Università degli Studi Roma Tre
Dipartimento di Matematica e Fisica

Geometria algebrica 1

- MAT/03 GE410 -

Raffaele Di Donna
Matricola: 523997

Indice

Geometria algebrica 1 (Matematica, Roma Tre)	Oct 2, 2020

Lezione 5

Raffaele Di Donna

Elementi nilpotenti e ideali radicali. k-algebre finitamente generate. Corrispondenza tra i chiusi di $\mathbb{A}^n_k$ e le k-algebre finitamente generate senza nilpotenti. Indipendenza algebrica, basi di trascendenza. Ogni insieme di elementi algebricamente indipendenti può essere completato a una base di trascendenza. Dimensione di un sottoinsieme chiuso di $\mathbb{A}^n_k$. Esempi di calcolo di dimensione.

Parte I
Spazi affini

Introduciamo, innanzitutto, alcune notazioni. Denotiamo $\mathbb{N}$ l'insieme dei numeri interi positivi, vale a dire $\mathbb{N} = \{1, 2, 3, \dots\}$. Dato invece un campo k, indichiamo con R_n l'anello dei polinomi a coefficienti in k nelle indeterminate $X_1, X_2, \dots, X_n$, cioè $R_n = k[X_1, X_2, \dots, X_n]$. Denotiamo infine $k(X_1, X_2, \dots, X_n)$ il campo dei quozienti di R_n.

1 Irriducibilità e componenti irriducibili

1.1 Chiusi e k-algebre

Definizione 1.1. Sia k un campo. Una *k-algebra* è un anello A con una moltiplicazione:

$$\begin{aligned} k \times A &\longrightarrow A \\ (\lambda, a) &\longmapsto \lambda a \end{aligned}$$

tale che:

(i) A sia un k-spazio vettoriale rispetto alle operazioni di somma e prodotto per uno scalare.

(ii) $(\lambda a)b = \lambda(ab)$ per ogni $a, b \in A$, $\lambda \in k$.

Una k-algebra A si dice *finitamente generata* se esistono $g_1, g_2, \dots, g_n \in A$ tali che:

$$A = k[g_1, g_2, \dots, g_n]$$

Osservazione 1.2. Data una k-algebra A, per ogni $g_1, g_2, \dots, g_n \in A$ l'inclusione $k[g_1, g_2, \dots, g_n] \subseteq A$ è vera sempre per definizione di k-algebra. Ne deduciamo che una k-algebra A è finitamente generata se e solo se vale $A \subseteq k[g_1, g_2, \dots, g_n]$.

Definizione 1.3. Sia A un anello. Un elemento $x \in A$ si dice *nilpotente* se $x \neq 0$ ed esiste un intero $n \in \mathbb{N}$ tale che $x^n = 0$.

Osservazione 1.4. Sia A un anello e sia I un ideale di A. Allora A/I non ha elementi nilpotenti se e solo se I è un ideale radicale di A.

Dimostrazione. Consideriamo un elemento $f + I \in A/I$. Allora valgono le seguenti equivalenze:

$$\begin{aligned} f \text{ è nilpotente} &\iff f + I \neq I \quad \text{ed esiste } n \in \mathbb{N} \text{ tale che } f^n + I = I \\ &\iff f \notin I \qquad\quad \text{ed esiste } n \in \mathbb{N} \text{ tale che } f^n \in I \\ &\iff f \in \sqrt{I} \setminus I \end{aligned}$$

Ne discende che A/I ammette un elemento nilpotente se e solo se I non è un ideale radicale. □

Proposizione 1.5.

(i) *Sia $X \subseteq \mathbb{A}^n_k$ un chiuso. Allora $R_n/\mathcal{I}(X)$ è una k-algebra finitamente generata che non ha nilpotenti. Se inoltre X è irriducibile, allora la k-algebra $R_n/\mathcal{I}(X)$ è un dominio.*

(ii) *Siano k un campo algebricamente chiuso, I un ideale radicale di R_n tale che R_n/I sia una k-algebra finitamente generata che non ha nilpotenti. Allora esiste un unico chiuso $X \subseteq \mathbb{A}^n_k$ tale che $I = \mathcal{I}(X)$. Se inoltre R_n/I è un dominio, allora X è irriducibile.*

Dimostrazione.

(i) Sappiamo che $\mathcal{I}(X)$ è un ideale radicale di R_n e dunque, per l'osservazione 1.4, si ha che $R_n/\mathcal{I}(X)$ non ha elementi nilpotenti. È facile verificare che $R_n/\mathcal{I}(X)$ è una k-algebra come conseguenza del fatto che R_n è una k-algebra. Osserviamo adesso che, per come sono definite le operazioni di somma e prodotto sugli anelli quoziente, se utilizziamo per semplicità la notazione della barretta in alto per indicare le classi laterali allora, per ogni $i, j = 1, 2, \ldots, n$ e per ogni $\lambda \in k$, abbiamo le tre condizioni:

$$\begin{aligned} \overline{X_i + X_j} &= \overline{X_i} + \overline{X_j} \\ \overline{X_i X_j} &= \overline{X_i}\,\overline{X_j} \\ \overline{\lambda X_i} &= \lambda \overline{X_i} \end{aligned}$$

Ne discende che la classe laterale di un polinomio nelle variabili $X_1, X_2, \ldots, X_n$ a coefficienti in k si può pensare come un polinomio in $\overline{X_1}, \overline{X_2}, \ldots, \overline{X_n}$ a coefficienti in k. Abbiamo perciò la condizione:

$$R_n/\mathcal{I}(X) = k[\overline{X_1}, \overline{X_2}, \ldots, \overline{X_n}]$$

Questo dimostra che la k-algebra $R_n/\mathcal{I}(X)$ è finitamente generata. La seconda parte dell'enunciato segue dal fatto che X è irriducibile se e solo se $\mathcal{I}(X)$ è un ideale primo di R_n, se e solo se $R_n/\mathcal{I}(X)$ è un dominio.

(ii) La prima parte deriva immediatamente dal teorema degli zeri di Hilbert, mentre la seconda parte si giustifica esattamente come visto nella dimostrazione del punto (i) precedente. □

Esempio 1.6. Gli elementi $\overline{X_1}, \overline{X_2}, \ldots, \overline{X_n}$, diversamente dalle variabili $X_1, X_2, \ldots, X_n$, non sempre sono indipendenti. Se per esempio consideriamo l'anello dei polinomi $k[X_1, X_2]$ allora, per definizione, le variabili X_1 e X_2 non soddisfano alcuna condizione, ma nell'anello $k[X_1, X_2]/(X_1X_2)$ le variabili $\overline{X_1}$ e $\overline{X_2}$ verificano:

$$\overline{X_1}\,\overline{X_2} = \bar{0}$$

1.2 Grado di trascendenza

Ricordiamo innanzitutto la seguente nozione di teoria dei campi.

Definizione 1.7. Sia $K \subseteq F$ un'estensione di campi. Un elemento $\alpha \in F$ si dice *algebrico su* K se esiste un polinomio non nullo $p \in K[X]$ tale che $p(\alpha) = 0$. Se α non è algebrico su K, ovvero se, per ogni polinomio $p \in K[X]$, da $p(\alpha) = 0$ segue che p è il polinomio nullo, diremo che α è *trascendente su* K.

La definizione precedente si generalizza facilmente sul numero degli elementi coinvolti.

Definizione 1.8. Sia $K \subseteq F$ un'estensione di campi e siano $\alpha_1, \alpha_2, \dots, \alpha_n \in F$. Gli elementi $\alpha_1, \alpha_2, \dots, \alpha_n$ si dicono *algebricamente dipendenti su* K se esiste un polinomio non nullo $p \in K[X_1, X_2, \dots, X_n]$ tale che $p(\alpha_1, \alpha_2, \dots, \alpha_n) = 0$. Se invece $\alpha_1, \alpha_2, \dots, \alpha_n$ non sono algebricamente dipendenti su K, cioè se, per ogni polinomio $p \in K[X_1, X_2, \dots, X_n]$, da $p(\alpha_1, \alpha_2, \dots, \alpha_n) = 0$ segue che p è il polinomio nullo, diremo allora che $\alpha_1, \alpha_2, \dots, \alpha_n$ sono *algebricamente indipendenti su* K.

Osservazione 1.9. La condizione di indipendenza algebrica è decisamente più forte di quella di indipendenza lineare, la quale richiede che ad annullarsi siano soltanto i polinomi lineari.

Osservazione 1.10. Se $\alpha_1, \alpha_2, \dots, \alpha_n$ sono algebricamente indipendenti su K, lo sono anche $\alpha_1, \alpha_2, \dots, \alpha_s$ per qualsiasi intero positivo $s < n$. In particolare (caso $s = 1$), gli elementi $\alpha_1, \alpha_2, \dots, \alpha_n$ sono trascendenti su K.

Definizione 1.11. Un'estensione di campi $K \subseteq F$ è detta *algebrica* se ciascun elemento di F è algebrico su K, mentre è detta *trascendente* se non è algebrica, cioè se almeno un elemento di F è trascendente su K.

Definizione 1.12. Sia $K \subseteq F$ un'estensione di campi. Un sottoinsieme finito $\{x_1, x_2, \dots, x_t\} \subseteq F$ si dice una *base di trascendenza di* F *su* K se:

(1) Gli elementi $x_1, x_2, \dots, x_t$ sono algebricamente indipendenti su K.

(2) L'estensione di campi $K(x_1, x_2, \dots, x_t) \subseteq F$ è algebrica.

Teorema 1.13. *Sia $K \subseteq F$ un'estensione di campi e sia $\{x_1, x_2, \dots, x_t\}$ una base di trascendenza di F su K. Allora una qualsiasi base di trascendenza di F su K è costituita da t elementi. Inoltre, per ogni sottoinsieme finito $\{y_1, y_2, \dots, y_s\} \subseteq F$ tale che $y_1, y_2, \dots, y_s$ siano algebricamente indipendenti su K:*

(i) *Vale che $s \leq t$.*

(ii) *Se $s = t$, allora $\{y_1, y_2, \dots, y_s\}$ è una base di trascendenza di F su K.*

(iii) *Se $s < t$, allora esistono $y_{s+1}, y_{s+2}, \dots, y_t \in F$ tali che $\{y_1, y_2, \dots, y_t\}$ sia una base di trascendenza di F su K.*

Dimostrazione. Si noti innanzitutto che, una volta dimostrata la proprietà (i), da questa seguirà facilmente la prima parte dell'enunciato, poiché potremo scegliere $\{x_1, x_2, \dots, x_t\}$ e $\{y_1, y_2, \dots, y_s\}$ come due qualsiasi basi di trascendenza di F su K. Fissiamo adesso un sottoinsieme $\{y_1, y_2, \dots, y_s\} \subseteq F$ tale che $y_1, y_2, \dots, y_s$ siano algebricamente indipendenti su K.

