Introduzione alle varietà algebriche
Un punto di vista costruttivo

Note di Giorgio Ottaviani

1. GENERALITÀ SULL'ANELLO DEI POLINOMI

Sia K un campo. Siamo interessati all'anello dei polinomi $K[x_1, \ldots, x_n]$. Come esempi consideriamo $K = \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Z}_p$ (quest'ultimo campo con p primo, $p \gg 0$ è molto utilizzato in computer algebra e può simulare con maggiore efficienza un campo di caratteristica zero quando i coefficienti dei polinomi in gioco sono "piccoli"). Useremo la seguente proprietà, nota dai corsi di algebra:

Teorema 1.1. *(Gauss) $K[x_1, \ldots, x_n]$ è un dominio a fattorizzazione unica (UFD) cioè ogni polinomio si decompone in modo unico come prodotto di fattori irriducibili.*

Ricordiamo che un anello A si dice noetheriano [1] se ogni suo ideale è finitamente generato. Questo equivale alla condizione della catena ascendente, cioè ogni catena ascendente di ideali $I_1 \subset I_2 \subset I_3 \subset \ldots$ è stazionaria nel senso che $\exists\ n$ tale che $I_n = I_{n+1} = I_{n+2} = \ldots$

In particolare ogni campo K è noetheriano perché gli unici suoi ideali sono 0 e K.

Teorema della base di Hilbert 1.2. *(Basissatz). Sia R un anello.*

$$R \text{ è noetheriano} \Longrightarrow R[x] \text{ è noetheriano}$$

Dimostrazione (H. Sarges, 1976) Sia R un anello noetheriano e consideriamo (per assurdo) un ideale $I \subset R[x]$ non finitamente generato. Scegliamo $f_1 \in I$ di grado minimo. Scegliamo poi $f_2 \in I \setminus (f_1)$ ancora di grado minimo e procedendo in questo modo troviamo $f_k \in I \setminus (f_1, \ldots, f_{k-1})$ di grado minimo. Sia $n_k := deg\ f_k$ e sia $f_k = a_k x^{n_k} + \ldots$ Abbiamo ovviamente $n_1 \leq n_2 \leq \ldots$ e $(a_1) \subset (a_1, a_2) \subset \ldots$. Per ipotesi $\exists\ \ p$ tale che $(a_1, \ldots, a_p) = (a_1, \ldots, a_{p+1})$ e quindi si può scrivere $a_{p+1} = \sum_{i=1}^{p} b_i a_i$ con $b_i \in R$. Poniamo $g := f_{p+1} - \sum_{i=1}^{p} x^{n_{p+1} - n_i} b_i f_i$. Quindi il termine di grado massimo di g è

$$a_{p+1} x^{n_{p+1}} - \sum_{i=1}^{p} b_i a_i x^{n_{p+1}} = 0$$

da cui $deg\ g < n_{p+1}$. D'altronde $g \in I$ e $g \notin (f_1, \ldots, f_p)$ (altrimenti $f_{p+1} \in (f_1, \ldots f_p)$). Questa è una contraddizione perché f_{p+1} era stato scelto come un polinomio di grado minimo in $I \setminus (f_1, \ldots, f_p)$.

Corollario 1.3. *Sia R un anello.*

$$R \text{ è noetheriano} \Longrightarrow R[x_1, \ldots, x_n] \text{ è noetheriano}$$

Dimostrazione Per induzione su n considerando che

$$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$$

Corollario 1.4. *Sia K un campo. Allora $K[x_1, \ldots, x_n]$ è noetheriano.*

La seguente proposizione sarà utile in seguito.

[1] in ricordo di Emmy Noether (1882-1935)

Proposizione 1.5. *Se un ideale I di un anello noetheriano R è generato da $(f_i)_{i\in I}$ allora si può estrarre dagli f_i un numero finito di generatori $f_{i_1}, \ldots, f_{i_n}$*

Dimostrazione Scegliamo $f_{i_1} \in I$. Se $(f_{i_1}) \subset_{\neq} I$ allora scegliamo $f_{i_2} \in I$ tale che $(f_{i_1}) \subset_{\neq} (f_{i_1}, f_{i_2})$. Se $(f_{i_1}, f_{i_2}) \subset_{\neq} I$ allora scegliamo $f_{i_3} \in I$ tale che $(f_{i_1}, f_{i_2}) \subset_{\neq} (f_{i_1}, f_{i_2}, f_{i_3})$. Così procedendo si trova ad un certo punto un numero finito di generatori oppure si costruisce una catena ascendente di ideali non stazionaria contro l'ipotesi.

Per $n = 1$ l'anello dei polinomi in una variabile gode di un'altra proprietà importante: è un dominio a ideali principali (PID). Infatti per ogni ideale I di $K[x]$ esiste $f \in K[x]$ tale che $I = (f)$. Quest'ultima proprietà permette di risolvere facilmente il seguente

Problema di appartenenza in $K[x]$. *Dato un ideale I in $K[x]$, esiste un algoritmo per decidere se $g \in I$?*

Infatti basta effettuare la divisione di g per il generatore f dell'ideale I. Abbiamo $g = qf + r$ con $deg\ r < deg\ f$. r si dice il resto. Segue che $g \in I$ se e solo se il resto della divisione di g per f è zero.

È naturale il seguente problema analogo

Problema di appartenenza in $K[x_1, \ldots, x_n]$. *Dato un ideale I in $K[x_1, \ldots, x_n]$, esiste un algoritmo per decidere se $g \in I$?*

Questo secondo problema è complicato dal fatto che l'ideale I non è necessariamente principale e quindi occorre eseguire una divisione per tutti i suoi generatori $f_1, \ldots, f_k$. Vorremmo trovare un'espressione $g = q_1 f_1 + \ldots + q_k f_k + r$ e concludere che $g \in I$ se e solo se $r = 0$. Per fare questo occorre generalizzare l'algoritmo di divisione al caso di più polinomi. Prima di fare questo è allora opportuno approfondire su quali concetti si basa effettivamente il ben noto algoritmo di divisione per polinomi in una variabile.

L'algoritmo di divisione per polinomi in una variabile.

Dato un polinomio $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ definiamo $LT(f) := a_n x^n$ (leading term) e $LM(f) := x^n$ (leading monomial). Ovviamente $deg\ (f) = deg(LT(f))$. Per effettuare la divisione di g per f controlliamo se $deg\ (LT(g)) < deg\ (LT(f))$. In caso affermativo il quoziente è zero ed il resto è uguale a g ($g = 0 \cdot f + g$). In caso negativo sommiamo $\frac{LT(g)}{LT(f)}$ al quoziente (che è inizialmente nullo), sostituiamo $g - \frac{LT(g)}{LT(f)} f$ al posto di g e continuiamo come sopra. Questo ciclo ha termine perché ad ogni passo $deg\ \left(g - \frac{LT(g)}{LT(f)} f\right) < deg\ g$ e quindi troviamo una successione strettamente decrescente di gradi che ad un certo punto diventano minori di $deg\ f$.

Il risultato può essere riassunto così:

Teorema 1.6. *Dati g, $f \in K[x]$ esistono (unici) q, $r \in K[x]$ tali che $g = fq + r$ e $deg\ r < deg\ f$. In piú esiste un algoritmo che determina q, r.*

Il lettore è invitato a verificare questo ben noto algoritmo nel caso $g = x^4 + x + 1$, $f = 2x^2 + x + 1$. Si trova $q = \frac{1}{2}x^2 - \frac{1}{4}x - \frac{1}{8}$, $r = \frac{11}{8}x + \frac{9}{8}$.

L'algoritmo può essere sintetizzato nel modo seguente:

$INPUT(g, f)$

$q := 0$

$r := g$

$WHILE \quad r \neq 0 \quad AND \quad deg\, LT(f) \leq deg\, LT(r) \quad DO$

$$q := q + \frac{LT(r)}{LT(f)}$$
$$r := r - \frac{LT(r)}{LT(f)} f$$

$OUTPUT(q, r)$

Osservazione. *Il fatto che ogni ideale di $K[x]$ è principale è una conseguenza dell' algoritmo di divisione. L'algoritmo euclideo per calcolare il MCD di due polinomi è basato sull' algoritmo di divisione e permette di calcolare il generatore di un ideale se è noto un insieme di generatori (necessariamente in numero finito per la noetherianità).*

Esercizio.

i) *Stabilire se* $x^4 + x^3 + x^2 + x + 1 \in \left(x^2 + x + 1\right)$.

ii) *Stabilire se* $x^3 + 4x^2 + 3x - 6 \in \left(x^3 - 3x + 2, x^4 - 1, x^6 - 1\right)$.

L'algoritmo di divisione per polinomi in più variabili. Ordini monomiali.

Uno dei fatti essenziali che assicura il successo dell'algoritmo di divisione per polinomi in una variabile è che dati due leading term uno dei due è sempre divisibile per l'altro. In altre parole la relazione "x^n divide x^m" è una relazione di ordine totale sui monomi in una variabile, che si identifica con la relazione di ordine usuale sull'insieme dei numeri naturali.

Inoltre una successione di monomi che è strettamente decrescente sui gradi termina dopo un numero finito di passi. Infatti l'ordine usuale sui numeri naturali è un buon ordinamento, cioè ogni sottoinsieme ammette un minimo.

Tra i monomi in più variabili la relazione di divisibilità definisce soltanto un ordine parziale. Ad esempio x non è divisibile per y e viceversa. Vogliamo definire alcuni ordini totali "ragionevoli" tra i monomi in più variabili. I monomi appartenenti all'anello $K[x_1, \ldots, x_n]$ sono in corrispondenza biunivoca con gli elementi di $\mathbf{Z}^n_{\geq 0}$, infatti possiamo identificare il monomio $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ con la n-pla $(\alpha_1, \ldots \alpha_n)$ dove α_i sono interi non negativi. Osserviamo che con queste notazioni $x^\alpha \cdot x^\beta = x^{\alpha+\beta}$. Poniamo $|\alpha| = \sum_i \alpha_i$.

Definizione 1.7. *Un ordine monomiale in $K[x_1, \ldots, x_n]$ è una relazione $>$ su $\mathbf{Z}^n_{\geq 0}$ tale che:*

i) *$>$ è un ordine totale*

ii) *$>$ è compatibile con la moltiplicazione, cioè $\forall \alpha, \beta, \gamma$ con $\alpha > \beta$ vale $\alpha + \gamma > \beta + \gamma$*

iii) *$>$ è un buon ordinamento.*

Scriveremo indifferentemente $\alpha > \beta$ oppure $x^\alpha > x^\beta$.

Lemma 1.8. *Notiamo che in un qualunque ordine monomiale* $1 < x^\alpha \quad \forall \alpha$.

Dimostrazione Altrimenti sarebbe $1 > x^\alpha$ da cui moltiplicando per x^α e usando ii) della def. 1.7 segue $x^\alpha > x^{2\alpha}$. Continuando si trova la catena $1 > x^\alpha > x^{2\alpha} > \ldots > x^{n\alpha} > \ldots$ in contrasto col fatto che ogni ordine monomiale è un buon ordinamento.

Corollario 1.9. *Se* x^α *divide* x^β *allora in un qualunque ordine monomiale* $x^\alpha < x^\beta$. *Pertanto ogni ordine monomiale è un raffinamento dell'ordine parziale definito dalla divisibilità.*

Dimostrazione Per ipotesi $\beta = \alpha + \gamma$ con $\gamma \in \mathbf{Z}^n_{\geq 0}$. Dal lemma $1 < x^\gamma$ e quindi dalla ii) della def. 1.7 segue $x^\alpha < x^{\alpha+\gamma} = x^\beta$.

Osservazione. *Dal corollario 1.9 segue che in* $K[x]$ *esiste un solo ordine monomiale che é quello usuale.*

È bene sapere subito che alcuni ordini monomiali sono preferibili ad altri dal punto di vista computazionale, secondo le applicazioni a cui si è interessati.

Ci sono tre ordini monomiali particolarmente importanti:

1) LEX ordine lessicografico: si definisce $\alpha >_{lex} \beta$ se in $\alpha - \beta$ il primo coefficiente non nullo da sinistra è positivo. In particolare $x_1 > x_2 > \ldots > x_n$ ed un monomio di grado 10 in x_1 è maggiore di tutti i monomi di grado 9 in x_1 e minore di tutti i monomi di grado 11 in x_1. Se il grado in x_1 è uguale si guarda il grado in x_2 e così via.

2) DEGLEX ordine lessicografico graduato: si definisce $\alpha >_{deglex} \beta$ se $\sum \alpha_i > \sum \beta_i$ oppure se $\sum \alpha_i = \sum \beta_i$ e in $\alpha - \beta$ il primo coefficiente non nullo da sinistra è positivo.

3) DEGREVLEX ordine lessicografico inverso graduato: si definisce $\alpha >_{degrevlex} \beta$ se $\sum \alpha_i > \sum \beta_i$ oppure se $\sum \alpha_i = \sum \beta_i$ e in $\alpha - \beta$ il primo coefficiente non nullo da destra è negativo.

I nomi LEX, DEGLEX, DEGREVLEX sono gli stessi usati dal sistema di calcolo simbolico Cocoa.

Vedremo che LEX è utile per eliminare variabili, (vedi§4) mentre DEGREVLEX è ottimale per il calcolo delle sizigie.

Un ordine monomiale si dice graduato se $x^\alpha > x^\beta$ quando $|\alpha| > |\beta|$. DEGLEX e DEGREVLEX sono graduati, mentre LEX non lo è.

Esempi.

$$x^2y >_{lex} xy^2 \qquad x^2y >_{degrevlex} xy^2$$

$$x^2yz^2 >_{lex} xy^3z \qquad x^2yz^2 <_{degrevlex} xy^3z$$

Definizione 1.10. *Sia fissato un ordine monomiale e sia* $f \in K[x_1, \ldots, x_n]$. *Il multigrado di* f *è la n-pla massima tra quelle corrispondenti ai termini di* f *con l'ordine prescelto e si indica con MULTIDEG(f). LT(f) é il termine di* f *corrispondente alla n-pla massima.*

Vediamo come possiamo impostare la divisione di f per $f_1, \ldots f_h$. Vogliamo scrivere $f = a_1 f_1 + \ldots + a_h f_h + r$. Analogamente al caso dei polinomi in una variabile, chiediamo che $LT(r)$ non divida nessun $LT(f_i)$, vedremo però che questo è troppo poco.

Procediamo nel modo seguente:

- Poni $p := f$ (resto ausiliario)
- Dividi $LT(p)$ successivamente per $LT(f_1), \ldots, LT(f_h)$ e quando questo è possibile aggiungi $LT(p)/LT(f_i)$ all'i-esimo quoziente e sottrai $f_i \frac{LT(p)}{LT(f_i)}$ dal resto ausiliario p. Quando $LT(p)$ non è più divisibile per nessuno tra $LT(f_1), \ldots, LT(f_h)$ allora aggiungi $LT(p)$ al resto e continua con $p - LT(p)$ al posto di p.

L'algoritmo ha termine quando il resto ausiliario diventa nullo. Questo accade sempre perché ad ogni passo il multigrado del resto ausiliario p decresce strettamente e l'ordine monomiale scelto è un buon ordinamento.

Esempio 1.11. *Dividiamo in $K[x,y]$ con DEGLEX $x^6y^3 + 2x^3y^2 - y + 1$ per $xy^2 - x$ e $y^3 - x$. Il LT del dividendo è x^6y^3 che è divisibile per xy^2. Dividendo otteniamo x^5y come primo quoziente ed il resto ausiliario è $x^6y + 2x^3y^2 - y + 1$ che ha x^6y come LT. x^6y non è divisibile per nessuno tra i LT dei divisori, pertanto si aggiunge x^6y al resto e si continua a dividere partendo da $2x^3y^2 - y + 1$. Continuando otteniamo il seguente schema:*

$x^6y^3 + 2x^3y^2 - y + 1$	$xy^2 - x$	$y^3 - x$	RESTO

Eseguiamo la divisione, scrivendo i resti ausiliari e le operazioni svolte sotto il dividendo:

$x^6y^3 + 2x^3y^2 - y + 1$	$xy^2 - x$	$y^3 - x$	RESTO
$x^6y^3 - x^6y$	x^5y		
$x^6y + 2x^3y^2 - y + 1$			
$2x^3y^2 - y + 1$ $\longrightarrow$			x^6y

Andando avanti:

$x^6y^3+2x^3y^2-y+1$	xy^2-x	y^3-x	RESTO
$x^6y^3-x^6y$	x^5y+2x^2		
$x^6y+2x^3y^2-y+1$			
$2x^3y^2-y+1$	$\longrightarrow$		x^6y
$2x^3y^2-2x^3$			
$2x^3-y+1$			
0	$\longrightarrow$		$2x^3-y+1$

da cui

$$x^6y^3+2x^3y^2-y+1=(x^5y+2x^2)(xy^2-x)+0(y^3-x)+x^6y+2x^3-y+1$$

Se scambiamo l'ordine dei divisori otteniamo

$x^6y^3+2x^3y^2-y+1$	y^3-x	xy^2-x	RESTO
$x^6y^3-x^7$	x^6	$2x^2$	
$x^7+2x^3y^2-y+1$			
$2x^3y^2-y+1$	$\longrightarrow$		x^7
$2x^3y^2-2x^3$			
$2x^3-y+1$			
0	$\longrightarrow$		$2x^3-y+1$

da cui

$$x^6y^3+2x^3y^2-y+1=2x^2(xy^2-x)+x^6(y^3-x)+x^7+2x^3-y+1$$

Quindi scambiando l'ordine dei divisori sia i quozienti che il resto cambiano.

Esercizio. *Verificare che dividendo con LEX* xy^2-x *per* $xy+1$ *e* y^2-1 *otteniamo*

$$xy^2-x=y(xy+1)+0(y^2-1)-y-x$$

mentre scambiando l'ordine dei divisori:

$$xy^2-x=0(xy+1)+x(y^2-1)$$

Osserviamo dall'esercizio precedente che la condizione

$$\text{resto della divisione di } f \text{ per } \{f_1,\dots,f_h\} \quad = \quad 0$$

è una condizione sufficiente ma non necessaria affinché $f \in (f_1, \ldots, f_h)$. Questo è in contrasto con quanto accade per polinomi in una variabile. Ovvieremo a questo inconveniente definendo un insieme opportuno di generatori per l'ideale $(f_1, \ldots, f_h)$, "adattato" all'ordine monomiale scelto.

Il diagramma di flusso che descrive l'algoritmo di divisione per polinomi in piú variabili é il seguente:

$INPUT(f_1, \ldots, f_h, f)$

$q_1 := 0, \ldots q_h := 0$

$r := 0, p := f$

$p = 0$? SI $OUTPUT(q_1, \ldots, q_h, r)$

NO

Qualcuno tra $LT(f_i)$

divide $LT(p)$?

SI NO

se $LT(f_j)$ divide $LT(p)$

poni

$q_j := q_j + \frac{LT(p)}{LT(f_j)}$

$p := p - \frac{LT(p)}{LT(f_j)} f_j$

$p := p - LT(p)$

$r := r + LT(p)$

L'algoritmo di divisione per polinomi in più variabili può essere descritto in linguaggio strutturato nel modo seguente:

$INPUT(f_1, \dots f_h, f)$

$q_1 := 0, \dots q_h := 0, r := 0$

$p := f$

$WHILE\ p \neq 0\ DO$

$i := 1$

$DIV := FALSE$

$WHILE\ i \leq h\ AND\ DIV = FALSE\ DO$

$IF\ LT(f_i)\ divide\ LT(p) THEN$

$q_i := q_i + \frac{LT(p)}{LT(f_i)}$

$p := p - f_i * \frac{LT(p)}{LT(f_i)}$

$DIV := TRUE$

$ELSE\ i := i + 1$

$IF\ DIV = FALSE\ THEN$

$r := r + LT(p)$

$p := p - LT(p)$

$OUTPUT(q_1, \dots, q_h, f)$

L'algoritmo di divisione si riassume nel seguente risultato

Teorema 1.12. *Sia fissato un ordine monomiale in* $K[x_1, \dots, x_n]$. *Siano dati*

$$f, f_1, \dots, f_h \in K[x_1, \dots, x_n]$$

Allora esistono

$$q_1, \dots, q_h, r \in K[x_1, \dots, x_n]$$

tali che

i) $f = \sum q_i f_i + r$

ii) nessun termine di r *è divisibile per* $LT(f_1), \dots, LT(f_h)$.

iii) se $q_i f_i \neq 0$ *vale* $MULTIDEG\ f \geq MULTIDEG\ (q_i f_i)$.

In piú esiste un algoritmo che determina $q_1, \dots, q_h, r$.

2. IDEALI MONOMIALI E BASI DI GRÖBNER

Definizione 2.1. *Un ideale si dice monomiale se può essere generato da monomi.*

Come corollario della prop. 1.5 abbiamo che ogni ideale monomiale è generato da un numero finito di monomi (lemma di Dickson).

Con la notazione $< f_i, i \in I >$ intendiamo l'ideale generato dagli elementi f_i.

Lemma 2.2. *Sia* $I =< x^\alpha, \alpha \in A >$ *un ideale monomiale. Abbiamo che*

$$x^\beta \in I \Longleftrightarrow x^\alpha | x^\beta \text{ per qualche } \alpha \in A$$

Dimostrazione $\Leftarrow$ è ovvia.

Per provare $\Rightarrow$ scriviamo $x^\beta = \sum h_i x^{\alpha(i)}$. A secondo membro ogni termine è divisibile per qualche $x^{\alpha(i)}$, pertanto tale proprietà deve rimanere vera anche a primo membro (dopo ever effettuato tutte le cancellazioni).

Lemma 2.3. *Sia* I *un ideale monomiale. Sono equivalenti*

i) $f \in I$

ii) ogni termine di f *appartiene a* I.

Dimostrazione ii) $\Rightarrow$ i) è banale.

Per provare i) $\Rightarrow$ ii) scriviamo $f = \sum_i f_i$ (ogni f_i è un termine)$= \sum_j g_j m_j$ (ogni m_j è un monomio in I). A secondo membro ogni termine appartiene a I, quindi questo è vero anche a primo membro che è ottenuto cancellando tra loro alcuni termini a secondo membro.

Corollario 2.4. *Due ideali monomiali sono uguali se e solo se contengono gli stessi monomi.*

Il corollario precedente permette quindi di identificare gli ideali monomiali con dei sottoinsiemi di $\mathbf{Z}^n_{\geq 0}$. Ad esempio gli ideali monomiali (x^4, x^3y, y^6) e (xy) in $K[x, y]$ corrispondono rispettivamente alle parti tratteggiate seguenti:

Da queste rappresentazioni il lettore interessato può ricavare una dimostrazione diretta del lemma di Dickson indipendente dal teorema della base di Hilbert (si veda [CLO]).

Definizione 2.5. *Un insieme di monomi B si dice una base minimale per un ideale monomiale I se i monomi di B generano I e se nessun monomio di B divide qualche altro monomio di B.*

La seguente proposizione dovrebbe essere evidente dalle rappresentazioni grafiche descritte sopra.

Proposizione 2.6. *Sia I un ideale monomiale. Allora esiste una unica base minimale per I.*

Dimostrazione L'esistenza di una base minimale segue subito prendendo un insieme di generatori ed eliminando i monomi divisi da qualcun altro. L'unicità è evidente dal lemma 2.2.

Definizione 2.7. *Sia I un ideale di $K[x_1, \ldots, x_n]$ e sia fissato un ordine monomiale. Poniamo*

$$LT(I) := \{LT(f) | f \in I\}$$

L'ideale generato da $LT(I)$ si indica con $< LT(I) >$ e risulta allora un ideale monomiale.

Osservazione. *Se $I = (g_1, \ldots g_k)$ allora $< LT(I) > \supset (LT(g_1), \ldots, LT(g_k))$ ma può valere l'inclusione stretta come mostra il seguente*

Esempio. *Sia $I = \left(x^2 + y, x^2 - y\right) \subset K[x, y]$ con un qualunque ordine monimiale graduato. Allora $y \in I$ da cui $y \in < LT(I) >$ mentre $y \notin \left(LT(x^2 + y), LT(x^2 - y)\right) = \left(x^2\right)$*

L'osservazione precedente motiva la seguente

Definizione 2.8. *Un insieme $(g_1, \ldots, g_k)$ di elementi di I si dice una base di Gröbner per I se*

$$< LT(I) >= (LT(g_1), \ldots, LT(g_k))$$

Proposizione 2.9. *Ogni ideale di $K[x_1, \ldots, x_n]$ ammette una base di Gröbner.*

Dimostrazione È sufficiente estrarre dall'insieme $LT(I)$ un numero finito di generatori per $< LT(I) >$. Questo è sempre possibile per noetherianità (si veda la prop.1.5).

La dimostrazione precedente è non costruttiva. Buchberger sviluppó nel 1965 (nella sua tesi di dottorato) un algoritmo per calcolare effettivamente una base di Gröbner a partire da un insieme di generatori. Vedremo questo algoritmo nel §3

Teorema 2.10. *Una base di Gröbner per I genera I.*

Dimostrazione

Sia $g_1, \ldots, g_k$ una base di Gröbner, pertanto $< LT(I) >= (LT(g_1), \ldots, LT(g_k))$. Se $f \in I$ allora per l'algoritmo di divisione possiamo scrivere $f = \sum a_i g_i + r$ da cui

$r = f - \sum a_i g_i \in I$ ed in particolare $LT(r) \in (LT(g_1), \ldots, LT(g_k))$. Se fosse $r \neq 0$ allora dal teorema 1.12 $LT(r)$ non è divisibile per nessuno dei $LT(g_i)$ e questa è una contraddizione con il lemma 2.2.

Esempio. *Sia $I = \left(x^2 + y^2, xy\right) \subset K[x, y]$ con l'ordine LEX. Una base di Gröbner per I è costituita da almeno tre elementi.*

Infatti osserviamo che tutti i monomi di grado 3 appartengono ad I (e quindi anche a $< LT(I) >$:

$$\begin{aligned} x^3 &= x(x^2 + y^2) - y(xy) \\ x^2 y &= x(xy) \\ xy^2 &= y(xy) \\ y^3 &= y(x^2 + y^2) - x(xy) \end{aligned}$$

Ne segue che tutti i polinomi omogenei di grado 3 appartengono a $< LT(I) >$. Siccome ogni monomio di grado ≥ 3 é divisibile per un monomio di grado 3, segue che ogni monomio di grado ≥ 3 appartiene a I (e quindi anche a $< LT(I) >$. Anche x^2 e xy appartengono a $< LT(I) >$ e devono appartenere ad un qualunque insieme di generatori di $< LT(I) >$. Infine notiamo che $y^3 \notin (x^2, xy)$ e quindi sono necessari almeno tre elementi come asserito. La rappresentazione grafica di $< LT(I) >$ è la seguente:

Esercizio. *Trovare una base di Gröbner per I dell'esempio precedente (affronteremo di nuovo questo problema nell'esercizio 3.2 1). L'utilità delle basi di Gröbner è subito illustrata dal seguente:*

Teorema 2.11. *Sia $G = g_1, \ldots, g_t$ una base di Gröbner per l'ideale $I \subset K[x_1, \ldots, x_n]$. Sia $f \in K[x_1, \ldots, x_n]$. Allora esiste unico $r \in K[x_1, \ldots, x_n]$ tale che:*

i) nessun termine di r è divisibile per qualche $LT(g_i)$

ii) esiste $g \in I$ tale che $f = g + r$

In particolare r è il resto della divisione di f per G.

Dimostrazione L'esistenza di r è mostrata dall'algoritmo di divisione (vedi teor. 1.12). Per provare l'unicità consideriamo $f = g' + r' = g'' + r''$. Allora $r'' - r' = g' - g'' \in I$ da cui $LT(r'' - r') \in < LT(I) >= (LT(g_1), \ldots, LT(g_k))$. Se $r'' - r' \neq 0$ allora $LT(r'' - r')$ sarebbe divisibile per qualche $LT(g_i)$ e questo è impossibile perché nessun termine di r' o di r'' è divisibile per qualche $LT(g_i)$.

Esercizi.

1) Sia $I = (g_1, g_2, g_3) \subset \mathbf{R}[x, y, z]$ dove $g_1 = xy^2 - xz + y$, $g_2 = xy - z^2$, $g_3 = x - yz^4$. Utilizzando LEX, dare un esempio di $g \in I$ tale che $LT(g) \notin < LT(g_1), LT(g_2), LT(g_3) >$.
2) Sia $G = \{x^4y^2 - z^5, x^3y^3 - 1, x^2y^4 - 2z\}$. Provare che G non è una base di Gröbner per $< G >$ rispetto a DEGREVLEX.
3) Sia $I \subset K[x_1, \ldots, x_n]$ un ideale principale. Provare che un sottoinsieme di I è una base di Gröbner per I se e solo se contiene un generatore di I.

Corollario 2.12. *Quando si divide per una base di Gröbner l'algoritmo di divisione porta sempre allo stesso resto qualunque sia l'ordine dei divisori.*

Pertanto secondo il corollario precedente esempi come 1.11 non possono capitare se si divide per una base di Gröbner. Di più vale

Corollario 2.13. *$f \in I \iff$ il resto della divisione di f con una base di Gröbner di I è zero*

Dimostrazione $\Leftarrow$ è ovvia
$\Rightarrow$ $f = f + 0$ nel teorema 2.11.

Il corollario precedente risolve quindi il problema di appartenenza posto dopo la prop. 1.5 se si conosce una base di Gröbner.

Proposizione 2.14. *Il resto della divisione di un polinomio f per una base di Gröbner di I dipende solo da I e non dalla base di Gröbner scelta.*

Dimostrazione Supponiamo di avere (con ovvie notazioni) $f = \sum a_i g_i + r = \sum a'_i g'_i + r'$. Allora come nella dimostrazione del teorema 2.11 abbiamo che $LT(r - r')$ sarebbe divisibile per qualche $LT(g_j)$ ed anche per qualche $LT(g'_k)$. Nessun termine di $r - r'$ può essere divisibile per qualche $LT(g_j)$ e per qualche $LT(g'_k)$ il che prova $r = r'$.

Definizione 2.15. *Scriveremo $f \ mod \ I$ per indicare il resto della divisione di f per una base di Gröbner di I. $f \ mod \ I$ dipende solo dall'ordine monomiale, ed in particolare*

$$f \in I \iff f \ mod \ I = 0$$

.

In Cocoa $f \ mod \ I$ è il resto della divisione di f per una base di Gröbner di I.

Esercizio. *Sia $f = x^4y + y^3$ e $I = (x^2 + y^2, xy)$. Fissato l'ordine LEX, calcolare $f \ mod \ I$.*

Osservazione. *L'esercizio 3.2, 2) mostra che i quozienti non sono unici: l'unicità del resto nella divisione è il massimo che si riesce ad ottenere.*

Definizione 2.16. *Siano $f, g \in K[x_1, \ldots, x_n]$ e sia $x^\gamma = m.c.m.(LM(f), LM(g))$. Definiamo la S-coppia:*

$$S(f, g) := \frac{x^\gamma}{LT(f)} f - \frac{x^\gamma}{LT(g)} g$$

Notiamo che in $S(f,g)$ i termini di multigrado γ si cancellano mentre tutti gli altri termini hanno multigrado $< \gamma$. Pertanto

$$\text{MULTIDEG } S(f,g) < \gamma$$

Una "ostruzione" a che $\{f_1, \ldots, f_h\}$ sia una base di Gröbner è

$$LT\left(S(f_i, f_j)\right) \notin \left(LT(f_1), \ldots, LT(f_h)\right)$$

Vedremo che questa è in sostanza l'unica ostruzione.

Lemma 2.17. *Supponiamo di avere una cancellazione tra i LT di un insieme di polinomi g_i. Cioè supponiamo di avere una combinazione $\sum_{i=1}^{t} c_i x^{\alpha_i} g_i$ con $c_i \in K$, $\alpha_i +$ MULTIDEG $g_i = \delta$ (se $c_i \neq 0$) e MULTIDEG $(\sum c_i x^{\alpha_i} g_i) < \delta$. Allora, posto $x^{\gamma_{jk}} := m.c.m.(LM(g_j), LM(g_k))$ esistono c_{jk} tali che*

$$\sum_{i=1}^{t} c_i x^{\alpha_i} g_i = \sum_{j,k=1}^{t} c_{jk} x^{\delta - \gamma_{jk}} S(g_j, g_k)$$

In particolare ogni termine del secondo membro ha multigrado $< \delta$

Dimostrazione Poniamo $LT(g_i) := d_i x^{\beta_i}$, quindi

$$\alpha_i + \beta_i = \delta \tag{2.1}$$

$$\sum_{i=1}^{t} c_i d_i = 0 \tag{2.2}$$

Adesso $x^{\delta-\gamma_{jk}} S(g_j, g_k) = x^{\delta-\gamma_{jk}} \left(\frac{x^{\gamma_{jk}} g_j}{d_j x^{\beta_j}} - \frac{x^{\gamma_{jk}} g_k}{d_k x^{\beta_k}} \right) =$ (per (2.1)) $= \frac{x^{\alpha_j} g_j}{d_j} - \frac{x^{\alpha_k} g_k}{d_k}$
Quindi $\sum_{i=1}^{t} c_i x^{\alpha_i} g_i = \sum_{i=1}^{t} c_i d_i \left(\frac{x^{\alpha_i} g_i}{d_i} \right) =$ (ponendo $g_{t+1} = 0$)
$= \sum_{i=1}^{t} c_i d_i \left(\sum_{j=i}^{t} \left(\frac{x^{\alpha_j} g_j}{d_j} - \frac{x^{\alpha_{j+1}} g_{j+1}}{d_{j+1}} \right) \right) =$ (scambiando le sommatorie)
$= \sum_{j=1}^{t} \sum_{i=1}^{j} c_i d_i \left(\frac{x^{\alpha_j} g_j}{d_j} - \frac{x^{\alpha_{j+1}} g_{j+1}}{d_{j+1}} \right) =$ (usando (2.2))
$\sum_{j=1}^{t-1} \sum_{i=1}^{j} c_i d_i x^{\delta - \gamma_{j,j+1}} S(g_j, g_{j+1})$ c.v.d.

3. L' ALGORITMO DI BUCHBERGER

Teorema 3.1. *(Criterio di Buchberger, 1965) Sia I un ideale di $K[x_1, \ldots, x_n]$ generato da $(g_1, \ldots, g_t)$. Sia fissato un ordine monomiale.*

$$\begin{array}{c} (g_1, \ldots, g_t) \\ \text{è una base di Gröbner per } I \end{array} \iff \begin{array}{c} \text{il resto della divisione} \\ \text{di } S(g_i, g_j) \text{per } (g_1, \ldots g_t) \\ \text{è zero } \forall i \neq j \end{array}$$

La divisione di $S(g_i, g_j)$ per $(g_1, \ldots g_t)$ può essere effettuata prendendo $g_1, \ldots, g_t$ in un ordine qualunque; segue in particolare (vedi cor.2.12) che se il resto è zero in un ordine rimane zero in tutti gli altri ordini.

Dimostrazione

$\Rightarrow$ è ovvia da $S(g_i, g_j) \in I$ e dal cor.2.13

$\Leftarrow$ Sia $f \in I$, voglio provare che $LT(f) \in < LT(g_1), \ldots, LT(g_t) >$. Per ipotesi abbiamo $f = \sum h_i g_i$ con multigrado $(f) \leq max\,(\text{multigrado}(h_i g_i))$. Sia δ il minimo tra tutte le espressioni $f = \sum h_i g_i$ di $max\,(\text{multigrado}(h_i g_i))$. Se multigrado $f = \delta$ abbiamo concluso. Sia per assurdo multigrado $f < \delta$ e poniamo $m(i) :=$ multigrado $(g_i h_i)$. Abbiamo:

$$f = \sum h_i g_i = (\text{dove il massimo multigrado a secondo membro è } \delta)$$

$$= \sum_{m(i)=\delta} h_i g_i + \sum_{m(i)<\delta} h_i g_i = \sum_{m(i)=\delta} LT(h_i) g_i + \sum_{m(i)=\delta} (h_i - LT(h_i))\, g_i + \sum_{m(i)<\delta} h_i g_i$$

I monomi nella seconda e terza somma hanno multigrado $< \delta$. Quindi nella prima somma abbiamo cancellazioni tra i LT dei g_i e possiamo applicare il lemma 2.17. Pertanto possiamo riscrivere la prima somma come combinazione dei $S(g_j, g_k)$. A loro volta questi ultimi polinomi possono essere scritti nella forma $S(g_j, g_k) = \sum a_{ijk} g_i$ per l'algoritmo di divisione (l'ipotesi è resto zero!). Siccome MULTIDEG $(a_{ijk} g_i) \leq$ MULTIDEG $S(g_j, g_k)$ (si veda il teor. 1.12), risostituendo nell' espressione iniziale abbiamo $f = \sum h'_i g_i$ con tutti i multigradi a secondo membro $< \delta$. Pertanto δ non è il minimo. Questa contraddizione conclude il ragionamento.

Esempio. *Proviamo che $(x - z^4, y - z^{10})$ è una base di Gröbner secondo LEX utilizzando il criterio di Buchberger. Abbiamo la sola S-coppia $S(x - z^4, y - z^{10}) = \frac{xy}{x}(x - z^4) - \frac{xy}{y}(y - z^{10}) = yx - yz^4 - xy + xz^{10} = xz^{10} - yz^4$. La divisione porta a:*

$xz^{10} - yz^4$	$x - z^4$	$y - z^{10}$	RESTO
$xz^{10} - z^{14}$	z^{10}	z^4	
$-yz^4 + z^{14}$ $\longrightarrow$			0
$yz^4 - z^{14}$			

$0 \longrightarrow 0$

Il resto è zero e quindi la condizione del criterio di Buchberger è verificata.

Osservazione critica. *Nel corso della dimostrazione dell'implicazione $\Leftarrow$ del criterio di Buchberger abbiamo scritto $S(g_j, g_k) = \sum a_{ijk} g_i$ usando l'algoritmo di divisione. Perché non si é fatto uso direttamente ndella definizione di $S(g_j, g_k)$ che lo esprime come combinazione di g_j e g_k?. Il punto é che la disuguaglianza*

$$MULTIDEG\ (a_{ijk} g_i) \leq MULTIDEG\ S(g_j, g_k)$$

non sarebbe stata soddisfatta!

Esercizi 3.2.

1) Provare che $G = \{x + z, y - z\}$ è una base di Gröbner rispetto a LEX.
2) Dividere xy per $x + z$, $y - z$ (rispetto a LEX, si veda l'eserc. 1). Poi dividere xy per $y - z$, $x + z$. Nei due casi il resto è lo stesso, in accordo con la prop. 2.14, ma i quozienti sono differenti. Quindi questo esercizio mostra che non si riesce ad avere l'unicità dei quozienti, in contrasto col caso dei polinomi in una sola variabile.
3) Si calcoli $S(f, g)$ rispetto a LEX nei seguenti casi:
   a) $f = 4x^2 z - 7y^2, g = xyz^2 + 3xz^4$
   b) $f = x^4 y - z^2, g = 3xz^2 - y$
   c) $f = x^7 y^2 z + 2ixyz, g = 2x^7 y^2 z + 4$
   d) $f = xy + z^3, g = z^2 - 3z$
4) $S(f, g)$ dipende dall'ordine monomiale scelto?

L'algoritmo di Buchberger

Il criterio di Buchberger suggerisce un algoritmo per costruire una base di Gröbner. Si considera $F = \{f_1, \ldots, f_k\}$ insieme di generatori di I. Indichiamo provvisoriamente con $f \mod F$ il resto della divisione di f per gli elementi di F nell'ordine in cui sono scritti. Aggiungiamo ad F stesso tutti gli elementi $[S(f_i, f_j) \mod F]$ e ripetiamo questa operazione col nuovo insieme F (più grande !). Continuando in questo modo si ottiene corrispondentemente una catena ascendente di ideali monomiali data ad ogni passo da $< LT(F) >$. Per Noetherianità la catena diventa stazionaria e questo vuol dire esattamente che dopo un certo numero di passi $[S(f_i, f_j) \mod F] = 0 \quad \forall \quad i, j$ e quindi per il criterio di Buchberger quando l'algoritmo ha termine F è una base di Gröbner.

Formalmente abbiamo:

ALGORITMO DI BUCHBERGER (Versione inefficiente)

$INPUT\ F = \{f_1, \ldots, f_k\}$

$G := F$

$REPEAT$

$G' := G$

$\forall$ coppia$\{p, q\}$ con $p \neq q$ in $G' DO$

$s := S(p, q) \bmod G'$

$IF\ s \neq 0\ THEN\ G := G \cup \{s\}$

$UNTIL\ G = G'$

$F := G$

$OUTPUT\ F$

In Cocoa il comando Gbasis(I) calcola una base di Gröbner di I mediante una versione più efficiente dell'algoritmo precedente (si veda [CLO] per approfondimenti). Precisamente viene calcolata la base di Gröbner ridotta (che vedremo nel teorema 3.6).

Esercizi.

1) *Si trovi una base di Gröbner per l'ideale $I = (x^2 + y^2, xy)$ rispetto a LEX utilizzando l'algoritmo di Buchberger.*
2) *Sia $A = (a_{ij})$ una matrice $n \times m$ a scala a coefficienti reali e sia $J \subset \mathbf{R}[x_1, \ldots, x_m]$ l'ideale generato dai polinomi $\sum_{j=1}^{m} a_{ij} x_j$ per $1 \leq i \leq n$. Provare che i generatori di J formano una base di Gröbner rispetto all'ordine LEX dove le variabili dei pivot sono maggiori rispetto alle altre.*

Come corollario abbiamo il

3.3 Algoritmo per la soluzione del problema di appartenenza in $K[x_1, \ldots, x_n]$.

Dati f e $I = (f_1, \ldots, f_k)$ per sapere se $f \in I$ è sufficiente eseguire i seguenti passi:

1) Si calcola una base di Gröbner G per I con l'algoritmo di Buchberger.
2) Si calcola il resto R della divisione di f per G.
3) Segue che $f \in I$ se e solo se $R = 0$.

Esercizi.

1) *Determinare se $f = xy^3 - z^2 + y^5 - z^3$ appartiene all'ideale $I = (-x^3 + y, x^2 y - z)$.*Suggerimento: utilizzando DEGREVLEX la base di Gröbner di I é costituita da 3 elementi, mentre utilizzando LEX o DEGLEX i calcoli sono piú complessi.
2) Determinare se $f = x^3 z - 2y^2$ appartiene all'ideale $I = (xz - y, xy + 2z^2, y - z)$.

Definizione 3.4. *Una base di Gröbner G si dice <u>minimale</u> se*

1) $\forall p \in G \quad p = x^\alpha + \ldots$ *(termini di multigrado inferiore), cioè se il coefficiente di $LT(p)$ è 1.*

2) $\forall p \in G \quad LT(p) \notin < LT(G \setminus \{p\}) >$

Da ogni base di Gröbner è sufficiente togliere elementi e poi normalizzare (dividendo ogni elemento per il coefficiente del suo LT) per trovare una base minimale. In pratica basta verificare se ogni $LT(p)$ con $p \in G$ è divisibile per qualche $LT(g)$ con $g \in G \setminus \{p\}$.

