

Polinomi e serie formali

§ Costruzione dei polinomi in una indeterminata

Definizione 6.1. Sia A un anello, allora l'anello dei polinomi $A[X]$ è l'insieme delle successioni quasi nulle ad elementi in A (ossia delle funzioni $f: \mathbb{N} \rightarrow A$ tali che $f(n) = 0$ per ogni $n \geq n_0$ per un certo n_0 dipendente da f), con le operazioni definite come segue: $\forall f, g \in A[X]$ e $\forall n \in \mathbb{N}$

$$(f + g)(n) = f(n) + g(n)$$

$$(fg)(n) = \sum_{i=0}^n f(i)g(n-i)$$

(il prodotto definito come sopra è anche detto prodotto di convoluzione).

Osservazione 6.2. Vi sono in $A[X]$ degli elementi particolari:

- i **polinomi costanti** definiti come ($\forall a \in A$)

$$f_a: \mathbb{N} \rightarrow A \quad f_a(n) = \delta_{0n}a$$

- e l'**indeterminata** X definita come

$$f_X: \mathbb{N} \rightarrow A \quad f_X(n) = \delta_{1n}$$

dove δ_{ij} vale 1 se $i = j$ e vale 0 se $i \neq j$ (delta di Kronecker).

Possiamo identificare canonicamente A col sottoanello di $A[X]$ formato dai **polinomi costanti**, ossia possiamo considerare come fossero la stessa cosa un elemento $a \in A$ e il polinomio costante $f_a \in A[X]$.

L'identificazione è lecita poiché l'applicazione $\phi: A \rightarrow A[X]$ data da $\phi(a) = f_a$ è un monomorfismo di anelli e quindi un isomorfismo tra A e l'immagine di ϕ . Nel seguito scriveremo quindi semplicemente a sia per indicare l'elemento di A sia per indicare il polinomio costante $f_a \in A[X]$. Possiamo ottenere ogni elemento f di $A[X]$ come

combinazione lineare di potenze di X con coefficienti in A ; si verifica infatti che come funzioni da \mathbb{N} in A un polinomio f coincide con $f_{a_0} + f_{a_1}f_X + f_{a_2}f_X^2 + \cdots + f_{a_n}f_X^n$ e che questa scrittura è unica. Utilizzando la suddetta identificazione tra elementi di A e polinomi costanti, ogni polinomio $f \in A[X]$ potrà essere indicato mediante la scrittura formale $a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ dove $a_i = f(i)$ se $0 \leq i \leq n$ e $f(i) = 0$ per ogni $i > n$. Il simbolo X che abbiamo usato per la successione speciale $(0, 1, 0, 0, \dots, 0, \dots)$ può essere così pensato anche semplicemente come un “segnaposto”. Questa convenzione risulta particolarmente comoda poiché la somma e il prodotto di polinomi possono essere ottenuti a partire da queste scritture formali mediante le abituali regole del calcolo algebrico.

Nel seguito useremo di solito lettere maiuscole per indicare i polinomi, spesso seguite dal nome dell’indeterminata, ossia indicheremo un polinomio in $A[X]$ con F oppure con $F(X)$.

Definizione 6.3. La **valutazione di un polinomio** $F(X) \in A[X]$ in un **elemento** x_0 di A si ottiene sostituendo formalmente all’indeterminata X l’elemento x_0 nell’espressione formale di $F(X) = a_0 + a_1X_0 + \cdots + a_nX_0^n$, ossia la valutazione di $F(X)$ in x_0 è data da

$$F(x_0) = a_0 + a_1x_0 + \cdots + a_nx_0^n.$$

Osservazione 6.4. La valutazione del polinomio nullo in ogni $x_0 \in A$ è 0. D’altra parte può capitare che un polinomio non nullo abbia valutazione 0 in ogni elemento $x_0 \in A$. Per esempio se l’anello A ha solo un numero finito di elementi, $A = \{a_1, \dots, a_n\}$, allora il polinomio non nullo $F(X) = (X - a_1) \cdots (X - a_n)$ ha valutazione 0 in ogni $a_i \in A$.

Definizione 6.5. Ad ogni polinomio $F \in A[X]$ possiamo associare una funzione $\bar{F}: A \rightarrow A$ che associa ad ogni $a \in A$ la valutazione $F(a)$ di $F(X)$ in a . Le funzioni così ottenute si dicono **funzioni polinomiali**.

Osservazione 6.6. Le funzioni polinomiali con le usuali operazioni di somma e prodotto “punto per punto” formano un anello che indichiamo con $\mathcal{F}A[X]$. L’applicazione canonica che associa ad ogni polinomio di $A[X]$ la corrispondente funzione polinomiale è un omomorfismo di anelli. Poiché tale omomorfismo è chiaramente suriettivo, grazie al I Teorema di Isomorfismo $\mathcal{F}A[X]$ è isomorfo al quoziente $A[X]/J$ dove J è il nucleo dell’epimorfismo canonico considerato.

Nei corsi di algebra di base si prova che se A è un campo infinito allora $J = (0)$ e quindi polinomi e funzioni polinomiali si possono considerare come concetti equivalenti (**Principio di identità dei polinomi**). In generale invece $J \neq (0)$ e quindi $A[X]$ e $\mathcal{F}A[X]$ non sono isomorfi.

§ Costruzione delle serie formali

Definizione 6.7. Sia A un anello. Indichiamo con $A[[X]]$ l'anello delle serie formali a coefficienti in A i cui elementi sono tutte le successioni (qualsiasi) di elementi di A con le operazioni di somma e prodotto definite in modo del tutto identico a quanto fatto per i polinomi: $\forall f, g \in A[[X]]$ e $\forall n \in \mathbb{N}$

$$(f + g)(n) = f(n) + g(n)$$

$$(fg)(n) = \sum_{i=0}^n f(i)g(n-i).$$

Osservazione 6.8. Risulta evidente da questa definizione che $A[X] \subset A[[X]]$ ed anzi $A[X]$ è sottoanello di $A[[X]]$; si può quindi dire che anche A è un sottoanello di $A[[X]]$. Inoltre anche in $A[[X]]$ vi è l'elemento speciale denotato X . In modo analogo a quanto fatto per i polinomi, potremo scrivere ogni serie formale in modo unico come: $a_0 + a_1X + a_2X^2 + \dots + a_nX^n + \dots$ (somma formale di infiniti termini). Si noti però che vi è una sostanziale differenza tra i due casi. Mentre per i polinomi, $A[X]$ è effettivamente il sottoanello di se stesso generato da A e da X , nel caso delle serie formali in genere non è possibile ottenere una serie mediante le costanti, la X e un numero finito di operazioni di somma e prodotto. La scrittura $a_0 + a_1X + a_2X^2 + \dots$ deve essere quindi intesa solo come scrittura formale con X nel ruolo di segnaposto. Inoltre, poiché non si richiede alle serie alcuna proprietà di convergenza, non si può estendere all'anello delle serie formali la nozione di valutazione in un elemento dell'anello o di funzione associata.

§ Elementi algebrici e trascendenti

Siano A un anello e B un suo sottoanello. Se x è un elemento di A , ricordiamo che il sottoanello di A generato da B e da x , ossia il minimo sottoanello di A che contiene $B \cup \{x\}$, è:

$$B[x] = \{a_0 + a_1x + \dots + a_nx^n \mid a_i \in B, n \in \mathbb{N}\}$$

(si veda Proposizione ??).

Definizione 6.9. Siano A, B ed x come sopra. Si dice che x è **trascendente su** B se due elementi $a_0 + a_1x + \dots + a_nx^n$ e $b_0 + b_1x + \dots + b_nx^n$ di $B[x]$ coincidono se e soltanto se $a_i = b_i$ per ogni $i = 1, \dots, n$, oppure, equivalentemente, se $a_0 + a_1x + \dots + a_nx^n = 0$ in $B[x]$ se e solo se $a_i = 0$ per $i = 1, \dots, n$.

Si dice che x è **algebrico su** B se x non è trascendente su B , ossia se esistono elementi $a_0, \dots, a_n \in B$ non tutti nulli tali che $a_0 + a_1x + \dots + a_nx^n = 0$.

Esempio 6.10. Siano $A = \mathbb{C}$ e $B = \mathbb{Z}$. I numeri complessi $x_1 = \frac{1}{2}$, $x_2 = \sqrt{2}$ e $x_3 = i$ sono algebrici su \mathbb{Z} , si ha infatti $1 - 2x_1 = 0$, $2 - x_2^2 = 0$ e $1 + x_3^2 = 0$. Invece π è trascendente su \mathbb{Z} .

Osservazione 6.11. Il fatto che un elemento $a \in A$ sia algebrico oppure trascendente dipende fortemente dal sottoanello B di A considerato. Ad esempio πi è trascendente su \mathbb{Z} , ma è algebrico sul sottoanello \mathbb{R} di \mathbb{C} . Più in generale ogni elemento di A risulta essere algebrico sul sottoanello banale A .

Esempio 6.12. L'indeterminata X di $A[X]$ (ossia la funzione $f_X(1) = 1$ e $f_X(n) = 0$ per ogni $n \neq 1$) è trascendente su A . Infatti una combinazione lineare $f = a_0 + a_1X + \dots + a_nX^n$ con $a_i \in A$ è lo zero di $A[X]$, ossia è la funzione nulla, se f è la funzione che associa ad ogni naturale lo zero di A ; ora si ha $f(0) = a_0$, $f(1) = a_1, \dots, f(n) = a_n$ e quindi si tratta della funzione nulla se e soltanto se tutti gli a_i sono nulli.

L'indeterminata X risulta essere trascendente su A anche se pensata come elemento dell'anello delle serie formali $A[[X]]$.

Possiamo condensare il significato del risultato seguente dicendo che “le indeterminate sono tutte uguali”.

Teorema 6.13. *Sia $\varphi: R \rightarrow S$ un omomorfismo di anelli e sia $s \in S$. Esiste allora un unico omomorfismo di anelli $\tilde{\varphi}: R[X] \rightarrow S$ tale che $\tilde{\varphi}(a) = \varphi(a)$ per ogni $a \in R$ e $\tilde{\varphi}(X) = s$.*

Dimostrazione. Definiamo intanto $\tilde{\varphi}$ su ogni elemento di $R[X]$:

$$\tilde{\varphi}(a_0 + \dots + a_nX^n) = \tilde{\varphi}(a_0) + \dots + \tilde{\varphi}(a_n)\tilde{\varphi}(X)^n = \varphi(a_0) + \dots + \varphi(a_n)s^n.$$

Si tratta effettivamente di una funzione (ossia è ben definita) grazie all'unicità della scrittura dei polinomi. Inoltre, l'applicazione così definita rispetta per costruzione la somma e il prodotto e, d'altra parte, è anche l'unica applicazione possibile che rispetta la somma, il prodotto e le richieste iniziali. ■

Corollario 6.14. *Siano A un anello, B un suo sottoanello e $\iota: B \rightarrow A$ l'applicazione che manda ogni elemento di B in se stesso (l'immersione di B in A).*

Un elemento $x \in A$ è trascendente su B se e soltanto se l'applicazione $\tilde{\iota}: B[X] \rightarrow A$ tale che $\tilde{\iota}|_B = \iota$ e $\tilde{\iota}(X) = x$ è un monomorfismo di anelli.

In particolare x è trascendente su B se e solo se l'anello di polinomi $B[X]$ e l'estensione $B[x]$ di B con x sono isomorfi.

Dimostrazione. Sia I il nucleo dell'applicazione $\tilde{\iota}$. Per il I Teorema di Isomorfismo si ha un isomorfismo naturale tra $B[x]$ e $B[X]/I$. Quindi $B[x]$ e $B[X]$ sono isomorfi se

e soltanto se $I = (0)$. Ora un polinomio $F(X) = a_0 + a_1X + \cdots + a_nX^n$ appartiene a I se e solo se la sua valutazione $F(x)$ in x si annulla ossia se e soltanto se $F(x) = a_0 + a_1x + \cdots + a_nx^n = 0$. ■

Corollario 6.15. *Sia B un sottoanello di A e siano x ed y due elementi dell'anello A trascendenti su B . Allora vi è un unico isomorfismo*

$$\phi: B[x] \rightarrow B[y]$$

tale che $\phi(b) = b$ per ogni $b \in B$ e $\phi(x) = y$. Quindi le estensioni $B[x]$ e $B[y]$ sono isomorfe in modo naturale.

Osservazione 6.16. Si noti che se B è un sottoanello di un anello A e se $x, y \in A$ sono due elementi trascendenti su B , non è detto che y sia trascendente su $B[x]$, anche escludendo il caso banale in cui $y \in B[x]$.

Esempio 6.17. I numeri reali π e $\sqrt{2}\pi$ sono entrambi trascendenti su \mathbb{Q} e inoltre $\sqrt{2}\pi \notin \mathbb{Q}[\pi]$, ma $\sqrt{2}\pi$ è algebrico su $\mathbb{Q}[\pi]$.

Definizione 6.18. Siano A un anello e $B = A[X]$ l'anello dei polinomi a coefficienti in A . Possiamo iterare il procedimento di costruzione dei polinomi partendo dall'anello B . Utilizziamo un nome diverso per la nuova indeterminata poiché come funzione differisce (ad esempio per il codominio) dall'indeterminata X : si ottiene così l'anello $B[Y] = A[X][Y]$.

Corollario 6.19. *Nelle ipotesi precedenti, esiste un (unico) isomorfismo di anelli $\psi: A[X][Y] \rightarrow A[X][Y]$ tale che $\psi(a) = a$ per ogni $a \in A$, $\psi(X) = Y$ e $\psi(Y) = X$.*

Dimostrazione. Posto $S = A[X][Y]$, sia $i: A \rightarrow S$ l'immersione naturale. La costruzione del Teorema 6.13 con $R = A$ ed $s = Y$ fornisce l'unico omomorfismo $\phi = \tilde{i}: A[X] \rightarrow S$ tale che $\phi(a) = a$ per ogni $a \in A$ e $\phi(X) = Y$. Poiché Y è trascendente su $A[X]$ e quindi, a maggior ragione su A , dal Corollario 6.14 segue che ϕ è un monomorfismo.

Ripetendo il ragionamento con $R = A[X]$ e l'elemento $s = X$ si ottiene poi il monomorfismo $\psi = \tilde{\phi}: R[Y] = A[X][Y] \rightarrow A[X][Y]$ tale che $\psi(a) = a$ per ogni $a \in A$, $\psi(X) = Y$ e $\psi(Y) = X$. Si verifica poi facilmente che ψ è anche suriettiva e quindi è un isomorfismo. ■

Osservazione 6.20. Si può verificare (con verifiche lunghe e non particolarmente significative) che ogni polinomio di $A[X, Y] = A[X][Y]$ si può scrivere in modo unico come:

$$\sum_{(i,j) \in E} a_{ij} X^i Y^j$$

dove E è un sottoinsieme **finito** di $\mathbb{N} \times \mathbb{N}$ e $a_{ij} \in A$ e che ogni espressione di questo tipo rappresenta un polinomio nelle indeterminate X ed Y a coefficienti in A .

Iterando il procedimento si possono costruire anelli di polinomi in un numero finito di indeterminate a coefficienti in A che indicheremo con

$$A[X_1, X_2, \dots, X_n].$$

I suoi elementi sono tutte e sole le espressioni del tipo:

$$\sum_{(i_1, \dots, i_n) \in E} a_{i_1 \dots i_n} X_1^{i_1} \cdots X_n^{i_n}$$

con E sottoinsieme finito del prodotto cartesiano di n copie di \mathbb{N} . Vedremo in seguito una notazione più sintetica per questi polinomi. Grazie al precedente risultato potremo semplicemente scrivere $A[X, Y]$ o, più in generale, $A[X_1, X_2, \dots, X_n]$ senza preoccuparci dell'ordine delle indeterminate.

Attenzione: Relativamente all'anello $A[X][Y] = A[X, Y]$ è necessario specificare di volta in volta se lo si considera come anello dei polinomi nelle indeterminate X e Y a coefficienti in A oppure come anello dei polinomi nell'indeterminata Y a coefficienti in $A[X]$. Senza questa precisazione potrebbero sorgere ambiguità ad esempio sul significato da attribuire al termine "costanti". Useremo preferibilmente la scrittura $A[X, Y]$ quando vorremo considerare come costanti solo gli elementi di A e la scrittura $A[X][Y]$ se vorremo considerare come costanti tutti gli elementi di $A[X]$.

§ Invertibili, zero-divisori, nilpotenti in $A[X]$

Ricordiamo ora alcune notazioni e terminologie probabilmente ben note.

Definizione 6.21. Sia $F = a_0 + a_1X + \dots + a_nX^n$ un polinomio non nullo di $A[X]$.

- i) Il **termine noto** di F è a_0 ; se F è un polinomio costante, esso coincide col suo termine noto.
- ii) Il **grado** di F è il massimo $m \in \mathbb{N}$ tale che $a_m \neq 0$. Si ha ovviamente $m \leq n$ perchè i termini omissi nella scrittura sono tutti nulli; la scrittura "più breve" di F è quella in cui si ha proprio $m = n$ e in genere (ma non necessariamente) è quella utilizzata. Indicheremo il grado di F con $\partial(F)$. Non si attribuisce alcun grado al polinomio nullo.
- iii) Il **coefficiente direttivo** o **coefficiente direttore** di F è la costante a_m dove $m = \partial(F)$, ossia tra tutti i coefficienti non nulli che compaiono in F è quello della massima potenza di X .

- iv) I **polinomi monici** sono i polinomi con coefficiente direttivo $a_m = 1$.
- v) I **termini** sono tutti i polinomi che hanno un solo coefficiente non nullo, ossia quelli del tipo aX^m .
- vi) I **monomi** sono i termini monici, ossia i polinomi del tipo X^m .

Possiamo allora dire che ogni polinomio è somma di un numero finito di termini oppure che è combinazione di un numero finito di monomi con coefficienti in A .

Possiamo utilizzare la locuzione termine noto anche per le serie formali, con ovvio significato, mentre non ha senso parlare di grado o di coefficiente direttivo di una serie formale.

Osserviamo che se $F, G \in A[X]$ sono polinomi con termine noto rispettivamente a_0 e b_0 , allora $F + G$ e FG hanno termine noto rispettivamente $a_0 + b_0$ e a_0b_0 (segue immediatamente dalle definizioni di somma e prodotto di polinomi). Meno semplici sono le relazioni con le operazioni per quel che riguarda il grado e il coefficiente direttivo.

Proposizione 6.22. *Siano A un anello e $F = a_0 + \dots + a_nX^n$, $G = b_0 + \dots + b_mX^m$ polinomi di $A[X]$ di grado n ed m rispettivamente. Allora:*

1. $\partial(F + G) \leq \max\{\partial(F), \partial(G)\}$ e vale '=' ogni volta che $\partial(F) \neq \partial(G)$.
2. $\partial(FG) \leq \partial(F) + \partial(G)$ e vale '=' ogni volta che A è un dominio oppure almeno uno tra F e G è monico.
3. Se $\partial(FG) = \partial(F) + \partial(G)$ il coefficiente direttivo di FG è a_nb_m .

Proposizione 6.23. *Sia A un anello e sia $F = a_0 + \dots + a_nX^n$ un polinomio di $A[X]$ di grado n . Allora:*

1. F è un elemento nilpotente di $A[X]$ se e solo se tutti i suoi coefficienti sono nilpotenti in A .
2. F è invertibile in $A[X]$ se e soltanto se a_0 è invertibile in A e a_i è nilpotente per ogni $i \geq 1$.
3. F è uno zero-divisore in $A[X]$ se e soltanto se esiste $b \in A$, $b \neq 0$, tale che $Fb = 0$ ossia $a_ib = 0$ per ogni $i \geq 0$.

Dimostrazione. Osserviamo innanzi tutto che le costanti sono invertibili, zero-divisori, nilpotenti come elementi di $A[X]$ se e solo se lo sono come elementi di A .

