Appunti del corso di Algebra II, proff. Patrizia Gianni e Carlo Traverso, a.a. 2009-2010

Daniele Agostini

30 marzo 2011

Indice

Capitolo 1

Anelli e Ideali

Definizione 1.1 (Anello)**.** Un anello è un gruppo abeliano $(A, +)$ dotato di un' operazione:

$$\begin{aligned} A \times A &\longrightarrow A \\ (a, b) &\mapsto ab \end{aligned}$$

tale che:

1. $a(bc) = (ab)c \quad \forall\ a, b, c \in A$
2. $a(b + c) = ab + bc \quad \forall\ a, b, c \in A$
3. $(a + b)c = ac + bc \quad \forall\ a, b, c \in A$

Noi con anello intenderemo sempre un anello commutativo con identità 1, cioè un anello per cui valgono anche le condizioni:

1. $ab = ba \quad \forall\ a, b, \in A$
2. $\exists\ 1 \in A \mid 1a = a1 = a \quad \forall\ a \in A$

Osservazione 1.0.1. Osserviamo che non è detto che sia $1 \neq 0$, però se in un anello A si ha che $1 = 0$, allora, per ogni $a \in A$, $a = a1 = a0 = 0$ e quindi $A = (0)$

Definizione 1.2. Sia A un anello.

- $u \in A$ si dice **invertibile** se esiste $v \in A$ tale che $uv = 1$. L'insieme degli elementi invertibili di un anello si indica con A^*. Un anello in cui ogni elemento non zero è invertibile si dice **campo**.
- $a \in A$ si dice **zerodivisore** se esiste $b \in A, b \neq 0$ tale che $ab = 0$. L'insieme degli elementi zerodivisori di A si indica con $\mathcal{D}(A)$. Un anello privo di zerodivisori si dice **dominio di integrità** o **dominio**.
- $a \in A$ si dice **nilpotente** se esiste $n \in \mathbb{N}$ tale che $a^n = 0$. L'insieme degli elementi nilpotenti si dice nilradicale di A e viene indicato con $\mathcal{N}(A)$. Un anello privo di nilpotenti si dice **ridotto**.
- $a \in A$ si dice **idempotente** se $a^2 = a$.

Vediamo alcune proprietà di questi elementi speciali:

Proposizione 1.0.1. *Sia A un anello.*

1. *$(A^*, \cdot)$ è un gruppo.*
2. *$A^* \cap \mathcal{D}(A) = \emptyset$. Inoltre, se A è finito, allora $A = A^* \cup \mathcal{D}(A)$.*
3. *$\mathcal{N}(A) \subseteq \mathcal{D}(A)$*

4. *A campo* $\implies$ *A dominio* $\implies$ *A ridotto.*

Dimostrazione. 1. Abbastanza chiaro.

2. Supponiamo che esista $a \in A^* \cap \mathcal{D}(A)$, allora esistono $u, b \in A$ con $b \neq 0$ tali che $au = 0$ e $ab = 0$. Ma allora $b = b1 = bau = 0u = 0$, assurdo. Poi, supponiamo che A sia un anello finito e fissiamo $a \in A$: considero allora l'omomorfismo di gruppi $x \mapsto ax$, vediamo che, se $a \notin A^*$, allora l'omomorfismo non è surgettivo, e quindi non è nemmeno iniettivo (perchè A è finito), quidi ha nucleo non banale, cioè esiste $b \neq 0$ tale che $ab = 0$; quindi $a \in \mathcal{D}(A)$.

3. Sia $a \in \mathcal{N}(A)$: se $a = 0$ è tutto ok, altrimenti, esiste $n \in N$ tale che $a^n \neq 0$ e $a^{n+1} = 0$. Ma allora $aa^n = 0$ e quindi $a \in \mathcal{D}(A)$.

4. Se A è un campo, allora $A^* = A \setminus (0)$, quindi $\mathcal{D}(A) = (0)$ e perciò A è un dominio. Se invece A è un dominio, allora $\mathcal{N}(A) \subseteq \mathcal{D}(A) = (0)$ e quindi $\mathcal{N}(A) = (0)$.

□

1.1 Ideali

Definizione 1.3 (Ideale)**.** Sia A un anello. $I \subseteq A$ si dice un ideale di A se:

1. $(I, +)$ è un sottogruppo di $(A, +)$.
2. per ogni $i \in I$ e per ogni $a \in A$, $ai \in I$.

Un ideale si dice proprio se è un sottoinsieme proprio di A.

Esempio 1.1.1. Qualsiasi anello A contiene sempre gli ideali A e $(0) = \{ 0 \}$. Inoltre, a meno che A non sia l'anello banale, l'ideale (0) è sempre proprio.

Vediamo alcune operazioni che possiamo fare con gli ideali:
Sia A un anello

1. **Intersezione di ideali**: sia $\{ I_\alpha \}_{\alpha \in H}$ una famiglia di ideali. Allora si verifica facilmente che $I = \bigcap_{\alpha \in H} I_\alpha$ è ancora un ideale di A. Quindi ha senso definire l'ideale generato da un sottoinsieme $S \subseteq A$ come l'intersezione di tutti gli ideali di A che contengono S: indichiamo quest'ideale con (S).

2. **Somma di ideali**: sia $\{ I_\alpha \}_{\alpha \in H}$ una famiglia di ideali di A. Allora si verifica facilmente che $\sum_{\alpha \in H} I_\alpha = \{ \text{somme finite di elementi di } \bigcup_{\alpha \in H} I_\alpha \}$ è ancora un ideale di A e che è l'ideale generato da $\bigcup_{\alpha \in H} I_\alpha$

3. **Ideale generato**: vogliamo determinare meglio l'ideale generato da $S \subseteq A$: intanto supponiamo che $S = \{ s \}$: allora si vede facilmente che $(S) = (s) = \{ as \mid a \in A \}$. Nel caso generale, è ancora facile vedere che $(S) = \sum_{s \in S} (s)$.

4. **Prodotto di ideali**: siano I, J due ideali di A: allora definiamo l'ideale prodotto IJ come $IJ = (ij \mid i \in I, j \in J)$.

5. **Quoziente di ideali**: siano I, J due ideali di A: allora definiamo il loro ideale quoziente come $(I : J) = \{ a \in A \mid aJ \subseteq I \}$; è facile vedere che questo è effettivamente un ideale. In particolare $(0 : I)$ viene detto l'**annullatore** di I ed è indicato con $\mathrm{Ann}(I)$.

6. **Radicale di un ideale**: sia I un ideale di A. Allora definiama il radicale di I come $\sqrt{I} = \{ a \in A \mid \exists\, n \in \mathbb{N} \text{ t.c. } a^n \in I \}$. Mostriamo che è effettivamente un ideale: siano $a, b \in \sqrt{I}$: allora esistono $n, m \in \mathbb{N}$ tali che $a^n, b^m \in I$. Allora, si vede facilmente che $(a + b)^{n+m-1} \in I$ e quindi che $a + b \in I$. Poi è abbastanza chiaro che, se $s \in A$, allora $as \in \sqrt{I}$.

Osservazione 1.1.2. Vediamo che, se A è un anello, allora $A = (1)$ e che un ideale I di A è proprio se e solo se $I \cap A^* = \emptyset$.

Osservazione 1.1.3. Osserviamo che, per ogni anello A, si ha che $\mathbb{N}(A) = \sqrt{(0)}$, e quindi il nilradilcale di A è un ideale di A.

Definizione 1.4 (Ideali massimali,primi,radicali,primari,irriducibili)**.** Sia A un anello e sia I un ideale proprio di A.

1. I si dice **massimale**, se non esiste un ideale proprio che lo contiene strettamente.
2. I si dice **primo**, se vale che $ab \in I \implies a \in I$ o $b \in I$.
3. I si dice **radicale**, se vale che $I = \sqrt{I}$.
4. I si dice **primario**, se vale che $ab \in I \implies a \in I$ o $b \in \sqrt{I}$.
5. I si dice **irriducibile**, se vale che $I = I_1 \cap I_2 \implies I_1 = A$ o $I_2 = A$.

Teorema 1.1.1. *Sia A un anello e sia I un ideale proprio di A. Allora esiste un ideale massimale $\mathfrak{m}$ tale che $\mathfrak{m} \supseteq I$.*

Dimostrazione. La dimostrazione richiede il lemma di Zorn: sia $X = \{ J \mid J \text{ ideale proprio }, J \supseteq I \}$ ordinato con l'inclusione insiemistica. Allora, X è non vuoto, perchè $I \in X$ e, se $\{ J_\alpha \}$ è una catena (cioè una sottofamiglia totalmente ordinata di X), allora $J = \bigcup J_\alpha$ è un maggiorante per questa catena: per dimostrare questo, basta vedere se $J \in X$: sicuramente $J \supseteq I$; poi, dimostriamo che J è un ideale: se $x, y \in J$, allora esistono J_1, J_2 tali che $x \in J_1$ e $y \in J_2$, e quindi , supponendo ad esempio $J_1 \subseteq J_2$, $x + y \in J_2 \subseteq J$. Poi, se $a \in A$, allora $ax \in J_1 \subseteq J$. Quindi J è un ideale; vediamo che è primo: supponiamo che $1 \in J$, allora $1 \in J_\alpha$ per un certo α il che è assurdo. Allora, per il lemma di Zorn, X possiede un elemento massimale, che è proprio l'ideale massimale $\mathfrak{m}$ che cerchiamo. □

Corollario 1.1.1. *Sia A un anello e sia $a \notin A^*$. Allora esiste un ideale massimale $\mathfrak{m}$ che contiente a.*

Dimostrazione. Basta applicare il teorema precedente all'ideale (a). □

Corollario 1.1.2. *Sia A un anello non banale. Allora A possiede un ideale massimale.*

Dimostrazione. Basta applicare il teorema precedente all'ideale (0). □

1.1.1 Anelli quoziente

Se A è un anello e I è un ideale di A, I è anche un sottogruppo normale di A e quindi possiamo costruire il gruppo quoziente $A/I = \{ x + I \mid x \in A \}$. Allora, possiamo dotare A/I di una struttura di anello, ponendo $a(x+I) = ax+I$; se mostriamo che quest'operazione è ben definita, è abbastanza facile vedere che $(A/I, +, \cdot)$ è effettivamente un anello: quindi, supponiamo che $x+I = y+I$ allora, $x = y + i, i \in I$ e quindi $a(x + I) = ax + I = a(y + i) + I = ay + ai + I = ay + I = a(y + I)$.

Teorema 1.1.2. *Sia A un anello e sia I un ideale di A. Allora*

1. *I è un ideale proprio $\iff A/I \neq (0)$.*
2. *I è un ideale massimale $\iff A/I$ è campo.*
3. *I è un ideale primo $\iff A/I$ è dominio.*
4. *I è un ideale radicale $\iff A/I$ è ridotto.*
5. *I è un ideale primario $\iff \mathcal{N}(A/I) = \mathcal{D}(A/I)$.*
6. *I massimale $\implies I$ primo $\implies I$ radicale e primario.*

Dimostrazione. 1. I non è un ideale proprio $\iff I = A \iff A/I = (0)$.

2. Supponiamo che I sia un ideale massimale e prendiamo $a+I \in A/I$, $a \notin I$. Allora $(a, I) = A$ e quindi esistono $x \in A, i \in I$ tali che $ax+i = 1$, e perciò $(a+I)(x+I) = ax+I = 1-i+I = 1+I$. Viceversa, supponiamo che A/I sia un campo, e sia J un ideale di A tale che $J \supseteq I$, allora se $x \in J$ e $x \notin I$, $x + I$ è invertibile in A/I, cioè esiste $a \in A$ tale che $ax + I = 1 + I$, perciò $1 = ax + i$ per un certo $i \in I$. Quindi $1 \in J$ e concludiamo.

3. Intanto vediamo che, in A/I, $(a + I)(b + I) = ab + I = 0 + I$ se e solo se $ab \in I$. Quindi, se I è primo, e $(a + I)(b + I) = 0 + I$ dev'essere che $a \in I$ o $b \in I$ e quindi $a + I = 0 + I$ oppure $b + I = 0 + I$, e quindi A/I è un dominio; viceversa, se A/I è dominio, allora $ab \in I$ implica $(a + I)(b + I) = 0 + I$ e quindi $a + I = 0 + I$ oppure $b + I = 0 + I$, cioè $a \in I$ opppure $b \in I$.

4. Vediamo che $(a + I)^n = a^n + I = 0 + I$ se e solo se $a^n \in I$. Quindi con un ragionamento simile al precedente, segue la tesi.

5. Supponiamo I primario e prendiamo $a + I \in \mathcal{D}(A/I)$, allora esiste $b \notin I$ tale che $ab \in I$ e quindi dev'essere $a \in \sqrt{I}$, ma allora $a^n \in I$ per un certo $n \in \mathbb{N}$ e quindi $a + I \in \mathcal{N}(A/I)$. Viceversa, se vale che $\mathcal{N}(A/I) = \mathcal{D}(A/I)$, se $ab \in I$ e $a \notin I$, allora $ab+I = 0+I$ e $a+I \neq 0+I$; quindi $b + I \in \mathcal{D}(A/I) = \mathcal{N}(A/I)$, cioè $b \in \sqrt{I}$.

6. I massimale $\implies$ A/I campo $\implies$ A/I dominio $\implies$ I primo $\implies$ A/I dominio $\implies$ $\mathcal{D}(A/I) = \mathcal{N}(A/I) = (0) \implies$ I primario e radicale.

