CAPITOLO 3 DIMENSIONE

versione del (9-4-2002)

1 Trascendenza

1.1 DEFINIZIONE. *Data un algebra A su un campo k diremo che elementi $a_i \in A,\ i \in I$ sono algebricamente indipendenti su k se l'omomorfismo di valutazione:*

$$k[x_i]_{i\in I} \to A,\ x_i \to a_i$$

è iniettivo, ovvero se non soddisfano alcun polinomio su k, altrimenti si dicono algebricamente dipendenti.

Applichiamo prima di tutto queste idee ai campi. Sia dunque $k \subset F$ una estensione di campi. Dati elementi $a_i \in F,\ i \in I$ usualmente si denota con $k(a_i)$ il campo generato dagli a_i su k. È il minimo campo contenente k e gli elementi a_i ed i suoi elementi si possono scrivere come frazioni di polinomi negli a_i.

OSSERVAZIONE Dati elementi $a_i \in F,\ i \in I$ algebricamente indipendenti su k, l'omomorfismo di valutazione: $k[x_i]_{i\in I} \to A,\ x_i \to a_i$ si estende ad un isomorfismo fra il campo $k(x_i)$ delle funzioni razionali e $k(a_i)$.

1.2 DEFINIZIONE. *Data $k \subset F$ una estensione di campi, diremo che elementi $a_i \in F,\ i \in I$ generano algebricamente F su k se ogni elemento di F è algebrico sul campo $k(a_i)$.*[1]
Se inoltre gli a_i sono algebricamente indipendenti su k diremo che formano una **base di trascendenza** *di F su k.*

Vi sono una serie di enunciati del tutto simili a quelli della dipendenza lineare che lasciamo da verificare al lettore.

1.3 PROPOSIZIONE.

(1) *Presi elementi $a_i \in F,\ i \in I$ che generano algebricamente F su k, esiste un sottoinsieme $a_j \in F,\ j \in J$ che sia massimale rispetto alla proprietà di essere anche algebricamente indipendente.*
(2) *Ogni tale sottoinsieme è una base di trascendenza di F su k.*
(3) *Dati tre campi $k \subset F \subset G$ elementi $a_i \in F,\ i \in I$ che generano algebricamente F su k e $b_j \in G,\ j \in J$ che generano algebricamente G su F, gli elementi $a_i,\ b_j \in G,\ i \in I,\ j \in J$ generano algebricamente G su k.*
(4) *Se gli elementi $a_i \in F,\ i \in I$ sono una base di trascendenza di F su k e gli elementi $b_j \in G,\ j \in J$ sono una base di trascendenza di G su F, gli elementi $a_i,\ b_j \in G,\ i \in I,\ j \in J$ sono una base di trascendenza di G su k.*

[1] Un linguaggio più simile a quello della dipendenza lineare è di dire che *ogni elemento di F è algebricamente dipendente dagli elementi a_i.*

La maggiore differenza formale fra il caso della dipendenza lineare e quella algebrica è probabilmente nel fatto che in generale per una estensione F di k non esistono elementi $a_i \in F,\ i \in I$ che siano una base di trascendenza di F su k e per cui $F = k(a_i)$. Se una tale proprietà è verificata si dice che F è *razionale* su k. questa è una proprietà molto delicata e vi sono moltissimi problemi aperti legati a questa questione.

Come negli spazi vettoriali l'invariante fondamentale è la dimensione cosí nei campi abbiamo il *grado di trascendenza* ovvero il numero di elementi di una base di trascendenza. Per mostrare che è un numero ben definito abbiamo bisogno del:

1.4 Lemma. *(di scambio) Data una base di trascendenza a_j , $j \in J$ di F su k ed un elemento $a \in F$ trascendente su k esiste un sottoinsieme proprio $T \subsetneq J$ tale che $\{a,\ a_i\}_{i\in T}$ è una base di trascendenza di F su k.*

Dim. Per ipotesi a è algebrico su $k(a_i)$ ma non su k, segue che esiste una equazione polinomiale $f(a, a_1, a_2, \ldots, a_n) = 0$ a coefficienti in k. Almeno uno degli a_i appare in questa equazione e quindi a_i è algebrico sul campo generato da a e dagli $a_j,\ j \neq i$. Da 1.3, 1) segue che fra questi elementi possiamo estrarre una base di trascendenza[2] che deve contenere necessariamente a. □

A questo punto studiamo il caso di maggior interesse, ovvero i campi finitamente generati.

1.5 Teorema. *Data una estensione F di k finitamente generata due basi di trascendenza di F su k hanno lo stesso numero di elementi.*

Dim. Sia $a_1, \ldots, a_n$ una base di trascendenza, se $b_1, \ldots, b_m$ sono algebricamente indipendenti mostriamo che $m \leq n$, questo basta. Ragioniamo per induzione su n. Se $n = 0$ l'estensione è algebrica e non c'è nulla da dimostrare. Per il lemma di scambio b_1 e al più $n-1$ degli a_i sono un'altra base di trascendenza. Quindi per induzione applicata alla estensione $F \supset k(b_1)$ vi sono al più $n-1$ elementi algebricamente indipendenti su $k(b_1)$. Poiché $b_2, \ldots, b_m$ sono algebricamente indipendenti su $k(b_1)$ si ha $m-1 \leq n-1$ come richiesto.