(i) Dato che $\{x_1, x_2, \dots, x_t\}$ è una base di trascendenza di F su K, l'estensione $K(x_1, x_2, \dots, x_t) \subseteq F$ è algebrica e allora y_1 è algebrico su $K(x_1, x_2, \dots, x_t)$. Ciò significa che esiste un polinomio non nullo $p \in K(x_1, x_2, \dots, x_t)[Y]$ tale che $p(y_1) = 0$. Osserviamo che p è un polinomio che ha per coefficienti quozienti di polinomi in $x_1, x_2, \dots, x_t$ e dunque possiamo cancellare i denominatori moltiplicando p per un opportuno polinomio. Formalmente, esiste un polinomio non nullo $b \in K[x_1, x_2, \dots, x_t]$ tale che $bp \in K[x_1, x_2, \dots, x_t][Y]$. In effetti, si potrebbe scegliere un tale polinomio b come il prodotto dei denominatori dei coefficienti di p. Sia adesso $q \in K[Z_1, Z_2, \dots, Z_t, Z_{t+1}]$ il polinomio ottenuto da bp sostituendo l'indeterminata Z_i a x_i per $i = 1, 2, \dots, t$ e la variabile Z_{t+1} a Y. Per costruzione, il polinomio q è non nullo e verifica $q(x_1, x_2, \dots, x_t, y_1) = 0$.

Osserviamo inoltre che q deve dipendere da Z_i per qualche indice $i \in \{1, 2, \dots, t\}$ perché, se così non fosse, allora $q \in K[Z_{t+1}]$ e $q(y_1) = 0$, cioè y_1 sarebbe algebrico su K e ciò contraddice l'ipotesi che $y_1, y_2, \dots, y_s$ siano algebricamente indipendenti su K. Possiamo dunque supporre, per semplicità, che q dipenda dalla variabile Z_1. Dal fatto che $q(x_1, x_2, \dots, x_t, y_1) = 0$ segue che x_1 è algebrico sul campo $K(x_2, \dots, x_t, y_1)$ in quanto x_1 è radice del polinomio $q' \in K(x_2, \dots, x_t, y_1)[Z_1]$ definito da $q'(Z_1) := q(Z_1, x_2, \dots, x_t, y_1)$. Abbiamo allora che le seguenti sono estensioni algebriche di campi:

$$K(x_2, \dots, x_t, y_1) \subseteq K(x_1, x_2, \dots, x_t, y_1) \subseteq F$$

Per transitività delle estensioni algebriche, anche l'estensione $K(x_2, \dots, x_t, y_1) \subseteq F$ è algebrica. In questa maniera abbiamo sostituito y_1 a x_1 nell'estensione algebrica $K(x_1, x_2, \dots, x_t) \subseteq F$ nota per ipotesi.

Ora $y_2 \in F$ e quindi y_2 è algebrico su $K(x_2, \dots, x_t, y_1)$. Ripetendo lo stesso argomento visto prima, si trova un polinomio non nullo $q \in K[Z_2, \dots, Z_t, Z_{t+1}, Z_{t+2}]$ tale che valga $q(x_2, \dots, x_t, y_1, y_2) = 0$. Come prima, tale polinomio deve dipendere da Z_i per qualche $i \in \{2, \dots, t\}$, altrimenti avremmo che $q \in K[Z_{t+1}, Z_{t+2}]$ e $q(y_1, y_2) = 0$, ovvero che y_1, y_2 sono algebricamente dipendenti su K e questo è assurdo. Possiamo allora supporre che q dipenda dalla variabile Z_2 e da questo segue che l'estensione $K(x_3, \dots, x_t, y_1, y_2) \subseteq F$ è algebrica.

Iterando, si ha che $K(x_{r+1}, \dots, x_t, y_1, \dots, y_r) \subseteq F$ è un'estensione algebrica per ogni $r = 1, 2, \dots, s$. A questo punto basta ragionare per assurdo: se fosse $s > t$ allora, prendendo $r := t$, otterremmo che l'estensione $K(y_1, y_2, \dots, y_t) \subseteq F$ è algebrica. In particolare, l'elemento $y_{t+1} \in F$ sarebbe algebrico su $K(y_1, y_2, \dots, y_t)$, cioè $y_1, y_2, \dots, y_{t+1}$ sarebbero algebricamente dipendenti su K e ciò è assurdo.

(ii) Per quanto già visto nella dimostrazione del punto (i) precedente, l'estensione $K(y_1, y_2, \dots, y_s) \subseteq F$ è algebrica. Sappiamo per ipotesi che gli elementi $y_1, y_2, \dots, y_s$ sono algebricamente indipendenti su K, quindi il sottoinsieme $\{y_1, y_2, \dots, y_s\} \subseteq F$ è per definizione una base di trascendenza di F su K.

(iii) Sarà sufficiente dimostrare che $\{y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_t\}$ è una base di trascendenza di F su K. Verifichiamo le due condizioni della definizione:

(1) Supponiamo per assurdo che $y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_t$ siano algebricamente dipendenti su K, cioè che $p(y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_t) = 0$ per un qualche polinomio $p \in K[Z_1, Z_2, \dots, Z_t]$ non nullo. Inoltre, tale polinomio dipende da almeno una delle variabili $Z_{s+1}, \dots, Z_t$ perché, se non dipendesse da nessuna di queste variabili, allora $p(y_1, y_2, \dots, y_s) = 0$ e ciò contraddice l'ipotesi che $y_1, y_2, \dots, y_s$ siano algebricamente indipendenti su K. Si può allora supporre, per esempio, che p dipenda da Z_t. Sia dunque $q \in K(y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_{t-1})[Z_t]$ il polinomio dato da:

$$q(Z_t) := p(y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_{t-1}, Z_t)$$

Allora x_t è algebrico su $K(y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_{t-1})$ in quanto q è un polinomio non nullo e $q(x_t) = 0$. Ricordando quanto già dimostrato nel punto (i) precedente (caso $r := s$), possiamo affermare che le seguenti estensioni di campi sono algebriche:

$$K(y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_{t-1}) \subseteq K(y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_{t-1}, x_t) \subseteq F$$

Per transitività delle estensioni algebriche, abbiamo che $K(y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_{t-1}) \subseteq F$ è un'estensione algebrica. Si noti ora che $y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_{t-1}$ non sono algebricamente indipendenti su K perché, se lo fossero, allora $\{y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_{t-1}\}$ sarebbe una base di trascendenza di F su K di cardinalità $t-1$ e ciò contraddice la prima asserzione del teorema, giustificata come conseguenza del punto (i) precedente.

Iterando il ragionamento precedente, otteniamo dunque che $y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_{t-r}$ sono algebricamente dipendenti su K per $r = 1, 2, \dots, t-s$. In particolare, per $r := t-s$ troviamo che $y_1, y_2, \dots, y_s$ sono algebricamente dipendenti su K, contraddicendo le ipotesi del teorema.

(2) Per quanto già osservato nella dimostrazione del punto (i) precedente (caso $r := s$), l'estensione di campi $K(y_1, y_2, \dots, y_s, x_{s+1}, \dots, x_{t-1}, x_t) \subseteq F$ è algebrica. □

Il teorema 1.13 ci permette di dare la seguente definizione.

Definizione 1.14. Sia $K \subseteq F$ un'estensione di campi. Definiamo il *grado di trascendenza di F su K* come:

$$\operatorname{trdeg}_K F := \begin{cases} 0 & \text{se l'estensione di campi } K \subseteq F \text{ è algebrica} \\ t & \text{se esiste una base di trascendenza } \{x_1, x_2, \dots, x_t\} \text{ di } F \text{ su } K \\ \infty & \text{altrimenti} \end{cases}$$

Si può mostrare che il grado di trascendenza di F su K è invariante per isomorfismi di anelli su F e su K.

Esempio 1.15. L'estensione di campi $K \subseteq K(X_1)$ è trascendente poiché X_1 è trascendente su K. Infatti, dato un polinomio $p \in K[X]$, da $p(X_1) = 0$ discende che p è il polinomio nullo per il principio di identità dei polinomi. Tuttavia, esiste una base di trascendenza di $K(X_1)$ su K ed è ovviamente $\{X_1\}$, dunque il grado di trascendenza di $K(X_1)$ su K è 1. Similmente, si vede che il grado di trascendenza di $K(X_1, X_2, \dots, X_t)$ su K è t. Consideriamo ora il campo dei quozienti dell'anello dei polinomi in infinite variabili a coefficienti in K, denotato $K(X_1, X_2, \dots)$. Ovviamente, anche l'estensione di campi $K \subseteq K(X_1, X_2, \dots)$ è trascendente, ma in questo caso non esiste una base di trascendenza. Infatti, per ogni $s \in \mathbb{N}$, $g_1, g_2, \dots, g_s \in K(X_1, X_2, \dots)$, l'estensione di campi $K(g_1, g_2, \dots, g_s) \subseteq K(X_1, X_2, ...)$ è trascendente poiché possiamo sicuramente fissare un intero $t \in \mathbb{N}$ in modo tale che X_t non occorra in g_i per ogni $i = 1, 2, \dots, s$ e allora, come è facile verificare, la variabile X_t è trascendente su $K(g_1, g_2, \dots, g_s)$.

Definizione 1.16. Sia $X \subseteq \mathbb{A}^n_k$ un chiuso. Il quoziente $\mathcal{A}_X = R_n/\mathcal{I}(X)$ è detto *anello delle coordinate su* X. Denotiamo con $\dim X$ la *dimensione di* X, definita nel modo seguente:

- Se X è vuoto, poniamo $\dim X := -1$.
- Se X è irriducibile, sia $\mathcal{F}_X$ il campo dei quozienti di $\mathcal{A}_X$. Poniamo $\dim X := \operatorname{trdeg}_k \mathcal{F}_X$.
- Se X è non vuoto e riducibile, infine, sia $X = X_1 \cup X_2 \cup \cdots \cup X_m$ la decomposizione in componenti irriducibili di X. Poniamo $\dim X := \max_{i=1,2,\dots,m} \dim X_i$.

La definizione precedente è ben posta per il punto (i) della proposizione 1.5 il quale ci garantisce che, se X è irriducibile, allora:

- L'anello $\mathcal{A}_X$ è un dominio e dunque esiste il suo campo dei quozienti.
- Se identifichiamo k con il sottoanello $\{\lambda + \mathcal{I}(X) \colon \lambda \in k\}$, allora $k \subseteq \mathcal{F}_X$ è un'estensione di campi e dunque il grado di trascendenza di $\mathcal{F}_X$ su k è definito.

Osservazione 1.17. Sia k un campo infinito. Allora $\dim \mathbb{A}^n_k = n$.

Dimostrazione. Per definizione:

$$\mathcal{A}_{\mathbb{A}^n_k} = R_n/\mathcal{I}(\mathbb{A}^n_k) = R_n = k[X_1, X_2, \dots, X_n]$$

Sappiamo che $\mathbb{A}^n_k$ è irriducibile se k è un campo infinito, quindi la sua dimensione sarà:

$$\dim \mathbb{A}^n_k = \operatorname{trdeg}_k k(X_1, X_2, \dots, X_n) = n \qquad \square$$

Vedremo che, se k è un campo finito, allora $\dim \mathbb{A}^n_k = 0$. In tal caso, infatti, le componenti irriducibili di $\mathbb{A}^n_k$ sono punti e, come vedremo, questi hanno dimensione nulla.

Lezione 6

Raffaele Di Donna

Funzioni regolari su un chiuso $X \subseteq \mathbb{A}^n_k$, la k-algebra $k[X]$ delle funzioni regolari su X. L'isomorfismo tra $k[X_1, \ldots, X_n]/\mathcal{I}(X)$ e $k[X]$. Morfismi (o applicazioni regolari) tra due chiusi. L'omomorfismo indotto da un morfismo tra due chiusi. Corrispondenza biunivoca tra l'insieme dei morfismi tra due chiusi e l'insieme degli omomorfismi tra k-algebre, prima parte della dimostrazione.