□

1.2 Omomorfismi di anelli

Definizione 1.5. Siano A, B due anelli. Un'applicazione $f : A \longrightarrow B$ è detta omomorfismo di anelli se:

1. $f(x + y) = f(x) + f(y)$ per ogni $x, y \in A$.
2. $f(xy) = f(x)f(y)$ per ogni $x, y \in A$.
3. $f(1_A) = 1_B$.

Un omomorfismo bigettivo è detto isomorfismo, e in questo caso diciamo che A e B sono isomorfi e scriviamo $A \cong B$. L'insieme degli omomorfismi di anelli da A a B si indica con $\mathrm{Hom}(A, B)$.

Osservazione 1.2.1. Si vede facilmente che composizione di omomorfismi è ancora un omomorfismo, così come si vede facilmente che l'inversa di un isomorfismo è ancora un isomorfismo. Quindi $\cong$ è una relazione di equivalenza tra gli anelli.

Lemma 1.2.1. *Siano A, B anelli e sia $f : A \longrightarrow B$ un omomorfismo di anelli. Allora*

1. *Ker $f = f^{-1}(0)$ è un ideale di A.*
2. *f è iniettivo se e solo se Ker $f = (0)$.*

Dimostrazione.

Siano $x, y \in \mathrm{Ker}\ f$ e sia $a \in A$. Allora $f(x + y) = f(x) + f(y) = 0 + 0 = 0$ e $f(ax) = f(a)f(x) = f(a)0 = 0$, quindi $x + y, ax \in \mathrm{Ker}\ f$.

Se f è iniettivo, allora è chiaro che $\mathrm{Ker}\ f = (0)$ (perchè sappiamo che $f(0) = 0$). Viceversa, sia $\mathrm{Ker}\ f = 0$ e supponiamo che $f(x) = f(y)$, allora $f(x) - f(y) = f(x - y) = 0$, cioè $x - y \in \mathrm{Ker}\ f$ e quindi $x - y = 0$, perciò f è iniettiva. □

Facciamo degli esempi:

Esempio 1.2.2. Sia A un anello, allora l'identità $id : A \longrightarrow A$ è un isomorfismo di anelli. Inoltre, esiste sempre l'omomorfismo banale $A \longrightarrow (0)$, $a \mapsto 0$.

Esempio 1.2.3. Se A è un sottoanello di un anello B, l'immarsione $i : A \longrightarrow B$ è un omomorfismo iniettivo.

Esempio 1.2.4. Se A è un anello e I un ideale, la proiezione $\pi : A \longrightarrow A/I$ definita da $\pi(a) = a + I$ è un omomorfismo surgettivo.

1.2.1 Ideali contratti ed estesi

Definizione 1.6 (Ideali estesi e contratti)**.** Siano A, B due anelli e sia $f : A \longrightarrow B$ un omomorfismo di anelli. Allora, se $I \subseteq A$ è un ideale di A, definiamo il suo ideale esteso come $I^e = (f(I))$. Invece, se $J \subseteq B$ è un ideale di B, definiamo il suo ideale contratto come $J^c = f^{-1}(J)$

Osservazione 1.2.5. Si vede facilmente che J^c è un ideale di I, infatti, se $x, y \in J^c$ e $a \in A$, allora $f(x + y) = f(x) + f(y) \in J$ e $f(ax) = f(a)f(x) \in J$, quindi $x + y, ax \in J^c$.
Poi, vediamo che come ideale esteso di I si prende l'ideale generato da $f(I)$, questo perchè in genere $f(I)$, non è un ideale di B (come controesempio, possiamo prendere l'immersione $i : \mathbb{Z} \longrightarrow \mathbb{Q}$); tuttavia, se f è surgettiva, allora si vede facilmente che $f(I)$ è un ideale e quindi che $I^e = f(I)$.

Lemma 1.2.2. *L'estensione e la contrazione di ideali mantengono le inclusioni, cioè:*

1. $I_1 \subseteq I_2 \implies I_1^e \subseteq I_2^e$
2. $J_1 \subseteq J_2 \implies J_1^c \subseteq J_2^c$

Dimostrazione. Facile. □

Vediamo quindi che $J^c \supseteq \text{Ker } f$ per ogni ideale J di B, infatti Ker $f = (0)^c$ e $0 \in J$.

Lemma 1.2.3. 1. $I^{ec} \supseteq I$.

2. $J^{ce} \subseteq J$.
3. $I^{ece} = I^e$.
4. $J^{cec} = J^c$.

Dimostrazione. 1. se $x \in I$, allora $f(x) \in I \subseteq I^e$, cioè $x \in I^{ec}$.

2. abbiamo che $J^{ce} = (f(J^c))$ e poichè $f(J^c) \subseteq J$ per definizione, abbiamo che $(f(J)) \subseteq J$.
3. dal punto 1 abbiamo che $I^{ec} \supseteq I \implies I^{ece} \supseteq I^e$. Per l'altra inclusione, vediamo che $I^{ec} = f^{-1}(I^e)$ e quindi $f(I^{ec}) = f(f^{-1}(I^e)) \subseteq I^e$, ma allora $I^{ece} \subseteq I^e$.
4. dal punto 2 abbiamo che $J^{ce} \subseteq J$ e quindi $J^{cec} \subseteq J^c$. Per l'altra inclusione, vediamo che $f(J^c) \subseteq J^{ce}$ e quindi $J^c \subseteq J^{cec}$.

□

Vediamo poi se l'estensione e la contrazione mantengono le proprietà degli ideali: per l' estensione vediamo subito che non possiamo aspettarci granchè, infatti se consideriamo l'immersione $i : \mathbb{Z} \longrightarrow \mathbb{Q}$, vediamo che $2\mathbb{Z}$ è massimale,primo,radicale e primario, ma $2\mathbb{Z})^e = \mathbb{Q}$ e quindi non è nè massimale, nè primo, nè radicale, nè primario. Lo stesso controesempio ci mostra che anche la contrazione non mantiene la massimalità: infatti (0) è massimale in $\mathbb{Q}$, ma $(0)^c = (0)$ non è massimale in $\mathbb{Z}$. Tuttavia, per il resto va un po'meglio:

Proposizione 1.2.1. 1. *J primo $\implies$ J^c primo.*

2. *J primario $\implies$ J^c primario.*
3. *J radicale $\implies$ J^c radicale.*

Dimostrazione. 1. Supponiamo che $xy \in J^c$, allora, $f(xy) = f(x)f(y) \in J$ e quindi $f(x) \in J$ o $f(y) \in J$, ma allora $x \in J^c$ oppure $y \in J^c$.

2. Supponiamo che $xy \in J^c$, allora, $f(xy) = f(x)f(y) \in J$ e quindi $f(x) \in J$ o $f(y)^n = f(y^n) \in J$ per un certo $n \in \mathbb{N}$; ma allora $x \in J^c$ oppure $y^n \in J^c$.

3. Supponiamo che $a^n \in J^c$, allora, $f(a^n) = f(a)^n \in J$ e quindi $f(a) \in J$, perciò $a \in J$.

□

Tuttavia, se l'omomorfismo f è surgettivo, le cose vanno molto meglio:

Teorema 1.2.1 (Teorema di Corrispondenza)**.** *Siano A, B anelli e sia $f : A \longrightarrow B$ un omomorfismo surgettivo. Allora, se I è un ideale di A che contiene $Ker\ f$ e J un ideale di B abbiamo che*

1. *$I = I^{ec}, J = J^{ce}$. Quindi l'estensione e la contrazione stabiliscono corrispondenze biunivoche (una l'inversa dell'altra) tra gli ideali di B e gli ideali di A che contengono $Ker\ f$.*

2. *L'estensione e la contrazione stabiliscono corrispondenze biunivoche (una l'inversa dell'altra) tra gli ideali **massimali** di B e gli ideali **massimali** di A che contengono $Ker\ f$.*

3. *L'estensione e la contrazione stabiliscono corrispondenze biunivoche (una l'inversa dell'altra) tra gli ideali **primi** di B e gli ideali **primi** di A che contengono $Ker\ f$.*

4. *L'estensione e la contrazione stabiliscono corrispondenze biunivoche (una l'inversa dell'altra) tra gli ideali **primari** di B e gli ideali **primari** di A che contengono $Ker\ f$.*

5. *L'estensione e la contrazione stabiliscono corrispondenze biunivoche (una l'inversa dell'altra) tra gli ideali **radicali** di B e gli ideali **radicali** di A che contengono $Ker\ f$.*

Dimostrazione. 1. Abbiamo che $I^{ec} = f^{-1}(I^e) = f^{-1}(f(I))$ e quindi, se $x \in I^{ec}$ allora $f(x) = f(i)$ per un certo $i \in I$ e quindi $x - i \in \text{Ker } f$, ma allora $x \in I$. Poi, abbiamo che $J^{ce} = f(J^c) = f(f^{-1}(J)) = J$ perchè f è surgettiva. Per gli altri punti, è facile vedere che, se $I \subseteq A$ è un ideale che contiene Ker f, allora $A/I \cong B/I^e$ e quindi che, se $J \subseteq B$ è un ideale, allora $A/J^c \cong B/J$; allora, concludiamo grazie al teorema 1.1.2.

□

Capitolo 2

Basi di Grobner

2.1 Ideali Monomiali

Iniziamo con un po' di notazioni: k indicherà sempre un campo, e poi scriveremo $k[\mathbf{x}] := k[x_1, x_2, \ldots, x_n]$ per indicare l'anello dei polinomi in n indeterminate a coefficienti in k. Inoltre indicheremo con lettere greche minuscole gli elementi di $\mathbb{N}^n$, ad esempio $\alpha = (a_1, a_2, \ldots, a_n)$ $a_i \in \mathbb{N}$); quindi, se $\alpha \in \mathbb{N}^n$ scriveremo $\mathbf{x}^\alpha = x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$ per indicare un monomio di $k[\mathbf{x}]$. Inoltre indicheremo il grado del monomio $\mathbf{x}^\alpha$ con $|a| = a_1 + \cdots + a_n$.

Definizione 2.1 (Ideale Monomiale)**.** Un ideale $I \subseteq k[\mathbf{x}]$ si dice monomiale se è del tipo $I = (\mathbf{x}^\alpha \mid \alpha \in A)$, con $A \subseteq \mathbb{N}^n$.

Lemma 2.1.1. *Sia $I = (\mathbf{x}^\alpha \mid \alpha \in A)$ un ideale monomiale di $k[\mathbf{x}]$. Allora $\mathbf{x}^\beta \in I \iff \exists\, \alpha \in A\,, \gamma \in \mathbb{N}^n$ t.c. $\mathbf{x}^\beta = \mathbf{x}^{\alpha+\gamma}$.*

Dimostrazione. ($\Longrightarrow$) Supponiamo che $\mathbf{x}^\beta \in I$, allora esistono $f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}) \in k[\mathbf{x}]$ e $\alpha_1, \ldots, \alpha_m \in A$ tali che $\mathbf{x}^\beta = \sum_{i=0}^m f_i(\mathbf{x}) x^{\alpha_i}$; allora, scrivendo gli f_i in modo esteso $f_i(\mathbf{x}) = \sum_{j=0}^{m_i} c_{i,j}\mathbf{x}^{\gamma_{i,j}}$ vediamo che $\mathbf{x}^\beta = \sum_{i=0}^m f_i(\mathbf{x})\mathbf{x}^{\alpha_i} = \sum_{i=0}^m \sum_{j=0}^{m_i} c_{i,j}\mathbf{x}^{\gamma_{i,j}}\mathbf{x}^{\alpha_i} = \sum c_{i,j}\mathbf{x}^{\gamma_{i,j}+\alpha_i}$, e quindi, per il principio di identità dei polinomi, vediamo che $\mathbf{x}^\beta = \mathbf{x}^{\gamma_{i,j}+\alpha_i}$ per certi i, j. □

Lemma 2.1.2. *In $k[\mathbf{x}]$ si ha che $\mathbf{x}^\alpha \mid \mathbf{x}^\beta \iff \exists\, \mathbf{x}^\gamma$ t.c. $\mathbf{x}^\beta = \mathbf{x}^\alpha\mathbf{x}^\gamma = \mathbf{x}^{\alpha+\beta}$*

Dimostrazione. ($\Longrightarrow$) se $\mathbf{x}^\alpha \mid \mathbf{x}^\beta$ allora $\mathbf{x}^\beta$ appartiene all'ideale monomiale $(\mathbf{x}^\alpha)$ e quindi concludiamo per il Lemma 2.1.3. ($\Longleftarrow$) Chiaro. □

Definizione 2.2 (Ideale Monomiale)**.** Un ideale $I \subseteq k[\mathbf{x}]$ si dice monomiale se è del tipo $I = (\mathbf{x}^\alpha \mid \alpha \in A)$, con $A \subseteq \mathbb{N}^n$.

