UNIVERSITÀ DEGLI STUDI DI MESSINA

Ideali Monomiali con applicazioni computazionali

Luca Amata

Anno Accademico 2020 - 2021

Indice

Introduzione **2**

1 Nozioni di base **2**

2 Operazioni tra ideali monomiali **4**

3 Radicale di un ideale monomiale **9**

4 Ideali monomiali Primi e Massimali **11**

5 Decomposizione Primaria di ideali monomiali **12**

Bibliografia **19**

Introduzione

Gli *ideali monomiali* costituiscono una particolare classe fra tutti gli ideali dell'anello dei polinomi $S = K[x_1, x_2, \dots, x_n]$. Un ideale si dice monomiale se generato da monomi, cioè se esiste un insieme di monomi che genera l'ideale.
Lo studio di tali ideali è più semplice, rispetto al caso generale, poiché alcuni metodi algoritmici costruiti *ad hoc* permettono di effettuare calcoli molto più semplicemente (e velocemente). Ciò è principlamente dovuto al fatto che la struttura degli ideali monomiali possiede maggiore regolarità ed è possibile studiarli applicando spesso dei procedimenti legati all'analisi combinatoria.
Un esempio importante dei metodi esclusivamente legati alla struttura monomiale è il *Lemma di Dickson* che afferma che ogni ideale monomiale è finitamente generato, indipendentemente dalla considerazione che l'anello dei polinomi sia noetheriano (e quindi ogni ideale è finitamente generato).
Un altro notevole vantaggio di questa classe di ideali è legato allo studio dell'*ideale iniziale* di un ideale qualsiasi, rispetto ad un fissato ordine monomiale. L'ideale iniziale, infatti, è un ideale monomiale che conserva alcune importanti proprietà dell'ideale a cui è associato.
Alcuni testi a cui poter fare riferimento per eventuali approfondimenti sono ad esempio [1, 2, 3].

1 Nozioni di base

Sia K un campo e $S = K[x_1, x_2, \dots, x_n]$ l'anello dei polinomi in n indeterminate a coefficienti in K. Si definisce **monomio** un qualsiasi prodotto del tipo $x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, con $a_i \in \mathbb{Z}_{\geq 0} = \{k \in \mathbb{Z} \ : \ k \geq 0\}$. Se $\mathrm{a} = (a_1, a_2, \dots, a_n) \in \mathbb{Z}^n_{\geq 0}$, si usa spesso la seguente notazione $\mathrm{x}^{\mathrm{a}} = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$.

Si indica con $\mathrm{Mon}(S)$ l'insieme dei monomi di S e si osserva che esso rappresenta una base per l'anello dei polinomi visto come spazio vettoriale su K, infatti ogni polinomio $f \in S$ può essere scritto come

$$f = \sum_{u \in \mathrm{Mon}(S)} \alpha_u u, \text{ con } \alpha_u \in K.$$

Si diranno *monomi di* f i monomi u della precedente scrittura per i quali $\alpha_u \neq 0$.

Definizione 1.1. Un ideale I dell'anello S si dice **monomiale** se esiste un suo insieme di generatori formato da monomi.

Esempio 1.2. L'ideale $I = (xyz, y^2, x^2yz + 3xy^2)$ è monomiale. Infatti anche se è presentato con tre generatori, fra i quali un polinomio, basta osservare che i monomi $x^2yz = x(xyz)$ e $3xy^2 = 3x(y^2)$ appartengono all'ideale e quindi vi appartiene anche la loro somma. Quindi si ha che l'ideale può essere scritto come $I = (xyz, y^2)$ (il terzo generatore è superfluo) ed è quindi generato esclusivamente da monomi.

Si può osservare che ogni ideale monomiale I può essere considerato come spazio vettoriale sul campo K generato da tutti i monomi in $\mathrm{Mon}(I)$. Infatti se $f \in I$ allora per definizione esistono dei monomi $u_1, \dots u_m$ di I e dei polinomi $f_1, \dots f_m$ di S tali che $f = \sum_{i=1}^{m} f_i u_i$. Quindi i monomi di f appartengono all'unione (degli insiemi) dei monomi dei polinomi $f_i u_i$, ma ogni monomio di $f_i u_i$ appartiene a $\mathrm{Mon}(I)$, per definizione di ideale (legge di *assorbimento*). Dunque tutti i monomi di f appartengono a $\mathrm{Mon}(I)$. Tale risultato può essere enunciato come segue:

Proposizione 1.3. *Sia $I \subset S$ un ideale monomiale e $f = \sum_{i=1}^{r} \alpha_i u_i \in S$ un polinomio non nullo. Allora $f \in I$ se e solo se $u_i \in I$ per ogni $i = 1, \dots, r$, cioè se e solo se ogni monomio di f appartiene a I.*

Quindi è possibile considerare la seguente caratterizzazione per gli ideali monomiali.