1. Se ogni coefficiente di F è nilpotente, sono allora nilpotenti tutti i termini di cui F è somma e quindi F , come somma di un numero finito di nilpotenti, è nilpotente esso stesso.

Per provare l'implicazione inversa procediamo per induzione sul grado di F . Se F ha grado 0, allora F è costante e l'asserto è vero. Supponiamo l'asserto vero per tutti i polinomi di grado $< n$ e proviamolo per F di grado n . Per ipotesi esiste un intero positivo k tale che $F^k = 0$. Il termine di grado kn in F^k è $a_n^k X^{nk}$; poiché F^k è il polinomio nullo, in particolare $a_n^k = 0$ e quindi a_n è nilpotente. Ora, il polinomio $G = F - a_n X^n = a_0 + \dots + a_{n-1} X^{n-1}$ ha grado $< n$ ed è nilpotente in quanto è somma di due nilpotenti. Si conclude allora che tutti gli a_i con $i = 0, \dots, n-1$ sono nilpotenti grazie all'ipotesi induttiva.

2. Se a_0 è invertibile e a_1, \dots, a_n sono nilpotenti, allora $a_1 X + \dots + a_n X^n$ è nilpotente per quanto visto al punto precedente. Il polinomio F è allora invertibile perché somma di un invertibile e di un nilpotente.

Supponiamo, viceversa, che F sia invertibile in $A[X]$ ossia che esista un polinomio $G = b_0 + \dots + b_m X^m$ tale che $FG = 1_{A[X]} = 1_A = 1$. Confrontando i termini noti nell'uguaglianza tra polinomi $FG = 1$ si ottiene $a_0 b_0 = 1$ e quindi a_0 è invertibile. Rimane da provare che tutti gli altri coefficienti in F sono nilpotenti. Moltiplicando per l'inverso di a_0 possiamo supporre senza perdere in generalità che F abbia termine noto 1 (e quindi che anche G abbia termine noto 1).

Procediamo per induzione sul grado di F .

Se $\partial(F) = 0$, non c'è nulla da provare. Supponiamo l'asserto vero per i polinomi di grado $< n$ e proviamolo per F di grado n .

Mediante un procedimento per discesa su i possiamo vedere che per ogni $i = m, \dots, 0$ esiste sempre un qualche esponente k tale che $a_n^k b_i = 0$.

Per $i = m$, basta considerare il coefficiente $a_n b_m = 0$ di X^{n+m} in FG .

Supponiamo che per ogni $i > i_0$ si abbia $a_n^h b_i = 0$. Calcolando il coefficiente di X^{n+i_0} in FG otteniamo $a_n b_{i_0} + \sum_{i>i_0} a_{n+i_0-i} b_i = 0$; moltiplicando i due membri per a_n^h otteniamo $a_n^{h+1} b_{i_0} = 0$ come volevasi.

Poiché $b_0 = 1$, allora $a_n^k = 0$ per un qualche k , e quindi il coefficiente direttivo di F è nilpotente. Il polinomio $F' = F - a_n X^n$ è allora nilpotente (in quanto somma di due nilpotenti), ha grado $< n$ e ha gli stessi coefficienti di F di grado $< n$; per l'ipotesi induttiva anche gli altri coefficienti di F di grado ≥ 1 sono nilpotenti. 3.

Sia $F = a_0 + a_1 X + \dots + a_n X^n$ uno zero-divisore e sia $G = b_0 + \dots + b_m X^m$ un polinomio non nullo di grado minimo tale che $FG = 0$. Proviamo che si ha $a_i b_j = 0$ per ogni $i \leq n$ e $j \leq m$.

Se così non fosse esisterebbe un minimo i , sia h , tale che $a_h G \neq 0$ e quindi un minimo j , sia k , tale che $a_h b_k \neq 0$. Osserviamo che $k \neq m$, perché il coefficiente del monomio di grado $h+m$ in FG è $a_h b_m$, grazie alle ipotesi fatte sulla minimalità di h , e quindi $a_h b_m = 0$. In tal caso però il polinomio non nullo $G' = a_h G$ avrebbe grado strettamente minore di m e inoltre si avrebbe $FG' = a_h(FG) = 0$, in contrasto con la minimalità del grado di G .

Allora $Fb_m = 0$ e quindi $a_i b_m = 0$ per ogni $i \leq n$, come volevasi. ■

Corollario 6.24. *Siano A un anello qualsiasi e $A[X]$ l'anello dei polinomi in una*

indeterminata a coefficienti in A .

1. L'indeterminata X non è un elemento invertibile e quindi $A[X]$ non è in alcun caso un campo.
2. A è un dominio di integrità se e soltanto se $A[X]$ è un dominio di integrità.
3. L'indeterminata X non è zero-divisore in $A[X]$.
4. Se $A = k$ è un campo, allora $k[X]$ è un dominio di integrità, ma non è un campo.

Corollario 6.25. *Siano A un anello qualsiasi e $A[X]$ l'anello dei polinomi in una indeterminata a coefficienti in A . Allora gli elementi del tipo $X - a$, con $a \in A$ e, più in generale, i polinomi monici di grado > 0 , non sono nè elementi invertibili nè zero-divisori e quindi $A[X]$ non è un anello locale.*

Dimostrazione. Che i polinomi monici non siano mai nè invertibili nè zero-divisori segue immediatamente dalla caratterizzazione di tali elementi in $A[X]$.

Per provare l'ultima affermazione dell'enunciato, consideriamo ad esempio i polinomi monici X e $X - 1$; sappiamo allora che esistono degli ideali massimali \mathcal{M}_1 e \mathcal{M}_2 in $A[X]$ tali che $X \in \mathcal{M}_1$ e $X - 1 \in \mathcal{M}_2$. Tali ideali massimali non possono coincidere perché nessun ideale proprio può contenere $1 = X - (X - 1)$ e quindi $A[X]$ possiede almeno due ideali massimali distinti. ■

La caratterizzazione degli elementi invertibili, nilpotenti, zero-divisori vista per $A[X]$ si estende immediatamente all'anello dei polinomi $A[X_1, \dots, X_n]$ in n indeterminate. Si ottiene una semplice dimostrazione di questo fatto procedendo per induzione su n e considerando $A[X_1, \dots, X_n] = B[X_n]$ dove $B = A[X_1, \dots, X_{n-1}]$.

Definizione 6.26. Sia $F = a_0 + \dots + a_n X^n$ un polinomio non nullo di $A[X]$. Si dice che F è **primitivo** se $(a_0, \dots, a_n) = (1)$.

Proposizione 6.27. *Siano $F, G \in A[X]$. Allora:*

FG è primitivo se e soltanto se F e G sono entrambi primitivi.

Dimostrazione. Una implicazione è molto semplice: se F (oppure G) non è primitivo, allora neppure FG può esserlo poichè i coefficienti di FG sono combinazioni lineari dei coefficienti di F e dei coefficienti di G .

Per provare l'implicazione inversa, supponiamo che FG non sia primitivo e indichiamo con \mathfrak{m} un massimale di A che contiene tutti i coefficienti di FG . Passando al quoziente modulo \mathfrak{m} , possiamo far corrispondere a F e G dei polinomi \overline{F} e \overline{G} in $k[X]$, dove k è il campo A/\mathfrak{m} . Poichè $\overline{F} \cdot \overline{G} = 0$ in $k[X]$ che è un dominio, allora $\overline{F} = 0$ (oppure $\overline{G} = 0$) e quindi tutti i coefficienti di F (o di G) appartengono a \mathfrak{m} .

Proposizione 6.28. *Sia A un anello e sia $F = a_0 + \cdots + a_n X^n + \cdots$ una serie formale di $A[[X]]$. Allora:*

1. F è invertibile in $A[[X]]$ se e soltanto se a_0 è invertibile in A ;
2. se F è uno zero-divisore in $A[[X]]$ e $a_i = 0$ per ogni $i < i_0$, allora a_{i_0} è uno zero-divisore in A ;
3. X non è nè invertibile nè zero-divisore in $A[[X]]$;
4. se F è un elemento nilpotente di $A[[X]]$, allora tutti i suoi coefficienti sono elementi nilpotenti in A .

Dimostrazione. 1. Se $FG = 1$, allora in particolare $a_0 b_0 = 1$ e quindi a_0 è invertibile. Proviamo allora l'implicazione non banale, ossia che a_0 invertibile in A è sufficiente ad assicurare che F sia invertibile in $A[[X]]$. Costruiamo esplicitamente i coefficienti della serie $G = b_0 + b_1 X + \cdots + b_n X^n + \cdots$ tale che $FG = 1$, procedendo per induzione su n . Per $n = 0$, $b_0 = a_0^{-1}$ in A . Sia ora $n > 0$ e supponiamo di aver costruito oltre b_0 anche b_1, \dots, b_{n-1} tali che per ogni $0 < i \leq n-1$ si abbia $\sum_{j=0}^i a_j b_{i-j} = 0$. L'unico elemento b_n che soddisfa la stessa relazione per $j = n$ è allora

$$b_n = a_0^{-1} \left(- \sum_{j=1}^n a_j b_{n-j} \right) = -b_0 \left(\sum_{j=1}^n a_j b_{n-j} \right).$$

Le affermazioni 2. e 3. seguono immediatamente dai punti precedenti e dalla definizione di prodotto tra serie formali.

4. Supponiamo che risulti $F^k = 0$ per un certo $k \in \mathbb{N}$ e proviamo per induzione su n che tutti i coefficienti di F sono elementi nilpotenti di A .

Per $n = 0$: il termine noto di F^k è a_0^k e quindi $a_0^k = 0$ in A .

Supponiamo di aver provato che a_i sia nilpotente in A per ogni $i \leq n-1$ e proviamo che anche a_n lo è. Per quanto visto in precedenza il polinomio $G = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$ è nilpotente e quindi lo è anche come serie formale; allora $F - G$ è nilpotente in quanto somma di due nilpotenti. Poiché $F - G = a_n X^n + \cdots$ possiamo scrivere $F - G$ come $X^n H$ dove $H = a_n + a_{n+1} X + \cdots$ è nilpotente essendo X un elemento che non è zero-divisore. Per quanto visto nel passo iniziale, a_n è allora nilpotente. ■

Attenzione: Vi sono serie formali che non sono nilpotenti, anche se tutti i coefficienti lo sono. Gli esempi di questo tipo sono però un po' complicati da costruire.

Corollario 6.29. *Se k è un campo, allora $k[[X]]$ è un anello locale il cui unico ideale massimale è $\mathfrak{m} = (X)$ ossia l'ideale costituito da tutte le serie a termine noto nullo.*

L'esempio seguente introduce uno dei concetti centrali della nostra trattazione della teoria degli anelli di polinomi e sarà ripreso ampiamente in seguito.

Esempio 6.30. Sia $R = k[X_1, \dots, X_n]$ l'anello di polinomi a coefficienti in un campo k . Possiamo pensare R come somma diretta di k -spazi vettoriali $R = \bigoplus_{i=0}^{\infty} R_i$ dove R_i è costituito dallo 0 e da tutti i **polinomi omogenei** di grado i , ossia è il sottospazio vettoriale generato dai monomi di grado i . Vedremo in seguito come una analoga decomposizione si ha anche per alcuni ideali I di R oppure per alcuni quozienti R/I . A una tale decomposizione si può associare una **funzione intera**

$$f: \mathbb{N} \longrightarrow \mathbb{N} \quad \text{data da} \quad f(i) = \dim_k R_i.$$

Se consideriamo come codominio non \mathbb{N} ma \mathbb{Z} , che è un anello, la funzione intera f non è altro che una serie formale:

$$f = f(0) + f(1)z + \dots + f(i)z^i + \dots = \sum_{i=0}^{\infty} f(i)z^i \in \mathbb{Z}[[z]].$$

Nel caso $n = 1$ ossia $R = k[X]$, si ha $R_i = X^i k$ e quindi $f(i) = 1$ per ogni $i \in \mathbb{N}$. Si ottiene così la serie:

$$f = 1 + z + z^2 + \dots + z^n + \dots = \sum_{i=0}^{\infty} z^i.$$

Poiché il termine noto è 1, questa serie è invertibile e il suo inverso è $1 - z$; possiamo allora scrivere l'uguaglianza:

$$\sum_{i=1}^{\infty} z^i = \frac{1}{1 - z}.$$

Notiamo che l'inverso di questa serie è di tipo particolare poiché è in realtà una serie definitamente nulla ossia un polinomio. Per $n > 1$ i monomi di grado i sono del tipo $X_1^{r_1} X_2^{r_2} \dots X_n^{r_n}$ con $r_1 + \dots + r_n = i$; i monomi diversi sono allora tanti quanti i modi di ottenere i come somma di n addendi interi non negativi, ossia:

$$f(i) = \binom{n+i-1}{i} = \binom{n+i-1}{n-1}.$$

Anche in questo caso la serie

$$f = 1 + nz + \frac{n(n+1)}{2}z^2 + \dots = \sum_{i=0}^{\infty} \binom{n+i-1}{n-1} z^i$$

è invertibile in $\mathbb{Z}[[z]]$ e anche questa volta la serie inversa è un polinomio poiché si ha:

$$f = \sum_{i=0}^{\infty} \binom{n+i-1}{n-1} z^i = \frac{1}{(1-z)^n}.$$

La serie f in $Z[[z]]$ sopra definita si chiamata la **serie di Hilbert** o (**serie di Hilbert-Poincaré**) di $R = k[X_1, \dots, X_n]$ ed è abitualmente denotata $HS_R(z)$.

Ideali di $k[X_1, \dots, X_n]$

§ Ideali in $A[X]$ e $A[[X]]$

Proposizione 7.1. *Sia I un ideale proprio di A . Allora*

$$I[X] := \{ \text{polinomi di } A[X] \text{ con coefficienti tutti in } I \}$$

è un ideale proprio di $A[X]$ e coincide con l'ideale generato da I . Inoltre $I[X]$ è strettamente contenuto nell'ideale

$$I + (X) := \{ \text{polinomi di } A[X] \text{ con termine noto in } I \}.$$

L'applicazione naturale:

$$\begin{aligned} i: A &\rightarrow A[X] \\ a &\mapsto a \end{aligned}$$

induce le seguenti applicazioni tra gli insiemi di ideali:

i)

$$\begin{aligned} \bar{i}: \text{Id}(A[X]) &\rightarrow \text{Id}(A) \\ \mathfrak{b} &\mapsto \mathfrak{b} \cap A. \end{aligned}$$

\bar{i} è suriettiva, ma non iniettiva; infatti si ha $\bar{i}(\mathfrak{a} + (X)) = \bar{i}(\mathfrak{a}[X]) = \mathfrak{a}$ per ogni ideale proprio \mathfrak{a} di A , anche se come già osservato $\mathfrak{a} + (X) \neq \mathfrak{a}[X]$.

ii)

$$\begin{aligned} \tilde{i}: \text{Id}(A) &\rightarrow \text{Id}(A[X]) \\ \mathfrak{a} &\mapsto \mathfrak{a}[X]. \end{aligned}$$

Si tratta di una applicazione iniettiva, ma non suriettiva. Se infatti $\mathfrak{a}_1 \neq \mathfrak{a}_2$, esiste un elemento $a \in \mathfrak{a}_1 \setminus \mathfrak{a}_2$ (oppure $a \in \mathfrak{a}_2 \setminus \mathfrak{a}_1$) e quindi $a \in \mathfrak{a}_1[X]$, ma $a \notin \mathfrak{a}_2[X]$.

Inoltre se \mathfrak{a} è un ideale proprio di A , allora $\mathfrak{a} + (X) \in \text{Id}(A[X])$, ma $\mathfrak{a} + (X) \notin \tilde{i}(\text{Id}(A))$.

iii)

$$\begin{aligned}\hat{i}: \text{Id}(A) &\rightarrow \text{Id}(A[X]) \\ \mathfrak{a} &\mapsto \mathfrak{a} + (X).\end{aligned}$$

Esattamente come nel caso precedente si prova che è una applicazione iniettiva, ma non suriettiva.

Lemma 7.2. *Sia A un anello. Le due condizioni seguenti sono equivalenti:*

1. *Ogni ideale di A è finitamente generato.*
2. *Ogni catena ascendente di ideali di A è stazionaria.*

Dimostrazione. “ \Rightarrow ” Supponiamo che valga 1. e consideriamo una famiglia \mathfrak{a}_i di ideali di A , dove i varia in un insieme totalmente ordinato I e $\mathfrak{a}_i \subseteq \mathfrak{a}_j$ per ogni coppia di indici $i, j \in I$ tali che $i < j$. L’unione \mathfrak{a} di tutti gli \mathfrak{a}_i risulta essere un ideale (poichè gli \mathfrak{a}_i formano una catena); per ipotesi esiste un numero finito di elementi $a_1, \dots, a_r \in A$ che generano \mathfrak{a} . Scegliamo quindi degli indici $i_1, \dots, i_r \in I$ tali che $a_n \in \mathfrak{a}_{i_n}$ e sia i_0 il loro massimo. Allora $a_1, \dots, a_r \in \mathfrak{a}_{i_0}$ e quindi $\mathfrak{a}_{i_0} = \mathfrak{a}$ e la catena da quel punto in poi è stazionaria.

“ \Leftarrow ” Supponiamo esista un ideale \mathfrak{a} di A che non è finitamente generato; consideriamo una successione a_n , con $n \in \mathbb{N}$, di elementi di \mathfrak{a} tali che $a_{n+1} \notin \mathfrak{a}_n = (a_1, \dots, a_n)$: una tale successione esiste certamente perchè in caso contrario a_1, \dots, a_n sarebbero generatori di \mathfrak{a} . Abbiamo così ottenuto una catena strettamente crescente di ideali di A . ■

Definizione 7.3. Un anello A si dice noetheriano se soddisfa le due condizioni equivalenti del lemma precedente.

Teorema 7.4. Teorema della base di Hilbert *Se A è un anello noetheriano allora anche $A[X]$ lo è.*

Dimostrazione. Sia I un ideale di $A[X]$ sia J_r il sottoinsieme di A degli elementi che sono il coefficiente direttivo di qualche polinomio di grado r in I . Si verifica facilmente che i J_r sono ideali di A e che si ha $J_r \subseteq J_{r+1}$ per ogni $r \in \mathbb{N}$. Poichè A è noetheriano, esiste r_0 tale che $J_{r_0} = J_r$ per ogni $r \geq r_0$. Allora I è generato dall’insieme finito di polinomi che si ottiene fissando un insieme finito di generatori di J_r per ogni $r \leq r_0$ e scegliendo quindi per ognuno dei generatori a di J_r un polinomio di grado r di cui a sia il coefficiente direttivo. ■

I risultati precedenti mostrano come la conoscenza degli ideali di $A[X]$ richiede una conoscenza preliminare di tutti gli ideali dell’anello A . Esaminiamo allora un caso in cui tutti gli ideali di A sono ben noti e molto semplici: il caso di un campo k . Ricordiamo alcuni fatti ben noti su $k[X]$

§ Ideali di $k[X]$.

Come è noto $k[X]$ è un dominio euclideo con la valutazione data dal grado; quindi $k[X]$ è un dominio a ideali principali e in esso vale la fattorizzazione unica.

Gli ideali di $k[X]$ sono allora tutti principali ossia del tipo (F) con $F \in k[X]$. Due ideali (F) e (G) coincidono se e solo se F e G sono associati tra loro. Quindi:

$$\text{Ideal}(A) \xrightarrow{1-1} k[X]/\sim$$

dove \sim è data da:

$$F \sim G \iff F = aG \text{ con } a \in k^*$$

poichè gli elementi non nulli di k sono gli unici elementi invertibili in $k[X]$.

Se \mathfrak{a} è un ideale non nullo di $k[X]$, sono equivalenti:

- 1) \mathfrak{a} è primo;
- 2) \mathfrak{a} è massimale;
- 3) $\mathfrak{a} = (F)$ con F irriducibile in $k[X]$.

L'ideale nullo è l'unico primo di $k[X]$ che non sia anche massimale.