Lemma 2.1.3. *Sia $I = (\mathbf{x}^\alpha \mid \alpha \in A)$ un ideale monomiale di $k[\mathbf{x}]$. Allora $\mathbf{x}^\beta \in I \iff \exists\, \alpha \in A$ t.c. $\mathbf{x}^\alpha \mid \mathbf{x}^\beta$.*

Dimostrazione. ($\Longrightarrow$) Supponiamo che $\mathbf{x}^\beta \in I$, allora esistono $f_1(\mathbf{x}), \ldots, f_m(\mathbf{x}) \in k[\mathbf{x}]$ e $\alpha_1, \ldots, \alpha_m \in A$ tali che $\mathbf{x}^\beta = \sum_{i=0}^m f_i(\mathbf{x}) x^{\alpha_i}$; allora, scrivendo gli f_i in modo esteso $f_i(\mathbf{x}) = \sum_{j=0}^{m_i} c_{i,j}\mathbf{x}^{\gamma_{i,j}}$ vediamo che $\mathbf{x}^\beta = \sum_{i=0}^m f_i(\mathbf{x})\mathbf{x}^{\alpha_i} = \sum_{i=0}^m \sum_{j=0}^{m_i} c_{i,j}\mathbf{x}^{\gamma_{i,j}}\mathbf{x}^{\alpha_i} = \sum c_{i,j}\mathbf{x}^{\gamma_{i,j}+\alpha_i}$, e quindi, sempre applicando il principio di identità, vediamo che $\mathbf{x}^\beta = \mathbf{x}^{\gamma_{i,j}+\alpha_i}$ per certi i, j. □

Diamo ora una caratterizzazione degli ideali monomiali

Proposizione 2.1.1. *Sia $I \subseteq k[\mathbf{x}]$ un ideale. Allora sono equivalenti:*

1. *I è un ideale monomiale.*
2. *se $f(\mathbf{x}) = \sum c_i\mathbf{x}^{\gamma_i} \in I$ allora $\mathbf{x}^{\gamma_i} \in I$ per ogni i.*

Dimostrazione. (1) $\implies$ (2) Supponiamo che $I = (\mathbf{x}^\alpha \mid \alpha \in A)$ e sia $f(\mathbf{x}) = \sum c_i \mathbf{x}^{\gamma_i} \in I$. Allora esistono $g_j(\mathbf{x})$ e $\alpha_j \in A$ tali che $f(\mathbf{x}) = \sum g_j(\mathbf{x})\mathbf{x}^{\alpha_j}$. Allora, scrivendo i g_j come somma di monomi e sviluppando, troviamo che per ogni γ_i esiste α_j tale che $\mathbf{x}^{\alpha_j} \mid \mathbf{x}^{\gamma_i}$.
(2) $\impliedby$ (1) Sia $A \subseteq \mathbb{N}^n$ l'insieme degli esponenti dei monomi contenuti in I. Allora, dall'ipotesi segue subito che $I = (\mathbf{x}^\alpha \mid \alpha \in A)$. □

Ora ci aspetta il risultato importante di questa sezione

Teorema 2.1.1 (Lemma di Dickson)**.** *Sia $I = (\mathbf{x}^\alpha \mid \alpha \in A)$ un ideale monomiale di $k[\mathbf{x}]$. Allora esistono $\alpha_1, \ldots, \alpha_r \in A$ tali che $I = (\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_r})$. In particolare, ogni ideale monomiale è finitamente generato.*

Dimostrazione. Intanto vediamo che basta dimostrare che I è generato da un munero finito di monomi: infatti se $I = (\mathbf{x}^{\beta_1} \ldots, \mathbf{x}^{\beta_s})$ allora per ogni i esiste $\alpha_i \in A$ tale che $\mathbf{x}^{\alpha_i} \mid \mathbf{x}^{\beta_i}$ e quindi $I = (\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_s})$. Procediamo per induzione sul numero di indeterminate n:
$[n = 1]$ $A \in \mathbb{N}$ quindi esiste $m = \min A$: allora per ogni $a \in A$ si ha che $x^a = x^m x^{a-m}$ e $a - m \geq 0$, quindi $I = (x^m)$.
$[n - 1 \implies n]$ Scriviamo le indeterminate come $\mathbf{x} = (x_1, \ldots, x_{n-1})$ e y. Poniamo $J = (\mathbf{x}^\alpha \mid \exists\, y^m \text{ t.c. } \mathbf{x}^\alpha y^m \in I)$, allora J è un ideale monomiale in $n - 1$ indeterminate e quindi per ipotesi induttiva esistono $\alpha_1, \ldots, \alpha_r$ tali che $J = (\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_r})$. Per definizione, per ogni α_i esiste $m_i \in \mathbb{N}$ tale che $\mathbf{x}^{\alpha_i} y^{m_i} \in I$; quindi, posto $m = \max\{ m_1, \ldots, m_r \}$, vediamo che per ogni $\mathbf{x}^\alpha y^p \in I$ con $p \geq m$, si ha che $\mathbf{x}^\alpha \in J$ e perciò $\mathbf{x}^{\alpha_i} \mid x^\alpha$ per un certo i, e dunque $\mathbf{x}^{\alpha_i} y^{m_i} \mid \mathbf{x}^\alpha y^p$. Allora, per $h = 0, 1, \ldots, m - 1$ poniamo $J_h = (\mathbf{x}^\alpha \mid \mathbf{x}^\alpha y^h \in I)$; sempre per ipotesi induttiva, si ha che esistono $\alpha_{h,1}, \ldots, \alpha_{h,r_h}$ tali che $J_h = (\mathbf{x}^{\alpha_{h,1}}, \ldots, \mathbf{x}^{\alpha_{h,r_h}})$. Allora si vede facilmente che $I = (\{ \mathbf{x}^{\alpha_1} y^{m_1}, \ldots, \mathbf{x}^{\alpha_r} y^{m_r} \} \cup \bigcup_{h=0}^{m-1} \{ \mathbf{x}^{\alpha_{h,1}} y^h, \ldots, \mathbf{x}^{\alpha_{h,r_h}} y^h \})$. □

Poichè ogni ideale monomiale è finitamente generato, esisterà un insieme di generatori monomiale di cardinalità minima: per questo ha senso la seguente definizione:

Definizione 2.3 (Escalier)**.** Se I è un ideale monomiale di $k[\mathbf{x}]$ definiamo l'escalier di I come un suo insieme di generatori monomiale di cardinalità minima.

Proposizione 2.1.2. *1. Sia $I = (\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_r})$ un ideale monomiale. Allora $\{ \mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_r} \}$ è un escalier per I $\iff$ $\mathbf{x}^{\alpha_i} \nmid \mathbf{x}^{\alpha_j}$ per $i \neq j$.*

2. Ogni ideale monomiale ha un unico escalier.

Dimostrazione. 1. ($\implies$) Procediamo per assurdo: supponiamo che, ad esempio, $\mathbf{x}^{\alpha_2} \mid \mathbf{x}^{\alpha_1}$: allora è chiaro che $I = (\mathbf{x}^{\alpha_2}, \ldots, \mathbf{x}^{\alpha_n})$ e quindi $\{ \mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_r} \}$ non è un escalier per I.
($\impliedby$) Procediamo anche qui per assurdo: supponiamo che $I = (\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_r}) = (\mathbf{x}^{\beta_1}, \ldots, \mathbf{x}^{\beta_s})$ con $s < r$. Allora, applicando il Lemma 2.1.3 insieme al principio dei piccioni, possiamo supporre che $\mathbf{x}^{\beta_1} \mid \mathbf{x}^{\alpha_1}, \mathbf{x}^{\alpha_2}$. Tuttavia, sappiamo anche che esiste α_i tale che $\mathbf{x}^{\alpha_i} \mid \mathbf{x}^{\beta_1}$ e quindi $\mathbf{x}^{\alpha_i} \mid \mathbf{x}^{\alpha_1}, \mathbf{x}^{\alpha_2}$ il che è impossibile per ipotesi.

2. Supponiamo che $\{ \mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_r} \}$ e $\{ \mathbf{x}^{\beta_1}, \ldots, \mathbf{x}^{\beta_r} \}$ siano due escalier per I. Allora $(\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_r}) = (\mathbf{x}^{\beta_1}, \ldots, \mathbf{x}^{\beta_r})$ e quindi, per il Lemma 2.1.3, possiamo supporre ad esempio che $\mathbf{x}^{\alpha_1} \mid \mathbf{x}^{\beta_1}$ e quindi, per il punto precedente, dev'essere che $\mathbf{x}^{\beta_1} \mid \mathbf{x}^{\alpha_1}$ e, per il Lemma 2.1.2, questo implica $\mathbf{x}^{\alpha_1} = \mathbf{x}^{\beta_1}$. Procedendo in questo modo, si vede che $\mathbf{x}^{\alpha_i} = \mathbf{x}^{\beta_i}$ per ogni i.

□

Osservazione 2.1.1. La proposizione precedente ci dice che un ideale monomiale è univocamente determinato dal suo escalier e ci dà anche un **algoritmo per trovare l'escalier** di un ideale monomiale $I = (\mathbf{x}^{\alpha_1} \ldots, \mathbf{x}^{\alpha_r})$: basta eliminare tutti quei monomi che sono divisi da un altro monomio.

2.2 Algoritmo di divisione

2.2.1 Ordinamenti monomiali

Vogliamo introdurre un algoritmo di divisione su $k[\mathbf{x}]$ su modello di quello che già conosciamo per i polinomi ad una sola variabile. Se pensiamo un momento al procedimento che seguiamo per dividere due polinomi, vediamo che un elemento fondamentale è l'ordinamento dei termini del polinomio e che nell'ordinare questi termini ci interessano soltanto gli esponenti dei monomi. Per questo introduciamo in $k[\mathbf{x}]$ gli ordinamenti monomiali come ordinamenti su $\mathbb{N}^n$:

Definizione 2.4 (Ordinamento Monomiale)**.** Un ordinamento $>$ su $\mathbb{N}^n$ si dice monomiale se:

1. $<$ è un ordinamento totale (cioè per ogni $\alpha, \beta \in \mathbb{N}^n$ si ha $\alpha < \beta, \alpha = \beta$ o $\alpha > \beta$).
2. se $\alpha < \beta$ allora per ogni $\gamma \in \mathbb{N}^n$ vale $\alpha + \gamma < \beta + \gamma$.
3. $<$ è un buon ordinamento (cioè ogni sottoinsieme non vuoto di $\mathbb{N}^n$ ammette minimo).

Se $<$ è un ordinamento monomiale su $\mathbb{N}^n$ diremo che $c\mathbf{x}^\alpha < d\mathbf{x}^\beta$ se e solo se $\alpha < \beta$. In questo modo un ordinamento monomiale induce un ordinamento su $k[\mathbf{x}]$.

Facciamo qualche esempio di ordinamento monomiale:

Esempio 2.2.1 (Ordinamento lex)*.* L'ordinamento lessicografico o lex assegna un peso diverso alle varie indeterminate $x_1, \ldots, \mathbf{x}_n$ in modo che x_1 sia più importante di x_2 che è a sua volta più importante di x_3, e così via. Allora avremo ad esempio $x_1^2 > x_2 x_3 x_4^3$ oppure $x_3^2 < x_2$. Formalmente definiamo quest'ordinamento così: dati $\alpha, \beta \in \mathbb{N}^n$ diciamo che $\alpha < \beta \iff$ il primo termine non nullo da sinistra di $\alpha - \beta$è negativo.

Esempio 2.2.2 (Ordinamento glex)*.* L'ordinamento graduato-lex o glex per gli amici è simile al lessicografico, però prende in considerazione per prima cosa il frado di un monomio: formalmente diciamo che, dati $\alpha, \beta \in \mathbb{N}^n$ si ha $\alpha < \beta \iff |\alpha| < |\beta|$ oppure $|\alpha| = |\beta|$ e il primo termine non nullo da sinistra di $\alpha - \beta$ è negativo.

Esempio 2.2.3 (Ordinamento grlex)*.* Questo è il più strano dei tre ma funziona meglio per i calcoli al computer: dati $\alpha, \beta \in \mathbb{N}^n$ diciamo che $\alpha < \beta \iff |\alpha| < |\beta|$ oppure $|\alpha| = |\beta|$ e il primo termine non nullo da destra è positivo.

Si verifica abbastanza facilmente che ciascuno di questi ordinamenti soddisfa le proprietà (1) e (2) ma il buon ordinamento è un po' una carogna. Quindi diamo due criteri: uno generico per tutti gli ordinamenti ed uno migliore per gli ordinamenti monomiali:

Lemma 2.2.1. *Un ordinamento $<$ su un insieme X è un buon ordinamento se e solo se ogni catena discendente $x_1 \geq x_2 \geq x_3 \geq \cdots \geq x_n \geq x_{n+1} \geq \ldots$ si stabilizza*

Dimostrazione. ($\Longrightarrow$) sia $x_1 \geq x_2 \geq x_3 \geq \cdots \geq x_n \geq x_{n+1} \geq \ldots$ una catena discendente, allora l'insieme $\{ x_n \}$ ammette minimo x_m e quinid la catena si stabilizza a x_m.
($\Longleftarrow$) Supponendo per assurdo che $<$ non sia un buon ordinamento è facile costruire una catena discendente che non si stabilizza: infatti se A è un sottoinsieme non vuoto di X che non ammette minimo, preso un qualunque $x_1 \in A$ esiste $x_2 \in A$ tale che $x_1 > x_2$,...prseguendo così si trova l'assurdo. □

Proposizione 2.2.1. *Un ordinamento $<$ su $\mathbb{N}^n$ che gode delle proprietà (1) e (2) è un ordinamento monomiale se e solo se $0 < \alpha$ per ogni $\alpha \in \mathbb{N}^n$.*

Dimostrazione. ($\Longrightarrow$) Sia α il minimo elemento di $\mathbb{N}^n$ secondo l'ordinamento monomiale $<$: supponendo per assurdo che $\alpha < 0$, abbiamo che $2\alpha = \alpha + \alpha < 0 + \alpha = \alpha$ il che è impossibile.
($\Longleftarrow$) Intanto vediamo che,se $\beta = \alpha + \gamma$ con $\gamma \neq 0$, allora $\beta > \alpha$, infatti, sicuramente $\beta \neq \alpha$ e se fosse $\beta < \alpha$ allora si avrebbe che $\beta + \gamma < \alpha + \gamma = \beta$, il che è assurdo, perchè $0 < \gamma$ implica $\beta < \beta + \gamma$. Allora, sia $A \subseteq \mathbb{N}^n$: per il Lemma di Dickson, l'ideale $I = (\mathbf{x}^\alpha \mid \alpha \in A)$ è finitamente generato ed in particolare $I = (\mathbf{x}^{\alpha_1}, \ldots, \mathbf{x}^{\alpha_r})$ per certi $\alpha_i \in A$: allora sia μ il minimo degli α_i

secondo l'ordinamento $<$ che stiamo considerando (il minimo di un insieme finito esiste sempre): allora ci piacerebbe che μ fosse anche il minimo di A. Ma questo, fortunatamente, è vero perchè se $\alpha \in A$,allora $\alpha \geq \alpha_i$ per un certo α_i e quindi $\alpha \geq \mu$. □

Osservazione 2.2.4. La dimostrazione dell'ultima proposizione ci dice anche che se $<$ è un ordinamento monomiale su $k[\mathbf{x}]$, allora se $\mathbf{x}^\alpha \mid \mathbf{x}^\beta$ si ha che $\mathbf{x}^\alpha < \mathbf{x}^\beta$. Il viceversa tuttavia non vale: infatti, con l'ordinamento lessicografico $(x > y)$ su $k[x, y]$ si ha che $y < x$ ma $y \nmid x$.