Corollario 1.4. *Sia I un ideale di S. Le seguenti condizioni sono equivalenti:*

(*a*) *I è un ideale monomiale;*

(*b*) *Per ogni $f \in S$ si ha: $f \in I$ se e solo se ogni monomio di f appartiene a I.*

Dimostrazione. $(a) \Rightarrow (b)$ Proposizione 1.3.
$(b) \Rightarrow (a)$ Sia $\{f_1, \ldots, f_r\}$ un sistema di generatori di I. Per la proprietà (b) tutti i monomi degli f_i appartengono ad I e, poiché questi ultimi generano I, allora anche tutti i monomi degli f_i generano I. Quindi I ha un insieme di generatori formato da monomi. □

Analogamente può essere enunciata la seguente proposizione:

Proposizione 1.5. *Sia $I \subset S$ un ideale monomiale. L'anello quoziente S/I è generato, come spazio vettoriale su K, dalle classi i cui rappresentanti sono i monomi che non appartengono a I.*

Nel caso degli ideali monomiali alcune considerazioni permettono di enunciare l'unicità del sistema minimale di generatori di un ideale.

Osservazione 1.6. Il problema dell'appartenenza di un monomio u ad un ideale monomiale I è molto semplice da risolvere, infatti se $\{u_1, \ldots, u_r\}$ è un insieme di generatori dell'ideale, per le osservazioni fatte in precedenza si ottiene che

$$u \in I \text{ se e solo se } u_j \mid u \text{ per qualche } j \in \{1, \ldots, r\}.$$

Quest'osservazione è utile anche per la ricerca di un insieme minimale di generatori per un ideale monomiale, infatti partendo da un qualsiasi sistema di generatori (che sappiamo essere finito) basta trovare il sottoinsieme dei monomi minimali rispetto alla relazione di divisibilità.

L'insieme minimale di generatori di un ideale monomiale è quindi univocamente determinato[1]. Tale insieme può essere indicato con $G(I)$.

2 Operazioni tra ideali monomiali

Si può subito osservare che intersezione, somma e prodotto di ideali monomiali sono ancora ideali monomiali. Inoltre dati due monomi, u e v, è possibile calcolare il minimo comune multiplo, $\text{mcm}(u, v)$, e il massimo comune divisore, $\text{MCD}(u, v)$, poiché

[1]nel caso generale sappiamo soltanto che tutti gli insiemi minimali di generatori hanno la stessa cardinalità

S è un dominio a fattorizzazione unica.

Seguono alcune proposizioni che permetteranno di effettuare operazioni con gli ideali monomiali nel modo più semplice possibile.

Proposizione 2.1. *Siano I e J due ideali monomiali, con $G(I) = \{u_1, \dots, u_r\}$ e $G(J) = \{v_1, \dots, v_s\}$. L'***intersezione** *$I \cap J$ è l'ideale monomiale generato dall'insieme*

$$I \cap J = (\mathrm{mcm}(u_i, v_j) \,:\, i = 1, \dots, r \;\; e \;\; j = 1, \dots, s)\,.$$

Dimostrazione. Preso un qualsiasi polinomio $f \in I \cap J$, sappiamo per la Proposizione 1.3 che tutti i suoi monomi apparterranno a I e a J, quindi a $I \cap J$. Ciò assicura che l'intersezione è un ideale monomiale.
Se w è un monomio di f, allora si ha che $u_i \mid w$ e $v_j \mid w$ per qualche i e j opportuni (per la caratterizzazione degli ideali monomiali). Quindi w è multiplo dei due monomi e quindi anche multiplo di $\mathrm{mcm}(u_i, v_j)$, questo assicura che ogni monomio appartenente all'intersezione può essere generato dall'insieme dei minimi comuni multipli. D'altra parte $\mathrm{mcm}(u_i, v_j) \in I \cap J$ per definizione di ideale, quindi la tesi. □

Somma e **prodotto** di due ideali monomiali I e J, con $G(I) = \{u_1, \dots, u_r\}$ e $G(J) = \{v_1, \dots, v_s\}$, sono ancora ideali monomiali e valgono le seguenti scritture:

$$\begin{aligned} I + J &= (u_1, \dots, u_r, v_1, \dots, v_s) \\ IJ &= (u_i v_j \,:\, i = 1, \dots, r \;\text{ e }\; j = 1, \dots, s) \end{aligned}$$

Infatti, sappiamo che gli elementi della somma sono tutte le possibili somme degli elementi degli ideali, $f = f_i u_i + f_j v_j$ con $f_i, f_j \in S$, e considerato che la somma contiene entrambi gli ideali ed è il più piccolo ideale per cui ciò accade, sicuramente l'unione $G(I) \cup G(J)$ genera $I + J$.
Per quanto riguarda il prodotto, l'elemento generico si scrive come somma finita di prodotti, $f = \sum_{i=1}^{n} (f_i u_i)(f_j v_j) = \sum_{i=1}^{n} (f_i f_j)(u_i v_j)$ con $n \in \mathbb{N}^*$, quindi sicuramente l'insieme di tutti i prodotti di monomi $u_i v_j$ genera IJ.