□

1.6 Definizione. *Data una estensione F di k finitamente generata il numero di elementi di una base di trascendenza di F su k è detto grado di trascendenza di F su k e denotato $Trdeg(F : k)$.*

Da 1.3, 4) segue immediatamente:

Corollario. *Dati tre campi $k \subset F \subset G$ si ha:*

$$Trdeg(G : k) = Trdeg(G : F) + Trdeg(F : k)$$

[2] vedremo immediatamente che in effetti gli elementi a e $a_j,\ j \neq i$ sono già algebricameente indipendenti.

2 Dimensione

Vogliamo subito applicare le idee precedenti alla dimensione di una varietà.

La prima idea che seguiamo è quella che la dimensione è *il massimo numero di parametri indipendenti.*

2.1 DEFINIZIONE. *Data una varietà irriducibile* V *con anello di coordinate* $A := k[V]$ *con campo delle frazioni* $F := k(V)$*, chiamiamo dimensione di* V *il grado di trascendenza di* F *su* k*.*

$$\dim(V) := Trdeg(k(V) : k)$$

Per una varietà riducibile $V = \cup V_i$ *poniamo* $\dim(V) := \max_i \dim(V_i)$.

La definizione appena data utilizza il campo delle frazioni $k(V)$, si usa dire che due varietà V, W sono **birazionalmente isomorfe** se i due campi $k(V)$, $k(W)$ sono isomorfi.

La dimensione è un invariante birazionale.

Ci sono moltissime ragioni per giustificare questa definizione e cominciamo a vederne alcune. Le varietà che seguono si assumono irriducibili.

2.2 PROPOSIZIONE. *i)* $\dim k^n = n$ *se* $V \subsetneq k^n$ *si ha* $\dim V < n$.

ii) $\dim(V \times W) = \dim V + \dim W$.

iii) Se $V \subset k^n$ *è definita da una unica equazione* $f(x) = 0$ *(*$f(x) \notin k$ *non costante) si ha* $\dim V = n - 1$.

iv) $\dim V = 0$ *se e solo se* V *è un punto*

DIM. i) Prima di tutto se $V \subset k^n$ si ha

$$k[V] = k[x_1, x_2, \ldots, x_n]/I, \ k(V) = k(x_1, x_2, \ldots, x_n),$$

quindi se $I = 0$ e $V = k^n$ abbiamo $\dim k^n = n$ altrimenti gli elementi x_i sono algebricamente dipendenti e $\dim V < n$.

ii) Se $V \subset k^n$, $W \subset k^m$ sono due varietà si ha $k[V] = k[x_1, x_2, \ldots, x_n]/I, k[V] = k[y_1, y_2, \ldots, y_m]/J$. Se $h = \dim V$, $k = \dim W$ si ha che h fra le classi $\overline{x}_i \in k[V]$ sono algebricamente indipendenti e le altre classi sono algebriche sui precedenti elementi, similmente per W. Per cui $k[V] \otimes \mathcal{O}(W) = \mathcal{O}(V \times W)$ contiene $h + k$ elementi algebricamente indipendenti su cui gli altri generatori sono algebrici e $\dim(V \times W) = \dim V + \dim W$.

iii) Sia $V \subset k^n$ definita da una unica equazione $f(x) = 0$. Dalla discussione del Cap. 1 in 3.12 possiamo assumere $f(x)$ irriducibile e quindi $k[V] = k[x_1, x_2, \ldots, x_n]/(f(x))$. Sappiamo già che $\dim V \leq n - 1$, poiché il polinomio $f(x)$ non è costante vi è almeno una variabile, ad esempio x_n che appare in $f(f)$, proviamo che le classi di $x_1, x_2, \ldots, x_{n-1}$ sono algebricamente indipendenti in $k[x_1, x_2, \ldots, x_n]/(f(x))$. Altrimenti esisterebbe un polinomio non nullo $g(x) := g(x_1, x_2, \ldots, x_{n-1})$ in $n - 1$ variabili, che svanisce su tali classi ovvero $g(x) \in (f(x)) \implies f(x)|g(x)$ ovvero $g(x) = f(x)h(x)$. Questo è assurdo perchè $f(x)$ contiene la variabile x_n mentre $g(x)$ non la contiene.

Finalmente sia $\dim V = 0$ pertanto il grado di trascendenza di $k(V)$ su k è 0, ovvero la estensione è algebrica, Poiché k è algebricamente chiuso si deve avere $k = k[V] = k(V)$ ovvero V è un punto. $\square$

Vi è un modo quantitativo per stimare quanti elementi fra un insieme dato siano algebricamente indipendenti che si presta a vaste generalizzazioni, anche in algebra non commutativa dove gioca un ruolo importante.

Facciamo qui dunque una digressione, seguendo le idee di Gelfand Kirillov.

Sia $A = k\langle a_1, \dots, a_k\rangle$ un'algebra finitamente generata, associativa ma non necessariamente commutativa. Per ogni intero positivo n sia $A_n := \{\langle a_{i_1} a_{i_2} \dots a_{i_m}\rangle,\ m \leq n\}$ lo spazio vettoriale generato dai monomi di grado $\leq n$ nei generatori a_i, sia $d(n) := \dim_k A_n$. L'idea è di definire la dimensione come una misura della crescita della dimensione lineare di A_n.

Gli spazi A_n godono delle seguenti proprietà,

$$A_n \subset A_{n+1}, \quad A_n A_m \subset A_{n+m}, \quad \cup_n A_n = A. \tag{2.3}$$

2.4 Definizione. *Una successione di sottospazi di un'algebra A che verifichino le proprietà 2.2 si chiama* **filtrazione crescente** *di A.*

Due esempi:

L'algebra dei polinomi non commutativi ha come base i monomi $a_{i_1} a_{i_2} \dots a_{i_m}$, vi sono esattamente k^m monomi di grado m e quindi in questo caso $d(n) = \sum_{m=0}^{n} k^m = \frac{k^{n+1}-1}{k-1}$.