Esempio 7.5. A parte (0) , gli unici ideali primi di $\mathbb{R}[X]$ sono quelli del tipo $(X - a)$ con $a \in \mathbb{R}$ e quelli del tipo $(X^2 + bX + c)$ con $b, c \in \mathbb{R}$ e $b^2 - 4ac < 0$.

A parte (0) , gli unici ideali primi di $\mathbb{C}[X]$ sono quelli del tipo $(X - a)$ con $a \in \mathbb{C}$.

Le seguenti osservazioni ci saranno utili in seguito.

Osservazione 7.6. La valutazione data dal grado e la conseguente struttura di dominio euclideo non forniscono solo informazioni di tipo generale sulle proprietà di $k[X]$, ma anche un metodo effettivo di calcolo.

Ad esempio, dati due ideali (F) e (G) di $k[X]$ si ha:

- i) $(F) + (G) = (H)$ dove $H = \text{MCD}(F, G)$;
- ii) $(F) \cap (G) = (L)$ dove $L = \text{mcm}(F, G)$;
- iii) $(F) \subseteq (G) \iff G \in F \iff G/F$ ossia se esiste $P \in k[X]$ tale che $F = PG$.

In tutti questi casi i polinomi H, L, P si possono calcolare mediante la divisione euclidea. Inoltre:

- iv) Nell'anello quoziente $k[X]/(F)$ due classi $\overline{G_1}, \overline{G_2}$ coincidono se e solo se il resto della divisione di G_1 per F e di G_2 per F coincidono. Quindi la divisione fornisce anche un metodo per lavorare nei quozienti di $k[X]$. Il resto della divisione di G per F è un **rappresentante privilegiato** di \overline{G} poichè in ogni classe vi è uno e un solo rappresentante di questo tipo.

Per eseguire materialmente la divisione tra due polinomi F e G per prima cosa li **riordiniamo** scrivendo i loro **termini in ordine decrescente** di grado:

$$F = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0, \quad G = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0;$$

quindi iniziamo a confrontare tra loro i termini di grado massimo $a_n X^n$ e $b_m X^m$: il quoziente tra F e G ha come termine di grado massimo il quoziente $a_n b_m^{-1} X^{n-m}$.

Si ottiene così il resto provvisorio $F_1 = F - a_n b_m^{-1} X^{n-m} G$ e si procede nella divisione ripetendo la stessa procedura a partire da F_1 .

Anche l'anello $k[X_1, \dots, X_n]$ è un dominio a fattorizzazione unica (Lemma di Gauss), ma per $n \geq 2$ non è un dominio a ideali principali (l'ideale massimale (X_1, \dots, X_n) non è principale); quindi non può essere neppure un dominio euclideo e non può possedere una divisione con resto come quella del caso di una sola variabile.

Ciò nonostante, vedremo come si può costruire un ordinamento dei termini e una specie di divisione con resto che permetteranno di generalizzare anche al caso di più variabili alcune delle precedenti procedure ed in particolare un metodo effettivo per stabilire se un polinomio appartiene o meno ad un dato ideale e un metodo per trovare in ogni classe del quoziente di $k[X_1, \dots, X_n]/\mathfrak{a}$ un rappresentante speciale.

§ Ideali di $k[X_1, \dots, X_n]$ e varietà algebriche di k^n .

Dati i polinomi F_1, \dots, F_r di $k[X_1, \dots, X_n]$ possiamo considerare il sottoinsieme $V = \mathcal{V}(F_1, \dots, F_r)$ di k^n delle soluzioni comuni alle equazioni $F_i = 0$. Un punto $P = (a_1, \dots, a_n)$ di k^n appartiene a V se $F_1(a_1, \dots, a_n) = \cdots = F_r(a_1, \dots, a_n) = 0$, ossia se è soluzione del sistema di equazioni:

$$\begin{cases} F_1(X_1, \dots, X_n) = 0 \\ F_2(X_1, \dots, X_n) = 0 \\ \dots \dots \\ F_r(X_1, \dots, X_n) = 0 \end{cases}$$

Più in generale, dato un sottoinsieme B di $k[X_1, \dots, X_n]$, possiamo considerare il sottoinsieme $V = \mathcal{V}(B)$ delle soluzioni comuni a tutte le equazioni $F = 0$ al variare di F in B , ossia:

$$\mathcal{V}(B) = \{P \in k^n \mid F(P) = 0, \forall F \in B\}.$$

Definizione 7.7. Ogni sottoinsieme V di k^n del tipo $V = \mathcal{V}(B)$ per un qualche $B \subseteq k[X_1, \dots, X_n]$ si dice **insieme algebrico** o **varietà algebrica affine**.

Lemma 7.8. *Le relazioni di inclusione tra sottoinsiemi di $k[X_1, \dots, X_n]$ corrispondono a inclusioni di verso rovesciato tra i corrispondenti insiemi algebrici, ossia:*

$$B_1 \subseteq B_2 \implies \mathcal{V}(B_1) \supseteq \mathcal{V}(B_2).$$

Uno stesso insieme algebrico V può essere ottenuto a partire da molti sottoinsiemi diversi di $k[X_1, \dots, X_n]$; a seconda dei casi potremo preferire un insieme di equazioni di V “più piccolo possibile” (e in tal caso vedremo che ne bastano in ogni caso un insieme finito) oppure l’insieme “più grande possibile” (e in tal caso si tratterà di un ideale).

Lemma 7.9. *Se $V = \mathcal{V}(B)$, allora si ha anche $V = \mathcal{V}(I)$ dove I è l’ideale generato da B .*

Dimostrazione. In virtù del lemma precedente si ha intanto $V = \mathcal{V}(B) \supseteq \mathcal{V}(I)$ poichè $B \subseteq I$. D’altra parte, se $P \in V(B)$ e $F \in I$, allora $F = G_1 F_1 + \dots + G_r F_r$ con $F_1, \dots, F_r \in B$ e quindi $F(P) = G_1(P)F_1(P) + \dots + G_r(P)F_r(P) = 0$.

Poichè ogni ideale dell’anello $k[X_1, \dots, X_n]$ possiede un insieme finito di generatori (cfr. Teorema 7.4), potremo definire un qualsiasi insieme algebrico anche usando soltanto un numero finito di polinomi ossia come l’insieme delle soluzioni comuni a un numero finito di equazioni polinomiali.

Esempio 7.10. L’ideale I generato da B non è in generale il più grande insieme che definisce $\mathcal{V}(B)$. Sia, ad esempio, F un polinomio non nullo di grado positivo di $k[X_1, \dots, X_n]$ e sia $V = \mathcal{V}(B = \{F^2\})$; l’ideale generato da B è l’ideale principale (F^2) . L’insieme algebrico V può essere ottenuta anche come $\mathcal{V}((F))$, ma si ha l’inclusione stretta di ideali $(F^2) \subset (F)$.

Lemma 7.11. *Se I è un ideale di $R = k[X_1, \dots, X_n]$ e $V = \mathcal{V}(I)$, allora si ha anche $V = \mathcal{V}(\sqrt{I})$.*

Dimostrazione. In virtù del Lemma 7.8 si ha intanto $\mathcal{V}(I) \supseteq \mathcal{V}(\sqrt{I})$ poichè $I \subseteq \sqrt{I}$. D’altra parte, se $P \in V(I)$ e $F \in \sqrt{I}$, allora $F^h \in I$ per un qualche esponente h e quindi $F(P) = 0$ poichè $F^h(P) = 0$ e k è un campo.

Definizione 7.12. Se W è sottoinsieme di k^n , si dice **ideale di W** l’insieme di tutti i polinomi che si annullano nei punti di W , ossia:

$$\mathcal{I}(W) = \{P \in k[X_1, \dots, X_n] \mid F(P) = 0 \text{ per ogni } P \in W\}.$$

(si noti che $\mathcal{I}(W)$ è effettivamente un ideale.)

Proposizione 7.13. *Siano \mathfrak{a} un ideale di $k[X_1, \dots, X_n]$ e W un sottoinsieme di k^n . Valgono allora le seguenti:*

- a) $\mathcal{I}(\mathcal{V}(\mathfrak{a})) \supseteq \mathfrak{a}$;
- b) $\mathcal{V}(\mathcal{I}(W)) \supseteq W$;
- c) $\mathcal{I}(\mathcal{V}(\mathfrak{a})) = \mathfrak{a}$ se e solo se $\mathfrak{a} = \mathcal{I}(W)$ per un qualche $W \subseteq k^n$;

d) $\mathcal{V}(\mathcal{I}(W)) = W$ se e solo se W è un insieme algebrico;

e) $\mathcal{I}(W) = \sqrt{\mathcal{I}(W)}$.

Anche se è perfettamente sensato definire l'ideale di tutti i polinomi che si annullano nei punti di un qualsiasi sottoinsieme di k^n , grazie alle proprietà precedenti non sarà restrittivo considerare soltanto ideali associati a sottoinsiemi algebrici.

Esempio 7.14. Sia W il sottoinsieme del piano \mathbb{R}^2 dei punti con ordinata nulla e ascissa positiva: concretamente, W è la semiretta positiva dell'asse X . Se $F(X, Y)$ è un polinomio di $\mathbb{R}[X, Y]$ che si annulla su tutti i punti di W , allora $F(X, 0)$ è un polinomio di $\mathbb{R}[X]$ che si annulla per ogni valore positivo a in \mathbb{R} . L'unico polinomio di $\mathbb{R}[X]$ con infinite radici è il polinomio nullo e quindi $F(X, 0) = 0$. Allora $F(X, Y) = YG(X, Y)$ si annulla in $(a, 0)$ per ogni $a \in \mathbb{R}$.

L'ideale $\mathcal{I}(W)$ è l'ideale principale (Y) e $\mathcal{I}(\mathcal{V}(Y)) = \mathcal{I}(W)$ è anche l'ideale dell'insieme algebrico $\mathcal{V}((Y))$ costituito dall'intero asse X .

Esempio 7.15. L'insieme vuoto \emptyset e k^n sono varietà algebriche definite rispettivamente dagli ideali improprio e nullo. Se k è infinito, (0) è l'unico ideale la cui varietà associata è tutto k^n ; anche in questo caso vi possono essere invece tanti diversi ideali che definiscono l'insieme algebrico vuoto. Ad esempio, in $\mathbb{R}[X]$ si ha $\mathcal{V}(I) = \emptyset$ anche con $I = (X^2 + 1)$.

È inoltre un insieme algebrico ogni insieme costituito da un solo punto $V = \{P\}$; si ha infatti $\mathcal{V}(I) = \{P = (a_1, \dots, a_n)\}$ prendendo ad esempio come I l'ideale massimale $(X_1 - a_1, \dots, X_n - a_n)$; in tal caso si ha proprio $I = \mathcal{I}(\mathcal{V}(I))$.

Anche se gli ideali associati a un insieme algebrico sono tutti ideali radicali, non si ha in generale corrispondenza biunivoca tra insiemi algebrici e gli ideali radicali. Vedremo in seguito che si ha una tale corrispondenza biunivoca se e soltanto se il campo k è **algebricamente chiuso**: si tratta di uno dei risultati fondamentali della Geometria Algebrica, noto come **Nullstellensatz** o **Teorema degli Zeri di Hilbert**.

Proposizione 7.16. *La famiglia degli insiemi algebrici di k^n è chiusa rispetto all'unione finita, all'intersezione e al prodotto cartesiano. Valgono infatti le seguenti relazioni per ideali \mathfrak{a}_j di $k[X_1, \dots, X_n]$ e insiemi algebrici V_j di k^n :*

$$i) \mathcal{V}(\mathfrak{a}_1) \cup \mathcal{V}(\mathfrak{a}_2) = \mathcal{V}(\mathfrak{a}_1 \cap \mathfrak{a}_2) = \mathcal{V}(\mathfrak{a}_1 \cdot \mathfrak{a}_2);$$

$$ii) \mathcal{I}(V_1 \cup V_2) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2);$$

$$iii) \bigcap_{j \in J} \mathcal{V}(\mathfrak{a}_j) = \mathcal{V}(\bigcup_{j \in J} \mathfrak{a}_j) = \mathcal{V}(\sum_{j \in J} \mathfrak{a}_j);$$

$$iv) \mathcal{I}(V_1 \cap V_2) \supseteq \mathcal{I}(V_1) + \mathcal{I}(V_2).$$

v) Se inoltre $V_1 = \mathcal{V}(\mathfrak{a}) \subseteq k^n$ con $\mathfrak{a} \in \text{Id}(k[X_1, \dots, X_n])$ e $V_2 = \mathcal{V}(\mathfrak{b}) \subseteq k^m$ con $\mathfrak{b} \in \text{Id}(k[Y_1, \dots, Y_m])$, allora

$$V_1 \times V_2 = \mathcal{V}(\mathfrak{a}[Y_1, \dots, Y_m] + \mathfrak{b}[X_1, \dots, X_n]) \subseteq k^{n+m}$$

dove $\mathfrak{a}[Y_1, \dots, Y_m] + \mathfrak{b}[X_1, \dots, X_n]$ è l'ideale di $k[X_1, \dots, X_n, Y_1, \dots, Y_m]$ generato da $\mathfrak{a} \cup \mathfrak{b}$.

Dimostrazione. Proviamo a titolo di esempio i).

Poichè le inclusioni $\mathcal{V}(\mathfrak{a}_1) \cup \mathcal{V}(\mathfrak{a}_2) \subseteq \mathcal{V}(\mathfrak{a}_1 \cap \mathfrak{a}_2) \subseteq \mathcal{V}(\mathfrak{a}_1 \cdot \mathfrak{a}_2)$ seguono immediatamente da proprietà generali, proviamo soltanto l'inclusione non banale $\mathcal{V}(\mathfrak{a}_1 \cdot \mathfrak{a}_2) \subseteq \mathcal{V}(\mathfrak{a}_1) \cup \mathcal{V}(\mathfrak{a}_2)$. Sia P un punto di $\mathcal{V}(\mathfrak{a}_1 \cdot \mathfrak{a}_2)$ e supponiamo che $P \notin \mathcal{V}(\mathfrak{a}_1)$. Allora esiste un elemento $F \in \mathfrak{a}_1$ tale che $F(P) \neq 0$; poichè per ogni $G \in \mathfrak{a}_2$ si ha $F \cdot G \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$, allora $F(P) \cdot G(P) = 0$ e quindi $G(P) = 0$ ossia $P \in \mathcal{V}(\mathfrak{a}_2)$.

Una immediata conseguenza della proposizione precedente è il fatto che gli insiemi algebrici di k^n costituiscono i chiusi di una topologia che si dice **topologia di Zariski** su k^n . Potremo quindi considerare relativamente ad essi le proprietà, le costruzioni e i risultati validi per i chiusi di una topologia, come ad esempio la nozione seguente.

Definizione 7.17. Si dice che un insieme algebrico V è **irriducibile** se non è l'unione di due insiemi algebrici strettamente contenuti in V ossia se:

$$V = V_1 \cup V_2 \text{ con } V_1 \text{ e } V_2 \text{ algebrici} \implies V = V_1 \text{ oppure } V = V_2.$$

V si dice **riducibile** se non è irriducibile, ossia se è l'unione di due insiemi algebrici ciascuno strettamente contenuto in V .

Attenzione: in alcuni testi il termine **varietà algebrica** è riservato agli insiemi algebrici irriducibili.

Proposizione 7.18. Sia V un insieme algebrico non vuoto di k^n . Allora:

$$V \text{ è irriducibile} \iff \mathcal{I}(V) \text{ è primo.}$$

Dimostrazione. “ \implies ”. Supponiamo che V sia irriducibile e siano F, G tali che $FG \in \mathcal{I}(V)$. Gli ideali $\mathfrak{a}_1 = (F) + \mathcal{I}(V)$ e $\mathfrak{a}_2 = (G) + \mathcal{I}(V)$ contengono entrambi $\mathcal{I}(V)$ e quindi gli insiemi algebrici ad essi associati $V_1 = \mathcal{V}(\mathfrak{a}_1)$ e $V_2 = \mathcal{V}(\mathfrak{a}_2)$ sono contenuti in V . Inoltre si ha $V_1 \cup V_2 = V$; infatti se $P \in V$ allora $P \in \mathcal{V}(\mathcal{I}(V))$ e inoltre $(FG)(P) = F(P)G(P) = 0$ e quindi $F(P) = 0$ oppure $G(P) = 0$: nel primo caso si ha $P \in \mathcal{V}(\mathfrak{a}_1)$ e nel secondo $P \in \mathcal{V}(\mathfrak{a}_2)$.

Poichè V è irriducibile, si ha $V = V_1$ (oppure $V = V_2$) e quindi $\mathcal{I}(V) \subseteq \mathfrak{a}_1 \subseteq \mathcal{I}(\mathcal{V}(\mathfrak{a}_1)) = \mathcal{I}(V_1) = \mathcal{I}(V)$ e quindi $\mathcal{I}(V) = \mathfrak{a}_1$. Allora $F \in \mathcal{I}(V)$ e possiamo concludere che $\mathcal{I}(V)$ è primo.

“ \Leftarrow ”. Supponiamo che $V = V_1 \cup V_2$ sia l’unione di due insiemi algebrici strettamente più piccoli. Allora $\mathcal{I}(V) = \mathcal{I}(V_1 \cup V_2) = \mathcal{I}(V_1) \cap \mathcal{I}(V_2)$, dove $\mathcal{I}(V_1)$ e $\mathcal{I}(V_2)$ sono ideali che contengono strettamente $\mathcal{I}(V)$. In tal caso $\mathcal{I}(V)$ non può essere primo (cfr Proposizione ???).

La Proposizione non vale in generale se si sostituisce $\mathcal{I}(V)$ con un qualsiasi ideale \mathfrak{a} tale che $\mathcal{V}(\mathfrak{a}) = V$. Abbiamo già visto infatti che per ogni insieme algebrico proprio V , anche irriducibile, l’ideale $\mathcal{I}(V)^2$ è un ideale non primo che definisce V . Viceversa, l’insieme algebrico definito da un ideale primo può risultare riducibile.

Esempio 7.19. L’ideale principale $((Y - 1)^2 + (Y - X^2)^2)$ di $\mathbb{R}[X, Y]$ è primo in quanto è un ideale di un dominio fattoriale generato da un elemento irriducibile. L’insieme algebrico da esso definito è l’intersezione tra la parabola di equazione $Y - X^2 = 0$ e la retta di equazione $Y - 1 = 0$ ed è quindi costituito dai due punti $P = (1, 1)$ e $Q = (-1, 1)$, ciascuno dei quali costituisce un insieme algebrico.

Esempio 7.20. L’insieme algebrico V di \mathbb{R}^2 definito dall’ideale $(XY - 1)$ è una iperbole del piano reale. Anche se V è unione insiemistica dei suoi due sottoinsiemi disgiunti detti rami, V è però un insieme algebrico irriducibile. I rami dell’iperbole non sono infatti, presi separatamente, degli insiemi algebrici.

Mostreremo in seguito che ogni insieme algebrico di k^n può essere decomposto nell’unione di un numero finito di varietà irriducibili. Proveremo questa proprietà tramite la corrispondente proprietà degli ideali radicali di $k[X_1, \dots, X_n]$ di poter essere scritti come intersezione di un numero finito di ideali primi ossia dell’esistenza in $k[X_1, \dots, X_n]$ della **decomposizione primaria**. Nel caso degli ideali del tipo $\mathcal{I}(V)$, le componenti irriducibili sono le varietà $\mathcal{V}(\mathfrak{p}_i)$ dove i \mathfrak{p}_i sono i primi minimali tra quelli che contengono $\mathcal{I}(V)$.

Vedremo inoltre come le proprietà degli ideali di $k[X_1, \dots, X_n]$ permettano di definire in modo algebrico, anzi in molti modi algebrici diversi, la dimensione di una varietà di k^n .

Definizione 7.21. Si dice **dimensione** di un insieme algebrico V la massima lunghezza delle catene:

$$V_0 \subsetneq V_1 \subsetneq \dots \subsetneq V_r \subseteq V$$

dove le V_i sono varietà irriducibili.