Osservazione. *Nel caso di polinomi in una sola variabile, una base minimale dell'ideale $(f_1, \ldots, f_k)$ è data dal M.C.D. di $f_1, \ldots, f_k$ e l'algoritmo di Buchberger si riconduce all'algoritmo euclideo per il calcolo del M.C.D.*

Definizione 3.5. *Una base di Gröbner G si dice ridotta se*

1) $\forall p \in G \quad p = x^\alpha + \ldots$ *(termini di multigrado inferiore), cioè se il coefficiente di $LT(p)$ è 1.*
2) $\forall p \in G$ *nessun termine di* $p \in < LT(G \setminus \{p\}) >$

Osservazione. *Base di Gröbner ridotta $\Rightarrow$ Base di Gröbner minimale*

Teorema 3.6. *Sia $I \neq 0$ un ideale di $K[x_1, \ldots, x_n]$. Sia fissato un ordine monomiale. Allora esiste una unica base di Gröbner ridotta per I ed il procedimento con cui si trova (descritto nella dimostrazione) è costruttivo.*

Dimostrazione

ESISTENZA

Partiamo da una base di Gröbner minimale per I (ottenuta con l'algoritmo di Buchberger, togliendo poi gli elementi superflui). Chiamiamo un elemento $g \in G$ ridotto per G se nessun termine di $g \in < LT(G \setminus \{g\}) >$. Preso $g \in G$ poniamo $g' := g \bmod (G \setminus \{g\})$ e consideriamo $G' := (G \setminus \{g\}) \cup \{g'\}$. Osserviamo che $LT(g) = LT(g')$ perché, nella divisione di g per $(G \setminus \{g\})$, $LT(g)$ va nel resto essendo G minimale. Inoltre g' è ridotto per G' e G' rimane una base di Gröbner minimale. Infine se un elemento era ridotto per G rimane ridotto anche per G'. Quindi procedendo in questo modo dopo un numero finito di sostituzioni successive tutti gli elementi diventano ridotti e si ottiene una base di Gröbner ridotta (eventualmente dopo avere normalizzato).

UNICITÀ

Notiamo subito che se $G, \tilde{G}$ sono due basi di Gröbner ridotte (è sufficiente che siano minimali) allora $LT(G) = LT(\tilde{G})$ ed in particolare hanno lo stesso numero di elementi (si veda la prop. 2.6 applicata a $LT(I)$). Siano adesso $g \in G$, $\tilde{g} \in \tilde{G}$ tali che $LT(g) = LT(\tilde{g})$. Vogliamo provare che $g = \tilde{g}$.

Siccome $g - \tilde{g} \in I$ abbiamo $g - \tilde{g} = 0 \bmod G$. Ma $LT(g)$ e $LT(\tilde{g})$ si cancellano in $g - \tilde{g}$ e tutti gli altri termini non sono divisibili per nessuno degli elementi di $LT(G) = LT(\tilde{G})$ perché G e $\tilde{G}$ sono ridotte. Quindi eseguendo la divisione di $g - \tilde{g}$ per G (o per $\tilde{G}$) tutti i termini vanno nel resto e si ottiene $0 = g - \tilde{g}\ mod\ G = g - \tilde{g}$ c.v.d.

Osservazione. *Nel caso di polinomi di grado 1 l'algoritmo con cui si trova una base di Gröbner minimale coincide con l'eliminazione di Gauss (si veda [CLO] per i dettagli).*

4. IL TEOREMA DI ELIMINAZIONE E L'INTERSEZIONE DI DUE IDEALI

Definizione 4.1. *Sia I un ideale di $K[x_1, \ldots, x_n]$, si pone*

$$I_k := I \cap K[x_{k+1}, \ldots, x_n]$$

I_k contiene le "conseguenze" dei polinomi di I che coinvolgono solo le variabili $x_{k+1}, \ldots, x_n$.

Teorema 4.2 (di eliminazione). *Sia I un ideale di $K[x_1, \ldots, x_n]$. Sia G una base di Gröbner per I rispetto a LEX. Allora $G_k := G \cap K[x_{k+1}, \ldots, x_n]$ è una base di Gröbner per I_k.*

Dimostrazione Riordiniamo gli elementi di $G = \{g_1, \ldots, g_m\}$ in modo che i primi r elementi $\{g_1, \ldots, g_r\}$ formino G_k. Facciamo vedere che $\{g_1, \ldots, g_r\}$ generano I_k. Dato $f \in I_k$, abbiamo che il resto della divisione di f per G è zero. Notiamo che $LT(g_{r+1}), \ldots, LT(g_m)$ contengono termini dove compare qualche $x_1, \ldots, x_k$ e quindi hanno multigrado maggiore (per LEX) di ogni monomio di f. Pertanto $g_{r+1}, \ldots g_m$ non entrano in gioco nella divisione di f per G e risulta $f = \sum_{i=1}^{r} a_i g_i$ come volevamo.

Usiamo il criterio di Buchberger per provare che $\{g_1, \ldots, g_r\}$ è una base di Gröbner per I_k. Se $1 \leq j, k \leq r$ abbiamo $S(g_j, g_k) \in I_k$. Per quanto visto sopra la divisione di $S(g_j, g_k)$ per G coincide con la divisione per G_k, quindi il resto della divisione è zero come volevamo.

Esercizi.

a) Provare che se $I = (x - y, x^2 + y^3) \subset K[x, y]$ allora $I_1 = (y^3 + y^2)$.

b) Provare che se $= (-x^3 + y, x^2 y - z) \subset K[x, y, z]$ allora $I_1 = (y^5 - z^3)$ e $I_2 = 0$.

In Cocoa il comando

$$Elim(x, I)$$

restituisce l'ideale ottenuto eliminando la x dall'ideale I. È utile anche la modifica $Elim(x..y, I)$ dove si eliminano tutte le indeterminate dell'anello comprese tra x e y (è necessario che $x > y$!).

Intersezione di due ideali

Vediamo adesso un algoritmo che permette di calcolare i generatori di $(f_1, \ldots, f_r) \cap (g_1, \ldots, g_s)$. Questo problema non è banale perché nel caso $(f) \cap I$ contiene il problema di appartenenza "$f \in I$?". Infatti $f \in I \iff (f) \cap I = (f)$.

Siano I, J due ideali di $K[x_1, \ldots, x_n]$. Definiamo tI come l'ideale di $K[x_1, \ldots, x_n, t]$ generato da tf con $f \in I$. Analogamente si puó definire $(1 - t)J$. Vale la

Proposizione 4.3.

$$I \cap J = [tI + (1 - t)J] \cap K[x_1, \ldots, x_n]$$

Dimostrazione

$\subset$ è ovvia scrivendo $f = tf + (1-t)f$

$\supset$ Sia $f(x) \in [tI + (1-t)J] \cap K[x_1, \ldots, x_n]$. Pertanto $f(x) = g(x,t) + h(x,t)$ con $g \in tI$ e $h \in (1-t)J$. In particolare

$$g(x,0) = 0 \text{ da cui } f(x) = h(x,0) \in J$$

$$h(x,1) = 0 \text{ da cui } f(x) = h(x,1) \in I$$

Quindi $f \in I \cap J$ come volevamo.

La proposizione precedente dà un algoritmo per calcolare l'intersezione di due ideali. Infatti se $I = (f_1, \ldots, f_r)$ e $J = (g_1, \ldots, g_s)$ allora si può trovare una base di Gröbner (e quindi un insieme di generatori) di $I \cap J$ eliminando t da

$$(tf_1, \ldots, tf_r, (1-t)g_1, \ldots, (1-t)g_s)$$

utilizzando il teorema 4.2

L'algoritmo per il calcolo dell'intersezione di due ideali I e J è implementato in Cocoa come

$$Intersect(I, J)$$

Intersection nelle versioni piú recenti di Cocoa.

Il minimo comune multiplo tra due polinomi f e g si può trovare come il generatore dell'ideale intersezione $(f) \cap (g)$. Segue $M.C.D.(f,g) = \frac{fg}{m.c.m.(f,g)}$. MCD e mcm possono essere trovati in Cocoa con i comandi $GCD(f_1, \ldots, f_k)$ e $LCM(f_1, \ldots, f_k)$, applicabili anche a più di due polinomi.

5. COMPLEMENTI SUGLI IDEALI DI UN ANELLO COMMUTATIVO

Sia A un anello commutativo con unità (ad esempio $A = K[x_1, \ldots, x_n]$).

Se I, J sono ideali di A allora $I \cup J$ non è un ideale in generale

$$(x, y \in (x) \cup (y) \text{ ma } x + y \notin (x) \cup (y)) .$$

Invece

$$I + J$$

$$I \cap J$$

$$IJ := < ij | i \in I, j \in J >$$

$$I{:}J \quad := \{a \in A | aj \in I \ \forall j \in J\} \tag{5.1}$$

sono tutti ideali di A.

Osservazione. *Vale $IJ \subset I \cap J$ e l'inclusione può essere stretta (esempio: $I = J = (x)$).*

Definizione 5.1. *Se $X \subset K^n$ è un sottoinsieme poniamo*

$$I(X) := \{f \in K[x_1, \ldots, x_n] | f(x) = 0 \quad \forall x \in X\}$$

È immediato verificare che I è un ideale di $K[x_1, \ldots, x_n]$.

Poniamo

$$\sqrt{I} := \{f \in A | \exists n \in \mathbf{N} \text{ tale che} f^n \in I\}$$

$\sqrt{I}$ si dice il radicale di I.

Lemma 5.2. *$\sqrt{I}$ è un ideale.*

Dimostrazione Siano $f \in \sqrt{I}, g \in K[x_1, \ldots, x_n$. Pertanto $\exists \quad n \in \mathbf{N}$ tale che $f^n, g^n \in I$. Quindi $(fg)^n = f^n g^n \in I$, da cui $fg \in \sqrt{I}$. Utilizzando lo sviluppo del binomio di Newton si verifica che $(f+g)^{2n} \in I$, da cui $f + g \in \sqrt{I}$.

Abbiamo le ovvie inclusioni:

$$I \subset \sqrt{I} \tag{5.2}$$

$$I \subset J \Rightarrow \sqrt{I} \subset \sqrt{J} \tag{5.3}$$

Esercizio 5.3. *Se $X \subset K^n$ provare che $\sqrt{I(X)} = I(X)$.*

Esempi. *Se $I = (x^2) \subset K[x]$ allora $\sqrt{I} = (x)$.*

Se $I =< xy^2z, x^3w^5 >$ allora $\sqrt{I} =< xyz, xw >$

Se $I =< x^\alpha >_{\alpha \in A}$ è un ideale monomiale, allora $\sqrt{I} =< x^{\alpha'} >$ dove

$$\alpha_i{}' = \begin{cases} 1 \text{ se } \alpha_i \neq 0 \\ \\ 0 \text{ se } \alpha_i = 0 \end{cases}$$

Esercizio 5.4. *Provare che*

$$\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$$

$$\sqrt{\sqrt{I}} = \sqrt{I}$$

Lemma 5.5. *Se I è primo allora $\sqrt{I} = I$.*

Dimostrazione Sia $f \in \sqrt{I}$ e sia n il minimo intero tale che $f^n \in I$. Considerando che $f^n = f \cdot f^{n-1}$ abbiamo $f \in I$ oppure $f^{n-1} \in I$. Se $n \geq 2$ questa è una contraddizione. Quindi $n = 1$ e $f \in I$.

L'esempio seguente è particolarmente importante:

Esempio 5.6. *Sia* $f: K \to K^3$ *data da* $f(t) = (t, t^2, t^3)$ *e poniamo* $V := Im\ f \subset K^3$. *V si chiama la* cubica gobba, *ed è parametrizzata dalle espressioni* $x = t$, $y = t^2$, $z = t^3$. *Adesso vogliamo provare direttamente che*

$$I(V) = (y - x^2, z - x^3)$$

cioè che un qualunque polinomio che si annulla su V è combinazione di $y - x^2$ *e* $z - x^3$. *Dato* $f \in I(V)$, *scegliendo l'ordine LEX con* $z > y > x$ *ed applicando l'algoritmo di divisione otteniamo* $f = (y - x^2)q_1 + (z - x^3)q_2 + r$ *dove nessun termine di r è divisibile per* $LT(y - x^2) = y$ *o per* $LT(z - x^3) = z$. *Pertanto* $r = r(x)$ *da cui si ricava*

$$0 \equiv f(t, t^2, t^3) = 0 + 0 + r(t)$$

e quindi $r \equiv 0$ *come volevamo.*

Esercizio. *Sia* $V \subset K^3$ *la cubica gobba. Provare che* $f = z^2 - x^4 y \in I(V)$ *e trovare esplicitamente una scrittura come combinazione lineare di* $y - x^2$ *e* $z - x^3$. *Ripetere l'esercizio con* $f = z - xy$, $f = xz - y^2$ *(si veda anche l'esercizio seguente).*

Esercizio. *Provare che* $y - x^2$ *e* $z - x^3$ *costituiscono una base di Gröbner di* $I(V)$ *secondo l'ordine LEX con* $z > y > x$.

Definizione 5.7. *Se I è un ideale di* $K[x_1, \ldots, x_n]$ *poniamo*

$$V(I) := \{x \in K^n | f(x) = 0 \quad \forall f \in I\}$$

$V(I)$ *si dice una* varietà algebrica affine.

Osservazione 5.8. *Notiamo subito che se* $I = (f_1, \ldots, f_r)$ *allora*

$$V(I) = \{x \in K^n | f_1(x) = \ldots f_r(x) = 0\}$$

cioè $V(I)$ *coincide con il luogo degli zeri dei polinomi* $f_1, \ldots, f_r$.

Esempi. *Se I è un ideale principale generato da un polinomio f, scriviamo* $V(I) = V(f)$. *Queste varietà si chiamano ipersuperfici. Se deg* $f = 1$ *si tratta di varietà lineari, se deg* $f = 2$ *allora* $V(f)$ *si dice una quadrica. Per il teorema della base di Hilbert e l'osservazione 5.8 ogni varietà algebrica è intersezione di un numero* finito *di ipersuperfici. La cubica gobba dell'esempio 5.6 è una varietà algebrica, infatti coincide con* $V(I)$ *dove* $I = (y - x^2, z - x^3)$ *(la verifica di questo fatto è immediata).*

Osservazione. *La cubica gobba C é una varietá algebrica affine. Infatti verifichiamo che* $C = V(I)$ *dove* $I = (y - x^2, z - x^3)$. *Se* $p = (x, y, z) \in C$ *allora* $\exists t$ *tale che* $p = (t, t^2, t^3)$ *e quindi* $p \in V(I)$. *Viceversa se* $p = (x, y, z) \in V(I)$ *allora* $y - x^2 = 0$ *e* $z - x^3 = 0$. *Pertanto posto* $t := x$ *abbiamo* $p = (t, t^2, t^3)$.

Approfondiremo lo studio delle varietá descritte da equazioni parametriche nel §8.

Esercizio 5.9. *Se $I \subset J$ sono due ideali, provare che $V(J) \subset V(I)$.*

Esercizio 5.10. *Provare che $V(I+J) = V(I) \cap V(J)$.*

Esercizio 5.11. *Provare che $V(I) = V(\sqrt{I})$.*

Esercizio 5.12. *Sia $V \subset \mathbf{R}^3$ la curva parametrizzata da (t, t^m, t^n) per $n, m \geq 2$. Provare che V è una varietà affine e calcolare $I(V)$.*

6. LA TOPOLOGIA DI ZARISKI SU K^n

Lemma 6.1.

i) $V((1)) = \emptyset$

ii) $V(0) = K^n$

iii) $V(f_1, \ldots, f_r) \cap V(g_1, \ldots, g_s) = V(f_1, \ldots, f_r, g_1, \ldots, g_s)$. *In generale* $V(I) \cap V(J) = V(I+J)$ *e* $\cap_{a \in \mathcal{A}} V(I_a) = V(\sum_{a \in \mathcal{A}} I_a)$

iv) $V(f_1, \ldots, f_r) \cup V(g_1, \ldots, g_s) = V((\ldots, f_i g_j, \ldots))$. *In generale* $V(I) \cup V(J) = V(IJ)$.

Quindi le varietà algebriche affini soddisfano gli assiomi degli insiemi chiusi per una topologia su K^n.

Dimostrazione i), ii), iii) seguono subito dalle definizioni. Per provare iv) notiamo che $I, J \supset IJ$ e quindi $V(I) \cup V(J) \subset V(IJ)$. Viceversa sia $x \in V(IJ)$. Se per assurdo $x \notin V(I)$ e $x \notin V(J)$ allora $\exists \quad i \in I$ tale che $i(x) \neq 0$ e $\exists \quad j \in J$ tale che $j(x) \neq 0$. Pertanto $ij(x) \neq 0$ che è una contraddizione.

Definizione 6.2. *La topologia su K^n che ha per chiusi le varietà algebriche affini $V(I)$ si dice* topologia di Zariski.

Esempio. *I chiusi della topologia di Zariski in K sono gli insiemi finiti. Se K è infinito questa topologia è $T1$ ma non di Hausdorff.*

Per rendersi conto di quanta cautela occorre lavorando con la topologia di Zariski, il lettore può verificare che l'applicazione somma $s\colon \mathbf{R} \times \mathbf{R} \to \mathbf{R}$ definita da $s(x,y) = x + y$ non è continua se definiamo su $\mathbf{R}$ la topologia di Zariski e nel dominio di s la topologia prodotto.

Proposizione 6.3.

$$V(I) \cup V(J) = V(I \cap J)$$

Dimostrazione

"$\subset$" Abbiamo $I, J \supset I \cap J$ da cui $V(I) \cup V(J) \subset V(I \cap J)$

"$\supset$" Abbiamo $IJ \subset I \cap J$ da cui $V(IJ) \supset V(I \cap J)$. A questo punto è sufficiente utilizzare il lemma 6.1 iv).

Esercizio 6.4. *Si trovi $I \subset \mathbf{R}[x,y,z]$ tale che $V(I) \subset \mathbf{R}^3$ consiste nell'unione del piano $\{z=0\}$ con l'asse delle z.*

Osservazione. *Vale $X \subset V(I(X))$, infatti se $x \in X$ allora $f(x) = 0 \ \forall f \in I(X)$.*

Lemma 6.5. *Se W è una varietà algebrica affine allora $W = V(I(W))$*

Dimostrazione Sia $W = V(J)$. Abbiamo che se $f \in J$ allora $f(x) = 0 \quad \forall x \in W$ e quindi $J \subset I(W)$. Pertanto $W = V(J) \supset V(I(W))$. L'altra inclusione è stata vista nell'osservazione precedente.

Più precisamente abbiamo la

Proposizione 6.6. *Se $S \subset K^n$ è un sottoinsieme allora $V(I(S)) = \overline{S}$ (chiusura secondo la topologia di Zariski)*

Dimostrazione Abbiamo già visto che $S \subset V(I(S))$ e quindi $\overline{S} \subset V(I(S))$. Viceversa consideriamo che $I(\overline{S}) \subset I(S)$ e quindi $V(I(S)) \subset V(I(\overline{S})) = \overline{S}$ per il lemma 6.5.

Corollario 6.7. *Sia $S \subset K^n$ con la topologia indotta. Allora ogni catena discendente di chiusi in S é stazionaria.*

Dimostrazione Si puó supporre $S = K^n$. Se $C_1 \supset C_2 \supset C_3 \supset \ldots$ allora $I(C_1) \subset I(C_2) \subset I(C_3) \subset \ldots$ e per noetherianitá quest'ultima catena é stazionaria. Dal lemma 6.5 segue la tesi.

Uno spazio topologico in cui ogni catena discendente di chiusi é stazionaria si dice noetheriano. Si potrebbe definire la dimensione di uno spazio noetheriano come la massima lunghezza di una catena di chiusi irriducibili. Tale definizione peró non é operativa. Riprenderemo la definizione di dimensione nel §19.

Osservazione 6.8. *Se J è un ideale di $K[x_1,\ldots,x_n]$ vale*

$$J \subset I(V(J))$$

infatti se $j \in J$ allora $j(x) = 0 \quad \forall x \in V(J)$. In questo caso però l'inclusione può essere stretta, come mostrano i due esempi:

$$J = (x^2) \subset \mathbf{R}[x] \quad \Rightarrow \quad I(V(J)) = I(\text{origine}) = (x) \supset_{\neq} (x^2) = J \tag{6.1}$$

$$J = (x^2+1) \subset \mathbf{R}[x] \quad \Rightarrow \quad I(V(J)) = I(\emptyset) = (1) \supset_{\neq} (x^2+1) = J \tag{6.2}$$

Il primo esempio (6.1)porta a considerare che:

Lemma 6.9. *Se J è un ideale di $K[x_1,\ldots,x_n]$ vale $\sqrt{J} \subset I(V(J))$.*

Dimostrazione Dall'osservazione 6.8 $J \subset I(V(J))$. Basta applicare (5.3) ed il fatto che $\sqrt{I(V(J))} = I(V(J))$ (eserc. 5.3).

Il secondo esempio (6.2) è di natura diversa da (6.1) ed è legato al fatto che $\mathbf{R}$ non è algebricamente chiuso. Infatti vale il

6.10 Teorema degli zeri di Hilbert (Hilbertnullstellensatz). *Sia K un campo algebricamente chiuso e sia J un ideale di $K[x_1, \ldots, x_n]$. Allora*

$$\sqrt{J} = I(V(J))$$

Dimostreremo nel §9 il teorema degli zeri di Hilbert.

Definizione 6.11. *Una varietà algebrica affine $V \subset K^n$ si dice <u>riducibile</u> se $V = V_1 \cup V_2$ con V_i sottovarietà proprie. Altrimenti si dice <u>irriducibile</u>.*

Teorema 6.12. *Sia V una varietà algebrica affine*

$$V \text{è irriducibile} \Longleftrightarrow I(V) \text{è primo}$$

Dimostrazione

$\Rightarrow$ Sia $fg \in I(V)$ e poniamo $V_1 := V \cap V(f)$, $V_2 := V \cap V(g)$. Se $f \notin I(V)$ allora $V \setminus V_1 \neq \emptyset$. Preso $x \in V \setminus V_1$ abbiamo $f(x) \neq 0$ e quindi $g(x) = 0$, cioè $x \in V_2$. Quindi $V = V_1 \cup V_2$ e per l'ipotesi $V = V_2$ da cui $V \subset V(g)$ e $g \in I(V)$.

$\Leftarrow$ Sia per assurdo $V = V_1 \cup V_2$ con V_i sottovarietà algebriche proprie. Pertanto esistono $f \in I(V_1) \setminus I(V)$ e $g \in I(V_2) \setminus I(V)$ da cui fg si annulla su $V_1 \cup V_2 = V$. Quindi $fg \in I(V)$ e per l'ipotesi $f \in I(V)$ oppure $g \in I(V)$.

Corollario 6.13. *Sia K algebricamente chiuso. C'é una corrispondenza biunivoca naturale tra varietá algebriche ed ideali radicali di $K[x_1, \ldots, x_n]$ data da $W \mapsto I(W)$ con inversa $J \mapsto V(J)$. La corrispondenza porta varietá algebriche irriducibili in ideali primi e viceversa.*

Dimostrazione La prima parte dell'enunciato segue direttamente dal teor.6.12. Se W é una varietá irriducibile allora $I(W)$ é primo per il teor.6.12 e $V(I(W)) = W$ per il lemma 6.5. Se J é un ideale primo $I(V(J)) = \sqrt{J} = J$ per il teorema 6.10 ed il lemma 5.7. Quindi $V(J)$ é irriducibile per il teorema 6.12.

Esercizi.

i) Sia f un monomio. Provare che $V(f)$ é dato dall'unione di sottovarietá lineari di codimensione 1.

ii) Descrivere $V(I)$ dove $I = (xy, xz) \subset K[x, y, z]$

iii) Sia I un ideale monimiale. Provare che $V(I)$ é dato dall'unione di sottovarietá lineari.

7. INTERPRETAZIONE GEOMETRICA DI $I\colon J$

Vediamo ora a quale varietà corrisponde l'ideale quoziente $I\colon J$. Questo studio ci permetterà anche di vedere una delle prime applicazioni del Nullstellensatz.

Lemma 7.1. *Siano I e J ideali in $K[x_1, \ldots, x_n]$. Allora*

$$I{:}J \subset I\,(V(I) \setminus V(J))$$

Dimostrazione Sia $f \in I{:}J$ e $x \in V(I) \setminus V(J)$. Dobbiamo provare che $f(x) = 0$. Per ogni $g \in J$ abbiamo $fg \in I$ e quindi $f(x)g(x) = 0$. Siccome $x \notin V(J)$ deve esistere $g \in J$ tale che $g(x) \neq 0$ e quindi segue $f(x) = 0$ c.v.d.

Proposizione 7.2. *Siano I e J ideali in $K[x_1, \ldots, x_n]$. Allora*

$$V(I) \supset V(I{:}J) \supset \overline{V(I) \setminus V(J)}$$

Se in più K è algebricamente chiuso e $I = \sqrt{I}$ allora

$$V(I{:}J) = \overline{V(I) \setminus V(J)}$$

Dimostrazione Dal lemma 7.1 e dalla proposizione 6.6 considerando V di entrambi i membri segue subito $V(I{:}J) \supset \overline{V(I) \setminus V(J)}$ e quindi la prima parte.
Per provare la seconda parte é sufficiente provare l'inclusione opposta nel lemma 7.1 ed applicare ancora la prop. 6.6. Sia dunque $h \in I(V(I) \setminus V(J))$, per provare che $h \in I{:}J$ scegliamo un qualunque $g \in J$. Allora hg si annulla su $V(I) = (V(I) \setminus V(J)) \cup V(J)$ perché h si annulla su $V(I) \setminus V(J)$ e g si annulla su $V(J)$. Pertanto per il Nullstellensatz 6.10 $hg \in I(V(I)) = \sqrt{I} = I$. Ne segue che $h \in I{:}J$ c.v.d.

Teorema 7.3. *Siano V e W varietà di K^n. Allora*

$$I(V){:}I(W) = I(V \setminus W)$$

Dimostrazione Basta applicare il lemma 7.1 al caso $I = I(V)$ e $J = I(W)$ ed otteniamo $I(V){:}I(W) \subset I(V \setminus W)$ (si veda anche il lemma 6.5). Viceversa se $f \in I(V \setminus W)$ e $g \in I(W)$ allora fg si annulla su $V \subset (V \setminus W) \cup W$ e quindi $fg \in I(V)$ e $f \in I(V){:}I(W)$ per definizione di ideale quoziente.

Il seguente teorema fornisce uno strumento per il calcolo esplicito dei generatori di $I{:}J$.

Teorema 7.4. *Siano I e $J = (g_1, \ldots, g_k)$ due ideali di $K[x_1, \ldots, x_n]$. Allora*

i) $I{:}J = \cap_{i=1}^{k} I{:}(g_i)$

ii) Se $h_1, \ldots, h_p$ è un sistema di generatori per $I \cap (g_i)$ allora $\frac{h_1}{g_i}, \ldots \frac{h_p}{g_i}$ generano $I{:}(g_i)$.

Dimostrazione

i) segue subito dalle definizioni

ii) Ovviamente $\frac{h_j}{g_i} \in I{:}(g_i)$. Prendiamo dunque $f \in I{:}(g_i)$. Pertanto $fg_i \in I \cap (g_i)$ ed esistono $r_1, \ldots r_p$ tali che $fg_i \in \sum_{j=1}^{p} r_j h_j$ e dividendo per g_i abbiamo la tesi.

Algoritmo per il calcolo di $I{:}J$

Se conosciamo $I = \{f_1, \ldots, f_q\}$ e $J = (g_1, \ldots, g_k)$ dalla prop. 4.3 possiamo calcolare dei generatori per $I \cap (g_i)$, da ii) del teorema 7.4 troviamo dei generatori per $I{:}(g_i)$ ed usando ancora la prop. 4.3 e i) del teor. 7.4 troviamo dei generatori per $I{:}J$.

L'algoritmo per il calcolo di $I{:}J$ è implementato in Cocoa e l'ideale $I{:}J$ si trova come Colon(I,J).

Esempio. *Sia* $I = (f, g) = (z - xy, xz - y^2) \subset \mathbf{R}[x, y, z]$. *Si vede subito che la retta* $L = \{y = z = 0\}$ *è contenuta in* $V(I)$ *e che* $V(I) = L \cap C$ *dove* C *é la cubica gobba dell'esempio 5.9. Posto* $J = (y, z)$ *allora* $V(I\colon J)$ *è la cubica gobba* C. *Su* $\mathbf{C}$ *questo segue dalla prop.7.2, ma in questo caso il risultato é vero anche su* $\mathbf{R}$. *La cubica gobba e la retta* L *sono un esempio di "varietà legate".*

8. IL RISULTANTE

Sia R un dominio a fattorizzazione unica (UFD). Ricordiamo dai corsi di algebra il teorema di Gauss per cui

$$R \text{ UFD} \Longrightarrow R[x] \text{ UFD}$$

Teorema 8.1. *Siano* F, G *polinomi in* $R[x]$ *di gradi rispettivamente* $f, g > 0$.

$$F, G \quad \textit{hanno un fattore irriduc. in comune} \Longleftrightarrow \begin{array}{l} \exists \quad A, B \quad \textit{di gradi risp. } g-1, f-1 \\ \qquad\qquad \textit{tali che } AF + BG = 0 \end{array}$$

Dimostrazione

$\Longrightarrow$ Sia $F = af_1$, $G = ag_1$. Poniamo $A := g_1$, $B := -f_1$. Allora abbiamo $Af + Bg = g_1 a f_1 - f_1 a g_1 = 0$. Se $deg\ A$, $deg\ B$ sono minori di quanto è richiesto basta moltiplicare A e B per lo stesso fattore.

$\Longleftarrow$ Per ipotesi $AF = -BG$. Quindi ogni fattore irriducibile di G divide A oppure F. Siccome $deg\ A = g - 1$ allora esiste un fattore irriducibile di G che divide F, come volevamo.

Adesso l'introduzione del risultante è semplice. Il problema è di trovare condizioni per cui due polinomi F, $G \in R[x]$ hanno un fattore in comune.

Si considera come incognite: $A := a_0 x^{g-1} + \ldots + a_{g-2} x + a_{g-1}$ $B := b_0 x^{f-1} + \ldots + b_{f-2} x + b_{f-1}$

e si pone la condizione

$$AF + BG = 0 \tag{8.1}$$

Questo è un sistema lineare con $f + g$ incognite e $f + g$ equazioni. Il determinante della matrice di (8.1) è il risultante di F e G.

Posto $F := f_0x^f + \ldots$, $G := g_0x^g + \ldots$ il sistema (8.1) diventa:

$$\begin{array}{lllll}
a_0f_0+ & & b_0f_0 & = 0 & \text{coeff. di } x^{f+g-1} \\
a_0f_1 + a_1f_0 & & b_0f_1 + b_1f_0 & = 0 & \text{coeff. di } x^{f+g-2} \\
\vdots & & \vdots & \vdots & \\
a_{g-1}f_f+ & & b_{f-1}g_g & = 0 & \text{coeff. di} x^0
\end{array}$$

e la sua matrice è

$$\begin{pmatrix}
f_0 & & & g_0 & & & \\
f_1 & f_0 & & g_1 & g_0 & & \\
\vdots & \ddots & & \vdots & \ddots & & \\
f_f & & f_0 & g_g & & g_0 & \\
& \ddots & & & \ddots & & \\
& & f_f & & & g_g &
\end{pmatrix}$$

Per comodità di scrittura si scrive il risultante come il determinante della matrice trasposta, cioè si pone:

$$Res(f,g,x) := \det \begin{vmatrix}
f_0 & f_1 & \ldots & f_f & & & & \\
 & f_0 & \ddots & & \ddots & & & \\
 & & \ddots & \ddots & & \ddots & & \\
 & & & f_0 & f_1 & \ldots & f_f & \\
g_0 & g_1 & \ldots & \ldots & g_g & & & \\
 & g_0 & \ddots & & & \ddots & & \\
 & & \ddots & \ddots & & & \ddots & \\
 & & & \ddots & \ddots & & & \ddots \\
 & & & & g_0 & g_1 & & g_g
\end{vmatrix}$$

Teorema 8.2. *Sia R un UFD.*

$$f, g \in R[x] \quad \textit{hanno un fattore in comune di grado} \geq 1 \iff Res(f,g,x) = 0$$

Dimostrazione

$\Longrightarrow$ Se fosse $Res(f,g,x) \neq 0$ allora consideriamo il sistema (8.1) nel campo dei quozienti di R. Dalla teoria dei sistemi lineari l'unica soluzione di (8.1) è quella nulla.

$\Longleftarrow$ Nel campo dei quozienti esiste una soluzione di (8.1) non nulla. Moltiplicando per il denominatore comune si trova una soluzione a coefficienti in R.

Esempio. *Siano*

$$F = x^2 - 4x + 3$$

$$G = x^2 - 6x + 5$$

che hanno a comune il fattore $x - 1$. *Infatti*

$$Res(f,g,x) = \begin{vmatrix} 1 & -4 & 3 & \\ & 1 & -4 & 3 \\ 1 & -6 & 5 & \\ & 1 & -6 & 5 \end{vmatrix} = 0$$

Il risultante di due polinomi F e G rispetto alla variabile x è implementato in Cocoa con il comando $Resultant(F, G, x)$

Esercizio. *Verificare se i polinomi* $x^5 + x + 1$ *e* $x^4 + x^3 + 1$ *hanno una radice in comune.*

Definizione 8.3. $Discr(f) := Res(f, f', x)$ *si dice il discriminante di* f.

Il discriminante del polinomio monico $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ é nullo se e solo se f ha una radice doppia.

Esempi. *Se* $f = ax^2 + bx + c$ *allora* $Discr(f) = a(4ac - b^2)$. *Se* $f = x^3 + px + q$ *allora* $Discr(f) = -(4p^3 + 27q^2)$

Teorema 8.4. *Dati* $p, q \in R[x]$ *esistono due polinomi* $A, B \in R[x]$ *tali che* $Ap + Bq = Res(p, q, x)$

Dimostrazione Se $Res(p, q, x) = 0$ la tesi è ovvia prendendo $A = q$ e $B = -p$. Se $Res(p, q, x) \neq 0$ scriviamo il sistema lineare (analogo di (8.1)) $\tilde{A}p + \tilde{B}q = 1$ con incognite $\tilde{A}$, $\tilde{B}$. Si trova un sistema lineare quadrato di ordine $deg\ p + deg\ q$ con termine noto $\begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ e determinante della matrice dei coefficienti $Res(p, q, x) \neq 0$. Risolvendo il sistema con la regola di Cramer nel campo dei quozienti di R troviamo $\tilde{A}$ e $\tilde{B}$ soluzioni che hanno a denominatore $Res(p, q, x)$. Posto $A = \tilde{A}Res(p, q, x)$ e $B = \tilde{B}Res(p, q, x)$ si ottiene la tesi.

Teorema 8.5. *Siano* $f, g \in K[x_1, \ldots x_n]$ *di grado positivo in* x_1. *Allora*

i) $Res(f, g, x_1) \in (f, g) \cap K[x_2, \ldots, x_n]$ *(che si dice il primo ideale di eliminazione)*

ii) $Res(f, g, x_1) \equiv 0 \iff f, g$ *hanno un fattore a comune di grado positivo in* x_1

Dimostrazione Consideriamo $f, g \in K[x_2, \ldots x_n][x_1]$. Allora per il teorema 8.4 esistono due polinomi $A, B \in K[x_2, \ldots x_n][x_1]$ tali che $Af + Bg = Res(f, g, x_1)$. Quindi $Res(f, g, x_1) \in (f, g) \cap K[x_2, \ldots, x_n]$.

La seconda parte è esattamente il teorema 8.2.

Osservazione critica 8.6. *Il risultante di due polinomi in piú variabili rispetto ad x_1 calcolato per un valore assegnato delle variabili rimanenti puó essere diverso dal risultante che si ottiene sostituendo subito i valori assegnati. Infatti nel secondo caso i gradi possono diminuire. Questa osservazione é cruciale per la comprensione della dimostrazione del teorema di estensione del §9. Ad esempio se $F(x_1, x_2) = (x_2 - 5)x_1 + 6$ e $G(x_1, x_2) = x_1^2 x_2^2 - (x_2 - 2)x_1 + 5x_2$ allora $Res(F(x_1, 0), G(x_1, 0), x_1) = -12$ e $Res(F, G, x_1)_{|\{x_2=0\}} = 60$*

Dal teorema 8.5 i) sorge spontanea la domanda se, dati $f, g \in K[x, y]$, il polinomio in y $Res(f, g, x)$ è il generatore dell'ideale principale $(f, g) \cap K[y]$. L' esempio seguente dà una risposta negativa.

Esempio. Siano $f = x^2 + y^2 - 1$, $g = x^3 + y^3 - 1$, ci si propone di calcolare $(f, g) \cap K[y]$ cioè il primo ideale di eliminazione di f e g. Il procedimento "intuitivo" per eliminare la x è il seguente:

$$x^2 = 1 - y^2 \qquad \text{mod } I$$

$$x^3 = 1 - y^3 \qquad \text{mod } I$$

e quindi $(1 - y^2)^3 - (1 - y^3)^2 \in I$. Infatti esplicitamente

$(1 - y^2)^3 - (1 - y^3)^2 = \left[(1 - y^2)^3 - x^6\right] - \left[(1 - y^3)^2 - x^6\right]$. Sviluppando la prima parentesi come differenza di 2 cubi e la seconda come differenza di 2 quadrati otteniamo che l'espressione precedente è uguale a:

$$\left[(1 - y^2) - x^2\right]\left[(1 - y^2)^2 + x^2(1 - y^2) + x^4\right] - \left[(1 - y^3) - x^3\right]\left[(1 - y^3) + x^3\right] =$$

$$= f\left[-(1 - y^2)^2 - x^2(1 - y^2) - x^4\right] + g[1 - y^3 + x^3]$$

L'espressione precedente coincide con $Res(f, g, x)$ a meno del segno. $(1-y^2)^3-(1-y^3)^2$ appartiene al primo ideale di eliminazione di f e g ma non è il generatore. Infatti, posto $p(y) := y^2(2y^3 + 2y^2 - y - 3) = \frac{(1-y^2)^3-(1-y^3)^2}{1-y}$ si trova

$$(f, g) \cap K[y] = (p(y)) \tag{8.2}$$

quando non è affatto evidente dalle espressioni precedenti che $p(y) \in (f, g)$.

Per provare (8.2) consideriamo l'ordine LEX con $x > y$ ed utilizziamo l'algoritmo di Buchberger. Abbiamo:

$$S(f, g) = xf - g = xy^2 - x - y^3 + 1 =: c(x, y)$$

$$S(f, c) \text{ mod } \{f, g, c\} = (y^2 f - xc) \text{ mod } \{f, g, c\} = y^2 f - xc - f - yc =$$

$$= xy - x + 2y^4 - y^2 - y + 1 =: d(x, y)$$

$$S(c, d) \text{ mod } \{f, g, c, d\} = (c - yd) \text{ mod } \{f, g, c, d\} = c - yd - d =: -p(y)$$

Risostituendo:

$$p(y) = -c + (y+1)d = -c + (y+1)\left(y^2 f - (x+y)c - f\right) =$$

$$= -(xf - g) + (y+1)\left(y^2 f - (x+y)(xf - g) - f\right) =$$

$$= f\left[-x + (y+1)(y^2 - x^2 - xy - 1)\right] + g\left[1 + (1+y)(x+y)\right]$$

ed adesso è facile verificare che $p(y)$ genera $(f,g) \cap K[y]$.

Calcolando tutti i resti delle restanti S-coppie ed eliminando gli elementi superflui si determina una base di Gröbner ridotta per (f,g) che è data da $\{f(x,y), d(x,y), p(y)\}$. Si può quindi applicare anche il teor. di eliminazione 4.2.

Osservazione. *L'esempio precedente illustra il fatto generale che il calcolo con l'algoritmo di Buchberger di un base di Gröbner a partire da un insieme di generatori dà anche le espressioni degli elementi della base di Gröbner come combinazione dei generatori. Questo algoritmo è analogo all' algoritmo euclideo, con cui dati due interi a, b si determina $MCD(a,b) = d$ e si trovano contemporaneamente due interi x, y tali che $d = ax + by$. (si veda ad esempio [Chi], I, cap. 3)*

Esempio. *Un altro esempio analogo al precedente (ma più semplice) si ha considerando $f = xy - 2$, $g = xy - 1$. In questo caso $Res(f,g,x) = y$ mentre $(f,g) \cap K[y] = (1)$. Notiamo che abbiamo anche $Res(f,g,y) = x$.*

9. IL TEOREMA DI ESTENSIONE E LA DIMOSTRAZIONE DEL TEOREMA DEGLI ZERI

Notiamo che dati due qualunque polinomi f, $g \in K[x,y]$, i punti di coordinate (x,y) appartenenti a $V(f,g)$ hanno la seconda coordinata che annulla ogni polinomio $q(y)$ nell'ideale di eliminazione. È interessante chiedersi il viceversa, cioè ogni radice y_0 del polinomio generatore dell'ideale di eliminazione corrisponde a qualche $(x_0, y_0) \in V(f,g)$? Nell'esempio precedente la risposta è affermativa ma aumentando il numero delle variabili ci vogliono delle ipotesi opportune. Questo problema va sotto il nome di problema di estensione delle soluzioni.

L'esistenza di alcune difficoltà è illustrata dal seguente esempio in tre variabili.

Esempio. *Siano* $f := xy - 1, g := xz - 1 \in K[x, y, z]$ *Eliminando la* x *troviamo* $y - z = -yg + zf$ *che è un generatore del primo ideale di eliminazione. Preso il punto di coordinate* $(y, z) = (a, a)$ *questo si estende a* $(\frac{1}{a}, a, a) \in V(f, g)$ *se* $a \neq 0$ *ma se* $a = 0$ *la soluzione non si estende! Il motivo è che il coefficiente di* x *si annulla per* $(a, a) = (0, 0)$. *Geometricamente la soluzione è andata all'infinito, vedremo infatti che nel proiettivo l'eliminazione è più semplice da trattare.*

9.1 Teorema di estensione.

(Teorema fondamentale della teoria dell'eliminazione, caso affine).