L'algebra dei polinomi commutativi ha invece come base i monomi $a_1^{i_1} a_2^{i_2} \dots a_k^{i_m}$, vi sono esattamente $\binom{n+k}{k}$ monomi di grado $\leq n$.

In definitiva nel caso non commutativo $d(n)$ può crescere in modo esponenziale mentre nel caso commutativo cresce in modo polinomiale. La crescita polinomiale può essere misurata ponendo:

$$\delta(A) := \inf\{\nu \mid d(n) \leq n^\nu,\ n >> 0\} = \limsup_{n\to\infty} \frac{\log d(n)}{\log n}.$$

Per giustificare la notazione dobbiamo provare che la stima data non dipende dai generatori scelti. Sia dunque $A = k\langle a_1, \dots, a_k\rangle = k\langle b_1, \dots, b_h\rangle$ da cui otteniamo due filtrazioni crescenti A_n, B_n usando i due sistemi di generatori che definiscono due funzioni $d(n) = \dim A_n$, $\delta(n) = \dim B_n$. Ora esiste certamente un N_1 tale che $b_i \in A_{N_1}$, $\forall i$ da cui $B_m \subset A_{N_1 m}$ similmente abbiamo un N_2 con $A_m \subset B_{N_2 m}$ e quindi:

$$d(n) \leq \delta(N_2 n), \quad \delta(n) \leq d(N_1 n),$$

$$\limsup_{n\to\infty} \frac{\log d(n)}{\log n} \leq \limsup_{n\to\infty} \frac{\log \delta(N_2 n)}{\log n} = \limsup_{n\to\infty} \frac{\log \delta(n)}{\log n - \log(N_2)} = \limsup_{n\to\infty} \frac{\log \delta(n)}{\log n}$$

2.5 Teorema. *Per un'algebra A finitamente generata* $\limsup_{n\to\infty} \frac{\log d(n)}{\log n}$ *non dipende dai generatori scelti e viene detta* **dimensione di Gelfand Kirillov** *di A.*

Esattamente nello stesso modo si può procedere per i moduli.

Se M è un modulo finitamente generato su un'algebra A finitamente generata, fissati generatori $a_1, \dots, a_k$ di A come algebra ed $m_1, \dots, m_h$ di M come modulo abbiamo una filtrazione $M_n := \{\langle a_{i_1} a_{i_2} \dots a_{i_m} m_i \rangle, \ m \leq n\}$ e valgono le proprietà:

$$M_n \subset M_{n+1}, \quad A_n M_m \subset M_{n+m}, \quad \cup_n M_n = M. \tag{2.6}$$

2.7 Teorema. *Per un modulo M finitamente generato su un'algebra A finitamente generata*

$$\dim_{GK} M := \limsup_{n\to\infty} \frac{\log \dim(M_n)}{\log n}$$

non dipende dai generatori scelti e viene detta **dimensione di Gelfand Kirillov** *di M.*

Lasciamo al lettore il semplice:

ESERCIZIO 2.8

(1) Data una successione esatta di moduli $0 \to N \to M \to P \to 0$ si ha:

$$\dim_{GK} M = \sup(\dim_{GK} N, \dim_{GK} P).$$

(2) Se $A \subset B$ sono algebre finitamente generate si ha $\dim_{GK} A \leq \dim_{GK} B$.

(3) Se M è un modulo finitamente fenerato su un'algebra finitamente generata A si ha $\dim_{GK} M \leq \dim_{GK} A$.

(4) Se $A \subset B$ sono algebre finitamente generate ed inoltre B è un $A-$modulo sinistro (o destro) su A finitamente generato si ha: $\dim_{GK} A = \dim_{GK} B$.

Un suggerimento per 4). Sia $B = \sum_{i=0}^k A u_i, \ u_0 = 1$, abbiamo $u_i u_j = \sum_{h=1}^k a_{i,j,h} u_h$. Se prendiamo un sistema di generatori di A fra cui appaiono tutti gli $a_{i,j,h}$ e per B aggiungiamo anche gli u_j abbiamo che in filtrazione $B(j) \subset \sum_{h=0}^k A(j) u_h$ quindi $\dim B(j) \leq (k+1) \dim A(j)$ da cui etc..

La teoria ora svolta è piuttosto generale, nel caso commutativo abbiamo un teorema più forte:

2.9 Teorema. *Per un modulo M finitamente generato su un'algebra A commutativa finitamente generata esiste un polinomio $p(t)$ a valori interi per cui*

$$\dim(M_n) = p(n), \ n >> 0.$$

Dimostreremo questo teorema come conseguenza di un'enunciato ancora più preciso.

3 Moduli graduati

Vi sono molte motivazioni per i concetti che introdurremo fra breve.

3.1 DEFINIZIONE. *Un anello graduato è un anello* $A = \oplus_{i=0}^{\infty} A_n$ *somma diretta di sottogruppi additivi per cui* $A_i A_j \subset A_{i+j}$.

Un modulo graduato su un anello graduato è un modulo $M = \oplus_{i=-\infty}^{\infty} M_n$ *somma diretta di sottogruppi additivi per cui* $A_i M_j \subset M_{i+j}$.