La definizione precedente potrebbe essere applicata al caso di uno spazio topologico qualsiasi, ma in generale non è detto che il massimo esista. Nel caso delle varietà algebriche l’esistenza del massimo è conseguenza di una proprietà algebrica dell’anello dei polinomi. Infatti ogni tale catena corrisponde ad una catena (con inclusioni rovesciate) di ideali:

$$\mathfrak{q}_0 = \mathcal{I}(V_0) \supsetneq \mathfrak{q}_1 = \mathcal{I}(V_1) \supsetneq \dots \supsetneq \mathfrak{q}_r = \mathcal{I}(V_r) \supseteq \mathcal{I}(V)$$

dove i \mathfrak{q}_i sono ideali primi. Dalla noetherianità dell'anello $k[X_1, \dots, X_n]$ discende che la lunghezza massima di tali catene è finita; tale lunghezza è legata all' **altezza** dell'ideale $\mathcal{I}(V)$ e permette di definire anche la nozione di **dimensione di Krull** di un anello.

La nozione di dimensione così definita corrisponde esattamente a quello che intuitivamente intendiamo quando diciamo che le rette e le coniche sono 1-dimensionali, le quadriche sono 2-dimensionali, i punti 0-dimensionali e così via.

§ L'anello delle coordinate di una varietà algebrica

Sia V un sottoinsieme algebrico di k^n e sia $I = \mathcal{I}(V)$ l'ideale associato. Ogni polinomio $F \in k[X_1, \dots, X_n]$ definisce una funzione:

$$\tilde{F}: V \rightarrow k \quad \text{data da} \quad P \mapsto F(P).$$

Definizione 7.22. L'anello $k[V]$ delle funzioni polinomiali su V dotato delle operazioni di somma e prodotto punto per punto si dice **anello delle coordinate** di V .

Due polinomi F e G definiscono la stessa funzione polinomiale in $k[V]$ se e soltanto se la loro differenza $F - G$ definisce la funzione nulla, ossia se $F - G \in I$. Allora $k[V]$ è canonicamente isomorfo a $k[X_1, \dots, X_n]/I$.

Analogamente a quanto visto nel caso di una indeterminata, l'anello $k[X_1, \dots, X_n]/I$ è l'estensione di k con gli elementi x_1, \dots, x_n , dove le x_i sono le classi nel quoziente delle indeterminate X_i . Spesso identificheremo i due anelli isomorfi e scriveremo $k[V] = k[X_1, \dots, X_n]/I$ oppure anche $k[V] = k[x_1, \dots, x_n]$ dove le x_i si dicono le **coordinate** su V .

Algoritmo di divisione in $k[X_1, \dots, X_n]$

Introduciamo ora una generalizzazione della divisione con resto al caso degli anelli di polinomi in più indeterminate che ci permetterà di rispondere in modo operativo a problemi del tipo seguenti:

1. **Ideal membership:** dati un ideale \mathfrak{a} e un elemento f di $k[X_1, \dots, X_n]$, stabilire se $f \in \mathfrak{a}$.
2. Stabilire se due ideali di $k[X_1, \dots, X_n]$ assegnati mediante insiemi di generatori sono uguali.
3. Trovare una base di $k[X_1, \dots, X_n]/\mathfrak{a}$ come k -spazio vettoriale.
4. Trovare in ogni classe di $k[X_1, \dots, X_n]/\mathfrak{a}$ un rappresentante speciale.
5. Stabilire se due classi \bar{f} e \bar{g} di $k[X_1, \dots, X_n]/\mathfrak{a}$ sono uguali.

0.1 Ordinamento di monomi

Definizione 8.1. Indicheremo con \mathbb{T}^n il sottoinsieme di $k[X_1, \dots, X_n]$ di tutti i monomi, ossia:

$$\mathbb{T}^n = \{X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n} \mid \alpha_i \in \mathbb{N}\}.$$

Spesso indicheremo un elemento di \mathbb{T}^n con la notazione abbreviata X^α dove $\alpha = (\alpha_1, \dots, \alpha_n)$ è la stringa ordinata degli esponenti e scriveremo $\alpha = \log(X^\alpha)$.

L'insieme \mathbb{T}^n con l'operazione di prodotto costituisce un monoide ordinato isomorfo in modo ovvio al monoide \mathbb{N}^n dotato dell'operazione di somma componente per componente ossia all'usuale somma di vettori se pensiamo \mathbb{N}^n come sottoinsieme di \mathbb{R}^n ; in questo modo anche le relazioni d'ordine in \mathbb{T}^n corrispondono alle relazioni d'ordine in \mathbb{N}^n .

Le relazioni d'ordine a cui siamo interessati devono soddisfare alcune proprietà:

Definizione 8.2. Diciamo **term order** ogni ordinamento \preceq su \mathbb{T}^n che:

i) è un ordine totale ossia $\forall X^\alpha, X^\beta \in \mathbb{T}^n$ si ha:

$$X^\alpha \preceq X^\beta \text{ oppure } X^\beta \preceq X^\alpha$$

ii) rispetta l'operazione di prodotto tra monomi ossia $\forall X^\alpha, X^\beta, X^\gamma \in \mathbb{T}^n$ si ha:

$$X^\alpha \preceq X^\beta \implies X^\alpha X^\gamma \preceq X^\beta X^\gamma.$$

iii) $1 \preceq X^\alpha$ per ogni $X^\alpha \in \mathbb{T}^n$

Nel seguito oltre a \preceq useremo i simboli \prec, \succeq e \succ col significato usuale.

Osservazione 8.3. Per ogni term order \preceq in \mathbb{T}^n vale la cancellazione, ossia $\forall X^\alpha, X^\beta, X^\gamma \in \mathbb{T}^n$ si ha

$$X^\alpha X^\gamma \prec X^\beta X^\gamma \iff X^\alpha \prec X^\beta.$$

Se infatti si avesse $X^\alpha \succ X^\beta$ allora si avrebbe anche $X^\alpha X^\gamma \succeq X^\beta X^\gamma$.

Lemma 8.4. *Un ordinamento totale \preceq in \mathbb{T}^n che rispetta il prodotto è un term order se e solo per ogni indeterminata X_i si ha $1 \prec X_i$.*

Dimostrazione. Proviamo soltanto l'implicazione non banale. Sia X^α un monomio di \mathbb{T}^n ; proviamo che si ha $1 \prec X^\alpha$ per induzione sul grado totale di X^α . Se il grado è 1 non c'è nulla da provare. Supponiamo che l'asserto valga per ogni monomio di grado inferiore a X^α e consideriamo una indeterminata X_i che compare in X^α con esponente positivo. Sia allora X^β tale che $X^\alpha = X_i \cdot X^\beta$. Usando la condizione ii) si ha allora $1 \prec X_i \preceq X_i \cdot X^\beta = X^\alpha$ come volevasi. ■

Proposizione 8.5. *Un ordinamento totale in \mathbb{T}^n che rispetta il prodotto è un term order se e solo se è un buon ordinamento.*

Dimostrazione. Supponiamo che \preceq sia un ordinamento totale che rispetta il prodotto ma che si abbia $1 \succ X_i$ per una qualche indeterminata. Allora si avrebbe anche:

$$1 \succ X_i \succ X_i^2 \succ \dots \succ X_i^n \succ \dots$$

L'insieme delle potenze di X_i sarebbe dunque una catena priva di minimo e quindi la relazione non sarebbe un buon ordinamento.

Se invece supponiamo che \preceq sia un term order e consideriamo una catena decrescente

$$\dots \succeq X^{\alpha_i} \succeq X^{\alpha_{i+1}} \succeq \dots$$

ad essa possiamo associare la catena crescente di ideali di $k[X_1, \dots, X_n]$:

$$\dots \subseteq \mathfrak{a}_i = (X^{\alpha_1}, \dots, X^{\alpha_i}) \subseteq \mathfrak{a}_{i+1} = (X^{\alpha_1}, \dots, X^{\alpha_{i+1}}) \subseteq \dots$$

Per la noetherianità di $k[X_1, \dots, X_n]$, esiste un indice r tale che per ogni $s \geq r$ si ha $\mathfrak{a}_r = \mathfrak{a}_s$ e quindi, in particolare, $X^{\alpha_s} \in \mathfrak{a}_r$. Poichè ogni elemento di \mathfrak{a}_r è combinazione lineare dei monomi $X^{\alpha_1}, \dots, X^{\alpha_r}$, allora ogni monomio di ogni elemento di \mathfrak{a}_r è multiplo di qualche X^{α_j} con $j \leq r$; in particolare avremmo allora che ogni X^{α_s} con $s > r$ è multiplo di qualche X^{α_j} con $j \leq r$, e quindi per la proprietà di cancellazione $1 \succeq X^{\alpha_s - \alpha_j}$. Poichè abbiamo supposto che \preceq è un term order, l'unica possibilità è $X^{\alpha_s - \alpha_j} = 1$ e quindi che la catena crescente in \mathbb{T}^n sia stazionaria. ■

Notiamo che ogni term order definisce in particolare un ordinamento totale sull'insieme delle variabili. A meno di un cambiamento di nome potremo sempre supporre che si abbia:

$$X_1 \succ X_2 \succ \dots \succ X_n \succ 1.$$

Esempio 8.6. L'ordinamento più naturale in \mathbb{Z}^n è quello lessicografico che indicheremo con \leq_{Lex} o semplicemente con \leq .

Per ogni coppia di elementi $(\alpha_1, \dots, \alpha_n), (\beta_1, \dots, \beta_n)$ di \mathbb{Z}^n si ha $(\alpha_1, \dots, \alpha_n) \leq (\beta_1, \dots, \beta_n)$ se vale una delle condizioni equivalenti:

1. $(\alpha_1, \dots, \alpha_n) = (\beta_1, \dots, \beta_n)$ oppure $\alpha_i = \beta_i$ per ogni $i < r$ e $\alpha_r < \beta_r$;
2. $(\alpha_1 - \beta_1, \dots, \alpha_n - \beta_n)$ è la n -upla nulla $(0, \dots, 0)$ oppure il suo primo elemento non nullo è positivo.

Ovviamente tale ordinamento in \mathbb{Z}^n induce un ordinamento anche sul sottoinsieme \mathbb{N}^n e quindi anche su \mathbb{T}^n : chiameremo entrambi ordinamento lessicografico, in breve *Lex* e useremo il simbolo \leq_{Lex} . Si verifica facilmente che *Lex* è un term order.

Due classi molto vaste di ordinamenti su \mathbb{T}^n , che comprende essenzialmente tutti i term order che useremo, è data dai risultati seguenti.

Proposizione 8.7. *Sia A una matrice $n \times n$ a entrate intere di rango massimo. La relazione \preceq_A in \mathbb{N}^n data da:*

$$(\alpha_1, \dots, \alpha_n) \preceq_A (\beta_1, \dots, \beta_n) \iff (\alpha_1, \dots, \alpha_n)^t A \leq_{Lex} (\beta_1, \dots, \beta_n)^t A$$

è una relazione d'ordine totale.

Inoltre \preceq_A è un term order se e solo se il primo elemento non nullo in ogni colonna di A è positivo.

Dimostrazione. Lasciamo al lettore la verifica che si tratta di un ordinamento totale; osserviamo soltanto che la proprietà antisimmetrica discende dal fatto che la matrice ha rango massimo. Per provare la caratterizzazione dei term orders, ricordiamo il Lemma 8.4. Grazie a tale risultato abbiamo che \preceq_A è un term order se e solo se per ogni $i = 1, \dots, n$ si ha $1 \preceq_A X_i$ e quindi se e solo se $(0, \dots, 1, 0, \dots, 0)^t A$ ha il primo elemento non nullo positivo. Ma il primo elemento non nullo di $(0, \dots, 0, 1, 0, \dots, 0)^t A$ è proprio il primo elemento non nullo della colonna i -esima di A . ■

Proposizione 8.8. *Sia $\mathbf{w} = (w_1, \dots, w_n)$ un vettore “generico” di \mathbb{R}^n ossia tale che nessun w_i sia combinazione lineare dei rimanenti a coefficienti interi.*

Allora la relazione in \mathbb{N}^n data da:

$$(\alpha_1, \dots, \alpha_n) \preceq_{\mathbf{w}} (\beta_1, \dots, \beta_n) \iff (\alpha_1, \dots, \alpha_n) \cdot \mathbf{w} \leq (\beta_1, \dots, \beta_n) \cdot \mathbf{w}$$

è una relazione d'ordine totale.

Inoltre $\preceq_{\mathbf{w}}$ è un term order se e solo $w_i > 0$ per ogni $i = 1, \dots, n$.

Dimostrazione. Lasciamo per esercizio la verifica che si tratta di un ordinamento totale; osserviamo soltanto che la proprietà antisimmetrica discende dal fatto che per la genericità delle coordinate di \mathbf{w} si ha $\alpha \cdot \mathbf{w} \neq 0$ per ogni stringa $\alpha \in \mathbb{N}^n$. La caratterizzazione dei term orders discende poi immediatamente dal Lemma 8.4. ■

Osserviamo che un vettore $\mathbf{w} = (w_1, \dots, w_n)$ soddisfa la condizione di genericità richiesta nell'enunciato precedente ad esempio se $\mathbb{Q}[w_1, \dots, w_n]$ è un sottocampo di \mathbb{R} con grado di trascendenza n su \mathbb{Q} ; estensioni siffatte esistono certamente poichè i sotto-campi di \mathbb{R} del tipo $\mathbb{Q}[a_1, \dots, a_r]$ hanno tutti cardinalità numerabile, mentre \mathbb{R} è più che numerabile.

Esempio 8.9. L'unico term order su \mathbb{T}^1 (ossia sui monomi di $k[X]$) è quello dato dal grado. Si ha infatti $1 < X$ e quindi, moltiplicando per X^n , $X^n < X^{n+1}$. L'applicazione *log* costituisce quindi una applicazione continua che conserva l'ordine tra \mathbb{T}^1 e \mathbb{N} .

Esempio 8.10. L'ordinamento lessicografico \leq_{Lex} in \mathbb{T}^n , per ogni $n \geq 2$, si può pensare come il term order \leq_A scegliendo come A la matrice identità. Anche se \mathbb{T}^n è un insieme numerabile, tuttavia \leq_{Lex} è molto diverso dall'ordinamento \leq in \mathbb{N} nel senso che non vi è nessuna applicazione biunivoca tra \mathbb{N} e \mathbb{T}^n che conserva l'ordinamento. Infatti tra due numeri naturali qualsiasi si trovano sempre un numero finito di altri numeri, mentre tra due monomi si possono trovare anche infiniti monomi, come nel caso seguente:

$$1 < X_2 < X_2^2 < X_2^3 < \dots < X_2^k < \dots < X_1.$$

L'esempio seguente mostra come vi siano sottoinsiemi di \mathbb{T}^n che non ammettono massimo rispetto a \leq_{Lex} , pur essendo superiormente limitati. Per questo motivo si preferisce spesso un altro ordinamento, strettamente legato a \leq_{Lex} , ma in cui situazioni “spiacevoli” di questo tipo non si verificano.

Esempio 8.11. Consideriamo la matrice:

$$A = \begin{pmatrix} 1 & 1 & \dots & \dots & 1 & 1 \\ 1 & 0 & \dots & \dots & 0 & 0 \\ 0 & 1 & \dots & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \dots & 1 & 0 \end{pmatrix}$$

Il term order \leq_A ad essa associato confronta innanzi tutto il grado totale dei monomi: il monomio più grande tra due è quello di grado maggiore; a parità di grado si confrontano poi gli esponenti a partire da quelli delle indeterminate maggiori, come in *Lex*. Perciò questo term order si chiama **lessicografico graduato** e si denota \leq_{DegLex} . In simboli:

$$X^\alpha \leq_{DegLex} X^\beta \text{ se } \partial(X^\alpha) < \partial(X^\beta) \text{ oppure } \partial(X^\alpha) = \partial(X^\beta) \text{ e } X^\alpha \leq_{Lex} X^\beta$$

Poichè in ogni grado vi sono soltanto un numero finito di monomi, tra due monomi se ne trovano solo un numero finito di altri. Si tratta quindi di un ordinamento molto simile a quello di \mathbb{N} .

Esempio 8.12. Vogliamo determinare tutti i term orders graduati su \mathbb{T}^2 , ossia sui monomi di $k[X, Y]$, supponendo $Y < X$. Se moltiplichiamo questa relazione per ogni monomio di grado $r - 1$, otteniamo un unico possibile ordinamento tra i monomi di grado r :

$$Y^r < XY^{r-1} < \dots < X^{r-i}Y^i < X^{r-i+1}Y^{i-1} < \dots < X^r.$$

Quindi vi sono solo due possibili ordinamenti graduati, questo e quello ottenuto ponendo $X < Y$. Tutte le matrici invertibili del tipo $\begin{pmatrix} 1 & 1 \\ a & b \end{pmatrix}$ individuano l'uno o l'altro a seconda del segno di $a - b$.

Esempio 8.13. Vogliamo determinare tutti i term orders graduati su \mathbb{T}^3 , ossia sui monomi di $k[X, Y, Z]$, supponendo $Z < Y < X$. Se moltiplichiamo questa relazione per ogni monomio di grado 1, otteniamo una serie di relazioni tra i monomi di secondo grado, ossia:

$$Z^2 < YZ < XZ < XY < X^2 \text{ e anche } Z^2 < YZ < Y^2 < XY < X^2$$

ma non otteniamo alcuna indicazione su quale sia il minore tra XZ e Y^2 . Porre $Y^2 < XZ$ porta all'unico ordinamento \leq_{DegLex} , ma vi è anche un term order per il quale $XZ < Y^2$, ed è quello associato alla matrice:

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}$$

Esempio 8.14. Generalizzando l'esempio precedente, consideriamo la matrice:

$$A = \begin{pmatrix} 1 & 1 & \dots & \dots & 1 & 1 \\ 0 & 0 & \dots & \dots & 0 & -1 \\ 0 & 0 & \dots & \dots & -1 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & -1 & \dots & \dots & 0 & 0 \end{pmatrix}$$

Il term order \leq_A su \mathbb{T}^n ad essa associato, detto **lessicografico inverso graduato** e denotato abitualmente con $\leq_{RevDegLex}$, è un term order graduato, ossia confronta innanzi tutto il grado totale dei monomi; nel caso in cui $\partial(X^\alpha) = \partial(X^\beta)$, allora:

$X^\alpha <_{RevDegLex} X^\beta$ se $\exists r (1 \leq r \leq n)$ tale che $\alpha_i = \beta_i$ per ogni $i > r$ e $\alpha_r > \beta_r$

Poichè vi sono soltanto un numero finito di monomi di ciascun grado, tra due monomi qualsiasi se ne trovano solo un numero finito di altri. Si tratta quindi di un ordinamento molto simile a quello di \mathbb{N} .

Nota bene: Il *DegRevLex* non è un ordinamento *DegLex* con una diversa gerarchia delle variabili poichè in entrambi i casi abbiamo fissato le relazioni $X_n < \dots < X_1$.

§ Ideali monomiali

Lemma 8.15. *Sia I un ideale di $k[X_1, \dots, X_n]$. Le seguenti condizioni sono equivalenti:*

1. *se F appartiene a I , allora ogni termine di F appartiene a I ;*
2. *I è generato dall'insieme dei suoi termini;*
3. *$I = (X^{\alpha_1}, \dots, X^{\alpha_r})$.*

Lasciamo al lettore la facile verifica dell'equivalenza delle tre condizioni; notiamo soltanto che la prova dell'implicazione 2. \Rightarrow 3. si ottiene facilmente grazie al Teorema della Base di Hilbert. Si potrebbe anche dimostrare direttamente tale implicazione, nota come **Lemma di Dickson** e da essa dedurre poi il Teorema della Base.

Definizione 8.16. Un ideale I di $k[X_1, \dots, X_n]$ che soddisfa le condizioni equivalenti del Lemma 8.15 si dice **ideale monomiale**. Un insieme di generatori monomiali di un ideale monomiale che sia minimale, ossia tale che nessun suo sottoinsieme proprio genera I , si dice **base** di I .

