più piccolo possibile, questo significa che $f_{ih} \in \mathcal{O}_p(C)$ per ogni i per tutto il ragionamento fatto sopra. Esisterà dunque un aperto $V \subseteq \alpha^{-1}(\{x_h \neq 0\})$ contenente p sul quale le f_{ih} sono tutte regolari, possiamo allora definire il morfismo

$$\psi : v \in V \cup X \to \begin{cases} \alpha(v) & \text{se } v \in X \\ [f_{0h}(v), f_{1h}(v), \dots, f_{nh}(v)] & \text{se } v \in V \end{cases}$$

chiaramente per come abbiamo definito le f_{ij} ψ è ben definita su $V \cap X$ e quindi posto $Y = X \cup V$ abbiamo ottenuto la tesi. ■

Corollario 2.9.8. *Due curve proiettive senza punti singolari C e C' sono isomorfe se e solo se i rispettivi campi delle funzioni razionali lo sono. In particolare due curve birazionali sono isomorfe.*

Dimostrazione. Se due curve non hanno punti singolari allora tutte le applicazioni razionali definite tra loro sono morfismi. ■

Grazie a questo risultato possiamo catalogare con molta facilità le curve proiettive. Per altri tipi di varietà questo risultato non è necessariamente verificato in quanto possono esistere varietà non singolari birazionali che non sono isomorfe.

Esempio 7. Le varietà $\mathbb{P}^m\mathbb{C} \times \mathbb{P}^m\mathbb{C}$ e $\mathbb{P}^{m+n}\mathbb{C}$ sono birazionali per ogni $m, n \in \mathbb{N}$ tramite i seguenti passaggi

$$\mathbb{P}^n\mathbb{C} \times \mathbb{P}^m\mathbb{C} \leftrightarrow \mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{m+n} \leftrightarrow \mathbb{P}^{m+n}\mathbb{C}$$

dove le frecce sono applicazioni birazionali. Però $\mathbb{P}^1\mathbb{C} \times \mathbb{P}^1\mathbb{C}$ non è isomorfo a $\mathbb{P}^2\mathbb{C}$, in quanto esiste chiaramente un morfismo suriettivo da $\mathbb{P}^1\mathbb{C} \times \mathbb{P}^1\mathbb{C}$ su $\mathbb{P}^1\mathbb{C}$ (la proiezione sulla prima coordinata omogenea). Se esistesse un morfismo da $\mathbb{P}^2\mathbb{C}$ in $\mathbb{P}^1\mathbb{C}$ non costante l'immagine deve essere necessariamente densa (l'immagine mediante una funzione continua di una spazio topologico irriducibile è irriducibile). Presi allora $a, b \in \mathbb{P}^1\mathbb{C}$ distinti le loro controimmagini saranno due curve in $\mathbb{P}^2\mathbb{C}$ disgiunte, ma ciò è impossibile. Visto online, booh

Per enunciare il prossimo risultato abbiamo bisogni di alcuni preliminari di teoria dei campi. Diremo che un'estensione algebrica L del campo K è *separabile* se per ogni $\alpha \in L$ i polinomi f e $\partial_x f$ sono coprimi, dove $f \in K[x]$ è il polinomio minimo di x. Si dimostra che se K ha caratteristica 0 allora tutte le sue estensioni sono separabili.

Teorema 2.9.9 (dell'elemento primitivo)**.** *Se un campo L è un'estensione algebrica finita di un altro campo K con caratteristica 0 allora esiste $\alpha \in L$ per cui $L = K(\alpha)$.*

Dimostrazione. Utilizzeremo l'induzione su n, se $n = 1$ è banale quindi supponiamo $n = 2$. Sia dunque $L = K(\alpha, \beta)$ esistono dunque dei polinomi minimi $f, g \in K[x]$ tali che $f(\alpha) = 0 = g(\beta)$.

Prendiamo L' il campo di spezzamento di f e g, cioè tale che esistono $a_i, b_j \in L'$ distinti per cui

$$f(x) = \prod_{i=1}^{r} (x - a_i)^{r_i} \qquad\qquad g(x) = \prod_{j=1}^{s} (x - b_j)^{s_j}$$

con $a_1 = \alpha$ e $b_1 = \beta$. Poiché K ha caratteristica 0 L' è separabile e quindi $r_i = s_j = 1$ e possiamo scegliere $\lambda \in K$ tale che per ogni $i, j \neq 1$

$$\lambda a_i + b_j \neq \lambda\alpha + \beta = \gamma$$

Sia $H = K(\gamma) \leq L'$ e $h(x) = g(\gamma - \lambda t) \in H[x]$ avremo che $h(a_i) \neq 0$ per ogni $i \neq 1$ mentre $h(\alpha) = 0$ mentre $f(a_i) = 0$ per ogni i. Dato che stiamo sempre lavorando in L' il fattore $(x - \alpha)$ è il massimo comune dei polinomi f e h che appartengono entrambi ad $H[x]$, ora essendo H campo il loro massimo comune divisore dovrà appartenere a $H[x]$ e quindi $\alpha \in H$. Da ciò segue immediatamente che $\beta \in H$ e quindi $L = H = K(\gamma)$.