Sia K un campo algebricamente chiuso. Siano

$$f_1 := g_1(x_2, \ldots, x_n)x_1^{N_1} + \ldots$$

$$\vdots$$

$$f_k := g_k(x_2, \ldots, x_n)x_1^{N_k} + \ldots$$

polinomi in $K[x_1, \ldots, x_n]$ e sia $I = (f_1, \ldots, f_k)$. Posto $I_1 := I \cap K[x_2, \ldots, x_n]$, sia $(a_2, \ldots, a_n) \in V(I_1)$ "soluzione parziale". Se $(a_2, \ldots, a_n) \notin V(g_1, \ldots, g_k)$ allora $\exists \quad a_1 \in K$ tale che $(a_1, a_2, \ldots, a_n) \in V(I)$

Dimostrazione

Possiamo assumere (rinumerando eventualmente $f_1, \ldots, f_k$) che $g_1(a_2, \ldots, a_n) \neq 0$. Introduciamo delle nuove indeterminate $u_2, \ldots, u_k$ e consideriamo

$$Res(f_1, u_2f_2 + \ldots + u_kf_k, x_1) = Af_1 + B(u_2f_2 + \ldots + u_kf_k) = \sum h_\alpha u^\alpha$$

$$\text{dove } \; u^\alpha = u_2^{\alpha_2} \ldots u_k^{\alpha_k} \qquad A, B \in K[u_2, \ldots, u_k, x_1, \ldots, x_n] \qquad h_\alpha \in K[x_2, \ldots, x_n]$$

Sviluppando l'ultima uguaglianza si ottiene $h_\alpha \in I_1$ e quindi $h_\alpha(a_2, \ldots, a_n) = 0 \quad \forall \alpha$. Sostituendo eventualmente f_2 con $\tilde{f}_2 := f_2 + x_1^N f_1 \; (N \gg 0)$ possiamo supporre che $g_2(a_2, \ldots, a_n) \neq 0$ e che f_2 ha grado in x_1 maggiore di $f_3, \ldots, f_n$. Lavoriamo adesso in $K[x_1, u_2, \ldots, u_k]$ sostituendo $(x_2, \ldots, x_n) = (a_2, \ldots, a_n)$. Allora

$$Res(f_1, u_2f_2 + \ldots + u_kf_k, x_1)_{|(x_2,\ldots,x_n)=(a_2,\ldots,a_n)} = 0 \tag{9.1}$$

Siccome i leading term in x_1 di f_1 e di $u_2f_2 + \ldots + u_kf_k$ non si annullano quando sostituisco $(x_2, \ldots, x_n) = (a_2, \ldots, a_n)$ posso dire che l'espressione (9.1) coincide con il risultante tra $f_{1\,|(x_2,\ldots,x_n)=(a_2,\ldots,a_n)}$ e $u_2f_2 + \ldots + u_kf_{k\,|(x_2,\ldots,x_n)=(a_2,\ldots,a_n)}$ nell'anello $K[x_1, u_2, \ldots, u_k]$ (si veda l'oss. critica 8.6). Per il teorema 8.5 ii) segue che f_1 e $u_2f_2 + \ldots + u_kf_k$ in $K[x_1, u_2, \ldots, u_k]$ hanno a comune un fattore F di grado positivo in x_1. Siccome $F|f_1$ abbiamo $F \in K[x_1]$ e quindi F divide anche $f_2, \ldots, f_k$. Per ipotesi K è algebricamente

chiuso, quindi esiste $a_1 \in K$ tale che $F(a_1) = 0$ da cui $f_i(a_1, a_2, \ldots, a_n) = 0$ e quindi $(a_1, a_2, \ldots, a_n) \in V(I)$ come volevamo.

Vediamo ora come utilizzare il teorema di estensione per provare il teorema degli zeri di Hilbert enunciato in 6.10.

Come passo intermedio, importante di per sé, si prova che il teorema degli zeri equivale ad una versione "debole" (qui il teorema di estensione ancora non interviene). La versione debole segue poi facilmente dal teorema di estensione.

9.2 Nullstellensatz debole. *Sia K un campo algebricamente chiuso e I un ideale di $K[x_1, \ldots, x_n]$. Abbiamo*

$$V(I) = \emptyset \Longleftrightarrow I = K[x_1, \ldots, x_n]$$

Proposizione 9.3.

$$\text{Nullstellensatz} \Longleftrightarrow \text{Nullstellensatz debole}$$

Dimostrazione

" $\Longrightarrow$ " Sia $V(I) = \emptyset$, allora per il Nullstellensatz $\sqrt{I} = (1)$ da cui $I = (1)$. Il viceversa è evidente.

" $\Longleftarrow$ " Sia $f \in I(V(f_1, \ldots, f_s))$. Vogliamo provare che esiste m tale che $f^m \in (f_1, \ldots, f_s)$. Sia $\tilde{I} := (f_1, \ldots, f_s, 1 - yf) \subset K[x_1, \ldots x_n, y]$. Affermo che $V(\tilde{I}) = \emptyset$. Se per assurdo esiste $P_0 := (a_1, \ldots, a_n, y_0) \in V(\tilde{I})$ allora in particolare $f_i(a_1, \ldots, a_n) = 0$, e quindi $(a_1, \ldots, a_n) \in V(f_1, \ldots, f_s)$ da cui $f(a_1, \ldots, a_n) = 0$ Pertanto $1 - yf$ vale 1 nel punto P_0 e questa è una contraddizione.
Per il Nullstellensatz debole segue $\tilde{I} = K[x_1, \ldots x_n, y]$, da cui

$$1 = \sum p_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf)$$

Sostituendo $y = 1/f$ abbiamo

$$1 = \sum p_i(x_1, \ldots, x_n, \frac{1}{f}) f_i$$

I termini della somma a secondo membro sono funzioni razionali aventi a denominatore qualche potenza di f. Raccogliendo sotto un unico denominatore si ottiene:

$$f^m = \sum \tilde{p}_i(x_1, \ldots, x_n) f_i$$

come volevamo.

Esercizio. *Sia $J = \left(x^2 + y^2 - 1, y - 1\right) \subset \mathbf{R}[x, y]$. Trovare $f \in I(V(J))$ tale che $f \notin J$.*

Dimostrazione del Nullstellensatz debole 9.2

Se $n = 1$ il teorema è vero perché K é algebricamente chiuso, quindi ragioniamo per induzione su n. Se $V(I) = V((f_1, \ldots, f_k)) = \emptyset$ vogliamo provare che $(f_1, \ldots, f_k) = (1)$. Possiamo assumere che

$$f_i(x_1, \ldots, x_n) = c_i x_1^{N_i} + \ldots$$

con $c_i \neq 0$. Infatti consideriamo l'automorfismo ϕ di $K[x_1, \ldots, x_n]$ definito da

$$x_1 \mapsto x_1$$

$$x_2 \mapsto x_2 + a_2 x_1$$

$$\vdots$$

$$x_n \mapsto x_n + a_n x_1$$

con $a_2, \ldots, a_n$ da determinare (l'inversa di ϕ si ottiene cambiando i segni precedenti da $+$ a $-$. Abbiamo $V(\phi(f_1), \ldots, \phi(f_k)) = \emptyset$ perché $\phi(f)(x_1, \ldots, x_n) = f(\phi(x_1), \ldots, \phi(x_n))$ ed ovviamente:

$$I = (1) \Longleftrightarrow \phi(I) = (1)$$

Sia $\phi(x^\alpha) = g_\alpha(a_2, \ldots, a_n) x_1^{\sum \alpha_i} + \ldots$ (termini di grado inferiore in x_1) e quindi $\phi(f_i) = c_i(a_2, \ldots, a_n) x_1^{N_i} + \ldots$ (termini di grado inferiore in x_1). Basta quindi scegliere $a_2, \ldots, a_n$ in modo che $c_i(a_2, \ldots, a_n) \neq 0$ Adesso possiamo applicare il teorema di estensione 9.1. Se fosse $V(I_1) \neq \emptyset$ avrei anche $V(I) \neq \emptyset$ che è una contraddizione. Quindi $V(I_1) = \emptyset$ e per l'ipotesi induttiva $1 \in I_1 \subset I$ c.v.d.

La dimostrazione del teorema degli zeri 6.10 è così completa.

Lemma 9.4. *La base di Gröbner ridotta dell'ideale* (1) *è data da* $\{1\}$ *per ogni ordinamento monomiale.*

Dimostrazione L'enunciato è evidente dalla unicità della base di Gröbner ridotta.

Dal Nullstellensatz (debole) segue in particolare

9.5 Algoritmo di consistenza. *Siano* $f_1, \ldots, f_s \in K[x_1, \ldots, x_n]$ *con* K *algebricamente chiuso. Vale:*

$$\begin{array}{c} \text{Il sistema } f_i(x_1, \ldots, x_n) = 0 \\ \\ \text{ha una soluzione} \end{array} \quad \Longleftrightarrow \quad \begin{array}{c} \text{La base di Gröbner ridotta} \\ \\ \text{dell'ideale } (f_1, \ldots, f_s) \\ \\ \text{non è uguale a } \{1\} \end{array}$$

Teorema 9.6. *Sia* K *algebricamente chiuso. Gli ideali massimali di* $K[x_1, \ldots, x_n]$ *sono tutti e soli quelli della forma* $(x_1 - a_1, \ldots, x_n - a_n)$

Dimostrazione Abbiamo $\frac{K[x_1, \ldots, x_n]}{(x_1 - a_1, \ldots, x_n - a_n)} \simeq K$ e quindi $(x_1 - a_1, \ldots, x_n - a_n)$ è massimale. Viceversa sia I un ideale massimale. Dal Nullstellensatz debole 9.2 abbiamo che esiste $(a_1, \ldots, a_n) \in V(I)$. Pertanto

$$I \subset I(V(I)) \subset I(a_1, \ldots a_n) = (x_1 - a_1, \ldots x_n - a_n)$$

e per la massimalità vale l'uguaglianza.

Corollario 9.7. *Sia K algebricamente chiuso e sia $V \subset K^n$ una varietá algebrica affine. Allora gli ideali massimali di $K[x_1, \ldots, x_n]/I(V)$ sono tutti e soli quelli della forma $(x_1 - a_1, \ldots, x_n - a_n)$ con $(a_1, \ldots, a_n) \in V$.*

Dimostrazione É sufficiente osservare che gli ideali di $K[x_1, \ldots, x_n]/I(V)$ sono in corrispondenza biunivoca con gli ideali di $K[x_1, \ldots, x_n]$ che contengono $I(V)$ e che $I(V) \subset (x_1 - a_1, \ldots x_n - a_n) \Longleftrightarrow (a_1, \ldots, a_n) \in V$.

Esercizi.

1. Si consideri il sistema di equazioni

$$x^2 + 2y^2 = 3$$

$$x^2 + xy + y^2 = 3$$

Se I è l'ideale generato da queste equazioni, si trovino generatori per $I \cap K[x]$ e $I \cap K[y]$. Si trovino tutte le soluzioni del sistema se $K = \mathbf{Q}, \mathbf{R}$ o $\mathbf{C}$.

2. Come nell'esercizio 1. per il sistema

$$x^2 + 2y^2 = 2$$

$$x^2 + xy + y^2 = 2$$

3. Trovare generatori per gli ideali di eliminazione I_1 e I_2 dove I è l'ideale generato da

$$x^2 + y^2 + z^2 = 4$$

$$x^2 + 2y^2 = 5$$

$$xz = 1$$

4. Si consideri il sistema di equazioni

$$x^5 + \frac{1}{x^5} = y$$

$$x + \frac{1}{x} = z$$

Sia I l'ideale in $\mathbf{C}[x, y, z]$ determinato da queste equazioni.

   a. Trovare una base per $I_1 \subset \mathbf{C}[y, z]$ e provare che $I_2 = 0$.
   b. Usare il teorema di estensione 9.1 per provare che ogni soluzione parziale $c \in V(I_2) = \mathbf{C}$ estende ad una soluzione $(x_0, y_0, c) \in V(I)$.
   c. Quali soluzioni parziali $(y, z) \in V(I_1) \subset \mathbf{R}^2$ si estendono a soluzioni in $V(I) \subset \mathbf{R}^3$? Confrontare la risposta con quanto affermato dal teorema di estensione.
   d. Guardando z come "parametro", risolvere il sistema con x, y funzioni razionali di z e trovare così una parametrizzazione di $V(I)$.

5. Siano $f,\ g \in \mathbf{C}[x,y]$. Questo esercizio è una guida per provare che

$$V(f,g) \text{ è infinito} \iff f \text{ e } g \text{ hanno un fattore a comune non costante in } \mathbf{C}[x,y]$$

   a. Provare che se f è non costante allora $V(f)$ è infinito (ridursi al teorema fondamentale dell'algebra in una variabile) .
   b. Provare $\Longleftarrow$ utilizzando il punto a.
   c. Provare $\Longrightarrow$ mostrando che se f e g non hanno fattori non costanti a comune allora $Res(f,g,x)$ e $Res(f,g,y)$ sono entrambi non nulli.

6. Sia K algebricamente chiuso e siano $y_1,\ldots,y_k$ tutte le radici di $Res(f,g,x)$ e $x_1,\ldots,x_s$ tutte le radici di $Res(f,g,y)$. Provare che tutte le soluzioni del sistema $\begin{cases} f=0 \\ g=0 \end{cases}$ sono contenute tra le (x_i,y_j) per $i=1,\ldots s,\ j=1,\ldots,k$ (è sufficiente quindi eseguire un numero finito di verifiche per conoscere tutte le soluzioni)

Teorema di chiusura 9.8 (Interpretazione geometrica dell'eliminazione). *Sia $V=V(I)\subset K^n$ una varietà algebrica affine e sia K algebricamente chiuso. Sia $K^n \xrightarrow{\pi_t} K^{n-t}$ la proiezione sulle ultime $n-t$ coordinate. Allora*

$$V(I_t) = \overline{\pi_t(V)}$$

Dimostrazione Intanto notiamo che $\pi_t(V)\subset V(I_t)$. Infatti sia $(a_1,\ldots,a_n)\in V$ e quindi $(a_{t+1},\ldots,a_n)\in\pi_t(V)$. Se $f\in I_t$ abbiamo $f(a_{t+1},\ldots,a_n)$ e quindi

$$(a_{t+1},\ldots,a_n)\in V(I_t)$$

Pertanto $V(I_t)\supset\overline{\pi_t(V)}$.

Per l'inclusione opposta affermiamo che

$$I(\pi_t(V))\subset\sqrt{I_t} \tag{9.2}$$

Se (9.2) è vera allora abbiamo $V(I_t)=V(\sqrt{I_t})\subset V(I(\pi_t(V)))=\overline{\pi_t(V)}$ (vedi la prop. 6.6) come volevamo.

Per provare (9.2) prendiamo $f\in I(\pi_t(V))\subset K[x_{t+1},\ldots,x_n]\subset K[x_1,\ldots,x_n]$. Quindi se $(a_{t+1},\ldots,a_n)\in\pi_t(V)$ abbiamo $f(a_{t+1},\ldots,a_n)=0$. Pertanto $f\in I(V)$ e per il Nullstellensatz $f\in\sqrt{I}$, cioè $\exists\ n$ tale che $f^n\in I\cap K[x_{t+1},\ldots,x_n]=I_t$, cioè $f\in\sqrt{I_t}$ c.v.d.

Osservazione. *Per verificare che l'ipotesi K algebricamente chiuso è necessaria nel teorema di chiusura è sufficiente considerare $I=(x^2+y^2,2x^2+y^2+1)\subset\mathbf{R}[x,y]$. Eliminando la x abbiamo $V(I_1)=\{-1,1\}\subset\mathbf{R}$ mentre $\pi_1(V)=\emptyset$*

Possiamo risolvere adesso facilmente il problema di appartenenza di un elemento al radicale $\sqrt{I}$ di un ideale I di $K[x_1,\ldots,x_n]$.

Teorema 9.9. *Sia $I = (f_1, \ldots, f_s)$ un ideale di $K[x_1, \ldots, x_n]$. Allora*

$$f \in \sqrt{I} \Longleftrightarrow 1 \in (f_1, \ldots, f_s, 1 - yf) \subset K[x_1, \ldots, x_n, y]$$

Dimostrazione

"$\Longleftarrow$" è stata essenzialmente già vista nella dimostrazione della prop. 9.3. Se abbiamo $1 = \sum p_i(x,y) f_i + g(x,y)(1 - yf)$ ponendo $y = \frac{1}{f}$ e semplificando i denominatori si ottiene la tesi.

"$\Longrightarrow$" Sia $f^m \in I \subset \tilde{I} := (f_1, \ldots, f_s, 1 - yf)$. Per definizione abbiamo anche $1 - yf \in \tilde{I}$. Pertanto

$$1 = y^m f^m + (1 - y^m f^m) = y^m f^m + (1 - yf)(1 + yf + \ldots + y^{m-1} f^{m-1}) \in \tilde{I}$$

c.v.d.

Seguendo 3.3 ed il teorema 9.9 abbiamo quindi un algoritmo per decidere se $f \in \sqrt{I}$ che equivale alla inclusione $V(I) \subset V(f)$.

Il seguente diagramma schematizza come si possono trovare alcune soluzioni di un sistema generico di m equazioni polinomiali in n variabili (con $m \geq n$) se ad ogni passo sono verificate le ipotesi del teorema di estensione.

sistema in n variab.	$\xrightarrow{\text{elim.}}$	sistema in $(n-1)$ variab.	$\xrightarrow{\text{elim.}}$	$\cdots$	$\xrightarrow{\text{elim.}}$	sistema in 1 variab. $\downarrow$
soluz. in n variab.	$\xleftarrow{\text{estens.}}$	$\cdots$	$\xleftarrow{\text{estens.}}$	soluz. in 2 variab.	$\xleftarrow{\text{estens.}}$	soluz. in 1 variab. (magari numerica)

10. PARAMETRIZZAZIONI,

VARIETÀ RAZIONALI E UNIRAZIONALI

Riflessioni sulle definizioni di varietà algebrica e di varietà differenziabile:

Una varietà differenziabile nonsingolare X di dimensione k in $\mathbf{R}^n$ può essere introdotta in uno dei due modi equivalenti:

i) PARAMETRICO

$\forall x \in X$ esiste un intorno aperto $x \in U \subset X$ (con la topologia indotta), un aperto $V \subset \mathbf{R}^k$ ed un'applicazione suriettiva C^∞ $F: V \to U \subset \mathbf{R}^n$ di rango k.

ii) IMPLICITO

$\forall x \in X$ esiste un intorno aperto $x \in W \subset \mathbf{R}^n$ ed una funzione C^∞ $G\colon W \to \mathbf{R}^k$ di rango k tale che $X \cap W = \{y \in W | G(y) = 0\}$.

La condizione i) dà localmente una parametrizzazione della varietà. La condizione ii) dà invece equazioni implicite.

L'equivalenza delle condizioni i) e ii) segue essenzialmente dal teorema della funzione implicita.

Se al posto di C^∞ leggiamo "analitico reale" allora le condizioni i) e ii) sono ancora equivalenti e definiscono una varietà analitica reale.

Le varietà algebriche nascono sostituendo le funzioni C^∞ con le funzioni razionali (con denominatore mai nullo dove sono definite). La condizione ii) definisce allora un aperto di una varietà algebrica affine. In questo caso la condizione i) implica la ii), ed il procedimento con cui si ottiene la funzione G va sotto il nome di eliminazione dei parametri.

La condizione ii) non implica la i). Questo è mostrato dal seguente

Esempio 10.1. *(Le curve di Fermat). Sia C la curva di $\mathbf{R}^2$ data dall'equazione*

$$x^n + y^n - 1 = 0$$

per $n \geq 3$. Allora non esistono funzioni razionali $x = x(t)$, $y = y(t)$ tali che $(x(t), y(t)) \in C$ per t in un aperto di $\mathbf{R}$.

Supponiamo che esistano $x(t) = \frac{p(t)}{r(t)}$, $y(t) = \frac{q(t)}{r(t)}$ come nell'enunciato con p, q, r polinomi senza fattori comuni.

Abbiamo

$$p^n(t) + q^n(t) - r^n(t) = 0$$

da cui p, q, r sono primi tra loro a due a due. Derivando rispetto a t otteniamo la relazione

$$np^{n-1}p' + nq^{n-1}q' - nr^{n-1}r' = 0$$

Le due relazioni precedenti si riassumono nella forma matriciale:

$$\begin{pmatrix} p & q & -r \\ p' & q' & -r' \end{pmatrix} \begin{pmatrix} p^{n-1} \\ q^{n-1} \\ r^{n-1} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

Quindi il vettore $(p^{n-1}, q^{n-1}, r^{n-1})$ risulta proporzionale al vettore dato dai tre minori 2×2 (a segni alterni) della matrice 2×3 precedente. Si ottengono facilmente le due relazioni

$$\begin{vmatrix} q & -r \\ q' & -r' \end{vmatrix} q^{n-1} = - \begin{vmatrix} p & -r \\ p' & -r' \end{vmatrix} p^{n-1}$$

$$\begin{vmatrix} q & -r \\ q' & -r' \end{vmatrix} r^{n-1} = \begin{vmatrix} p & q \\ p' & q' \end{vmatrix} p^{n-1}$$

da cui le seguenti condizioni di divisibilità:

$$p^{n-1} \mid \begin{vmatrix} q & -r \\ q' & -r' \end{vmatrix}$$

$$q^{n-1} \mid \begin{vmatrix} p & -r \\ p' & -r' \end{vmatrix}$$

$$r^{n-1} \mid \begin{vmatrix} p & q \\ p' & q' \end{vmatrix}$$

Poniamo $deg\ p = P$, $deg\ q = Q$, $deg\ r = R$.

Le tre relazioni precedenti forniscono

$$(n-1)P \leq Q + R - 1$$

$$(n-1)Q \leq P + R - 1$$

$$(n-1)R \leq P + Q - 1$$

e sommando

$$(n-1)(P+Q+R) \leq 2(P+Q+R) - 3$$

che è una contraddizione se $n \geq 3$.

L'esempio delle curve di Fermat puó essere ripetuto parola per parola in ogni campo K con car K che non divide n. Infatti la derivata di un polinomio puó essere definita formalmente in un campo qualunque.

Osservazione. Se $n = 2$ allora

$$x = \frac{1-t^2}{1+t^2} \qquad y = \frac{2t}{1+t^2} \tag{10.1}$$

è una parametrizzazione razionale della conica $x^2 + y^2 - 1 = 0$.

Se $t = \frac{p}{q}$ si ricava (eliminando i denominatori) che $(p^2 - q^2, 2pq, p^2 + q^2)$ sono terne pitagoriche.

Se $n = 1$ si trova la retta $x + y - 1 = 0$ che ammette la parametrizzazione

$$x = t \qquad y = -t + 1$$

Parametrizzazioni polinomiali

Sia $F: K^m \to K^n$ una funzione polinomiale definita da $F = (f_1, \ldots, f_n)$ con f_i polinomi in $t_1, \ldots, t_m$.

Abbiamo così una parametrizzazione polinomiale di $Im\ F = F(K^m)$. Il teorema seguente mostra che si possono sempre trovare con un procedimento di eliminazione delle equazioni per la chiusura di Zariski di $F(K^m)$.

Teorema 10.2. *Sia K un campo algebricamente chiuso. Sia $F = (f_1, \dots, f_n): K^m \to K^n$ una funzione polinomiale. Sia $I = (x_1 - f_1(t_1, \dots, t_m), \dots, x_n - f_n(t_1, \dots, t_m)) \subset K[t_1, \dots, t_m, x_1, \dots, x_n]$ e sia $I_m = I \cap K[x_1, \dots, x_n]$ l'm-esimo ideale di eliminazione. Allora*

$$\overline{F(K^m)} = V(I_m)$$

Dimostrazione

Consideriamo il diagramma

$$\begin{array}{ccccc} V(I) & \subset & K^{n+m} & & \\ & i \nearrow & & \searrow \pi_m & \\ K^m & & \longrightarrow^F & & K^n \end{array} \tag{10.2}$$

dove $i(t_1, \dots, t_m) := (t_1, \dots, t_m, f_1(t_1, \dots, t_m), \dots, f_n(t_1, \dots, t_m))$.

È facile verificare che $i(K^m) = V(I)$, che si dice il grafico di F. Pertanto $F(K^m) = \pi_m(i(K^m)) = \pi_m(V(I))$ e quindi dal teorema di chiusura 9.8 $\overline{F(K^m)} = V(I_m)$ come volevamo.

Il teorema precedente è vero se K è un qualunque campo infinito, anche non algebricamente chiuso (ad esempio $\mathbf{R}$). Naturalmente non è possibile applicare il teorema di chiusura e quindi la dimostrazione va modificata nel modo seguente. Sia $K \subset \overline{K}$ (chiusura algebrica). Come sopra abbiamo $F(K^m) = \pi_m(V(I)) \subset V(I_m)$ e quindi $\overline{F(K^m)} \subset V(I_m)$ Sia adesso $V_K(g_1, \dots, g_s) \subset K^n$ una qualunque varietà tale che $F(K^m) \subset V_K(g_1, \dots, g_s)$. Quindi $g_i \circ F \equiv 0$ come polinomi in $t_1, \dots, t_m$. Il principio di identità dei polinomi vale su qualunque campo infinito, quindi g_i si annullano su $F(\overline{K}^m)$, da cui $V_{\overline{K}}(g_1, \dots, g_s) \supset \overline{F(\overline{K}^m)} = V_{\overline{K}}(I_m) \supset V_K(I_m)$ (l' uguaglianza per il teorema 10.2) . Quindi

$$V_K(g_1, \dots, g_s) \supset V_K(I_m)$$

da cui $V_K(I_m) \subset \overline{F(K^m)}$ come volevamo.

Il teorema precedente mostra che eseguendo l'eliminazione da $(x_1 - f_1, \dots, x_n - f_n)$ si trova la più piccola varietà contenente $F(K^m)$. In generale $F(K^m)$ può essere strettamente contenuto nella sua chiusura (anche se K é algebricamente chiuso). Ad esempio si prenda $F: K^2 \to K^2$ definita da $F(x, y) = (xy, y)$. $Im\ F$ é uguale a $\{y \neq 0\} \cup \{(0, 0)\}$ e $\overline{Im\ F} = K^2$. $Im\ F$ é un tipico esempio di insieme costruibile, come vedremo nel §16.

Invece con le notazioni del teorema 10.2 $F(K)$ (corrispondente a $m = 1$) é chiuso. Cioé vale la

Proposizione 10.3. *Sia K algebricamente chiuso. Sia $F = (f_1, \dots, f_n): K \to K^n$ una funzione polinomiale. Sia $I = (x_1 - f_1(t), \dots, x_n - f_n(t)) \subset K[t, x_1, \dots, x_n]$. Allora*

$$F(K) = \overline{F(K)} = V(I_1)$$

Dimostrazione Seguendo la dimostrazione del teorema 10.2 abbiamo $F(K) = \pi_1(V(I))$. Adesso se $(x_1, \dots, x_n) \in V(I_1)$ dal teorema 9.1 esiste t tale che $(t, x_1, \dots, x_n) \in V(I)$ e quindi $(x_1, \dots, x_n) \in \pi_1(V(I))$. Pertanto $V(I_1) = \pi_1(V(I)) = F(K)$ e quindi $F(K)$ é chiuso.

Esercizio. *Trovare un esempio di una parametrizzazione polinomiale F dove K non é algebricamente chiuso e $F(K)$ non é chiuso.*

Suggerimento: $F(x) = x^2$ su $\mathbf{R}$.

Parametrizzazioni razionali

Esempio 10.4. *Consideriamo $x = \frac{u^2}{v}$, $y = \frac{v^2}{u}$, $z = u$. Si vede subito che l'immagine di questa parametrizzazione F (che è definita per $u \neq 0$, $v \neq 0$) è contenuta in $x^2y - z^3 = 0$ Eliminando i denominatori abbiamo l'ideale*

$$I = (vx - u^2, uy - v^2, z - u) \subset K[u, v, x, y, z]$$

Eliminando u, v si trova $I_2 = \big(z(x^2y - z^3)\big)$. Pertanto in questo caso

$$V(I_2) = V(x^2y - z^3) \cup V(z) \supset_{\neq} V(x^2y - z^3) \supset \overline{F(K^2)}$$

Questo esempio mostra che il teorema 10.2 non puó essere generalizzato al caso di parametrizzazioni razionali semplicemente eliminando i denominatori.

Nel caso generale abbiamo

$$\begin{aligned} x_1 &= \frac{f_1(t_1, \ldots, t_m)}{g_1(t_1, \ldots, t_m)} \\ &\vdots \\ x_n &= \frac{f_n(t_1, \ldots, t_m)}{g_n(t_1, \ldots, t_m)} \end{aligned} \tag{10.3}$$

dove f_i, g_i sono polinomi. In questo caso si dice che abbiamo una parametrizzazione razionale, che è definita dove $g_i \neq 0$. Precisamente, posto $W = V(g_1, \ldots, g_n) \subset K^m$ le (10.3) definiscono

$$F\colon K^m \setminus W \to K^n \tag{10.4}$$

dove $F = (\frac{f_1}{g_1} \ldots \frac{f_n}{g_n})$. Consideriamo il diagramma (analogo a (10.2))

$$\begin{array}{ccccc} V(I) & \subset & K^{n+m} & & \\ & i \nearrow & & \searrow \pi_m & \\ K^m \setminus W & & \longrightarrow^F & & K^n \end{array}$$

Se $I := (g_1x_1 - f_1, \ldots, g_nx_n - f_n)$ allora l'esempio 10.4 mostra che può essere

$$i(K^m \setminus W) \subset_{\neq} V(I)$$

e quindi non si può ripetere la costruzione del teor. 10.2.

Per trattare questo problema l'approccio giusto sta nel definire $g := g_1 g_2 \cdots g_n$ e considerare il diagramma

$$\begin{array}{ccccc} W = V(J) & \subset & K^{n+m+1} & & \\ & j \nearrow & & \searrow \pi_m & \\ K^m \setminus W & & \longrightarrow^F & & K^n \end{array}$$

dove $j(t_1, \ldots, t_m) = (\frac{1}{g(t_1,\ldots,t_m)}, t_1, \ldots, t_m, \frac{f_1}{g_1}, \ldots, \frac{f_n}{g_n})$ e dove

$$J := (g_1 x_1 - f_1, \ldots, g_n x_n - f_n, 1 - gy) \subset K[y, t_1, \ldots, t_m, x_1, \ldots, x_n]$$

Lemma 10.5.

$$j(K^m \setminus W) = V(J)$$

Dimostrazione
"$\subset$" *È ovvia dalle definizioni*
"$\supset$" *Se* $(y, t_1, \ldots, t_m, x_1, \ldots, x_n) \in V(J)$ *allora abbiamo* $g(t_1, \ldots, g_m)y = 1$ *da cui*

$$g_i(t_1, \ldots, t_m) \neq 0$$

e quindi $x_i = \frac{f_i}{g_i}$ *c.v.d.*

Teorema 10.6. *Se* K *è un campo infinito allora*

$$\overline{F(K^m \setminus W)} = V(J_{m+1})$$

La dimostrazione è analoga al teorema 10.2 ed all'osservazione successiva e viene lasciata come esercizio.

Ovviamente $F(K^m \setminus W)$ puó essere strettamente contenuto nella sua chiusura, anche se $m = 1$. Si veda ad esempio le equazioni (10.1) che definiscono tutta la circonferenza meno il punto $(-1, 0)$.

Esercizio. *Sia* $W = V(xy) \subset K^2$ *e sia* $F: K^2 \setminus W \to K^2$ *definita da* $F(x, y) = (\frac{x}{y^2}, \frac{y}{x^2}, x)$. *Calcolare* $\overline{F(K^2 \setminus W)}$.

Definizione 10.7. *Una varietà* $V \subset K^n$ *immagine di una parametrizzazione razionale si dice unirazionale. Cioè se* V *è unirazionale deve esistere* F *come in (10.4) e*

$$\overline{F(K^m \setminus W)} = V$$

.

Vedremo che se $K = \mathbf{C}$ una varietá unirazionale per cui esiste una parametrizzazione razionale F iniettiva si dice razionale.

Daremo nella sezione seguente la definizione generale di varietá razionale con la nozione di applicazione razionale tra varietà.

Ogni varietá razionale é anche unirazionale. Pertanto l'esempio 10.1 mostra che le curve di Fermat non sono unirazionali se $n \geq 3$ mentre sono razionali se $n \leq 2$. Un classico teorema di Lüroth afferma che le curve unirazionali sono razionali.

Il teorema 10.6 dà un algoritmo per trovare le equazioni di varietà unirazionali. Nel caso di curve che ammettono una parametrizzazione razionale con un solo parametro l'algoritmo precedente può essere semplificato. Il seguente lemma mostra in sostanza che il fenomeno visto con l'esempio 10.4 non si può ripetere nel caso di curve.

Lemma 10.8. *Sia K un campo infinito. Consideriamo le equazioni $x_i = \frac{f_i(t)}{g_i(t)}$ per $i = 1, \ldots, n$ con $f_i, g_i \in K[t]$ polinomi primi tra loro. Sia $W := V(g_1 \cdots g_n) \subset K$, sia $F: K \setminus W \to K^n$ data da $F(t) := (\frac{f_1(t)}{g_1(t)}, \ldots, \frac{f_n(t)}{g_n(t)})$, sia $I = (\ldots g_i(t)x_i - f_i(t), \ldots) \subset K[t, x_1, \ldots, x_n]$ e sia $i: K \to K^{n+1}$ definita da $i(t) := (t, \frac{f_1(t)}{g_1(t)}, \ldots, \frac{f_n(t)}{g_n(t)})$. Allora*

i) $V(I) = i(K \setminus W)$

ii) $\overline{F(K \setminus W)} = V(I_1)$

Dimostrazione Si considera il diagramma

$$\begin{array}{ccccc} V(I) & \subset & K^{n+1} & & \\ & i \nearrow & & \searrow \pi_1 & \\ K \setminus W & & \longrightarrow^F & & K^n \end{array}$$

Per provare i) abbiamo che l'inclusione $\supset$ è banale. Viceversa sia $(\tilde{t}, \tilde{x}_1, \ldots, \tilde{x}_n) \in V(I)$. Allora $g_i(\tilde{t})\tilde{x}_i - f_i(\tilde{t}) = 0 \quad \forall i$. Se $g_i(\tilde{t}) = 0$ allora anche $f_i(\tilde{t}) = 0$ e quindi f_i, g_i sarebbero divisibili per $t - \tilde{t}$ in contrasto con l'ipotesi. Pertanto $\tilde{t} \notin W$ e quindi si ricava $\tilde{x}_i = \frac{f_i(\tilde{t})}{g_i(\tilde{t})}$. Adesso ii) segue come nel teorema 10.2

Esempio. *Il folium di Cartesio.*

Si considera la parametrizzazione razionale

$$x = \frac{3t}{1 + t^3} \tag{10.5a}$$

$$y = \frac{3t^2}{1 + t^3} \tag{10.5b}$$

Con la tecnica del teorema 10.8 occorre per trovare equazioni implicite eliminare la t dall'ideale

$$\left((1 + t^3)x - 3t, (1 + t^3)y - 3t^2\right) \tag{10.6}$$

e si ottiene l'equazione

$$x^3 + y^3 - 3xy = 0 \tag{10.7}$$

Per il teorema 10.8 l'equazione rappresenta la chiusura del luogo descritto dalla parametrizzazione. Quindi $\overline{F(K \setminus W)} = V(I_1)$

Viceversa ogni punto in $\mathbf{C}^2$ che soddisfa l' equazione (10.7) proviene dalla parametrizzazione. Infatti il punto $(x, y) = (0, 0)$ viene ottenuto per $t = 0$, mentre per gli altri valori di x e y uno dei coefficienti di t^3 in (10.6) è $\neq 0$ e quindi dal teorema di estensione 9.1 si ha la tesi. Quindi in questo caso $F(K \setminus W) = \overline{F(K \setminus W)} = V(I_1)$.

Esercizio. *Provare che ogni $(x_0, y_0) \in \mathbf{R}^2$ appartenente al folium di Cartesio $x^3 + y^3 - 3xy = 0$ proviene da un $t_0 \in \mathbf{R}$ secondo la parametrizzazione (10.5).*

Suggerimento: $\mathbf{R}$ non é algebricamente chiuso e quindi non si puó applicare il teorema 9.1. Posto $f = (1 + t^3)x - 3t$, $g = (1 + t^3)y - 3t^2$, possiamo supporre $x_0 \neq 0, y_0 \neq 0$ ed abbiamo $Res(f(x_0, y_0, t), g(x_0, y_0, t), t) = 0$. Pertanto $f(x_0, y_0, t)$ e $g(x_0, y_0, t)$ hanno un fattore a comune in $\mathbf{R}[t]$. Se questo fattore ha grado due allora si puó scrivere $t^3 x_0 - 3t + x_0 = (t^2 + bt + c)(tx_0 - \alpha)$ e $t^3 y_0 - 3t^2 + y_0 = (t^2 + bt + c)(ty_0 - \beta)$ da cui $-\alpha c = x_0$, $-\beta c = y_0$, $\beta x_0 = \alpha y_0$ e quindi ...

11. MORFISMI TRA VARIETÁ ALGEBRICHE

Siano $V \subset K^m$ e $W \subset K^n$ due varietà algebriche affini irriducibili.

Definizione 11.1. *Una funzione $\phi: V \to W$ si dice un <u>morfismo regolare</u> (tra varietà) se esistono polinomi $f_1, \ldots, f_n \in K[x_1, \ldots, x_m]$ tali che*

$$\phi(a_1, \ldots, a_m) = (f_1(a_1, \ldots, a_m), \ldots f_n(a_1, \ldots, a_m))$$

per ogni $(a_1, \ldots, a_m) \in V$

Possiamo scrivere $\phi = (f_1, \ldots, f_n)$.

Se $W = K$ allora i morfismi regolari da V a K si dicono <u>funzioni regolari</u> e formano in modo naturale un anello isomorfo a $\frac{K[x_1, \ldots, x_n]}{I(V)}$ che si dice anello delle coordinate di V e si indica con $K[V]$. $K[V]$ ha in più una struttura di K-algebra con unità. In pratica due funzioni regolari su K^n sono uguali nel quoziente $K[V]$ (per $V \subset K^n$) quando hanno lo stesso valore su V. Ad esempio possiamo sommare ad uno qualunque dei polinomi che definiscono una funzione regolare su V un altro polinomio scelto tra le equazioni che definiscono V ed otteniamo ancora la stessa funzione regolare.

Esercizio. *Siano V e W due varietà algebriche affini.*

i) Ogni morfismo regolare da V a W è una funzione continua (con la topologia di Zariski) (suggerimento: provare che la retroimmagine di un chiuso è ancora un chiuso).

ii) Trovare una funzione continua tra due varietà algebriche che non è un morfismo regolare (suggerimento: si prenda $V = W = K \ldots$).

Teorema 11.2. *Sia V una varietá irriducibile. Sia K algebricamente chiuso e sia $f: V \to K$ tale che $\forall p \in V \quad \exists\, U_i$ aperto di V con $f = \frac{g_i}{h_i}$ su U_i con g_i, h_i polinomi e $h_i(x) \neq 0$ se $x \in U_i$. Allora f é una funzione regolare.*

Dimostrazione Per ipotesi $fh_i - g_i = 0$ su U_i e per l'irriducibilitá segue che $fh_i - g_i = 0$ su tutto V. Consideriamo l'ideale J generato dai denominatori h_i e sia $V = V(I) = V(f_1, \ldots, f_k)$. Per ipotesi $V(I + J) = \emptyset$ e quindi per il teorema degli zeri (debole) si ha $I + J = (1)$, cioé si puó scrivere $1 = \sum q_i h_i + \sum k_j f_j$ (entrambe sono somme finite). Pertanto in $K[V]$ abbiamo $1 = \sum q_i h_i$. Segue che in $K[V]$

$$f = \sum q_i h_i f = \sum q_i g_i$$

che é una funzione regolare.

Osservazione. *Ricordiamo che se A e B sono due K-algebre con unità allora un morfismo di K-algebre con unità $f: A \to B$ è un morfismo di anelli tale che $f(1) = 1$ e tale che $f(ka) = kf(a) \forall a \in A, k \in K$. Quindi $f(k) = f(k \cdot 1) = kf(1) = k \ \forall k \in K$. Pertanto i morfismi di K-algebre con unità da $K[W]$ a $K[V]$ possono essere identificati con i morfismi di anelli che valgono l'identità sugli elementi di K.*

Proposizione 11.3. *Un morfismo regolare $\phi: V \to W$ tra varietà algebriche affini induce un morfismo di K-algebre con unità $\phi^*: K[W] \to K[V]$ definito da $\phi^*(f) := f \circ \phi$ Questa corrispondenza è funtoriale nel senso che*

$$\phi^* \circ \psi^* = (\psi \circ \phi)^* \tag{11.1a}$$

$$(1_V)^* = 1_{K[V]} \tag{11.1b}$$

(denotiamo con 1 l'isomorfismo identitá)

Dimostrazione ϕ^* è ben definita perché se $f \in I(W)$ allora $f \circ \phi \in I(V)$. Segue subito dalla definizione che ϕ^* conserva somme e prodotti come anche le altre affermazioni dell'enunciato.

Proposizione 11.4. *Sia $w: K[W] \to K[V]$ un morfismo di K-algebre con unità. Allora esiste un <u>unico</u> morfismo regolare $\phi: V \to W$ tale che $\phi^* = w$.*

Dimostrazione Siano $y_1, \ldots, y_n$ coordinate su K^n. Pertanto $[y_i] \in K[W]$ e per ipotesi esistono polinomi $a_i(x_1, \ldots, x_m)$ tali che $w([y_i]) = [a_i(x_1, \ldots, x_m)]$. Definiamo $\phi := (a_1, \ldots, a_n): K^m \to K^n$. Dobbiamo provare che $\phi(V) \subset W$ e che $\phi^* = w$.

Abbiamo dalla definizione $w([y_i]) = [y_i \circ \phi]$ e siccome w è un morfismo di K-algebre $w([y_i^2]) = [y_i^2 \circ \phi]$, $w([y_i^3 y_j]) = [y_i^3 y_j \circ \phi]$ e quindi per ogni polinomio $F \in K[y_1, \ldots, y_n]$

$$w([F]) = [F \circ \phi] \tag{11.2}$$

Pertanto $\forall\ g \in I(W)$ abbiamo $[g \circ \phi] = w([g]) = w(0) = 0$ cioè $g \circ \phi \in I(V)$. Ne segue che se $c \in V$ e $g \in I(W)$ vale $g(\phi(c)) = 0$ e quindi $\phi(c) \in V(I(W)) = W$, cioè $\phi(V) \subset W$ come volevamo. La formula (11.2) si interpreta allora come $\phi^* = w$.

Rimane da provare che ϕ è unico. Infatti se abbiamo $\psi := (b_1, \ldots, b_n)$ tale che $\psi^* = w = \phi^*$ segue $[b_i] = [y_i \circ \psi] = \psi^*[y_i] = \phi^*[y_i] = [y_i \circ \phi] = [a_i]$. Quindi $b_i = a_i$ su V, c.v.d.

Definizione 11.5. *Due varietà algebriche V e W si dicono isomorfe se esistono morfismi regolari $a\colon V \to W$ e $b\colon W \to V$ tali che $a \circ b = 1_W$ e $b \circ a = 1_V$.*

Teorema 11.6. *Due varietà algebriche V e W sono isomorfe se e solo se le K-algebre con unità $K[V]$ e $K[W]$ sono isomorfe.*

Dimostrazione Se $a \circ b = 1_W$ e $b \circ a = 1_V$ allora dalle (11.1) $a^* \circ b^* = 1_{K[W]}$ e $b^* \circ a^* = 1_{K[V]}$, pertanto a^* e b^* sono isomorfismi (uno inverso dell'altro). Viceversa se abbiamo $w\colon K[W] \to K[V]$ isomorfismo con inversa $v\colon K[V] \to K[W]$ allora dalla prop. 11.4 esistono morfismi regolari $a\colon V \to W$ e $b\colon W \to V$ tali che $a^* = w$ e $b^* = v$. Pertanto $(a \circ b)^* = b^* \circ a^* = v \circ w = 1_{K[W]} = (1_W)^*$. Dall'unicità nella prop. 11.4 segue $a \circ b = 1_W$ ed analogamente si prova $b \circ a = 1_V$ da cui V e W sono isomorfe.