Terminiamo questa parte sugli ordinamenti con un po' di definizioni: se $<$ è un ordinamento monomiale su $k[\mathbf{x}]$ e $f(\mathbf{x}) = \sum c_i \mathbf{x}^{\alpha_i}$ definiamo $\mathrm{Deg}(f)$ come il massimo degli α_i e definiamo il leading term di f, $\mathrm{lt}(f)$, come il termine di f corrispondente a $\mathrm{Deg}(f)$ ed il leading coefficient,$\mathrm{lc}(f)$, ed il leading monomial,$\mathrm{lm}(f)$, come il coefficiente e la parte monomiale di $\mathrm{lt}(f)$ rispettivamente.

2.2.2 Algoritmo di divisione

Presentiamo finalmente l'algoritmo di divisione in $k[\mathbf{x}]$:

Teorema 2.2.1 (Algoritmo di divisione)**.** *Sia fissato un ordinamento monomiale su $k[\mathbf{x}]$ e siano $f \in k[\mathbf{x}]$ un polinomio e $(f_1, \ldots, f_s)$ un insieme ordinato di polinomi. Allora, esistono $a_i \in k[\mathbf{x}]$ e $r \in k[\mathbf{x}]$ tali che*

$$f = a_1 f_1 + a_2 f_2 + \cdots + a_s f_s + r$$

ed inoltre

1. *$Deg(a_i f_i) \leq Deg(f)$.*
2. *$lt(f_i)$ non divide nessun termine di r.*

Dimostrazione. Scriviamo l'algoritmo in pseudocodice: **ALGORITMO DA SCRIVERE** Vediamo che l'algoritmo termina sempre: infatti ad ogni passaggio si passa da un polinomio f ad un polinomio f' tale che $\mathrm{Deg}(f) > \mathrm{Deg}(f)$, quindi, se l'algoritmo non terminasse, avremmo una catena discendente infinita $\mathrm{Deg}(f) > \mathrm{Deg}(f') > \mathrm{Deg}(f'') > \ldots$ il che è assurdo perchè $<$ è un ordinamento monomiale. Poi è facile vedere che gli $a_1, a_2, \ldots, a_s, r$ restituiti dall'algoritmo godono delle proprietà richieste. □

Quest'algoritmo è molto buono, però ha alcune magagne.

Osservazione 2.2.5. Il fatto che gli f_i formino un insieme ordinato è importante: infatti il risultato dell'algoritmo dipende fortemente dall'ordinamento degli f_i. **ESEMPIO DA INSERIRE**.

Osservazione 2.2.6. Sia $I = (f_1, \ldots, f_s)$ un ideale di $k[\mathbf{x}]$ e sia $f \in k[\mathbf{x}]$: allora se dividiamo f per $(f_1, \ldots, f_s)$ ed otteniamo un resto zero, questo implica che $f \in I$. Tuttavia il viceversa non è in generale vero: **ESEMPIO DA INSERIRE**.

Però non disperiamo: nel prossimo paragrafo riusciremo a risolvere questi problemi!

2.3 Basi di Grobner

Sia I un ideale di $k[\mathbf{x}]$ e sia $<$ un ordinamento monomiale su $k[\mathbf{x}]$: allora definiamo $\mathrm{Lt}(I) := \{\, \mathrm{lt}(f) \mid f \in I \,\}$, vediamo che, praticamente per definizione, $(\mathrm{Lt}(I))$ è un ideale monomiale (perchè è generato dai leading monomial) e quindi, per il Lemma di Dickson esistono $f_1, \ldots, f_r \in I$ tali che $(\mathrm{lt}(f_1), \ldots, \mathrm{lt}(f_r)) = (\mathrm{Lt}(I))$. Abbiamo appena dimostrato l'esistenza delle Basi di Grobner:

Definizione 2.5 (Base di Grobner)**.** Sia $<$ un ordinamento monomiale su $k[\mathbf{x}]$ e sia $I \subseteq k[\mathbf{x}]$ un ideale. Allora $G = \{\, g_1, \ldots, g_r \,\} \subseteq I$ è una Base di Grobner (o BdG) per I secondo l'ordinamento $<$ se $\mathrm{Lt}(G) = \{\, \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_r) \,\}$ genera $(\mathrm{Lt}(I))$.

le BdG hanno proprio le proprietà che ci servono per migliorare l'algoritmo di divisione:

Teorema 2.3.1. *Sia $<$ un ordinamento monomiale e sia $G = \{\, g_1, \ldots, g_s \,\}$ una BdG per l'ideale I. Sia poi $f \in k[\mathbf{x}]$, allora:*

1. *Esiste un unico* $r \in k[\mathbf{x}]$ *tale che* $f = g + r$ *con* $g \in I$ *e tale che nessun termine di* r *è diviso da alcun* $lt(g_i)$.

2. *Il resto della divisione di* f *per* G *non dipende dall'ordine dei* g_i. *Indichiamo questo resto con* $\overline{f}^G$.

3. $f \in I \iff \overline{f}^G = 0$.

4. $I = (g_1, \dots, g_s)$.

Dimostrazione. 1. Sicuramente un tale r esiste: basta eseguire la divisione di f per $(g_1, \dots, g_s)$ e prendere il resto. Ora mostriamo che è unico: supponiamo che $f = g + r = g' + r'$ con $g, g \in I$ e r, r' tali che nessun loro termine è diviso da alcun $\mathrm{lt}(g_i)$. Allora $r - r' = g' - g \in I$ e, se fosse $r - r' \neq 0$ avremmo che $\mathrm{lt}(r - r') \in (\mathrm{Lt}(I))$ e quindi esisterebbe un g_i tale che $\mathrm{lt}(g_i) \mid \mathrm{lt}(r - r')$ il che è assurdo, quindi dev'essere $r - r' = 0$.

2. Segue subito dal punto precedente.

3. Supponiamo che $f \in I$ ed eseguiamo la divisione di f per G: allora $f = a_1 g_1 + \cdots + a_s g_s + \overline{f}^G$ e quindi $\overline{f}^G = f - a_1 g - 1 - \cdots - a_s g_s \in I$ e quindi, se fosse $\overline{f}^G \neq 0$, si avrebbe che $\mathrm{lt}(\overline{f}^G) \in \mathrm{Lt}(I)$ e quindi esisterebbe $g - i$ tale che $\mathrm{lt}(g_i) \mid \mathrm{lt}(\overline{f}^G)$ il che è assurdo. Quindi $\overline{f}^G = 0$. Il viceversa è chiaro.

4. Poichè $G \subseteq I$ si ha che $(g_1, \dots, g_s) \subseteq I$. Ora, sia $f \in I$, allora $\overline{f}^G = 0$ e quindi $f = \sum a_i g_i$ per certi $a_i \in k[\mathbf{x}]$ e quindi $I \subseteq (g_1, \dots, g_s)$.

□

Corollario 2.3.1 (Teorema della base di Hilbert)**.** $k[\mathbf{x}]$ *è noetheriano.*

Dimostrazione. Per il teorema precedente, ogni ideale di $k[\mathbf{x}]$ è finitamente generato da una sua BdG, e quindi $k[\mathbf{x}]$ è noetheriano. □

Quindi in genere si ripete la situazione che avevamo visto per gli ideali monomiali: in particolare, poichè ogni ideale ammette una BdG ne esisterà almeno una di cardinalità minima. Quindi diamo la seguente definizione:

Definizione 2.6 (Base di Grobner minimale)**.** Sia $<$ un ordinamento monomiale su $k[\mathbf{x}]$ e sia $I \subseteq k[\mathbf{x}]$ un ideale. Allora diciamo che una BdG $G = \{ g_1, \dots, g_s \}$ per I è minimale se i g_i sono monici e se è una BdG di cardinalità minima.

Proposizione 2.3.1 (Criterio di minimalità per le BdG)**.** *Sia* $<$ *un ordinamento monomiale su* $k[\mathbf{x}]$ *e sia* $I \subseteq k[\mathbf{x}]$ *un ideale. Sia poi* $G = \{ g_1, \dots, g_s \}$ *una BdG per* I *con i* g_i *monici. Allora sono equivalenti:*

1. G *è minimale.*

2. $lt(g_i) \nmid lt(g_j)$ *se* $i \neq j$.

3. $Lt(G) = \{ lt(g_1), \dots, lt(g_s) \}$ *è l' escalier di* $(Lt(I))$.

Dimostrazione. Osserviamo che G è una BdG minimale per I se e solo se $\mathrm{Lt}(G)$ è un insieme di generatori minimale per $(\mathrm{Lt}(I))$. Quindi la tesi segue subito ricordando la Prop 2.1.2. □

Osservazione 2.3.1. Ricordando l' Oss 2.1.1 abbiamo anche un **algoritmo per trovare una BdG minimale**: se G è una BdG per un ideale I, si può ottenere una BdG minimale da G semplicemente eliminando tutti i polinomi il cui termine di testa è diviso dal termine di testa di un altro polinomio.

Osservazione 2.3.2. Si vede però che c'è una differenza con gli ideali monomiali: infatti uno stesso ideale I può ammenttere BdG minimali differenti. **ESEMPIO DA INSERIRE**. Però si può risolvere questo problema richiedendo qualcosina in più:

Definizione 2.7 (Base di Grobner ridotta)**.** Sia $<$ un ordinamento monomiale su $k[\mathbf{x}]$ e sia $I \subseteq k[\mathbf{x}]$ un ideale. Una Bdg $G = \{ g_1, \dots, g_s \}$ di I si dice ridotta se:

1. G è una BdG minimale.
2. $\mathrm{lt}(g_i)$ non divide nessun termine di g_j per $i \neq j$.

Proposizione 2.3.2. *Sia $<$ un ordinamento monomiale su $k[\mathbf{x}]$ e sia $I \subseteq k[\mathbf{x}]$ un ideale. Allora esiste un'unica BdG ridotta per I.*

Dimostrazione. Dimostriamo intanto l'unicità: se $G = \{ g_1, \dots, g_s \}$ e $G' = \{ g'_1, \dots, g'_s \}$ sono BdG ridotte per I allora in particolare sono BdG minimali e quindi, a meno di riordinare, possiamo supporre che sia $\mathrm{lt}(g_i) = \mathrm{lt}(g'_i)$ per $i = 1, \dots, s$ (infatti $\mathrm{Lt}(G) = \mathrm{Lt}(G')$ perchè sono entrambi l'escalier di $(\mathrm{Lt}(I))$). Allora consideriamo ad esempio $g_1 - g'_1$: abbiamo che $g_1 - g'_1 \in I$ e quindi $\overline{g_1 - g'_1}^G = 0$, tuttavia eseguendo la divisione, vediamo che tutti i termini di $g_1 - g'_1$ vanno nel resto: infatti se $\mathrm{lt}(g_1) = \mathrm{lt}(g'_1)$ dividesse uno di questi termini non sarebbe il termine di testa di g_1 per l'Oss 2.2.4 e poi $\mathrm{lt}(g_i) = \mathrm{lt}(g'_i)$ con $i > 1$ non divide nessuno di questi termini per l'ipotesi di BdG ridotta. Quindi si ha che $g_1 - g'_1 = \overline{g_1 - g'_1}^G = 0$ ed analogamente si vede che $g_i = g'_i$ per ogni $i = 1, \dots, s$.
Ora dimostriamo l'esistenza: lo facciamo dando un **algoritmo per calcolare la BdG ridotta** di un ideale: sia intanto $G = \{ g_1, \dots, g_s \}$ una BdG minimale per I. Allora sia $\overline{g_1}$ il resto della divisione di g_1 per $G \setminus \{ g_1 \}$ (secondo un ordine qualsiasi): vediamo che $\mathrm{lt}(\overline{g_1}) = \mathrm{lt}(g_1)$ per il criterio di minimalità per le BdG, quindi $G_1 = \{ \overline{g_1}, g_2, \dots, g_s \}$ è ancora una BdG minimale per I, e poi vediamo anche che $\mathrm{lt}(g_i)$ (con $i > 1$) non divide nessun termine di $\overline{g_1}$. Quindi, sia $\overline{g_2}$ il resto della divisione di g_2 per $G_1 \setminus g_2$ (secondo un ordine qualsiasi): allora vediamo di nuovo che $G_2 = \{ \overline{g_1}, \overline{g_2}, g_3, \dots, g_s \}$ è una BdG minimale per I e che $\mathrm{lt}(\overline{g_1}), \mathrm{lt}g_i$ (con $i > 2$) non dividono nessun termine di $\mathrm{lt}(\overline{g_2})$; inoltre vale anche che $\mathrm{lt}(\overline{g_2})$ non divide nessun termine di $\overline{g_1}$ perchè $lt(\overline{g_2}) = \mathrm{lt}(g_2)$. Allora, procedendo in questo modo, vediamo che G_s è la BdG ridotta di I. □

Abbiamo visto che le Basi di Grobner hanno proprietà molto utili e soprattutto facilmente calcolabili. Tuttavia il lettore attento avrà forse notato che non abbiamo ancora detto se c'è un metodo pratico per calcolare le BdG: fortunatamente il tizio che ha inventato le BdG ha pensato anche a questo.