Proposizione 8.17. *Un ideale monomiale I possiede un'unica base $\{X^{\alpha_1}, \dots, X^{\alpha_r}\}$.*

Dimostrazione. Possiamo ottenere un insieme di generatori minimale a partire da un qualsiasi insieme di generatori monomiali, cancellando ogni monomio che sia multiplo di un altro.

Se poi $\{X^{\alpha_1}, \dots, X^{\alpha_r}\}$ e $\{X^{\beta_1}, \dots, X^{\beta_s}\}$ sono due basi di I , allora per ogni $i \leq r$ il monomio X^{α_i} dovrebbe dividere un monomio X^{β_j} , il quale a sua volta dovrebbe dividere un monomio $X^{\alpha_{i'}}$. Poichè per costruzione nessun monomio di una base può dividerne un altro della stessa base, allora $X^{\alpha_i} = X^{\alpha_{i'}}$ e quindi $X^{\alpha_i} = X^{\beta_j}$. ■

Se $I = (X^{\alpha_1}, \dots, X^{\alpha_r})$ è un ideale monomiale, è molto semplice trovare delle strategie operative per rispondere ai problemi posti all'inizio di questo capitolo. Per sapere se un polinomio F appartiene a I , basta controllare se ogni termine di F è multiplo di uno dei monomi X^{α_i} ; per determinare un generatore speciale in ogni classe \overline{G} di $k[X_1, \dots, X_n]/I$ basta cancellare da G ogni termine che è multiplo di uno degli X^{α_i} , e così via.

Vedremo ora come un term order permetta di trovare strategie analoghe a queste, ma applicabili anche nel caso di un ideale qualsiasi.

Introduciamo alcune notazioni. Sia F un polinomio non nullo di $k[X_1, \dots, X_n]$. **Supponiamo fissato un term order in \mathbb{T}^n .**

Definizione 8.18. Dato un polinomio F , consideriamo l'unica scrittura $F = \sum_{j=1}^s a_j X^{\gamma_j}$ con $0 \neq a_j \in k$ per ogni $j = 1, \dots, s$. Si dice:

- **monomio iniziale** (in inglese **leading monomial**) di F , denotato $Lm(F)$ il massimo (rispetto a \preceq) degli X^{γ_j} ;
- **termine iniziale** (in inglese **leading term**) di F , denotato $Lt(F)$ il termine $a_j X^{\gamma_j}$, dove $X^{\gamma_j} = Lm(F)$;
- **coefficiente iniziale o coefficiente direttivo** (in inglese **leading coefficient**) di F , denotato $Lc(F)$ il coefficiente a_j in F di $X^{\gamma_j} = Lm(F)$.

Valgono le ovvie relazioni per ogni coppia di polinomi non nulli:

- i. $Lt(F) = Lc(F)Lm(G)$;
- ii. $Lm(FG) = Lm(F)Lm(G)$, $Lc(FG) = Lc(F)Lc(G)$, $Lt(FG) = Lt(F)Lt(G)$;
- iii. $Lm(F + G) = \max\{Lm(F), Lm(G)\}$ e vale "=" se $Lm(F) \neq Lm(G)$.

Definizione 8.19. Se I è un ideale di $k[X_1, \dots, X_n]$, si dice **ideale iniziale** di I (rispetto a \preceq) l'ideale monomiale $In(I)$ generato da

$$\{X^\gamma \in \mathbb{T}^n \mid X^\gamma = Lm(F) \text{ per qualche } F \in I\}$$

Proposizione 8.20. Sia I un ideale di $k[X_1, \dots, X_n]$. Consideriamo un insieme di generatori monomiali $\{X^{\alpha_1}, \dots, X^{\alpha_r}\}$ di $In(I)$ ossia, e per ogni i , ($1 \leq i \leq r$) dei polinomi $F_i \in I$ tali che $Lm(F_i) = X^{\alpha_i}$.

Allora $I = (F_1, \dots, F_r)$.

Dimostrazione. Supponiamo per assurdo che ci siano polinomi di I che non si possono scrivere come combinazione lineare a coefficienti in $k[X_1, \dots, X_n]$ degli F_i ; nell'insieme di tali polinomi ve ne è (almeno) uno il cui monomio è minimo iniziale rispetto al prefissato term order: sia F tale polinomio.

Per costruzione si ha $Lm(F) = X^\beta \in In(I) = (X^{\alpha_1}, \dots, X^{\alpha_r})$ e quindi vi sono un indice $s \leq r$ e un monomio X^γ tali che $X^\beta = X^\gamma \cdot X^{\alpha_s}$. Il polinomio $F - Lc(F) \cdot X^\gamma \cdot F_s$ appartiene quindi ad I , non è combinazione degli F_j (altrimenti anche F lo sarebbe) e ha monomio iniziale minore di F , contro l'ipotesi. ■

Le proprietà sopra provate per gli ideali monomiali e le basi monomiali non valgono per ideali qualsiasi o per insiemi qualsiasi di generatori di un ideale, come mostra l'esempio seguente.

Esempio 8.21. Consideriamo l'ideale $I = (X, Y)$ di $k[X, Y]$. Si tratta di un ideale monomiale e $\{X, Y\}$ è la sua base. Per ogni intero $r \geq 1$, l'ideale I possiede anche l'insieme minimale di generatori $B_r = \{X, Y - Y^2, Y^2 - Y^3, \dots, Y^{r-1} - Y^r, Y^r\}$ costituito da $r + 2$ polinomi.

Se fissiamo ad esempio l'ordinamento *DegLex* e l'intero $r = 2$, l'insieme dei monomi iniziali di B_2 è $\{X = Lm(X), Y^2 = Lm(Y - Y^2) = Lm(Y^2)\} = \{X, Y^2\}$ che non costituisce un insieme di generatori per $In(I) = I$.

Esempio 8.22. Consideriamo come prima l'ordinamento *DegLex* e sia I l'ideale di $k[X, Y, Z]$ generato da $\{F_1 = XY - Y + 1, F_2 = Y^2Z - X\}$.

Il polinomio $G = X^2 + YZ - X$ appartiene ad I , poichè $G = YZ \cdot F_1 - (X - 1) \cdot F_2$; però $X^2 = Lm(G) \notin (XY = Lm(F_1), Y^2Z = Lm(F_2))$.

Definizione 8.23. Chiamiamo **base di Gröbner** o **base standard** di un ideale I di $k[X_1, \dots, X_n]$ (rispetto a un fissato term order) un insieme di polinomi $\{F_1, \dots, F_r\} \subset I$ tali che $(Lm(F_1), \dots, Lm(F_r)) = In(I)$.

Un base di Gröbner si dice **ridotta** se per ogni $i \leq r$ si ha $Lc(F_i) = 1$ e $Lm(F_i)$ non divide alcun monomio che compare in F_j se $j \neq i$.

Proposizione 8.24. *Ogni ideale I ha una sola base di Gröbner ridotta.*

Dimostrazione. Possiamo intanto osservare che due basi di Gröbner ridotte hanno lo stesso numero di elementi (tanti quanti ne ha l'insieme minimale di generatori monomiali di $In(I)$). Se $B_1 = \{F_1, \dots, F_r\}$ e $B_2 = \{G_1, \dots, G_r\}$ sono due basi di Gröbner ridotte, possiamo supporre, riordinando eventualmente gli indici, che $Lm(F_i) = Lm(G_i)$ per ogni $i \leq r$. Allora il polinomio $F_i - G_i$ deve essere nullo, perchè altrimenti il suo monomio iniziale, che compare in F_i oppure in G_i , dovrebbe essere multiplo di un monomio iniziale $Lm(F_j) = Lm(G_j)$, contro l'ipotesi. ■

In virtù della Proposizione 8.20, una base di Gröbner di I è anche un insieme (non necessariamente minimale) di generatori di I . Quando diremo che un insieme di polinomi B è una base di Gröbner senza specificare qual è l'ideale, l'ideale sottinteso sarà quello generato da B .

§ L'algoritmo di divisione

In questo paragrafo supporremo fissato un term order \preceq in $k[X_1, \dots, X_n]$ con la solita convenzione sull'ordine delle indeterminate.

Vogliamo estendere all'anello $k[X_1, \dots, X_n]$ l'algoritmo di divisione che in $k[X]$ porta a determinare il quoziente e il resto tra due polinomi.

Sia $B = \{F_1, \dots, F_r\}$ un insieme finito di polinomi e sia I l'ideale da essi generato. Preso un qualsiasi polinomio G possiamo considerare la sua scrittura $G = \sum_{i=1}^s c_j X^{\alpha_j}$ con $c_j \neq 0$ e $X^{\alpha_j} \succ X^{\alpha_{j-1}}$. Possiamo confrontare i monomi di G con i $Lm(F_i)$: se non ne troviamo diciamo che G **non è riducibile mediante B** ; in caso contrario operiamo un passo di riduzione di G mediante B nel modo seguente.

Sia X^{α_h} il maggiore dei monomi di G divisibile per qualche monomio iniziale dei polinomi in B : sia ad esempio

$$X^{\alpha_h} = X^\beta \cdot Lm(F_i).$$

Costruiamo il nuovo polinomio $G_1 = G - c_h X^\beta \cdot F_i$; indicheremo la relazione così ottenuta col simbolo:

$$G \xrightarrow{B} G_1.$$

Il polinomio G_1 ha gli stessi coefficienti di G per ogni monomio $X^{\alpha_j} > X^{\alpha_h}$, ma non contiene X^{α_h} . Possiamo poi ripetere il procedimento a partire da G_1 fino a che è possibile ossia fino a che non otteniamo un polinomio non ulteriormente riducibile.

Ad ogni passo si prende in considerazione un monomio più piccolo di quello esaminato al passo precedente; tali monomi formano una successione decrescente che è quindi finita, grazie al fatto che un term order è un buon ordine.

Useremo il simbolo

$$G \xrightarrow{B}_+ G'$$

per dire che con un tale procedimento possiamo passare dal polinomio G a G' .

Osservazione 8.25. Fissati un term order \preceq in \mathbb{T}^n e un insieme di polinomi $B \subset k[X_1, \dots, X_n]$, la costruzione precedente individua su $k[X_1, \dots, X_n]$ una relazione d'ordine (non totale) data da $G_1 \succeq G_2$ se $G_1 = G_2$ oppure $G_1 \xrightarrow{B} G_2$.

Analogamente possiamo costruire un grafo orientato $\mathcal{G}(B)$ i cui vertici sono i polinomi e i cui spigoli sono le relazioni $G \xrightarrow{B} G'$. In particolare fissato un polinomio G possiamo considerare il sottografo orientato $\mathcal{G}_G(B)$ su $\{G' \in k[X_1, \dots, X_n] \mid G \xrightarrow{B} G'\}$ che risulta essere un albero.

La terminologia "albero" è giustificata anche dal fatto che $\mathcal{G}_G(B)$ è in ogni caso un insieme finito. In caso contrario, potremmo considerare, nell'insieme dei polinomi G per cui $\mathcal{G}_G(B)$ è infinito, un polinomio G_0 che ha monomio iniziale minimo. Al primo passo di riduzione di G_0 si prende in considerazione $Lm(G_0)$ (in caso contrario si ottiene un polinomio con la stessa proprietà ma monomio iniziale

più piccolo cancellando $Lm(G_0)$ da G_0). Il primo passo di riduzione si può effettuare al più in $r = \text{card}(B)$ modi diversi e quindi almeno uno dei polinomi ottenuti dopo tale primo passo soddisfa la stessa proprietà e ha monomio iniziale minore, contro l'ipotesi.

Di conseguenza, in ciascun insieme $\mathcal{G}_G(B)$ vi sono solo un numero finito di possibili polinomi non ulteriormente riducibili.

Il procedimento di riduzione prima definito risulta in generale insoddisfacente, in quanto non porta a determinare un unico resto e non risolve il problema dell'ideal membership.

Esempio 8.26. Consideriamo l'ordinamento *DegLex* in $k[X, Y]$ e l'insieme di polinomi $B = \{F_1 = 2XY^2 + 4Y^2 + 3X, F_2 = Y^2 - 2Y - 2\}$.

Il polinomio $G = 2X^3Y^3 + 4Y^2$ si può ridurre ai due polinomi (entrambi non ulteriormente riducibili)

$$G_1 = -3X^3Y - 24X^2Y - 16X^2 + 8Y + 8$$

con la procedura $G_1 = (((G - X^2YF_1) + 4X^2YF_2) + 8X^2F_2) - 4F_2$, ma anche a

$$G_2 = 12X^3Y + 8X^3 + 8Y + 8$$

con la procedura $G_2 = ((G - 2X^3YF_2) - 4X^3F_2) - 4F_2$.

Il polinomio $F = F_1 - (2X + 4)F_2 = 4XY + 7X + 8Y + 8$ appartiene ovviamente all'ideale I generato da B ; però, se non conoscessimo già la sua scrittura come combinazione di F_1 e F_2 , il procedimento di riduzione non ci permetterebbe di ricavarla; anzi F non è riducibile mediante B .

Teorema 8.27. *Siano \preceq un term order in \mathbb{T}^n e $B = \{F_1, \dots, F_r\}$ un sottoinsieme finito di un ideale I di $k[X_1, \dots, X_n]$. Le seguenti affermazioni sono equivalenti:*

1. B è una base di Gröbner di I ;
2. $\forall G \in I, G \neq 0, \exists F_i \in B$ tale che $Lm(F_i)$ divide $Lm(G)$;
3. $\forall G \in I, G \neq 0$, si ha $G \xrightarrow{B}_+ 0$;
4. $\forall G \in I, G \neq 0$, si ha $G = \sum_{i=1}^r H_i F_i$ con $Lm(G) = \max_i \{Lm(H_i F_i)\}$.

Dimostrazione. 4. \implies 1. e 1. \implies 2. seguono immediatamente dalla definizione di base di Gröbner.

"2. \implies 3." Supponiamo valga 2.; allora ogni polinomio non nullo di I può essere ridotto mediante B .

Come abbiamo già visto, ogni catena di riduzioni è finita. Quindi se $G \in I$, esiste R non ulteriormente riducibile tale che $G \xrightarrow{B}_+ R$; per costruzione $R = G - \sum H_i F_i$ e quindi anche R appartiene a I . Allora $R = 0$.

“3. \implies 4.” Per come è stato definito l’algoritmo di riduzione, se $G \xrightarrow{B}_+ 0$, allora $G = \sum_{j=1}^t K_j F_{i_j}$ dove al crescere di i i monomi $Lm(K_j F_{i_j})$ sono strettamente decrescenti. In particolare $Lm(G) = Lm(K_1 F_{i_1}) = \max_j \{ Lm(K_j F_{i_j}) \}$. Raccogliendo i coefficienti di ciascun F_i otteniamo l’asserto. ■

Corollario 8.28. *Fissato un term order in \mathbb{T}^n , siano I un ideale di $k[X_1, \dots, X_n]$ e B una base di Gröbner di I .*

Allora per ogni polinomio $G \in k[X_1, \dots, X_n]$, esiste un unico polinomio non ulteriormente riducibile R tale che $G \xrightarrow{B}_+ R$.

Inoltre tale polinomio R è invariante nella classe $G + I$.

Dimostrazione. Supponiamo che si abbia $G \xrightarrow{B}_+ R$ e $G' \xrightarrow{B}_+ R'$ con $G - G' \in I$. Per come è stato definito l’algoritmo di riduzione si ha $R = G - \sum H_i F_i$ e quindi $G - R \in I$; analogamente anche $G' - R' \in I$ e quindi $R - R' \in I$.

In virtù del risultato precedente, $R - R' \xrightarrow{B}_+ 0$. Se R e R' non sono ulteriormente riducibili, allora nessun monomio che compare in essi è multiplo di uno dei $Lm(F_i)$ e anche $R - R'$ non è ulteriormente riducibile. Quindi $R - R' = 0$. ■

Definizione 8.29. L’unico polinomio non ulteriormente riducibile modulo B nella classe $G + I$ si dice **resto** (per analogia col caso di una sola indeterminata) o **forma normale** di G modulo B .

I risultati precedenti mostrano che le basi di Gröbner sono la risposta ai problemi posti all’inizio di questo capitolo. Tramite una base di Gröbner possiamo infatti sapere dopo un numero finito di passi di riduzione se un dato polinomio appartiene o meno a I e possiamo anche trovare un rappresentante speciale in ogni classe di equivalenza in $k[X_1, \dots, X_n]/I$.

§ Proiezioni e sezioni

Sia V un insieme algebrico di k^n e sia $H \cong k^{n-1}$ l’**iperpiano** definito dall’equazione $X_n = 0$.

Due metodi classici per studiare le proprietà di V sono:

- 1) **sezionare** V con H , ossia studiare l’insieme algebrico $W_1 = V \cap H$ di $H = k^{n-1}$;
- 2) **proiettare** V su H da un punto esterno P , ossia costruire il cono C su V di vertice P e studiare l’insieme algebrico $W_2 = C \cap H$.

Il corrispettivo algebrico di tali metodi geometrici è quello di studiare le proprietà di un ideale I di $k[X_1, \dots, X_n]$ attraverso quelle degli ideali J_1 e J_2 di $k[X_1, \dots, X_{n-1}]$ ottenuti nel modo seguente:

- 1) $J_1 = I + (X_n)/(X_n)$ in $k[X_1, \dots, X_n]/(X_n) \cong k[X_1, \dots, X_{n-1}]$.
- 2) $J_2 = I \cap k[X_1, \dots, X_{n-1}]$.

Volendo utilizzare tali tecniche insieme a quella degli ideali iniziali potrebbero risultare utili le seguenti proprietà di *RevLex* e *Lex*:

- 1) utilizzando \preceq_{RevLex} (con $X_n < X_{n-1} < \dots < X_1$)¹, per ogni polinomio F e per ogni indice $i \leq n$ si ha:

$$Lm(F) \in (X_i, \dots, X_n) \text{ se e soltanto se } F \in (X_i, \dots, X_n)$$

e quindi:

$$In(I) + (X_n)/(X_n) = In(I + (X_n)/(X_n)).$$

- 2) utilizzando \preceq_{Lex} (con $X_1 < X_2 < \dots < X_n$) per ogni polinomio F e per ogni indice $i \leq n$ si ha:

$$Lm(F) \in k[X_1, \dots, X_i] \text{ se e soltanto se } F \in k[X_1, \dots, X_i]$$

e quindi:

$$(In(I) \cap k[X_1, \dots, X_{n-1}]) = In(I \cap k[X_1, \dots, X_{n-1}]).$$

Nel caso in cui si lavori con varietà proiettive e quindi con ideali omogenei e polinomi omogenei le stesse proprietà valgono relativamente a *DegRevLex* e *DegLex* rispettivamente.

¹Si noti che *RevLex* è un ordinamento totale dei monomi, ma non un term order.

Estensioni di anelli e algebre affini

§ Algebre

Definizione 9.1. Sia A un anello. Si dice A -algebra un anello B dotato di un omomorfismo di anelli $\phi: A \rightarrow B$. Mediante ϕ rimane indotta su B la struttura di A -modulo per restrizione degli scalari ossia la struttura di A -modulo, compatibile con quella di anello su B , data per ogni $a \in A$ e $b \in B$ da:

$$a \cdot b = \phi(a)b$$

dove il prodotto a secondo membro è il prodotto in B .

Esempio 9.2. Gli anelli di polinomi $A[X_1, \dots, X_n]$, di serie formali $A[[X_1, \dots, X_n]]$ e di funzioni razionali $A(X_1, \dots, X_n)$ sono esempi importanti di A -algebre, in cui l'omomorfismo ϕ è l'immersione canonica di A come sottoanello delle costanti.

Esempio 9.3. Se \mathfrak{a} è un ideale di A , l'anello quoziente $B = A/\mathfrak{a}$ è in modo naturale una A -algebra prendendo come omomorfismo ϕ la proiezione sul quoziente.