Il teorema 11.6 chiarisce il corollario 9.7 secondo cui c'é una corrispondenza biunivoca naturale tra punti di V e ideali massimali di $K[V]$.

Esempio. *Sia $C \subset \mathbf{R}^3$ la cubica gobba (si veda l'esempio 5.6) e $W = V(v - u - u^2) \subset \mathbf{R}^2$. Allora $\phi(x, y, z) = (xy, z + x^2 y^2)$ definisce un morfismo regolare da C a W.*

Basta verificare che $\phi(t, t^2, t^3) = (t^3, t^3 + t^6)$ soddisfa all'equazione di W. Infatti $v - u - u^2 = (t^3 + t^6) - t^3 - (t^3)^2 = 0$.

Esercizio. *Provare che $a(x, y, z) = (2x^2 + y^2, z^2 - y^3 + 3xz)$ e $b(x, y, z) = (2y + xz, 3y^2)$ rappresentano lo stesso morfismo regolare dalla cubica gobba $C \subset \mathbf{R}^3$ a $\mathbf{R}^2$.*

Esercizio. *Provare che ogni ipersuperficie in K^n luogo degli zeri di*

$$x_n - f(x_1, \ldots, x_{n-1})$$

(grafico del polinomio f) è isomorfa a K^{n-1}.

Esempio 11.7. *Proveremo che la cubica "ellittica" $C = V(y^2 - x^3 + x) \subset K^2$ dove $K = \mathbf{R}$ oppure $\mathbf{C}$ <u>non</u> è isomorfa a K. Infatti consideriamo per assurdo un morfismo regolare $\phi\colon K \to C$ dato da $\phi = (a(t), b(t))$. Abbiamo $b^2 - a^3 + a = 0$ e quindi $b^2 = a(a^2 - 1)$. I due fattori nel secondo membro sono primi tra loro. Quindi, decomponendo a e b in*

fattori irriducibili, tutti i fattori irriducibili distinti sia di a che di a^2-1 devono apparire con esponente pari. Pertanto esiste $c(t) \in K[t]$, primo con a, tale che $c^2 = a^2 - 1$. In particolare deg a = deg c. Se questo grado è positivo derivando otteniamo $2cc' = 2aa'$ e quindi a divide c' che è impossibile per questioni di grado. Pertanto a (e quindi anche b) deve essere un polinomio costante, che è una contraddizione.

Esempio 11.8. *In questo esempio costruiremo un morfismo regolare biunivoco tra due varietà che non è un isomorfismo. Sia $C = V(y^2 - x^3) \subset \mathbf{R}^2$. V è una cubica razionale cuspidata. $\phi(x,y) := y$ è un morfismo regolare da C a $\mathbf{R}$ ed è facile verificare che è biunivoco. Se esistesse una inversa $\psi = (c(u), d(u))$ da $\mathbf{R}$ a C allora avremmo $d(u)^3 = c(u)^2 \quad \forall u \in \mathbf{R}$. Possiamo supporre (eventualmente sostituendo u con $u + u_0$) che $(c(0), d(0)) = (0,0)$. Allora, posto*

$$c(u) = c_1 u + c_2 u^2 + \dots$$

$$d(u) = d_1 u + d_2 u^2 + \dots$$

abbiamo

$$c_1 u^2 + 2c_1 c_2 u^3 + \dots = d_1^3 u^3 + \dots$$

da cui uguagliando i coefficienti con lo stesso grado: $c_1 = 0$, $2c_1 c_2 = d_1$ e segue anche $d_1 = 0$. Consideriamo ora $\psi^*: K[C] \to K[\mathbf{R}] = K[u]$. Abbiamo visto in (11.2) che $\psi^*[f] = f(c(u), d(u))$. Quindi l'immagine di ψ^* è costituita dai polinomi in $c(u) = c_2 u^2 + \dots$ e $d(u) = d_2 u^2 + \dots$ e non può contenere u (basta guardare i gradi). Ne segue che ψ^* non può essere un isomorfismo, come volevamo.

Osservazione. *Se $V \subset K^n$ è una varietà irriducibile allora da 6.12 $I(V)$ è un ideale primo e quindi $K[V] = K[x_1, \dots, x_n]/I(V)$ è un dominio di integrità. Denotiamo con $K(V)$ il campo delle frazioni di $K[V]$ per V varietà irriducibile. Pertanto $K(V) = \{\frac{\phi}{\psi} : \phi, \psi \in K[V], \psi \neq 0\}$. Indichiamo con $K(x_1, \dots, x_n)$ il campo delle frazioni di $K[x_1, \dots, x_n]$.*

Definizione 11.9. *Siano $V \subset K^m$ e $W \subset K^n$ due varietà affini irriducibili. Un morfismo razionale da V a W è una funzione ϕ rappresentata da*

$$\phi(x_1, \dots, x_m) = \left(\frac{f_1(x_1, \dots, x_m)}{g_1(x_1, \dots, x_m)}, \dots, \frac{f_n(x_1, \dots, x_m)}{g_n(x_1, \dots, x_m)} \right)$$

dove $\frac{f_i}{g_i}$ soddisfano a:

i) $\exists\, x \in V$ tale che $x \notin V(\prod_{j=1}^n g_j)$

ii) $\forall x \in V \setminus V(\prod_{j=1}^n g_j)$ vale $\phi(x) \in W$.

ϕ non è una funzione da V a W nel senso usuale del termine e $V \setminus V(\prod_{j=1}^n g_j)$ viene ad essere il luogo dove ϕ è definita (luogo dove ϕ é regolare). Per questo motivo si indica un morfismo razionale da V a W con la notazione:

$$\phi: V - - \to W$$

Due morfismi razionali ϕ e ψ da V a W si dicono uguali se esiste una sottovarietà propria $V' \subset V$ tale che ϕ e ψ sono entrambe definite su $V \setminus V'$ e $\phi(x) = \psi(x)\ \forall x \in V \setminus V'$. (Per essere precisi dovremmo definire un morfismo razionale da V a W come una classe di equivalenza tra le coppie (Z, ϕ) con Z aperto di Zariski non vuoto in V e $\phi: Z \to W$ rappresentata da quozienti di polinomi dove (Z, ϕ) è equivalente a (Z', ϕ') se $\phi = \phi'$ su $Z \cap Z'$).

Lemma 11.10. *Siano $\phi, \psi: V -- \to W$ due morfismi razionali rappresentati da*

$$\phi = \left(\frac{f_1}{g_1}, \ldots \frac{f_n,}{g_n}\right) \qquad \psi = \left(\frac{h_1}{k_1}, \ldots \frac{h_n,}{k_n}\right)$$

Allora $\phi = \psi \iff f_i k_i - h_i g_i \in I(V) \quad \forall i$

Dimostrazione

$\Longrightarrow$ Se ϕ e ψ sono definiti ed uguali su $V \setminus V'$ allora $\frac{f_i}{g_i} = \frac{h_i}{k_i} \quad \forall i$ su $V \setminus V'$. Quindi $f_i k_i - h_i g_i$ si annullano su $V \setminus V'$, da cui $V = V(f_i k_i - h_i g_i) \cup V'$ e per l'irriducibilità di V abbiamo $V = V(f_i k_i - h_i g_i)$ e pertanto $f_i k_i - h_i g_i \in I(V)$

$\Longleftarrow$ Poniamo $V_1 := V(g_1, \ldots, g_n)$ e $V_2 := V(k_1, \ldots, k_n)$. Siccome ϕ e ψ sono definite in qualche punto di V abbiamo che V_1 e V_2 sono sottovarietà proprie di V. V è irriducibile e quindi anche $V' := V_1 \cup V_2$ è una sottovarietà propria. Quindi ϕ e ψ sono entrambe definite su $V \setminus V'$ e per ipotesi abbiamo $\frac{f_i}{g_i} = \frac{h_i}{k_i} \quad \forall i$ su $V \setminus V'$.

Lemma 11.11. *Sia K algebricamente chiuso. Un morfismo razionale definito su tutto V é un morfismo regolare.*

Dimostrazione (é analoga a quella del teor. 11.2). Sia $V = V(I)$. Con le notazioni della definizione 11.9 poniamo $g = \prod_{j=1}^{n} g_j$. Allora $V(I + (g)) = \emptyset$ e quindi $(1) = I + (g)$ cioé in $K[V]$ esiste h tale che $gh = 1$. Pertanto $\frac{f_i}{g_i} = f_i \prod_{j \neq i} g_j h$.

Corollario 11.12. *Sia K algebricamente chiuso. Una funzione razionale definita su tutto V é una funzione regolare.*

Definizione 11.13. *Dati $\phi: V -- \to W$ e $\psi: W -- \to Z$ morfismi razionali diciamo che $\psi \circ \phi$ è definita se esiste $p \in V$ tale che ϕ è definita in p e ψ è definita in $\phi(p)$.*

Lemma 11.14. *Siano $\phi: V -- \to W$ e $\psi: W -- \to Z$ due morfismi razionali tali che $\psi \circ \phi$ è definita. Allora esiste una sottovarietà propria $V' \subset V$ tale che*

i) ϕ è definita su $V \setminus V'$ e ψ è definita su $\phi(V \setminus V')$

ii) $\psi \circ \phi: V -- \to Z$ è un morfismo razionale definito su $V \setminus V'$.

Dimostrazione Sia

$$\phi(x_1, \ldots, x_m) = \left(\frac{f_1(x_1, \ldots, x_m)}{g_1(x_1, \ldots, x_m)}, \ldots, \frac{f_n(x_1, \ldots, x_m)}{g_n(x_1, \ldots, x_m)}\right)$$

$$\psi(y_1, \ldots, y_m) = \left(\frac{h_1(y_1, \ldots, y_m)}{k_1(y_1, \ldots, y_m)}, \ldots, \frac{h_n(y_1, \ldots, y_m)}{k_n(y_1, \ldots, y_m)}\right)$$

La j-esima coordinata di $\psi \circ \phi$ è $\frac{h_j(f_1/g_1,\ldots,f_n/g_n)}{k_j(f_1/g_1,\ldots,f_n/g_n)} = \frac{P_j}{Q_j}$ dove $P_j,\ Q_j \in K[x_1,\ldots,x_n]$ sono ottenuti raccogliendo i termini dell'espressione a primo membro a denominatore comune. Per ipotesi esiste $p \in V$ tale che $g_i(p) \neq 0 \quad \forall i$ e $k_j(f_1(p)/g_1(p),\ldots,f_n(p)/g_n(p)) \neq 0 \quad \forall j$. Pertanto $Q_j(p) \neq 0$. Poniamo $V' := V(Q_1,\ldots,Q_m)$. È immediato verificare che V' soddisfa alle condizioni dell'enunciato.

Esempio. *Se* $\phi: \mathbf{R} \dashrightarrow \mathbf{R}^3$ *e* $\psi: \mathbf{R}^3 \dashrightarrow \mathbf{R}$ *sono definite da*

$$\phi(t) = (t, \frac{1}{t}, t^2) \qquad \psi(x,y,z) = \frac{x+yz}{x-yz}$$

allora $\psi \circ \phi$ *non è definita.*

Definizione 11.15. *Un morfismo razionale* $\phi: V \dashrightarrow W$ *si dice dominante se è definito su* $V \setminus V'$ *e se* $\phi(V \setminus V')$ *è denso in* W *(con la topologia di Zariski)*

La composizione di due morfismi razionali dominanti é ben definita ed é ancora un morfismo razionale dominante. In particolare le varietá algebriche insieme ai morfismi razionali dominanti costituiscono una categoria.

Definizione 11.16. *Due varietà algebriche* V *e* W *si dicono birazionalmente equivalenti se esistono morfismi razionali* $a: V \dashrightarrow W$ *e* $b: W \dashrightarrow V$ *tali che* $a \circ b = 1_W$ *e* $b \circ a = 1_V$ *(come morfismi razionali).*

Definizione 11.17. *Una varietá si dice* razionale *se é birazionalmente equivalente a* K^n. *Vedremo al termine del §16 che se* $K = \mathbf{C}$ *questa definizione é equivalente all'esistenza di una parametrizzazione razionale iniettiva.*

Ovviamente varietá isomorfe sono anche birazionalmente equivalenti. L'esempio seguente mostra che non vale il viceversa.

Esempio. *La cubica cuspidata* $C = V(y^2 - x^3) \subset \mathbf{R}^2$ *che abbiamo visto nell'esempio 11.8 non essere isomorfa a* $\mathbf{R}$ *è invece birazionalmente equivalente a* $\mathbf{R}$ *e quindi è razionale. Infatti si possono definire* $\phi: C \dashrightarrow \mathbf{R}$ *dato da* $\phi(x,y) = \frac{y}{x}$ *e* $\psi: \mathbf{R} \dashrightarrow C$ *data da* $\psi(u) = (u^2, u^3)$ *ed è facile verificare che* ϕ *e* ψ *sono morfismi razionali inversi l'uno dell'altro.*

Classicamente lo studio delle varietà algebriche avveniva modulo trasformazioni birazionali, seguendo il "Programma di Erlangen" di F. Klein secondo cui lo studio della geometria consiste nello studio delle proprietà invarianti per un gruppo di trasformazioni (quindi con l'azione del gruppo delle isometrie abbiamo la geometria metrica, con l'azione delle affinità abbiamo la geometria affine e così via).

La nozione algebrica corrispondente ai morfismi razionali è illustrata dalla seguente

Proposizione 11.18. *Un morfismo razionale dominante* $\phi: V \to W$ *tra varietà algebriche affini induce un omomorfismo di campi* $\phi^*: K(W) \to K(V)$ *tale che* $\phi^*_{|K} = 1_K$ *definito da* $\phi^*(f) := f \circ \phi$. *Questa corrispondenza è funtoriale nel senso che*

$$\phi^* \circ \psi^* = (\psi \circ \phi)^*$$

$$1_V^* = 1_{K(V)}$$

Dimostrazione La definizione di ϕ^* equivale a $\phi^*(\frac{[f]}{[g]}) = \left[\frac{f\circ\phi}{g\circ\phi}\right]$ dove $[f]$, $[g] \in K[Y]$, $[g] \neq 0$. Se $[g] \neq 0$ allora $\{y \in V | g(y) = 0\}$ è incluso in una sottovarietà propria di V e quindi siccome ϕ è dominante esiste $x \in V$ tale che $g(\phi(x)) \neq 0$. ϕ^* risulta in modo naturale un omomorfismo di campi.

Proposizione 11.19. *Sia $w: K(W) \to K(V)$ un omomorfismo di campi tale che $w_{|K} = 1_K$. Allora esiste un <u>unico</u> morfismo razionale dominante $\phi: V \to W$ tale che $\phi^* = w$.*

Dimostrazione Siano $y_1, \ldots, y_n$ coordinate su K^n. Pertanto $[y_i] \in K[W]$ e per ipotesi esistono polinomi $f_i(x_1, \ldots, x_m), g_i(x_1, \ldots, x_m)$ tali che $w([y_i]) = \frac{[f_i]}{[g_i]}$. Definiamo $\phi := (\frac{f_1}{g_1}, \ldots \frac{f_n}{g_n})$ che è un morfismo razionale da V a W. Affermiamo che ϕ è dominante, infatti se l'immagine di ϕ fosse contenuta in una sottovarietà propria di W allora esisterebbe qualche $F \in K[W]$ tale che $F(\frac{f_1}{g_1}, \ldots \frac{f_n}{g_n}) = 0$. Pertanto avremmo $F(w[y_1], \ldots, w[y_n]) = 0$ e siccome w è un omomorfismo tale che $w_{|K} = 1_K$ vale $w(F(y_1, \ldots, y_n)) = 0$. Ogni omomorfismo tra campi è iniettivo e quindi $F(y_1, \ldots, y_n) = 0$ in $K(W)$.

Quindi possiamo scrivere $w([f]/[g]) = [f \circ \phi]/[g \circ \phi]$ da cui segue $\phi^* = w$ ed è facile verificare analogamente alla dimostrazione di 11.4 che ϕ è unica.

Teorema 11.20. *Due varietà algebriche V e W sono birazionalmente equivalenti se e solo se i due campi $K(V)$ e $K(W)$ sono due estensioni isomorfe di K.*

Dimostrazione La dimostrazione è formalmente analoga a quella del teorema 11.6.

12. IDEALI OMOGENEI E VARIETÁ PROIETTIVE

Consideriamo lo spazio proiettivo $\mathbf{P}^n(K)$ sul campo K con coordinate omogenee $(x_0, \ldots, x_n)$. Se $f(x_0, \ldots, x_n) = f(x)$ è un polinomio qualunque non è possibile definire il luogo degli zeri $\{x \in \mathbf{P}^n(K) | f(x) = 0\}$. Invece se f è un polinomio omogeneo, cioè se tutti i suoi termini hanno lo stesso grado allora posto $d = deg\ f$ vale la relazione $f(\lambda x_0, \lambda x_1, \ldots, \lambda x_n) = \lambda^d f(x_0, x_1, \ldots, x_n)$. Pertanto $f(\lambda x) = 0$ se e solo se $f(x) = 0$. Quindi é ben definito in $\mathbf{P}^n(K)$ il luogo degli zeri di un polinomio omogeneo. Abbiamo la:

Definizione 12.1. *Se f è un polinomio omogeneo in $K[x_0, \ldots, x_n]$ allora*

$$V(f) = \{x \in \mathbf{P}^n(K) | f(x) = 0\}$$

si dice una ipersuperficie proiettiva.

Definizione 12.2. *Se $f_1, \ldots f_p$ sono polinomi omogenei in $K[x_0, \ldots, x_n]$ allora*

$$V(f_1, \ldots f_p) = \{x \in \mathbf{P}^n(K) | f_1(x) = \ldots = f_p(x) = 0\}$$

si dice una varietà (algebrica) proiettiva.

Notiamo che ogni polinomio è somma delle sue componenti omogenee, cioé se $f \in K[x_0, \ldots, x_n]$ abbiamo $f = \sum_{i=0}^{d}$ dove f_i é omogeneo di grado d.

Vediamo adesso che in termini algebrici le varietà proiettive corrispondono agli ideali omogenei di $K[x_0, \ldots, x_n]$.

Definizione 12.3. *Un ideale I di $K[x_0, \ldots, x_n]$ si dice omogeneo se è generato da polinomi omogenei.*

Lemma 12.4. *Sia I un ideale*

$$I \text{ è omogeneo} \Longleftrightarrow \text{se } g \in I \text{ anche le sue componenti omogenee } \quad g_i \in I \quad \forall i$$

.

Dimostrazione

$\Longrightarrow$ Siano $\{f_1, \ldots, f_p\}$ generatori omogenei di I. Allora esistono $a_j \in K[x_0, \ldots, x_n]$ tali che

$$g = \sum g_i = \sum a_j f_j \tag{12.1}$$

Posto $a_j = \sum a_{jk}$ (componenti omogenee), sostituiamo queste espressioni in (12.1) ed otteniamo $\sum g_i = \sum a_{jk} f_j$. Eguagliando tra loro i termini di ogni grado si ottiene che ogni g_i è combinazione dei f_j.

$\Longleftarrow$ Basta prendere le componenti omogenee di un insieme di generatori e si ottiene ancora un insieme di generatori.

Conviene guardare in questo contesto a $S = K[x_0, \ldots, x_n]$ come ad un anello graduato, cioè posto $S_d = \{f \in S | deg\ f = d\}$ si ha $S = \oplus_{d \geq 0} S_d$ (somma diretta di spazi vettoriali) con la struttura moltiplicativa che soddisfa a $S_d \cdot S_{d'} \subset S_{d+d'}$. Allora il lemma 12.4 si traduce nel fatto che I è omogeneo se e solo se $I = \oplus_{d \geq 0}(I \cap S_d)$.

Se I è un ideale omogeneo generato da $f_1, \ldots, f_p$ allora $V(I) = V(f_1, \ldots, f_p) \subset \mathbf{P}^n(K)$ è una varietà proiettiva ed ogni varietá proiettiva ha questa forma. Precisamente si puó definire

$$V(I) = \{x \in \mathbf{P}^n | f(x) = 0 \quad \forall f \text{ omogeneo } \in I\}$$

Analogamente a quanto visto nel caso affine, le varietà proiettive sono gli insiemi chiusi per la topologia di Zariski su $\mathbf{P}^n(K)$ (la dimostrazione che soddisfano agli assiomi per gli insiemi chiusi é analoga a quella vista nella §6).

$\mathbf{P}^n(K)$ è ricoperto da $n+1$ aperti affini standard $U_i := \{x \in P^n | x_i \neq 0\}$ ciascuno dei quali è isomorfo a K^n. Se $V = V(f_1, \ldots, f_p)$ è una varietà proiettiva allora $V \cap U_i$ è la varietà affine $V(g_1, \ldots, g_p) \subset U_i$ dove $g_j(y_0, \ldots, \hat{y_i}, \ldots, y_n) = f_j(y_0, \ldots, 1, \ldots, y_n)$

Proposizione 12.5. *Se I è un ideale omogeneo allora $\sqrt{I}$ è un ideale omogeneo.*

Dimostrazione Sia f un elemento di $\sqrt{I}$. Per il lemma 12.4 è sufficiente provare che tutte le sue componenti omogenee appartengono ancora a $\sqrt{I}$.

Infatti sia $f = \sum f_i$ e sia f_{max} la componente omogenea di grado massimo. Abbiamo per definizione che $\exists\ n$ tale che $f^n \in I$. Siccome I è omogeneo per il lemma 12.4 $(f^n)_{max} \in I$. È facile verificare che $(f^n)_{max} = (f_{max})^n$ e quindi $f_{max} \in \sqrt{I}$. Si può ripetere il ragionamento per $f - f_{max}$ provando così che tutte le componenti omogenee di f appartengono a $\sqrt{I}$.

Se $V = V(I) \subset \mathbf{P}^n(K)$ è una varietà proiettiva allora è definito il cono affine $C_V = \{x \in K^{n+1} | f(x) = 0 \quad \forall f \in I\}$. C_V è un cono per l'origine perché se $x \in C_V$ allora $\lambda x \in C_V\ \forall \lambda \in K$. In particolare C_V è un insieme finito se e solo se C_V coincide con l'origine. Questo può essere espresso nel modo seguente:

$$V \subset P^n(K) \text{ è vuota} \iff C_V \text{ è finito} \tag{12.2}$$

Se V è una varietà proiettiva allora

$$I(V) := \{f \in K[x_0, \ldots, x_n] | f(a_0, \ldots, a_n) = 0 \quad \forall \quad \text{n-pla di coord. omogenee} \quad (a_0, \ldots, a_n) \in V\}$$

Lemma 12.6. *Se K è un campo infinito e $V \subset \mathbf{P}^n(K)$ è una varietà proiettiva allora $I(V)$ è un ideale omogeneo.*

Dimostrazione Sia $f \in I(V)$. Allora per ogni $(a_0, \ldots, a_n) \in V$ e per ogni $\lambda \in K$ abbiamo $f(\lambda a_0, \ldots, \lambda a_n) = 0$. Se $f = \sum f_i$ (decomposizione nelle componenti omogenee) l'equazione precedente diventa $\sum \lambda^i f_i(a_0, \ldots, a_n) = 0 \quad \forall \lambda \in K$. Dal principio di identità dei polinomi segue $f_i(a_0, \ldots, a_n) = 0\ \forall i$ e quindi $f_i \in I(V)$ c.v.d.

Se $V \subset \mathbf{P}^n(K)$ é una varietá proiettiva, l'anello graduato $K[x_0, \ldots, x_n]/I(V)$ si dice l'anello delle coordinate omogeneo di V.

Nella parte restante di questa sezione studieremo le relazioni tra ideali omogenei e varietà proiettive. Occorre osservare subito che il Nullstellensatz debole non si estende parola per parola al caso proiettivo. Infatti $K[x_0, \ldots, x_n]$ contiene l'ideale massimale omogeneo $\mathcal{M} = (x_0, \ldots, x_n)$ per cui $V(\mathcal{M}) = \emptyset$ (mentre per il Nullstellensatz debole affine se $I \neq K[x_0, \ldots, x_n]$ allora $V(I) \neq \emptyset$). Considerazioni analoghe possono essere fatte per il Nullstellensatz forte. Fortunatamente i casi patologici sono tutti della stessa natura di questo. L'ideale $\mathcal{M}$ assume un ruolo speciale nella teoria delle varietà proiettive ed è chiamato col nome di ideale massimale irrilevante.

Queste considerazioni portano a denotare con simboli diversi gli ideali associati a varietà proiettive o affini. Quando non é chiaro dal contesto scriviamo $V_a(I)$ per denotare la varietà affine associata a I e $I_a(V)$ per denotare l'ideale (generalmente non omogeneo) associato alla varietà affine V. Notiamo che se I è omogeneo allora $V_a(I) = C_V$ (cono).

Si ricava la seguente versione proiettiva del Nullstellensatz debole:

Teorema 12.7. *(Nullstellensatz debole proiettivo). Sia $V(I) \subset \mathbf{P}^n(K)$ una varietà proiettiva con K algebricamente chiuso. Allora*

$$V(I) = \emptyset \Longleftrightarrow \exists \quad r : (x_0, \ldots, x_n)^r = \mathcal{M}^r \subset I$$

Dimostrazione

$\Longrightarrow$ Per ipotesi $V_a(I) = C_V$ coincide con l'origine O. Quindi per il Nullstellensatz forte affine $\sqrt{I} = I_a(V_a(I)) = I_a(O) = \mathcal{M}$. In particolare esiste N tale che $x_i^N \in I \quad \forall i$ e quindi $\mathcal{M}^{N(n+1)} \subset I$.

$\Longleftarrow$ Per ipotesi $x_i^r \in I$, quindi $C_V = V_a(I)$ coincide con l'origine e pertanto $V(I) = \emptyset$

Teorema 12.8. *(Nullstellensatz proiettivo) Sia I un ideale omogeneo in $K[x_0, \ldots, x_n]$ con K algebricamente chiuso. Se $\mathbf{P}^n(K) \supset V(I) \neq \emptyset$ allora*

$$I(V(I)) = \sqrt{I}$$

Dimostrazione Affermiamo che $I_a(V_a(I)) = I(V(I))$. Infatti se $f \in I_a(V_a(I))$ e $x \in V(I)$ allora ogni espressione di x in coordinate omogenee appartiene a $V_a(I)$ e quindi f si annulla su tutte le coordinate omogenee di x. Pertanto $f \in I(V(I))$. Viceversa sia $f \in I(V(I))$. Se $0 \neq x \in V_a(I)$ allora x dà coordinate omogenee per un punto di $V(I)$ e quindi $f(x) = 0$. Rimane da provare che f si annulla nell'origine. Siccome $I(V(I))$ è omogeneo, la componente di f di grado zero f_0 deve appartenere ancora a $I(V(I))$ e quindi f_0 si deve annullare su $V(I)$. Per ipotesi $V(I) \neq \emptyset$ e quindi $f_0 = 0$.

Quindi usando la versione affine 6.10 abbiamo $\sqrt{I} = I_a(V_a(I)) = I(V(I))$, c.v.d.

Osservazione. *Il lettore interessato può ripercorrere i passi dell'algoritmo di divisione e verificare che quando si divide un polinomio omogeneo f per dei polinomi omogenei $f_1, \ldots, f_r$ si ottiene $f = \sum a_i f_i + r$ dove i quozienti a_i ed il resto r sono ancora polinomi omogenei. In particolare se $r \neq 0$ allora $deg\ r = deg\ f$. Se f e g sono omogenei allora la S-coppia $S(f, g)$ è omogenea. Analizzando l'algoritmo di Buchberger, segue che un ideale omogeneo ha una base di base di Groebner formata da polinomi omogenei.*

Esercizio. *Sia I un ideale omogeneo in $K[x_0, \ldots, x_n]$. Provare che I è primo se e solo se $V(I) \subset \mathbf{P}^n$ è irriducibile.*

Vediamo adesso la relazione tra una varietà affine e la sua chiusura proiettiva. Lo spazio affine K^n con coordinate $(x_1, \ldots, x_n)$ può essere completato con un "iperpiano all'∞" ed immerso come aperto in $\mathbf{P}^n(K)$ con coordinate omogenee $(x_0, \ldots, x_n)$

Definizione 12.9. *Sia g un polinomio in $K[x_1, \ldots, x_n]$ di grado d. Allora*

$$g^h := x_0^d g(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$$

è un polinomio omogeneo in $K[x_0, \ldots, x_n]$ ancora di grado d che si dice l'omogeneizzato di g.

Esempio. *Se $g = x_1 + x_2 x_3 + 5x_2^2 x_3$ allora $g^h = x_0^2 x_1 + x_0 x_2 x_3 + 5x_2^2 x_3$.*

Lemma 12.10.

i) $g^h(1, x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$ *cioè deomogeneizzando si riottiene* g

ii) Sia $F(x_0, \ldots, x_n)$ *un polinomio omogeneo e sia* x_0^e *la massima potenza di* x_0 *che divide* F. *Se* $f = F(1, x_1, \ldots, x_n)$ *è la deomogeneizzazione di* F *allora* $F = x_0^e \cdot f^h$.

iii) $(g^h)^m = (g^m)^h$ *per ogni* $m \in \mathbf{N}$.

Dimostrazione i) e iii) sono evidenti dalle definizioni. Per provare ii) osserviamo che f ha grado $d - e$ e quindi $f^h = x_0^{d-e} F(1, \frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) = x_0^{-e} F(x_0, x_1, \ldots, x_n)$.

Definizione 12.11. *Sia* I *un ideale in* $K[x_1, \ldots, x_n]$. *Definiamo*

$$I^h := < f^h | f \in I > \subset K[x_0, \ldots, x_n]$$

I^h è un ideale omogeneo.

Osservazione. *Se* $f_1, \ldots, f_p$ *generano* I *allora può essere* $(f_1^h, \ldots, f_p^h) \subset_{\neq} I^h$. *Ad esempio consideriamo* $I(C) = (f_1, f_2) = (x_2 - x_1^2, x_3 - x_1^3) \subset \mathbf{R}[x_1, x_2, x_3]$ *ideale della cubica gobba (si veda l'esempio 5.6). Allora* $(f_1^h, f_2^h) = (x_2 x_0 - x_1^2, x_3 x_0^2 - x_1^3)$. *Abbiamo* $(f_2 - x_1 f_1)^h = (x_3 - x_1 x_2)^h = x_0 x_3 - x_1 x_2 \in I^h$ *ma l'ultimo polinomio non è combinazione di* f_1^h *e* f_2^h *(basta guardare i gradi).*

Teorema 12.12. *Sia* I *un ideale di* $K[x_1, \ldots, x_n]$ *e sia* $G = \{g_1, \ldots, g_s\}$ *una base di Gröbner di* I *rispetto ad un ordine monomiale graduato. Allora* $G^h = \{g_1^h, \ldots, g_s^h\}$ *genera* I^h.

Dimostrazione Proveremo l'enunciato più forte che G^h è una base di Gröbner per I^h rispetto ad un conveniente ordine monomiale in $K[x_0, \ldots, x_n]$ che andiamo a definire. Ogni monomio in $K[x_0, \ldots, x_n]$ si può scrivere come $x_1^{\alpha_1} \ldots x_n^{\alpha_n} x_0^d = x^\alpha x_0^d$. Allora possiamo estendere l'ordine graduato $>$ ad un ordine $>_h$ in $K[x_0, \ldots, x_n]$ dato da

$$x^\alpha x_0^d >_h x^\beta x_0^e \Longleftrightarrow x^\alpha > x^\beta \text{oppure } x^\alpha = x^\beta \text{e } d > e$$

È facile verificare che $>_h$ è un ordine monomiale e che $LM_{>_h}(f^h) = LM_>(f) \quad \forall f \in K[x_1, \ldots, x_n]$ (infatti x_0 è minore rispetto a $>_h$ di qualunque polinomio in $x_1, \ldots, x_n$ e quindi $LM_{>_h}(f^h)$ non contiene x_0 ed è un monomio che appariva già in f).

Dobbiamo provare che $< LT_{>_h}(I^h) >$ è generato da $LT_{>_h}(G^h)$. Infatti sia $F \in I^h$. Abbiamo $F = \sum a_j f_j^h$ con $f_j \in I$. Allora

$$f := F(1, x_1, \ldots, a_n) = \sum a'_j f_j^h(1, x_1, \ldots, x_n) = \sum a'_j f_j \in I$$

(l'ultima uguaglianza per il lemma 12.10) Adesso sempre dal lemma 12.10 abbiamo $F = x_0^e \cdot f^h$ e quindi

$$LM_{>_h}(F) = x_0^e \cdot LM_{>_h}(f^h) = x_0^e \cdot LM_>(f)$$

Siccome G è una base di Gröbner per I $LM_>(f)$ è un multiplo di qualche $LM_>(g_i) = LM_{>_h}(g_i^h)$ e quindi anche $LM_{>_h}(F)$ è un multiplo di qualche $LM_{>_h}(g_i^h)$ c.v.d.

Confrontando il teorema 12.12 con l'osservazione che lo precede e con l'esempio 5.4 il lettore può notare che $(x_2 - x_1^2, x_3 - x_1^3)$ è una base di Gröbner per l'ideale della cubica gobba $I(C)$ con LEX ma non può esserlo per un ordine graduato.

I comandi di CoCoA relativi all'omogeneizzazione sono $Homog(x, F)$ dove F é un polinomio e $Homog(x, I)$ dove I é un ideale (quest'ultimo comando é basato sul teor. 12.12).

Definizione 12.13. *Se $W \subset K^n$ allora la chiusura proiettiva $\overline{W}$ è la chiusura di W nella topologia di Zariski di $\mathbf{P}^n(K)$.*

Teorema 12.14. *Sia $W \subset K^n$ una varietà affine. Allora*

$$\overline{W} = V(I_a(W)^h)$$

Dimostrazione

$\subset$ Proviamo che $W \subset V(I_a(W)^h)$. Infatti se $x \in W$ e $f \in I_a(W)$ abbiamo $f(x) = 0$ da cui $f^h(x) = 0$ e quindi tutti i polinomi di $I_a(W)^h$ si annullano su x. La tesi segue prendendo la chiusura di ambo i membri.

$\supset$ Sia $\overline{W} = V(F_1, \ldots, F_s)$. Ogni F_i si annulla su $\overline{W}$ e quindi $f_i = F_i(1, x_1, \ldots, x_n)$ si annulla su W. Pertanto $f_i \in I_a(W)$ da cui $f_i^h \in I_a(W)^h$. Abbiamo $F_i =$ (vedi 12.10) $x_0^{e_i} f_i^h \in I_a(W)^h$ e quindi $(F_1, \ldots, F_s) \subset I_a(W)^h$ e prendendo V di ambo i membri si ha la tesi.

Teorema 12.15. *Sia K un campo algebricamente chiuso e sia $I \subset K[x_1, \ldots, x_n]$ un ideale. Allora*

$$\overline{V_a(I)} = V(I^h) \subset \mathbf{P}^n(K)$$

Dimostrazione

$\subset$ $V_a(I) \subset$ (dall'analoga inclusione del teorema precedente) $V(I_a(V_a(I))^h) =$ (dal Nullstellensatz) $V((\sqrt{I})^h) \subset V(I^h)$

$\supset$ Sia $\overline{V_a(I)} = V(F_1, \ldots, F_s)$. Come nell'analoga inclusione del teorema precedente abbiamo $(F_1, \ldots, F_s) \subset I_a(V_a(I))^h$. Per il Nullstellensatz l'ultimo ideale è uguale a $(\sqrt{I})^h$ ed è facile verificare che a sua volta questo ideale è incluso in $\sqrt{I^h}$ (occorre usare il lemma 12.10 iii). Pertanto $(F_1, \ldots, F_s) \subset \sqrt{I^h}$ e prendendo V di ambo i membri si ottiene $\overline{V_a(I)} \supset V(\sqrt{I^h}) = V(I^h)$ c.v.d.

Dai teoremi 12.15 e 12.12 si ottiene l'algoritmo per calcolare la chiusura proiettiva di una varietà affine su un campo algebricamente chiuso. Si procede nel modo seguente:

Se $W = V(I)$ è una varietà affine si calcola una base di Gröbner G di I rispetto ad un ordine graduato. Allora $\overline{W}$ è definita in $\mathbf{P}^n(K)$ da G^h.

Osservazione. *Il teorema 12.15 è falso su $\mathbf{R}$. Ad esempio se $I = (x_1^2 + x_2^4) \subset \mathbf{R}[x, y]$ allora $V_a(I) \subset \mathbf{R}^2$ consiste solo dell'origine e quindi la sua chiusura proiettiva è data dal punto di coordinate omogenee $(1, 0, 0) \subset \mathbf{P}^2(\mathbf{R})$. D'altronde $V(I^h) = V(x_0^2 x_1^2 + x_2^4) = (1, 0, 0) \cup (0, 1, 0)$.*

12.16 Algoritmo di consistenza nel proiettivo. *Sia fissato un ordine monomiale. Sia I un ideale omogeneo in $K[x_0, \ldots, x_n]$ e sia K algebricamente chiuso. Vale*

$$V(I) = \emptyset \quad \Leftrightarrow \quad \forall i \quad \exists n_i \quad | \quad x_i^{n_i} \in LT(I)$$

Dimostrazione

$\Rightarrow$ Per il teorema 12.7 $\exists r$ tale che $\mathcal{M}^r \subset I$ e quindi $\forall i \quad x_i^r \in I$ da cui $x_i^r 0 LT(x_i^r) \in LT(I)$.

$\Leftarrow$ Posto $N = max\{n_i\}$ abbiamo $\mathcal{M}^{N(n+1)} \subset I$ e quindi tutti i monomi di grado $\geq N(n+1)$ appartengono a $LT(I)$ e $S = \{x^\alpha | x^\alpha \notin LT(I)\}$ é un insieme finito di monomi. Definiamo S_K come lo spazio vettoriale su K formato dalle combinazioni lineari degli elementi di S a coefficienti in K. Quindi S_K é un sottospazio di $K[x_0, \ldots, x_n]$ di dimensione finita. Definiamo adesso l'applicazione

$$\phi: K[x_0, \ldots, x_n]/I \to S_K$$

$$\phi(f) := f mod I$$

ϕ é ben definita perché se $f - f' \in I$ allora $(f - f')\ mod\ I = 0$ (corollario 2.13). Inoltre dal teorema 2.11 segue che se r é il resto della divisione di f per una base di Gröbner di I e r' é il resto di f' allora $r + r'$ é il resto di $f + f'$. Quindi ϕ é un'applicazione lineare. ϕ é iniettiva perché se $(f - f')\ mod\ I = 0$ allora $f - f' \in I$ (ancora per il corolario 2.13). Pertanto $K[x_0, \ldots, x_n]/I$ é isomorfo ad un sottospazio di S_K ed ha anch'esso dimensione finita. Pertanto considerando le classi modulo I

$$[1], [x_i], [x_i^2], \ldots$$

queste devono essere linearmente dipendenti, cioé devono esistere delle costanti $c_j \in K$, $c_j \neq 0$ tali che $\sum c_j x_i^{d_j} \in I$. Siccome I é omogeneo segue che $x_i^{d_i} \in I$ per qualche d_i. Quindi $C_V = V_a(I)$ é contenuto nell'origine ed abbiamo $V(I) = \emptyset$.

L'algoritmo precedente puó essere pensato come una versione costruttiva del Nullstellensatz debole proiettivo (teor. 12.7). Infatti i generatori di $LT(I)$ possono essere calcolati facilmente da una base di Gröbner di I.

Dato un ideale omogeneo $I \subset K[x_0, \ldots, x_n]$, con CoCoA si puó verificare se la varietá $V(I) \subset \mathbf{P}^n$ é vuota con il comando $LeadingTerm(I)$ che fornisce una base minimale per $LT(I)$.

Definizione 12.17. *Un morfismo razionale tra due varietà proiettive irriducibili $X \subset \mathbf{P}^n$ e $Y \subset \mathbf{P}^m$ è un morfismo razionale tra due convenienti parti affini $X \cap K^n$ e $Y \cap K^m$.*

I morfismi razionali sono espressi in coordinate da polinomi omogenei tutti dello stesso grado.

Spieghiamo nei dettagli questa affermazione. In un conveniente sistema di coordinate abbiamo $(z_1, \ldots, z_n)$ coordinate su K^n e $(x_0, \ldots, x_n)$ coordinate omogenee su $\mathbf{P}^n \supset X$. Analogamente siano $(w_1, \ldots, w_m)$ coordinate su K^m e $(y_0, \ldots, y_m)$ coordinate omogenee su $\mathbf{P}^m \supset Y$. Allora un morfismo razionale f da X a Y si esprime in coordinate come

$$\left(\frac{f_1(z_1, \ldots, z_n)}{g_1(z_1, \ldots, z_n)}, \ldots, \frac{f_m(z_1, \ldots, z_n)}{g_m(z_1, \ldots, z_n)}\right) = \left(\frac{f_1(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})}{g_1(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})}, \ldots, \frac{f_m(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})}{g_m(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})}\right) =$$

$$= \left(\frac{\tilde{f}_1(x_0, \ldots, x_n)}{\tilde{g}_1(x_0, \ldots, x_n)}, \ldots, \frac{f_m(x_0, \ldots, x_n)}{g_m(x_0, \ldots, x_n)}\right)$$

dove $deg\ \tilde{f}_i = deg\ \tilde{g}_i$. Riducendo a denominatore comune si ha

$$\left(\frac{h_1(x_0,\ldots,x_n)}{g(x_0,\ldots,x_n)},\ldots,\frac{h_m(x_0,\ldots,x_n)}{g(x_0,\ldots,x_n)}\right)$$

con $deg\ h_i = deg\ g$ e passando a coordinate omogenee l'ultima espressione diventa

$$(g(x_0,\ldots,x_n),h_1(x_0,\ldots,x_n),\ldots,h_m(x_0,\ldots,x_n))$$

L'ultima espressione é infatti formata da polinomi omogenei tutti dello stesso grado.

Esempio. *$\phi\colon \mathbf{P}^2 - - \to \mathbf{P}^2$ definito da $\phi(x_0,x_1,x_2) = (x_1x_2, x_0x_2, x_0x_1)$ è un morfismo razionale definito su tutto $\mathbf{P}^2$ escluso i tre punti di coordinate $(1,0,0)$, $(0,1,0)$, $(0,0,1)$. È interessante verificare che $\phi^2(x_0,x_1,x_2) = x_0x_1x_2(x_0,x_1,x_2)$ e quindi ϕ è un morfismo birazionale tale che $\phi^{-1} = \phi$. Una rappresentazione equivalente di ϕ è la seguente: $\phi(x_0,x_1,x_2) = (\frac{1}{x_0},\frac{1}{x_1},\frac{1}{x_2})$. ϕ è un esempio di trasformazione quadratica, cioè può essere rappresentata da polinomi di grado 2. Un teorema classico di Cremona afferma che il gruppo dei morfismi birazionali di $\mathbf{P}^2$ è generato dalle trasformazioni quadratiche.*

Esempio 12.18(la proiezione da un punto). *Se $P \in \mathbf{P}^n$ ha coordinate $(0,\ldots,0,1)$ allora la proiezione da P sull'iperpiano $\mathbf{P}^{n-1}$ definito da $x_n = 0$ è data da*

$$\pi_P\colon \mathbf{P}^n \setminus P \to \mathbf{P}^{n-1}$$

$$\pi_P(x_0,\ldots,x_n) = (x_0,\ldots,x_{n-1})$$

La proiezione da P può essere considerata come morfismo razionale $\pi_P\colon \mathbf{P}^n - - \to \mathbf{P}^{n-1}$.