2.3.1 Algoritmo di Buchberger

Definizione 2.8 (S-polinomio)**.** Sia $<$ un ordinamento monomiale su $k[\mathbf{x}]$ e siano $f, g \in k[\mathbf{x}]$ con $f, g \neq 0$. Poniamo $\mathbf{x}^\gamma = \mathrm{lcm}(lm(f), lm(g))$. Allora definiamo l'S-polinomio di f e g come:

$$S(f,g) = \frac{\mathbf{x}^\gamma}{\mathrm{lt}(f)} f - \frac{\mathbf{x}^\gamma}{\mathrm{lt}(g)} g.$$

Teorema 2.3.2 (Criterio di Buchberger)**.** *Sia $<$ un ordinamento monomiale su $k[\mathbf{x}]$ e sia $I = (f_1, \dots, f_r)$ un ideale di $k[\mathbf{x}]$. Allora $G = \{ g_1, \dots, g_r \}$ è una BdG per I se e solo se $\overline{S(g_i, g_j)}^G = 0$, per ogni i, j (dove con $\overline{S(g_i, g_j)}^G$ indichiamo il resto della divisione di $S(g_i, g_j)$ per G secondo un ordine qualsiasi).*

Dimostrazione. Sul Cox. □

Sempre Buchberger ha scoperto un algoritmo per calcolare BdG di un ideale:

Teorema 2.3.3 (Algoritmo di Buchberger)**.** *Sia $<$ un ordinamento monomiale su $k[\mathbf{x}]$ e sia $I = (f_1, \dots, f_r)$ un ideale. Allora si può calcolare una BdG di I in un numero finito di passi.*

Dimostrazione. scriviamo l'algoritmo: **ALGORITMO DA SCRIVERE** Vediamo che ad ogni passaggio dell'algoritmo l'ideale generato da G non cambia, e alla fine si ha che $\overline{S(g_i, g_j)}^G = 0$ per ogni i, j e quindi G è una BdG per I. Dobbiamo dimostrare solamente che l'algoritmo termina: ma, se questo non terminasse, otterremo una catena ascendente infinita $(\mathrm{Lt}(G_1)) \subseteq (\mathrm{Lt}(G_2)) \subseteq (\mathrm{Lt}(G_3)) \subseteq \dots$, il che è assurdo perchè $k[\mathbf{x}]$ è noetheriano. □

Visto che calcolare S-polinomi è abbastanza importante, analizziamoli un po' più da vicino:

Lemma 2.3.1. ***PROPRIETA' DEGLI S-POLINOMI DA COPIARE***

Capitolo 3

Risultanti

Definizione 3.1 (Risultante di due polinomi)**.** Sia R un anello e siano $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ e $g(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$ due polinomi in $R[x]$ non entrambi costanti. Allora definiamo la matrice di Sylvester di (f, g) come la matrice $(m+n) \times (m-n)$

$$Syl(f,g) := \begin{pmatrix} a_n & a_{n-1} & \cdots\cdots & a_1 & a_0 & & \\ & a_n & a_{n-1} & \cdots\cdots & a_1 & a_0 & \\ & & \ddots & \ddots & & \ddots & \ddots \\ & & & a_n & a_{n-1} & \cdots\cdots & a_1 & a_0 \\ b_m & b_{m-1} & \cdots\cdots & b_1 & b_0 & & & \\ & b_m & b_{m-1} & \cdots\cdots & b_1 & b_0 & & \\ & & \ddots & \ddots & & \ddots & \ddots & \\ & & & b_m & b_{m-1} & \cdots\cdots & b_1 & b_0 \end{pmatrix}$$

in cui i coefficienti di f sono ripetuti per m righe e i coefficienti di g sono ripetuti per n righe. Definiamo quindi il risultante di f e g come $Res(f,g) := \det Syl(f,g) \in R$.

Lemma 3.0.2 (Proprietà del risultante - (1))**.** *Sia R un anello e siano $f(x), g(x) \in R[x]$ due polinomi non entrambi costanti di grado n ed m rispettivamente. Allora si ha che*

1. $Res(g,f) = (-1)^{nm} Res(f,g)$
2. $Res(af, g) = a^m Res(f,g)$ *per* $a \in R$.
3. $Res(a,g) = a^m$ *per* $a \in R$.

Dimostrazione. La dimostrazione di tutte le proprietà segue facilmente dalle proprietà del determinante. □

Proposizione 3.0.3. *Sia D un dominio e siano $f, g \in D[x]$ non nulli e di gradi non entrambi nulli. Allora esistono due polinomi $A, B \in D[x]$ non nulli e con* $\deg A < \deg g$ *e* $\deg B < \deg f$ *tali che*

$$Af + Bg = Res(f,g)$$

Dimostrazione. Supponiamo che $f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ e che $g = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$: allora scriviamo due polinomi generici $A, B \in D[x]$ di grado minore di m ed n rispettivamente: abbiamo $A[x] = \alpha_{m-1}x^{m-1} + \alpha_{m-2}x^{m-2} + \cdots + \alpha_1 x + \alpha_0$ e $B[x] = \beta_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0$. Ora imponiamo che $Af + Bg = Res(f,g)$: troviamo la condizione equivalente:

$$\begin{aligned} a_n\alpha_{m-1} + b_m\beta_{n-1} &= 0 \\ a_{n-1}\alpha_{m-1} + a_n\alpha_{m-2} + b_{m-1}\beta_{n-1} + b_m\beta_{n-1} &= 0 \\ \vdots & \vdots \\ a_0\alpha_1 + a_1\alpha_0 + b_0\beta_1 + b_1\beta_0 &= 0 \\ a_0\alpha_0 + b_0\beta_0 &= Res(f,g). \end{aligned}$$

Allora ci accorgiamo che questo non è altro che un sistema lineare nelle incognite $\alpha_{m-1}, \alpha_{m-2}, \ldots, \alpha_0, \beta_{n-1}, \beta_{n-2},$ e, scrivendolo in forma matriciale vediamo che viene così:

$$\begin{pmatrix} a_n & & & & b_m & & & \\ a_{n-1} & a_n & & & b_{m-1} & b_m & & \\ \vdots & a_{n-1} & \ddots & & \vdots & b_{m-1} & \ddots & \\ \vdots & \vdots & \ddots & a_n & \vdots & \vdots & \ddots & b_m \\ a_1 & \vdots & & a_{n-1} & b_1 & \vdots & & b_{m-1} \\ a_0 & a_1 & & \vdots & b_0 & b_1 & & \\ & a_0 & \ddots & \vdots & & b_0 & \ddots & \\ & & \ddots & a_1 & & & \ddots & b_1 \\ & & & a_0 & & & & b_0 \end{pmatrix} \begin{pmatrix} \alpha_{m-1} \\ \alpha_{m-2} \\ \vdots \\ \vdots \\ \alpha_0 \\ \beta_{n-1} \\ \beta_{n-2} \\ \vdots \\ \vdots \\ \beta_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ 0 \\ Res(f,g) \end{pmatrix}$$

Quindi vediamo che la matrice M associata al sistema è proprio la trasposta di $Syl(f,g)$ ed in particolare si ha che $\det M = Res(f,g)$. Ora distinguiamo due casi:

- Supponiamo che $Res(f,g) = 0$, allora il sistema ha soluzioni non banali nel campo delle frazioni $Q = Q(D)$ e quindi esistono $\tilde{(}A), \tilde{(}B) \in Q[x]$ non entrambi nulli e di grado minore di m ed f rispettivamente tali che $\tilde{A}f + \tilde{B}g = 0$: allora, moltiplicando entrambi i membri dell'equazione per il prodotto di tutti i denominatori dei coefficienti di $\tilde{A}$ e $\tilde{B}$, otteniamo che esistono due polinomi $A, B \in D[x]$ di grado uguale ad $\tilde{A}, \tilde{B}$ rispettivamente e tali che $Af + Bg = 0$.

- Supponiamo ora che $Res(f,g) \neq 0$, allora la matrice M è invertibile e sappiamo che la sua inversa è data da $M^{-1} = \frac{1}{Res(f,g)}\text{cof } M$, dove cof M indica la matrice dei cofattori di M, che sappiamo essere a coefficienti in D. Allora l'unica soluzione del sistema precedente è data da

  $$\mathbf{x} = M^{-1}Res(f,g)\mathbf{e}_{m+n} = \frac{1}{Res(f,g)}Res(f,g)(\text{cof } M)\mathbf{e}_{m+n} = (\text{cof } M)\mathbf{e}_{m+n}$$

  che ha le componenti in D. Vittoria!

□

Corollario 3.0.2. *Sia D un UFD e siano $f, g \in D[x]$ non entrambi costanti. Allora sono equivalenti:*

1. *f e g hanno un fattore comune non costante.*
2. *esistono $A, B \in D[x]$ con $\deg A < \deg g$ e $\deg B < \deg f$ tali che $Af + Bg = 0$.*
3. *$Res(f,g) = 0$.*

Dimostrazione. (1 $\implies$ 2) Supponiamo che h, con $\deg h \geq 1$, sia un fattore comune di f e g, allora $f = \tilde{f}h$ e $g = \tilde{g}h$ per certi $\tilde{f}, \tilde{g} \in D[x]$. Allora si ha che $\tilde{g}f + (-\tilde{f})g = \tilde{g}\tilde{f}h - \tilde{f}\tilde{g}h = 0$ ed è chiaro che $\tilde{f}, \tilde{g}$ hanno grado minore di f e g rispettivamente, perchè h ha grado maggiore o uguale a 1.
(2 $\implies$ 1) Viceversa, supponiamo che esistano A e B come nell'enunciato: allora si ha che $Af = -Bg$.Quindi scomponiamo f in fattori irriducibili: $f = ap_1 \ldots p_s$ con $a \in D$ e $p_i \in D[x]$ e $\deg p_i \geq 1$; allora si ha che $p_i \mid Bg$ per ogni i e quindi, poichè gli irriducibili in un UFD sono anche primi, si ha che $p_i \mid B$ o $p_i \mid g$; ma se fosse che ogni p_i divide B, allora f dividerebbe B, il che è assurdo perchè $\deg f > \deg B$. Quindi esiste un p_i che divide g.
(2 $\implies$ 3) Se esistono A e B come nell'enunciato, allora la matrice M nella dimostrazione della Prop 3.0.3 è singolare, e quindi $\det M = Res(f,g) = 0$.
(3 $\implies$ 2) Segue subito dalla Prop 3.0.3. □

Osservazione 3.0.3. Sia R un anello e sia $f \in R[x]$ di grado positivo. Allora definiamo il discriminante di f come $\Delta(f) := Res(f, f')$, dove f' è la derivata (formale) di f. Quindi,il Corollario precedente ci dice che, se D è un UFD, allora f ha una radice multipla (eventualmente in un'opportuna estensione del campo dei quozienti di D) se e solo se $\Delta(f) = 0$. Vediamo allora che, se $f = ax^2 + bx + c$ è un polinomio di grado 2, questo risultato ci riporta a quanto conoscevamo già per le equazioni di secondo grado.

Effettivamente, possiamo studiare un po' più a fondo la correlazione fra risultante e fattori comuni: prendiamo un dominio D e consideriamo l'anello dei polinomi a n indeterminate $A = D[y_1, y_2, \dots, y_n]$: allora considero il polinomio $F_n(x) = (x - y_1)(x - y_2)\dots(x - y_n) \in A[x]$; sviluppando il prodotto, vediamo che $F_n(x) = a_n^{(n)}x^n + a_{n-1}^{(n)}x^{n-1} + \dots + a_1^{(n)}x + a_0^{(n)}$ dove gli $a_i^{(n)}$ sono in relazione alle funzioni simmetriche elementari in questo modo:

$$\begin{aligned} a_n^{(n)} &= 1 \\ a_{n-1}^{(n)} &= -(y_1 + y_2 y + \dots + y_n) \\ a_{n-2}^{(n-1)} &= y_1y_2 + y_1y_3 + \dots + y_{n-1}y_n \\ &\dots \\ a_0^{(n)} &= (-1)^n y_1y_2\dots y_n \end{aligned}$$

Quindi vediamo che le a_i sono funzioni multilineari negli y_i e vediamo anche che

$$\begin{aligned} &a_i^{(n)}(y_1, y_2, \dots, y_{n-1}, 0) = a_{i-1}^{(n-1}(y_1, y_2, \dots, y_{n-1}) \text{ per } i = 1, \dots, m \\ &a_0^{(n)}(y_1, y_2, \dots, y_{n-1}, 0) = 0 \end{aligned}$$

Allora abbiamo quello che ci serve per dimostrare un importante teorema:

Teorema 3.0.4. *Sia D un dominio e sia $A = D[y_1, \dots, y_n]$. Siano poi $F_n(x) = (x-y_1)\dots(x-y_n) \in A[x]$ e $g(x) \in D[x] \subset A[x]$. Allora*

$$Res(F_n, g) = \prod_{i=1}^{n} g(y_i)$$

.