Esempio 9.4. Ogni anello B è in modo naturale e unico una \mathbb{Z} -algebra, prendendo come ϕ l'omomorfismo intero.

In questo capitolo ci occuperemo essenzialmente del caso in cui A è un campo k .

Definizione 9.5. Una A -algebra B si dice **finita** se B è un A -modulo finitamente generato.

Definizione 9.6. Una A -algebra B si dice **finitamente generata** se esiste un epimorfismo:

$$\pi: A[X_1, \dots, X_n] \rightarrow B$$

che estende l'omomorfismo ϕ che definisce la struttura di A -algebra su B . Le immagini b_i delle indeterminate X_i si dicono generatori di B come A -algebra.

Se b_1, \dots, b_n sono generatori di B come A -algebra, allora B coincide con l'estensione di $A' = \phi(A)$ con b_1, \dots, b_n ; scriveremo quindi $B = A'[b_1, \dots, b_n]$.

Proposizione 9.7. *Se B è una A -algebra finita, allora è anche a maggior ragione una A -algebra finitamente generata.*

Nel caso in cui $A = k$ è un campo, l'omomorfismo ϕ è necessariamente iniettivo e usualmente si scrive $B = k[b_1, \dots, b_n]$. Se $\mathfrak{a} = \text{Ker}(\pi)$, allora per il primo teorema di omomorfismo ogni k -algebra finitamente generata è (isomorfa a un anello) del tipo $k[X_1, \dots, X_n]/\mathfrak{a}$. Poiché gli anelli delle coordinate delle varietà algebriche affini sono di questo tipo, ogni k -algebra finitamente generata si dice anche **k -algebra affine**.

Lemma 9.8. *Siano $A \subseteq B$ due k -algebre tali che B è una k -algebra affine ed è anche un A -modulo finito. Allora A è una k -algebra affine.*

Dimostrazione. Per ipotesi si ha $B = k[b_1, \dots, b_n]$ ed anche $B = \beta_1 A + \dots + \beta_r A$ per opportuni elementi $b_i, \beta_j \in B$. Allora per ogni $i = 1, \dots, n$ abbiamo una relazione:

$$b_i = \sum a_{ij} \beta_j \quad \text{per opportuni } a_{ij} \in A$$

e per ogni j, j' abbiamo una relazione:

$$\beta_j \beta_{j'} = \sum c_{jj'h} \beta_h \quad \text{per opportuni } c_{jj'h} \in A.$$

Ogni elemento di B può essere quindi scritto come una espressione polinomiale di grado 1 nelle β_j a coefficienti nella k -algebra affine $A_0 = k[a_{ij}, c_{jj'h}]$. L'anello B è quindi anche un A_0 -modulo finitamente generato e quindi noetheriano. Allora ogni suo sotto- A_0 -modulo è finitamente generato: in particolare lo è A . Se $\alpha_1, \dots, \alpha_m$ sono generatori di A come A_0 modulo, allora $A = k[a_{ij}, c_{jj'h}, \alpha_t]$ è una k -algebra affine. ■

Esempio 9.9. L'anello dei polinomi $k[X_1, \dots, X_n]$ è ovviamente una k -algebra finitamente generata, ma non è finita. Se $R = k$ è un campo, la struttura di k -modulo non è altro che la struttura di k -spazio vettoriale e, come è ben noto, $k[X_1, \dots, X_n]$ non ha dimensione finita su k .

§ Anelli graduati

Definizione 9.10. Un **anello graduato** B è un anello dotato di una struttura di algebra su un suo sottoanello B_0 e di una decomposizione in somma diretta $B = \bigoplus_i B_i$ dove ogni B_i è un B_0 -sottomodulo di B e per ogni $a \in B_i$ e $b \in B_j$ si ha $ab \in B_{i+j}$.

Esempio 9.11. L'anello dei polinomi $S = k[X_1, \dots, X_n]$ può essere pensato come anello graduato in molti modi. Quello più naturale è $S = \bigoplus_{i \in \mathbb{N}} S_i$ dove S_i è il k -spazio vettoriale dei **polinomi omogenei** di grado i rispetto alla graduazione (totale) standard. Se non diversamente specificato, intenderemo sempre S dotato della struttura di anello graduato in questo modo.

Vi sono però tanti altri modi diversi. Uno tra i tanti è quello di prendere $S_0 = k[X_1, \dots, X_{n-1}]$ e $S_i = X_n^i S_0$ sottomodulo dei polinomi omogenei di grado i rispetto alla graduazione nella sola indeterminata X_n .

Definizione 9.12. Sia $S = \bigoplus_i S_i$ un anello graduato. Un elemento $a \in S$ si dice **omogeneo** se esiste $i \in \mathbb{N}$ tale che $a \in S_i$. La definizione di somma diretta impone che per ogni $i \neq j$ si abbia $S_i \cap S_j = \{0\}$. Per ogni elemento omogeneo $a \neq 0$ esiste quindi un solo indice i tale che $a \in S_i$: si dice allora che i è il **grado** di a . Ogni elemento non nullo $s \in S$ ha una e una sola scrittura $s = \sum_i s_i$ con s_i omogenei di grado i e $s_i = 0$ per ogni i maggiore di un certo intero $n = n(s)$; le s_i si dicono le **componenti omogenee** di s e il minimo intero n si dice **grado** di s .

Proposizione 9.13. Sia I un ideale di un anello graduato S . Le seguenti condizioni sono equivalenti:

- 1) per ogni $s \in I$, si ha anche $s_i \in I$ per ogni componente omogenea s_i di s ;
- 2) $I = \bigoplus_i (I \cap S_i)$;
- 3) I ha un insieme di generatori formato da elementi omogenei;
- 4) l'anello quoziente S/I ha una struttura naturale di anello graduato indotta da quella di S .

Dimostrazione. “1) \implies 2)” segue immediatamente dalla definizione di somma diretta.

“2) \implies 3)” segue subito dall'osservazione che I è generato dall'insieme di elementi omogenei $\bigcup_i (I \cap S_i)$. Più generalmente, dato un insieme qualsiasi di generatori di I , si può ottenere un insieme di generatori omogenei prendendo l'insieme di tutte le componenti omogenee dei generatori.

“3) \implies 1)” Se I ha un insieme di generatori omogenei e $s \in I$, allora si ha $s = h_1 f_1 + \dots + h_r f_r$ con f_j elementi di un insieme di generatori omogenei di I e $h_j \in S$; se si scrive ogni coefficiente h_j come somma delle sue componenti omogenee e si usa la proprietà distributiva, si ottiene una scrittura di s come somma di addendi omogenei ciascuno dei quali ha uno degli f_j come fattore. La componente omogenea di ciascun grado l di s si ottiene sommando tra loro tutti gli addendi di grado l ; quindi ogni componente omogenea di s è combinazione degli f_j e dunque appartiene a I .

“1) \iff 4)” Supponiamo che I soddisfi la condizione 1) e indichiamo con π la proiezione canonica di S nel quoziente S/I . Proviamo che ogni classe $\bar{s} \in S/I$

ha una unica scrittura come somma di classi $\bar{s}_i \in \pi(S_i)$. Una scrittura si ottiene da quella di $s \in S$ come $s = s_1 + \dots + s_r$ con $s_j \in S_j$. Per provare che tale scrittura è unica basta provare che $\bar{0}$ ha una sola scrittura. Se $\bar{0} = \bar{a}_1 + \dots + \bar{a}_r$, allora $a_1 + \dots + a_r \in I$ e quindi $a_j \in I$ per ogni j . Allora $\bar{a}_j = \bar{0}$ e l'affermazione è provata.

Se viceversa I non soddisfa la condizione 1) esisterà un elemento $s \in I$ non omogeneo tale che una sua componente omogenea s_i non appartiene a I . Allora S/I non potrebbe ereditare da S la struttura di anello graduato poichè $\bar{s}_i = \overline{s - s_i} \neq \bar{0}$ dovrebbe avere due diverse scritture come somma di componenti omogenee. ■

Definizione 9.14. Un ideale I di un anello graduato S per cui valgono le condizioni equivalenti della Proposizione precedente si dice **ideale omogeneo**.

Definizione 9.15. Una k -algebra graduata B è un anello graduato $B = \bigoplus_i B_i$ tale che B_0 è una k -algebra e ogni B_i è un k -spazio vettoriale.

Possiamo estendere la nozione di funzione di Hilbert, già introdotta per gli anelli di polinomi (cfr. Esempio 6.30), al caso delle k -algebre graduate.

Se $B = \bigoplus_i B_i$ è una k -algebra graduata, la sua **funzione di Hilbert** è la funzione intera:

$$f: \mathbb{N} \longrightarrow \mathbb{N} \cup \{\infty\} \quad \text{data da} \quad f(i) = \dim_k B_i.$$

Nel caso in cui B sia una k algebra affine graduata, ossia $B = k[X_1, \dots, X_n]/I$ con I ideale omogeneo, allora $\dim(B_i) < \infty$ e quindi come codominio si può prendere \mathbb{N} .

§ Estensioni algebriche e trascendenti

La locuzione “estensione” può risultare ambigua poichè si parla di estensione di un anello ed anche di estensione di un campo (che è anche un anello). Il significato nei due casi è però differente. Se A è sottoanello di B e $x \in B$, l'estensione $A[x]$ dell'anello A con x è costituita da tutte le espressioni polinomiali $a_0 + a_1x + \dots + a_nx^n$ con $a_i \in A$; nel caso in cui $A = k$ e $B = K$ siano campi, l'estensione di campi $k(x)$ di k con x è il minimo campo che contiene $k[x]$ e quindi vi appartengono tutte le espressioni $\frac{a_0 + a_1x + \dots + a_nx^n}{c_0 + c_1x + \dots + c_mx^m}$, con $a_i, c_j \in k$, e denominatore non nullo.

I due tipi di estensioni coincidono nel caso di estensioni algebriche.

Lemma 9.16. *Sia $k[x]$ una estensione algebrica del campo k . Allora $k[x]$ è un k -modulo (= k -spazio vettoriale) finitamente generato.*

Se inoltre $k[x]$ è un dominio, allora è un campo e quindi $k[x] = k(x)$.

Dimostrazione. Per la prima affermazione basta osservare che se $F(X) \in k[X]$ è un polinomio non nullo tale che $F(x) = 0$ e d è il suo grado, allora $1, x, \dots, x^{d-1}$ è un insieme di generatori di $k[x]$ come k -modulo.

Supponiamo ora che $k[x]$ sia un dominio. Per ipotesi l'applicazione:

$$\pi : k[X] \rightarrow k[x] \text{ data da } X \mapsto x$$

ha nucleo non nullo: sia $(F) = \text{Ker}(\pi)$. Quindi $k[x]$ è un dominio se e soltanto se F è un polinomio irriducibile, ossia se e soltanto se (F) è un ideale massimale. ■

Definizione 9.17. Sia F un campo che è una estensione del campo k . Si dice che F ha **grado di trascendenza** finito r su k , in simboli $\text{trdeg}_k(F) = r$, se r è il massimo intero per il quale esiste un monomorfismo:

$$\phi : k(X_1, \dots, X_r) \hookrightarrow F.$$

Gli elementi $\phi(X_1), \dots, \phi(X_n)$ si dicono algebricamente indipendenti su k .

Non approfondiamo la teoria delle estensioni di campo (per la quale rimandiamo ad esempio al libro: Hungerford Algebra); ricordiamo soltanto, perché ci saranno utili in seguito queste due proprietà nel caso in cui $F = k(x_1, \dots, x_n)$:

- i) se $r = \text{trdeg}_k(F)$, allora $r \leq n$;
- ii) si possono riordinare le variabili in modo che x_1, \dots, x_r siano algebricamente indipendenti su k e ogni x_i con $i > r$ (e quindi tutto F) sia algebrico su $k(x_1, \dots, x_r)$.

Definizione 9.18. Se A è una estensione dell'anello B , gli elementi a_1, \dots, a_n di A si dicono **algebricamente indipendenti** su B se non esiste alcun polinomio non nullo $F \in B[X_1, \dots, X_n]$ tale che $F(a_1, \dots, a_n) = 0$.

Equivalentemente potremmo dire che a_1, \dots, a_n sono algebricamente indipendenti se l'omomorfismo di B -algebre $\phi : B[X_1, \dots, X_n] \rightarrow A$ data da $\phi(X_i) = a_i$ è iniettivo e quindi identifica il sottoanello $B[a_1, \dots, a_n]$ di A con l'anello dei polinomi $B[X_1, \dots, X_n]$.

Lemma 9.19. Sia $A = k[x_1, \dots, x_n]$ un dominio e sia $K(A)$ il suo campo dei quozienti. Il massimo numero di elementi algebricamente indipendenti di A è $r = \text{trdeg}_k K(A)$ e quindi $r \leq n$.

Dimostrazione. Basta osservare che un insieme di elementi di A algebricamente indipendenti su k lo è anche se lo consideriamo come sottoinsieme di $K(A)$ e che, viceversa, possiamo scegliere r elementi algebricamente indipendenti tra gli x_i e quindi in A poiché $K(A) = k(x_1, \dots, x_n)$. ■

Lemma 9.20. Se X è trascendente sul campo k , il campo $k(X)$ non è una k -algebra affine.

Dimostrazione. Supponiamo per assurdo che lo sia, ossia $k(X) = k[y_1, \dots, y_n]$. Allora le y_i si possono esprimere come funzioni razionali in X della forma:

$$y_i = \frac{F_i(X)}{G(X)}$$

dove si è supposto di avere messo denominatore comune. In tal caso la funzione razionale $\frac{1}{XG(X)+1}$ si dovrebbe poter scrivere come una espressione polinomiale $H(y_1, \dots, y_n)$ a coefficienti in k , da cui si ricaverebbe l'uguaglianza tra funzioni razionali:

$$\frac{1}{XG(X)+1} = \frac{H'(F_1, \dots, F_n, G)}{G^s} = \frac{H''(X)}{G^s}$$

e quindi l'uguaglianza tra polinomi: $G^s = (XG + 1)H''$ chiaramente impossibile poiché $XG + 1$ non è invertibile e non ha alcun fattore in comune con G . ■

Proposizione 9.21. *Se X è una indeterminata su k , il campo $k(X)$ non è sottoalgebra di alcuna k -algebra affine.*

Dimostrazione. Supponiamo per assurdo che esista una inclusione $k(X) \subseteq k[y_1, \dots, y_n]$. Se \mathfrak{m} è un ideale massimale di $k[y_1, \dots, y_n]$, componendo con la proiezione sul quoziente $k[y_1, \dots, y_n]/\mathfrak{m}$ otterremmo una immersione di $k(X)$ in un campo che è anche una k -algebra affine: supponiamo allora che già $k[y_1, \dots, y_n]$ lo sia. Proviamo che una tale inclusione non esiste.

Sia per assurdo $f: k(X) \rightarrow B = k[y_1, \dots, y_n] = K(B)$ e indichiamo con A il campo $k(X)$.

Se tutte le y_i fossero algebriche su k , allora ogni elemento di B sarebbe algebrico su k , mentre l'inclusione $k[X] \subseteq B$ prova che in B vi è almeno un elemento trascendente su k .

Allora almeno una delle y_i deve essere trascendente su k : supponiamo che y_1, \dots, y_r siano algebricamente indipendenti su k e y_{r+1}, \dots, y_n algebriche sul campo $k(y_1, \dots, y_r)$.

Sostituendo se $r > 1$ il campo k col campo $k(y_1, \dots, y_{r-1})$, possiamo supporre $r = 1$.

La k algebra affine $k[y_1, \dots, y_n] = k(y_1)[y_2, \dots, y_n]$ è quindi un $k(y_1)$ -modulo finitamente generato; segue allora dal Lemma 9.8 che $k(y_1)$ è una k -algebra affine, in contrasto con quanto prima dimostrato. ■

Concludiamo questo capitolo col risultato di cui vedremo le importantissime conseguenze geometriche nel prossimo capitolo.

Corollario 9.22. *Sia \mathfrak{m} un ideale massimale di $k[X_1, \dots, X_n]$. Allora $k[X_1, \dots, X_n]/\mathfrak{m}$ è una estensione algebrica di k e quindi è un k -spazio vettoriale finitamente generato e per ogni $i \leq n$ esiste un polinomio $F_i \in \mathfrak{m}$ nella sola indeterminata X_i .*

Dimostrazione. Se una delle classi $x_{i_0} = \overline{X_{i_0}}$ fosse trascendente su k , allora il monomorfismo $k[X] \hookrightarrow k[X_1, \dots, X_n]/\mathfrak{m}$ dato da $X \mapsto x_{i_0}$ si estenderebbe ad una immersione di campi $k(X) \hookrightarrow k[X_1, \dots, X_n]/\mathfrak{m}$, in contrasto col Lemma 9.21. Allora ogni classe x_i è radice di un qualche polinomio $F_i(X) \in k[X]$ ossia $F_i(x_i) \in \mathfrak{m}$.

Se infine $\partial F_i = r_i$, un insieme finito di generatori di $k[X_1, \dots, X_n]/\mathfrak{m}$ come k -spazio vettoriale è dato dall'insieme $\{x_1^{m_1} \cdots x_n^{m_n} \mid m_1 \leq r_1, \dots, m_n \leq r_n\}$. ■

Nullstellensatz e normalizzazione

§ Il teorema degli zeri di Hilbert

Vediamo ora come dai risultati algebrici precedenti seguano importanti proprietà delle varietà algebriche affini e dei relativi ideali associati.

Teorema 10.1 (Nullstellensatz debole). *Sia k un campo algebricamente chiuso. Se I è un ideale proprio di $k[X_1, \dots, X_n]$, allora $\mathcal{V}(I) \neq \emptyset$.*

Dimostrazione. Supponiamo I proprio e sia \mathfrak{m} un ideale massimale che lo contiene. Poiché $\mathcal{V}(I) \supseteq \mathcal{V}(\mathfrak{m})$, sarà sufficiente provare l'asserto per l'ideale \mathfrak{m} . In virtù del Corollario 9.22, il quoziente $k[X_1, \dots, X_n]/\mathfrak{m}$ è una estensione algebrica di k e quindi, essendo k algebricamente chiuso, coincide con k stesso. Se a_i è l'elemento di k rappresentante della classe $\overline{X_i}$, allora $\overline{X_i - a_i} = 0$ e quindi $X_i - a_i \in \mathfrak{m}$. Poiché $(X_1 - a_1, \dots, X_n - a_n)$ è un ideale massimale ed è contenuto in \mathfrak{m} , non può che coincidere con \mathfrak{m} stesso e quindi $\mathcal{V}(\mathfrak{m}) = \{(a_1, \dots, a_n)\}$. ■

Corollario 10.2. *Sia k un campo algebricamente chiuso. Se $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$ è un ideale massimale di $k[X_1, \dots, X_n]$, allora la base di Gröbner ridotta di \mathfrak{m} rispetto ad un qualsiasi term order è $\{X_1 - a_1, \dots, X_n - a_n\}$*

Dimostrazione. Sia \leq un qualsiasi term order; possiamo supporre, a meno di un cambiamento di indici che $X_1 < \dots < X_n$. Allora $X_1 - a_1$ è l'elemento (non nullo) di \mathfrak{m} con termine iniziale minore e quindi deve far parte della base di Gröbner ridotta.

Se $n = 1$ la tesi è così provata.