Definizione 12.19. *Siano $X \subset \mathbf{P}^n$ e $Y \subset \mathbf{P}^m$ due varietá proiettive. Una funzione $f\colon X \to Y$ si dice un morfismo regolare in $x' \in X$ se esiste un intorno aperto U di x' e polinomi omogenei $f_0,\ldots,f_m$ dello stesso grado tali che $\forall x \in U$ abbiamo $(f_0(x),\ldots,f_m(x)) = f(x)$*

In particolare deve esistere j tale che $f_j(x') \neq 0$.

Definizione 12.20. *Una funzione $f\colon X \to Y$ si dice un morfismo regolare se é regolare $\forall x \in X$.*

In particolare un morfismo razionale puó essere visto come un morfismo regolare in almeno un punto (e quindi in un aperto). Un morfismo razionale regolare in tutti i punti é un morfismo regolare.

Osservazione importante. *Una collezione di polinomi omogenei tutti dello stesso grado $f_0,\ldots,f_m$ con $f_i \in K[x_0,\ldots,x_n]$ che non si annullano contemporaneamente su $X \subset \mathbf{P}^n$ definisce un morfismo regolare da X a $\mathbf{P}^m$. Esistono peró morfismi regolari che <u>non</u> si possono definire in questo modo (si veda l'esempio seguente).*

Esempio 12.21. *Sia X é la conica in $\mathbf{P}^2$ definita da $x^2+y^2-z^2$ ((x,y,z) coordinate omogenee) allora la proiezione stereografica $p\colon X \to \mathbf{P}^1$ é definita su $X \setminus \{(0,1,1)\}$ da*

$p(x,y,z) = (x, y-z)$ *mentre é definita su* $X \setminus \{(0,1,-1)\}$ *da* $p(x,y,z) = (y+z, -x)$. *Il lettore dovrebbe verificare che la definizione é ben posta nell'intersezione.*

Analogamente al caso affine, possiamo definire due varietá proiettive V e W isomorfe se esistono due morfismi regolari $f: V \to W$ e $g: W \to V$ tali che $f \circ g = 1_W$ e $g \circ f = 1_V$. L'isomorfismo di K-algebre $K[V] \simeq K[W]$ é equivalente all'isomorfismo tra i coni affini C_V e C_W, che a sua volta implica che V e W sono isomorfe. Non vale peró il viceversa, ad esempio una conica nonsingolare ed una retta (proiettive) sono isomorfe ma i loro coni affini non lo sono. Pertanto il teorema 11.6 non si estende al caso proiettivo.

L'isomorfismo tra K-algebre graduate $K[V]$ e $K[W]$ é equivalente ad un fatto molto piú forte, vale a dire che esiste $\alpha: \mathbf{P}^n \to \mathbf{P}^n$ proiettivitá tale che $\alpha(V) = W$. Due varietá siffatte si dicono proiettivamente isomorfe.

Se V é una varietá proiettiva, si puó definire $K(V)$ campo delle frazioni graduato di $K[V]$, che contiene solo elementi del tipo $\frac{[f]}{[g]}$ con $deg\ f = deg\ g$. Gli elementi di $K(V)$ si possono identificare con i morfismi razionali $V - - \to K$ od anche con i morfismi razionali $V - - \to \mathbf{P}^1$. Vale che $K(V)$ é isomorfo al campo delle funzioni di una sua parte affine, cioé a $K(V \cap K^n)$. In particolare V e W varietá proiettive sono birazionalmente equivalenti se e solo se $K(V) \simeq K(W)$ come estensioni di K (in analogia con il teorema 11.20).

13. CURVE PIANE

Studiamo brevemente le varietá date da una singola equazione in K^2 (curve piane affini) o in $P^2(K)$ (curve piane proiettive). In questo paragrafo supporremo sempre K algebricamente chiuso. Questo per il

Lemma 13.1. *Sia* $f \in K[x,y]$ *e sia* $C = V(f) \subset K^2$ *una curva piana affine. Se* K *é algebricamente chiuso allora* C *consiste di infiniti punti.*

Dimostrazione Ricordiamo che ogni campo algebricamente chiuso K ha infiniti elementi. (infatti se $K = \{k_1, \ldots k_p\}$ il polinomio $p(x) = \prod_{i=1}^{p}(x - k_i) + 1$ non avrebbe radici in K.) Se f dipende solo da x allora per ogni radice x_0 di f tutti i punti $(x_0, y) \quad \forall y \in K$ appartengono a C. Se f ha grado positivo in y allora $\forall x' \in K$ l'equazione $f(x', y) = 0$ ha almeno una soluzione e quindi esistono infiniti punti su C.

Esempio. *Se* $f = x^2 + y^2 \in \mathbf{R}[x,y]$ *allora* $V(f) \subset \mathbf{R}^2$ *consiste di un solo punto. Quindi l'ipotesi che* K *sia algebricamente chiuso é necessaria nel lemma 13.1.*

Proposizione 13.2. *Sia* $f \in K[x,y]$ *e sia* $C = V(f) \subset K^2$ *una curva affine. Allora* $V(f^h) \subset \mathbf{P}^2(K)$ *é la chiusura proiettiva di* C.

Dimostrazione Dalla definizione segue che se $I = (f)$ allora $I^h = (f^h)$. La tesi segue allora dal teorema 12.15 .

Lemma 13.3. *Sia $f \in K[x,y]$. $V(f) \subset K^2$ é irriducibile se e solo se f é irriducibile.*

Dimostrazione Per il teorema 6.12 $V(f)$ é irriducibile se e solo se $I(V(f))$ é primo. Per il teorema degli zeri di Hilbert 6.10 $I(V(f)) = \sqrt{(f)}$. Se $f = f_1^{a_1} \cdots f_k^{a_k}$ é la decomposizione di f in polinomi irriducibili segue facilmente che $\sqrt{(f)} = (f_1 \cdots f_k)$. Quindi $V(f)$ é irriducibile se e solo se $(f_1 \cdots f_k)$ é primo. Abbiamo che $(f_1 \cdots f_k)$ é primo se solo se $f_1 \cdots f_k$ é irriducibile, cioé se e solo se f é irriducibile da cui la tesi.

Se $f = f_1^{a_1} \cdots f_k^{a_k}$ é la decomposizione di f in fattori irriducibili allora $V(f)$ é unione delle sue componenti irriducibili $V(f_i)$. Se poniamo

$$f_{rid} := f_1 \cdots f_k$$

allora evidentemente $V(f) = V(f_{rid})$ e $\sqrt{(f)} = (f_{rid})$.

Definizione 13.4. *Un polinomio f si dice ridotto se $f = f_{rid}$ cioé se f é irriducibile oppure contiene i suoi fattori irriducibili con molteplicitá 1.*

Lemma 13.5. *Sia $f \in K[x_1, \ldots, x_n]$ e sia car $K = 0$. Allora*

$$f_{rid} = \frac{f}{MCD(f, f_{x_1}, \ldots, f_{x_n})}$$

Dimostrazione Sia $f = f_1^{a_1} \cdots f_k^{a_k}$ la decomposizione di f in fattori irriducibili. É sufficiente provare che

$$MCD(f, f_{x_1}, \ldots, f_{x_n}) = f_1^{a_1 - 1} \cdots f_k^{a_k - 1}$$

Abbiamo

$$f_{x_i} = \sum_{j=1}^{k} a_j \frac{\partial f_j}{\partial x_i} f_1^{a_1} \cdots f_j^{a_j - 1} \cdots f_k^{a_k} = f_1^{a_1 - 1} \cdots f_k^{a_k - 1} \sum_{j=1}^{k} a_j \frac{\partial f_j}{\partial x_i} f_1 \cdots \hat{f}_k \cdots f_k \qquad (13.1)$$

Quindi $f_1^{a_1 - 1} \cdots f_k^{a_k - 1}$ divide f e tutte le sue derivate prime f_{x_i}. É facile verificare da (13.1) che $\forall j \quad f_j^{a_j}$ non divide tutte le derivate prime di f e quindi segue la tesi.

Nel resto di questo paragrafo consideriamo sempre curve $C = V(f)$ con f polinomio ridotto. Il lemma 13.5 mostra che possiamo sempre ricondurci a questo caso (almeno se car $K = 0$)

Lemma 13.6. *Sia $f \in K[x,y]$ di grado totale d. Allora l'intersezione di $V(f)$ con una retta che non é una sua componente irriducibile consiste al piú di d punti.*

Dimostrazione La retta puó essere parametrizzata da $x = x_0 + at$, $y = y_0 + bt$. Sostituendo abbiamo l'equazione $f(x_0 + at, y_0 + bt) = 0$ che é un polinomio non nullo di grado $\leq d$ nella variabile t e quindi ha al piú d radici.

Definizione 13.7. *Sia $P = (x_0, y_0)$ un punto di intersezione tra una retta L ed una curva $C = V(f) \subset K^2$. Sia L parametrizzata da $x = x_0 + at$, $y = y_0 + bt$, (in modo che P corrisponde al valore $t = 0$). La molteplicitá della radice $t = 0$ del polinomio $p(t) = f(x_0 + at, y_0 + bt)$ si dice molteplicitá di intersezione di L e C nel punto P.*

Studiamo ora come varia la molteplicitá di intersezione tra una curva C ed una retta L in un punto $P \in C$ al variare di L tra le rette passanti per P. Se $P = (x_0, y_0)$ abbiamo che $f(x_0, y_0) = 0$ e L é parametrizzata da $x = x_0 + at$, $y = y_0 + bt$ al variare di $(a, b) \in \mathbf{P}^1$.

Consideriamo lo sviluppo di Taylor

$$f(x_0+at, y_0+bt) = f(x_0, y_0)+[f_x(x_0, y_0)a + f_y(x_0, y_0)b]\, t+\ldots (\text{termini di grado superiore in } t) \tag{13.2}$$

Ne segue che

i) Se $f_x(x_0, y_0) = f_y(x_0, y_0) = 0$ allora tutte le rette per P hanno molteplicitá di intersezione ≥ 2 con C in P .

ii) Se $(f_x(x_0, y_0), f_y(x_0, y_0)) \neq (0, 0)$ allora la molteplicitá di intersezione della retta L é 1 se $[f_x(x_0, y_0)a + f_y(x_0, y_0)b] \neq 0$ mentre é ≥ 2 se $[f_x(x_0, y_0)a + f_y(x_0, y_0)b] = 0$.

Notiamo che l'equazione $[f_x(x_0, y_0)a + f_y(x_0, y_0)b] = 0$ é risolta da $a = f_y(x_0, y_0)$ e $b = -f_x(x_0, y_0)$. Eliminando il parametro la retta corrispondente ha equazione

$$f_x(x_0, y_0)(x - x_0) + f_y(x_0, y_0)(y - y_0) = 0$$

Questa osservazione motiva le seguenti

Definizione 13.8. *Un punto $P \in C = V(f)$ curva piana affine si dice singolare se $f_x(P) = f_y(P) = 0$. Altrimenti P si dice nonsingolare. Una curva si dice nonsingolare (o liscia) se tutti i suoi punti sono nonsingolari.*

Definizione 13.9. *In un punto $P = (x_0, y_0) \in C = V(f)$ nonsingolare la retta di equazione*

$$f_x(x_0, y_0)(x - x_0) + f_y(x_0, y_0)(y - y_0) = 0$$

si dice la retta tangente.

Algoritmo per la nonsingolaritá di una curva. *Sia K algebricamente chiuso. Una curva $C = V(f)$ é nonsingolare se e solo se $V(f, f_x, f_y) = \emptyset$, ovvero (dal teorema degli zeri di Hilbert) se e solo se $(f, f_x, f_y) = (1)$. Quest'ultima condizione puó essere verificata calcolando una base di Gröbner dell'ideale (f, f_x, f_y).*

Definizione 13.10. *Un punto $p \in V(f)$ si dice di molteplicitá r se tutte le derivate parziali di f di ordine $\leq r - 1$ si annullano in P e se esiste una derivata parziale di ordine r non nulla in P. Un punto di molteplicitá $2, 3, \ldots$ si dice anche doppio, triplo, ...*

I punti nonsingolari corrispondono ai punti di molteplicitá 1. Calcolando i termini successivi dello sviluppo di Taylor (13.2), otteniamo che in un punto P di molteplicitá r

tutte le rette per P incontrano C con molteplicitá di intersezione in $P = r$ escluso un numero finito, dato dalle soluzioni in (a, b) di

$$\sum_{i=0}^{r} \binom{r}{i} \frac{\partial f}{\partial^{r-i} x \partial^i y}(P) a^{r-i} b^i = 0 \tag{13.3}$$

Le rette appena menzionate possono essere considerate come rette tangenti in P.

Definizione 13.11. *Un punto singolare di molteplicitá $r(\geq 2)$ si dice ordinario se ha esattamente r tangenti distinte, cioé se il discriminante del polinomio in (13.3) é non nullo.*

Esempi. *La curva $V(y^2 - x^2(x+1))$ ha un punto doppio ordinario nell'origine. La curva $V(y^2 - x^3)$ ha un punto doppio non ordinario nell'origine, che si dice cuspide. La curva $V(x^4 - x^2 + y^2)$ (il cui grafico reale é un "otto") ha un punto doppio ordinario nell'origine.*

Teorema 13.12 Forma debole del Teorema di Bezout. *Siano $C = V(f)$ e $D = V(g)$ due curve senza componenti comuni con f, g di gradi rispettivamente d, e. Allora $C \cap D$ consiste al piú in de punti.*

Dimostrazione Se uno dei due polinomi f, g dipende solo da x o solo da y allora la curva corrispondente é data da una unione di rette, ed in questo caso il risultato é evidente. Altrimenti le coordinate dei punti di intersezione devono soddisfare le due equazioni non nulle $Res(f, g, x) = 0$ (in y) e $Res(f, g, y) = 0$ (in x) e quindi i punti di intersezione sono in numero finito che denotiamo con $\{P_1, \ldots, P_k\}$. Sia L_{ij} la retta per P_i e P_j. Per valutare il numero dei punti conviene scegliere un nuovo sistema di coordinate (con un cambiamento affine) dove gli assi coordinati non sono paralleli alle rette L_{ij} per $1 \leq i < j \leq k$. Osserviamo che un cambiamento di coordinate affine non altera i gradi dei polinomi, che chiamiamo ancora con f e g. Adesso per ogni radice x_i del polinomio $Res(f, g, y)$ esiste al piú un valore y_i tale che $(x_i, y_i) \in C \cap D$. Quindi é sufficiente osservare che il grado di $Res(f, g, y)$ é $\leq de$. Infatti scriviamo $f = \sum_{i=0}^{d} a_i(x) y^{d-i}$ e $g = \sum_{j=0}^{e} b_j(x) y^{e-j}$ con $deg\ a_i \leq i$ e $deg\ b_j \leq j$ e calcoliamo

$$\det \begin{vmatrix}
a_0 & a_1 & \ldots & a_d & & & & & \\
 & a_0 & \ddots & & \ddots & & & & \\
 & & \ddots & \ddots & & \ddots & & & \\
 & & & a_0 & a_1 & \ldots & a_d & & \\
b_0 & b_1 & \ldots & \ldots & b_e & & & & \\
 & b_0 & \ddots & & & \ddots & & & \\
 & & \ddots & \ddots & & & \ddots & & \\
 & & & \ddots & \ddots & & & \ddots & \\
 & & & & b_0 & b_1 & & & b_e
\end{vmatrix}$$

Il determinante é una somma di tanti monomi in $a_i(y)$ e $b_j(y)$. Il monomio corrispondente alla diagonale é di grado $\leq de$. Tutti gli altri monomi si ottengono con permutazioni da questo ed é facile vedere che il grado rimane $\leq de$ (conviene pensare di riempire i coefficienti nulli con $a_{-1}, a_{-2}, \ldots a_{d+1}, a_{d+2}, \ldots$ in modo che i gradi siano sempre crescenti di una unitá andando verso destra).

Definizione 13.13. *Un punto $P \in V(f) = C$ nonsingolare si dice un flesso se la tangente in P ha molteplicitá di intersezione ≥ 3 con C in P.*

Esempi. *(é istruttivo negli esempi seguenti disegnare il grafico reale)*

i) L'origine é un flesso per la curva $y - x^3 = 0$.

ii) La curva

$$2x^4 - 3x^2y + y^2 - 2y^3 + y^4 = 0$$

ha molteplicitá 2 nell'origine. La molteplicitá di intersezione della tangente (generalizzata) $y = 0$ nell'origine é 4. L'origine si dice un tacnodo.

iii) La curva

$$(x^2 + y^2)^2 + 3x^2y - y^3 = 0$$

ha un punto triplo ordinario nell'origine.

iv) La curva

$$(x^2 + y^2)^3 - 4x^2y^2 = 0$$

("quadrifoglio") ha un punto quadruplo non ordinario nell'origine.

Proposizione 13.14. *Un punto P nonsingolare per $V(f)$ é un flesso se e solo se*

$$det \begin{vmatrix} 0 & f_x & f_y \\ f_x & f_{xx} & f_{xy} \\ f_y & f_{xy} & f_{yy} \end{vmatrix} = 0 \tag{13.4}$$

Dimostrazione Sostituendo $(a, b) = (-f_y, f_x)$ all'equazione (13.3) $af_{xx} + 2abf_{xy} + b^2 f_{yy} = 0$ si ottiene esattamente la (13.4).

Osservazione. *Una curva differenziabile in $\mathbf{R}^2$ di equazione implicita $f(x, y) = 0$ ha curvatura nei punti nonsingolari uguale a*

$$k = \pm \frac{det \begin{vmatrix} 0 & f_x & f_y \\ f_x & f_{xx} & f_{xy} \\ f_y & f_{xy} & f_{yy} \end{vmatrix}}{(f_x^2 + f_y^2)^{3/2}}$$

Pertanto i punti di flesso corrispondono ai punti di curvatura nulla.

Sia ora $F \in K[x, y, z]$ un polinomio omogeneo. Consideriamo la curva proiettiva $V(F) \subset \mathbf{P}^2$ che ha parte affine definita da $f(x, y) = F(x, y, 1)$.

Possiamo definire un punto $P \in V(F)$ di molteplicitá r se per un aperto affine standard $K^2 \subset \mathbf{P}^2$ contenente P abbiamo che P é di molteplicitá r per la curva affine $V(F) \cap K^2$. Analogamente possiamo definire la molteplicitá di intersezione con una retta e la retta tangente. I punti singolari sono quelli di molteplicitá ≥ 2.

Lemma 13.15. *Un punto P é singolare per la curva $V(F) \subset \mathbf{P}^2$ se e solo se $F_x(P) = F_y(P) = F_z(P) = 0$.*

Dimostrazione La relazione di Eulero $(deg\ F)F = xF_x + yF_y + zF_z$ mostra che le equazioni $F_x(P) = F_y(P) = F_z(P) = 0$ implicano $F(P) = 0$. Sia $P = (x_0, y_0, z_0)$. Possiamo supporre (a meno di cambiare nome alle coordinate) che $z_0 \neq 0$. Allora poniamo $f(x, y) = F(x, y, 1)$, da cui $f_x = F_x$, $f_y = F_y$ e la tesi segue dalla definizione.

13.16 Algoritmo per la nonsingolaritá di una curva proiettiva. *Sia $C = V(F) \subset \mathbf{P}^2$ con F polinomio omogeneo in $K[x, y, z]$ e K algebricamente chiuso. Per verificare se C é nonsingolare si procede nel modo seguente:*

i) Si sostituisce F con F_{rid} mediante 13.5.

ii) Si calcola una base di Gröbner G per l'ideale generato da F_x, F_y, F_z.

iii) Si applica 12.16. Se esistono tre interi a, b, c tali che x^a, y^b e z^c appartengono a $LT(I)$ allora C é nonsingolare (e viceversa).

Esercizi.

a) *Verificare che la curva $x^2 + y^2 - 1 = 0$ é nonsingolare e la sua chiusura proiettiva rimane nonsingolare.*

b) *Verificare che la curva $y - x^3 = 0$ é nonsingolare mentre la sua chiusura proiettiva ha un punto singolare ("acquista una singolaritá all' infinito").*

c) *Per quali valori di $\lambda \in K$ la curva*

$$x^3 + y^3 + z^3 + 3\lambda xyz = 0$$

é nonsingolare in $\mathbf{P}^2(K)$? Soluzione: per $\lambda \neq -1, -\rho, -\rho^2$ (ρ radice cubica dell'unitá) e nei casi esclusi si spezza in 3 rette.

d) Per quali valori di $\lambda \in K$ la curva

$$x^3 + y^3 + z^3 + \lambda(x + y + z)^3 = 0$$

é nonsingolare in $\mathbf{P}^2(K)$? Soluzione: per $\lambda \neq -1/9, -1$.

Per curve proiettive la nonsingolaritá puó essere espressa anche attraverso alcuni "invarianti". Ad esempio é ben noto che la conica definita da $\sum_{i,j=0}^{2} a_{ij}x_ix_j$ con a_{ij} matrice simmetrica 3×3 é nonsingolare se e solo se $det\ a_{ij} \neq 0$. In generale una curva di grado d é nonsingolare se un certo polinomio omogeneo di grado $3(d-1)^2$ nei coefficienti della curva (detto discriminante) é $\neq 0$ (vedi F. Enriques, O. Chisini, Lezioni... III pag. 166).

Se F, $G \in K[x, y, z]$ sono due polinomi omogenei di gradi d, e allora vale l'analogo del teorema 13.12: il numero dei punti di intersezione é $\leq de$ (per dimostrarlo é sufficiente

prendere un piano affine che contiene tutti i punti di intersezione). In ambito proiettivo il teorema di Bezout si puó enunciare in modo piú preciso. Infatti si puó definire la molteplicitá di intersezione di due curve in un punto ed il numero dei punti di intersezione di $V(F)$ e $V(G)$ in $\mathbf{P}^2$ é dato esattamente da de se ogni punto é contato con la sua molteplicitá.

Gli esercizi seguenti estendono alcuni dei concetti precedenti al caso proiettivo.

Esercizio. *Provare che la retta tangente alla curva $F(x,y,z) \subset \mathbf{P}^2$ nel punto nonsingolare P é data da*

$$xF_x(P) + yF_y(P) + zF_z(P) = 0$$

Esercizio. *Sia K algebricamente chiuso. Provare che 2 curve piane in $\mathbf{P}^2(K)$ si incontrano almeno in un punto.*

Esercizio. *Provare che un punto nonsingolare $P \in V(F) \subset \mathbf{P}^2$ é un flesso se e solo se*

$$H(F) \quad = \quad det \begin{vmatrix} F_{xx} & F_{xy} & F_{xz} \\ F_{xy} & F_{yy} & F_{yz} \\ F_{xz} & F_{yz} & F_{zz} \end{vmatrix} \quad = \quad 0$$

Dedurre che se $deg\ F = d$ allora $V(F)$ ha al piú $3d(d-2)$ flessi.

Una cubica ha al piú 9 flessi (sono esattamente 9 se contati in modo opportuno). Un celebre teorema di Newton afferma che la retta congiungente due flessi di una cubica incontra la cubica ancora in un punto di flesso.

14. MORFISMI DI SEGRE E SCOPPIAMENTI

Studiamo adesso gli spazi prodotto $K^n \times K^m$, $K^n \times \mathbf{P}^m(K)$, $\mathbf{P}^n(K) \times \mathbf{P}^m(K)$.

Definizione 14.1. *In $K^n \times K^m$ definiamo una topologia che ha per insiemi chiusi $V(f_1, \ldots, f_N)$ con $f_i \in K[x_1, \ldots, x_n, y_1, \ldots, y_m]$.*

Questo equivale a considerare $K^n \times K^m \simeq K^{n+m}$ e prendere la topologia di Zariski su quest'ultimo spazio. La topologia che si ottiene non è la topologia prodotto tra le topologie di Zariski di K^n e K^m. Ad esempio i chiusi per la topologia prodotto in $K \times K$ sono dati dall'unione di un numero finito di punti e di rette "orizzontali" o "verticali".

Definizione 14.2. *Se $X \subset K^n$ e $Y \subset K^m$ sono varietà algebriche allora il prodotto $X \times Y \subset K^n \times K^m \simeq K^{n+m}$ risulta una varietà algebrica le cui equazioni sono date dall'unione delle equazioni che definiscono X e Y.*

Grafico di un morfismo regolare 14.3. *Se $V \subset K^n$ e $W \subset K^m$ sono varietá irriducibili e $f: V \to W$ é un morfismo regolare allora $G(f) = \{(x, f(x)) | x \in V\} \subset V \times W$ é una varietá algebrica isomorfa a V che si dice il grafico di f. $G(f)$ é definito dalle equazioni (con ovvie notazioni) $y_i - f_i(x_1, \ldots, x_n)$ (si veda il teorema 10.2).*

Esercizio 14.4. *Consideriamo il morfismo regolare $K^n \times K^m \xrightarrow{f} K^{nm}$ definito da*

$$f(x_1, \ldots, x_n, y_1, \ldots, y_m) = (\ldots, x_i y_j, \ldots)$$

Chiamando z_{ij} le coordinate di K^{nm}, f è definito dalle equazioni $z_{ij} = x_i y_j$. Provare che

i) l'immagine di f è una varietà algebrica che si può identificare con le matrici $Z = (z_{ij})$ di rango ≤ 1.

ii) Se $p \in Im(f)$ allora $f^{-1}(p) \simeq K^*$ se $p \neq 0$ e $f^{-1}(0) \simeq [K^n \times 0] \cup [0 \times K^m]$.

Definizione 14.5. *In $K^n \times \mathbf{P}^m$ definiamo una topologia che ha per insiemi chiusi $V(f_1, \ldots, f_N)$ con $f_i \in K[x_1, \ldots, x_n, y_1, \ldots, y_m]$ omogenei nelle y_j, cioè f_i è una somma di monomi del tipo $c x_1^{a_1} \cdots x_n^{a_n} y_0^{b_0} \cdots y_m^{b_m}$ dove $\sum_{j=0}^m b_j$ è costante.*

$K^n \times \mathbf{P}^m$ non è una varietà affine né proiettiva. È un aperto di una varietà proiettiva (che definiremo al punto seguente). Gli aperti di varietà proiettive si dicono varietà quasi-proiettive.

Definizione 14.6. *In $\mathbf{P}^n \times \mathbf{P}^m$ definiamo una topologia che ha per insiemi chiusi $V(f_1, \ldots, f_N)$ con $f_i \in K[x_0, \ldots, x_n, y_1, \ldots, y_m]$ omogenei separatemente nelle x_i e nelle y_j, cioè f_i è una somma di monomi del tipo $c x_0^{a_0} \cdots x_n^{a_n} y_0^{b_0} \cdots y_m^{b_m}$ dove $\sum_{i=0}^n a_i = d$ e $\sum_{j=0}^m b_j = d'$ sono costanti. f si dice biomogeneo di grado d nelle x_i e di grado d' nelle y_j. Abbiamo $f(\lambda x, \mu y) = \lambda^d \mu^{d'} f(x, y) \forall \quad \lambda, \mu \in K$, quest'ultima equazione puó essere presa come definizione equivalente di polinomio biomogeneo.*

Dalle definizioni precedenti segue la catena di inclusioni continue ed aperte:

$$K^n \times K^m \subset K^n \times \mathbf{P}^m \subset \mathbf{P}^n \times \mathbf{P}^m$$

Teorema 14.7. *(C. Segre) $\mathbf{P}^n \times \mathbf{P}^m$ è una varietà proiettiva.*

Dimostrazione La dimostrazione di questo teorema è importante quanto l'enunciato. Infatti si tratta di costruire il morfismo di Segre $s: \mathbf{P}^n \times \mathbf{P}^m \to \mathbf{P}^{(n+1)(m+1)-1}$ e provare che è un omeomorfismo sull' immagine (immersione). La tecnica è analoga a quella dell'esercizio 14.4. Poniamo $x_0, \ldots, x_n$ coordinate omogenee su $\mathbf{P}^n$, $y_0, \ldots, y_m$ coordinate omogenee su $\mathbf{P}^m$ e z_{ij} con $0 \leq i \leq n$, $0 \leq j \leq m$ coordinate omogenee su $\mathbf{P}^{(n+1)(m+1)-1}$. Definiamo $s(x, y) = (\ldots, x_i y_j, \ldots)$ cioè s è dato dalle equazioni $z_{ij} = x_i y_j$.

Sia $I \subset K[\ldots, z_{ij}, \ldots]$ l'ideale omogeneo definito dai minori 2×2 della matrice $Z = (z_{ij})$, cioè I è generato da

$$z_{ij}z_{kl} - z_{il}z_{kj}$$

$\forall i, j, k, l$. È immediato verificare che $Im(s) \subset V(I)$, infatti $x_i y_j x_k y_l - x_i y_l x_k y_j = 0$ (in modo più elegante $(x_i y_j)$ ha rango 1). Viceversa se $(\ldots, z_{ij}, \ldots) \in V(I)$ allora sia $z_{i_0 j_0}$ una coordinata $\neq 0$. Posto

$$x_i = \frac{z_{ij_0}}{z_{i_0 j_0}} \qquad y_j = \frac{z_{i_0 j}}{z_{i_0 j_0}}$$

allora $x_i y_j = \frac{z_{ij_0} z_{i_0 j}}{z^2_{i_0 j_0}} = \frac{z_{ij}}{z_{i_0 j_0}}$ (l'ultima uguaglianza dalle equazioni di $V(I)$). Quindi $s(x, y)$ e $(\ldots, z_{ij}, \ldots)$ hanno le stesse coordinate omogenee e segue $Im(s) = V(I)$.

Per provare che s è iniettiva supponiamo $s(x, y) = s(x', y')$, quindi $\exists \quad \lambda \neq 0$ tale che $x_i y_j = \lambda x'_i y'_j \quad \forall i, j$. Adesso per qualche i_0, j_0 abbiamo $x_{i_0} \neq 0$, $y_{j_0} \neq 0$, da cui $x'_{i_0} y'_{j_0} \neq 0$ e quindi $x'_{i_0} \neq 0$, $y'_{j_0} \neq 0$. Pertanto posto $c := \frac{\lambda y'_{j_0}}{y_{j_0}}$ abbiamo $c \neq 0$ e dall'equazione $x_i y_{j_0} = \lambda x'_i y'_{j_0} \quad \forall i$ si ricava $x_i = c x'_i \quad \forall i$ e quindi $x = x'$ in $\mathbf{P}^n(K)$. Analogamente $y = y'$. Per provare che s è un omeomorfismo sull'immagine ricordiamo che una base per gli aperti in $\mathbf{P}^n \times \mathbf{P}^m$ è data da $\{(x, y) | f(x, y) \neq 0, f$ biomogeneo di grado d in x e d' in $y\}$ al variare di f, d, d'. È sufficiente prendere gli aperti precedenti con $d = d'$ per avere una base. Infatti se ad esempio $d \geq d'$ allora $\{(x, y) | f(x, y) \neq 0\} = \cup_{j=0}^{m} \{(x, y) | y_j^{d-d'} f(x, y) \neq 0\}$. Inoltre ogni polinomio f in (x, y) biomogeneo di grado d sia in x che in y si può scrivere come un polinomio F in $x_i y_j$. Pertanto $s\left(\{(x, y) \in \mathbf{P}^n \times \mathbf{P}^m | f(x, y) \neq 0\}\right) = V(I) \cap \{(z_{ij}) \in \mathbf{P}^{(n+1)(m+1)-1} | F(z_{ij}) \neq 0\}$ e quindi s è un omeomorfismo, c.v.d.

Osservazione. *Si può provare che l'ideale I definito nella dimostrazione del teor. 14.7 è primo.*

Osservazione. *Il lettore avrá notato che la definizione 14.6 é stata fatta esattamente per far valere il teorema 14.7. Equivalentemente si puó definire la topologia in $\mathbf{P}^n \times \mathbf{P}^m$ come la topologia indotta da quella di Zariski sull'immagine $s(\mathbf{P}^n \times \mathbf{P}^m) \subset \mathbf{P}^{(n+1)(m+1)-1}$.*

Esercizio. *Provare che $\mathbf{P}^n \times \mathbf{P}^m$ é un varietá razionale.*

Definizione 14.8. *Se $X \subset \mathbf{P}^n(K)$ e $Y \subset \mathbf{P}^m(K)$ sono due varietà proiettive definite rispettivamente dai polinomi $f_i(x_0, \ldots, x_n)$ e $g_j(y_0, \ldots, y_m)$ per $1 \leq i \leq I$ e $1 \leq j \leq J$ allora il prodotto $X \times Y \subset \mathbf{P}^n \times \mathbf{P}^m \subset \mathbf{P}^{(n+1)(m+1)-1}$ è una varietà proiettiva definita dai polinomi $f_i(z_{0k}, \ldots, z_{nk})$ e $g_j(z_{p0}, \ldots, z_{pm})$ per $1 \leq i \leq I$, $0 \leq k \leq m$, $1 \leq j \leq J$, $0 \leq p \leq n$.*

Lemma 14.9. *Se $f: X \to Y$ é un morfismo regolare tra varietá proiettive (irriducibili) allora il grafico $G(f) \subset X \times Y$ é una sottovarietá di $X \times Y$ isomorfa a X.*

Dimostrazione Con ovvie notazioni le equazioni del grafico in $X \times Y$ sono date da

$$y_i f_j(x_0, \ldots, x_n) - y_j f_i(x_0, \ldots, x_n)$$

al variare degli aperti su cui é definita f (si veda l'esempio seguente).

Esempio. *Sia X la conica in $\mathbf{P}^2$ definita da $x^2+y^2-z^2=0$ e sia $p\colon X \to \mathbf{P}^1$ la proiezione stereografica (si veda l'esempio 12.21). Se (w_0, w_1) sono coordinate omogenee in $\mathbf{P}^1$ le equazioni del grafico $G(p)$ in $X \times \mathbf{P}^1$ sono date da*

$$w_0(y-z) = w_1 x$$

$$-w_0 x = w_1(y+z)$$

$$x^2+y^2-z^2 = 0$$

Lo scoppiamento(blow-up) in un punto

Siano $(x_0, \ldots, x_n)$ coordinate omogenee in $\mathbf{P}^n$ e $(y_0, \ldots, y_{n-1})$ coordinate omogenee in $\mathbf{P}^{n-1}$. Definiamo $Z = V(\ldots, x_i y_j - x_j y_i, \ldots)_{0 \le i,j \le n-1} \subset \mathbf{P}^n \times \mathbf{P}^{n-1}$.

Z è definita equivalentemente tagliando l'immagine del morfismo di Segre (vedi la dimostrazione del teorema 14.7) con gli iperpiani $z_{ij} - z_{ji} = 0$ per $0 \le i,j \le n-1$.

Consideriamo la proiezione sul primo fattore $p_1\colon \mathbf{P}^n \times \mathbf{P}^{n-1} \to \mathbf{P}^n$ e sia $\sigma = p_{1\,|Z}\colon Z \to \mathbf{P}^n$. Sia $P \in \mathbf{P}^n$ il punto di coordinate $(0, \ldots 0, 1)$. Allora vale:

i) $\sigma^{-1}(P) = P \times \mathbf{P}^{n-1} \simeq \mathbf{P}^{n-1}$.
Infatti è immediato verificare che $P \times \mathbf{P}^{n-1} \subset Z$

ii) se $Q \in \mathbf{P}^n$, $Q \neq P$ allora $\sigma^{-1}(Q)$ è dato da uno e un solo punto di Z. In particolare σ è suriettivo.
Infatti se $Q = (x_0, \ldots, x_n)$ con $x_i \neq 0$ per qualche i compreso tra 0 e $n-1$ allora $y_j = \frac{x_j}{x_i}$ determina l'unico punto $(x,y) \in Z$ tale che $\sigma(x,y) = Q$. Geometricamente P, Q e $(y_0, \ldots, y_{n-1}, 0)$ sono allineati.

Definizione 14.10. *Z insieme a $\sigma\colon Z \to \mathbf{P}^n$ si dice lo scoppiamento di $\mathbf{P}^n$ nel punto P di coordinate $(0, \ldots, 0, 1)$.*

È utile osservare che la proiezione sul secondo fattore $\rho\colon Z \to \mathbf{P}^{n-1}$ si fattorizza nel diagramma

$$\begin{array}{ccc} Z & & \\ \downarrow \sigma & \searrow \rho & \\ \mathbf{P}^n & \underset{\pi_P}{\dashrightarrow} & \mathbf{P}^{n-1} \end{array}$$

e quindi ρ può essere pensata come un'applicazione che risolve π_P (si veda l'esempio 12.18) nel punto P dove π_P non è definita.

$E := \sigma^{-1}(P) = P \times \mathbf{P}^{n-1}$ si dice il *divisore eccezionale* dello scoppiamento.

Lemma 14.11. *Z è irriducibile.*

Dimostrazione $Z \setminus E$ è irriducibile perché isomorfo a $\mathbf{P}^n \setminus P$. Quindi è sufficiente provare che $E \subset \overline{Z \setminus E}$. Pensiamo $\mathbf{P}^{n-1}$ immerso in $\mathbf{P}^n$ come l'iperpiano $x_0 = 0$. Per

ogni $y \in \mathbf{P}^{n-1}$ sia $\mathcal{L}_y$ la retta in $\mathbf{P}^n$ per y e P. Allora $(\mathcal{L}_y \setminus P) \times \{y\} \subset Z \setminus E$. Infatti se $x = (x_0, \ldots, x_n)$ é allineato con y e P allora si annullano i minori 3×3 della matrice

$$\begin{pmatrix} x_0 & \ldots & x_{n-1} & x_n \\ y_0 & \ldots & y_{n-1} & 0 \\ 0 & \ldots & 0 & 1 \end{pmatrix}$$

Tali minori corrispondono ai minori 2×2 della matrice

$$\begin{pmatrix} x_0 & \ldots & x_{n-1} \\ y_0 & \ldots & y_{n-1} \end{pmatrix}$$

cioé alle equazioni di Z.

Quindi $(P, y) \in (\mathcal{L}_y) \times \{y\} \subset \overline{Z \setminus E}$ c.v.d.

In seguito utilizzeremo anche la seguente

Proposizione 14.12. *Sia* $U_i = \mathbf{P}^{n-1} \setminus \{y_i = 0\} \simeq K^{n-1}$. *Allora* $\rho^{-1}(U_i) \simeq U_i \times \mathbf{P}^1$

Dimostrazione Se $(y_0, \ldots, 1, \ldots, y_{n-1})$ sono coordinate su U_i allora possiamo costruire l'isomorfismo $f_i : U_i \times \mathbf{P}^1 \to \rho^{-1}(U_i) \subset Z \subset \mathbf{P}^n \times \mathbf{P}^{n-1}$ dato da

$$f_i\,(y_0, \ldots, 1, \ldots, y_{n-1}; x_i, x_n) = (x_i y_0, x_i y_1, \ldots, x_i, \ldots, x_i y_{n-1}, x_n; y_0, \ldots, 1, \ldots, y_{n-1})$$

È facile verificare che f_i ammette inversa.

Lo scoppiamento si rivela uno strumento molto potente per studiare le singolaritá. Se $X \subset \mathbf{P}^n$ possiamo definire $\tilde{X} \subset Z$ come $\overline{\sigma^{-1}(X \setminus \{P\})}$. $\tilde{X}$ si dice la *trasformata propria* di X. Se X é una curva con un nodo in P a tangenti distinte allora $\tilde{X}$ incontra il divisore eccezionale E in 2 punti distinti corrispondenti alle due tangenti (si dice che i 2 rami di X si sono separati).

$Z \xrightarrow{\rho} \mathbf{P}^{n-1}$ ha tutte le fibre isomorfe a $\mathbf{P}^1$ e si dice un $\mathbf{P}^1$-fibrato che proviene da un fibrato di rango 2 su $\mathbf{P}^{n-1}$. Si puó provare che Z non é isomorfo a $\mathbf{P}^1 \times \mathbf{P}^{n-1}$, che corrisponde al fibrato banale. I fibrati hanno numerose applicazioni in matematica e in fisica.

15. IL TEOREMA FONDAMENTALE

DELLA TEORIA DELL'ELIMINAZIONE

Il lemma seguente mostra che il risultante é in modo naturale un oggetto proiettivo.

Lemma 15.1. *Siano* $f = \sum_{i=0}^{d} a_i x_0^i x_1^{d-i}$ *e* $g = \sum_{j=0}^{d'} b_j x_0^j x_1^{d'-j}$ *due polinomi* (x_0, x_1)*-omogenei a coefficienti in un campo* K*. Poniamo*

$$Res(f,g) := \det \begin{vmatrix} a_0 & a_1 & \dots & a_d & & & & & \\ & a_0 & \ddots & & \ddots & & & & \\ & & \ddots & \ddots & & \ddots & & & \\ & & & a_0 & a_1 & \dots & a_d & & \\ b_0 & b_1 & \dots & \dots & b_{d'} & & & & \\ & b_0 & \ddots & & & \ddots & & & \\ & & \ddots & \ddots & & & \ddots & & \\ & & & \ddots & \ddots & & & \ddots & \\ & & & & b_0 & b_1 & & & b_{d'} \end{vmatrix}$$

Allora

i) $Res(f,g) = 0 \iff f$ e g hanno a comune un fattore irriducibile in $K[x_0, x_1]$

ii) Se K é algebricamente chiuso

$$Res(f,g) = 0 \quad \iff \quad f, g \text{ si annullano in un punto comune di } \mathbf{P}^1$$

Dimostrazione Proviamo ii) (i) segue con piccole modifiche). Poniamo $f = x_0^\alpha f'$ e $g = x_0^\beta g'$ con f', g' non divisibili per x_0. Se $\alpha \neq 0$, $\beta \neq 0$ allora $(x_0, x_1) = (0, 1) \in \mathbf{P}^1$ é una soluzione comune e corrispondentemente $Res(f,g) = 0$ perché la prima colonna é nulla. Se $\alpha = \beta = 0$ allora $Res(f,g) = Res(f(1, x_1), g(1, x_1), x_1)$ ed il risultato segue dal teorema 8.2. Se $\alpha = 0$ e $\beta \neq 0$ allora $a_0 \neq 0$ e $Res(f,g) = a_0^\beta Res(f, g')$ e ci si riconduce al caso precedente. Analogamente se $\alpha \neq 0$ e $\beta = 0$.

Teorema 15.2. *(Main theorem of elimination theory, versione proiettiva) Sia* K *algebricamente chiuso. Allora la proiezione*

$$p\colon \mathbf{P}^n(K) \times \mathbf{P}^m(K) \to \mathbf{P}^m(K)$$

è chiusa.