Per anelli e moduli graduati valgono varie proprietà categoriche. Un morfismo graguato di anelli graduati $A = \oplus_{i=0}^{\infty} A_n$, $B = \oplus_{i=0}^{\infty} B_n$ è un morfismo $f : A \to B$ che preserva i gradi ovvero $f(A_i) \subset B_i$, $\forall i$.

Per un morfismo graguato $f : A \to B$ abbiamo che il nucleo è un *ideale omogeneo* $I = \oplus_{i=0}^{\infty} I_n$, e l'immagine un sottoanello graduato.

Anche per i moduli un morfismo graduato preserva i gradi, però in questo caso è utile considerare anche morfismi che cambiano i gradi.

Un morfismo di grado i di moduli $M = \oplus_{i=-\infty}^{\infty} M_n \xrightarrow{f} N = \oplus_{i=-\infty}^{\infty} N_n$ è un morfismo per cui $f(M_j) \subset N_{i+j}$, $\forall i$.
Vi è un altro modo di esprimere lo stesso concetto, definire il *modulo traslato*:

$$M[i], \qquad M[i]_n := M_{i+n}.$$

Un morfismo di grado i di moduli $M \xrightarrow{f} N$ è un morfismo di grado 0 di moduli $M \xrightarrow{f} N[i]$.

ESEMPIO Sia $A_n \subset A_{n+1}$, $\quad A_n A_m \subset A_{n+m}$, $\quad \cup_{n=0}^{\infty} A_n = A$ una filtrazione crescente di un anello A. Ad esempio la filtrazione indotta da un insieme di generatori. Consideriamo il gruppo abeliano $gr(A) := \oplus_{n=0}^{\infty} A_n / A_{n-1}$, (dove $A_{-1} = 0$). Abbiamo una struttura naturale di anello graduato su $gr(A)$ definita come segue, se $\overline{a} \in A_n/A_{n-1}$, $\overline{b} \in A_m/A_{m-1}$ sono le classi di $a \in A_n$, $b \in A_m$ la classe di $ab \in A_{n+m}$ modulo A_{n+m-1} è ben definita poiché ad esempio se $u \in A_{n-1}$ si ha $(a+u)b = ab + ub$, $ub \in A_{n+m-1}$.

Una costruzione simile per $M_n \subset M_{n+1}$, $\quad A_n M_m \subset M_{n+m}$, $\quad \cup_n M_n = M$ un modulo filtrato su un anello filtrato A, si ottiene un modulo graduato $gr(M)$ sul graduato $gr(A)$.[3]
Oltre alle filtrazioni crescenti di un anello A sono interessanti anche le filtrazioni decrescenti $A_n \supset A_{n+1}$, $\quad A_n A_m \subset A_{n+m}$, $\quad A_0 = A$. Per costruzione $AA_n = A_0 A_n \subset A_n$ e quindi gli A_n sono ideali. Spesso si incontrano filtrazioni decrescenti per cui $\cap_i A_i = 0$. Similmente una filtrazione decrescente per un modulo $M_n \supset M_{n+1}$, $\quad A_n M_m \subset M_{n+m}$.

Anche in questo caso ponendo $gr(A) := \oplus_{n=0}^{\infty} A_n/A_{n+1}$, $gr(M) := \oplus_{n=0}^{\infty} M_n/M_{n+1}$, da un modulo filtrato su un anello filtrato A, si ottiene un modulo graduato $gr(M)$ sul graduato $gr(A)$.

Per semplificare la discussione prendiamo come anello graduato $A = k[x_1, x_2, \ldots, x_n]$ l'anello dei polinomi, in cui le variabili hanno grado 1.

Consideriamo un modulo graduato M finitamente generato su A, scomponendo i generatori in parti omogenee possiamo assumere che $M = \sum_{i=1}^{m} Au_i$ con u_i omogeneo di grado h_i. Ne deduciamo:

[3]La costruzione si può fare anche per anelli non commutativi, vi sono degli esempi molto interessanti in cui partendo da un anello non commutativo il graduato associato è commutativo!

3.2 Lemma.

$$M_i = 0, \ \forall i < \min(h_1, \dots, h_m), \quad \dim M_i < \infty, \ \forall i.$$

Dim.

$$M_i = \{\sum_{k=1}^m f_k u_k\}, \ f_k \in A_{i-h_k}, \quad A_{i-h_k} = 0, \ \forall i < h_k, \quad \dim M_i \le \sum_{k=1}^m \dim A_{i-h_k}.$$

□

Dato un modulo graduato M finitamente generato su un anello graduato finitamente generato possiamo definire la sua *serie di Laurent*

$$\chi_M(t) := \sum_{i=-\infty}^{\infty} \dim M_i t^i \tag{3.3}$$

Il primo esempio è:

3.4 Teorema. *Se $A_n := k[x_1, \dots, x_n]$ graduato secondo il grado usuale:*

$$\chi_{A_n}(t) = \frac{1}{(1-t)^n} = \sum_{j=0}^{\infty} \binom{n+j-1}{j} t^j.$$

Dim. L'identità $\frac{1}{(1-t)^n} = \sum_{j=0}^{\infty} \binom{n+j-1}{j} t^j$ si dimostra semplicemente per induzione su n.

Due semplici dimostrazioni. Una combinatoria, i monomi di grado j in n variabili sono tanti quante le sequenze $h_1, h_2, \dots, h_n, \ |h_i \ge 0, \ \sum h_i = j$ che sono tante quante le sequenze $k_1 := h_1 + 1, k_2 := h_2 + 1, \dots, k_n := h_n + 1, \ |k_i \ge 1, \ \sum k_i = n + j$. Dare una tale sequenza è come dare gli $n-1$ numeri $k_1, k_1 + k_2, \dots, k_1 + k_2 + \dots + k_{n-1}$ fra $1, 2, \dots, n+j-1$ che si fa in $\binom{n+j-1}{j}$ modi.