Ricordiamo la definizione di dimensione di un chiuso affine.

Definizione 1.16. Sia $X \subseteq \mathbb{A}^n_k$ un chiuso. Il quoziente $\mathcal{A}_X = R_n/\mathcal{I}(X)$ è detto *anello delle coordinate su* X. Denotiamo con $\dim X$ la *dimensione di* X, definita nel modo seguente:

- Se X è vuoto, poniamo $\dim X := -1$.
- Se X è irriducibile, sia $\mathcal{F}_X$ il campo dei quozienti di $\mathcal{A}_X$. Poniamo $\dim X := \operatorname{trdeg}_k \mathcal{F}_X$.
- Se X è non vuoto e riducibile, infine, sia $X = X_1 \cup X_2 \cup \cdots \cup X_m$ la decomposizione in componenti irriducibili di X. Poniamo $\dim X := \max_{i=1,2,\ldots,m} \dim X_i$.

Abbiamo già dimostrato il seguente fatto.

Osservazione 1.17. Sia k un campo infinito. Allora $\dim \mathbb{A}^n_k = n$.

Vediamo ora il seguente risultato.

Osservazione 1.18. Sia $p \in \mathbb{A}^n_k$ un punto. Allora $\dim p = 0$. In particolare, se k è finito, vale che $\dim \mathbb{A}^n_k = 0$.

Dimostrazione. Consideriamo l'applicazione:

$$\begin{aligned} \Phi\colon R_n &\longrightarrow k \\ f &\longmapsto f(p) \end{aligned}$$

Si vede immediatamente che Φ è un omomorfismo di anelli. Inoltre è suriettivo perché, preso un qualunque $\lambda \in k$, l'omomorfismo Φ manda il polinomio costante di valore λ nello scalare λ. D'altra parte, abbiamo che:

$$\operatorname{Ker} \Phi = \{f \in R_n \colon f(p) = 0\} = \mathcal{I}(p)$$

Dal primo teorema di isomorfismo segue dunque che:

$$R_n/\mathcal{I}(p) \cong k$$

Usando il fatto che il grado di trascendenza è invariante per isomorfismi di anelli, si può perciò affermare che:

$$\dim p = \operatorname{trdeg}_k k = 0$$

Si noti ora che, se $X = \{x_1, x_2, \ldots, x_m\}$ è un chiuso finito di $\mathbb{A}^n_k$, allora la decomposizione di X in componenti irriducibili è:

$$X = \{x_1\} \cup \{x_2\} \cup \cdots \cup \{x_m\}$$

Ne discende che $\dim X = 0$ per definizione di dimensione. In particolare, se k è un campo finito, allora $\mathbb{A}^n_k$ è finito, perciò $\dim \mathbb{A}^n_k = 0$. $\square$

Osservazione 1.19. Sia $X \subseteq \mathbb{A}^n_k$ un chiuso. Allora $\dim X \leq n$.

Dimostrazione. Per definizione di dimensione, possiamo ridurci a considerare il caso in cui X è irriducibile. Per quanto si era osservato nella dimostrazione del punto (i) della proposizione 1.5, abbiamo la condizione:

$$\mathcal{A}_X = k[\overline{X_1}, \overline{X_2}, \dots, \overline{X_n}]$$

Passando quindi al campo dei quozienti, otteniamo che:

$$\mathcal{F}_X = k(\overline{X_1}, \overline{X_2}, \dots, \overline{X_n})$$

Ora, se $\overline{X_1}, \overline{X_2}, \dots, \overline{X_n}$ sono algebricamente indipendenti su k, allora essi formano una base di trascendenza di $\mathcal{F}_X$ su k e dunque $\dim X = n$. Se invece sono algebricamente dipendenti su k, allora esiste un polinomio non nullo $p \in k[Z_1, Z_2, \dots, Z_n]$ tale che $p(\overline{X_1}, \overline{X_2}, \dots, \overline{X_n}) = 0$. Notiamo che p dipende da almeno una delle variabili $Z_1, Z_2, \dots, Z_n$, altrimenti p sarebbe il polinomio nullo. Possiamo dunque supporre che p dipenda da Z_1 e allora $\overline{X_1}$ è algebrico su $k(\overline{X_2}, \dots, \overline{X_n})$ in quanto annulla il polinomio $q \in k(\overline{X_2}, \dots, \overline{X_n})[Z_1]$ definito da:

$$q(Z_1) := p(Z_1, \overline{X_2}, \dots, \overline{X_n})$$

Abbiamo allora un'estensione algebrica:

$$k(\overline{X_2}, \dots, \overline{X_n}) \subseteq k(\overline{X_1}, \overline{X_2}, \dots, \overline{X_n}) = \mathcal{F}_X$$

Adesso, se $\overline{X_2}, \dots, \overline{X_n}$ sono algebricamente indipendenti su k, allora essi formano una base di trascendenza di $\mathcal{F}_X$ su k e dunque $\dim X = n - 1$. In caso contrario, si può ripetere lo stesso argomento di prima e assumere, senza perdita di generalità, che $\overline{X_2}$ sia algebrico su $k(\overline{X_3}, \dots, \overline{X_n})$. Da questo deduciamo, come prima, che l'estensione $k(\overline{X_3}, \dots, \overline{X_n}) \subseteq \mathcal{F}_X$ è algebrica. Iterando questo ragionamento, si ottiene che $\dim X \leq n$. □

2 Funzioni regolari e morfismi di spazi affini

2.1 Funzioni regolari

Definizione 2.1. Sia $X \subseteq \mathbb{A}^n_k$ un chiuso. Un'applicazione $\phi\colon X \to k$ è detta una *funzione regolare su* X se esiste un polinomio $f \in R_n$ tale che $\phi(p) = f(p)$ per ogni $p \in X$ oppure, equivalentemente, tale che $\phi = \phi_f$. L'insieme delle funzioni regolari su X prende il nome di *anello delle funzioni regolari su* X e si denota $k[X]$.

Osservazione 2.2. Sia $X \subseteq \mathbb{A}^n_k$ un chiuso. Allora $k[X]$ è una k-algebra.

Dimostrazione. Siano ϕ e ψ funzioni regolari su X. Consideriamo le operazioni usuali di somma e prodotto tra funzioni e la solita operazione di prodotto di una funzione per uno scalare. Per definizione, esistono due polinomi $f, g \in R_n$ tali che si abbia $\phi(p) = f(p)$, $\psi(p) = g(p)$ per ogni $p \in X$ e dunque, per qualsiasi punto $p \in X$, abbiamo:

$$(\phi + \psi)(p) = \phi(p) + \psi(p) = f(p) + g(p) = (f + g)(p)$$

Perciò $\phi + \psi$ è una funzione regolare su X. In modo simile, si dimostra che $\phi\psi$ e $\lambda\phi$ sono funzioni regolari su X per qualsiasi $\lambda \in k$. A questo punto si verifica assai facilmente che $k[X]$ acquista, con queste operazioni, una struttura di k-algebra. □

Proposizione 2.3. *Sia $X \subseteq \mathbb{A}^n_k$ un chiuso. Allora:*

$$k[X] \cong \mathcal{A}_X$$

In particolare:

(i) *L'anello $k[X]$ è una k-algebra finitamente generata priva di elementi nilpotenti.*

(ii) *Il chiuso $X \subseteq \mathbb{A}^n_k$ è irriducibile se e solo se $k[X]$ è un dominio.*

Dimostrazione. Basterà dimostrare la prima parte dell'enunciato in quanto il resto segue dall'isomorfismo e dalla proposizione 1.5. Consideriamo allora l'applicazione:

$$\begin{aligned} \Phi\colon R_n &\longrightarrow k[X] \\ f &\longmapsto \phi_f \end{aligned}$$

È evidentemente una mappa ben definita e suriettiva per definizione di funzione regolare. Inoltre, si verifica assai facilmente che è un omomorfismo di k-algebre (basta verificare che Φ rispetta le operazioni di somma, prodotto e prodotto per uno scalare). Ora:

$$\begin{aligned} \operatorname{Ker}\Phi &= \{f \in R_n \colon \phi_f = 0\} \\ &= \{f \in R_n \colon \phi_f(p) = 0 \,\text{per ogni}\, p \in X\} \\ &= \{f \in R_n \colon f(p) = 0 \,\text{per ogni}\, p \in X\} = \mathcal{I}(X) \end{aligned}$$

L'asserto discende quindi dal primo teorema di isomorfismo. □

Esempio 2.4. Sia k un campo infinito. Allora $k[\mathbb{A}^n_k] \cong R_n$. Infatti, per la proposizione precedente, vale che:

$$k[\mathbb{A}^n_k] \cong R_n/\mathcal{I}(\mathbb{A}^n_k) = R_n$$

Esempio 2.5. Sia $p \in \mathbb{A}^n_k$ un punto. Allora $k[p] \cong k$. In effetti, dalla dimostrazione dell'osservazione 1.18 e dalla proposizione precedente segue che:

$$k[p] \cong R_n/\mathcal{I}(p) \cong k$$

Osservazione 2.6. Sia $p \in \mathbb{A}^n_k$ un punto e assumiamo che $p = (a_1, a_2, \dots, a_n)$. Allora abbiamo la condizione:

$$\mathcal{I}(p) = (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$$

Dimostrazione. Sia $f \in \mathcal{I}(p)$ un polinomio. Scriviamo f come una somma di monomi di grado j al variare di tutti i possibili $j = 0, 1, \dots, d$, dove d è il grado complessivo del polinomio. Formalmente, per un opportuno intero $d \geq 0$ e per certi $\alpha_{i_1,i_2,\dots,i_n} \in k$, con $i_1, i_2, \dots, i_n \geq 0$ interi la cui somma è compresa tra 0 e d, si ha:

$$\begin{aligned} f &= \sum_{j=0}^{d} \sum_{\substack{i_1,i_2,\dots,i_n \geq 0 \text{ interi} \\ i_1+i_2+\dots+i_n=j}} \alpha_{i_1,i_2,\dots,i_n} X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n} \\ &= \sum_{j=0}^{d} \sum_{\substack{i_1,i_2,\dots,i_n \geq 0 \text{ interi} \\ i_1+i_2+\dots+i_n=j}} \alpha_{i_1,i_2,\dots,i_n} (X_1 - a_1 + a_1)^{i_1} (X_2 - a_2 + a_2)^{i_2} \cdots (X_n - a_n + a_n)^{i_n} \end{aligned}$$

Dal teorema binomiale segue dunque che $f = g + c$ per qualche $g \in (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$ e per un certo $c \in k$. Ma $f \in \mathcal{I}(p)$, quindi:

$$0 = f(p) = g(p) + c = c$$

Abbiamo dunque dimostrato che $f = g$ e, in particolare, che $f \in (X_1 - a_1, X_2 - a_2, \dots, X_n - a_n)$. L'altra inclusione è banale. □

2.2 Morfismi di spazi affini

Definizione 2.7. Siano $X \subseteq \mathbb{A}^n_k$ e $Y \subseteq \mathbb{A}^m_k$ chiusi. Un'applicazione $\phi\colon X \to Y$ prende il nome di *morfismo* (o *applicazione regolare*) se esistono dei polinomi $f_1, f_2, \dots, f_m \in R_n$ tali che, per qualunque $p \in X$, si abbia:

$$\phi(p) = (f_1(p), f_2(p), \dots, f_m(p))$$

Equivalentemente, si richiede che esistano $\phi_1, \phi_2, \ldots, \phi_m$ funzioni regolari su X tali che, per qualsiasi punto $p \in X$, valga:

$$\phi(p) = (\phi_1(p), \phi_2(p), \ldots, \phi_m(p))$$

Si dice che ϕ è un *isomorfismo* se esiste un morfismo $\psi\colon Y \to X$ tale che $\psi \circ \phi = \mathrm{id}_X$ e $\phi \circ \psi = \mathrm{id}_Y$. Inoltre, se esiste un isomorfismo tra X e Y, diremo che X e Y sono *isomorfi* e scriveremo $X \cong Y$. Infine, si dirà che ϕ è *dominante* se $\phi(X)$ è denso in Y.