Dimostrazione. Supponiamo che $g(x) = b_m x^m + b_{m-1}x^{m-1} + \dots + b_1 x + b_0$. Sviluppando $F_n(x)$, troviamo $F_n(x) = a_n^{(n)}x^n + a_{n-1}^{(n-1)} + \dots + a_1^{(n)}x + a_0^{(n)}$, dove gli $a_i^{(n)}$ sono quelli di cui ci siamo occupati sopra. Abbiamo perciò:

$$Syl(F_n, g) = \begin{pmatrix} a_n^{(n)} & a_{n-1}^{(n)} & \dots & a_1^{(n)} & a_0^{(n)} & & \\ & a_n^{(n)} & a_{n-1}^{(n)} & \dots & a_1^{(n)} & a_0^{(n)} & \\ & & \ddots & \ddots & & \ddots & \ddots \\ & & & a_n^{(n)} & a_{n-1}^{(n)} & \dots & a_1^{(n)} & a_0^{(n)} \\ b_m & b_{m-1} & \dots & b_1 & b_0 & & \\ & b_m & b_{m-1} & \dots & b_1 & b_0 & \\ & & \ddots & \ddots & & \ddots & \ddots \\ & & & b_m & b_{m-1} & \dots & b_1 & b_0 \end{pmatrix}$$

Allora, per $j = 1, \dots, m+n-1$, moltiplichiamo la j-esima colonna per y_n^{m+n-j} ed aggiungiamola all'ultima colonna: troviamo la matrice:

$$M = \begin{pmatrix} a_n^{(n)} & a_{n-1}^{(n)} & \dots & a_1^{(n)} & a_0^{(n)} & & & y_n^{m-1}F_n(y_n) \\ & a_n^{(n)} & a_{n-1}^{(n)} & \dots & a_1^{(n)} & a_0^{(n)} & & y_n^{m-2}F_n(y_n) \\ & & \ddots & \ddots & & \ddots & \ddots & \vdots \\ & & & a_n^{(n)} & a_{n-1}^{(n)} & \dots & a_1^{(n)} & F_n(y_n) \\ b_m & b_{m-1} & \dots & b_1 & b_0 & & & y_n^{n-1}g(y_n) \\ & b_m & b_{m-1} & \dots & b_1 & b_0 & & y_n^{n-2}g(y_n) \\ & & \ddots & \ddots & & \ddots & \ddots & \vdots \\ & & & b_m & b_{m-1} & \dots & b_1 & g(y_n) \end{pmatrix} =$$

quindi vediamo che

$$\det M = g(y_n) \det \begin{pmatrix} a_n^{(n)} & a_{n-1}^{(n)} & \dots & a_1^{(n)} & a_0^{(n)} & & & 0 \\ & a_n^{(n)} & a_{n-1}^{(n)} & \dots & a_1^{(n)} & a_0^{(n)} & & 0 \\ & & \ddots & \ddots & & \ddots & \ddots & \vdots \\ & & & a_n^{(n)} & a_{n-1}^{(n)} & \dots & a_1^{(n)} & 0 \\ b_m & b_{m-1} & \dots & b_1 & b_0 & & & y_n^{n-1} \\ & b_m & b_{m-1} & \dots & b_1 & b_0 & & y_n^{n-2} \\ & & \ddots & \ddots & & \ddots & \ddots & \vdots \\ & & & b_m & b_{m-1} & \dots & b_1 & 1 \end{pmatrix} = g(y_n) \det N$$

e cioè

$$Res(F_n, g) = \det Syl(F_n, g) = \det M = g(y_n) \det N$$

Allora, consideriamo $Res(F_n, g)$ come un polinomio nell'indeterminata y_n: vediamo che, essendo gli $a_i^{(n)}$ di grado 1 in y_n se $i \neq n$ e di grado 0 se $i = n$, $Res(F_n, g)$ ha grado al più m in y_n; tuttavia, $g(y_n)$ ha già grado m in y_m e quindi $\det N$ dev'essere indipendente da y_n. Quindi, per calcolarlo, possiamo porre $y_n = 0$: allora, vediamo, finalmente, che

$$\det N = \det \begin{pmatrix} a_{n-1}^{(n-1)} & a_{n-2}^{(n-1)} & \dots & a_0^{(n-1)} & & & & 0 \\ & a_{n-1}^{(n-1)} & a_{n-2}^{(n-1)} & \dots & a_0^{(n-1)} & & & 0 \\ & & \ddots & \ddots & & \ddots & \ddots & \vdots \\ & & & a_{n-1}^{(n-1)} & a_{n-2}^{(n-1)} & \dots & a_0^{(n-1)} & 0 \\ b_m & b_{m-1} & \dots & b_1 & b_0 & & & 0 \\ & b_m & b_{m-1} & \dots & b_1 & b_0 & & 0 \\ & & \ddots & \ddots & & \ddots & \ddots & \vdots \\ & & & b_m & b_{m-1} & \dots & b_1 & 1 \end{pmatrix}$$

Allora calcoliamo questo determinante sviluppando lungo l'ultima colonna: se $n = 1$, vediamo che $\det N = 1$, altrimenti, vediamo che $\det N = Res(F_{n-1}, g$; quindi, se $n = 1$, $Res(F_1, g) = g(y_1)$, altrimenti $Res(F_n, g) = g(y_n)Res(F_{n-1}, g)$. Quindi la tesi segue facilmente per induzione. □

Segue facilmente questo utile corollario:

Corollario 3.0.3. *Sia D un dominio e sia $A = D[\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$; siano poi $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_1)$, $g(x) = b_m \prod_{j=1}^{m}(x - \beta_j)$ polinomi (con $a_n, b_m \in D$) in $A[x]$. Allora*

$$Res(f, g) = a_n^m \prod_{i=1}^{n} g(\alpha_i)$$

$$Res(f, g) = (-1)^{nm} b_m^n \prod_{j=1}^{m} f(\beta_j)$$

$$Res(f, g) = a_n^m b_m^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j)$$

E anche questo:

Corollario 3.0.4 (Proprietà del risultante - (2))**.** *Sia D un dominio e siano $f, g_1, g_2 \in D[x]$ non costanti. Allora*

$$Res(f, g_1 g_2) = Res(f, g_1) Res(f, g_2).$$

Dimostrazione. Consideriamo f, g_1, g_2 come polinomi nel campo dei quozienti $Q = Q(D)$: allora, estendendo Q ad un campo algebricamente chiuso K, possiamo supporre che $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_1)$ e quindi la tesi segue agilmente dal Teorema 3.0.4 □

Come ultima applicazione del risultante diamo questo teorema:

Teorema 3.0.5 (Loos 1973)**.** *Sia D un dominio e sia $A = D[\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m]$; siano poi $f(x) = a_n \prod_{i=1}^{n}(x - \alpha_1)$, $g(x) = b_m \prod_{j=1}^{m}(x - \beta_j)$ polinomi di grado positivo (con $a_n, b_m \in D$) in $A[x]$. Allora*

1. *$r(x) = Res(f(y), g(x - y))$ è un polinomio che ha come uniche radici $\beta_j + \alpha_i$.*
2. *$r(x) = Res(f(y), g(x + y))$ è un polinomio che ha come uniche radici $\beta_j - a_i$.*
3. *$r(x) = Res(f(y), y^m g(\frac{x}{y}))$ è un polinomio che ha come uniche radici $\beta_j \alpha_i$.*
4. *$r(x) = Res(f(y), g(xy))$ è un polinomio che ha come uniche radici $\frac{\beta_j}{\alpha_i}$ (naturalmente dev'essere $\alpha_i \neq 0$).*

Dimostrazione.

1. $r(x) = Res(f(y), g(x - y)) = a_n^m \prod g(x - \alpha_i) = a_n^m b_m^n \prod (x - \alpha_i - \beta_j) = a_n^m b_m^n \prod (x - (\alpha_i + \beta_j))$.
2. $r(x) = Res(f(y), g(x+y)) = a_n^m \prod g(x+\alpha_i) = a_n^m b_m^n \prod (x+\alpha_i-\beta_j) = a_n^m b_m^n \prod (x-(\beta_j-\alpha_i))$.
3. $r(x) = Res(f(y), y^m g(\frac{x}{y})) = a_n^m \prod \alpha_i^m g(\frac{x}{\alpha_i}) = a_n^m b_m^n \prod \alpha_i^m \prod (\frac{x}{\alpha_i} - \beta_j) = a_n^m b_m^n \prod (x - \alpha_i \beta_j)$.
4. $r(x) = Res(f(y), g(xy)) = a_n^m \prod g(x\alpha_i)) = a_n^m b_m^n \prod (x\alpha_i - \beta_j) = a_n^m b_m^n \prod \alpha_i^m (x - \frac{\beta_j}{\alpha_i})$.

□

Capitolo 4

Ideali e Varietà

Ritorniamo al nostro amato $k[\mathbf{x}]$: una delle cose che facciamo di solito con un polinomio è trovarne gli zeri, quindi se prendiamo $S \subseteq k[\mathbf{x}]$, ha senso considerare $\mathbf{V}(S) := \{\, \mathbf{c} \in k^n \mid f(\mathbf{c}) = 0 \quad \forall\ f \in S \,\}$: tuttavia si vede facilmente che, se $I = (S)$ è l'ideale generato da S abbiamo che $\mathbf{V}(I) = \mathbf{V}(S)$: infatti se $\mathbf{c} \in \mathbf{V}(I)$, allora, poichè $I \supseteq S$, in particolare $\mathbf{c} \in \mathbf{V}(S)$; viceversa, sia $\mathbf{c} \in \mathbf{V}(S)$, allora ogni elemento $f \in I$ è del tipo $f = \sum c_i f_i$ con $f_i \in S$, e quindi $\mathbf{c} \in \mathbf{V}(I)$. Allora diamo la seguente definizione:

Definizione 4.1 (Varietà)**.** Sia I un ideale di $k[\mathbf{x}]$: allora definiamo la varietà relativa a I come

$$\mathbf{V}(I) := \{\, \mathbf{c} \in k^n \mid f(\mathbf{c}) = 0 \quad \forall\ f \in I \,\}$$

Lemma 4.0.3 (Proprietà di $\mathbf{V}(*)$)**.** *Siano $I, J \subseteq k[\mathbf{x}]$ ideali. Allora*

1. $I \subseteq J \implies \mathbf{V}(I) \supseteq \mathbf{V}(J)$
2. $\mathbf{V}(I + J) = \mathbf{V}(I) \cap \mathbf{V}(J)$ *(vale anche per somma arbitraria di ideali)*
3. $\mathbf{V}(IJ) = \mathbf{V}(I \cap J) = \mathbf{V}(I) \cup \mathbf{V}(J)$ *(vale anche per intersezione e prodotto arbitrari)*
4. $\mathbf{V}(I^n) = \mathbf{V}(I)$
5. $\mathbf{V}(\sqrt{I}) = \mathbf{V}(I)$

Dimostrazione.

1. Sia $\mathbf{c} \in \mathbf{V}(J)$, allora $f(\mathbf{c}) = 0$ per ogni $f \in J$ ed in particolare $f(\mathbf{c}) = 0$ per ogni $f \in I$, quindi $\mathbf{c} \in \mathbf{V}(I)$.
2. $I + J \supseteq I, J$, quindi $\mathbf{V}(I) \subseteq \mathbf{V}(I) \cap \mathbf{V}(J)$. Tuttavia, se $\mathbf{c} \in \mathbf{V}(I) \cap \mathbf{V}(J)$ e $h = f + g \in I + J$ con $f \in I, g \in J$,allora $h(\mathbf{c}) = 0$, quindi $\mathbf{V}(I) \cap \mathbf{V}(J) \subseteq \mathbf{V}(I + J)$.
3. $IJ \subseteq I \cap J \subseteq I$ e $IJ \subseteq I \cap J \subseteq J$, quindi $\mathbf{V}(IJ) \supseteq \mathbf{V}(I \cap J) \supseteq \mathbf{V}(I) \cup \mathbf{V}(J)$. Viceversa, supponiamo per assurdo che esista $\mathbf{c} \in \mathbf{V}(IJ)$ e $\mathbf{c} \notin \mathbf{V}(I) \cup \mathbf{V}(J)$, allora esistono $f \in I$ e $g \in J$ tali che $f(\mathbf{c}) \neq 0$ e $g(\mathbf{c}) \neq 0$, ma allora $(fg)(\mathbf{c}) \neq 0$, il che è impossibile.
4. Segue subito dal punto precedente.
5. Abbiamo che $I \subseteq \sqrt{I}$ e quindi $\mathbf{V}(I) \supseteq \mathbf{V}(\sqrt{I})$; viceversa, sia $\mathbf{c} \in \mathbf{V}(I)$ e sia $f \in \sqrt{I}$: allora $f^n \in I$ per un certo $n \in \mathbb{N}$ e quindi $f^n(\mathbf{c}) = 0$ e cioè $f(\mathbf{c}) = 0$, quindi $\mathbf{V}(I) \subseteq \mathbf{V}(\sqrt{I})$.

□

Allora, visto che abbiamo le varietà, perchè non fare la stessa cosa a rovescia? Prendiamo un insieme $E \subseteq k^n$ allora ci chiediamo quali sono i polinomi che si annullano contemporaneamente su E, cioè vogliamo conoscere $\mathbf{I}(E) := \{\, f \in k[\mathbf{x}] \mid f(\mathbf{c}) = 0 \ \ \forall\ \mathbf{c} \in E \,\}$. Tuttavia, per simmetria, ci occupiamo solo del caso in cui $E = V$ è una varietà.