Dimostrazione

1) *Il teorema equivale alla versione locale*

Consideriamo il diagramma

$$\begin{array}{ccc} \mathbf{P}^n(K) \times K^m & \subset & \mathbf{P}^n(K) \times \mathbf{P}^m(K) \\ \downarrow p' & & \downarrow p \\ K^m & \subset & \mathbf{P}^m \end{array}$$

Le inclusioni del diagramma sono continue. Quindi se p è chiusa anche p' è chiusa (prendendo la chiusura proiettiva). Viceversa se p' è chiusa per ogni aperto affine $K^m \subset \mathbf{P}^m$ allora anche p è chiusa (basta osservare che un insieme C in $\mathbf{P}^m$ tale che $C \cap K^m$ è chiuso per ogni aperto affine standard $K^m \subset \mathbf{P}^m$ ha complementare aperto e quindi è anch'esso chiuso.)

2) *Il teorema è vero se* $n = 1$

Per il primo punto è sufficiente considerare $p' : \mathbf{P}^1 \times K^m \to K^m$. Sia $S \subset \mathbf{P}^1 \times K^m$ e sia $I(S) \subset K[z_1, \ldots, z_m, x_0, x_1]$ l'ideale generato da tutti i polinomi $(x_0, x_1)-$omogenei che si annullano su S. È sufficiente provare che

$$(z_1, \ldots, z_m) \in p'(S) \Longleftrightarrow \forall f, g \in I(S) \quad (x_0, x_1) - \text{omogenei si ha } R(f, g)(z_1, \ldots, z_m) = 0$$

$\Longrightarrow$ Infatti $f(z_1, \ldots, z_m, x_0, x_1)$ e $g(z_1, \ldots, z_m, x_0, x_1)$ hanno una soluzione a comune come polinomi omogenei in (x_0, x_1) (si veda il lemma 15.1).

$\Longleftarrow$ Sia per assurdo $(z_1, \ldots, z_m) \notin p'(S)$. Sia $f \in I(S)$ e siano $P_i = (x_0^{(i)}, x_1^{(i)})$ per $i = 1, \ldots N$ gli zeri del polinomio $f(z_1, \ldots, z_m, x_0, x_1)$. Pertanto per $i = 1, \ldots N$ esistono $g_i \in I(S)$ tali che $g_i(P_i) \neq 0$ (altrimenti $\exists P_j$ tale che $P_j \in V(I(S)) = \overline{S} = S$ e sarebbe $(z_1, \ldots, z_m) \in p'(S)$). Posto $g := 1 - \prod_{i=1}^{N} \left(1 - \frac{g_i}{g_i(P_i)}\right) \in I(S)$ (svolgendo il prodotto il termine 1 si semplifica) segue $g(P_j) = 1$ per $j = 1, \ldots N$ e quindi per il lemma 15.1 $R(f, g)(z_1, \ldots, z_m) \neq 0$ contro l'ipotesi.

3) *Il teorema è vero in generale*

Si dimostra per induzione su n. Sia Z lo scoppiamento di $\mathbf{P}^n$ lungo un punto. Consideriamo il diagramma commutativo

$$\begin{array}{ccc} & Z \times K^m & \\ a \swarrow & & \searrow b \\ \mathbf{P}^n \times K^m & & \mathbf{P}^{n-1} \times K^m \\ p' \searrow & & \swarrow c \\ & K^m & \end{array}$$

a è suriettiva e continua , quindi abbiamo $p'(S) = p' \circ a \circ a^{-1}(S) = c \circ b \circ a^{-1}(S)$. Per induzione c è chiusa ed è sufficiente provare che b è chiusa. A questo proposito osserviamo che in modo analogo al punto 1) è sufficiente provare che per un ricoprimento $U_i \simeq K^{n-1}$ di aperti affini di $\mathbf{P}^{n-1}$ vale che il morfismo $b^{-1}(U_i \times K^m) \xrightarrow{b} U_i \times K^m$ è chiuso. Questo ultimo fatto segue dalla proposizione 14.12 e dal punto 2).

Corollario 15.3. *Sia V una varietá (affine o proiettiva) e sia K algebricamente chiuso. Allora la proiezione $\mathbf{P}^n(K) \times V \to V$ é chiusa.*

Definizione 15.4. *Una varietá X tale che per ogni varietá affine o (equivalentemente) proiettiva V la proiezione $X \times V \to V$ é chiusa si dice completa.*

Il corollario 15.3 prova che $\mathbf{P}^n(K)$ con K algebricamente chiuso é uno spazio completo. La completezza sostituisce nell'ambito algebrico la compattezza. Si ricordi infatti che uno spazio topologico X é compatto se e solo se per ogni spazio topologico V la proiezione $X \times V \to V$ é chiusa (prendendo la topologia prodotto!) ([N. Bourbaki, Elements de Math., livre III] nel caso Hausdorff).

Corollario 15.5. *Ogni varietá proiettiva definita su K algebricamente chiuso é completa.*

Corollario 15.6. *Sia X una varietá proiettiva definita su K algebricamente chiuso e sia $f: X \to \mathbf{P}^m(K)$ un morfismo regolare. Allora $f(X)$ é una varietá.*

Dimostrazione Basta applicare il corollario 15.5 alla proiezione $X \times P^m \to P^m$ e considerare l'immagine del grafico $G(f)$ (si veda 14.3).

Corollario 15.7. *Sia K algebricamente chiuso e sia*

$$\pi_P: \mathbf{P}^n \setminus P \to \mathbf{P}^{n-1}$$

la proiezione da P (si veda l'esempio12.18). Se $X \subset \mathbf{P}^n$ é una varietá non contenente P allora $\pi_P(X)$ é una varietá in $\mathbf{P}^{n-1}$ e le fibre di π_P sono finite.

Il corollario 15.6 é una versione algebrica del celebre (e molto piú difficile) Proper Mapping Theorem di Remmert che vale in ambito analitico.

Lemma 15.8. *Sia $f: X \to Y$ un morfismo regolare dominante. Se X é irriducibile allora Y é irriducibile.*

Dimostrazione Se $Y = V_1 \cup V_2$ allora $X = f^{-1}(V_1) \cup f^{-1}(V_2)$. Per l'ipotesi sará $X = f^{-1}(V_1)$ da cui $f(X) \subset V_1$ e quindi $Y = \overline{f(X)} \subset V_1$.

Teorema 15.9. *Sia X una varietá proiettiva irriducibile e sia K algebricamente chiuso. Allora ogni morfismo regolare $f: X \to K^n$ é costante.*

Dimostrazione É sufficiente provare che una funzione regolare $f: X \to K$ é costante. Sia $i: K \to \mathbf{P}^1$ l'immersione naturale. Dal corollario 15.6 e dal lemma 15.8 segue che $(i \circ f)(X)$ é una varietá irriducibile propria di $\mathbf{P}^1$ e quindi é un punto.

In ambito analitico ($K = \mathbf{C}$) il teorema 15.9 segue dal principio di massimo.

È possibile dare una versione costruttiva del teorema 15.2. In particolare si puó ottenere come conseguenza anche un algoritmo per il calcolo dell'immagine di una varietá proiettiva.

Definizione 15.10. *Dato un ideale $I \subset K[x_0, \ldots, x_n, y_1, \ldots, y_m]$ generato da polinomi $(x_0, \ldots, x_n)-$ omogenei allora l'ideale di eliminazione proiettivo è*

$$\hat{I} := \{f \in K[y_1, \ldots, y_m] | \forall\ 0 \leq i \leq n \quad \exists\ e_i \text{ tale che } x_i^{e_i} f \in I\}$$

Definizione 15.11. *Dato un ideale $I \subset K[x_0, \ldots, x_n, y_0, \ldots, y_n]$ generato da polinomi biomogenei (si veda la def.14.6) allora l'ideale di eliminazione proiettivo è*

$$\hat{I} := < f \in K[y_0, \ldots, y_m] omogeneo | \forall\ 0 \leq i \leq n \quad \exists\ e_i \text{ tale che } x_i^{e_i} f \in I\} >$$

$\hat{I}$ è in ogni caso un ideale, questo è mostrato anche dalla seguente

Proposizione 15.12.

i) Dato un ideale $I \subset K[x_0, \ldots, x_n, y_1, \ldots, y_n]$ generato da polinomi $(x_0, \ldots, x_n)-$ omogenei allora per tutti gli interi e sufficientemente grandi si ottiene

$$\hat{I} := (I{:} < x_0^e, \ldots, x_n^e >) \cap K[y_1, \ldots, y_m]$$

ii) *Dato un ideale $I \subset K[x_0, \ldots, x_n, y_0, \ldots, y_n]$ generato da polinomi biomogenei allora per tutti gli interi e sufficientemente grandi si ottiene*

$$\hat{I} := (I{:} < x_0^e, \ldots, x_n^e >) \cap K[y_0, \ldots, y_m]$$

Dimostrazione Dimostriamo solo i) essendo ii) completamente analoga. L'inclusione $\supset$ è evidente. Poi si considera la catena ascendente di ideali $I{:} < x_0, \ldots, x_n > \subset I{:} < x_0^2, \ldots, x_n^2 > \subset \ldots$. Questa catena è stazionaria e quindi esiste un intero e tale che

$$I{:} < x_0^d, \ldots, x_n^d > = I{:} < x_0^e, \ldots, x_n^e > \tag{15.1}$$

per ogni $d \geq e$. Se $f \in \hat{I}$ allora $\forall i \quad \exists \quad e_i$ tale che $x_i^{e_i} f \in I$. Posto $d := \max\{e_i\}$ allora $x_i^d f \in I \quad \forall i$ e quindi $f \in I{:}(x_0^d, \ldots, x_n^d)$. Per (15.1) abbiamo $f \in (I{:} < x_0^e, \ldots, x_n^e >) \cap K[y_1, \ldots, y_m]$ come volevamo.

Teorema 15.13. *(Main theorem of elimination theory, versione proiettiva "costruttiva") Sia K algebricamente chiuso.*

i) Sia I un ideale generato da polinomi $(x_0, \ldots, x_n)-$omogenei in $K[x_0, \ldots, x_n, y_1, \ldots, y_n]$ e sia $p{:}\mathbf{P}^n(K) \times K^m \to K^m$ la proiezione. Allora

$$p(V(I)) = V(\hat{I})$$

(si veda la def.15.10)

ii) Sia I un ideale generato da polinomi biomogenei in $K[x_0, \ldots, x_n, y_0, \ldots, y_n]$ e sia $p{:}\mathbf{P}^n(K) \times \mathbf{P}^m(K) \to \mathbf{P}^m(K)$ la proiezione. Allora

$$p(V(I)) = V(\hat{I})$$

(si veda la def.15.11)

Dimostrazione Dimostriamo solo i) essendo ii) completamente analoga.

$\subset$ Sia $(a_0, \ldots, a_n, b_1, \ldots, b_m) \in V(I)$ e $f \in \hat{I}$. Occorre provare che $f(b_1, \ldots, b_m) = 0$. Per ipotesi $\forall i \quad \exists e_i$ tale che $x_i^{e_i} f \in I$ e quindi

$$a_i^{e_i} f(b_1, \ldots, b_m) = 0$$

Inoltre $\exists i$ tale che $a_i \neq 0$ da cui la tesi.

$\supset$ Cominciamo col provare che

$$I(p(V(I))) \subset \sqrt{\hat{I}} \tag{15.2}$$

Se $f \in I(p(V(I))) \subset K[y_1, \ldots, y_m] \subset K[x_0, \ldots, x_n, y_0, \ldots, y_n]$ e se $(b_1, \ldots, b_m) \in p(V(I))$ allora f si annulla su $(b_1, \ldots, b_m)$. Pertanto se $(a_0, \ldots, a_n, b_1, \ldots, b_m) \in V_a(I)$ abbiamo che f e quindi anche $x_i f$ si annulla su $(a_0, \ldots, a_n, b_1, \ldots, b_m)$. Segue dal Nullstellensatz che per qualche n vale $x_i^n f^n \in I \forall \quad i$ e quindi $f^n \in \hat{I}$, il che prova (15.2). Adesso applicando V a (15.2) si ottiene

$$V(\hat{I}) = V(\sqrt{\hat{I}}) \subset V(I(p(V(I)))) = \overline{p(V(I))} = p(V(I))$$

dove l'ultima uguaglianza segue dal teorema 15.2.

Osservazione. *Il lettore interessato può elaborare un algoritmo che calcola $\hat{I}$ quando sono noti i generatori di I. Infatti é un utile esercizio provare che se*

$$I{:}< x_0^e, \ldots, x_n^e >= I{:}< x_0^{e+1}, \ldots, x_n^{e+1} >$$

allora

$$I{:}< x_0^e, \ldots, x_n^e >= I{:}< x_0^d, \ldots, x_n^d >$$

per ogni $d \geq e$. Si puó quindi trovare l'intero e e poi calcolare $\hat{I}$ con l'algoritmo visto nel §7.

16. IL TEOREMA DI CHEVALLEY

Abbiamo visto che l'immagine di una varietá proiettiva mediante un morfismo regolare é ancora una varietá proiettiva (corollario 15.6) mentre l'immagine di una varietá affine puó non essere una varietá (esempio dopo il teorema 10.2). Proveremo in questo paragrafo che l'immagine di una varietá é sempre un insieme costruibile.

Definizione 16.1. *X sottoinsieme di uno spazio topologico si dice <u>costruibile</u> se X si ottiene dagli insiemi aperti e chiusi dopo aver effetuato un numero finito di operazioni di unione e intersezione. Equivalentemente $X = \cup_{i=1}^{p}(A_i \cap C_i)$ con A_i aperti e C_i chiusi.*

Complementari, unioni e intersezioni finite di costruibili sono ancora costruibili. Se $f{:}X \to Y$ é continua e $V \subset Y$ é costruibile allora $f^{-1}(V)$ é costruibile.

Saremo interessati agli insiemi costruibili in K^n e in $\mathbf{P}^n$ con le rispettive topologie di Zariski.

Lemma 16.2. *Sia Z un insieme costruibile in K^n o in $\mathbf{P}^n$ tale che $\overline{Z}$ é irriducibile. Allora Z é localmente chiuso, cioé esiste un aperto A tale che $Z = \overline{Z} \cap A$.*

Dimostrazione Sia $Z = \cup_i^r (A_i \cap C_i)$ con A_i aperti, C_i chiusi irriducibili distinti (qui é sufficiente utilizzare il fatto che ogni chiuso é unione finita di chiusi irriducibili). Allora per l'irriducibilitá $\overline{A_i \cap C_i} = C_i$ e $\overline{Z} = \cup \overline{(A_i \cap C_i)} = \cup C_i$. Quindi $r = 1$ da cui la tesi.

Proposizione 16.3. *Sia Z un insieme costruibile in K^n o in $\mathbf{P}^n$. Allora*

$$Z = C_1 \setminus (C_2 \setminus (C_3 \setminus (\ldots \setminus C_p)))$$

con chiusi $C_p \subset_{\neq} C_{p-1} \subset_{\neq} \ldots \subset_{\neq} C_1$ tali che $\overline{C_i \setminus C_{i+1}} = C_i$ e $\overline{C_1 \setminus C_2} = C_1 = \overline{Z}$.

Dimostrazione Poniamo $C_1 = \overline{Z} = \cup F_i$ (componenti irriducibili). Abbiamo $Z = C_1 \setminus H_1$ con $H_1 \subset C_1$ costruibile. Poniamo quindi $C_2 = \overline{H_1}$. Affermiamo che

$$C_2 \cap F_i \subset_{\neq} F_i \tag{16.1}$$

Altrimenti vale $C_2 \cap F_i = F_i$. In questo caso se $x \in F_i$ allora $x \in Z$ e $x \in C_2$ ed ogni intorno di x incontra $\overline{Z}$ e $\overline{C_2}$. Pertanto $\overline{Z \cap F_i} = F_i$ e $\overline{H_1 \cap F_i} = F_i$. Dal lemma 16.2 $Z \cap F_i$ e $H_1 \cap F_i$ sono aperti disgiunti in F_i e questo contraddice l'irriducibilitá di F_i. Quindi abbiamo provato (16.1). In particolare $C_2 \subset_{\neq} C_1$. Adesso considera che

$$\overline{C_1 \setminus C_2} = \cup_i \overline{(F_i \setminus (C_2 \cap F_i))} = \cup_i F_i = C_1$$

A questo punto poniamo $H_1 = C_2 \setminus H_2$ con $H_2 \subset C_2$ costruibile e possiamo procedere come sopra. La catena discendente dei C_i cosí costruiti deve arrivare a $\emptyset$ per noetherianitá.

Corollario 16.4. *Sia Z un insieme costruibile in K^n o in $\mathbf{P}^n$. Allora esiste $\emptyset \neq V \subset Z$ tale che V é un aperto in $\overline{Z}$. Inoltre $\overline{V} = \overline{Z}$.*

Dimostrazione Basta prendere $V = Z \setminus C_2$ nella prop. 16.3.

Corollario 16.5. *Sia Z un insieme costruibile in K^n o in $\mathbf{P}^n$. Allora $Z = \cup_{i=1}^r G_i$ dove i G_j sono insiemi localmente chiusi disgiunti tra loro tali che $\overline{G_i} \supset \overline{G_{i+1}}$.*

Dimostrazione Basta prendere $G_1 = C_1 \setminus C_2$, $G_2 = C_3 \setminus C_4, \ldots$ nella prop. 16.3.

Lemma 16.6. *Sia $X \subset \mathbf{P}^n$ con coordinate omogenee $(x_0, \ldots, x_n)$. Sia $K_i^n = \{x_i \neq 0\}$ un aperto affine standard. Le due proprietá seguenti sono equivalenti:*

i) X é costruibile

ii) $X \cap K_i^n$ é costruibile per $i = 0, \ldots, n$.

Dimostrazione i)$\Longrightarrow$ii) é ovvia. Per provare ii)$\Longrightarrow$i) basta considerare che $X \cap K_i^n$ é costruibile anche in P^n e quindi $X = \cup_{i=0}^n [X \cap K_i^n]$ é costruibile perché unione finita di costruibili.

Teorema 16.7. *(Chevalley). Sia K algebricamente chiuso. Sia $X \subset K^n$ un insieme costruibile e $f: X \to \mathbf{P}^m$ un morfismo regolare. Allora $f(X)$ é costruibile.*

Corollario 16.8. *Sia K algebricamente chiuso. Sia $X \subset K^n$ una varietá e $f: X \to \mathbf{P}^m$ un morfismo regolare. Allora $f(X)$ é costruibile.*

Dimostrazione del teorema di Chevalley Per il lemma 16.6 possiamo supporre che l'immagine di f sia in K^m. Considerando il grafico di f, vedi (14.3), possiamo supporre che $S \subset K^n \times K^m$ e se $\pi: K^n \times K^m \to K^m$ é la proiezione dobbiamo provare che $\pi(S)$ é costruibile. Prendendo successive proiezioni possiamo supporre $n = 1$. Facciamo la seguente affermazione:

$$\text{se } U \subset K \times K^m \text{ é costruibile allora } \exists\ V \subset \pi(U) \text{ aperto non vuoto in } \overline{\pi(U)} \qquad (16.2)$$

Supponiamo dapprima che (16.2) sia vera. In particolare $V = \overline{\pi(U)} \cap A$ per qualche A aperto e quindi V é costruibile. Inoltre $V = \pi(U) \cap A$ e quindi V é aperto anche in $\pi(U)$. Sia $U_1 = U \cap (X \setminus \pi^{-1}(V))$ (chiuso in U) da cui $\pi(U) = \pi(U_1) \cup V$ e quindi se $\pi(U_1)$ é costruibile anche $\pi(U)$ é costruibile. Notiamo che siccome $V \neq \emptyset$ abbiamo $U_1 \subset_{\neq} U$. Se $U_1 \neq \emptyset$ per (16.2) allora esiste $V_1 \neq \emptyset$ tale che $V_1 \subset \pi(U_1)$ e V_1 é aperto in $\overline{\pi(U_1)}$. Posto $U_2 = U_1 \cap (X \setminus \pi^{-1}(V_1))$ (chiuso in U_1 e quindi in U) abbiamo $U_2 \subset_{\neq} U_1 \subset_{\neq} U$ e $\pi(U_1) = \pi(U_2) \cup V_1$ da cui se $\pi(U_2)$ é costruibile anche $\pi(U_1)$ é costruibile. Se $U_2 \neq \emptyset$ possiamo trovare U_3 e continuando troviamo una catena $U \supset_{\neq} U_1 \supset_{\neq} \ldots$ con U_i chiusi in U. Per il corollario 6.7 esiste j tale che $U_j = \emptyset$ da cui $\pi(U_{j-1}) = \pi(U_j) \cup V_{j-1} = V_{j-1}$ é costruibile. Pertanto anche $\pi(U)$ é costruibile come volevamo.

Rimane da provare (16.2). Possiamo sostituire K^m con $Y = \overline{\pi(U)}$ e $K \times K^m$ con $\pi^{-1}(Y) = Y \times K$. Possiamo considerare $U =\subset Y \times \mathbf{P}^1$, $\pi: Y \times \mathbf{P}^1 \to Y$ con $\pi(U)$ denso in Y e dobbiamo provare che $\pi(U)$ contiene un aperto di Y. Dal corollario 16.4 abbiamo che U contiene V localmente chiuso tale che $\overline{V} = \overline{U}$. Inoltre $Y = \overline{\pi(U)} = \pi(\overline{U})$ (l'ultima uguaglianza perché π é chiusa per il corollario 14.5) da cui $\pi(V)$ é denso in Y e quindi per provare (16.2) possiamo supporre $U = A \cap C$ localmente chiuso.

Sia T il complementare di A. Se $C = Y \times \mathbf{P}^1$ la tesi é vera perché il luogo dei punti p di Y tali che $T \supset \{p\} \times \mathbf{P}^1$ é una sottovarietá di Y. Pertanto $C \subset_{\neq} Y \times \mathbf{P}^1$. Per il corollario15.3 $\pi(C)$ e $\pi(C \cap T)$ sono chiusi. Siccome $\pi(C) \supset \overline{\pi(U)} = Y$ é sufficiente provare che $\pi(C \cap T) \subset_{\neq} Y$. Possiamo supporre che C sia irriducibile. Gli ideali di C e di T sono generati da polinomi F della forma

$$F(z, w) = a_0 z^k + a_1 z^{k-1} w + \ldots + a_k w^k$$

con $a_i \in K[Y]$ e (z, w) coordinate omogenee su $\mathbf{P}^1$. Sia $F \in I(C)$ un polinomio irriducibile. Esiste $G \in I(T)$ che non contiene F come fattore irriducibile. In particolare per il lemma 15.1 $Res(F, G) \in K[Y]$ é non nullo (si possono considerare i polinomi a coefficienti nel campo dei quozienti $K(Y)$). Quindi $\pi(C \cap T)$ é contenuto nella sottovarietá propria di Y definita dall'annullarsi di $Res(F, G)$. La dimostrazione del teorema di Chevalley é cosí completa.

Osservazione. *Una applicazione del teorema di Chevalley é collegata al teorema di chiusura del cap. 9. Infatti con le notazioni del cap. 9 dal teorema di Chevalley segue $\pi_t(V)$ contiene $V(I_t) \setminus W$ dove W é un chiuso di Zariski.*

Teorema 16.9. *Sia $f: X \to Y$ un morfismo razionale dominante di varietá (affini o proiettive) e sia $f^*: K(Y) \to K(X)$ l'inclusione indotta. Denotiamo con $[K(X): K(Y)]$ il grado dell'estensione. Sono equivalenti le tre proprietá seguenti:*

i) $[K(X): K(Y)]$ é finito
ii) Per ogni sottovarietá $C \subset_{\neq} X$ si ha $\overline{f(C)} \subset_{\neq} Y$
iii) $\exists\, U \subset Y$ aperto $\neq \emptyset$ tale che $\forall y \in U f^{-1}(y)$ é finito

*Cenno di dimostrazione*Siccome l'enunciato riguarda morfismi razionali possiamo sostituire X e Y con degli aperti di varietá affini dove f é definita. Considerando il grafico di f (si veda 14.3) ci riconduciamo al caso in cui f é la restrizione ad un sottoinsieme X di K^n (aperto di una varietá) di una proiezione da K^n a K^m. Proveremo che $i) \Leftrightarrow$ii) e poi che i)$\Leftrightarrow$iii). Consideriamo per induzione la composizione di proiezioni

$$K^n \xrightarrow{f_1} K^{m+1} \xrightarrow{f_2} K^m$$

e poniamo $X_1 = \overline{f_1(X)}$. Segue dal teorema di Chevalley che $f_1(X)$ contiene un aperto in X_1. É facile vedere che é sufficiente dimostrare il teorema nel caso in cui $n = m + 1$.

i)$\Rightarrow$ii) Sia $p(z, y_1, \ldots, y_m) = p(z, y) = z^k + a_{k-1}(y)z^{k-1} + \ldots a_0(y)$ il polinomio minimo di $K(X)$ su $K(Y)$ con $a_i(y) \in K(Y)$. Sia $g(z, y)$ una equazione che si annulla su C e sia $R(y) = Res(p, g, z)$. Se fosse $R(y) \equiv 0$ in $K(Y)$ allora p e g avrebbero un fattore in comune in $K(Y)[z]$. Ma $K(X_1) \simeq K(Y)[z]/(p)$ da cui (p) é massimale, quindi primo e p é irriducibile. Pertanto R non é nullo, abbiamo $R = \alpha p + \beta g$ con α, $\beta \in K(Y)$ e togliendo i denominatori $tR = \alpha' p + \beta' g$ con $t, \alpha', \beta' \in K[Y]$. Segue $\overline{f(C)} \subset \{tR = 0\}$.

ii)$\Rightarrow$i) Siano $(z, y_1, \ldots, y_m)$ coordinate in K^n e pensiamo $z \in K(X)$. Se z é trascendente su $K(Y)$ allora per ogni $h \in I(X)$ scritto come $h(z, y) = a_d(y)z^d + a_{d-1}(y)z^{d-1} + \ldots$ deve essere a_i nullo su Y e quindi h si annulla su $f^{-1}(y)$ per ogni $y \in Y$, cioé $f^{-1}(y) \subset V(I(X)) = \overline{X}$ e quindi X é un aperto di $Y \times K \subset \overline{X}$. Il complementare di X in $Y \times K$ puó contenere solo un numero finito di fibre $Y \times \{k\}$ al variare di $k \in K$. Sia $k_0 \in K$ tale che $Y \times \{k_0\}$ non é contenuto nel complementare di X. Pertanto posto $C = Y \times \{k_0\} \cap X$ segue $\overline{f(C)} = Y$.

i)$\Rightarrow$ iii) Se z é algebrico su $K(Y)$ consideriamo sempre il polinomio minimo $p(z, y) = z^k + a_{k-1}(y)z^{k-1} + \ldots a_0(y)$ di z su $K(Y)$. Fuori dal luogo dove si annullano i denominatori di $a_i \in K(Y)$ abbiamo che le fibre di f sono finite.

iii)$\Rightarrow$ i) Se z é trascendente su $K(Y)$ allora come nel punto ii)$\Rightarrow$i) abbiamo che X é un aperto di $Y \times K \subset \overline{X}$.

Definizione 16.10. *Se una delle condizioni equivalenti del teorema 16.9 é soddisfatta allora f si dice genericamente finito.*

Proposizione 16.11. *Sia $f: X \to Y$ un morfismo (razionale dominante) genericamente finito. Se K é algebricamente chiuso e se car $K = 0$ allora*

$$[K(X): K(Y)] = \sharp\{f^{-1}(y)\} \text{ per } y \in U$$

Dimostrazione

Con le stesse considerazioni fatte nella dimostrazione del teorema 16.10 possiamo considerare il polinomio minimo $p(z, y)$. Togliendo i denominatori possiamo supporre $p(z, y) = a_k(y)z^k + a_{k-1}(y)z^{k-1} + \ldots$ con a_i regolari su Y e $k = [K(X): K(Y)]$. Sia $\Delta \in K[Y]$ il discriminante di p come polinomio in z. Se $\Delta \equiv 0$ allora p e $\frac{dp}{dz}$ avrebbero un fattore in comune (qui gioca *car* $K = 0$) contro l'irriducibilitá di p. Pertanto Δ é non nullo e nel complementare di $V(a_0\Delta)$ la fibra consiste esattamente di d punti.

Corollario 16.12. *Sia K algebricamente chiuso e car $K = 0$. Se $f: X - - \to Y$ é un morfismo razionale dominante (genericamente finito) iniettivo su un aperto U allora é un'equivalenza birazionale.*

Dimostrazione Dal teorema 16.9 e dalla prop. 16.11 abbiamo $[K(U): K(Y)] = [K(X): K(Y)] =$ 1 e quindi $K(X) \simeq K(Y)$. La tesi segue allora dal teorema 11.20.

Il corollario precedente chiarisce la differenza tra varietá razionali e unirazionali.

Esistono esempi di varietá nonsingolari di dimensione 3 su $\mathbf{C}$ unirazionali ma non razionali.

Esercizio. *Sia $Q_{n-1} \subset K^n$ una ipersuperficie quadrica e $P \in Q_{n-1}$ un punto che non é un vertice di Q. Se car $K = 0$ e K é algebricamente chiuso provare che $\pi_P: Q_{n-1} - - \to K^{n-1}$ é un'equivalenza birazionale.*

17. FUNZIONE E POLINOMIO DI HILBERT

Sia $K[x_1, \ldots, x_n]_{\leq s}$lo spazio vettoriale dei polinomi di grado $\leq s$. In particolare

$$dim\ K[x_1, \ldots, x_n]_{\leq s} \quad = \quad \binom{n+s}{s}$$

(conviene pensare ai polinomi omogenei di grado s in $n+1$ variabili). Definiamo

$$I_{\leq s} = I \cap K[x_1, \ldots, x_n]_{\leq s}$$

, esso contiene i polinomi di I di grado $\leq s$.

Definizione 17.1 La funzione di Hilbert di un ideale $I \subset K[x_1, \ldots, x_n]$ è

$$F_I(s) := dim K[x_1, \ldots, x_n]_{\leq s}/I_{\leq s}$$

$F_I(s)$ è una funzione non decrescente definita sugli interi ≥ 0 che assume valori interi ≥ 0. Una delle scoperte fondamentali compiute da Hilbert nel suo celebre lavoro pubblicato su Mathematische Annalen del 1890 fu il comportamento polinomiale di $F_I(s)$ per $s \gg 0$. Il grado di questo polinomio è uguale alla dimensione di $V(I)$.

Ricordiamo che un ordine monomiale si dice graduato se $x^\alpha < x^\beta$ quando $\sum \alpha_i < \sum \beta_i$ In particolare DEGLEX e DEGREVLEX sono ordini monomiali graduati, mentre LEX non lo è. Il passo fondamentale per il calcolo esplicito della funzione di Hilbert fu compiuto da Macaulay nel 1927.

Teorema 17.2 (Macaulay) Fissiamo un ordine monomiale graduato. Allora I e $LT(I)$ hanno la stessa funzione di Hilbert.

Dimostrazione Dobbiamo provare che $dim_K\ I_{\leq s} = dim_K\ LT(I)_{\leq s}$. Fissato $s \geq 0$ abbiamo $\{LM(f)|f \in I_{\leq s}\} = \{LM(f_1), \ldots, LM(f_m)\}$ dove $LM(f_1) > LM(f_2) > \ldots > LM(f_m)$. Affermiamo che $\{f_1, \ldots, f_m\}$ formano una base di $I_{\leq s}$ come spazio vettoriale su K. Infatti se $\sum a_j f_j = 0$ con $a_j \in K$ pesi non nulli, poniamo $i = min\{j|a_j \neq 0\}$. Allora $a_i LT(f_i)$ non può essere cancellato nella somma precedente, quindi $f_1, \ldots, f_m$ sono linearmente indipendenti. Poniamo ora $W =< f_1, \ldots, f_m >$. Se per assurdo $W \neq I_{\leq s}$ scegliamo $f \in I_{\leq s} \backslash W$ con $LM(f)$ minimo. Allora $\exists \lambda \in K, i \geq 0$ tali che $LM(f - \lambda f_i) < LM(f)$ ed anche $f - \lambda f_i \in I_{\leq s} \backslash W$, da cui una contraddizione.
Affermiamo anche che $\{LM(f_1), \ldots, LM(f_m)\}$ formano una base di $LT(I)_{\leq s}$. Ovviamente gli elementi sono indipendenti. Inoltre $LT(I)_{\leq s} =< LM(f)|f \in I, LM(f)$ha grado $\leq s >$. Per ipotesi l'ordine è graduato, quindi $degf = degLM(f)$, pertanto $LT(I)_{\leq s} =< LM(f)|f \in I_{\leq s} >=< LM(f_1), \ldots, LM(f_m) >$ come volevamo.

Definizione 17.3 Un polinomio $p(t) \in \mathbf{Q}[t]$ si dice un *polinomio numerico* se $p(t) \in \mathbf{Z}$ per $t \gg 0$, $t \in \mathbf{Z}$.

Esempio 17.4 $\binom{t+i}{i} = \frac{(t+i)(t+i-1)\ldots(t+1)}{i!}$ è un polinomio numerico se $i \geq 0$, dove $\binom{i}{0} = 1$. Secondo questa definizione $\binom{t+i}{i} \neq 0$ per $t \ll 0$, a differenza dell'usuale coefficiente binomiale.

I due insiemi $\{1, t, t^2, \ldots, t^d\}$ e $\{1, (t+1), \binom{t+2}{2}, \ldots, \binom{t+d}{d}\}$ sono due basi dello spazio vettoriale $\mathbf{Q}[t]_{\leq d}$. La seconda base è più conveniente per scrivere i polinomi numerici.Il sistema CoCoA é dotato di alcuni comandi che permettono di passare da una base all'altra.

Teorema 17.5 $P(t)$ è un polinomio numerico di grado $d \Leftrightarrow P(t) = \sum_{i=0}^{d} a_i \binom{t+i}{i}$

con $a_i \in \mathbf{Z}$

Dimostrazione $\Leftarrow$ è ovvia
$\Rightarrow$ si prova per induzione su d. Per $d = 0$ il risultato è banale. In generale abbiamo che $P(t)-P(t-1)$ è un polinomio numerico di grado $d-1$ e per ipotesi induttiva $P(t)-P(t-1) = \sum_{i=0}^{d-1} c_i \binom{t+i}{i}$ con $c_i \in \mathbf{Z}$. Poniamo $P(t) = \sum_{i=0}^{d} a_i \binom{t+i}{i}$ con a_i da determinare. Allora $P(t)-P(t-1) = \sum_{i=0}^{d} a_i \binom{t+i}{i} - a_i \binom{t+i-1}{i} = \sum_{i=1}^{d} a_i \binom{t+i-1}{i-1} = \sum_{i=0}^{d-1} a_{i+1} \binom{t+i}{i}$. Abbiamo allora $a_i = c_{i-1} \in \mathbf{Z}$

per $i \geq 1$. Inoltre $P(t) = a_0 + \sum_{i=1}^{d} a_i \binom{t+i}{i}$ da cui $a_0 \in \mathbf{Z}$.

Corollario 17.6 Se $P(t)$ è un polinomio numerico abbiamo $P(t) \in \mathbf{Z} \quad \forall t \in \mathbf{Z}$.

Esercizio Scrivere la matrice 4×4 del cambiamento di base in $\mathbf{Q}[t]_{\leq 3}$tra le due basi precedenti. In generale tali matrici sono sempre triangolari.

Lemma 17.7 Siano $\{A_i\}_{i=1\ldots n}$ insiemi finiti ed indichiamo con $|A_i|$ il numero degli elementi di A_i. Allora $|A_1 \cup \ldots \cup A_n| = \sum_{r=1}^{n} (-1)^{r-1} \left(\sum_{1 \leq i_1 < \ldots < i_r \leq n} |A_{i_1} \cap \ldots \cap A_{i_r}| \right)$.

Dimostrazione Se $n = 2$ l'enunciato è $|A \cup B| = |A| + |B| - |A \cap B|$. Il caso generale segue facilmente per induzione su n.

Teorema 17.8 Sia $I \subset K[x_1, \ldots, x_n]$ un ideale. La funzione di Hilbert $F_I(s)$ è un polinomio numerico per $s \gg 0$.

Dimostrazione Per il teorema di Macaulay è sufficiente dimostrare la tesi quando I è un ideale monomiale. Siccome $F_I(s) = \binom{n+s}{s} - dim\ I_{\leq s}$ faremo vedere che $dim\ I_{\leq s}$ è un polinomio numerico per $s \gg 0$. Ricordiamo che poichè I è monomiale un polinomio appartiene a I se e solo se ogni suo termine appartiene a I. Pertanto $dim I_{\leq s} = |$ monomi in I di grado $\leq s|$. Siano $x^{\alpha_1}, \ldots, x^{\alpha_k}$ i generatori di I e definiamo gli insiemi (per $\alpha \in \mathbf{Z}^n_{\geq 0}$) $F_\alpha = \{$monomi multipli di $x^\alpha\}$, $F^s_\alpha = \{$monomi multipli di x^α di grado $\leq s\}$. E' chiaro che $|F^s_\alpha| = \binom{s-multideg\alpha+n}{n}$per $s \gg 0$ è un polinomio numerico in s.

Inoltre $F_{\alpha_{i_1}} \cap \ldots \cap F_{\alpha_{i_r}} = F_\gamma$ dove $x^\gamma = LCM(x^{\alpha_{i_1}}, \ldots, x^{\alpha_{i_r}})$ ed in particolare $|F^s_{\alpha_{i_1}} \cap \ldots \cap F^s_{\alpha_{i_r}}| = |F^s_\gamma|$ per $s \geq 0$. Abbiamo $dim I_{\leq s} = |\cup_{i=1}^{k} F^s_{\alpha_i}|$. Dal lemma 17.7 la cardinalità di questa unione può essere espressa attraverso una somma finita di termini ciascuno dei quali è un polinomio numerico per $s \gg 0$, da cui la tesi.

Osservazione. *Otterremo un'altra dimostrazione del teorema 17.8 facendo uso del teorema delle sizigie di Hilbert.*

Definizione **17.9** Sia $I \subset K[x_1, \ldots, x_n]$ un ideale. Il polinomio numerico $P_I(t)$ tale che $P_I(t) = F_I(t)$ per $t \gg 0$ si dice *polinomio di Hilbert* di I.

In linea di principio la dimostrazione precedente permette di calcolare esplicitamente la funzione di Hilbert e il polinomio di Hilbert di un ideale dell'anello dei polinomi. Questo algoritmo(opportunamente modificato) è stato implementato in molti sistemi di calcolo simbolico.

Ad esempio in COCOA il comando $Hilbert(R/I)$ mostra il polinomio di Hilbert di I nell'ambiente proiettivo; quando vogliamo un risultato nell'affine per la varietà $V(I)$ dove $I \subset K[x_1, \ldots, x_n]$ bisogna avere l'accortezza di aggiungere una variabile ausiliaria all'anello e quindi lavorare in $K[x_1, \ldots, x_n, t]$. Se ad esempio $I = (y - x^2, z - x^3)$ occorre definire come anello $K[x, y, z, t]$, posto $I = ideal(y - x^2, z - x^3)$ il comando $Hilb(R/I)$ dà la risposta corretta $P_I(s) = 3s + 1$. $HilbCoeff(R/I)$ scrive i coefficienti a segni alterni rispetto alla base $\binom{t+i}{i}$. In questo caso $P_I(s) = 3(s+1) - 2$ ed i coefficienti sono $3, 2$. Il comando $HilbertFn(R/I)$ dà la funzione di Hilbert $F_I(s)$. In generale, per valori piccoli di s, $F_I(s)$ e $P_I(s)$ non si limitano tra di loro. Il più piccolo s_0 per cui $F_I(s) = P_I(s)$ quando $s \geq s_0$ si chiama indice di regolarità di I e può essere ottenuto col comando $Reg(R/I)$. Nell'esempio precedente $reg = 0$.

Esempio (facile). Sia $I = (xy, x^3) \subset K[x, y]$. Allora $F_I(0) = 1$, $F_I(1) = 3$, $F_I(s) = s + 3$ per $s \geq 2$. Qui $P_I(s) = s + 3$ e $Reg(R/I) = 2$.

Esempio Sia $I = (y - x^3, z - x^4) \subset K[x, y, z]$. Il polinomio di Hilbert è $P_I(s) = 4s + 1 = 4(s+1) - 3$ mentre $F_I(0) = 1, F_I(1) = 4$ e $F_I(s) = 4s + 1$ per $s \geq 2$. Qui $Reg(R/I) = 2$.

18. DIMENSIONE DI UNA VARIETÁ ALGEBRICA

Vogliamo sviluppare un algoritmo che ci permetta di determinare la dimensione dell'insieme delle soluzioni di un sistema

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \qquad \vdots \\ f_k(x_1, \ldots, x_n) = 0 \end{cases}$$

dove f_i sono polinomi a coefficienti in un campo K algebricamente chiuso.

Dal teorema degli zeri di Hilbert 9.2 siamo già in grado di determinare quando l'insieme delle soluzioni è vuoto (dimensione= -1): questo accade se e solo se l'ideale $I = (f_1, \ldots, f_k)$ è l'ideale (1), oppure se e solo se $LT(I) = (1)$ per un qualunque ordine

monomiale, e questa ultima condizione può essere verificata calcolando una base di Gröbner di I, ad esempio con l'algoritmo di Buchberger.

Ci proponiamo ora di caratterizzare il caso successivo, in cui dim $V(I) = 0$, cioè il caso in cui le soluzioni sono un numero finito.

Teorema 18.1 Sia $I \subset K[x_1, \ldots, x_n]$ un ideale e sia $S =< x^\alpha | x^\alpha \notin LT(I) >$ sottospazio (su K) di $K[x_1, \ldots, x_n]$. Allora $K[x_1, \ldots, x_n]/I \simeq S$ come spazi vettoriali su K. L'isomorfismo non è canonico ma dipende dalla scelta di un ordine monomiale.

Dimostrazione Fissiamo un ordine monomiale, e sia $G = \{g_1, \ldots, g_s\}$ una base di Gröbner per I. Indichiamo con $[f] \in K[x_1, \ldots, x_n]/I$ gli elementi del quoziente ($f \in K[x_1, \ldots, x_n]$) e definiamo $\phi : K[x_1, \ldots, x_n]/I \to S$ data da $\phi([f]) = \overline{f}^{G}$ (resto della divisione per G, che abbiamo indicato anche come $f \ mod \ I$). Se $f = \sum h_i g_i + r$ è la divisione poniamo quindi $\phi([f]) = r$. ϕ è ben definito perchè se $f - f' \in I$ abbiamo $f = \sum h_i g_i + r, f' = \sum h'_i g_i + r'$ (divisioni per G) e quindi $r - r' \in I$. Pertanto se $r \neq r'$ abbiamo $LT(r - r')$ divisibile per qualche $LT(g_j)$ (per definizione di base di Gröbner) in contraddizione con l'algoritmo di divisione. ϕ è suriettiva perchè se $x^\alpha \in S$ abbiamo $\phi([x^\alpha]) = x^\alpha$. Inoltre se $\overline{f}^{G} = \overline{f'}^{G}$ è ovvio che $f - f' \in I$, quindi ϕ è iniettiva. E' facile verificare che $\phi(k[f]) = k\phi([f])$. Rimane da far vedere che ϕ conserva la somma. Infatti se $f = g + r, f' = g' + r'$ dove nessun termine di r, r' appartiene a $LT(I)$ segue che $f + f' = (g + g') + (r + r')$ dove nessun termine di $(r + r')$ appartiene a $LT(I)$. Sia r''il resto della divisione di $f + f'$ per G, allora $f + f' = g'' + r''$ dove nessun termine di r'' appartiene a $LT(I)$. Quindi se $(r + r') - r'' \neq 0$ abbiamo $LT[(r + r') - r''] \in LT(I)$ che è una contraddizione. Pertanto $r + r' = r''$, cioè $\phi([f]) + \phi([f']) = \phi([f + f'])$.