Per la seconda si noti che se $M = \oplus_{i=0}^{\infty} M_i, \ N = \oplus_{j=0}^{\infty} N_j$ sono due spazi vettoriali graduati e $M \otimes N$ è graduato da $(M \otimes N)_i = \oplus_{h+k=i} M_h \otimes N_k$ si ha:

$$\sum_{i=0}^{\infty} \dim(M \otimes N)_i t^i = (\sum_{i=0}^{\infty} \dim M_i t^i)(\sum_{i=0}^{\infty} \dim N_i t^i)$$

da cui per induzione.

$$\chi_{A_1}(t) = \sum_{i=0}^{\infty} t^i = \frac{1}{1-t}, \qquad \chi_{A_n}(t) = \chi_{A_1}(t)\chi_{A_{n-1}}(t) = \frac{1}{1-t}\frac{1}{(1-t)^{n-1}} = \frac{1}{(1-t)^n}$$

□

La seconda dimostrazione si presta alla seguente generalizzazione. Consideriamo di nuovo l'anello dei polinomi $A = k[x_1, \dots, x_n]$, ma questa volta cambiamo i gradi definendo $deg\, x_i := a_i > 0$.[4]

ESERCIZIO Provare nel caso precedente che:

$$\chi_A(t) = \prod_{i=1}^{n} \frac{1}{(1 - t^{a_i})}.$$

3.5 TEOREMA. *Consideriamo un modulo graduato* $M = \sum_{i=1}^{m} Au_i$ *finitamente generato su* $A = k[x_1, x_2, \dots, x_n]$ *l'anello dei polinomi, con* u_i *omogeneo di grado* ≥ 0.

$$\chi_M(t) := \sum_{i=0}^{\infty} \dim M_i t^i = \frac{p(t)}{(1-t)^n} \tag{3.6}$$

Con $p(t)$ *un polinomio a coefficienti interi.*

DIM. Per induzione su n. Se $n = 0$ si ha che M è uno spazio vettoriale di dimensione finita, quindi $\dim M_i = 0$ per i grande e $\chi_M(t)$ è un polinomio (a coefficienti interi positivi).

In generale consideriamo il morfismo $M \xrightarrow{x_n} M$ di moltiplicazione per x_n sia $N := \{m \in M \,|\, x_n m = 0\}$ il nucleo e $P := M/x_n M$ il conucleo. Si ha la successione esatta $0 \to N \to M \xrightarrow{x_n} M \to P \to 0$ e N, P sono in modo naturale moduli finitamente generati in grado ≥ 0 sull'anello dei polinomi $k[x_1, x_2, \dots, x_{n-1}]$ in una variabile in meno.

Per ogni grado abbiamo la successione esatta e la relazione:

$$0 \to N_i \to M_i \xrightarrow{x_n} M_{i+1} \to P_{i+1} \to 0, \quad \dim N_i - \dim M_i + \dim M_{i+1} - \dim P_{i+1} = 0$$

Da cui:

$$\sum_{i=-1}^{\infty} (\dim N_i - \dim M_i + \dim M_{i+1} - \dim P_{i+1}) t^{i+1} = 0$$

$$t\chi_N(t) - t\chi_M(t) + \chi_M(t) - \chi_P(t) = 0, \quad \chi_M(t) = \frac{\chi_P(t) - t\chi_N(t)}{1-t}$$

Per induzione $\chi_P(t) = \frac{p_1(t)}{(1-t)^{n-1}}$, $\chi_N(t) = \frac{p_2(t)}{(1-t)^{n-1}}$ e $\chi_M(t) = \frac{p_1(t) - tp_2(t)}{(1-t)^n}$ □

In modo analogo provare:

ESERCIZIO Consideriamo un modulo graduato $M = \sum_{i=1}^{m} Au_i$ finitamente generato su $A = k[a_1, a_2, \dots, a_n]$ un anello graduato generato dagli a_i in grado k_i, con u_i omogeneo di grado $\geq -N$.

$$\chi_M(t) := \sum_{i=-N}^{\infty} \dim M_i t^i = t^{-N} \frac{p(t)}{\prod_{i=1}^{n}(1 - t^{k_i})} \tag{3.7}$$

---

[4]Usualmente questo tipo di gradi appare come un *peso* rispetto a qualche toro.

Con $p(t)$ un polinomio a coefficienti interi.

Un importante conseguenza del precedente teorema è la teoria del polinomio di Hilbert-Samuel.

3.8 Teorema. *Per un modulo graduato $M = \sum_{i=1}^{m} Au_i$ finitamente generato su $A = k[x_1, x_2, \ldots, x_n]$ l'anello dei polinomi, esiste un polinomio $q_M(t)$ a valori interi di grado $\leq n-1$ per cui* $\dim M_i = q_M(i), \ \forall i >> 0$

Dim. Dal precedente teorema ed esercizio si ha che

$$\chi_M(t) := \sum_{i=-N}^{\infty} \dim M_i t^i = (\sum_{i=-N}^{N} a_i t^i)\frac{1}{(1-t)^n} = (\sum_{i=-N}^{N} a_i t^i)\sum_{j=0}^{\infty}\binom{n+j-1}{j} t^j.$$

$$\chi_M(t) = \sum_{i=-N}^{N} a_i \sum_{j=0}^{\infty}\binom{n+j-1}{n-1} t^{j+i} = \sum_{i=-N}^{N} a_i \sum_{h=i}^{\infty}\binom{n+h-i-1}{n-1} t^h.$$

Pertanto per $h \geq N$ si ha:

$$\dim M_h = \sum_{i=-N}^{N} a_i \binom{h+n-i-1}{n-1} := q_M(h).$$

Ora $\binom{h}{b} = \frac{h(h-1)\ldots(h-b+1)}{b!}$ è un polinomio di grado b in h. $\square$

È utile a questo punto fare una breve digressione aritmetica.