Ragionando per induzione si ottiene la tesi. ■

Corollario 2.9.10. *Ogni curva proiettiva C è birazionale ad una curva proiettiva in $\mathbb{P}^2\mathbb{C}$.*

Dimostrazione. Se C è una curva proiettiva allora esiste $t \in \mathbb{C}(C)$ tale che $\mathbb{C}(C)$ è una estensione algebrica di $\mathbb{C}(t)$. Per il teorema dell'elemento primitivo esiste $s \in \mathbb{C}(C)$ per cui $\mathbb{C}(C) = [\mathbb{C}(t)](s)$ ed esisterà $p \in \mathbb{C}[x, y]$ tale che $p(s, t) = 0$. Otterremo così un polinomio omogeneo $p(x, y, z)$ che induce una curva in $\mathbb{P}^2\mathbb{C}$. ■

Possiamo però utilizzare un approccio più geometrico a questo corollario, di cui faremo solo dei cenni. Consideriamo una proiezione $\pi : \mathbb{P}^n\mathbb{C} \to \mathbb{P}^{n-1}\mathbb{C}$ (che non definiremo ancora) che manda punti della curva C in punti che non gli appartengono. Questa proiezione definisce un morfismo tra C e la chiusura dell'immagine.

Posto $Sec(C)$ l'insieme delle rette secanti e tangenti ad C, esso è un sottoinsieme di $\mathbb{P}^n\mathbb{C}$ le cui componenti irriducibili hanno dimensione al più 3 (la parametrizzazione locale è data da $P, Q \in C$ indicanti i punti da intersecare e $t \in \mathbb{P}^1\mathbb{C}$ il coefficiente angolare della retta). Se $n \geq 4$ allora possiamo prendere come centro della proiezione π un punto O che non appartiene a $Sec(C)$ in modo tale che la proiezione ristretta a C diventi un isomorfismo di curve di cui una planare.

Nel caso in cui $n = 3$ possiamo tranquillamente supporre che in O passino solamente un numero finito di secanti e nessuna tangente, poi con altre ipotesi la proiezione diventa un'applicazione birazionale.

Esempio 8. Consideriamo una curva piana $C = \mathcal{V}(f) \subseteq \mathbb{A}^2$ con f di grado $n \geq 2$ e sia $p \in C$ di molteplicità $n-1$ (si veda (2.14)). Quindi a meno di una traslazione possiamo supporre $p = (0,0)$ e

$$f(x,y) = r_n(x,y) + r_{n-1}(x,y)$$

Definiamo le applicazioni razionali

$$\phi : (x,y) \in C \to \frac{y}{x} \in \mathbb{A} \quad \psi : t \in \mathbb{A} \to \left(-\frac{r_{n-1}(1,t)}{r_n(1,t)}, -t\frac{r_{n-1}(1,t)}{r_n(1,t)} \right) \in C$$

allora $\phi \circ \psi(t) = t$ mentre per ogni (x,y) appartenenti ad un opportuno aperto di C avremo che

$$\psi \circ \phi(x,y) = \left(-\frac{\frac{1}{x^{n-1}} r_{n-1}(x,y)}{\frac{1}{x^n} r_n(x,y)}, -\frac{y}{x}\frac{\frac{1}{x^{n-1}} r_{n-1}(x,y)}{\frac{1}{x^n} r_n(x,y)} \right) = -\frac{r_{n-1}(x,y)}{r_n(x,y)}(x,y)$$

che appartiene ancora ad C, quindi C è birazionale a $\mathbb{A}$.

Esempio 9. Se $n \geq 3$ consideriamo la curva piana di Fermat $C : x^n + y^n = 1$ e supponiamo che esista un'applicazione razionale dominante $\psi(t) = (a(t)/b(t), c(t)/d(t))$ da $\mathbb{A}$ in C e quindi

$$(ad)^n + (cb)^n = (bd)^n$$

posto $p = ad, q = cb, r = bd$ avremo che $a/b = p/r$ e $c/d = q/r$. Per come abbiamo definito la curva C nessuno di questi due rapporti e nemmeno p/q possono essere costanti altrimenti ψ non sarebbe dominante. Ancora possiamo supporre senza perdere in generalità che p, q ed r non abbiano fattori a due a due comuni in quanto, se ce li avessero, anche il terzo lo avrebbe e si potrebbe semplificare.