Teorema 18.2 Sia K algebricamente chiuso e $I \subset K[x_1, \ldots, x_n]$ un ideale. Sono equivalenti:
i) $V(I)$ è finito
ii) $\forall i = 1, \ldots, n \ \exists m_i \geq 0$ tale che ${x_i}^{m_i} \in LT(I)$
iii) lo spazio vettoriale $K[x_1, \ldots, x_n]/I (\simeq S$ vedi teor. 18.1) ha dimensione finita
Dimostrazione

i) $\Rightarrow$ *ii)* Se $V(I) = \emptyset$ abbiamo $1 \in LT(I)$ dal teorema degli zeri e basta porre $m_i = 0$. Se $V(I) \neq \emptyset$ siano $\{a_j\}_{j \in J(i)}$ tutte le i-esime coordinate dei punti di $V(I)$. Posto $f_i = \prod_{j \in J(i)} (x_i - a_j)$ abbiamo $f_i \in I(V(I)) = \sqrt{I}$ dal teorema degli zeri.
Quindi $\exists \ k_i : {f_i}^{k_i} \in I$ e $LT({f_i}^{k_i}) =: {x_i}^{m_i} \in LT(I)$ come volevamo.

ii) $\Rightarrow$ *iii)* Se $x^\alpha \in S =< x^\alpha | x^\alpha \notin LT(I) >$ (l'uguaglianza per il teor. 18.1) deve essere $\alpha_i \leq m_i - 1$. Quindi $dim S \leq \prod_{i=1}^{n} m_i$.

iii) $\Rightarrow$ *i)* Per ipotesi gli elementi $[1], [x_1], [{x_1}^2], \ldots, [{x_1}^n], \ldots$sono linearmente dipendenti, quindi $\exists \ c_j \in J$ tali che $\sum c_j {x_1}^j \in I$. In particolare i punti di $V(I)$ possono avere solo un numero finito di

coordinate differenti al primo indice (le radici del polinomio precedente). Il ragionamento si ripete anche per gli altri indici.

La condizione ii) del teorema precedente dà un algoritmo per stabilire se l'insieme delle soluzioni di un sistema di polinomi è finito, una volta calcolata una base di Gröbner. In caso affermativo la dimostrazione mostra anche che il numero delle soluzioni è limitato da $\prod_{i=1}^{n} m_{\mathrm{i}}$ (se ci fossero $\prod_{i=1}^{n} m_{\mathrm{i}} + 1$ soluzioni potrei costruire $\prod_{i=1}^{n} m_{\mathrm{i}} + 1$ polinomi ciascuno dei quali si annulla in tutti i punti escluso uno, e questi polinomi sarebbero indipendenti in $K[x_1, \ldots, x_{\mathrm{n}}]/I$).

Esercizi Nei casi seguenti determinare quando $V(I)$ è finito e limitare il numero dei punti di $V(I)$.
i) $I \subset \mathbf{C}[x, y, z]$ con base di Gröbner data da$(x^2 y, y^3 z, z^5, xz)$
ii) $I \subset \mathbf{C}[x, y, z]$con base di Gröbner data da $(x^2, xy, y^3, yz^{10}, z^7)$
iii) $I \subset \mathbf{C}[x_1, x_2, x_3, x_4]$ con base di Gröbner data da $(x_1^2, x_2^2, x_3^2, x_1x_4, x_2x_4, x_3x_4)$
Risposta: $V(I)$ è finito solo nel caso ii) ed il numero di punti è≤ 42.
Osserviamo che i risultati precedenti possono essere interpretati come segue:

$$dim V(I) = -1 \Leftrightarrow F_I(s) \equiv 0 \quad \forall s \qquad \text{Nullstellensatz debole}$$

$$dim V(I) = 0 \Leftrightarrow F_I(s) \text{ è costante per } s \gg 0 \qquad \text{teorema 18.2}$$

Definizione 18.3. *Sia V una varietá algebrica. La dimensione di V è il grado del polinomio di Hilbert di $I(V)$.*

Verificheremo piú avanti che questa definizione di dimensione coincide con quella nota sui complessi perché é uguale al grado di trascendenza su K del campo delle funzioni razionali. In generale $I(V)$ è difficile da calcolare. Se K é algebricamente chiuso vedremo che la definizione 18.3 é operativa (vedi teor.18.13 e l'algoritmo seguente).

Il caso proiettivo
Vediamo quali modifiche occorre apportare alla teoria precedente nel caso di una varietá proiettiva $V = V(I) \subset \mathbf{P}^n$ definita da un ideale omogeneo $I \subset K[x_0, \ldots, x_{\mathrm{n}}]$. Sia $C_V \subset K^{n+1}$ il cono affine corrispondente.
Si pone (se $V \neq \emptyset$)

$$dim V := dim C_V - 1 \tag{18.1}$$

La dimensione di V puó essere calcolata direttamente nell'ambito proiettivo introducendo la funzione di Hilbert proiettiva (che con abuso di notazione chiameremo con lo stesso simbolo). Si pone (si ricordi la def. 18.1)

$$K[x_0,\ldots,x_n]_s := \{p \in K[x_0,\ldots,x_n] | deg\ p = s\}$$

$$I_s := I \cap K[x_0,\ldots,x_n]_s$$

Definizione 18.4. *Se I é un ideale omogeneo la sua funzione di Hilbert proiettiva é*

$$F_I(s) := dim \frac{K[x_0,\ldots,x_n]_s}{I_s}$$

Siccome I é omogeneo segue subito dal lemma 12.4 che come spazi vettoriali si ha

$$\frac{K[x_0,\ldots,x_n]_{\leq s}}{I_{\leq s}} \simeq \oplus_{j=0}^{s} \frac{K[x_0,\ldots,x_n]_j}{I_j}$$

e quindi se $F_I^a(s)$ é la funzione di Hilbert affine abbiamo

$$F_I(s) = F_I^a(s) - F_I^a(s-1) \tag{18.2}$$

É facile verificare che se $P(s)$ é un polinomio di grado d allora $P(s) - P(s-1)$ é un polinomio di grado $d-1$. Quindi $degF_I(s) = degF_I^a(s) - 1$ ed in accordo con la def.18.3 e con (18.1) e (18.2) segue che se $V \subset \mathbf{P}^n$ allora

$$dimV = degF_{I(V)}(s) \tag{18.3}$$

Siccome $LT(I)$ é ancora un ideale omogeneo, abbiamo da (18.2) e dal teorema17.2 che per ogni ordine monomiale graduato

$$F_I(s) = F_I^a(s) - F_I^a(s-1) = F_{LT(I)}^a(s) - F_{LT(I)}^a(s-1) = F_{LT(I)}(s)$$

L'uguaglianza $F_I(s) = F_{LT(I)}(s)$ nell'ambito proiettivo (analoga del teorema 17.2) é vera per qualunque ordine monomiale, anche non graduato, ma non dimostreremo qui questo fatto.

Se si è interessati soltanto al calcolo della dimensione e non di tutto il polinomio di Hilbert l'algoritmo del paragrafo 17 può essere notevolmente semplificato. Scopo dei teoremi seguenti é descrivere questa semplificazione (sia nel caso affine che in quello proiettivo. L'algoritmo che ne risulta é esposto dopo il teorema 18.13. Cominciamo col notare che

$$V(x_{i_1}^{\alpha_1} \cdots x_{i_r}^{\alpha_r}) = \{x_{i_1} = 0\} \cup \ldots \cup \{x_{i_r} = 0\} = V(x_{i_1}) \cup \ldots \cup V(x_{i_r})$$

ed in generale la varietà di un ideale monomiale I è data dall'unione di certi sottospazi vettoriali di K^n visto come spazio vettoriale.

Definizione 18.5. *Sia I un ideale monomiale. Poniamo*

$$C(I) := \{\alpha \in \mathbf{Z}^n_{\geq 0} | \mathrm{x}^\alpha \notin \mathrm{I}\}$$

insieme dei monomi nel complemento di I.

$C(I)$ corrisponde a S del teor. 18.1.
Poniamo $e_1 = (1, 0, \ldots, 0), e_2 = (0, 1, 0, \ldots), \ldots, e_\mathrm{n} = (0, \ldots, 0, 1)$ corrispondenti ai monomi $x_1, x_2, \ldots, x_\mathrm{n}$. Definiamo i sottospazi coordinati di $\mathbf{Z}^n_{\geq o}$ come gli insiemi definiti da $< e_{i_1}, \ldots, e_{i_r} >_{\mathbf{Z}_{\geq 0}} \subset \mathbf{Z}^n_{\geq 0}$ per qualche $i_1 < \ldots < i_r$. Il teorema seguente afferma che i sottospazi vettoriali di $V(I)$ corrispondono ai sottospazi coordinati in $C(I)$.

Teorema 18.6. Sia I un ideale monomiale. Vale

$$W := \cap_{i \notin \{i_1, \ldots, i_\mathrm{r}\}} V(x_\mathrm{i}) \subset V(I) \quad \Leftrightarrow \quad < e_{i_1}, \ldots, e_{i_\mathrm{r}} >_{\mathbf{Z}_{\geq 0}} \subset C(I)$$

In particolare W é un sottospazio vettoriale di K^n di dimensione r.

Dimostrazione

$\Rightarrow$ W contiene il punto p di coordinate $\begin{cases} x_i = 0 \text{ se } i \notin \{i_1, \ldots, i_r\} \\ x_i = 1 \text{ se } i \in \{i_1, \ldots, i_r\} \end{cases}$. Quindi p$\in V(I)$. Se $\alpha \in <$ $e_{i_1}, \ldots, e_{i_\mathrm{r}} >_{\mathbf{Z}_{\geq 0}}$ abbiamo che x^α calcolato in p vale 1 e quindi $x^\alpha \notin I$, cioè $\alpha \in C(I)$.

$\Leftarrow$ Sia $< e_{i_1}, \ldots, e_{i_\mathrm{r}} >_{\mathbf{Z}_{\geq 0}} \subset C(I)$. Allora se $x^\alpha \in I$ in x^α compare una variabile diversa da $x_{i_1}, \ldots, x_{i_\mathrm{r}}$. Pertanto $x^\alpha \in I(W)$. Abbiamo provato che I$\subset I(W)$ e quindi W$\subset V(I)$ come volevamo.

Lemma 18.7. *Sia I un ideale monomiale. $C(I)$ é dato da una unione finita di traslati di sottospazi coordinati.*

Dimostrazione Se I é principale ed é generato dal monomio x^α allora

$$C(I) = \cup_{i=1}^n \left[\cup_{j=0}^{\alpha_i - 1} \{(\beta_1, \ldots, \beta_n) \in \mathbf{Z}^n_{\geq 0} | \beta_i = j\}\right] \tag{18.4}$$

Per induzione, se la proprietá é vera per gli ideali generati da $k-1$ monomi allora se $I = (m_1, \ldots, m_k)$ abbiamo

$$C(I) = C(m_1, \ldots, m_{k-1}) \cap C(m_k)$$

e quindi la proprietá é vera per I.

Lemma 18.8. *Sia I un ideale monomiale e sia W un sottospazio coordinato in $\mathbf{Z}^n_{\geq 0}$. Se $\exists \quad a \in \mathbf{Z}^n_{\geq 0}$ tale che $W + a \subset C(I)$ allora $W \subset C(I)$.*

Dimostrazione La proprietá é vera se I é principale (si veda (18.4)). Quindi la tesi si dimostra per induzione sul numero dei generatori di I come nel lemma precedente.

Proposizione 18.9. *Sia I un ideale monomiale. Il grado del polinomio di Hilbert di I coincide con la massima dimensione di un sottospazio vettoriale incluso in $V(I)$.*

Dimostrazione Per il teorema 18.6 la massima dimensione di un sottospazio incluso in $V(I)$ è uguale alla massima dimensione di un sottospazio coordinato in $C(I)$. Per il lemma18.8 la massima dimensione di un sottospazio coordinato incluso in $C(I)$ é uguale alla massima dimensione di un traslato di un sottospazio coordinato incluso in $C(I)$. Per il lemma 18.7 $C(I) = \cup_{i=1}^{p} C_i$ dove C_i sono traslati di sottospazi coordinati. Allora

$$P_I(s) = \sharp C(I)_{\leq s} = \sharp \left(\cup_{i=1}^{p} C_i\right)_{\leq s}$$

Notiamo che se C_j é un traslato di uno spazio coordinato di dimensione p allora $\sharp(C_j)_{\leq s}$ é un polinomio in s di grado p. Usando il lemma 17.7 per valutare $(\cup_{i=1}^{p} C_i)_{\leq s}$ ed il fatto che l'intersezione di due distinti traslati di sottospazi coordinati C_1 e C_2 é ancora un traslato di un sottospazio coordinato di dimensione minore di $max\ (dim\ C_1, dim\ C_2)$ segue la tesi.

Corollario 18.10. *Sia I un ideale di $K[x_1, \ldots, x_n]$ e sia fissato un ordine monomiale graduato. Il grado del polinomio di Hilbert di I coincide con la massima dimensione di un sottospazio vettoriale incluso in $V(LT(I))$.*

Dimostrazione Segue dalla prop. 18.9 e dal teorema di Macaulay 17.2.

Lemma 18.11. *Sia I un ideale. Allora*

$$LT(\sqrt{I}) \subset \sqrt{LT(I)}$$

Dimostrazione Se m é un monomio in $LT(\sqrt{I})$, allora $LT(f)|m$ per qualche $f \in \sqrt{I}$. Pertanto $\exists \quad q$ tale che $f^q \in I$ da cui $LT(f^q) = LT(f)^q | m^q$ e quindi $m^q \in LT(I)$ che é la tesi.

Lemma 18.12. *Sia I un ideale monomiale, allora*

$$deg\ P_I = deg\ P_{\sqrt{I}}$$

Dimostrazione Abbiamo $V(I) = V(\sqrt{I})$ e quindi la tesi segue dalla prop. 18.9.

Teorema 18.13. *Sia K algebricamente chiuso. Sia $V = V(I)$ una varietá algebrica. Allora*

$$dim\ V = deg\ P_I$$

Dimostrazione Per la definizione 18.3 abbiamo che $dim\ V = deg\ P_{I(V)}$. Dal teorema degli zeri di Hilbert 6.10 segue $I(V) = \sqrt{I}$. Quindi é sufficiente provare che

$$deg\ P_I = deg\ P_{\sqrt{I}}$$

Dalla inclusione $I \subset \sqrt{I}$ segue subito la disuguaglianza $deg\ P_{\sqrt{I}} \leq deg\ P_I$. Inoltre per il teorema 17.2 ed il lemma 18.12 segue

$$deg\ P_I = deg\ P_{LT(I)} = deg\ P_{\sqrt{LT(I)}}$$

Applicando il lemma 18.11 ed ancora il teorema 17.2 abbiamo

$$deg\ P_{\sqrt{LT(I)}} \leq deg\ P_{LT(\sqrt{I})} = deg\ P_{\sqrt{I}}$$

come volevamo.

Algoritmo per il calcolo della dimensione

Un semplice algoritmo per calcolare la dimensione di una varietá $V(I) \subset K^n$ su un campo K algebricamente chiuso basato sul corollario 18.10 e sul teorema 18.13 è il seguente: se $LT(I) = (m_1, \ldots, m_t)$ con m_i monomi poniamo $M_j = \{k \in \{1, \ldots, n\} | x_k$ divide $m_j\}$ per j= $1, \ldots, t$ (M_j è sempre non vuoto se I è proprio). Sia allora $\mathcal{M} = \{J \subset \{1, \ldots, n\} | J \cap M_j \neq \emptyset$ per j= $1, \ldots, t\}$. E' facile verificare che

$$dim V(I) = n - min\{|J| : J \in \mathcal{M}\}$$

Nel caso proiettivo la dimensione calcolata in questo modo va diminuita di 1

L'algoritmo precedente è implementato in COCOA col comando dim(R/I) che mostra la dimensione (affine) di V(I). In questo caso non bisogna aggiungere variabili ausiliarie a R. Questo è il comando più veloce per trovare la dimensione, e funziona bene anche per basi di Gröbner molto grosse (centinaia o migliaia di elementi) quando invece il calcolo esplicito del polinomio di Hilbert risulta molto laborioso.

Esercizio

Torniamo a studiare i tre esempi
i) I$\subset \mathbf{C}[x, y, z]$ con base di Gröbner data da (x^2y, y^3z, z^5, xz)
ii) I$\subset \mathbf{C}[x, y, z]$ con base di Gröbner data da $(x^2, xy, y^3, yz^{10}, z^7)$
iii) I$\subset \mathbf{C}[x_1, x_2, x_3, x_4]$ con base di Gröbner data da $(x_1^2, x_2^2, x_3^2, x_1x_4, x_2x_4, x_3x_4)$

Determinare dim V(I) (affine) mediante l'algoritmo precedente.
Risposta Nel caso i) dim V(I)= 1 e $\{1, 3\}$ oppure $\{2, 3\} \in \mathcal{M}$ di cardinalità minima.
Nel caso ii) dim V(I)= 0 e $\{1, 2, 3\}$ è l'elemento di $\mathcal{M}$ di cardinalità minima.
Nel caso iii) dim V(I)= 1 e $\{1, 2, 3\}$ è l'elemento di $\mathcal{M}$ di cardinalità minima.

Nell' esercizio precedente, nel caso i) $P_I(z) = 3z + 12$ e Reg(R/I)= 6. Nel caso ii) $P_I(z) = 28$, questo significa che V(I) è formato da 28 punti, contati con molteplicità opportune e Reg(R/I)= 8. Nel caso iii) $P_I(z) = 2z + 5$ e $Reg(R/I) = 2$

Definizione 18.14. *Sia V una varietá proiettiva e sia $P_{I(V)} = a_d t^d + \ldots$. Allora si pone*

$$deg\ V := a_d d!$$

Esempio. *Sia $f \in K[x_0, \ldots, x_n]$ un polinomio omogeneo di grado d. Consideriamo l'ipersuperficie $V(f) \subset \mathbf{P}^n$. Allora*

$$dim\ V(f) = n - 1 \qquad deg\ V(f) = d$$

Infatti per $s \geq d$

$$dim\ \frac{K[x_0, \ldots, x_n]_{\leq s}}{(f)_s} = \binom{n+s}{n} - \binom{n-d+s}{n} =$$

$$= \left(s^n + \frac{n(n-1)}{2 \cdot n!} s^{n-1} + \ldots\right) - \left(s^n + \frac{n(n-1) - 2dn}{2 \cdot n!} s^{n-1} + \ldots\right) = \frac{d}{(n-1)!} s^{n-1} + \ldots$$

Nel caso di varietá proiettive il polinomio di Hilbert e la funzione di Hilbert hanno una interpretazione coomologica (formula di Riemann-Roch).

I coefficienti del polinomio di Hilbert hanno un significato geometrico.

La definizione 18.14 mostra che il coefficiente di s^d definisce il grado di V. Se V(I)= C è una curva nonsingolare (dim(C)= 1) allora $P_I(s) = deg(C)s - g + 1$. C è omeomorfa come superficie di Riemann ad una sfera con g manici e g si dice il genere di C. In questo caso il genere può essere ricavato dal polinomio di Hilbert. In particolare g= 0 se e solo se C è razionale (o unirazionale), quindi è possibile stabilire dal polinomio di Hilbert (e quindi dalle equazioni che definiscono C usando gli algoritmi visti in precedenza) se C è razionale! Nel caso delle curve si ha $F_I(s) \leq P_I(s)\ \forall s \geq 0$.Se $S = V(J) \subset \mathbf{P}^n$ é una superficie (i.e. $dim = 2$) allora vale

$$p_J(t) = d\binom{t+2}{2} + (1 - g - d)(t + 1) + (p_a + g)$$

dove $d = deg\ S$, g é il genere di una curva tagliata su S da un iperpiano generico e p_a si dice il genere aritmetico di S.

Vogliamo adesso provare che il grado del polinomio di Hilbert di una varietá algebrica V é uguale al grado di trascendenza su K del campo delle funzioni razionali di V. Abbiamo cosí a disposizione una definizione alternativa di dimensione. Questo permette anche di verificare che quando $K = \mathbf{C}$ la definizione che abbiamo dato di dimensione coincide con quella usuale. Per semplicitá consideriamo solo il caso affine, lasciando al lettore le semplici modifiche necessarie nel caso proiettivo.

Ricordiamo che il grado di trascendenza su K di un campo K' che contiene K come sottocampo é uguale al massimo numero di elementi di K' algebricamente indipendenti su K (quando questo numero é finito).

Teorema 18.15. *Sia V una varietá e sia K algebricamente chiuso. Il grado del polinomio di Hilbert dell' ideale $I = I(V)$ é uguale al grado di trascendenza su K del campo delle funzioni razionali $K(V)$. Pertanto si puó scrivere*

$$dim\ V = deg\ tr_K\ K(V) \tag{18.5}$$

La (18.5) é presa spesso come definizione di dimensione. La definizione 18.3 ha il vantaggio di essere operativa.

Dimostrazione
1) $deg\ p_I \leq deg\ tr\ K(V)$
Sia $d = deg\ p_I$. Facciamo vedere che possiamo trovare d elementi di $K[V]$ che sono algebricamente indipendenti su K.
Infatti dal corollario 18.10 esistono $i_1 < \ldots < i_d$ compresi tra 1 e n tali che $W := \cap_{j \notin \{i_1,\ldots,i_d\}} V(x_j) \subset V(LT(I))$. Possiamo supporre, riordinando le indeterminate, che $\{i_1, \ldots, i_d\} = \{1, \ldots, d\}$. Mostriamo che $[x_1], \ldots, [x_d]$ sono algebricamente indipendenti su K. Sia p un polinomio a coefficienti in K tale che $p([x_1], \ldots, [x_d]) = [0]$. Quindi $[p(x_1, \ldots, x_d)] = [0]$ da cui

$$p(x_1, \ldots, x_d) \in I \tag{18.6}$$

Sia P il punto di coordinate $(1, \ldots, 1, 0, \ldots, 0)$ (le prime d coordinate uguali a 1). Allora $P \in W \subset V(LT(I))$. Quindi ogni monomio in $LT(I)$ si annulla in P e pertanto non puó dipendere soltanto da $x_1, \ldots, x_d$. Siccome $LT(I)$ é un ideale monomiale segue $LT(I) \cap K[x_1, \ldots, x_d] = 0$. Quindi

$$I \cap K[x_1, \ldots, x_d] = 0 \tag{18.7}$$

perché un elemento non nullo $f \in I \cap K[x_1, \ldots, x_d]$ darebbe $LT(f) \in LT(I) \cap K[x_1, \ldots, x_d]$. Da (18.6) e (18.7) segue immediatamente $p = 0$ come volevamo.

2) $deg\ p_I \geq deg\ tr\ K(V)$
Poniamo sempre $d = deg\ p_I$. Se $\phi_1, \ldots, \phi_r \in K(V)$ sono algebricamente indipendenti, dobbiamo provare che $r \leq d$. Possiamo supporre che $\phi_i = [f_i]/[f]$ con $[f_1], \ldots, [f_r], [f] \in K[V]$, $[f] \neq 0$. Sia $N = max\{deg\ f_1, \ldots, deg\ f_r, deg\ f\}$. Se $p \in K[y_1, \ldots, y_r]$ ha grado $\leq s$ allora $f^s p(f_1/f, \ldots, f_r/f)$ é un polinomio in $K[x_1, \ldots, x_n]$ di grado $\leq Ns$. Pertanto si puó definire il morfismo

$$\beta: K[y_1, \ldots, y_r]_{\leq s} \to \frac{K[x_1, \ldots, x_n]_{\leq Ns}}{I_{\leq Ns}}$$

dato da

$$\beta(p) := [f^s p(f_1/f, \ldots, f_r/f)]$$

Vogliamo provare che β é iniettiva. Sia pertanto p tale che $[f^s p(f_1/f, \ldots, f_r/f)] = 0$ Siccome $\frac{K[x_1,\ldots,x_n]_{\leq Ns}}{I_{\leq Ns}}$ si inietta in $K[V]$ e quindi in $K(V)$ abbiamo $[f]^s p(\phi_1, \ldots, \phi_r) = 0$ in $K(V)$ e quindi $p(\phi_1, \ldots, \phi_r) = 0$ in $K(V)$. Segue che β é iniettiva. Quindi

$$\binom{r+s}{r} = dim\ K[y_1, \ldots, y_r]_{\leq s} \leq P_I(Ns)$$

da cui $P_I(Ns)$ é un polinomio in s di grado $\geq r$ e quindi $deg\ p_I \geq r$ come volevamo.

Corollario 18.16. *Due varietá birazionalmente equivalenti hanno la stessa dimensione.*

19. RICHIAMI SUI MODULI NOETHERIANI E SUI MODULI GRADUATI

Sia A un anello commutativo con unità. Un gruppo abeliano M si dice un A-modulo se esiste una moltiplicazione $A \times M \to$ M (denotata con am per $a \in A, m \in M$) tale che

$$a(m+m') = am + am'$$
$$(a+a')m = am + a'm$$
$$(aa')m = a(a'm)$$
$$1m = m$$
$$\forall a, a' \in A,\ \forall m, m' \in M$$

Se A è uguale ad un campo K, M risulta quindi un K-spazio vettoriale.
Ogni anello è un modulo su se stesso e ogni ideale I$\subset A$ è in modo naturale un A-modulo. Se A $\stackrel{\mathrm{f}}{\to}$ B è un morfismo di anelli, B è un A-modulo definendo a$\cdot b = f(a)b$. Ogni gruppo abeliano è uno $\mathbf{Z} - modulo$ ponendo ng$= g + g + \ldots + g$ (n volte) $\forall n \geq 0$, $\forall g \in G$ e $(-1)g = -g$.

Un sottogruppo N$\subset M$ si dice un sottomodulo se A$\cdot N \subset N$. In particolare i sottomoduli di un anello visto come modulo su se stesso sono gli ideali. Se N$\subset M$ e' un sottomodulo è ben definito il modulo quoziente M$/N$. La somma diretta di A-moduli è in modo naturale un A-modulo. In particolare $A^r = A^{\oplus r}$ si dice A-modulo *libero di rango* r.

Esempio 19.1 Sia A un anello e siano $f_1, \ldots, f_{\mathrm{r}} \in A$.

$$Syz(f_1, \ldots, f_{\mathrm{r}}) = \{(g_1, \ldots, g_{\mathrm{r}}) \in A^r | \sum_{\mathrm{i}=1}^{\mathrm{r}} \mathrm{g_i f_i} = 0\}$$

è un A-modulo (sottomodulo di A^r) e si dice modulo delle sizigie su $f_1, \ldots, f_{\mathrm{r}}$. Ad esempio $(1,1,-x-y) \in Syz(x^2, y(y+2x), x+y) \subset K[x,y]^3$.

Un morfismo di A-moduli f:M $\to$ N è un morfismo di gruppi tale che $f(am) = af(m)$ $\forall a \in A$, $\forall m \in M$. Ker f (risp. Im f) risulta in modo naturale un sottomodulo di M (risp. N).

Sia M un A-modulo con A anello locale e $\mathcal{M} \subset A$ l'ideale massimale. Allora M$/\mathcal{M}M$ è in modo naturale un A$/\mathcal{M} - modulo$, quindi uno spazio vettoriale perchè A$/\mathcal{M}$ è un campo. Un risultato fondamentale in questo contesto è il

19.2 Lemma di Nakayama
$f_1, \ldots, f_{\mathrm{k}}$ generano M come A-modulo$\Leftrightarrow$ $[f_1], \ldots, [f_{\mathrm{k}}]$ generano M$/\mathcal{M}M$ come $A/\mathcal{M}$-spazio vettoriale
Dimostrazione $\Rightarrow$ è ovvia
$\Leftarrow$ Sia N il sottomodulo di M generato da $f_1, \ldots, f_{\mathrm{k}}$. Per ipotesi ogni m$\in M$ si può scrivere nella forma m$= \sum_{\mathrm{i}=1}^{\mathrm{k}} a_{\mathrm{i}} f_{\mathrm{i}} + r$ con $a_{\mathrm{i}} \in A$, r$\in \mathcal{M}M$. Quindi M$= N + \mathcal{M}M$. Vogliamo provare M$/N = 0$. Altrimenti siano $g_1, \ldots, g_{\mathrm{n}}$ generatori minimali di $\frac{M}{N} = \frac{N+\mathcal{M}M}{N} = \mathcal{M}\frac{M}{N}$.

Dunque $g_n = \sum_{i=1}^{n} b_i g_i$ in $\frac{M}{N}$ con $b_i \in \mathcal{M}$. Allora $(1-b_n)g_n = \sum_{i=2}^{n} b_i g_i$ in $\frac{M}{N}$. Siccome A è locale $1-b_n$ è invertibile e g_n risulta una combinazione lineare di $g_2, \ldots, g_n$ contro l'ipotesi di minimalità.

Successioni esatte Una successione di morfismi di A-moduli

$$\ldots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \longrightarrow \ldots$$

si dice *esatta* se Im f_{i-1} = Ker f_i $\forall i$. In particolare quindi la composizione di due morfismi successivi è zero, cioè $f_i \circ f_{i-1} = 0$. Questa ultima condizione equivale a Im $f_{i-1} \subset Ker\ f_i$.

Ad esempio, dato f:M $\to$ N abbiamo

$$\text{f iniettivo} \Leftrightarrow 0 \to \text{M} \to \text{N esatta}$$
$$\text{f suriettivo} \Leftrightarrow \text{M} \to \text{N} \to 0 \text{ esatta}$$

Una successione esatta di tre moduli

$$0 \to \text{M} \to \text{N} \to \text{P} \to 0$$

si dice *successione esatta corta.* Una successione esatta

$$\ldots \to M_{i-1} \xrightarrow{f_{i-1}} M_i \xrightarrow{f_i} M_{i+1} \xrightarrow{f_{i+1}} \ldots \tag{19.1}$$

si spezza in tante successioni esatte corte

$$\ldots$$
$$0 \to \text{Ker } f_{i-1} \to M_{i-1} \to \text{Im } f_{i-1} \to 0$$
$$0 \to \text{Ker } f_i \to M_i \to \text{Im } f_i \to 0$$
$$0 \to \text{Ker } f_{i+1} \to M_{i+1} \to \text{Im } f_{i+1} \to 0$$
$$\ldots$$

dove la condizione di esattezza fa sì che l'ultimo termine di una successione sia uguale al primo termine della successiva.

Viceversa le successioni esatte corte

$$\ldots$$
$$0 \to M_{i-1} \to N_{i-1} \to M_i \to 0$$
$$0 \to M_i \to N_i \to M_{i+1} \to 0$$
$$0 \to M_{i+1} \to N_{i+1} \to M_{i+2} \to 0$$
$$\ldots$$

si "rincollano" nella successione esatta lunga

$$\ldots \to N_{i-1} \to N_i \to N_{i+1} \to \ldots$$

Esercizio Dati M, N, P A-moduli con A locale e $\mathcal{M} \subset A$ massimale, si usi il lemma di Nakayama per provare che

M $\to$ N $\to$ P $\to 0$ è esatta $\Leftrightarrow$ M/$\mathcal{M}M \to$ N/$\mathcal{M}N \to$ P/$\mathcal{M}P \to 0$ è esatta

(Questo fatto si esprime dicendo che il funtore M$\mapsto M/\mathcal{M}M$ è esatto a destra)

Esercizio 19.3. *Sia K un campo. Se*

$$0 \longrightarrow M_0 \longrightarrow M_1 \longrightarrow \ldots \longrightarrow M_p \longrightarrow 0$$

é una successione esatta di spazi vettoriali su K (K-moduli), provare che

$$\sum_{i=0}^{p}(-1)^i dim\ M_i = 0$$

Suggerimento: si cominci a provare il caso $p = 2$.

Osservazione. *Se $0 \to M/\mathcal{M}M \to N/\mathcal{M}N$ è esatta anche $0 \to M \to N$ è esatta ma non vale il viceversa (controesempio istruttivo: M= N = A anello locale delle funzioni razionali in un intorno di p= $(p_1, \ldots, p_n) \in K^n$ dove K è un campo, cioè gli elementi di A hanno la forma $\frac{f(x_1,\ldots,x_n)}{g(x_1,\ldots,x_n)}$ con $g(p_1, \ldots, p_n) \neq 0$, il morfismo è dato dalla moltiplicazione per $x_1 - p_1$).*

Osservazione Se nella successione esatta (19.1) si ha $M_{i-1} = M_{i+1} = 0$ segue $M_i = 0$. Se si ha $M_{i-1} = M_{i+2} = 0$ segue $M_i \simeq M_{i+1}$. Questa osservazione è semplice ma molto utile.

Proposizione 19.4 Sia M un A-modulo. Sono condizioni equivalenti:
i) ogni catena ascendente di sottomoduli è stazionaria
ii) ogni sottomodulo è finitamente generato
Dimostrazione i)$\Rightarrow$ *ii)* Sia per assurdo N$\subset M$ non finitamente generato. Allora esiste una successione $\{m_i\}$ di elementi di N tali che $(m_1) \subset (m_1, m_2) \subset (m_1, m_2, m_3) \subset \ldots$ e tutte le inclusioni sono strette.
ii) $\Rightarrow$ i) Se $M_1 \subset M_2 \subset \ldots \subset M_i \subset \ldots$ è una catena di sottomoduli si considera $\cup M_i$ che è un sottomodulo finitamente generato per ipotesi. Sia $\cup M_i = (m_1, \ldots, m_t)$ con $m_i \in M_{k_i}$ e sia k= $max(k_1, \ldots, k_t)$. Segue $M_k = M_{k+1} = M_{k+2} = \ldots$ come volevamo

Definizione 19.5 Un A-modulo che soddisfa i) o ii) si dice *noetheriano*. In particolare un anello noetheriano è un modulo noetheriano su se stesso.

Teorema 19.6 Sia $0 \to M_1 \xrightarrow{\alpha}$ M $\xrightarrow{\beta} M_2 \to 0$ esatta.
M è noetheriano $\Leftrightarrow$ M_1, M_2 sono noetheriani

Dimostrazione
$\Rightarrow$ Ogni catena ascendente in M_1 è una catena ascendente in M e dunque è stazionaria. Se $\{N_i\}$ è una catena ascendente in M_2 allora $\beta^{-1}(N_i)$ è stazionaria per ipotesi. Siccome $\beta(\beta^{-1}(N_i)) = N_i$ segue la tesi.
$\Leftarrow$ Sia L_n una catena ascendente in M. Allora $L_n \cap M_1$ è stazionaria in M_1 e $\beta(L_n)$ è stazionaria in $M_2 \simeq M/M_1$. Quindi se $n \geq N$ segue

a) $L_n + M_1 = L_{n+1} + M_1$
b) $L_n \cap M_1 = L_{n+1} \cap M_1$

Sia $l_{n+1} \in L_{n+1}$. Da a) segue $l_{n+1} = l_n + m$ con $l_n \in L_n$, m$\in M_1$. Quindi m= $l_{n+1} - l_n \in L_{n+1} \cap M_1 = L_n \cap M_1$ per b), da cui $l_{n+1} \in L_n$. Pertanto L_n è stazionaria.

Corollario 19.7 Se $\{M_i\}_{i=1,\ldots,k}$ sono A-moduli noetheriani allora $\oplus_{i=1}^{k} M_i$ è noetheriano

Dimostrazione Per induzione su k dalla successione

$$0 \to \oplus_{i=1}^{k-1} M_{\mathrm{i}} \to \oplus_{i=1}^{k} M_{\mathrm{i}} \to M_{\mathrm{k}} \to 0$$

Corollario 19.8 Sia A un anello noetheriano e M un A-modulo.

M è noetheriano $\Leftrightarrow$ M è un quoziente del modulo libero A^r per qualche r$\in \mathbf{N}$.

(la seconda condizione equivale a dire che M è finitamente generato).

Dimostrazione $\Leftarrow$ A^r è noetheriano per il corollario precedente ed ogni quoziente di A^r è noetheriano per il teorema 19.6.

$\Rightarrow$ Se M è generato da $m_1, \ldots, m_{\mathrm{k}}$ il morfismo $A^k \to M$ dato da $(a_1, \ldots, a_k) \mapsto \sum_{i=1}^{k} a_i m_i$ é suriettivo.

In particolare il corollario precedente caratterizza tutti i moduli noetheriani M sull'anello $S = K[x_0, \ldots, x_{\mathrm{n}}]$. Ogni M appare in una successione esatta

$$0 \longrightarrow K \longrightarrow S^r \longrightarrow M \longrightarrow 0$$

dove K é un sottomodulo di S^r. Lo studio degli S-moduli noetheriani si riconduce quindi a quello dei sottomoduli di S^r.

Ricordiamo che un anello A si dice *graduato* se $A = \oplus_{d \in \mathbf{N}} A_d$ con A_d sottogruppi tali che $A_d \cdot A_e \subset A_{d+e} \quad \forall d, e \in \mathbf{N}$. L'esempio principale di anello graduato é dato da $S = K[x_0, \ldots, x_n]$. Gli elementi di A_d si dicono di grado d.

Sia A un anello graduato, un A-modulo M si dice graduato se $M = \oplus_{d \in \mathbf{Z}} M_d$ e vale $A_d M_e \subset M_{d+e}$. In particolare S é un S-modulo graduato.

Definizione 19.9. *Sia M un modulo graduato e sia $d \in \mathbf{Z}$. Il modulo graduato $M(d)$ é un modulo isomorfo a M con graduazione $M(d)_e := M_{d+e}$*

Un morfismo di moduli graduati $f\colon M \to N$ é un morfismo di moduli tale che $f(M_d) \subset N_d$. Un A-modulo graduato libero di rango r é per definizione isomorfo a $\oplus_{i=1}^{r} A(d_i)$ per qualche $d_i \in \mathbf{Z}$.

Esempi 19.10. *Se $a \in S_d$ allora $S \xrightarrow{f} S(d)$ definito da $f(s) := as$ é un morfismo di moduli graduati. Un morfismo di moduli graduati $F\colon \oplus_{i=1}^{r} S(a_i) \to \oplus_{j=1}^{s} S(b_j)$ é rappresentato da una matrice $s \times r$ a coefficienti polinomi omogenei. Precisamente il coefficiente di posto (j, i) é un polinomio omogeneo di grado $b_j - a_i$. Notiamo che se conosciamo i gradi degli elementi di una riga e di una colonna sono individuati i gradi degli elementi di tutta la matrice.*

20. SIZIGIE

Esempio 20.1 Sia A= $K[x_1, \ldots, x_{\mathrm{n}}]$ e sia I= $(f_1, \ldots, f_{\mathrm{k}})$ un ideale di A. Si ha al-

lora la successione esatta $0 \to \mathrm{syz}(f_1, \ldots, f_\mathrm{k}) \to A^k \to \mathrm{I} \to 0$, da cui per il teorema19.6 $\mathrm{syz}(f_1, \ldots, f_\mathrm{k})$ è noetheriano (si veda l'esempio19.1). In particolare esistono $(g_1^j, \ldots g_\mathrm{k}^j) \in syz(f_1, \ldots, f_\mathrm{k})$ (j= $1, \ldots, s$) generatori. Quindi se $\sum_{i=1}^k g_i f_i = 0$ segue $(g_1, \ldots, g_\mathrm{k}) = \sum_{j=1}^s a_j(g_1^j, \ldots, g_k^j)$ cioè una qualunque sizigia è combinazione lineare di un numero finito di sizigie fissate. Questo fatto fu provato per la prima volta da Hilbert (Math. Ann. 1890) e la sua soluzione fu una delle motivazioni del Basissatz (teor. 1.2).

Risoluzioni libere Sia A un anello noetheriano e M un A-modulo noetheriano. Pertanto abbiamo una risoluzione $0 \to K_1 \to F_0 \to \mathrm{M} \to 0$ con F_0 libero, dove K_1 è il modulo delle sizigie sui generatori di M. Anche K_1 è noetheriano, quindi si ottiene $0 \to K_2 \to F_1 \to K_1 \to 0$ dove F_1 è libero e K_2 è il modulo delle sizigie sui generatori di K_1 (sizigie delle sizigie). Continuando in questo modo si ottiene una risoluzione libera

$$\ldots \to F_\mathrm{n} \to \ldots \to F_2 \to F_1 \to F_0 \to M \to 0$$

La risoluzione non è unica ma dipende dai generatori scelti. In generale la risoluzione precedente continua a sinistra con infiniti termini.

20.2 Teorema delle sizigie di Hilbert Sia S= $K[x_1, \ldots, x_\mathrm{n}]$ e sia M un S-modulo finitamente generato.

i) Esiste una risoluzione libera della forma
$$0 \to F_\mathrm{n} \to \ldots \to F_2 \to F_1 \to F_0 \to \mathrm{M} \to 0$$
ii) Se M é graduato si puó scegliere la risoluzione in i) formata da moduli graduati liberi e da morfismi di moduli graduati.

Dimostreremo alla fine di questo paragrafo il teorema 20.2.

Si dice che la lunghezza della risoluzione precedente è n, e si chiama dimensione proiettiva di M (pd(M)) la minima lunghezza di una risoluzione libera di M. In particolare M è libero se e solo se pd(M)= 0 e pd misura "di quanto M non è libero". Il teorema delle sizigie afferma che dopo n passi le sizigie non hanno relazioni, cioè il modulo delle sizigie è libero. Dunque pd(M)$\leq n$ per ogni S-modulo M. Dimostreremo il teorema delle sizigie alla fine di queste note, insieme ad un algoritmo di calcolo per le risoluzioni libere.

In particolare il teorema delle sizigie si applica al caso in cui M è un ideale di S. In questo caso si cercano quindi le sizigie di un insieme di polinomi $\{f_1, \ldots, f_\mathrm{k}\}$. Notiamo che i morfismi che appaiono nelle risoluzioni libere di S-moduli sono rappresentati da matrici con coefficienti polinomi e le sizigie sono le relazioni tra le righe di queste matrici.