Ci si potrebbe chiedere se un morfismo biiettivo sia o meno un isomorfismo, cioè se l'applicazione inversa di un morfismo sia a sua volta un morfismo. La risposta a questa domanda è negativa: si possono costruire morfismi biiettivi che non sono tuttavia degli isomorfismi. Ne vedremo un esempio nella lezione successiva.

Osservazione 2.8. Nella definizione 2.7 è implicito che $f_1, f_2, \ldots, f_m \in R_n$ siano tali che, per qualsiasi $p \in X$:

$$(f_1(p), f_2(p), \ldots, f_m(p)) \in Y$$

Naturalmente, vale lo stesso per le funzioni regolari $\phi_1, \phi_2, \ldots, \phi_m$ menzionate nella definizione equivalente.

Facciamo ora alcune considerazioni di natura topologica.

Osservazione 2.9. Siano $X \subseteq \mathbb{A}^n_k$ e $Y \subseteq \mathbb{A}^m_k$ due chiusi. Un morfismo $\phi\colon X \to Y$ è un'applicazione continua.

Dimostrazione. Assumiamo $\phi(p) = (f_1(p), f_2(p), \ldots, f_m(p))$ per ogni $p \in X$. Sarà sufficiente mostrare che la preimmagine di un chiuso in Y tramite ϕ è un chiuso in X. Un chiuso in Y è l'intersezione di un chiuso in $\mathbb{A}^m_k$ con Y, perciò consideriamo un chiuso $\mathcal{Z}(g_1, g_2, \ldots, g_s) \subseteq \mathbb{A}^m_k$, dove $g_1, g_2, \ldots, g_s \in R_m$. Consideriamo inoltre, per ogni $i = 1, 2, \ldots, s$, il polinomio composto:

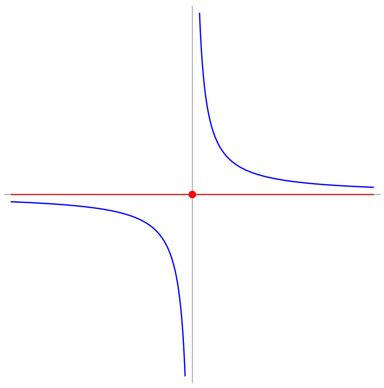
$$h_i(X_1, X_2, \ldots, X_n) := g_i(f_1(X_1, X_2, \ldots, X_n), f_2(X_1, X_2, \ldots, X_n), \ldots, f_m(X_1, X_2, \ldots, X_n))$$

Allora:

$$\begin{aligned}
\phi^{-1}(\mathcal{Z}(g_1, g_2, \ldots, g_s) \cap Y) &= \{p \in X\colon \phi(p) \in \mathcal{Z}(g_1, g_2, \ldots, g_s)\} \\
&= \{p \in X\colon g_i(\phi(p)) = 0 \text{ per ogni } i = 1, 2, \ldots, s\} \\
&= \{p \in X\colon h_i(p) = 0 \text{ per ogni } i = 1, 2, \ldots, s\} = \mathcal{Z}(h_1, h_2, \ldots, h_s)
\end{aligned}$$

□

In generale, un morfismo di spazi affini non è un'applicazione chiusa né aperta: lo dimostrano i seguenti controesempi.



Esempio 2.10. Andiamo a considerare la proiezione $\pi\colon \mathbb{A}^2_k \to \mathbb{A}^1_k$ sulla prima componente, cioè la mappa data da $\pi(x_1, x_2) := x_1$. Si tratta di una funzione regolare e dunque di un morfismo, ma $\mathcal{Z}(X_1X_2 - 1)$ in $\mathbb{A}^2_k$ ha per immagine l'aperto $\mathbb{A}^1_k \setminus \{0\}$.

Esempio 2.11. Consideriamo ora l'applicazione $\phi\colon \mathbb{A}^2_k \to \mathbb{A}^2_k$ definita da $\phi(x_1, x_2) := (x_1, x_1x_2)$. È chiaro che ϕ sia un morfismo di spazi affini. Facciamo vedere adesso che l'immagine dell'aperto $\mathbb{A}^2_k \setminus \mathcal{Z}(X_2)$ tramite ϕ è l'insieme $S := (\mathbb{A}^2_k \setminus \mathcal{Z}(X_1X_2)) \cup \{(0,0)\}$. Si fissi allora un qualsiasi punto $p \in \mathbb{A}^2_k \setminus \mathcal{Z}(X_2)$, $p = (x_1, x_2)$. Abbiamo $x_2 \neq 0$ e di conseguenza:

$$\phi(x_1, x_2) = (x_1, x_1x_2) \in \begin{cases} \{(0,0)\} & \text{se } x_1 = 0 \\ \mathbb{A}^2_k \setminus \mathcal{Z}(X_1X_2) & \text{se } x_1 \neq 0 \end{cases}$$

Viceversa, sia $(x_1, x_2) \in S$. Se $(x_1, x_2) = (0,0)$, allora $(x_1, x_2) = \phi(0,1)$, mentre se $(x_1, x_2) \in \mathbb{A}^2_k \setminus \mathcal{Z}(X_1X_2)$ si ha $x_1 \neq 0$. In particolare, abbiamo che $(x_1, x_2) = \phi(x_1, x_2/x_1)$. Si noti ora che S non è un insieme aperto di $\mathbb{A}^2_k$ in quanto il suo complementare, vale a dire $\mathcal{Z}(X_1X_2) \setminus \{(0,0)\}$, non è un chiuso. Infatti, la sua chiusura è $\mathcal{Z}(X_1X_2)$.

Per dimostrarlo, consideriamo un chiuso $\mathcal{Z}(I)$, con I ideale di $k[X_1, X_2]$, contenente $\mathcal{Z}(X_1X_2)\setminus\{(0,0)\}$ e fissiamo $f \in I$. Allora f dovrà annullarsi su tutti i punti di $\mathcal{Z}(X_1X_2)\setminus\{(0,0)\}$, vale a dire su ogni punto del tipo $(a, 0)$ oppure $(0, a)$ con $a \in k$, $a \neq 0$. In particolare, i polinomi $f(a, X_2)$ e $f(X_1, a)$ in una indeterminata sono nulli in 0. Dunque[1] i monomi X_1 e X_2 dividono f e quindi X_1X_2, che è il loro minimo comune multiplo, dovrà dividere f. In altre parole, si ha che $f \in (X_1X_2)$. Avendo mostrato che $I \subseteq (X_1X_2)$, si può concludere che $\mathcal{Z}(I) \supseteq \mathcal{Z}(X_1X_2)$ e di conseguenza $\mathcal{Z}(X_1X_2)$ è il più piccolo chiuso di $\mathbb{A}^2_k$ contenente $\mathcal{Z}(X_1X_2)\setminus\{(0,0)\}$.

Proposizione 2.12. *Siano $X \subseteq \mathbb{A}^n_k$ e $Y \subseteq \mathbb{A}^m_k$ due chiusi.*

(i) *Se $\phi\colon X \to Y$ è un morfismo, allora è definito un omomorfismo di k-algebre:*

$$\begin{aligned} \phi^*\colon k[Y] &\longrightarrow k[X] \\ \psi &\longmapsto \psi \circ \phi \end{aligned}$$

(ii) *Sia $\chi\colon k[Y] \to k[X]$ un omomorfismo di k-algebre. Allora esiste un unico morfismo $\phi\colon X \to Y$ tale che si abbia $\chi = \phi^*$.*

(iii) *Un morfismo $\phi\colon X \to Y$ è un isomorfismo se e solo se ϕ^* è un isomorfismo di k-algebre.*

Dimostrazione.

(i) Dobbiamo innanzitutto assicurarci che ϕ^* sia una mappa ben definita, ovvero che $\psi \circ \phi \in k[X]$. Per definizione, esistono $f_1, f_2, \dots, f_m \in R_n$ tali che $\phi(p) = (f_1(p), f_2(p), \dots, f_m(p))$ per ogni $p \in X$ ed esiste un polinomio $g \in R_m$ tale che $\psi(q) = g(q)$ per qualsiasi punto $q \in Y$. Sia ora $h \in R_n$ dato da:

$$h(X_1, X_2, \dots, X_n) := g(f_1(X_1, X_2, \dots, X_n), f_2(X_1, X_2, \dots, X_n), \dots, f_m(X_1, X_2, \dots, X_n))$$

Allora $\psi \circ \phi$ è una funzione regolare su X perché, per ogni $p \in X$, si ha:

$$(\psi \circ \phi)(p) = \psi(\phi(p)) = g(f_1(p), f_2(p), \dots, f_m(p)) = h(p)$$

Si noti adesso che, per ogni $\psi, \psi' \in k[X]$ e per qualunque punto $p \in X$, valgono le seguenti identità:

$$\begin{aligned} \phi^*(\psi + \psi')(p) = ((\psi + \psi') \circ \phi)(p) &= (\psi + \psi')(\phi(p)) = \psi(\phi(p)) + \psi'(\phi(p)) \\ &= (\psi \circ \phi)(p) + (\psi' \circ \phi)(p) = \phi^*(\psi)(p) + \phi^*(\psi')(p) \end{aligned}$$

Abbiamo così dimostrato che $\phi^*(\psi + \psi') = \phi^*(\psi) + \phi^*(\psi')$. In modo del tutto analogo si dimostra che $\phi^*(\psi\psi') = \phi^*(\psi)\phi^*(\psi')$ e che $\phi^*(\lambda\psi) = \lambda\phi^*(\psi)$ per ogni $\lambda \in k$. Concludiamo allora che ϕ^* è un omomorfismo di k-algebre.