Dal teorema di interpolazione di Lagrange è chiaro che un polinomio a valori interi sugli interi, deve avere coefficienti razionali. Lo spazio vettoriale dei polinomi $\mathbb{Q}[t]$ oltre alla ovvia base dei monomi t^k ha anche la base (su $\mathbb{Q}$) dei polinomi $p_b(h) := \binom{h}{b}$ un polinomio di grado b in h a valori interi.

Sia $\mathbb{P}_{\mathbb{Z}}$ il sottogruppo di $\mathbb{Q}[t]$ formato dai polinomi che prendono sugli interi valori interi. Definiamo l'operatore (derivata finita):

$$\Delta f(h) := f(h+1) - f(h)$$

che trasforma evidentemente $\mathbb{P}_{\mathbb{Z}}$ in se. Si ha dal triangolo di Tartaglia

$$\Delta p_b = \Delta\binom{h}{b} = \binom{h+1}{b} - \binom{h}{b} = \binom{h}{b-1} = p_{b-1}. \tag{3.9}$$

3.10 Teorema. *Un polinomio* $f(h) = \sum_{i=0}^{n} a_i \binom{h}{i}$ *è in* $\mathbb{P}_{\mathbb{Z}}$ *se e solo se* $a_i \in \mathbb{Z}, \ \forall i$.

Dim. Per induzione su n, se $n = 0$ il polinomio è costante e l'enunciato evidente. Se $a_i \in \mathbb{Z}, \ \forall i$ è chiaro che $f \in \mathbb{P}_{\mathbb{Z}}$. Viceversa se $f \in \mathbb{P}_{\mathbb{Z}}$ si ha anche $\sum_{i=1}^{n} a_i \binom{h}{i-1} = \Delta f \in \mathbb{P}_{\mathbb{Z}}$ e per induzione $a_i \in \mathbb{Z}, \ \forall i > 0$ anche $a_0 \in \mathbb{Z}$ perché $a_0 = f(0)$. □

Abbiamo una specie di *integrale finito* $\Sigma f(j) := \sum_{i=0}^{j-1} f(i)$. Abbiamo

$$\Delta\Sigma f(j) = \sum_{i=0}^{j} f(i) - \sum_{i=0}^{j-1} f(i) = f(j), \quad \Sigma\binom{h}{i} = \binom{h}{i+1}.$$

Segue da 3.8 che nelle ipotesi del teorema, se $\dim M_i$ è un polinomio per i grande di grado $b-1$ si ha che, per i grande, $\sum_{i \leq n} \dim M_i$ è un polinomio di grado $b \leq n$ e che il suo coefficiente direttivo è del tipo $\frac{a}{b!}$ con a intero positivo.

3.11 Definizione. *I numeri* b, a *precedenti vengono detti:*
dimensione *e* **molteplicità** *del modulo* M.

Riprendiamo la dimensione di Gelfand Kirillov.
Sia M un modulo finitamente generato su $A = k[x_1, \ldots, x_n]$, fissiamo dei generatori $m_1, \ldots, m_h$ di M come modulo, abbiamo la filtrazione $M_n := \{\langle x_{i_1} x_{i_2} \ldots x_{i_m} m_i \rangle, \ m \leq n\}$ e la costruzione di $gr(M) := \oplus M_{i+1}/M_i$.

Evidentemente $\dim M_i = \sum_{j<i} \dim \frac{M_{j+1}}{M_j}$ pertanto $\dim M_i$ è un polinomio di grado $b \leq n$ per $i >> 0$ e

$$\dim_{GK} M := \limsup_{i \to \infty} \frac{\log \dim(M_i)}{\log i} = b$$

Se n_h sono altri generatori si ha che $n_h \in M_N$ per qualche N e per la filtrazione M_i' data dagli n_h si ha $M_i' \subset M_{i+N}$ quindi non solo i gradi dei due polinomi dati dalle due foltrazioni sono uguali ma anche i coefficienti direttivi, In definitiva abbiamo provato che possiamo definire per M sia la dimensione che la molteplicità.

4 Complementi sui campi

Sia $F \subset G$ una estensione finita di campi e $n = [G : F]$ il suo grado. Preso un elemento $g \in G$ consideriamo il sottocampo $F[g]$ si ha $n = [G : F] = [G : F[g]][F[g] : F]$. Possiamo pensare a g come ad una trasformazione lineare $G \to G, \ u \to gu$ di G come spazio vettoriale, se $u_1, \ldots, u_k$ è una base di G su $F[g]$ si ha che $G = \oplus_{i=1}^{k} F[g]u_i$, la trasformazione di moltiplicazione per g si decompone in k blocchi ciascuno isomorfo a $F[g]$. Se $f(x)$ è il polinomio minimo di g su F si ha $F[g] = F[x]/(f(x))$ ed il polinomio caratteristico di g come trasformazione lineare di G è $f(x)^k$.