Se p/r non è costante allora avremo sull'aperto $\{r \neq 0\}$

$$0 \neq \partial_t \left(\frac{p(t)}{r(t)} \right) = \frac{p'(t)r(t) - p(t)r'(t)}{r^2(t)} \Rightarrow p'(t)r(t) \neq p(t)r'(t)$$

e quindi la matrice

$$\begin{pmatrix} p & q & -r \\ p' & q' & -r' \end{pmatrix}$$

ha tutti i minori di ordine 2 non nulli per quasi ogni t. La terna $(x,y,z) = (p^{n-1}(t), q^{n-1}(t), r^{n-1}(t))$ è soluzione del sistema

$$\begin{cases} p(t)x + q(t)y - r(t)z = 0 \\ p'(t)x + q'(t)y - r'(t)z = 0 \end{cases}$$

e per quanto detto prima sui minori possiamo sempre scrivere due termini della terna risolutiva in funzione del terzo. Utilizzando il metodo di Cramer avremo che p^{n-1} divide $q'r - qr'$, q^{n-1} divide $p'r - pr'$ ed r^{n-1} divide $q'p - qp'$.

Ma allora se $\deg p \geq \deg q \geq \deg r$ otterremmo

$$(n-1)\deg p \leq \deg q - 1 + \deg r \leq 2\deg p - 1$$

e poiché i polinomi sono non costanti seguirebbe che $n \leq 2$ in contraddizione con l'ipotesi iniziale $n \geq 3$.

Abbiamo appena dimostrato che l'insieme delle soluzioni razionali dell'equazione $x^n + y^n = 1$, se esistessero, non sarebbero esprimibili tramite polinomi. Se invece $n = 2$ i suoi punti hanno molteplicità 1 e possiamo applicare l'esempio precedente, inoltre la seguente applicazione

$$\psi(t) = \left(\frac{2t}{1+t^2}, \frac{1-t^2}{1+t^2}\right)$$

è in realtà birazionale. Mentre se $n \geq 3$ e (x_0, y_0) è un punto di C allora avremmo che

$$x^n + y^n - 1 = \sum_{i=0}^{n} \binom{n}{i} \left[(x-x_0)^i x_0^{n-i} + (y-y_0)^i y_0^{n-i}\right] - 1$$

e quindi (x_0, y_0) ha molteplicità $1 \neq n-1$ dato che almeno una delle due coordinate è non nulla.

2.10 Scoppiamenti

Concluderemo questo capitolo con la definizione di scoppiamento o blow-up, con il quale trasformeremo una varietà con un numero finito di singolarità in un'altra birazionale ma senza punti singolari. Se la varietà è una curva allora grazie al corollario 2.8.9 il numero dei suoi punti singolari è certamente finito. Un procedimento simile per le varietà differenziabili è già stato trattato, il procedimento è tutto sommato simile.

A titolo di esempio effettuiamo lo scoppiamento di $\mathbb{A}^n$ nell'origine.

Proposizione 2.10.1. *La varietà $\mathbb{A}^n \times \mathbb{P}^{n-1}\mathbb{C}$ è una varietà quasi proiettiva.*

Dimostrazione. Posto $U_k = \{x_k \neq 0\} \subseteq \mathbb{P}^n\mathbb{C}$, l'immersione di Segre $p : \mathbb{P}^n\mathbb{C} \times \mathbb{P}^{n-1}\mathbb{C} \to Z$ manderà $U_k \times \mathbb{P}^{n-1}\mathbb{C}$ nell'insieme aperto di Z

$$\bigcup_{l=0}^{n-1} \{[z_{ij}] \in Z \mid z_{kl} \neq 0\}$$

e quindi $\mathbb{A}^n \times \mathbb{P}^{n-1}\mathbb{C} \cong U_k \times \mathbb{P}^{n-1}\mathbb{C}$ è isomorfo ad un aperto di Z. ■

In $\mathbb{A}^n \times \mathbb{P}^{n-1}\mathbb{C}$ indicheremo sempre con $x_1, \ldots, x_n$ le componenti affini e con $y_1, \ldots, y_n$ le coordinate omogenee. Consideriamo ora l'insieme chiuso

$$X = \{x_i y_j = x_j y_i \quad \forall i, j\}$$

inoltre la proiezione sul primo fattore $f : X \to \mathbb{A}^n$ è chiaramente un morfismo di varietà per come abbiamo definito l'immersione di Segre, inoltre per ogni $p = (a_1, \dots, a_n) \in \mathbb{A}^n$ se $a_i \neq 0$ allora la sua controimmagine è determinata dall'equazione

$$y_j = \frac{a_j}{a_i} y_i$$

per ogni j, quindi $y_i \neq 0$ e la controimmagine coincide con il solo punto $(a_1, \dots, a_n) \times [a_1, \dots, a_n]$. Invece se $p = 0$ allora $f^{-1}(0) = \mathbb{P}^{n-1}\mathbb{C}$, abbiamo così trasformato $\mathbb{A}^n$ in un'altra varietà che manda l'origine in uno spazio proiettivo mentre gli altri punti rimangono invariati.