(ii) Consideriamo le seguenti applicazioni:

$$\begin{array}{ccccccc} k[Y_1, Y_2, \dots, Y_m] & \xrightarrow{\pi} & k[Y_1, Y_2, \dots, Y_m]/\mathcal{I}(Y) & \xrightarrow{\alpha} & k[Y] & \xrightarrow{\chi} & k[X] \\ g & \longmapsto & \bar{g} & \longmapsto & \phi_g & \longmapsto & \chi(\phi_g) \end{array}$$

Sappiamo che l'applicazione quoziente π è un omomorfismo di k-algebre, mentre α è l'isomorfismo la cui esistenza e buona definizione discendono dall'applicazione del primo teorema di isomorfismo alla fine della dimostrazione della proposizione 2.3. Definiamo $\phi_i := \chi((\alpha \circ \pi)(Y_i))$ per $i = 1, 2, \dots, m$ e consideriamo l'applicazione:

$$\begin{aligned} \phi\colon X &\longrightarrow Y \\ p &\longmapsto (\phi_1(p), \phi_2(p), \dots, \phi_m(p)) \end{aligned}$$

[1]Questa è una facile conseguenza del teorema di Ruffini, del quale ricordiamo l'enunciato: siano A un dominio, $\alpha \in A$ e sia $f \in A[X]$ un polinomio non costante. Allora il resto della divisione di f per $(X - \alpha)$ è $f(\alpha)$. La dimostrazione di questo risultato è stata già trattata nel corso AL110.

Per poter affermare che ϕ è un morfismo di spazi affini, dobbiamo prima dimostrare che $\phi(p) \in Y$ per ogni $p \in X$. Osserviamo che, essendo π, α e χ omomorfismi di k-algebre, per ogni $i, j = 1, 2, \dots, m$ e per ogni $\lambda \in k$ si ha:

$$\begin{aligned}
\chi((\alpha \circ \pi)(Y_i + Y_j)) &= \chi((\alpha \circ \pi)(Y_i)) + \chi((\alpha \circ \pi)(Y_j)) = \phi_i + \phi_j \\
\chi((\alpha \circ \pi)(Y_i Y_j)) &= \chi((\alpha \circ \pi)(Y_i))\chi((\alpha \circ \pi)(Y_j)) = \phi_i \phi_j \\
\chi((\alpha \circ \pi)(\lambda Y_i)) &= \lambda \chi((\alpha \circ \pi)(Y_i)) = \lambda \phi_i
\end{aligned}$$

Ne segue che, per qualsiasi polinomio $g \in k[Y_1, Y_2, \dots, Y_m]$, si ha $\chi((\alpha \circ \pi)(g)) = g(\phi_1, \phi_2, \dots, \phi_m)$. A questo punto si noti che, se $g \in \mathcal{I}(Y)$, allora $\pi(g) = \bar{0}$ e di conseguenza $\chi((\alpha \circ \pi)(g))$, che coincide con $g(\phi_1, \phi_2, \dots, \phi_m)$, è la funzione regolare nulla su X. Ne deduciamo che, per ogni punto $p \in X$, si ha $g(\phi_1(p), \phi_2(p), \dots, \phi_m(p)) = 0$ e, poiché questo vale per ogni polinomio $g \in \mathcal{I}(Y)$, concludiamo che $\phi(p) = (\phi_1(p), \phi_2(p), \dots, \phi_m(p)) \in \mathcal{Z}(\mathcal{I}(Y)) = Y$. Con questo abbiamo dimostrato che ϕ è un morfismo di spazi affini. Nella prossima lezione vedremo che $\chi = \phi^*$ per concludere la dimostrazione del punto (ii) e poi ci occuperemo del punto (iii).

Geometria algebrica 1 (Matematica, Roma Tre)	Oct 7, 2020

Lezione 7

Raffaele Di Donna

La corrispondenza biunivoca tra l'insieme dei morfismi tra due chiusi e l'insieme degli omomorfismi tra k-algebre, seconda parte della dimostrazione. Due chiusi affini isomorfi hanno la stessa dimensione. Se k è algebricamente chiuso, ogni k-algebra finitamente generata e priva di nilpotenti è la k-algebra delle funzioni regolari di un unico chiuso affine (a meno di isomorfismo). Un morfismo è dominante se e solo se è iniettivo l'omomorfismo indotto. Se l'omomorfismo indotto è suriettivo e k è algebricamente chiuso, allora il morfismo è iniettivo e l'immagine è chiusa. Un esempio di morfismo biiettivo con omomorfismo indotto non suriettivo (la cubica con cuspide).

Torniamo al seguente risultato.

Proposizione 2.12. *Siano $X \subseteq \mathbb{A}^n_k$ e $Y \subseteq \mathbb{A}^m_k$ due chiusi.*

(i) *Se $\phi\colon X \to Y$ è un morfismo, allora è definito un omomorfismo di k-algebre:*

$$\begin{aligned} \phi^*\colon k[Y] &\longrightarrow k[X] \\ \psi &\longmapsto \psi \circ \phi \end{aligned}$$

(ii) *Sia $\chi\colon k[Y] \to k[X]$ un omomorfismo di k-algebre. Allora esiste un unico morfismo $\phi\colon X \to Y$ tale che si abbia $\chi = \phi^*$.*

(iii) *Un morfismo $\phi\colon X \to Y$ è un isomorfismo se e solo se ϕ^* è un isomorfismo di k-algebre.*

Dimostrazione. Abbiamo già dimostrato il punto (i) nella scorsa lezione. Riprendiamo la dimostrazione del punto (ii).

(ii) Avevamo considerato le seguenti applicazioni:

$$\begin{array}{ccccccc} k[Y_1, Y_2, \ldots, Y_m] & \xrightarrow{\pi} & k[Y_1, Y_2, \ldots, Y_m]/\mathcal{I}(Y) & \xrightarrow{\alpha} & k[Y] & \xrightarrow{\chi} & k[X] \\ g & \longmapsto & \bar{g} & \longmapsto & \phi_g & \longmapsto & \chi(\phi_g) \end{array}$$

Avevamo definito $\phi_i := \chi((\alpha \circ \pi)(Y_i))$ per ogni $i = 1, 2, \ldots, m$ e avevamo dimostrato che la seguente applicazione è un morfismo di spazi affini:

$$\begin{aligned} \phi\colon X &\longrightarrow Y \\ p &\longmapsto (\phi_1(p), \phi_2(p), \ldots, \phi_m(p)) \end{aligned}$$

In particolare, avevamo osservato che $\chi((\alpha \circ \pi)(g)) = g(\phi_1, \phi_2, \ldots, \phi_m)$ per un qualsiasi polinomio $g \in k[Y_1, Y_2, \ldots, Y_m]$. Adesso dimostriamo che $\chi = \phi^*$ cioè che, per una funzione regolare $\psi \in k[Y]$ qualsiasi, si ha $\chi(\psi) = \phi^*(\psi)$. Basta osservare che, per definizione di funzione regolare su Y, esiste un polinomio $g \in k[Y_1, Y_2, \ldots, Y_m]$ tale che $\psi(q) = g(q)$ per ogni punto $q \in Y$ e che, di conseguenza, per ogni $p \in X$ si hanno le seguenti identità:

$$\begin{aligned} \phi^*(\psi)(p) = (\psi \circ \phi)(p) = \psi(\phi(p)) &= g(\phi_1(p), \phi_2(p), \ldots, \phi_m(p)) \\ &= (\chi(\alpha \circ \pi)(g))(p) = \chi(\phi_g)(p) = \chi(\psi)(p) \end{aligned}$$

Adesso ci rimane da dimostrare l'unicità del morfismo $\phi\colon X \to Y$ tale che $\chi = \phi^*$. Sia $\psi\colon X \to Y$ un morfismo tale che $\chi = \psi^*$. Per definizione di morfismo, esistono m funzioni regolari $\psi_1, \psi_2, \ldots, \psi_m$ su X tali che, per ogni punto $p \in X$, si abbia $\psi(p) = (\psi_1(p), \psi_2(p), \ldots, \psi_m(p))$. Per concludere che

$\phi = \psi$ basterà dimostrare che, per ogni $p \in X$, vale $\phi(p) = \psi(p)$, ossia $\phi_i(p) = \psi_i(p)$ per ogni indice $i = 1, 2, \ldots, m$. Notiamo che, per ogni $i = 1, 2, \ldots, m$, l'applicazione $\phi_{yi} := (\alpha \circ \pi)(Y_i)$ è la funzione regolare su Y che calcola la i-esima coordinata di un punto. Ne segue che, per ogni $i = 1, 2, \ldots, m$ e per ogni $p \in X$, si ha:

$$\psi_i(p) = \phi_{yi}(\psi(p)) = \psi^*(\phi_{yi})(p) = \phi^*(\phi_{yi})(p) = \phi_{yi}(\phi(p)) = \phi_i(p)$$

(iii) Prima di procedere con la dimostrazione vera e propria osserviamo preliminarmente che, se $Z \subseteq \mathbb{A}^p_k$ è un chiuso e $\phi\colon X \to Y$, $\psi\colon Y \to Z$ sono morfismi di spazi affini, allora $\psi \circ \phi\colon X \to Z$ è a sua volta un morfismo, come è facile verificare e vale che $(\psi \circ \phi)^* = \phi^* \circ \psi^*$, o equivalentemente il diagramma di applicazioni che segue è commutativo:

$$\begin{tikzcd} k[Z] \arrow[r, "\psi^*"] \arrow[rr, bend right, "(\psi\circ\phi)^*"'] & k[Y] \arrow[r, "\phi^*"] & k[X] \end{tikzcd}$$

Inoltre, si ha che $\mathrm{id}_X^* = \mathrm{id}_{k[X]}$. Anche questi due fatti si dimostrano facilmente.

Procediamo con la dimostrazione del punto (iii). Supponiamo che ϕ sia un isomorfismo, ovvero che esista un morfismo $\psi\colon Y \to X$ tale che $\psi \circ \phi = \mathrm{id}_X$ e $\phi \circ \psi = \mathrm{id}_Y$. Ne deduciamo, in particolare, che $(\psi \circ \phi)^* = \mathrm{id}_X^*$ e $(\phi \circ \psi)^* = \mathrm{id}_Y^*$ ma questo, per quanto abbiamo osservato preliminarmente, è del tutto equivalente a richiedere che valga $\phi^* \circ \psi^* = \mathrm{id}_{k[X]}$ e $\psi^* \circ \phi^* = \mathrm{id}_{k[Y]}$. Questo dimostra che ϕ^* è un isomorfismo perché abbiamo trovato una sua inversa bilatera. Viceversa, supponiamo che ϕ^* sia un isomorfismo. Allora ϕ^* possiede un'inversa $\chi\colon k[X] \to k[Y]$. Per il punto (ii) precedente, esiste inoltre un morfismo $\psi\colon Y \to X$ tale che si abbia $\chi = \psi^*$. Abbiamo allora le due seguenti condizioni:

$$(\psi \circ \phi)^* = \phi^* \circ \psi^* = \phi^* \circ \chi = \mathrm{id}_{k[X]} = \mathrm{id}_X^*$$
$$(\phi \circ \psi)^* = \psi^* \circ \phi^* = \chi \circ \phi^* = \mathrm{id}_{k[Y]} = \mathrm{id}_Y^*$$

Ancora per il punto (ii), otteniamo le condizioni $\psi \circ \phi = \mathrm{id}_X$ e $\phi \circ \psi = \mathrm{id}_Y$. Abbiamo allora che ϕ è un isomorfismo e quindi la dimostrazione è conclusa. □

Vediamo ora qualche conseguenza di questa proposizione.

Osservazione 2.13. Siano $X \subseteq \mathbb{A}^n_k$ e $Y \subseteq \mathbb{A}^m_k$ due chiusi non vuoti. Se $X \cong Y$, allora si ha $\dim X = \dim Y$.