Sia allora $n > 1$ e procediamo per discesa su n . Una volta provato che $X_1 - a_1, \dots, X_r - a_r$ appartengono alla base ridotta di \mathfrak{m} , in ogni altro elemento della base ridotta non compaiono monomi contenenti alcuna delle variabili X_1, \dots, X_r . Poiché $X_{r+1} - a_{r+1} \in \mathfrak{m}$, tale elemento è sicuramente tra gli elementi ridotti rispetto a $X_1 - a_1, \dots, X_r - a_r$ quello con termine iniziale minore e quindi deve a sua volta fare parte della base di ridotta. ■

In modo del tutto analogo a quanto visto sopra possiamo provare il seguente risultato più generale:

Corollario 10.3. *Se \mathfrak{m} è un ideale massimale di $k[X_1, \dots, X_n]$. Se consideriamo il term order Lex tale che $X_\nu < X_i$ per ogni $i \neq \nu$ allora nella base di Gröbner ridotta di \mathfrak{m} compare un polinomio irriducibile F_ν nella sola variabile X_ν .*

Dimostrazione. Osserviamo che in \mathfrak{m} vi è un solo polinomio monico irriducibile F_ν nella sola indeterminata X_ν (F_ν è il generatore monico dell'ideale primo e non nullo $\mathfrak{m} \cap k[X_\nu]$ di $k[X_\nu]$). Infatti in un polinomio il cui monomio iniziale sia del tipo X_ν^s non può comparire alcuna altra indeterminata. ■

Contrariamente al caso del campo algebricamente chiuso, però, non è vero in generale che i polinomi monici e irriducibili $F_i(X_i) \in \mathfrak{m}$ costituiscano da soli una base di Gröbner di \mathfrak{m} .

Esempio 10.4. Consideriamo l'ideale $I = (X + Y, Y^2 + 1)$ di $\mathbb{R}[X, Y]$. Tale ideale contiene oltre a $Y^2 + 1$ anche il polinomio $X^2 + 1$ nella sola indeterminata X , ma l'unica base di Gröbner ridotta rispetto a ogni term order in cui $Y < X$ è $\{X + Y, Y^2 + 1\}$ e l'unica base di Gröbner ridotta rispetto a ogni term order in cui $X < Y$ è $\{Y + X, X^2 + 1\}$.

Definizione 10.5. Un anello A si dice **di Jacobson** se ogni suo ideale primo è l'intersezione di tutti i massimali che lo contengono:

$$\mathfrak{p} = \bigcap_{\mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m}.$$

Proposizione 10.6. *L'anello dei polinomi $k[X_1, \dots, X_n]$ a coefficienti in un campo è di Jacobson.*

Dimostrazione. Sia \mathfrak{p} un primo di $A = k[X_1, \dots, X_n]$ e sia $\mathfrak{q} = \bigcap \mathfrak{m}_\alpha$, dove gli \mathfrak{m}_α sono tutti i massimali di A che contengono \mathfrak{p} . Ovviamente si ha $\mathfrak{p} \subseteq \mathfrak{q}$. Proviamo che vale anche l'inclusione inversa.

Supponiamo esista un polinomio $F \in \mathfrak{q} \setminus \mathfrak{p}$. Se $B = A/\mathfrak{p}$ e f è la classe di F in B , allora $fY + 1$ considerato come polinomio nella sola Y nel dominio $B[Y]$ non è invertibile (cfr. Proposizione 6.23) e quindi esiste un ideale massimale \mathfrak{n} che lo contiene. L'ideale $\mathfrak{m} = \pi^{-1}(\mathfrak{n})$, dove $\pi: A[Y] \rightarrow B[Y]$ è la proiezione canonica, è massimale in A e quindi, per il Teorema 10.3, contiene dei polinomi $F_i(X_i)$ ciascuno nella sola variabile X_i . Quindi anche $\mathfrak{m} \cap A$ è massimale (poiché è primo e contiene i polinomi $F_i(X_i)$: cfr. Lemma 9.16) e contiene anche \mathfrak{p} , ossia $\mathfrak{m} \cap A = \mathfrak{m}_\alpha$ per un qualche α . In tal caso $F \in \mathfrak{m}_\alpha \subseteq \mathfrak{m}$ e d'altra parte $FY + 1 \in \mathfrak{m}$, in contrasto col fatto che \mathfrak{m} è proprio. ■

Corollario 10.7. *Ogni ideale radicale di $k[X_1, \dots, X_n]$ è intersezione dei massimali che lo contengono.*

Dimostrazione. Segue subito ricordando che gli ideali radicali sono l'intersezione dei primi che li contengono. ■

Teorema 10.8 (Nullstellensatz forte). *Sia k un campo algebricamente chiuso. Se I è un ideale di $k[X_1, \dots, X_n]$, allora $\mathcal{I}(\mathcal{V}(I)) = \sqrt{I}$.*

Dimostrazione. Abbiamo già visto che $\mathcal{I}(\mathcal{V}(I)) \supseteq \sqrt{I}$. Ci basta allora provare l'inclusione inversa. Sia $F \in \mathcal{I}(\mathcal{V}(I))$; allora F si annulla se valutato in ogni punto di $(a_1, \dots, a_n) \in \mathcal{V}(I)$ e quindi $F \in (X_1 - a_1, \dots, X_n - a_n)$ per ogni ideale massimale $\mathfrak{m} = (X_1 - a_1, \dots, X_n - a_n)$ contenente I . D'altra parte tutti gli ideali massimali di $k[X_1, \dots, X_n]$ sono di questo tipo e quindi $F \in \mathfrak{m}$ per ogni massimale contenente I . Allora $F \in \bigcap_{\mathfrak{m} \supseteq I} \mathfrak{m} = \bigcap_{\mathfrak{m} \supseteq \sqrt{I}} \mathfrak{m} = \sqrt{I}$ dove l'ultima eguaglianza segue dal Corollario 10.7. ■

Se k è algebricamente chiuso, otteniamo così una corrispondenza biunivoca tra le varietà algebriche affini di k^n e gli ideali radicali di $A = k[X_1, \dots, X_n]$ ed in particolare tra le varietà irriducibili e gli ideali primi di A . Se poi consideriamo una varietà $V = \mathcal{V}(I) \subseteq k^n$ e il suo anello delle coordinate $k[V] = A/\mathcal{I}(V)$, il Nullstellensatz stabilisce anche una corrispondenza biunivoca tra i punti di V e gli ideali massimali di $k[V]$, in quanto questi ultimi corrispondono biunivocamente ai massimali di A contenenti I (o equivalentemente contenenti $\sqrt{I} = \mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(V)$).

§ Il Lemma di Normalizzazione di Noether

In questo paragrafo vedremo un modo alternativo per dimostrare il Nullstellensatz, che ci permetterà di dare una definizione puramente algebrica di dimensione di una varietà. Ci limiteremo per semplicità a considerare il caso dei domini, anche se molto di quello che diremo vale più in generale.

Definizione 10.9. Sia A una estensione di un anello B e sia $a \in A$. Diremo che a è **intero** su B se esiste un polinomio monico $F(X) \in B[X]$ tale che $F(a) = 0$.

Se $B = k$ è un campo, chiaramente le nozioni di algebrico e di intero sono equivalenti, ma in generale “algebrico \Rightarrow intero”, ma non viceversa. Ad esempio tutti gli elementi di $\mathbb{Q} \setminus \mathbb{Z}$ sono algebrici su \mathbb{Z} , ma nessuno di essi è intero su \mathbb{Z} .

Proposizione 10.10. *Sia A una estensione di un anello B e sia $a \in A$. Le seguenti condizioni sono equivalenti:*

- (i) a è intero su B ;
- (ii) $B[a]$ è un B -modulo finitamente generato;
- (iii) $B[a]$ è contenuto in una B -algebra C di A finitamente generata come B -modulo.

Dimostrazione. “(i) \Rightarrow (ii)” Se $F(X) = X^s + b_1 X^{s-1} + \dots + b_s$ è un polinomio di $B[X]$ tale che $F(a) = 0$, allora $B[a]$ è generato su B da $1, a, \dots, a^{s-1}$.

“(ii) \Rightarrow (iii)” Basta prendere $C = B[s]$.

“(iii) \Rightarrow (i)” Siano c_1, \dots, c_m generatori di C come B -modulo. Poiché $ac_i \in C$, esistono delle relazioni $ac_i = \sum_j b_{ij}c_j$, che possiamo anche scrivere, usando il simbolo di Kronecker, come $\sum_j (\delta_{ij}a - b_{ij})c_j = 0$ con $b_{ij} \in B$. Se b è il determinante della matrice dei coefficienti delle c_j , allora $bc_j = 0$ per ogni $j = 1, \dots, m$ e quindi $bC = 0$. Poiché $1 \in C$, allora $b = 0$. Sostituendo una indeterminata ad a , il determinante della matrice $(\delta_{ij}X - b_{ij})$ è un polinomio monico di $B[X]$ che si annulla in a , come volevasi. ■

I quattro risultati seguenti si possono facilmente dedurre dalla Proposizione 10.10.

Corollario 10.11. *Se A è una estensione di B finitamente generata come B -modulo, allora A è una estensione intera di B ossia ogni suo elemento è intero su B .*

Corollario 10.12. *Se A è una estensione intera di B e B è una estensione intera di D , allora A è una estensione intera di D .*

Corollario 10.13. *Se A è una estensione di B e a_1, \dots, a_n sono elementi di A interi su B , allora $B[a_1, \dots, a_n]$ è una estensione intera di B finitamente generata come B -modulo.*

Teorema 10.14. *Sia A una estensione di B e sia C il sottoinsieme degli elementi di A che sono interi su B . Allora C è un sottoanello di A (che ovviamente è intero su B che contiene ogni sottoanello di A intero su B).*

Definizione 10.15. L'anello C definito dall'enunciato precedente si dice **chiusura integrale** di B in A . Se $C = B$, B si dice **integralmente chiuso** in A . Un dominio B si dice integralmente chiuso, se lo è nel suo campo delle frazioni $K(B)$.

Teorema 10.16 (Lemma di Normalizzazione di Noether). *Sia $A = k[x_1, \dots, x_n]$ una k -algebra affine, integra, e sia $r = \text{trdeg}_k(A)$. Allora si possono determinare degli elementi $y_1, \dots, y_n \in A$ tali che $A = k[y_1, \dots, y_n]$, y_1, \dots, y_r siano algebricamente trascendenti su k e, per ogni $i > r$, y_i sia intero su $k[y_1, \dots, y_{i-1}]$.*

Dimostrazione. Se x_1, \dots, x_n sono algebricamente indipendenti su k , non c'è nulla da provare.

Supponiamo allora che x_n sia algebrico su $k[x_1, \dots, x_{n-1}]$. Proviamo che è possibile determinare degli elementi $y_1, \dots, y_{n-1} \in A$ tali che $A = k[y_1, \dots, y_{n-1}][y_n]$ e y_n sia intero su $k[y_1, \dots, y_{n-1}]$.

Per ipotesi esiste un polinomio $F(X_1, \dots, X_n)$ tale che $F(x_1, \dots, x_n) = 0$: sia $F = \sum_j c_j X^{\alpha_j}$, dove $\alpha_j = (\alpha_{j1}, \dots, \alpha_{jn})$ è la sequenza degli esponenti di ciascun monomio. Operiamo la sostituzione $Y_n = X_n$ e $Y_i = X_i - X_n^{p_i}$ per ogni $i < n$, dove p è un numero naturale maggiore di tutti gli α_{ji} .

Notiamo che la sostituzione operata si inverte ($X_i = Y_i + Y_n^{p^i}$) e quindi se definiamo $y_n = x_n$ e $y_i = x_i - x_n^{p^i}$ si ha $k[x_1, \dots, x_n] = k[y_1, \dots, y_n]$.

Da ciascun monomio di F $c_j X^{\alpha_j} = c_j \prod X_i^{\alpha_{ji}}$ di F si ottiene $c_j \prod (Y_i + Y_n^{p^i})^{\alpha_{ji}}$ che sviluppato si trasforma in una somma di monomi; tra questi quello di grado maggiore è la potenza di Y_n con esponente $\beta_j = \alpha_{j1}p + \alpha_{j2}p^2 + \dots + \alpha_{jn}p^n$. Per la scelta fatta di p , gli esponenti di questi monomi di grado massimo sono tutti diversi al variare della sequenza dei coefficienti (si pensi alla scrittura posizionale in base p dei numeri naturali). Sia β_{j_0} il massimo degli esponenti.

Il polinomio $F(X_1, \dots, X_n)$ mediante il cambio di variabili si trasforma in un polinomio $G(Y_1, \dots, Y_n)$ il cui termine di grado massimo è $c_{j_0} Y_n^{\beta_{j_0}}$, tale che $G(y_1, \dots, y_n) = 0$. Allora $c_{j_0}^{-1} G(y_1, \dots, y_{n-1}, Y)$ è un polinomio monico di $k[y_1, \dots, y_{n-1}][Y]$ che si annulla in y_n .

Se $n = 1$ la tesi è così completamente provata. Se $n > 1$ e supponiamo che l'asserto sia vero per $n - 1$, allora $A' = k[y_1, \dots, y_{n-1}]$ si può scrivere come $A' = k[z_1, \dots, z_r][z_{r+1}, \dots, z_{n-1}]$ con z_i interi su $k[z_1, \dots, z_r]$ per ogni $i = r + 1, \dots, n - 1$. Poiché y_n è intero su A' e A' è intero su $k[z_1, \dots, z_r]$, si conclude in virtù del Corollario 10.12 ■

La dimostrazione presentata è essenzialmente dovuta a Nagata. Vi sono altre dimostrazioni in cui si utilizzano cambi lineari di variabili, forse intuitivamente più semplici, ma meno generali poiché richiedono l'ulteriore ipotesi che il campo k sia infinito.

Sia \mathfrak{p} un ideale primo di $k[X_1, \dots, X_n]$ e siano $A = k[X_1, \dots, X_n]/\mathfrak{p}$ e $K = K(A)$. Scelto il term order Lex con $X_1 < X_2 < \dots < X_n$, sia F_1, \dots, F_h la base di Gröbner di \mathfrak{p} . Le classi x_1, \dots, x_n sono algebricamente indipendenti se e soltanto se in \mathfrak{p} non vi è alcun polinomio non nullo nelle sole variabili X_1, \dots, X_r e quindi se e soltanto se non vi è alcun monomio nelle sole variabili X_1, \dots, X_r tra i monomi $Lm(F_i)$. Cambiando l'ordine delle variabili, si possono determinare il numero $r = \text{trdeg}_k(K(A))$ e un insieme di r tra le x_i che siano algebricamente indipendenti.

La dimostrazione del Lemma di Normalizzazione indica poi un metodo costruttivo per trovare gli $n - r$ elementi interi.

Sia V una varietà irriducibile di k^n . Indichiamo con $k[V]$ l'anello delle coordinate di V e con $k(V) = K(k[V])$ il campo delle funzioni razionali su V . Se $r = \text{trdeg}_k(k(V))$, grazie al Lemma di Normalizzazione possiamo scrivere $k[V]$ come $k[X_1, \dots, X_r][x_{r+1}, \dots, x_n] = k[X_1, \dots, X_n]/\mathfrak{p}$ con X_1, \dots, X_r algebricamente indipendenti su k e x_i intere su $k[X_1, \dots, X_r]$ per ogni $i > r$.

Teorema 10.17. *Nelle ipotesi precedenti la funzione:*

$$\phi : V \rightarrow k^r \text{ data da } \phi(a_1, \dots, a_n) = (a_1, \dots, a_r)$$

è suriettiva e a fibre finite.

Dimostrazione. Proviamo inanzi tutto che ϕ è suriettiva. Sia (a_1, \dots, a_r) un qualsiasi punto in k^r e proviamo che esistono degli elementi a_{i+1}, \dots, a_n tali che $P = (a_1, \dots, a_n) \in V$.

Usiamo ora il seguente classico risultato la cui dimostrazione sarà oggetto di seminari:

Teorema 10.18. *Siano A e B anelli, B intero su A e sia \mathfrak{p} un ideale primo di A . Allora esiste un ideale primo \mathfrak{q} di B tale che $\mathfrak{q} \cap A = \mathfrak{p}$.*

Applichiamo tale risultato agli anelli $A = k[X_1, \dots, X_r]$ e $B = k[V]$ che possiamo scrivere come $B = k[X_1, \dots, X_r][x_{r+1}, \dots, x_n] = A[x_{r+1}, \dots, x_n]$ con ciascuna x_i intera su A , e all'ideale primo $\mathfrak{p} = (X_1 - a_1, \dots, X_r - a_r)$ di A . Esiste allora un ideale primo \mathfrak{q} di B che contiene \mathfrak{p} e quindi contiene gli elementi $X_1 - a_1, \dots, X_r - a_r$. Poiché B è intero su A , per ogni x_i con $i > r$ esiste un polinomio $F_i \in k[X_1, \dots, X_r][T]$ (monico in T) tale che $F(X_1, \dots, X_r, x_i) \in \mathfrak{q}$ e quindi anche $F_i(a_1, \dots, a_r, x_i) \in \mathfrak{q}$.

Poiché il campo k è algebricamente chiuso, il polinomio $F_i(a_1, \dots, a_r, T)$ di $k[T]$ si decompone in fattori lineari $F_i = \Pi(T - c_{ij})$ e quindi $\Pi(x_i - c_{ij}) \in \mathfrak{q}$; essendo \mathfrak{q} un ideale primo, deve contenere almeno uno dei fattori. Se $x_i - c_{ij_0} \in \mathfrak{q}$, posto $a_i = c_{ij_0}$, avremo $\mathfrak{m} = (X_1 - a_1, \dots, X_r - a_r, x_{r+1} - a_{r+1}, \dots, x_n - a_n) \subseteq \mathfrak{q}$; ma \mathfrak{m} è massimale e quindi $\mathfrak{q} = \mathfrak{m}$.

Se $\pi: k[X_1, \dots, X_n] \rightarrow k[V] = k[X_1, \dots, X_n]/\mathcal{I}(V)$ è la proiezione sul quoziente, allora $\pi^{-1}(\mathfrak{q})$ è un massimale di $k[X_1, \dots, X_n]$ che contiene $\mathcal{I}(V)$ e quindi $(a_1, \dots, a_r, a_{r+1}, \dots, a_n) \in V$.

Dalla prima parte della dimostrazione segue poi che ϕ ha fibre finite. Se infatti $(a_1, \dots, a_n) \in V$, ciascun a_i con $i > r$ appartiene all'insieme finito delle radici del polinomio $F_i(a_1, \dots, a_r, T)$ e quindi fissate le prime r coordinate, per le $n - r$ rimanenti ci sono soltanto un numero finito di scelte (maggiorato dal prodotto dei gradi nella variabile T dei polinomi F_i). ■

Teoria della dimensione

Introdurremo ora alcuni modi differenti per definire la dimensione di una varietà algebrica. Poiché una trattazione è piuttosto vasta, daremo soltanto alcuni cenni delle proprietà e dei legami che intercorrono tra le varie nozioni. Inoltre non presenteremo la trattazione nelle ipotesi più ampie possibili privilegiando la comprensione delle interconnessioni alla generalità.

§ Altezza di un ideale e dimensione di Krull

Abbiamo già visto come si possa introdurre la dimensione di V dal punto di vista topologico utilizzando la topologia di Zariski. Vediamo come si possa darne una versione totalmente algebrica.

Definizione 11.1. Si dice **altezza** $h(\mathfrak{p})$ di un ideale primo \mathfrak{p} di un anello A la massima lunghezza r di catene di ideali primi contenuti in \mathfrak{p} :

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r = \mathfrak{p}.$$

Si dice altezza $h(\mathfrak{a})$ di un ideale \mathfrak{a} qualsiasi la minima altezza dei suoi primi associati. Infine si dice **dimensione di Krull** $\dim(A)$ di un anello A la massima altezza dei suoi ideali (massimali).

Grazie alla corrispondenza tra ideali (primi) di un anello A contenenti un suo ideale primo \mathfrak{p} ed ideali (primi) di A/I e, rispettivamente, tra ideali contenuti in \mathfrak{p} e ideali primi di $A_{\mathfrak{p}}$, è immediato vedere che valgono le relazioni:

$$\dim(A/I) + h(I) \leq \dim(A)$$

$$h(\mathfrak{p}) = \dim(A_{\mathfrak{p}}).$$

Nel caso in cui A sia l'anello delle coordinate $k[V]$ di una varietà irriducibile V su un campo algebricamente chiuso k , la dimensione di V coincide poi con la lunghezza delle catene di primi contenenti $\mathcal{I}(V)$ e quindi si ha:

$$\dim(V) = \dim(k[V]).$$

In realtà questa uguaglianza vale più in generale, ma la verifica non è immediata.