Lemma 4.0.4 (Proprietà di $\mathbf{I}(*)$)**.** *Siano $V, W \subseteq k^n$ varietà. Allora*

1. $\mathbf{I}(V)$ *è un ideale radicale.*

2. $V \subseteq W \implies \mathbf{I}(V) \supseteq \mathbf{I}(W)$.

3. $\mathbf{I}(V \cup W) = \mathbf{I}(V) \cap \mathbf{I}(W)$.

4. $\mathbf{I}(V \cap W) \supseteq \mathbf{I}(V) + I(W)$ *ma in generale non c'è uguaglianza .*

Dimostrazione. 1. Siano $f, g \in \mathbf{I}(V)$, allora si vede facilmente che $f + g \in \mathbf{I}(V)$ e che $af \in \mathbf{I}(V)$ per ogni $a \in k$: infatti, se $\mathbf{c} \in V$, allora $(f + g)(\mathbf{c}) = f(\mathbf{c}) + g(\mathbf{c}) = 0 + 0 = 0$ e $(af)(\mathbf{c}) = af(\mathbf{c}) = a0 = 0$. Mostriamo che $\mathbf{I}(V)$ è radicale: supponiamo che $f^m \in \mathbf{I}(V)$ per un certo $m \in \mathbb{N}$, allora $f(\mathbf{c})^m = 0$ per ogni $\mathbf{c} \in V$ e quindi $f(\mathbf{c}) = 0$ per ogni $\mathbf{c} \in V$, cioè $f \in \mathbf{I}(V)$.

2. Sia $f \in \mathbf{I}(W)$, allora $f(\mathbf{c}) = 0$ per ogni $\mathbf{c} \in W$ e in particolare $f(\mathbf{c}) = 0$ per ogni $\mathbf{c} \in V$; quindi $f \in \mathbf{I}(V)$.

3. $V \cup W \supseteq V, W$, quindi $\mathbf{I}(V \cup W) \subseteq \mathbf{I}(V) \cap \mathbf{I}(W)$. Viceversa, se $f \in \mathbf{I}(V) \cap \mathbf{I}(W)$, allora $f(\mathbf{c}) = 0$ per ogni $\mathbf{c} \in V$ e per ogni $\mathbf{c} \in W$ e quindi $f \in \mathbf{I}(V \cup W)$.

4. $V \cap W \subseteq V, W$ quindi $\mathbf{I}(V \cap W) \supseteq \mathbf{I}(V) + \mathbf{I}(W)$. Per vedere che il viceversa è in generale falso, consideriamo in $\mathbb{R}[x, y]$ $V = \mathbf{V}(x^2 - y)$ e $W = \mathbf{V}(y - 1)$: allora, graficamente si vede bene che $V \cap W = \emptyset$ ma $\mathbf{I}(V) + \mathbf{I}(W) \neq \mathbb{R}[x, y] = I(\emptyset)$.

□

Allora, vediamo che abbiamo stabilito due mappe:

$$\{ \text{ ideali di } k[\mathbf{x}] \} \longrightarrow \{ \text{ varietà di } k^n \}$$
$$J \mapsto \mathbf{V}(J)$$

$$\{ \text{ varietà di } k^n \} \longrightarrow \{ \text{ ideali di } k[\mathbf{x}] \}$$
$$W \mapsto \mathbf{I}(W)$$

Il nostro obbiettivo di adesso è indagare la relazione fra queste due applicazioni. In particolare vediamo subito che

Lemma 4.0.5. 1. $\mathbf{I}(\mathbf{V}(J)) \supseteq \sqrt{J}$. *Ma in generale non vale l'uguaglianza.*

2. $\mathbf{V}(\mathbf{I}(W)) = W$. *Quindi la mappa* $W \mapsto \mathbf{I}(W)$ *è iniettiva.*

Dimostrazione. 1. Sia $f \in \sqrt{J}$, allora esiste $n \in \mathbb{N}$ tale che $f^n \in J$ e quindi se $\mathbf{c} \in \mathbf{V}(J)$, si ha che $f^n(\mathbf{c}) = 0$, ma allora $f(\mathbf{c}) = 0$ e abbiamo finito. **INSERIRE CONTROESEMPIO**.

2. Supponiamo che $W = \mathbf{V}(J)$ per un certo ideale J. Allora $\mathbf{V}(\mathbf{I}(W)) = \mathbf{V}(\mathbf{I}(\mathbf{V}(J))) \subseteq \mathbf{V}(\sqrt{J}) = \mathbf{V}(J) = W$. Viceversa, se $\mathbf{c} \in W$, allora segue dalla definizione che $\mathbf{c} \in \mathbf{V}(\mathbf{I}(W))$.

□

4.1 Eliminazione ed Estensione

Teorema 4.1.1 (Proprietà di Eliminazione dell'ordinamento lex)**.** *Sia* $I \subset k[x_1, x_2, \ldots, x_n]$ *un ideale e sia* $G = \{ g_1, \ldots, g_s \}$ *una BdG di* I *per l'ordinamento lex* $(x_1 > x_2 > \cdots > x_n)$. *Siano poi il* $k-$*esimo ideale di eliminazione* $I_k = I \cap k[x_{k+1}, \ldots, x_n]$ *e* $G_k = G \cap k[x_{k+1}, \ldots, x_n]$. *Allora* G_k *è una BdG di* I_k *per l'ordinamento lex.*

Dimostrazione. Intanto vediamo che I_k è effettivamente un ideale di $k[x_{k+1}, \ldots, x_n]$: se consideriamo l'omomorfismo di immersione $i : k[x_k + 1, \ldots, x_n] \to k[x_1, \ldots, x_n]$, vediamo che $I_k = I^c$, e quindi è un ideale. Ora, sicuramente $G_k \subset I_k$, quindi dobbiamo solo verificare che $\mathrm{Lt}(G_k)$ genera $(\mathrm{Lt}(I_k))$: ma questo è immediato, perchè se $f \in I_k$, allora $\mathrm{lt}(f) \in (Lt(I))$ e quindi esiste g_i tale che $\mathrm{lt}(g_i) \mid \mathrm{lt}(f)$ e quindi $\mathrm{lt}(g_i) \leq \mathrm{lt}(f)$ secondo l'ordinamento lex; ma allora dev'essere che $g_i \in G_k$ e quindi abbiamo finito. □

Diamo ora due esempi di applicazione di questa proprietà:

Esempio 4.1.1 (Implicitizzazione). Supponiamo di avere un insieme di k^n descritto tramite equazioni parametriche:

$$\begin{aligned} x_1 &= f_1(t) \\ x_2 &= f_2(t) \\ &\vdots \\ x_n &= f_n(t) \end{aligned}$$

con gli f_i polinomi in $k[t]$: allora vogliamo esprimere quest'insieme come una varietà: allora calcoliamo una BdG G dell' ideale $I = (f_1(t) - x_1, f_2(t) - x_2, \ldots, f_n(t) - x_n)$ in $k[t, \mathbf{x}]$ con $t > x_1 > x_2 > \cdots > x_n$, allora $G \cap k[\mathbf{x}]$ ci da una BdG dell'ideale di eliminazione I_1 e la varietà $\mathbf{V}(I)$ è proprio quello che cercavamo. In verità, non è sempre possibile esprimere un insieme in forma parametrica come una varietà, ma questo metodo ci dà la più piccola varietà che contiene l'insieme.

Per il prossimo esempio abbiamo prima bisogno di un lemma:

Lemma 4.1.1. *Siano $I, J \subseteq k[\mathbf{x}]$ due ideali. Allora si ha che*

$$I \cap J = ((1-t)I + tJ) \cap k[\mathbf{x}]$$

dove il secondo ideale è visto in $k[\mathbf{x}, t]$.

Dimostrazione. Sia $f \in I \cap J$, allora $f = (1-t)f + tf$ e chiaramente $(1-t)f + tf \in ((1-t)I + tJ)$. Viceversa, sia $h = h(\mathbf{x}, t) = (1-t)f(\mathbf{x}) + tg(\mathbf{x}) \in ((1-t)I + tJ) \cap k[\mathbf{x}]$ con $f \in I$ e $g \in J$; allora, poichè $h(\mathbf{x}, t) \in k[\mathbf{x}]$, si ha che $h = h(\mathbf{x}, 0) = f(\mathbf{x})$ e $h = h(\mathbf{x}, 1) = g(\mathbf{x})$, perciò $h \in I \cap J$. □

Esempio 4.1.2 (Intersezione di ideali). Siano $I, J \in k[\mathbf{x}]$ due ideali. Allora, per calcolare $I \cap J$, basta calcolare una BdG G per l'ideale $(1-t)I + tJ$ in $k[\mathbf{x}, t]$ con l'ordinamento lessicografico $t > x_1 > x_2 > \cdots > x_n$, e poi prendere $G \cap k[\mathbf{x}]$.

Teorema 4.1.2 (Teorema di estensione)**.** *Sia k un campo algebricamente chiuso e sia $I = (f_1, \ldots, f_s)$ un ideale in $k[x_1, \mathbf{x}]$. Allora, scriviamo*

$$\begin{aligned} f_1(x_1, \mathbf{x}) &= g_1(\mathbf{x})x_1^{N_1} + (\textit{termini in cui } x_1 \textit{ ha grado} < N_1) \\ f_2(x_1, \mathbf{x}) &= g_2(\mathbf{x})x_1^{N_2} + (\textit{termini in cui } x_1 \textit{ ha grado} < N_2) \\ &\vdots \\ f_s(x_1, \mathbf{x}) &= g_s(\mathbf{x})x_1^{N_s} + (\textit{termini in cui } x_1 \textit{ ha grado} < N_s). \end{aligned}$$

Sia dunque $\mathbf{c} \in \mathbf{V}(I_1)$ e tale che $\mathbf{c} \notin \mathbf{V}(g_1, \ldots, g_x)$: allora esiste $c \in k$ tale che $(c, \mathbf{c}) \in \mathbf{V}(I)$.

Dimostrazione. Consideriamo l'omomorfismo di anelli

$$\begin{aligned} \phi : k[x_1, \mathbf{x}] &\longrightarrow k[x_1] \\ f(x_1, \mathbf{x}) &\mapsto f(x_1, \mathbf{c}) \end{aligned}$$

Allora, ϕ è surgettivo e quindi $\phi(I) = I^e$ è un ideale di $k[x_1]$ che è PID, e dunque $I^e = (u(x_1))$ per un certo $u(x_1)$. Ora, se $u(x_1)$ è non costante, allora, poichè k è algebricamente chiuso, esiste $\mathbf{c} \in k$ tale che $u(c) = 0$; ma allora $(c, \mathbf{c}) \in \mathbf{V}(I)$ e lo stesso discorso vale anche se $u(x_1) = 0$. Allora, supponiamo che $u(x_1)$ sia costante e non nullo: ciò significa che $1 \in I^e$ e quindi che esiste $f \in I$ tale che $f(x_1, \mathbf{c}) = 1$; ora, per ipotesi, abbiamo che $\mathbf{c} \notin \mathbf{V}(g_1, \ldots, g_s)$ e, quindi, senza perdita di generalità possiamo supporre che $g_1(\mathbf{c}) \neq 0$. Quindi sia

$$h(\mathbf{x}) = Res(f(x_1, \mathbf{x}), f_1(x_1, \mathbf{x})$$

abbiamo che $h(\mathbf{c}) = Res(f(x_1, \mathbf{c}), f_1(\mathbf{x}_1, \mathbf{c})) = Res(1, f_1(\mathbf{x}_1, \mathbf{c})) = 1^{N_1} = 1$ ma questo è assurdo perchè sappiamo che esistono $A, B \in k[x_1, \mathbf{x}]$ tali che $h = Af + Bf_1$ e quindi $h \in I_1$. Allora $u(x_1)$ non può essere costante e non nullo e quindi abbiamo finito. □

L'accoppiata eliminazione-estensione permette di generalizzare il metodo di sostituzione che usiamo di solito per risolvere i sistemi. Tuttavia il teorema di estensione porta a molte altre conseguenze interessanti, come vedremo fra poco.

4.2 Corrispondenza Ideali radicali-Varietà

Iniziamo con due teoremi fomdamentali:

Teorema 4.2.1 (Nullstellensatz debole)**.** *Sia k un campo algebricamente chiuso e sia I un ideale di $k[\mathbf{x}]$. Allora $\mathbf{V}(I) = \emptyset$ se e solo se $I = k[\mathbf{x}]$.*

Dimostrazione. Procediamo per induzione sul numero n di indeterminate:

- $n = 1$: allora I è un ideale di $k[x_1]$ che è PID e quindi $I = (u(x))$ per un certo $u(x-1) \in k[x_1]$. Allora, se $\mathbf{V}(I) = \emptyset$, dev'essere che $u(x_1)$ è costante e non nullo, quindi $1 \in I$.
- $n-1 \implies n$: supponiamo che $I = (f_1, \ldots, f_s)$. Se f_1 è costante, abbiamo finito, quindi supponiamo che $f_1 = f_1(x_1, \ldots, x_n)$ abbia grado totale (cioè il massimo grado dei suoi monomi) $N > 1$: allora consideriamo l'omomorfismo di valutazione:

$$\begin{aligned} \phi : k[x_1, x_2, \ldots, x_n] &\longrightarrow k[\tilde{x_1}, \tilde{x_2}, \ldots, \tilde{x_n}] \\ x_1 &\mapsto \tilde{x_1} \\ x_2 &\mapsto \tilde{x_2} + a_2\tilde{x_1} \\ &\vdots \\ x_n &\mapsto \tilde{x_n} + a_n\tilde{x_1} \end{aligned}$$

  allora, ϕ è un omomorfismo surgettivo, e quindi $\phi(I) = I^e$ è un ideale, inoltre si vede che $\mathbf{V}(I) = \emptyset \implies \mathbf{V}(I^e) = \emptyset$. Allora, vediamo che $\phi(f) = f(\tilde{x_1}, \tilde{x_2} + a_2\tilde{x_1}, \ldots, \tilde{x_n} + a_n\tilde{x_1}) = c(a_2, \ldots, a_n)x_1^N +$ (termini in cui x_1 ha grado $< N$) e $c(a_2, \ldots, a_n)$ è un polinomio negli a_i: allora vediamo che, poichè k è un campo algebricamente chiuso e quindi infinito, possiamo scegliere gli a_i in modo che $c(a_2, \ldots, a_n) \neq 0$(la verifica è lasciata per esercizio). Ma allora, dev'essere anche che $\mathbf{V}(I_1^e) = \emptyset$, altrimenti potremmo applicare il teorema di estensione ed ottenere che $\mathbf{V}(I^e) \neq 0$; perciò , per ipotesi induttiva, abbiamo che $1 \in I_1^e \subseteq I^e$. Ma allora, poichè ϕ non modifica le costanti, abbiamo anche che $1 \in I$ e abbiamo finito.