Dimostrazione. Ricordiamo innanzitutto che, per l'osservazione 2.9, i morfismi sono applicazioni continue. Dall'ipotesi che $X \cong Y$ discende allora, in particolare, che X è omeomorfo a Y e, sotto questa condizione, si stabilisce facilmente che X è riducibile se e solo se Y è riducibile. Se infatti ϕ è un omeomorfismo da X a Y, allora ϕ fa corrispondere a una decomposizione in irriducibili $Y = Y_1 \cup Y_2 \cup \cdots \cup Y_s$ una decomposizione in irriducibili $X = \phi^{-1}(Y_1) \cup \phi^{-1}(Y_2) \cup \cdots \cup \phi^{-1}(Y_s)$.

Possiamo dunque distinguere il caso in cui X e Y sono irriducibili da quello in cui essi sono riducibili. Nel primo caso, dall'ipotesi che $X \cong Y$ e dal punto (iii) della proposizione 2.12 discende che $k[X] \cong k[Y]$. Dalla proposizione 2.3 segue allora che $\mathcal{A}_X \cong \mathcal{A}_Y$. Ma per il punto (i) della proposizione 1.5 e per l'ipotesi che X e Y siano irriducibili sappiamo che gli anelli $\mathcal{A}_X$ e $\mathcal{A}_Y$ sono in realtà domini, per cui possiamo considerare i rispettivi campi dei quozienti $\mathcal{F}_X$ e $\mathcal{F}_Y$ i quali, ovviamente, saranno anch'essi isomorfi. Otteniamo allora che $\operatorname{trdeg}_k \mathcal{F}_X = \operatorname{trdeg}_k \mathcal{F}_Y$, cioè che $\dim X = \dim Y$.

Assumiamo adesso che i chiusi X e Y siano riducibili e che $Y = Y_1 \cup Y_2 \cup \cdots \cup Y_s$ sia una decomposizione di Y in irriducibili. Come si è già detto, se ϕ è un isomorfismo, allora $X = \phi^{-1}(Y_1) \cup \phi^{-1}(Y_2) \cup \cdots \cup \phi^{-1}(Y_s)$ è una decomposizione di X in irriducibili. Inoltre, per ogni indice $i = 1, 2, \ldots, s$, la restrizione di ϕ a $\phi^{-1}(Y_i)$ è un isomorfismo da $\phi^{-1}(Y_i)$ in Y_i quindi, essendo $\phi^{-1}(Y_i)$ e Y_i chiusi irriducibili isomorfi, per quanto abbiamo dimostrato prima essi hanno la stessa dimensione. Ma allora:

$$\dim X = \max_{i=1,2,\ldots,s} \dim \phi^{-1}(Y_i) = \max_{i=1,2,\ldots,s} \dim Y_i = \dim Y$$ □

Più avanti vedremo che, in generale, non vale il viceversa dell'osservazione precedente, cioè due chiusi non vuoti che hanno la stessa dimensione non sono necessariamente isomorfi. Costruiremo un esempio esplicito quando avremo introdotto la nozione di equivalenza birazionale. Altra conseguenza della proposizione 2.12 è il seguente risultato.

Corollario 2.14. *Sia k un campo algebricamente chiuso e sia A una k-algebra finitamente generata priva di elementi nilpotenti. Allora esistono un intero $n \in \mathbb{N}$ e un chiuso $X \subseteq \mathbb{A}_k^n$ tale che valga $k[X] \cong A$. Inoltre, un tale chiuso X è unico a meno di isomorfismo cioè, se $Y \subseteq \mathbb{A}_k^m$ è un chiuso tale che $k[Y] \cong A$, allora $Y \cong X$.*

Dimostrazione. Per ipotesi, esistono $g_1, g_2, \ldots, g_n \in A$ tali che $A = k[g_1, g_2, \ldots, g_n]$. Questa condizione ci garantisce che è suriettiva l'applicazione $\Phi\colon R_n \to A$ che, per ogni $i = 1, 2, \ldots, n$, manda l'indeterminata X_i nell'elemento $g_i \in A$. Chiaramente, la mappa Φ è per costruzione un omomorfismo di k-algebre. Definiamo ora per semplicità $I := \operatorname{Ker} \Phi$ e applichiamo il primo teorema di isomorfismo, dal quale segue che $R_n/I \cong A$. Per ipotesi, sappiamo che A non ha elementi nilpotenti e dunque anche R_n/I è privo di elementi nilpotenti. Dall'osservazione 1.4 segue quindi che I è un ideale radicale di R_n e allora, se applichiamo il punto (ii) della proposizione 1.5, otteniamo un chiuso $X \subseteq \mathbb{A}_k^n$ tale che $I = \mathcal{I}(X)$. Da questo fatto e dalla proposizione 2.3 segue che $k[X] \cong A$ e la prima parte dell'enunciato è dunque dimostrata. La seconda parte, invece, non è che una conseguenza immediata del punto (iii) della proposizione 2.12 perché, preso un chiuso $Y \subseteq \mathbb{A}_k^m$ tale che $k[Y] \cong A$, in particolare abbiamo $k[Y] \cong k[X]$ e quindi $Y \cong X$. □

Esempio 2.15. In generale, l'intero $n \in \mathbb{N}$ e il chiuso $X \subseteq \mathbb{A}_k^n$ non sono unici. Notiamo infatti che, sebbene il punto (ii) della proposizione 1.5 garantisca esistenza e unicità di un chiuso $X \subseteq \mathbb{A}_k^n$, la scelta degli elementi $g_1, g_2, \ldots, g_n \in A$ all'inizio della dimostrazione non è univoca. In particolare, la k-algebra R_n/I alla quale applichiamo il punto (ii) della proposizione 1.5 non è univocamente determinata. Un controesempio esplicito all'unicità è il seguente: prendiamo $A := k$ e consideriamo due punti $p \in \mathbb{A}_k^n$ e $q \in \mathbb{A}_k^m$, con $n, m \in \mathbb{N}$ interi qualsiasi. Allora $k[p] \cong A \cong k[q]$ per quanto avevamo osservato nell'esempio 2.5.

Lemma 2.16. *Sia A un anello e siano I e J due ideali di A tali che $J \subseteq I$. Se I/J è un ideale radicale di A/J, allora I è un ideale radicale di A.*

Dimostrazione. Sia $a \in \sqrt{I}$ fissato. Per definizione, esiste un intero $s \in \mathbb{N}$ tale che si abbia $a^s \in I$ e quindi, in particolare, abbiamo $(a + J)^s = a^s + J \in I/J$. Ma poiché per ipotesi I/J è un ideale radicale di A/J, si ha anche $a + J \in I/J$ e dunque esiste $x \in I$ tale che $a + J = x + J$. Esiste quindi un elemento $y \in J$ tale che $a - x = y$, ma allora $a = x + y$ e dunque $a \in I$ perché $x \in I$, $y \in J$ e $J \subseteq I$. □

Proposizione 2.17. *Siano $X \subseteq \mathbb{A}_k^n$ e $Y \subseteq \mathbb{A}_k^m$ due chiusi e sia $\phi\colon X \to Y$ un morfismo.*

(i) *Vale che ϕ^* è iniettiva se e solo se ϕ è dominante.*

(ii) *Se k è un campo algebricamente chiuso e ϕ^* è suriettiva, allora ϕ è iniettiva e inoltre $\phi(X) \subseteq Y$ è un chiuso.*

Dimostrazione.

(i) Assumiamo che ϕ^* sia iniettiva e dimostriamo che ϕ è un morfismo dominante, cioè che la chiusura di $\phi(X)$, denotata $\overline{\phi(X)}$, coincide con Y. Basterà dimostrare che $\mathcal{I}(\overline{\phi(X)}) \subseteq \mathcal{I}(Y)$ in quanto l'altra inclusione è banale. Sia dunque $f \in \mathcal{I}(\overline{\phi(X)})$ un polinomio fissato. Allora, per ogni $p \in X$, abbiamo:

$$\phi^*(\phi_f)(p) = (\phi_f \circ \phi)(p) = f(\phi(p)) = 0$$

Sappiamo per ipotesi che ϕ^* è iniettiva e dunque otteniamo che ϕ_f è identicamente nulla su Y, cioè che $f \in \mathcal{I}(Y)$.

Viceversa, se ϕ è dominante, sia ψ una funzione regolare su Y tale che $\phi^*(\psi)$ sia l'applicazione nulla. Per concludere che ϕ^* è iniettiva, ci basterà dimostrare che ψ è identicamente nulla. Innanzitutto, poiché ψ è una funzione regolare su Y, esiste un polinomio $g \in R_m$ tale che $\psi = \phi_g$. Osserviamo che, per ogni $p \in X$, si ha:

$$g(\phi(p)) = \phi_g(\phi(p)) = \phi^*(\psi)(p) = 0$$

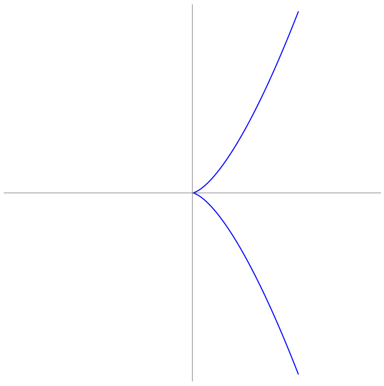
Dunque $\phi(X) \subseteq \mathcal{Z}(g)$. Dall'ipotesi che ϕ sia dominante e dalla definizione di chiusura segue quindi che $Y \subseteq \mathcal{Z}(g)$ e in particolare $g \in \mathcal{I}(Y)$. Con questo concludiamo che $\psi = \phi_g$ è l'applicazione nulla.

(ii) Supponiamo che ϕ^* sia suriettiva e definiamo $I := \operatorname{Ker} \phi^*$. Se ϕ^* è suriettiva, allora $k[Y]/I \cong k[X]$ per il primo teorema di isomorfismo. Per la proposizione 2.3, possiamo pensare I come un ideale della k-algebra $\mathcal{A}_Y = k[Y_1, Y_2, \dots, Y_m]/\mathcal{I}(Y)$ la quale, per il punto (i) della proposizione 1.5, non possiede elementi nilpotenti. In particolare, per l'osservazione 1.4, otteniamo che I è un ideale radicale di $\mathcal{A}_Y$. Per una nota conseguenza[2] del teorema di corrispondenza, abbiamo un ideale I' di $k[Y_1, Y_2, \dots, Y_m]$ contenente $\mathcal{I}(Y)$ tale che $I = I'/\mathcal{I}(Y)$ e inoltre, per il lemma 2.16, un tale ideale I' è anche radicale. Allora, per il teorema degli zeri di Hilbert, esiste un chiuso $W \subseteq \mathbb{A}^m_k$ tale che $I' = \mathcal{I}(W)$. Inoltre, si ha $\mathcal{I}(W) \supseteq \mathcal{I}(Y)$ e quindi $W \subseteq Y$. La proposizione 2.3 e il terzo teorema di isomorfismo forniscono allora gli isomorfismi seguenti:

$$k[W] \cong k[Y_1, Y_2, \dots, Y_m]/I' \cong \big(k[Y_1, Y_2, \dots, Y_m]/\mathcal{I}(Y)\big)/\big(I'/\mathcal{I}(Y)\big) \cong k[Y]/I \cong k[X]$$

Riprendendo le definizioni di questi isomorfismi dalle dimostrazioni dei risultati utilizzati, si verifica assai facilmente che la composizione di tali isomorfismi è semplicemente la restrizione di ϕ^* su $k[W]$. Ma allora, per il punto (iii) della proposizione 2.12, otteniamo che ϕ induce un isomorfismo tra X e $W \subseteq Y$. Dunque $\phi\colon X \to Y$ è iniettiva e $\phi(X) = W$ è un chiuso di Y. □

Il viceversa del punto (ii) della proposizione 2.17 non vale in generale, come dimostra il seguente controesempio.