Consideriamo adesso una qualunque varietà $Y \subseteq \mathbb{A}^n$ passante per l'origine, definiamo lo *scoppiamento* di Y in 0 la varietà

$$Y^* = \overline{f^{-1}(Y \setminus \{0\})}$$

ovvero la più piccola varietà affine contenente $f^{-1}(Y \setminus \{0\})$.

Poiché $f : Y^* \setminus f^{-1}(0) \to Y \setminus \{0\}$ è un isomorfismo allora Y e Y^* sono birazionalmente equivalenti e questa restrizione in particolare consiste in un ingrandimento di Y nell'origine, per questo motivo si chiama anche blow-up.

È possibile scoppiare anche il punto $[0, 0, \dots, 0, 1]$ di $\mathbb{P}^n\mathbb{C}$ proiettandolo su U_n e ragionando in maniera analoga. Lo scoppiamento $X \subseteq \mathbb{P}^n\mathbb{C} \times \mathbb{P}^{n-1}\mathbb{C}$ di una qualunque varietà proiettiva è ancora una varietà proiettiva e quindi è possibile iterare lo scoppiamenti quante volte si vuole.

Esempio 10. Siano $(a, b) \in \mathbb{A}^2$ e $[x, y] \in \mathbb{P}^1\mathbb{C}$ allora lo scoppiamento di $\mathbb{A}^2$ è la varietà $X \subseteq \mathbb{A}^2 \times \mathbb{P}^1\mathbb{C}$ definita dall'equazione $\{ay = bx\}$, in particolare se $U = \{y \neq 0\}$ allora $\mathbb{A}^2 \times U \cong \mathbb{A}^3$ e $X \setminus \{(a, 0) \times [1, 0]\}$ è isomorfa alla varietà $a = bc$ in $\mathbb{A}^3$. Essa può essere vista come una ipersuperficie di $\mathbb{A}^3$ formata dalle rette passanti per l'origine che ruotano con coefficiente angolare c. Se si aggiunge pure la parte mancante $(\mathbb{A} \times [1, 0])$ osserviamo che X è un "nastro di Möbius complesso".(Attenzione a questa affermazione, è personale)

Prendiamo adesso la seguente varietà affine

$$Y : b^2 = a^2(a + 1)$$

dunque la controimmagine di Y mediante f è il chiuso

$$Y' = \left\{ax = by, b^2 = a^2(a + 1)\right\}$$

e lavoriamo prima su $U_1 = \{x \neq 0\}$ e poi su $U_2 = \{y \neq 0\}$. nel primo caso ponendo $z = y/x$ avremo che

$$Y' \cap U_1 \cong \left\{(a, b, c) \;\middle|\; a = bc, b^2 = a^2(a + 1) = b^2c^2(bc + 1)\right\}$$

e in particolare avremo che $b^2[1 - c^2(bc + 1)] = 0$. Il nostro insieme Y' sarà dunque ricoperto dalle due varietà

$$f^{-1}(0) : a = 0, b = 0, c \text{ arbitrario } \cong \mathbb{P}^1\mathbb{C}$$
$$Y^* \cap U_1 : c^2(bc + 1) = 1, a = bc$$

Nell'esempio 5 abbiamo visto che la varietà Y ha l'origine come punto singolare, mentre la matrice jacobiana di $Y^* \cap U_1$ è pari a

$$\begin{pmatrix} 0 & c^3 & 3c^2b + 2c \\ 1 & -c & -b \end{pmatrix}$$

e dato che c non si può mai annullare Y^* è composta interamente da punti regolari. Osserviamo inoltre che Y^* interseca $f^{-1}(0)$ in $c = \pm 1$. Se tracciamo il grafico di Y su $\mathbb{A}^2$ osserviamo che nell'origine possiede una singolarità a nodo, nel quale possiede due rette tangenti una di coefficiente angolare 1 e l'altra -1. Lo scoppiamento Y^* di Y prende le due rette tangenti e le separa mettendole in due punti distinti che saranno così regolari.

Lavorando invece su U_2 arriveremmo alle stesse e identiche conclusioni.

Indice analitico