Il teorema delle sizigie è falso per moduli noetheriani su anelli diversi da $\mathrm{K}[x_1, \ldots, x_\mathrm{n}] = S$. Ad esempio si può provare che l'ideale $I = (x_0, x_2, x_4)$ nell'anello

$$S' = K[x_0, x_1, \mathrm{x}_2, \mathrm{x}_3, \mathrm{x}_4, \mathrm{x}_5]/(\mathrm{x}_0\mathrm{x}_1 - \mathrm{x}_2\mathrm{x}_3 + \mathrm{x}_4\mathrm{x}_5)$$

non ammette una risoluzione libera finita di S'-moduli. Geometricamente V(I) è un piano

proiettivo nella quadrica di Klein. Questo esempio è legato alla rappresentazione spin del gruppo ortogonale.

Esempio Il campo K è un S-modulo ed il nucleo del morfismo $S \to K \to 0$ è formato dall'ideale $I = (x_1, \ldots, x_{\mathrm{n}})$. Il nucleo W del morfismo $S^n \to I \to 0$ è generato dagli elementi $(x_2, -x_1, 0, \ldots, 0), (x_3, 0, -x_1, 0, \ldots, 0), \ldots$ e si ha quindi

$$S^{\binom{\mathrm{n}}{2}} \to \mathrm{W} \to 0$$

Continuando in questo modo si ottiene la risoluzione di lunghezza n

$$0 \to S^{\binom{\mathrm{n}}{\mathrm{n}}} \to \mathrm{S}^{\binom{\mathrm{n}}{\mathrm{n-1}}} \to \ldots \to \mathrm{S}^{\binom{\mathrm{n}}{2}} \to \mathrm{S}^{\binom{\mathrm{n}}{1}} \to \mathrm{S} \to \mathrm{K} \to 0 \qquad (20.1)$$

che è un caso particolare del cosiddetto *complesso di Koszul*. Si può provare che $\mathrm{pd(K)} = n$, cioè il massimo consentito dal teorema delle sizigie.
Nel contesto dei moduli graduati la (20.1) diventa

$$0 \longrightarrow S(-n) \longrightarrow S(-n+1)^{\binom{n}{n-1}} \longrightarrow \ldots \longrightarrow S(-2)^{\binom{n}{2}} \longrightarrow S(-1)^{\binom{n}{1}} \longrightarrow S \longrightarrow K \longrightarrow 0 \qquad (20.2)$$

Osservazione Se A è locale è ben definita una unica *risoluzione minimale* di ogni A-modulo finitamente generato M (vedi ad esempio E.Kunz, Commutative algebra and algebraic geometry). La risoluzione minimale

$$\ldots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

ha la proprietá che quozientando per l'ideale massimale $\mathcal{M} \subset A$ tutti i morfismi indotti

$$\frac{F_i}{\mathcal{M}F_i} \to \frac{F_{i-1}}{\mathcal{M}F_{i-1}}$$

sono nulli. In questo caso i ranghi dei moduli liberi che appaiono nella risoluzione minimale si dicono i numeri di Betti di M. Considerazioni analoghe si possono ripetere quando M è un S-modulo graduato. In questo caso una risoluzione libera é minimale se quozientando per l'ideale massimale irrilevante $(x_1, \ldots, x_n)$ si ottengono morfismi nulli. Questo equivale a chiedere che le matrici associate ai morfismi (si veda l'esempio 19.10) non contengano coefficienti costanti non nulli.

Esempi. *Se W consiste nell'unione di tre punti non allineati in $\mathbf{P}^2$ allora il modulo graduato $I(W)$ ha risoluzione minimale data da*

$$0 \longrightarrow S(-3)^2 \longrightarrow S(-2)^3 \longrightarrow I(W) \longrightarrow 0$$

In un opportuno sistema di coordinate omogenee (x, y, z) i morfismi della risoluzione precedente sono dati da

$$0 \longrightarrow S(-3)^2 \xrightarrow{\begin{pmatrix} -y & 0 \\ 0 & -x \end{pmatrix}} S(-2)^3 \xrightarrow{(xy \quad xz \quad yz)} I(W) \longrightarrow 0$$

Se W' consiste nell'unione di tre punti (distinti) allineati in $\mathbf{P}^2$ allora il modulo graduato $I(W')$ ha risoluzione minimale data da

$$0 \longrightarrow S(-4) \longrightarrow S(-1) \oplus S(-3) \longrightarrow I(W') \longrightarrow 0$$

In questo secondo caso i morfismo sono dati da

$$0 \longrightarrow S(-4) \xrightarrow{\begin{pmatrix} yz(y-z) \\ -x \end{pmatrix}} S(-1) \oplus S(-3) \xrightarrow{(x \quad yz(y-z))} I(W') \longrightarrow 0$$

Se M é un S-modulo graduato finitamente generato allora

$$F_M(t) = dim\ M_t$$

si dice funzione di Hilbert (proiettiva) di M.
Si puó provare che $F_M(s)$ é un polinomio numerico per $s \gg 0$ (che si dice polinomio di Hilbert di M).
In entrambi gli esempi precedenti il polinomio di Hilbert (proiettivo) é lo stesso, infatti

$$p_{I(W)}(t) = p_{I(W')}(t) = \binom{t+2}{2} - 3 = \frac{1}{2}(t^2 + 3t - 4)$$

(vedi esempio 17.4)

Esercizio. *Sia $S = K[x_0, \ldots, x_n]$. Provare che*

$$F_{S(d)}(t) = \begin{cases} \binom{d+t+n}{n} & \text{se } t \geq -d-n \\ 0 & \text{se } t \leq -d-n-1 \end{cases}$$

Esercizio. *Se*

$$0 \longrightarrow M_0 \longrightarrow M_1 \longrightarrow \ldots \longrightarrow M_p \longrightarrow 0$$

é una successione esatta di S-moduli graduati provare che

$$\sum_{i=0}^{k} f_{M_i}(t) = 0 \qquad \sum_{i=0}^{k} P_{M_i}(t) = 0$$

Suggerimento: si tenga conto dell' eserc. 19.3

Osservazione. *Le funzioni ed i polinomi di Hilbert possono essere calcolati anche dalle risoluzioni, ad esempio*

$$p_{I(W)}(t) = 3p_{S(-2)}(t) - 2p_{S(-3)}(t) = 3\binom{t}{2} - 2\binom{t-1}{2} = \frac{1}{2}(t^2 + 3t - 4)$$

Per quanto riguarda le funzioni di Hilbert (proiettive) abbiamo

$$F_{I(W)}(t) = p_{I(W)}(t) \quad per\ t \geq 1$$

$$F_{I(W)}(t) = 0 \qquad per\ t \leq 0$$

mentre

$$F_{I(W')}(t) = p_{I(W')}(t) \quad \text{per } t \geq 2$$

$$F_{I(W')}(1) = 1$$

$$F_{I(W')}(t) = 0 \qquad \text{per } t \leq 0$$

I moduli $I(W)$ e $I(W')$ hanno quindi regolaritá diversa.
I gradi che appaiono nella risoluzione minimale (graduata) di un modulo graduato M si dicono ancora i numeri di Betti di M.
Le risoluzioni libere di ideali omogenei associati a varietà proiettive riflettono proprietà geometriche delle varietà stesse. Questo legame è oggetto attuale di ricerca (congetture di Green).

Per dimostrare il teorema delle sizigie è necessario estendere la teoria delle basi di Gröbner al contesto più generale dei sottomoduli di S^m. Indichiamo con e_{i} l'elemento $(0,\ldots,1,\ldots,0) \in S^m$ (1 al i-esimo posto) e sia $E^m = \{e_1,\ldots,e_{\mathrm{m}}\} \subset \mathbf{Z}^m_{\geq 0}$. Un monomio di S^m è un elemento della forma $\mathrm{m}e_{\mathrm{i}}$ con m monomio in S. Quindi i monomi di S^m sono associati in modo naturale agli elementi di $\mathbf{Z}^n_{\geq 0} \times E^m \subset \mathbf{Z}^{n+m}_{\geq 0}$. Un *sottomodulo monomiale* di S^m è per definizione un sottomodulo generato da monomi. Analogamente a quanto visto per gli ideali (prop. 2.6) si può verificare che esiste unica base minimale di monomi per sottomoduli monomiali. Per la noetherianità tale base è finita e può essere estratta da un qualunque insieme di monomi generatori.

Esercizio Sia M un sottomodulo monomiale di S^m. Allora
f$\in M \Leftrightarrow$ ogni termine di f appartiene a M

Cenno agli ordini monomiali per moduli

E' definito in S^m (e quindi in ogni suo sottomodulo) un *ordine parziale naturale* sui monomi dato da $\mathrm{m}e_{\mathrm{i}} \mid \mathrm{m}'e_{\mathrm{j}}$ se e solo se m $\mid$ m$'$ e i$= j$. Se i monomi sono identificati con a,b $\in \mathbf{Z}^n_{\geq 0} \times E^m \subset \mathbf{Z}^{n+m}_{\geq 0}$ questo equivale a dire che a divide b se e solo se $a_1 \leq b_1,\ldots,a_{\mathrm{n+m}} \leq b_{\mathrm{n+m}}$. Un ordine $<$ sui monomi di S^m si dice compatibile con la moltiplicazione se $a < b$ implica $ac < bc\ \forall a,b \in S^m$, c$\in S$.

La proposizione seguente generalizza il corollario 1.9.
Proposizione 20.3 Sia $>$ un ordine sui monomi di S^m che sia totale e compatibile con la moltiplicazione. Sono equivalenti:
i) $>$ è un buon ordinamento
ii) $>$ raffina l'ordine parziale naturale

Dimostrazione i)$\Rightarrow$ *ii)* se ii) non è verificata esiste $x^\alpha e_\mathrm{i} \mid x^\beta e_\mathrm{i}$ con $\alpha > \beta$. Quindi $x^\beta = x^\alpha x^\gamma$ con $\gamma < 0$ (ordine indotto su $\mathbf{Z}^n_{\geq 0}$) e quindi $1 > x^\gamma$. Allora la catena $1 > x^\gamma > x^{2\gamma} > \ldots > x^{n\gamma}$ non ammette minimo.
ii)$\Rightarrow$ *i)* se A è un qualunque insieme di monomi sia $\{x^{\alpha_1} e_{i_1}, \ldots, x^{\alpha_\mathrm{k}} e_{i_\mathrm{k}}\}$ con $x^{\alpha_1} e_{i_1} < \ldots < x^{\alpha_\mathrm{k}} e_{i_\mathrm{k}}$ un insieme di generatori estratto da A per il sottomodulo generato da A. Allora $x^{\alpha_1} e_{i_1}$ è il minimo di A.

Definizione 20.4 Un ordine sui monomi di S^m che sia totale, compatibile con la moltiplicazione e soddisfi i) o ii) della prop. 20.3 si dice un *ordine monomiale*. Analogamente al caso degli elementi di S, se f$\in S^m$ è definito il *leading term* LT(f) rispetto ad un ordine monomiale.

Un esempio di ordine monomiale su S^m è il LEX secondo cui $a < b$ se e solo se il primo coeff. $\neq 0$ (da sinistra) di $a - b \in \mathbf{Z}^{n+m}$ è negativo. Quindi se $m, m' \in S$ con $m < m'$ nell'usuale LEX si ha $me_\mathrm{i} < m'e_\mathrm{j}$ $\forall i, j$, mentre ad esempio $xe_1 > xe_2 > \ldots > xe_\mathrm{n}$. Analogamente si possono definire DEGLEX e DEGREVLEX.

Molte proprietà viste per gli ideali di S si estendono in modo naturale ai sottomoduli di S^m. Vediamo alcuni risultati, lasciando al lettore i dettagli.

Sia fissato un ordine monomiale su S^m. Se M è un sottomodulo di S^m è definito il sottomodulo monomiale LT(M), generato da LT(f) per f$\in M$. Un insieme di generatori $f_1, \ldots f_\mathrm{k}$ di M tale che $\mathrm{LT}(f_1), \ldots LT(f_\mathrm{k})$ generano LT(M) si dice *base di Gröbner* per M.

Si può definire un algoritmo di divisione in S^m come nel caso dei polinomi (si veda il teorema 1.12). In particolare se divido f$\in S^m$ per $f_1, \ldots f_\mathrm{k} \in S^m$ si ha f$= \sum_{i=1}^{k} q_\mathrm{i} f_\mathrm{i} + r$ con $q_\mathrm{i} \in S$, r$\in S^m$, nessun termine di r è divisibile per $\mathrm{LT}(f_\mathrm{i})$ e $\mathrm{LM}(q_\mathrm{i} f_\mathrm{i}) \leq LM(f)$. L'algoritmo termina sempre per il buon ordinamento. Nel caso in cui si divide per una base di Gröbner $\{g_1, \ldots g_\mathrm{k}\}$ di M$\subset S^m$ si ottiene che dato f$\in S^m$, $\exists! g \in (g_1, \ldots, g_\mathrm{k})$, r$\in S^m$ tali che $f = g + r$ e nessun termine di r è divisibile per $LT(g_\mathrm{i})$ (analogo del teorema 2.11). Vale quindi il
20.5 Criterio di appartenenza per i moduli (vedi coroll. 2.13 e algoritmo 3.3)

$$f \in M \quad \Leftrightarrow \quad \bar{\mathrm{f}}^{G} = 0$$

($\bar{\mathrm{f}}^{G}$ é il resto della divisione per una base di Gröbner G di M)

Siano f,g$\in S^m$, con un ordine moniomiale fissato e sia LT(f)$= c_1 f' e_\mathrm{i}$. LT(g)$= c_2 g' e_\mathrm{j}$ con $c_1, c_2 \in K$, f', g' monomi. Sia $x^\gamma = m.c.m.(f', g')$. Poniamo
Definizione 20.6.

$$S(f,g) := \begin{cases} 0 & \text{se } i \neq j \\ \frac{x^\gamma}{c_1 f'} f - \frac{x^\gamma}{c_2 g'} g & \text{se } i = j \end{cases}$$

In particolare $\mathrm{LT}(\frac{x^\gamma}{c_1 f'} f) = LT(\frac{x^\gamma}{c_2 g'} g) = x^\gamma e_\mathrm{i}$ e questi termini si cancellano, quindi

$$LT(S(f,g)) < x^\gamma e_\mathrm{i}$$

Vale ancora l'analogo del teorema 3.1

20.7 Criterio di Buchberger per i moduli Siano $g_1, \ldots, g_t$ generatori di M$\subset S^m$.

$$\text{G}= \{g_1, \ldots, g_t\} \text{ è base di Gröbner per M} \Leftrightarrow \overline{\text{S}(g_i, g_j)}^{G} = 0 \ \forall i, j$$

Il criterio dà un algoritmo efficiente per calcolare una base di Gröbner da un insieme di generatori G aggiungendo successivamente a G gli eventuali resti non nulli delle divisioni degli elementi $\text{S}(g_i, g_j)$ per G. Trovata una base di Gröbner si può poi estrarre l'unica base di Gröbner ridotta. Il lettore puó provare a dimostrare il criterio di Buchberger per i moduli utilizzando i teoremi successivi di questo capitolo. I dettagli sono in [E].

Questo algoritmo è implementato in Cocoa. Un modulo M$\subset S^m$ è definito dalle righe di una matrice con m colonne ed il comando gbasis(M) fornisce la base di Gröbner ridotta. Il comando mod non dà il resto in questo caso, però si può ugualmente verificare l'appartenenza di un elemento ad un sottomodulo di S^m calcolando le sizigie come vedremo.

Eercizio. *(generalizzazione del teor. 17.8) Sia M un S-modulo graduato finitamente generato. Provare che $F_M(s)$ é un polinomio numerico per $s \gg 0$.*

I comandi $Hilbert(M)$ e $Hilbertfn(M)$ sono implementati in CoCoA anche nel caso di sottomoduli $M \subset S^r$.

Definizione 20.8 Abbiamo S$= K[x_1, \ldots, x_n]$ e poniamo $S_k = K[x_{k+1}, \ldots, x_n]$. Se M$\subset S^m$ sia $M_k = M \cap (S_k)^m$ il *k-esimo modulo di eliminazione.*

Teorema 20.9 Se G è una base di Gröbner per M rispetto all'ordine monomiale LEX allora $G_k = G \cap (S_k)^m$ è base di Gröbner per M_k.
La dimostrazione è analoga al caso degli ideali di S (teor. 4.2).

L'eliminazione di variabili è utile anche per calcolare l'intersezione di sottomoduli di S^m, come nel caso degli ideali di S. Siano infatti $M_1, M_2 \subset S^m$ e consideriamo S$\subset K[x_1, \ldots, x_n, t]$ (t variabile ausiliaria). Sia tM_1 il sottomodulo di $\text{K}[x_1, \ldots, x_n, t]^m$ generato dagli elementi tm com m$\in M_1$ e analogamente consideriamo $(1-t)M_2 \subset K[x_1, \ldots, x_n, t]^m$. E' facile verificare la formula $M_1 \cap M_2 = [tM_1 + (1-t)M_2] \cap S^m$ (analoga della prop. 4.3) e quindi l'intersezione $M_1 \cap M_2$ può essere calcolata eliminando la variabile t usando il teorema precedente.

Osserviamo a questo proposito che i comandi Elim e Intersect di Cocoa sono implementati anche nel caso di sottomoduli di S^m.

Calcolo delle sizigie

Definizione 20.10. *Siano $m_1, \ldots, m_t$ termini in S^m, quindi $m_i = c_i x^{\alpha_i} e_{k(i)}$. Per ogni coppia di indici* i,j *tali che* k(i) = k(j) *poniamo* $m_{ij} = \frac{m.c.m.(x^{\alpha_i}, x^{\alpha_j})}{c_j x^{\alpha_j}}$ *allora* $S(m_i, m_j) = m_{ji} m_i - m_{ij} m_j = 0$ *e quindi*

$$\tau_{ij} := m_{ji} e_i - m_{ij} e_j \in Syz(m_1, \ldots, m_t) = \{ \sum h_i e_i | \sum h_i m_i = 0 \}.$$

Proposizione 20.11 Con le notazioni della def. 20.10 gli elementi τ_{ij} $\forall i, j$ tali che $i < j$ e $k(i) = k(j)$ generano Syz$(m_1, \ldots, m_t)$

Dimostrazione E' sufficiente provare la tesi quando $m_1, \ldots, m_{\rm t} \in S$ (cioè quando m= 1). Sia T il sottomodulo di Syz$(m_1, \ldots, m_{\rm t})$ generato da $\tau_{\rm ij}$. Se h= $(h_1, \ldots, h_{\rm t}) \in Syz(m_1, \ldots, m_{\rm t})$ definiamo

$$\delta(h) = \max_{\rm i}(\text{multigrado}(h_{\rm i} m_{\rm i}))$$

Se per assurdo $Syz(m_1, \ldots, m_t) \setminus T \neq \emptyset$ scegliamo $h \in Syz \setminus T$ con minimo $\delta(h)$. Consideriamo gli indici v tali che multigrado$(\mathrm{LT}(h_{\rm v}) m_{\rm v}) = \delta$. Quindi $\sum LT(h_{\rm v}) m_{\rm v} = 0$ e nel lemma 20.12 vedremo che $h' = \sum LT(h_{\rm v}) e_{\rm v} \in T$. Ma $\delta(h - h') < \delta(h)$ da cui una contraddizione.

Lemma 20.12. *(generalizzazione del lemma 2.17) Con le notazioni della dim. della prop. 20.11 se* $\sum_{v=1}^{k} LT(h_v) m_v = 0$ *e* $x^{\delta} = LM(h_v) LM(m_v) \quad \forall v = 1, \ldots, k$ *allora* $h' := \sum_{v=1}^{k} LT(h_v) e_v \in T$.

Dimostrazione Poniamo $LT(h_v) = \phi_v LM(h_v)$ e $m_v = c_v LM(m_v)$. Per ipotesi $\sum_{v=1}^{k} \phi_v c_v = 0$. Sia

$$x^{\gamma_{vs}} := m.c.m.(LM(h_v), LM(h_s))$$

in modo che $m_{vs} = \frac{x^{\gamma_{vs}}}{c_s LM(m_s)}$. Abbiamo

$$tau_{ij} = m_{ji} e_i - m_{ij} e_j = \frac{x^{\gamma_{ji}} e_i}{c_i LM(m_i)} - \frac{x^{\gamma_{ij}} e_j}{c_j LM(m_j)}$$

da cui

$$x^{\delta - \gamma_{ij}} \tau_{ij} = \frac{LM(h_i) e_i}{c_i} - \frac{LM(h_j) e_j}{c_j} \tag{20.3}$$

Pertanto abbiamo

$$h' = \sum_{v=1}^{k} \phi_v c_v \frac{LM(h_v) e_v}{c_v} = \sum_{v=1}^{k} \phi_v c_v \left(\sum_{j=1}^{v} \frac{LM(h_j) e_j}{c_j} - \frac{LM(h_{j-1}) e_{j-1}}{c_{j-1}} \right) =$$

$$= \sum_{j=1}^{k} \frac{LM(h_j) e_j}{c_j} - \frac{LM(h_{j-1}) e_{j-1}}{c_{j-1}} \sum_{v=j}^{k} \phi_v c_v$$

L'addendo per $j = 1$ dell'ultima sommatoria é nullo per ipotesi e quindi usando anche (20.3) rimane

$$h' = \sum_{j=2}^{k} x^{\delta - \gamma_{j,j-1}} \tau_{j,j-1} \left(\sum_{v=j}^{k} \phi_v c_v \right) \in T$$

come volevamo.

Definizione 20.13. *Sia ora* $g_1, \dots g_t$ *una base di Gröbner per* $(g_1, \dots, g_t) \subset S^m$ *e sia* $LT(g_i) = c_i x^{\alpha_i} e_{k(i)}$. *Per ogni coppia di indici* i,j *tali che* k(i) = k(j) *e tali che* $i < j$

poniamo $m_{ij} = \frac{m.c.m.(x^{\alpha_i}, x^{\alpha_j})}{c_j x^{\alpha_j}}$, allora $S(g_i, g_j) = m_{ji} g_i - m_{ij} g_j = \sum_{u=1}^{t} f_u^{i,j} g_u$ con $f_u^{i,j} \in S$ dall'algoritmo di divisione (qui usiamo l'ipotesi che la base sia di Gröbner) e quindi

$$\tau_{ij} := m_{ji} e_i - m_{ij} e_j - \sum_{u=1}^{t} f_u^{i,j} e_u \in Syz(g_1, \dots, g_t).$$

E' importante osservare che dall'algoritmo di divisione segue

$$multigrado(f_u^{i,j} g_u) \leq multigrado S(g_i, g_j) < multigrado(m_{ji} g_i) = multigrado(m_{ij} g_j)$$

quindi gli addendi dell'espressione di τ_{ij} *non* si cancellano.

Teorema 20.14. (Schreyer) Se $g_1, \dots g_t$ è base di Gröbner per il sottomodulo $(g_1, \dots, g_t) \subset S^m$ allora τ_{ij} definite con 20.13 per $i < j$ sono una base di Gröbner per $Syz(g_1, \dots, g_t)$ (per un ordine definito nel corso della dimostrazione); in particolare generano $Syz(g_1, \dots, g_t)$.

Dimostrazione Definiamo un ordine monomiale in $\oplus_{j=1}^{t} S e_j = S^t$ ponendo
$m e_u > n e_v$ se e solo se $LT(m g_u) > LT(n g_v)$ oppure $LT(m g_u) = LT(n g_v)$ e u< v. E' facile verificare che l'ordine appena definito è un ordine monomiale. Abbiamo già osservato che $LT(m_{ji} g_i) = LT(m_{ij} g_j) > LT(f_u^{i,j} g_u)\ \forall u$, pertanto con l'ordine monomiale sopra definito abbiamo $LT(\tau_{ij}) = m_{ji} e_i$. Quindi se $\tau = \sum f_v e_v \in Syz(g_1, \dots, g_t)$ è sufficiente provare che $LT(\tau)$ è un multiplo di $m_{ji} e_i$ per qualche i,j con i< j. Sia $n_v = LT(f_v)$ per v= $1, \dots, t$, dunque $LT(f_v e_v) = n_v e_v$. Questi termini non possono cancellarsi, quindi $LT(\tau) = n_p e_p$ per qualche p. Sia $\sigma = \sum' n_v e_v$ la somma sugli indici v tali che $LM(n_v g_v) = LM(n_p g_p)$. Gli indici di questa somma devono essere $\geq p$ perchè $LT(\tau) = n_p e_p$ e per come abbiamo definito l'ordine monomiale su S^t. Quindi $\sum' n_v LT(g_v) = 0$ e σ è una sizigia su $LT(g_v)$ con v$\geq p$. Per la proposizione 20.11 σ è combinazione di $m_{ji} e_i - m_{ij} e_j$ con $i, j \geq p$ e quindi n_p appartiene all'ideale generato da m_{jp} con j> p come volevamo.

Il teorema precedente è particolarmente importante perchè dà un algoritmo per il calcolo delle sizigie di una base di Gröbner, semplicemente attraverso l'algoritmo di divisione. Siccome si ottiene automaticamente una base di Gröbner per Syz, il procedimento può essere iterato per calcolare le sizigie delle sizigie e così via, fino ad ottenere una risoluzione libera del modulo generato da $g_1, \dots, g_t$.

Se si vuole calcolare $Syz(f_1, \dots, f_k)$ dove $f_1, \dots, f_k$ sono elementi qualunque di S^m, l'algoritmo di Buchberger permette di calcolare una base di Gröbner $g_1, \dots, g_t$ per il modulo generato da $f_1, \dots, f_k$. L'algoritmo (attraverso i resti di $S(f_i, f_j)$) dà anche come sottoprodotto le espressioni esplicite $g_i = \sum a_{ij} f_j$ e le espressioni delle τ_{ij} del teorema (si riveda l'oss. alla fine del §8). E' facile verificare che sostituendo $g_i = \sum a_{ij} f_j$ nelle sizigie su $\{g_i\}$ date da τ_{ij} si ottengono tutte le sizigie su $\{f_i\}$. Con sostituzioni successive si trovano anche le sizigie delle sizigie e così via.

Teorema 20.15 Con le notazioni del teorema precedente, ordiniamo $g_1, \ldots, g_t$ in modo tale che quando $LT(g_i) = \lambda_i e_{k(i)}$, $LT(g_j) = \lambda_j e_{k(j)}$ con k(i)= $k(j)$ allora $i < j$ se e solo se $\lambda_i > \lambda_j$ secondo LEX su $K[x_1, \ldots, x_n]$. Se $x_1, \ldots, x_s$ mancano da $LT(g_i)$ allora $x_1, \ldots, x_s, x_{s+1}$ mancano da $LT(\tau_{ij})$ per $i < j$.

Dimostrazione Ricordiamo che $LT(g_i) = c_i x^{\alpha_i} e_{k(i)}$ e che $LT(\tau_{ij}) = m_{ji} e_i$ con $m_{ji} = \frac{m.c.m.(x^{\alpha_i}, x^{\alpha_j})}{c_i x^{\alpha_i}}$ (con l'ordine monomiale definito nel corso della dimostrazione del teorema 20.14). Dal momento che $i < j$ per la costruzione fatta $x_1, \ldots, x_s$ mancano ancge da $LT(g_j)$. Siccome $x_1, \ldots x_s$ non appaiono in $LT(g_i), LT(g_j)$ e $LT(g_i) \geq LT(g_j)$ secondo LEX segue che x_{s+1} appare in $LT(g_i)$ a potenza maggiore che in $LT(g_j)$. Quindi x_{s+1} non appare in m_{ji} come volevamo.

Dimostrazione del teorema 20.2 delle sizigie di Hilbert

ii) segue da i) con considerazioni elementari, pertanto ci limitiamo a provare i). Sia $(g_1, \ldots, g_t)$ una base di Gröbner per M. Abbiamo
$0 \to Syz(g_1, \ldots, g_t) \to S^t \to M \to 0$ e possiamo costruire per il teorema 20.15 una base di Gröbner per Syz dove non appare x_1 nei leading term. Allo stesso modo i leading term delle sizigie di tale base non contengono x_1, x_2. Dopo n passi otteniamo un modulo dove tra i leading term dei generatori non compaiono $x_1, \ldots, x_n$ e quindi i generatori stessi non contengono $x_1, \ldots, x_n$. Tale modulo è quindi generato da alcuni tra gli e_i, ed è perciò libero.

La dimostrazione precedente è costruttiva e permette di costruire una risoluzione libera di un qualunque S-modulo noetheriano se sono noti i suoi generatori. Nelle applicazioni è sufficiente saper calcolare le divisioni rispetto ad un ordine fissato.

Osservazione. *Un lavoro di Bayer-Stillman (Inventiones math. 87(1987)) mostra che DEGREVLEX è mediamente l'ordine più efficiente per calcolare le sizigie.*

In Cocoa sono implementati i comandi Syz(I) e MinResolution(I) dove I può essere un ideale di S o un sottomodulo di S^m. Gli interi che appaiono nelle risposte sono i gradi (numeri di Betti) che hanno senso solo nel caso omogeneo. Si trovano variazioni di questi comandi attraverso Help. Può essere istruttivo calcolare la risoluzione dell'ideale massimale $(x_1, \ldots, x_n) \subset K[x_1, \ldots, x_n]$ (complesso di Koszul).

Esercizio Sia I= $(w^2 - xz, wx - yz, x^2 - wy, xy - z^2, y^2 - wz) \subset K[w, x, y, z] = S$. Si calcoli la risoluzione dell' S-modulo S/I assumendo DEGREVLEX.

Infine osserviamo che se $f \in (f_1, \ldots, f_r) \subset S^m$ allora in $Syz(f, f_1, \ldots, f_r)$ c'è un elemento con una costante al primo posto (e viceversa!) e questo permette di risolvere il problema di appartenenza per sottomoduli di S^m attraverso il calcolo delle sizigie (comando Syz di Cocoa).

BIBLIOGRAFIA

[Chi] L. Childs, Algebra, un'introduzione concreta, ETS 1989

[CLO] D. Cox, J. Little, D. O'Shea, Ideals, Varieties and Algorithms. An introduction to Computational Algebraic Geometry and Commutative Algebra, Springer 1992

[Cocoa] A. Giovini, G. Niesi, Cocoa , a system for doing Computations in Commutative Algebra, Genova 1991

[E] D. Eisenbud, Commutative algebra, GTM 150 Springer 1995

[H] J. Harris, Algebraic geometry. A first course. Springer 1992 GTM 133

[K] E. Kunz, Introduction to commutative algebra and algebraic geometry, Birkhauser 1985

[M] D. Mumford, Algebraic Geometry I, Complex Projective Varieties, Grundl. der Math. Wiss. 221, Springer 1976

APPENDICE

INTRODUZIONE ALL'USO DI COCOA

CoCoA è un sistema di calcolo simbolico, scritto da A. Giovini e G. Niesi, Dipartimento di Matematica, Università di Genova. Può essere copiato e distribuito gratuitamente, con la condizione che il sistema sia citato in ogni ricerca che ne fa uso. Esistono versioni per personal computer Macintosh e MS/DOS, e recentemente è disponibile anche una versione UNIX.

Il "nocciolo" del programma è costituito da una implementazione dell' algoritmo di Buchberger (in una versione più efficiente di quella vista nel §3). La maggior parte dei comandi sfrutta questo algoritmo. Molti di essi sono descritti nelle note che precedono questa appendice.

Si rimanda al manuale per una descrizione completa del sistema. Qui vogliamo solo introdurre alcuni comandi elementari (essenzialmente quelli che ancora non fanno uso dell'algoritmo di Buchberger). Ci riferiamo principalmente alla versione MS/DOS.

Anello di base. Il sistema esegue calcoli in un anello $K[x_1, \ldots, x_n]$. Viene assunto all'inizio un anello chiamato R con 4 indeterminate t, x, y, z (in quest'ordine!) con car $K = 0$ e l'ordine DEGREVLEX (vedi §1). Tutti questi parametri possono essere cambiati con l'istruzione $Ring$. Ad esempio $Ring(R; 0; abcde; 1; lex)$ definisce un anello $R = K[a, b, c, d, e]$ dove car$K = 0$, con l'ordine lex. Il parametro 1 significa che tutte le variabili hanno peso 1 e si consiglia inizialmente di non cambiarlo.

Importante: per eseguire una istruzione in Cocoa bisogna terminare con Ctrl+Enter (Enter su Macintosh).

Operazioni algebriche. La sintassi è quella usuale. Ad esempio (x^ 2+y^ 2)/(x+y) è $\frac{(x^2+y^2)}{(x+y)}$. Gli esponenti possono essere impostati anche con Alt 1, Alt 2,... Alt 9. Analogamente Alt Q,... ,Alt P (cioè la riga inferiore a quella dei numeri) permette di impostare degli indici. Ogni nuovo polinomio può essere chiamato con una lettera (maiuscolo$\neq$ minuscolo) seguita eventualmente da un indice numerico.

Oggetti definiti sull'anello. Cocoa può operare su polinomi, liste di polinomi (racchiusi tra graffe), matrici di polinomi, ideali e moduli (visti come sottomoduli di un modulo libero). Ad esempio F=x^ 2+y^ 3 assegna ad F il polinomio $x^2 + y^3$. Per matrici ed ideali si veda la lista dei comandi alla fine.

Istruzioni multiple. Il sistema può eseguire più istruzioni quando vengono impostate successivamente separate da punto e virgola. Si può tornare indietro spostando il cursore con le frecce e possono essere modificate e poi eseguite delle istruzioni già impostate in precedenza. Si può anche isolare una serie di istruzioni come "blocco" cominciando con Ctrl+KB e terminando con Ctrl+KK. In questo caso le istruzioni vengono eseguite con Ctrl+KD (invece che con Ctrl+Enter). Valgono tutti i comandi degli editor Wordstar, Q e di molti comuni Word Processor.

Input e output di files. Un blocco giá evidenziato viene salvato con Ctrl+KW, mentre Ctrl+KR legge un file.

Sostituzione di variabili. Si provi P=x^ 2+y;Q=P[x=3,y=z+1];Q. Questo comando permette di verificare l'effetto di un morfismo tra due anelli.
Per uscire da Cocoa. Quit Ctrl+Enter. In caso di collegamento da un terminale, ricordarsi sempre di eseguire logout.
F1 chiama un aiuto. F10 permette di cambiare alcune opzioni (si esce con Esc). Elenchiamo di seguito alcuni comandi utili:

$AdjMatrix(A)$
calcola la matrice aggiunta di A.
$Cancel(F)$
cancella F.
$Der(F, x)$
calcola la derivata di F rispetto a x.
$Der(F, n, x)$
calcola la derivata n-esima di F rispetto a x.
$Det(A)$
calcola il determinante della matrice A.
$Ideal(f_1, \ldots, f_k)$
definisce l'ideale generato da $f_1, \ldots, f_k$. Sugli ideali I e J si può operare con $I + J$.
$IdealOfMinors(p, A)$
definisce l'ideale generato da tutti i minori $p \times p$ della matrice A.
$List$
elenca gli oggetti definiti.
$Matrix(r, s, f_{11}, f_{12}, \ldots, f_{rs})$
definisce una matrice $r \times s$ con coefficienti f_{ij}.
$Transpose(A)$
definisce la matrice trasposta di A.
$Write(obj)$
scrive sullo schermo il contenuto dell'oggetto obj. Ad esempio $Write(Ring)$ scrive l'anello di base.

Esercizi per introdursi a Cocoa

1) Si assegni $A = (x+y)^3, B = (x-y)^3, C = x^3 - y^3$ (polinomi in $K[x,y]$) e si semplifichi $A-B$, $A+B$, A/B, A/C, $2A(B+C)$
   Soluzione: A=(x+y)^ 3; B=(x-y)^ 3; C=x^ 3-y^ 3 Ctrl+Enter
   oppure si possono impostare gli esponenti con Alt+3
   e successivamente (o anche nello stesso rigo) A-B;A+B;A/B;A/C;2A*(B+C) Ctrl+Enter
2) Si sostituisca nei polinomi A, B, C dell'eserc. 1) $x = t$ e $y = 2z$
   Soluzione: A_1=A[x=t,y=2z];A_1;B_1=B[x=t,y=2z];B_1;C_1
3) Dato $P(x,y) = x^3 - x^2y + 5xy^2 - 7$ si calcoli $P(x,2)$, P_y e $P_y(x,3)$.
   Soluzione: P=x^3-x^2y+5xy^2-7; PP=P[y=2];PP; Py=Der(P,y); PPy=Py[y=3];PPy
4) Si scriva un polinomio omogeneo F di grado d in x, y, z e si verifichi la relazione di Eulero $dF - F_x - F_y - F_z = 0$
5) Si ponga $I = (x, y^2)$, $J = (x^2 + y)$ e si calcolino generatori per l'ideale $I + J^2$.
   Soluzione: I=Ideal(x,y^2);J=(x^2+y);K=I+J^2;K
6) Si ripeta l'esercizio 5) con $J = (3x^2 + y)$
   Soluzione: Si sposti il cursore con le frecce evidenziando l'espressione precedente con Ctrl+KB all'inizio e Ctrl+KK alla fine. Dopo aver corretto J si esegua con Ctrl+KD
7) Si ponga $I = (x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2)$. É vero che $x^2 - 4 \in I$?
   Prima soluzione: I=Ideal(x^3+x^2-4x-4,x^3-x^2-4x+4, x^3-2x^2-x+2);g=gbasis(I);g e dal risultato si vede subito che la risposta é sí
   Seconda soluzione: I=Ideal(x^3+x^2-4x-4,x^3-x^2-4x+4, x^3-2x^2-x+2);(x^2-4) mod I
   mod calcola direttamente il resto della divisione per una base di Gröbner, siccome viene zero possiamo concludere che $x^2 - 4 \in I$
   Si provi ad impostare senza parentesi x^2-4 mod I. Come interpretate il risultato?
   Terza soluzione (valida solo perché abbiamo polinomi in una sola variabile): g=GCD(x^3+x^2-4x-4,x^3-x^2-4x+4, x^3-2x^2-x+2). A questo punto si puó ragionare come nella prima soluzione. Si noti che questa assegnazione per g cancella tutte le precedenti.
8) Determinare se $xy^3 - z^2 + y^5 - z^3$ appartiene all'ideale $I = (-x^3 + y, x^2y - z)$
9) Si calcoli una base di Gröbner per $I = (-x^3 + y, x^2y - z)$ rispetto a DEGREVLEX, DEGLEX e LEX.
   Soluzione: Degrevlex é l'ordine che Cocoa assume dall'inizio, quindi basta usare il comando gbasis. Per cambiare l'ordine con Deglex occorre impostare un nuovo anello, ad esempio con $Ring(R; 0; xyz; 1; deglex)$. Per cambiare anello puó essere utile stampare l'anello di base con Write(Ring), eseguire le modifiche necessarie tornando indietro con le frecce, evidenziare l'istruzione ed infine eseguirla con Ctrl+KD.
   Si noti che la risposta ottenuta con LEX permette di ricavare gli ideali di eliminazione.
10) Determinare se $f = xy^3 - z^2 + y^5 - z^3$ appartiene all'ideale $I = (-x^3 + y, x^2y - z)$.
10) Si calcoli la base di Gröbner (ridotta) dell'ideale generato da $x+y+z-1$, $2x-3y+4z-2$, $x-5y-6z-6$. Si interpreti la risposta come soluzione di un sistema lineare. La risposta cambia usando Lex o Deglex al posto di Degrevlex?

11) Si ponga $F = x^1 1 - x^1 0 + 2x^8 - 4x^7 + 3x^5 - 3x^4 + x^3 + 3x^2 - x - 1$, $G = Der(F, x)$,$H = F/GCD(F, G)$ e si stampi H. Cosa si puó dedurre sul polinomio F.
Risposta: il polinomio F contiene un fattore irriducibile ripetuto almeno due volte.

12) Sia $L = \{xy^2 - xz + y, xy - z^2, x - yz^4\}$. L é una lista di polinomi che si imposta in Cocoa racchiusa tra parentesi graffe. Sia I l'ideale generato da L. Si calcoli (con LEX) LeadingTerm(L) (che calcola il LT di ciascun polinomio) e LeadingTerm(I). Si calcoli infine la base di Gröbner di I. Si ripeta il calcolo con Degrevlex.

13) Sia $I = (t^2 + x^2 + y^2 + z^2, t^2 + 2x^2 - xy - z^2, t + y^3 - z^3)$. Si calcoli una base di Gröbner per I rispetto a Lex e rispetto a Degrevlex.

14) Si ripeta l'esercizio 13) per $I = (x - t^4, y - t^3, z - t^2)$

15) Si calcoli la base di Gröbner G per $I = (x^2 + y, x^4 + 2x^2y + y^2 + 3)$. Si osservi che, data la forma particolare dei polinomi, il risultato puó essere predetto in anticipo e non cambia al variare dell'ordine monomiale. Qual é la varietá $V(I)$?

16) Si calcoli la base di Gröbner G per $J = (xz - y, xy + 2z^2, y - z) = (j_1, j_2, j_3)$. Si calcolino i resti delle divisioni per G dei polinomi $F_1 = x^3z - 2y^2$, $F_2 = x^3z - 2y^2 - 2z$, $F_3 = x^3z - 2y^2 + 5$. In generale é vero che i resti sono additivi? Si provi anche ad impostare $F_1 div J$ che dá la matrice dei coefficienti (q_1, q_2, q_3) tali che $F-(F mod J) = j_1q_1+j_2q_2+j_3q_3$.

17) Sia I l'ideale generato da $(x^2 + y + z - 1, x + y^2 + z - 1, x + 3y + z^2 - 1)$. Si calcoli I_1 dapprima eliminando la x e poi eliminando la y.
Prima soluzione: si calcoli una base di Gröbner per I con $Ring(R; 0; xyz; 1; lex)$ e poi con $Ring(R; 0; yxz; 1; lex)$
Seconda soluzione: si esegua $Elim(x, I)$ e poi $Elim(y, I)$

18) Si calcoli il risultante dei polinomi $x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4$ (si veda l'esercizio 7))
Soluzione: F=x^3+x^2-4x-4; G=x^3-x^2-4x+4; R=Resultant(F,G,x).

19) Si calcoli il discriminante del polinomio generale di terzo grado $ax^3 + bx^2 + cx + d$

20) Si calcoli il risultante rispetto a x dei polinomi $x^3 + y^3 - 1$, $x^8 + y^8 - 1$. Si noti che il risultante ha grado 24. Si elimini poi la x dall'ideale $(x^3 + y^3 - 1, x^8 + y^8 - 1)$. Si noti che il generatore ha grado 22. In che relazione é il generatore con il risultante?

21 Sia $I = (x^3 + y^2 - 1, x + z - 1)$, $J = (yx^3 + y)$. Si trovino generatori per l'ideale $I \cap J$
Prima soluzione: Si introduca una variabile ausiliaria t e si lavori con $Ring(R; 0; txy; 1; lex)$. Si trovino generatori per tI e per $(1-t)J$ ed infine si elimini la t da $tI+(1-t)J$ calcolando una base di Gröbner oppure con Elim.
Seconda soluzione: Intersect(I,J)

22) Sia $f = x^3 + y + 3x^2 + 2xy + 6$, $g = x^2y^2 + 2y^2 - 9x^3 - 18x$. Calcolare $(f) \cap (g)$ ed anche il minimo comune multiplo tra f e g. Quest'ultimo puó essere calcolato anche con $LCM(f, g)$.

23) Sia $I = (z - xy, xz - y^2)$ e sia $J = (y, z)$. Si calcoli $I\colon J$.