Si definisce *traccia* risp. *norma* di g la traccia ed il determinante di g come trasformazione lineare, per mettere in evidenza i campi si scrive $Tr_{G/F}(g)$, $N_{G/F}(g)$ per questi due elementi di F. Si ha evidentemente che se $g, h \in G$, $f \in F$,

$$Tr_{G/F}(g+h) = Tr_{G/F}(g) + Tr_{G/F}(h), \qquad Tr_{G/F}(f) = nf$$

$$N_{G/F}(gh) = N_{G/F}(g) N_{G/F}(h), \qquad N_{G/F}(f) = f^n$$

Per procedere ulteriormente è necessario ricordare un poco di teoria di Galois.

Dato un polinomio monico irriducibile $f(x)$ di grado n a coefficienti in un campo F lo possiamo spezzare su una chiusura algebrica come $f(x) = \prod_{i=1}^n (x - a_i)$ dove a_i sono le sue radici. Dalla analisi precedente segue che per ogni i la norma $N_{F[a_i]/F}(a_i) = \prod_{j=1}^n a_j$.

Ricordiamo i fondamenti della teoria di Galois, gli elementi a_i sono un insieme di elementi coniugati fra loro, ma è possibile che appaiano con molteplicità positiva. Questo è un fenomeno di caratteristica $p > 0$.

Un modo formale di organizzare l'analisi è di considerare, per una estensione $F \supset E$ di grado finito, l'insieme degli E isomorfismi $\sigma : F \to \overline{F}$ dove $\overline{F}$ è la chiusura algebrica di F e σ è l'identità su E. I coniugati di un elemento $a \in F$ sono gli elementi $\sigma(a)$. F contiene una massima estensione separabile F_s di E e $[F; F_s] = p^k$ mentre $[F_s : E]$ è uguale al numero di isomorfismi σ segue facilmente che $N_{F/E}(a) = [\prod_\sigma \sigma(a)]^{p^k}$.

Sia ora $E \subset F$ una estensione finita, $g \in G$ dalla analisi precedente segue che

$$N_{G/E}(a) = N_{F/E}(N_{G/F}(a)).$$

5 Applicazioni

Vediamo ora che per una varietà irriducibile V le due idee di dimensione, tramite il grado di trascendenza o alla Gelfand Kirillov, sono uguali. Sia A l'anello delle coordinate di V su k.

Sappiamo dal lemma di normalizzazione che, se il grado di trascendenza di A su k è s allora A è un modulo di tipo finito sull'anello $k[x_1, \ldots, x_s]$ e quindi la sua dimensione di Gelfand Kirillov è $\leq s$ (cf. Esercizio 2.8, 4)). Ma anche $A \supset k[x_1, \ldots, x_s]$, ne segue immediatamente che la sua dimensione di Gelfand Kirillov è esattamente s. In altre parole:

5.1 TEOREMA. *Una varietà V ha dimensione n se e solo se esiste un morfismo suriettivo e finito $p : V \to k^n$.*

Se $p : V \to W$ è un morfismo finito e suriettivo $\dim V = \dim W$.

DIM. La prima parte è una riformulazione dei teoremi di normalizzazione e delle osservazioni sulla dimensione. La seconda segue dalla prima. □

Riprendiamo ora la discussione del teorema 10.5 partiamo da un morfismo $p : V \to W$ dominante di varietà irriducibili. Esiste una $f \neq 0$ tale che il morfismo ristretto agli aperti $p_f : V_f \to W_f$ si può scomporre come:

$$p_f : V_f \xrightarrow{q} W_f \times k^s \xrightarrow{\pi_1} W_f, \quad q \quad \text{finito e,} \quad \pi_1 \quad \text{la prima proiezione}$$

Per un punto $Q \in W_f$ si ha che $p^{-1}(Q) = q^{-1}(\pi^{-1}(Q)) = q^{-1}(Q \times k^s)$, poichè $q : q^{-1}(Q \times k^s) \to Q \times k^s$ è finito e suriettivo si ha $\dim p^{-1}(Q) = s$:

$$\dim V = \dim V_f = \dim(W_f \times k^s) = \dim W_f + s = \dim W + s = \dim W + \dim p^{-1}(Q)$$

In altre parole:

5.2 Teorema. *Per un morfismo dominante $p : V \to W$ di varietà irriducibili la dimensione della fibra generica è* $\dim V - \dim W$.

Passiamo ora ad un'altra importante caratteristica della dimensione.

5.3 Teorema. *Sia V una varietà irriducibile, $f \in k[V]$ una funzione e W una componente (non vuota) della sottovarietà $V(f)$ definita da $f = 0$.*

$$\dim W = \dim V - 1, \quad \text{teorema dell'ideale principale} \tag{5.4}$$

Dim. In 2.2 iii) abbiamo visto questo Teorema nel caso in cui $V = k^n$ lo spazio affine, in questo caso abbiamo sfruttato la fattorizzazione unica dei polinomi, questa non è vera in generale e faremo una riduzione a tale caso. Prima di tutto ci possiamo ridurre al caso in cui $V(f)$ è irriducibile. Decomponiamo $V(f) = W \cup Z$, sia g una funzione che si annulla su Z ma non su W si ha $V(f) \cap V_g = W \cap V_g$. Possiamo sostituire V con V_g, poiché $\dim W \dim W_g$ e supporre W irriducibile. Ora applichiamo il Lemma di normalizzazione e troviamo un morfismo finito e suriettivo $p : V \to k^n$, $n = \dim V$. Basta pertanto provare che $p(W)$ ha dimensione $n - 1$ (dal teorema precedente).