Esempio 2.18 (Cubica con cuspide)**.** Consideriamo il caso particolare in cui $X := \mathbb{A}^1_{\mathbb{C}}$ e prendiamo $Y := \mathcal{Z}(Y_2^2 - Y_1^3) \subseteq \mathbb{A}^2_{\mathbb{C}}$. Per costruzione, l'applicazione seguente è un morfismo di spazi affini:

$$\begin{aligned} \phi\colon \mathbb{A}^1_{\mathbb{C}} &\longrightarrow Y \\ t &\longmapsto (t^2, t^3) \end{aligned}$$

Inoltre, si vede facilmente che ϕ è ben definita in quanto la sua immagine è effettivamente contenuta in Y. Vediamo adesso che ϕ è iniettiva. Siano dunque $t, s \in \mathbb{A}^1_{\mathbb{C}}$ tali che $t^2 = s^2$ e $t^3 = s^3$. Distinguiamo due casi:

- Se $s = 0$, allora $t = 0$ e dunque $t = s$.
- Se $s \neq 0$, allora da $ts^2 = t^3 = s^3 = ss^2$ segue che $t = s$.

Osserviamo che ϕ è anche suriettiva perché, dato un punto $(a, b) \in Y$, si ha $b^2 = a^3$ e dunque $b = \pm a^{3/2}$. Ma allora, ponendo $t := \pm a^{1/2}$, otteniamo che $\phi(t) = (a, b)$. In particolare, abbiamo che $\phi(X) \subseteq Y$ è un chiuso. D'altra parte, non è suriettivo l'omomorfismo:

$$\begin{aligned} \phi^*\colon \mathbb{C}[Y] &\longrightarrow \mathbb{C}[\mathbb{A}^1_{\mathbb{C}}] \\ \psi &\longmapsto \psi \circ \phi \end{aligned}$$

Prima di dimostrarlo, ricordiamo che $\mathbb{C}[\mathbb{A}^1_{\mathbb{C}}] \cong \mathbb{C}[X_1]$ per quanto già visto nell'esempio 2.4, perciò possiamo identificare $\mathbb{C}[X_1]$ e il codominio di ϕ^* senza perdita di generalità. Si osservi ora che le funzioni regolari su Y associate a polinomi costanti sono mappate nei polinomi costanti e dunque un polinomio in $\mathbb{C}[X_1]$ che non sia nell'immagine di ϕ^* va cercato tra i polinomi non costanti. In effetti, il monomio X_1 non può appartenere

[2] Si veda l'osservazione 7.9 nelle dispense del corso AL210.

all'immagine di ϕ^*, perché altrimenti esisterebbe $\psi \in \mathbb{C}[Y]$ tale che $\phi^*(\psi) = X_1$ e in particolare esisterebbe un polinomio $g \in \mathbb{C}[Y_1, Y_2]$ tale che:

$$g(t^2, t^3) = (\psi \circ \phi)(t) = \phi^*(\psi)(t) = X_1(t) = t$$

Questo contraddice il principio di identità dei polinomi perché t è un polinomio di grado 1, mentre $g(t_2, t_3)$ è un polinomio senza termini di grado 1. Concludiamo dunque che ϕ^* non è suriettiva.

Osservazione 2.19. La discussione precedente ci fornisce anche un esempio di morfismo biiettivo che non è un isomorfismo. Abbiamo infatti dimostrato che ϕ è un morfismo biiettivo e adesso osserviamo che non può essere un isomorfismo perché, se lo fosse, allora anche ϕ^* sarebbe un isomorfismo in virtù del punto (iii) della proposizione 2.12. Ma questo è assurdo perché abbiamo dimostrato che ϕ^* è un omomorfismo non suriettivo.

Geometria algebrica 1 (Matematica, Roma Tre)	Oct 13, 2020

Lezione 8

Raffaele Di Donna

Prodotto di due chiusi affini $X \subseteq \mathbb{A}^n_k$, $Y \subseteq \mathbb{A}^m_k$. L'isomorfismo $k[X \times Y] \cong k[X] \otimes_k k[Y]$.

3 Esempi notevoli

3.1 Prodotti

Definizione 3.1. Siano $n, m \in \mathbb{N}$ interi. Lo spazio affine $\mathbb{A}^{n+m}_k$ è detto il *prodotto di* $\mathbb{A}^n_k$ *e* $\mathbb{A}^m_k$. Introduciamo quindi la notazione $\mathbb{A}^n_k \times \mathbb{A}^m_k := \mathbb{A}^{n+m}_k$.

In generale, la topologia di Zariski su $\mathbb{A}^n_k \times \mathbb{A}^m_k$ non coincide con la topologia prodotto, come dimostra il seguente controesempio.

Esempio 3.2. Consideriamo il caso particolare in cui k è un campo infinito e $n := m := 1$. Consideriamo la diagonale $\Delta := \{(x, x) \in \mathbb{A}^2_k\}$, che è un chiuso nella topologia di Zariski di $\mathbb{A}^2_k$ in quanto $\Delta = \mathcal{Z}(X_1 - X_2)$. Osserviamo che, se Δ fosse un chiuso della topologia prodotto allora, per un noto risultato[3] di topologia, lo spazio affine $\mathbb{A}^1_k$ sarebbe uno spazio di Hausdorff. Ma ciò è assurdo perché, sotto l'ipotesi che k sia un campo infinito, due aperti non vuoti in $\mathbb{A}^1_k$ hanno intersezione non vuota. Perciò Δ non è un chiuso della topologia prodotto.

Osservazione 3.3. Dall'esempio 2.4 segue immediatamente che:

$$k[\mathbb{A}^n_k \times \mathbb{A}^m_k] \cong k[X_1, X_2, \ldots, X_n, Y_1, Y_2, \ldots, Y_m]$$

Chiaramente, se $X \subseteq \mathbb{A}^n_k$ e $Y \subseteq \mathbb{A}^m_k$ sono due chiusi, potremo assegnare al loro prodotto cartesiano, ossia a $X \times Y$, la topologia indotta dalla topologia di Zariski di $\mathbb{A}^n_k \times \mathbb{A}^m_k$. Vedremo che $X \times Y \subseteq \mathbb{A}^n_k \times \mathbb{A}^m_k$ è un chiuso.

Proposizione 3.4. *Siano $X \subseteq \mathbb{A}^n_k$ e $Y \subseteq \mathbb{A}^m_k$ due chiusi e siano $I = \mathcal{I}(X)$ un ideale di $k[X_1, X_2, \ldots, X_n]$, $J = \mathcal{I}(Y)$ un ideale di $k[Y_1, Y_2, \ldots, Y_m]$.*

(i) *Vale che $\mathcal{I}(X \times Y) = (I, J)$, con (I, J) ideale generato da I e J in $k[X_1, X_2, \ldots, X_n, Y_1, Y_2, \ldots, Y_m]$.*

(ii) *Si ha $k[X \times Y] \cong k[X] \otimes_k k[Y]$.*

(iii) *Abbiamo che $X \times Y \subseteq \mathbb{A}^n_k \times \mathbb{A}^m_k$ è un chiuso.*

Per dimostrare questa proposizione, ci sarà utile il seguente risultato preliminare. Prima però ricordiamo che le k-algebre sono in particolare k-spazi vettoriali, quindi ha senso considerare una base di una k-algebra.

Lemma 3.5. *Siano $\{f_s + I\}_{s \in S}$ e $\{g_t + J\}_{t \in T}$ basi delle k-algebre $k[X_1, X_2, \ldots, X_n]/I$, $k[Y_1, Y_2, \ldots, Y_m]/J$ rispettivamente. Per ogni $s \in S$, $t \in T$, sia $\lambda_{st} \in k$ e supponiamo che valga $\lambda_{st} \neq 0$ per al più un numero finito di indici $s \in S$, $t \in T$. Consideriamo inoltre il polinomio $h \in k[X_1, X_2, \ldots, X_n, Y_1, Y_2, \ldots, Y_m]$ definito da:*

$$h = \sum_{s \in S, t \in T} \lambda_{st} f_s g_t$$

Se $h \in \mathcal{I}(X \times Y)$, allora $\lambda_{st} = 0$ per ogni $s \in S$, $t \in T$.

[3] Vedere gli appunti del corso GE220.

Dimostrazione. Supponiamo che $h \in \mathcal{I}(X \times Y)$ e fissiamo un qualunque punto $p \in X$. Allora il polinomio seguente appartiene a $J = \mathcal{I}(Y)$:

$$h(p, Y_1, Y_2, \dots, Y_m) = \sum_{s \in S, t \in T} \lambda_{st} f_s(p) g_t(Y_1, Y_2, \dots, Y_m)$$

Passando alle classi laterali modulo J otteniamo quindi:

$$\sum_{s \in S, t \in T} \lambda_{st} f_s(p) g_t + J = J$$

Equivalentemente, possiamo scrivere:

$$\sum_{t \in T} \Big(\sum_{s \in S} \lambda_{st} f_s(p) \Big) (g_t + J) = J$$

Dall'ipotesi che $\{g_t + J\}_{t \in T}$ sia una base di $k[Y_1, Y_2, \dots, Y_m]/J$ deduciamo allora che, per ogni $t \in T$, si ha:

$$\sum_{s \in S} \lambda_{st} f_s(p) = 0$$

Adesso, per arbitrarietà del punto $p \in X$, il polinomio $\sum_{s \in S} \lambda_{st} f_s$ appartiene a $I = \mathcal{I}(X)$ e dunque, per ogni $t \in T$, abbiamo che:

$$\sum_{s \in S} \lambda_{st} (f_s + I) = I$$

Utilizzando infine l'ipotesi che $\{f_s + I\}_{s \in S}$ sia una base di $k[X_1, X_2, \dots, X_n]/I$, otteniamo che $\lambda_{st} = 0$ per ogni $s \in S$, $t \in T$, cioè la tesi. □

Vediamo ora la dimostrazione della proposizione 3.4.

Dimostrazione. Mostreremo prima un'inclusione dell'uguaglianza al punto (i), poi passeremo a dimostrare il punto (ii), torneremo al punto (i) per stabilire l'altra inclusione e concluderemo dimostrando il punto (iii).