Lasciamo al lettore la semplice verifica delle seguenti proprietà:

1. Un anello noetheriano locale (A, \mathfrak{m}, k) ha dimensione finita. Infatti per la noetherianità \mathfrak{m} ha altezza finita e questa coincide con la dimensione di Krull di A .
2. Sia \mathfrak{p} un ideale primo dell'anello A . Allora l'altezza di \mathfrak{p} coincide con la dimensione della localizzazione $A_{\mathfrak{p}}$.
3. Sia \mathfrak{a} un ideale dell'anello A . Allora l'altezza di \mathfrak{a} coincide con l'altezza di $\sqrt{\mathfrak{a}}$.
4. Gli anelli artiniani possono anche essere caratterizzati come anelli noetheriani di dimensione di Krull 0. In particolare un campo k ha dimensione 0.

Si noti che in un anello noetheriano ogni ideale ha altezza finita, ma l'anello può anche avere dimensione di Krull infinita: per un esempio, dovuto a Nagata, si veda Atiyah-MacDonald Introduzione all'algebra commutativa Ch. 11 Ex. 4.

È abbastanza semplice provare che la dimensione di Krull dell'anello dei polinomi $k[X_1, \dots, X_n]$ è $\geq n$; basta infatti considerare la catena di primi

$$(0) \subsetneq (X_1) \subsetneq (X_1, X_2) \dots (X_1, \dots, X_n).$$

La disuguaglianza $\dim(k[X_1, \dots, X_n]) \geq n$ è in realtà una uguaglianza, ma la verifica è tutt'altro che immediata. Per provare questo risultato occorrono risultati importanti della teoria della dimensione, come il seguente, che è uno dei più significativi dell'algebra commutativa.

Teorema 11.2 (Hauptidealsatz o Teorema dell'ideale principale di Krull).

Sia A un anello noetheriano e sia x un suo elemento che non è né unità né zero-divisore.

Allora ogni primo minimale di x ha altezza 1

Per una dimostrazione diretta si veda ad esempio il libro Computational methods in Commutative Algebra and Algebraic Geometry di W. Vasconcelos.

Corollario 11.3. *Sia A un anello noetheriano e sia $I = (x_1, \dots, x_n)$ un suo ideale. Allora $h(I) \leq n$.*

Corollario 11.4. *Sia (A, \mathfrak{m}, k) un anello noetheriano locale e sia $I = (x_1, \dots, x_n)$ un ideale \mathfrak{m} -primario. Allora $\dim(A) \leq n$.*

Corollario 11.5. $\dim(k[X_1, \dots, X_n]) = n$.

Dimostrazione. Proviamo la disuguaglianza non banale $\dim(A) \leq n$.

Per ottenerla, basta provare che per ogni massimale \mathfrak{m} di A si ha $h(\mathfrak{m}) = \dim(A)$.

Come abbiamo visto nei capitoli precedenti, per ogni $i \leq n$ in \mathfrak{m} vi è (esattamente) un polinomio F_i nella sola indeterminata X_i , monico e irriducibile. L'ideale $\mathfrak{q} = (F_1, \dots, F_n)$ di A ha come primi associati solo dei massimali; infatti se \mathfrak{n} è un

primo che contiene \mathfrak{q} , allora A/\mathfrak{n} è dominio ed è una estensione algebrica di k e quindi è un campo).

Passando alla localizzazione in \mathfrak{m} , l'estensione dell'ideale \mathfrak{q} a $A_{\mathfrak{m}}$ è un ideale che ha come unico primo associato $\mathfrak{m}A_{\mathfrak{m}}$ e quindi è $\mathfrak{m}A_{\mathfrak{m}}$ -primario; inoltre è generato da n elementi. Otteniamo così grazie al Corollario 11.4:

$$h(\mathfrak{m}) = h(\mathfrak{m}A_{\mathfrak{m}}) = h(\mathfrak{q}A_{\mathfrak{m}}) \leq n.$$

■

Citiamo infine una importante conseguenza dei risultati noti come **Going-up** e **Going-down** (che saranno oggetto di seminari) che ha notevoli applicazioni in geometria algebrica relativamente alla cosiddetta "risoluzione delle singolarità".

Teorema 11.6. *Sia A un dominio integralmente chiuso e sia B un dominio intero su A . Allora $\dim(A) = \dim(B)$.*

Corollario 11.7. *Sia $A = k[V]$ l'anello delle coordinate di una varietà affine irriducibile. Se $k[V] = k[X_1, \dots, X_r][x_{r+1}, \dots, x_n]$, con le x_i intere sull'anello di polinomi $k[X_1, \dots, X_r]$ (Lemma di normalizzazione), allora:*

$$\dim(V) = \dim(k[V]) = \text{trdeg}_k(k(V)) = r.$$

Dimostrazione. L'unica uguaglianza ancora da provare è $\dim(k[V]) = r$.

Per questo basta ricordare che $\dim(k[X_1, \dots, X_r]) = r$ e che $\dim(k[V]) = \dim(k[X_1, \dots, X_r])$ poiché il primo è un dominio intero sul secondo. ■

§ Funzioni di Hilbert

Dato un ideale I di $A = k[X_1, \dots, X_n]$ possiamo considerare i k -sottospazi vettoriali del quoziente A/I :

$$(A/I)_{\leq s} := \{\overline{F} \in A/I \mid \partial(F) \leq s\}.$$

Fissato un term order graduato, si verifica immediatamente che

$$(A/I)_{\leq s} = \{\overline{F} \in A/I \mid F \text{ è in forma normale rispetto a } I \text{ e } \partial(F) \leq s\}.$$

Grazie al term order, possiamo anche considerare i k -sottospazi vettoriali:

$$(A/I)_s := \{\overline{M} \in A/I \mid M \text{ è omogeneo e in forma normale rispetto a } I \text{ e } \partial(F) = s\}.$$

I sottospazi così definiti sono legati tra loro dalla sequenza esatta di k -spazi vettoriali:

$$0 \rightarrow (A/I)_{\leq s-1} \rightarrow (A/I)_{\leq s} \rightarrow (A/I)_s \rightarrow 0 \tag{1}$$

e quindi vale la relazione tra le dimensioni:

$$\dim_k((A/I)_s) = \dim_k((A/I)_{\leq s}) - \dim_k((A/I)_{\leq s-1}). \quad (2)$$

Più in generale si ha:

$$(A/I)_{\leq s} = \bigoplus_{i=0}^s (A/I)_i.$$

Osservazione 11.8. Si noti che, mentre $(A/I)_{\leq s}$ è indipendente dal term order graduato fissato, $(A/I)_s$ ne dipende fortemente e quindi il simbolo, in cui il term order non compare, è ambiguo. Per evitare l'ambiguità potremmo definire $(A/I)_s$ mediante la sequenza esatta (1) come il quoziente $(A/I)_{\leq s}/(A/I)_{\leq s-1}$. In realtà quello che a noi interessa in questo contesto è soltanto la dimensione di $(A/I)_s$, che è invariante rispetto all'ordinamento graduato scelto.

Inoltre, nel caso in cui I sia un ideale omogeneo, allora A/I è una k -algebra graduata e i sottospazi vettoriali

$$(A/I)_s := \{\bar{F} \in A/I \mid F \text{ è omogeneo e } \partial(F) = s\}$$

sono proprio le componenti graduate di A/I .

Definizione 11.9. Si dice **funzione di Hilbert affine** di $B = A/I$ la seguente funzione intera:

$$HF_B^a(s): \mathbb{N} \longrightarrow \mathbb{N} \text{ data da } s \mapsto \dim_k((A/I)_{\leq s})$$

In modo analogo, si dice **funzione di Hilbert** di B la funzione intera:

$$HF_B(s): \mathbb{N} \longrightarrow \mathbb{N} \text{ data da } s \mapsto \dim_k((A/I)_s).$$

Proposizione 11.10. Siano I un ideale di $A = k[X_1, \dots, X_n]$ e J il suo ideale iniziale rispetto ad un fissato term order graduato. Allora:

- i) $HF_{A/I}^a = HF_{A/J}^a$, $HF_{A/I} = HF_{A/J}$;
- ii) $HF_{A/J}(s)$ coincide col il numero di monomi di A di grado s non appartenenti a J .

Dimostrazione. Entrambe le uguaglianze in i) seguono dall'isomorfismo di k -spazi vettoriali:

$$A/I \longrightarrow A/J \text{ dato da } \bar{F} = \overline{N(F)} \mapsto \text{In}(N(F))$$

dove $N(F)$ indica la forma normale di F modulo I .

Per ii) basta osservare che i monomi sono una base per i polinomi e che un monomio è in forma normale rispetto a J se e solo se non gli appartiene. ■

Le considerazioni seguenti, scritte per semplicità relativamente alla sola funzione di Hilbert, valgono però in modo del tutto analogo anche per la funzione di Hilbert affine.

Teorema 11.11. *Sia I un ideale di $A = k[X_1, \dots, X_n]$.*

Per $s \gg 0$ la funzione di Hilbert di A/I è una funzione polinomiale, ossia esiste un polinomio $P(T) \in \mathbb{Q}[T]$ tale che $HF_{A/I}(s) = P(s)$ per ogni $s \gg 0$.

Se inoltre k è infinito allora $\partial(P(T)) = r - 1$, dove r è il massimo numero di elementi di A/I algebricamente indipendenti su k .

Dimostrazione. Proviamo innanzi tutto che per $s \gg 0$ la funzione di Hilbert è polinomiale.

Grazie alla Proposizione 11.10 possiamo limitarci a provare l'asserto supponendo che I sia un ideale monomiale.

Fissato un insieme di generatori monomiali di I , sia ρ il grado del loro minimo multiplo comune. Per ogni $s \geq \rho$, possiamo calcolare $HF_{A/I}(s)$ contando quanti monomi di grado s non appartengono a I :

- i monomi di grado s in tutto sono $\binom{s+n-1}{n-1}$;
- a questo numero bisogna sottrarre per ciascun generatore di I il numero $\binom{s+n-1-d_i}{n-1}$ dei suoi multipli;
- poiché i multipli comuni a due generatori sono stati sottratti più volte, riaggiungiamo al totale il loro numero;
-
- e così via fino ad arrivare ai multipli comuni a tutti i generatori, secondo la formula della cardinalità dell'unione di insiemi.

Sostituendo ad s una variabile T , otteniamo così un polinomio di grado $\leq n - 1$ la cui valutazione in s coincide con $HF_{A/I}(s)$ per ogni $s \geq \rho$.

Proviamo ora che il grado di $P(T)$ è $r - 1$. Possiamo limitarci a provare l'asserto supponendo I omogeneo.

Se $n = r$, allora $A/I = k[X_1, \dots, X_n] = A$ è un anello di polinomi e $\dim_k(A)_s = \binom{s+n-1}{n-1}$. Quindi

$$P(T) = \frac{(T+n-1)(T+n-2)\cdots(T+1)}{(n-1)!} := \binom{T+n-1}{n-1}$$

ha grado $n - 1 = r - 1$, come volevasi. Si noti che l'asserto vale anche per $n = 0$: in tal caso $P(T)$ è il polinomio nullo il cui grado può essere posto convenzionalmente pari a -1 .

Procediamo allora per induzione su n . Se $n = r$ l'asserto è vero; supponiamo allora $r < n$ e sia $G(X_1, \dots, X_n)$ un polinomio non nullo di grado positivo d tale che $G(x_1, \dots, x_n) = 0$. Poiché k è infinito possiamo operare un opportuno cambiamento lineare di variabili del tipo $Y_i = X_i + \lambda_i X_n$ in modo che G si trasformi in un polinomio

in cui compare X_n^d , così che $x_n \in A/I$ risulta essere intero su $B = k[y_1, \dots, y_{n-1}]$ e A/I diventa un modulo su B generato da $1, x_n, \dots, x_n^{d-1}$: si noti che un siffatto cambiamento di variabili non altera le componenti graduate di A/I .

Inoltre il massimo numero di elementi algebricamente indipendenti di B è lo stesso di A ossia r .

Per ipotesi induttiva $HF_B(s) = P_1(s)$ per $s \gg 0$, con $P_1(T)$ polinomio di grado $r - 1$.

Poiché $B_s \subseteq (A/I)_s$, allora $P(T)$ ha grado $\geq r - 1$.

D'altra parte, per $s > d$, $(A/I)_s = B_s + x_n B_{s-1} + \dots + x_n^{d-1} B_{s-d+1}$ e quindi $HF_{A/I}(s) \leq P_1(s) + P_1(s-1) + \dots + P_1(s-d+1)$.

Ma $P_1(T) + P_1(T-1) + \dots + P_1(T-d+1)$ è un polinomio di grado $r - 1$ e quindi $\partial(P(T)) \leq r - 1$, da cui l'asserto. ■

Si noti, che per costruzione, $P(T)$ ha coefficienti razionali, non necessariamente interi; tuttavia è un **polinomio intero** ossia assume valori interi se valutato in ogni numero intero.

Definizione 11.12. Dato un ideale I di $A = k[X_1, \dots, X_n]$, il polinomio introdotto nel Teorema 11.11 si dice **polinomio di Hilbert** di A/I , denotato $HP_{A/I}$.

In modo del tutto analogo si definisce il polinomio di Hilbert affine $HP_{A/I}^a(T)$.

Segue poi immediatamente da (2) che $HP_{A/I}(T) = HP_{A/I}^a(T) - HP_{A/I}^a(T-1)$.

Nel caso in cui I sia l'ideale di una varietà V su un campo k algebricamente chiuso, abbiamo visto come la dimensione r di V definita in modo topologico coincida con la dimensione di Krull di $k[V]$, col massimo numero di elementi algebricamente indipendenti di $k[V]$ e con $\text{trdeg}_k(k(V))$; il Teorema 11.11 mette poi in relazione questo numero col grado del polinomio di Hilbert e quindi:

$$\dim(V) = \partial(HP_{A/I}) + 1 = \partial(HP_{A/I}^a).$$

Analoghe relazioni sussistono anche nel caso delle varietà proiettive con piccoli aggiustamenti di una unità: in quel caso il grado della funzione di Hilbert coincide esattamente con la dimensione della varietà.

La relazione tra la dimensione della varietà e il grado di un certo polinomio compare anche in una diversa forma collegata anche questa alla funzione di Hilbert

§ La serie di Hilbert-Poincaré

Definizione 11.13. Sia I un ideale di $A = k[X_1, \dots, X_n]$. Si dice **serie di Hilbert** (o di **Hilbert-Poincaré**) di A/I la serie formale:

$$HS_{A/I}(t) = \sum_{s=0}^{\infty} HF_{A/I}(s)t^s.$$

Teorema 11.14 (Hilbert, Serre). *Sia I un ideale di $A = k[X_1, \dots, X_n]$. Esiste un intero r tale che:*

$$HS_{A/I}(t) = \frac{f(t)}{(1-t)^r}$$

dove $f(t) \in \mathbb{Z}[t]$.

Inoltre il minimo intero r siffatto è $\partial(HP_{A/I}(T)) + 1$.

Dimostrazione. Grazie al Teorema 11.11 sappiamo che $HF_{A/I}(s)$ coincide, per $s \gg 0$, con la valutazione in s del polinomio $HP_{A/I}(T)$ che per brevità chiameremo $P(T)$: sia d il suo grado.

Osserviamo intanto che l'asserto è vero per la serie completa se e soltanto se è vero per $\sum_{s=s_0}^{\infty} HF_{A/I}(s)t^s$: basta portare a secondo membro il pezzo iniziale della serie e fare denominatore comune.

Scegliamo s_0 in modo che $HF_{A/I}(s) = P(s)$ ossia consideriamo la serie formale $\Sigma(t) = \sum_{s=s_0}^{\infty} P(s)t^s$.

Moltiplicando la serie $\Sigma(t)$ per $(1-t)$ otteniamo la serie:

$$\Delta(t) = P(s_0)t^{s_0} + \sum_{s=s_0+1}^{\infty} (P(s) - P(s-1))t^s = a_{s_0}t^{s_0} + \sum_{s=s_0+1}^{\infty} (\Delta P(s))t^s$$

dove $\Delta P(s)$ è un polinomio di grado $d-1$.

Moltiplicando per $(1-t)^{d+1}$ otteniamo quindi un polinomio di grado -1 ossia il polinomio nullo. In conclusione:

$$\Sigma(t) \cdot (1-t)^{d+1} = a_{s_0}t^{s_0} + \dots + a_{s_0+d}t^{s_0+d}$$

da cui l'asserto.

Se k è infinito, abbiamo provato (Teorema 11.11) che $d = r - 1$ dove r è il grado del polinomio di Hilbert di A e quindi il massimo numero di elementi di A algebricamente indipendenti su k . ■

Corollario 11.15. *Se V è una varietà algebrica irriducibile di dimensione d in k^n e sia $I = I(V)$ il corrispondente ideale in $A = k[X_1, \dots, X_n]$.*

Allora il minimo intero r tale che

$$HS_{A/I}(t) = \frac{f(t)}{(1-t)^r}$$

è la dimensione di V .

Corollario 11.16. *Sia A una k -algebra e sia $x \in A$ un elemento che non è né unità né zero-divisore. Allora:*

$$\partial(HP_A) = \partial(HP_{A/(x)}) + 1.$$

Dimostrazione. In questo caso conviene dimostrare l'asserto per la funzione di Hilbert affine. Sia $A = k[X_1, \dots, X_n]/I$ e sia d il grado della forma normale modulo I di un rappresentante di x in $k[X_1, \dots, X_n]$ (rispetto a un term order graduato prefissato).

La sequenza esatta di k -spazi vettoriali:

$$0 \longrightarrow A \xrightarrow{\cdot x} A \longrightarrow A/(x) \longrightarrow 0$$

induce per ogni s la sequenza esatta:

$$0 \longrightarrow A_{\leq s-d} \xrightarrow{\cdot x} A_{\leq s} \longrightarrow (A/(x))_{\leq s} \longrightarrow 0.$$

Allora per $s \gg 0$ si ha $HP_{A/(x)}^a(T) = HP_A^a(T) - HP_A^a(T-d)$ da cui l'asserto. ■

Ci sono tanti altri modi ancora per calcolare la dimensione di un anello. Si può ad esempio considerare il caso di un anello locale (A, \mathfrak{m}, k) (localizzando ad esempio in un massimale) e quindi calcolare:

- il massimo numero di elementi $t_1, \dots, t_r \in A$ tali che $\overline{t_{i+1}}$ non è né unità né zero-divisore in $A/(t_1, \dots, t_i)$;
- il minimo numero di generatori di un ideale \mathfrak{m} -primario;
- la dimensione dell'anello graduato associato $G_{\mathfrak{m}}(A) = \bigoplus_i (\mathfrak{m}^i / \mathfrak{m}^{i+1})$

....

§ Esercizi

Esercizio 11.17. Sia $P(T) \in \mathbb{Q}[T]$ un polinomio non nullo. Provare che per ogni $a \in \mathbb{N}$ $a \geq 1$ si ha:

- a. $\partial(P(T) - P(T-a)) = \partial(P(T)) - 1$;
- b. $\partial(P(T) + P(T-1) + \dots + P(T-a)) = \partial(P(T))$.

Esercizio 11.18. Sia A una k -algebra finitamente generata $A = k[x_1, \dots, x_n]$ (che non è necessariamente un dominio).

Provare che il massimo numero di elementi di A algebricamente indipendenti su k è n .

Esercizio 11.19. Provare che l'anello dei polinomi $A = k[X_1, \dots, X_n]$ è universalmente catenario, ossia che per ogni \mathfrak{p} primo in A si ha:

$$h(\mathfrak{p}) + \dim(A/\mathfrak{p}) = n.$$

È vero che per ogni primo di una k -algebra finitamente generata $A = k[x_1, \dots, x_n]$ si ha :

$$h(\mathfrak{p}) + \dim(A/\mathfrak{p}) = \dim(A)?$$