□

Teorema 4.2.2 (Nullstellensatz forte)**.** *Sia k un campo algebricamente chiuso e sia J un ideale di $k[\mathbf{x}]$. Allora*

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

Dimostrazione. Sia $J = (f_1, \ldots, f_s)$. Sappiamo che vale sempre che $\mathbf{I}(\mathbf{V}(J)) \supseteq \sqrt{J}$; quindi, sia $f \in \mathbf{I}(\mathbf{V}(J))$; allora, usiamo uno sporco trucco: consideriamo l'ideale $\tilde{J} = (f_1, \ldots, f_s, 1 - yf)$ in $k[\mathbf{x}, y]$ e mostriamo che $\mathbf{V}(\tilde{J}) = \emptyset$. Supponiamo che esista $(\mathbf{c}, v) \in \mathbf{V}(\tilde{J})$: allora $\mathbf{c} \in \mathbf{V}(J)$ e quindi $(1 - yf)(\mathbf{c}, v) = 1$, il che è assurdo. Quindi, per il Nullstellensatz debole, esistono $a_1(\mathbf{x}, y), \ldots, a_s(\mathbf{x}, y), a(\mathbf{x}, y) \in k[\mathbf{x}, y]$ tali che

$$\sum_{i=1}^{s} a_i(\mathbf{x}, y) f_i(\mathbf{x}) + a(\mathbf{x}, y)(1 - yf(\mathbf{x})) = 1$$

Allora, ponendo $y = \frac{1}{f}$ vediamo che otteniamo

$$\sum_{i=1}^{s} a_i(\mathbf{x}, \frac{1}{f}) f_i(\mathbf{x}) = 1$$

e quindi, moltiplicando ad entrambi i membri per una potenza opportuna di f , abbiamo che

$$\sum_{i=1}^{s} b_i(\mathbf{x}) f_i(\mathbf{x}) = f^m$$

per certi $\beta_i \in k[\mathbf{x}]$. Quindi esiste $m \in \mathbb{N}$ tale che $f^m \in J$, cioè $f \in \sqrt{J}$. □

Quindi, possiamo finalmente stabilire una corrispondenza fra ideali radicali e varietà

Corollario 4.2.1. *Sia k un campo algebricamente chiuso. Allora le due applicazioni*

$$\{ \textit{ ideali radicali di } k[\mathbf{x}] \} \longrightarrow \{ \textit{ varietà di } k^n \}$$
$$J \mapsto \mathbf{V}(J)$$

$$\{ \textit{ varietà di } k^n \} \longrightarrow \{ \textit{ ideali radicali di } k[\mathbf{x}] \}$$
$$W \mapsto \mathbf{I}(W)$$

sono inverse una dell'altra.

In particolare, possiamo vedere subito a quali varietà corrispondono gli ideali massimali di $k[\mathbf{x}]$:

Proposizione 4.2.1 (Corrispondenza Ideali massimali - punti)**.** *Sia k un campo algebricamente chiuso. Allora ogni ideale massimale di $k[\mathbf{x}]$ è del tipo $(x_1 - c_1, \ldots, x_n - c_n)$, cioè la corrispondenza ideali-varietà induce una corrispondenza biunivoca fra ideali massimali e punti di k^n.*

Dimostrazione. Sappiamo già che ogni ideale del tipo $I = (x_1 - c_1, \ldots, x_n - c_n)$ è massimale perchè $k[\mathbf{x}]/I \cong k$. Invece, sia $\mathfrak{m}$ un ideale massimale di $k[\mathbf{x}]$, allora $\mathfrak{m}$ è un ideale proprio e quindi $\mathbf{V}(\mathfrak{m}) \neq \emptyset$: quindi sia $\mathbf{c} = (c_1, c_2, \ldots, c_n) \in \mathbf{V}(\mathfrak{m})$, allora si ha che $\mathbf{I}(\mathbf{c}) \supseteq \mathbf{I}(\mathbf{V}(\mathfrak{m})) = \sqrt{\mathfrak{m}} = \mathfrak{m}$ e perciò $\mathfrak{m} = \mathbf{I}(\mathbf{c}) = (x_1 - c_1, x_2 - c_2, \ldots, x_n - c_n)$. □

Allora, ci chiediamo a cosa corrispondano gli ideali primi: la risposta è nella prossima sezione.

4.3 Ideali primi e varietà irriducibili

Definizione 4.2 (Varietà Irriducibile)**.** Una varietà $V \subseteq k^n$ si dice irriducibile se vale che

$$V = V_1 \cup V_2 \implies V = V_1 \text{ o } V = V_2$$

dove V_1, V_2 sono ancora varietà.

Proposizione 4.3.1. *Una varietà V è irriducibile se e solo se $\mathbf{I}(V)$ è primo.*

Dimostrazione. ($\Longrightarrow$) Supponiamo che $fg \in \mathbf{I}(V)$: allora $\mathbf{I}(V) = \mathbf{I}(V) \cup (fg)$ e quindi $V = \mathbf{V}(\mathbf{I}(V)) = \mathbf{V}(\mathbf{I}(V) \cup (fg)) = \mathbf{V}(\mathbf{I}(V)) \cap \mathbf{V}(fg) = V \cap (\mathbf{V}(f) \cup \mathbf{V}(g)) = (V \cap \mathbf{V}(f)) \cap (V \cap \mathbf{V}(g))$. Ma allora, dev' essere che $V = V \cap \mathbf{V}(f)$ o $V = V \cap \mathbf{V}(g)$: supponiamo che $V = V \cap \mathbf{V}(f)$, allora $V \subseteq \mathbf{V}(f)$ e quindi $\mathbf{I}(V) \supseteq \mathbf{I}(\mathbf{V}(f))$, perciò $f \in \mathbf{I}(V)$.
($\Longleftarrow$) Supponiamo che $V = V_1 \cap V_2$: allora $\mathbf{I}(V) = \mathbf{I}(V_1 \cap V_2) = \mathbf{I}(V_1) \cup \mathbf{I}(V_2)$, ma poichè $\mathbf{I}(V)$ è primo dev'essere $\mathbf{I}(V) = \mathbf{I}(V_1)$ o $\mathbf{I}(V) = \mathbf{I}(V_2)$, e cioè $V = V_1$ o $V = V_2$. □

Ora, supponiamo che $V_1 \supseteq V_2 \supseteq V_3 \supseteq \ldots$ sia una catena discendente di varietà in k^n: allora abbiamo che $\mathbf{I}(V_1) \subseteq \mathbf{I}(V_2) \supseteq \mathbf{I}(V_3) \ldots$ è una catena ascendente di ideali in $k[\mathbf{x}]$, che è noetheriano; quindi questa catena si stabilizza, e cioè esiste r tale che $\mathbf{I}(V_r) = \mathbf{I}(V_n)$ per ogni $n \geq r$. Ma, allora, questo implica che $V_r = V_n$ per ogni $n \geq r$; quindi vale la DCC (descending chain condition) sulle varietà di k^n. Questo ci permette di dimostrare la seguente proposizione:

Proposizione 4.3.2. *Ogni varietà V si scrive come intersezione finita di varietà irriducibili $V = \bigcup_{i=1}^{m} V_i$. Inoltre esiste una decomposizione tale che $V_i \nsubseteq V_j$ per ogni $i \neq j$: una tale decomposizione si dice irridondante. Inoltre la decomposizione irridondante è unica.*

Dimostrazione. Supponiamo che esista una varietà V che non possa essere scritta come unione finita di varietà irriducibili: allora, in particolare, V stessa non è irriducibile e quindi esistono V_1, V' tali che $V = V_1 \cup V'$ e $V \supsetneq V_1$ e $V \supsetneq V'$; in particolare, vediamo che almeno una fra V_1, V' non può essere scritta come unione finita di irriducibili, altrimenti lo sarebbe anche V: supponiamo che questa sia V_1, allora, con lo stesso argomento di prima, vediamo che esiste una varietà V_2 tale che $V_1 \supsetneq V_2$ e tale che V_2 non può essere scritta come unione di varietà irriducibili. Continuando così, costruiamo una catena discendente infinita $V \supsetneq V_1 \supsetneq V_2 \supsetneq \dots$, il che è assurdo per la DCC. Ora, da una decomposizione finita $V = \bigcup_{i=1}^m V_1$ è facile ottenere una decomposizione irridondante: basta eliminare i V_i che sono contenuti in un V_j per $j \neq i$. Mostriamo che questa decomposizione è unica: supponiamo che $V = \bigcap_{i=1}^n V_i = \bigcap_{j=1}^m V'_j$ siano due decomposizioni irridondanti: allora, $V_1 = V_1 \cap V = \bigcup(V_1 \cap V'_j)$ e quindi possiamo supporre che $V_1 = V_1 \cap V'_1$ e cioè che $V_1 \subseteq V'_1$. Lo stesso ragionamento ci dice anche che $V'_1 \subseteq V_i$ per un cero i, ma allora si ha che $V_1 \subseteq V'_1 \subseteq V_i$ e per l'irridondanza dev'essere che $V_i = V_1$. In questo modo si prova che le due decomposizioni coincidono: infatti, supponendo $n \leq m$, procedendo come abbiamo fatto prima, vediamo che $V_i = V'_i$ per $i = 1, 2, \dots, n$ e a questo punto supponiamo che $m > n$, allora, abbiamo che, per $j \geq n$, $V'_j \subseteq V = \bigcap_{i=1}^n V_i = \bigcap_{i=1}^n V'_i$ e quindi $V'_j \subseteq V'_i$ per un certo $i < j$, il che è assurdo, perchè la decomposizione è irridondante. □

Un risultato analogo vale per gli ideali di $k[\mathbf{x}]$:

Teorema 4.3.1. *1. Ogni ideale radicale I di $k[\mathbf{x}]$ si scrive come intersezione finita di ideali primi: $I = \bigcup_{i=1}^m I_i$. Inoltre esiste una decomposizione irridondante, cioè tale che $I_i \not\supseteq I_j$ per $i \neq j$, ed è unica.*

2. Gli ideali primi della decomposizione irridondante di I sono esattamente gli ideali primi della famiglia $\{ (I : f) \mid f \in k[\mathbf{x}] \}$

Dimostrazione. 1. Dimostriamo l'esistenza solo nel caso in cui k è un campo algebricamente chiuso: sia I un ideale radicale, allora consideriamo la decomposizione irridondante della sua varietà $\mathbf{V}(I) = \bigcap_{i=1}^m V_i$: per il Nullstellensatz, si ha che $I = \mathbf{I}(\mathbf{V}(I)) = \mathbf{I}(\bigcap_{i=1}^m V_i) = \bigcup_{i=1}^m \mathbf{I}(V_i)$ e $\mathbf{I}(V_i)$ sono ideali primi; inoltre, poichè $V_i \not\subseteq V_j$ per $i \neq j$, allora $\mathbf{I}(V_i) \not\supseteq \mathbf{I}(V_j)$ per $i \neq j$. Abbiamo mostrato che esiste una decomposizione irridondante, vediamo che è unica: supponiamo che $I = \bigcap_{i=1}^n I_i = \bigcap_{j=1}^m I'_j$ siano due decomposizioni irridondanti, allora $I_1 \supseteq \bigcup_{j=1}^m I'_j$ e quindi dev'essere che $I_1 \supseteq I'_j$ per un certo j; possiamo supporre senza problemi che $I_1 \supseteq I'_1$,...poi si continua in modo analogo a come fatto per le varietà...

2. Intanto, si vede facilmente che, se P è un ideale primo, allora $(P : f) = k[\mathbf{x}]$ se $f \in P$ e $(P : f) = P$ altrimenti. Supponiamo che $I = \bigcup_{i=1}^m I_i$ sia la decomposizione irriducibile di I. Allora, preso $f \in k[\mathbf{x}]$, vediamo che $(I : f) = (\bigcap_{i=1}^m : f) = \bigcap_{i=1}^m (I_i : f)$ quindi, se $(I : f)$ è primo, allora, $(I : f) = (I_i : f)$ per un certo i, e visto che non può essere $(I : f) = k[\mathbf{x}]$, dev'essere che $(I : f) = (I_i : f) = I_i$. Viceversa, per vedere che ogni I_i può essere ottenuto come $(I : f_i)$: basta scegliere $f_i \in \bigcap_{j \neq i}$ e $f \notin I_i$ (vediamo che un tale f esiste per l'irridondanza).

□