Consideriamo l'estensione finita di campi $k(V) \supset k(k^n) = k(x_1, \dots, x_n)$. La moltiplicazione per f è una trasformazione lineare di $k(V)$ pensato come spazio vettoriale su $k(x_1, \dots, x_n)$ il suo determinante è detto norma $N(f)$ di f. Mostriamo che, $N(f) \in k[x_1, \dots, x_n]$ e che $p(W)$ coincide con la ipersuperficie $V(N(f))$. Questo termina la dimostrazione. f soddisfa per ipotesi un polinomio monico a coefficienti in $k[x_1, \dots, x_n]$ le cui radici sono pertanto integrali su $k[x_1, \dots, x_n]$, lo stesso vale dunque per il polinomio minimo e per il polinomio caratteristico che è una potenza del polinomio minimo, ne segue che $N(f) \in k(x_1, \dots, x_n)$ è integrale su $k[x_1, \dots, x_n]$, poiché quest'ultimo è integralmente chiuso si ha $N(f) \in k[x_1, \dots, x_n]$, lo stesso vale per tutti i coefficienti del polinomio caratteristico $t^n + a_1 t^{n-1} + \cdots + N(f)$, di f. Da $f^n + a_1 f^{n-1} + \cdots + N(f) = 0$ segue che, se $Q \in V(f)$ allora $p(Q) \in V(N(f)$, vediamo il viceversa. Se $g \in k[x_1, \dots, x_n]$ svanisce su $p(V(f))$ vuol dire che $g \in \sqrt{(f)}$ ovvero $g^m = af \in k[V]$. Prendendo le norme si ha $g^{nm} = N(g^m) = N(a)N(f)$ ovvero $g \in \sqrt{N(f)}$.

□

A questo punto possiamo vedere la dimensione di una varietà irriducibile in un modo diverso che si può generalizzare agli anelli Noetheriani.

5.5 PROPOSIZIONE. *Siano $V \supsetneq W$ varietà irriducibili e supponiamo che W sia massimale in V ovvero non vi sia alcuna varietà irriducibile Z con $V \supsetneq Z \supsetneq W$. Allora* $\dim W = \dim V - 1$.

DIM. Sia $f \in k[V]$ una funzione non nulla che si annulla su W, pertanto $W \subset V(f)$ è contenuta in una delle componenti irriducibili di $V(f)$. Dalle ipotesi fatte W è una delle componenti irriducibili di $V(f)$. Basta applicare dunque 5.3. □

COROLLATIO. *Se V è una varietà irriducibile e $V = V_0 \supsetneq V_1 \cdots \supsetneq V_{n-1} \supsetneq V_n$ è una catena massimale di varietà irriducibili (non vuote), allora $n = \dim V$.*

DIM. Dalla proposizione precedente $\dim V_{i+1} = \dim V_i - 1$ pertanto $\dim V_n = \dim V - n$. Se $P \in V_n$ è un punto si deve avere $P = V_n$ altrimenti la catena si potrebbe allungare con P pertanto $\dim V - n = \dim V_n = 0$. □

6 Dimensione 0

Vogliamo studiare il caso speciale di un algebra $F[a_1, \ldots, a_n]$ finitamente generata su un campo F e di dimensione 0.

Questo vulo dire che ogni a_i è algebrico su F pertanto.

6.1 PROPOSIZIONE. *Un algebra $F[a_1, \ldots, a_n]$ finitamente generata su un campo F è di dimensione 0 se e solo se ha dimensione finita su F.*

Se R è un algebra di dimensione finita su F ed è un dominio, necessariamente è un campo, pertanto in un algebra di dimensione finita su F ogni ideale primo è massimale.

Se consideriamo una decomposizione primaria irridondante di $\{0\} = Q_1 \cap Q_2 \cap \cdots \cap Q_r$ abbiamo un monomorfismo $i : R \to \oplus_{i=1}^r R/Q_i$, vogliamo provare che è un isomorfismo. Vi sono vari modi di vederlo, vediamone uno ora ed un altro nel prossimo capitolo. Dalla teoria svolta nel Cap. 2 per verificare l'enunciato basta provare che i è un isomorfismo per localizzazione a tutti gli ideali massimali. Evidentemente gli ideali massimali sono gli ideali $P_i := \sqrt{Q_i}$.

Localizziamo ad esempio a P_1, preso Q_i, $i \neq 1$ poichè $P_i \subsetneq P_1$ abbiamo un $s \in P_i$, $s \notin P_1$ e per qualche k, $s^k \in Q_i$, $s^k \notin P_1$. Segue che $R_{P_1} \otimes_R R/Q_i = 0$, $\forall i \neq 1$. D'altra parte $i : R_{P_1} \to R_{P_1} \otimes_R R/Q_1$ è chiaramente suriettivo e per piattezza un isomorfismo. Osserviamo inoltre che dalla analisi fatta segue il diagramma commutativo:

$$\begin{array}{ccc} R & \xrightarrow{i} & \oplus_{i=1}^r R/Q_i \\ \downarrow & & \downarrow \\ R_{P_1} & \xrightarrow{\bar{i}} & R_{P_1} \otimes_R R/Q_1 = R_{P_1} \otimes_R \oplus_{i=1}^r R/Q_i \end{array}$$

Ne segue facilmente che, per ogni i si ha che Q_i è il nucleo della localizzazione $R \to R_{P_i}$. Abbiamo provato:

6.2 TEOREMA. *Un algebra R di dimensione finita su un campo F è somma diretta in modo unico di algebre locali.*