(i,$\supseteq$) Sia $h \in (I, J)$ un polinomio. Per definizione di ideale generato da un sottoinsieme di un anello, che in questo caso è l'unione di I e J in $k[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_m]$, vi sono degli insiemi di polinomi:

- $\{a_s\}_{s \in S}$ e $\{b_t\}_{t \in T}$ in $k[X_1, X_2, \dots, X_n, Y_1, Y_2, \dots, Y_m]$,
- $\{f_s\}_{s \in S}$ in $I \subseteq k[X_1, X_2, \dots, X_n]$,
- $\{g_t\}_{t \in t}$ in $J \subseteq k[Y_1, Y_2, \dots, Y_m]$,

tali che:

$$h = \sum_{s \in S} a_s f_s + \sum_{t \in T} b_t g_t$$

Adesso, preso un qualunque punto $(p, q) \in X \times Y$, dato che per ipotesi $I = \mathcal{I}(X)$, $J = \mathcal{I}(Y)$, si ha:

$$h(p, q) = \sum_{s \in S} a_s(p, q) f_s(p) + \sum_{t \in T} b_t(p, q) g_t(q) = 0$$

E questo dimostra che $h \in \mathcal{I}(X \times Y)$. □

Geometria algebrica 1 (Matematica, Roma Tre) Oct 14, 2020

Lezione 9

Raffaele Di Donna

Polinomi omogenei.

Parte II

Varietà proiettive

Sia k un campo e sia $n \in \mathbb{N}$. Definiamo $S := k[X_0, X_1, \ldots, X_n]$. Preso un intero $d \geq 0$, un polinomio $F \in S$ sarà detto *omogeneo di grado d* se tutti i suoi monomi sono di grado d. In altre parole, al variare degli indici interi $i_0, i_1, \ldots, i_n \geq 0$ tali che $i_0 + i_1 + \cdots + i_n = d$, esistono dei coefficienti $a_{i_0,i_1,\ldots,i_n} \in k$ tali che si abbia:

$$F = \sum_{\substack{i_1,i_2,\ldots,i_n \geq 0 \text{ interi} \\ i_1+i_2+\cdots+i_n=d}} a_{i_0,i_1,\ldots,i_n} X_0^{i_0} X_1^{i_1} \cdots X_n^{i_n}$$

Per ogni intero $d \geq 0$, denotiamo inoltre $S_d := \{F \in S \colon F \text{ è omogeneo di grado } d\}$. Si noti che il polinomio nullo è omogeneo di grado d per un qualsiasi intero $d \geq 0$. Ha dunque senso introdurre la notazione S_d^* per riferirsi all'insieme dei polinomi non nulli in S_d. Ricordiamo poi che S è un k-spazio vettoriale e osserviamo che S_d è un suo sottospazio vettoriale. Una sua base è costituita da tutti i monomi $X_0^{i_0} X_1^{i_1} \cdots X_n^{i_n}$ al variare degli interi $i_0, i_1, \ldots, i_n \geq 0$ tali che $i_0 + i_1 + \cdots + i_n = d$ e il numero di scelte possibili per tali $i_0, i_1, \ldots, i_n$ è dato[4] da:

$$\binom{d+n}{n}$$

Tale intero[5] rappresenta dunque la dimensione del sottospazio vettoriale S_d di S. Ovviamente, i sottospazi vettoriali S_d sono a due a due disgiunti e quindi potremo considerare S come somma diretta delle sue parti omogenee di grado fissato, cioè:

$$S = \bigoplus_{d \geq 0 \text{ intero}} S_d$$

In altre parole, per ogni polinomio $f \in S$, potremo scrivere $f = f_0 + f_1 + \cdots + f_d$ per opportuni polinomi omogenei $f_0, f_1, \ldots, f_d$ di grado $0, 1, \ldots, d$ rispettivamente. Osserviamo anche che, per ogni scelta di interi $d, e \geq 0$, vale l'inclusione $S_d S_e \subseteq S_{d+e}$. Si dice allora che S è un *anello graduato*.

[4] Tale coefficiente binomiale rappresenta il numero di maniere possibili per inserire d palline indistinguibili in $n+1$ buche distinte. Infatti, è del tutto equivalente considerare $n+d$ palline e sceglierne n da identificare come separatori tra le buche.

[5] I coefficienti binomiali sono sempre numeri interi. Per la dimostrazione, si veda la nota 5 nelle dispense del corso TN410.

Geometria algebrica 1 (Matematica, Roma Tre)	Oct 16, 2020
Lezione 10	
Raffaele Di Donna	

Spazio proiettivo n-dimensionale su un campo k: $\mathbb{P}^n_k$. Topologia di Zariski di $\mathbb{P}^n_k$. Chiusi proiettivi, il cono affine su un chiuso proiettivo.

4 Spazi proiettivi

Diversamente dal corso GE210, in cui ci siamo soffermati sulla loro struttura lineare, qui tratteremo gli spazi proiettivi da un punto di vista algebrico, geometrico e topologico. Nel seguito, per ogni $n \in \mathbb{N}$, indicheremo con $\mathbf{0}$ il vettore nullo di k^n. Per semplicità di notazione, poniamo anche $k^* := k \setminus \{0\}$.

Definizione 4.1. Sia k un campo e sia $n \in \mathbb{N}$. Sia $\sim$ la relazione di equivalenza su $k^{n+1} \setminus \{\mathbf{0}\}$ tale che, per ogni $(a_0, a_1, \ldots, a_n), (b_0, b_1, \ldots, b_n) \in k^{n+1} \setminus \{\mathbf{0}\}$, si abbia $(a_0, a_1, \ldots, a_n) \sim (b_0, b_1, \ldots, b_n)$ se esiste $\lambda \in k^*$ tale che $a_i = \lambda b_i$ per $i = 0, 1, \ldots, n$. Si dice allora *n-spazio proiettivo a coefficienti in k* l'insieme quoziente:

$$\mathbb{P}^n_k := (k^{n+1} \setminus \{\mathbf{0}\})/\sim$$

Gli elementi di $\mathbb{P}^n_k$ sono detti *punti*. La classe di equivalenza del punto di coordinate affini $(a_0, a_1, \ldots, a_n)$ in $\mathbb{P}^n_k$ verrà indicata con la notazione $(a_0 : a_1 : \ldots : a_n)$. Per ogni punto $p \in \mathbb{P}^n_k$, gli elementi $a_0, a_1, \ldots, a_n \in k$ tali che $p = (a_0 : a_1 : \ldots : a_n)$ si dicono *coordinate omogenee di p*.

Una prima conseguenza immediata di questa definizione è che le coordinate omogenee di un punto sono determinate a meno di una costante moltiplicativa $\lambda \in k^*$.

Osservazione 4.2. Sia $F \in S$ un polinomio omogeneo di grado $d \geq 0$ e sia $p \in \mathbb{P}^n_k$, $p = (a_0 : a_1 : \ldots : a_n)$ un punto. In generale, la valutazione del polinomio F nel punto p non è ben definita perché, dato un qualunque $\lambda \in k^*$, si ha $p = (\lambda a_0 : \lambda a_1 : \ldots : \lambda a_n)$ mentre:

$$F(\lambda a_0, \lambda a_1, \ldots, \lambda a_n) = \lambda^d F(a_0, a_1, \ldots, a_n)$$

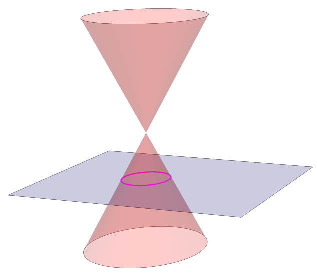
Quindi la valutazione di F in p può dipendere dalla scelta di $\lambda \in k^*$. Tuttavia, la proprietà di essere o meno una radice del polinomio non dipende da λ. Infatti, per l'identità precedente si ha $F(\lambda a_0, \lambda a_1, \ldots, \lambda a_n) = 0$ se e solo se $F(a_0, a_1, \ldots, a_n) = 0$. Ha dunque senso chiedersi se $F(p) = 0$.

L'osservazione precedente permette di definire, come nel caso affine, i sottoinsiemi di $\mathbb{P}^n_k$ su cui si annulla una data collezione di polinomi omogenei.

Definizione 4.3. Sia $T \subseteq S$ un sottoinsieme costituito da soli polinomi omogenei (ma non necessariamente dello stesso grado). Definiamo:

$$\mathcal{V}(T) := \{p \in \mathbb{P}^n_k \colon F(p) = 0 \text{ per ogni } F \in T\}$$

Osservazione 4.4. Si dimostra, esattamente come fatto nel caso affine, che i sottoinsiemi $\mathcal{V}(T)$ di $\mathbb{P}^n_k$ sono i chiusi di una topologia, detta *topologia di Zariski di* $\mathbb{P}^n_k$. Tali chiusi si diranno, in analogia con il caso affine, *chiusi proiettivi di* $\mathbb{P}^n_k$, mentre gli aperti corrispondenti verranno chiamati *aperti proiettivi di* $\mathbb{P}^n_k$.



A questo punto è piuttosto naturale domandarsi che relazione ci sia tra la topologia di Zariski affine e quella proiettiva. Consideriamo allora la mappa quoziente rispetto alla relazione di equivalenza $\sim$, vale a dire l'applicazione:

$$\begin{aligned} \sigma\colon \mathbb{A}_k^{n+1} \setminus \{\mathbf{0}\} &\longrightarrow \mathbb{P}_k^n \\ (a_0, a_1, \ldots, a_n) &\longmapsto (a_0 : a_1 : \ldots : a_n) \end{aligned}$$

Geometricamente, l'immagine inversa tramite σ di un chiuso di $\mathbb{P}_k^n$ è un cono in $\mathbb{A}_k^{n+1} \setminus \{\mathbf{0}\}$ perché la fibra di un punto in $\mathbb{P}_k^n$ è una retta di $\mathbb{A}_k^{n+1}$ che passa per l'origine, escludendo tuttavia l'origine stessa. Si ha il seguente risultato.

Osservazione 4.5. Sia $T \subseteq S$ un sottoinsieme di polinomi omogenei tale che $T \cap k^* = \varnothing$, cioè non contenente polinomi costanti non nulli. Allora $\mathcal{Z}(T) = \sigma^{-1}(\mathcal{V}(T)) \cup \{\mathbf{0}\}$.

Dimostrazione. Osserviamo, innanzitutto, che $\mathbf{0} \in \mathcal{Z}(T)$. Infatti, per ogni $F \in T$, abbiamo due possibilità:

- Se F è il polinomio nullo, allora $F(\mathbf{0}) = 0$ banalmente.
- Se invece F è un polinomio non nullo, allora F è non costante per ipotesi e di conseguenza $\deg F \geq 1$. Dall'ipotesi che F sia un polinomio omogeneo segue quindi che $F(\mathbf{0}) = 0$.

Sia ora $q \in \mathbb{A}_k^{n+1}$ un punto fissato e assumiamo che valga $q \neq \mathbf{0}$. Si osservi che, in vista dell'osservazione 4.2, per ogni polinomio $F \in T$ si ha $F(q) = 0$ se e solo se $F(\sigma(q)) = 0$. Abbiamo allora le seguenti equivalenze:

$$\begin{aligned} & q \in \sigma^{-1}(\mathcal{V}(T)) \\ \iff & \sigma(q) \in \mathcal{V}(T) \\ \iff & F(\sigma(q)) = 0 \,\text{per ogni}\, F \in T \\ \iff & F(q) = 0 \,\text{per ogni}\, F \in T \\ \iff & q \in \mathcal{Z}(T) \end{aligned}$$

□

Definizione 4.6. Sia $T \subseteq S$ un sottoinsieme di polinomi omogenei tale che $T \cap k^* = \varnothing$. Diremo che $\mathcal{Z}(T)$ è il *cono affine su* $\mathcal{V}(T)$.