Esempio 2.2. Dati gli ideali I e J tali che $G(I) = \{x^3, xy, y^4\}$ e $G(J) = \{x^2, xy^2\}$, calcoliamo i sistemi minimali di generatori per la loro intersezione, somma e prodotto:

$$\begin{aligned}
I \cap J =& \big(\mathrm{mcm}(x^3, x^2), \mathrm{mcm}(x^3, xy^2), \dots, \mathrm{mcm}(y^4, x^2), \mathrm{mcm}(y^4, xy^2)\big)\\
=&(x^3, x^3y^2, x^2y, xy^2, x^2y^4, xy^4);\\
G(I \cap J) =& \{x^3, x^2y, xy^2\}.
\end{aligned}$$

$$\begin{aligned}
I + J =&(x^3, xy, y^4, x^2, xy^2);\\
G(I + J) =&\{x^2, xy, y^4\}.
\end{aligned}$$

$$\begin{aligned}
IJ =&(x^5, x^4y^2, x^3y, x^2y^3, x^2y^4, xy^6);\\
G(IJ) =&\{x^5, x^3y, x^2y^3, xy^6\}.
\end{aligned}$$

Osserviamo che è pressoché immediato verificare l'appartenenza fra ideali monomiali: per verificare che $I \subseteq J$ basta osservare che $G(I) \subseteq G(J)$ ed essendo in presenza di sistemi minimali univocamente determinati di monomi è molto semplice verificare la divisibilità degli elementi. Nell'esempio precedente si osserva immediatamente che $IJ \subset I \cap J$.

Sappiamo già[2] che se I, J, K sono ideali di S allora $I \cap J + I \cap K \subseteq I \cap (J + K)$, ma in generale non vale l'inclusione inversa. Per gli ideali monomiali, invece, si verifica l'uguaglianza.

Proposizione 2.3. *Siano I, J, K ideali monomiali di S, allora $I \cap (J + K) \subseteq I \cap J + I \cap K$.*

Dimostrazione. Sia $f \in I \cap (J + K)$ quindi $f \in I$ e si scrive come $f = f_1 + f_2$ con $f_1 \in J$ e $f_2 \in K$. Poiché J e K sono ideali monomiali, allora tutti i monomi di f_1 appartengono a J e i monomi di f_2 appartengono a K. Se alcuni monomi comparissero contemporaneamente in f_1 e f_2 potremmo associarli in modo da ottenere una scrittura unica senza cambiare le condizioni di appartenenza, quindi possiamo supporre che i monomi in f_1 e in f_2 siano distinti. A questo punto, poiché I è un

[2] vedere l'Esercizio 1.6 e l'Esercizio 1.7 della Lezione 1 di Algebra Commutativa

ideale monomiale, tutti i monomi di f_1 e di f_2 appartengono anche ad I. Quindi $f_1 \in I \cap J$ e $f_2 \in I \cap K$ da cui $f = f_1 + f_2 \in I \cap J + I \cap K$. $\square$

Come immediata conseguenza si ottiene il risultato che avevamo già dimostrato sull'intersezione di ideali, indipendentemente dalla conoscenza delle operazioni fra ideali monomiali.

Corollario 2.4. *Siano I e J due ideali monomiali, con $G(I) = \{u_1, \ldots, u_r\}$ e $G(J) = \{v_1, \ldots, v_s\}$. Vale che*

$$\begin{aligned} I \cap J =& (u_1, \ldots, u_r) \cap (v_1, \ldots, v_s) = \sum_{i=1}^{r} \sum_{j=1}^{s} (u_i) \cap (v_j) = \sum_{i=1}^{r} \sum_{j=1}^{s} (\mathrm{mcm}(u_i, v_j)) \\ &= (\mathrm{mcm}(u_i, v_j) \ : \ i = 1, \ldots, r \ \ e \ \ j = 1, \ldots, s) \,. \end{aligned}$$

Dati gli ideali $I, J \subset S$, l'ideale **colon**, o **trasportatore** di J in I, è definito da

$$I : J = \{f \in S \ : \ fg \in I \ \text{ per ogni } \ g \in J\}.$$

Anche per gli ideali monomiali (essendo l'anello dei polinomi un dominio a fattorizzazione unica) vale il seguente risultato[3], che viene dimostrato per evidenziare alcune tecniche interessanti:

Proposizione 2.5. *Siano $I, J \subset S$ ideali monomiali, con $G(I) = \{u_1, \ldots, u_r\}$ e $G(J) = \{v_1, \ldots, v_s\}$. Allora vale che*

$$I : J = \bigcap_{j=1}^{s} I : (v_j),$$

dove $I : (v_j) = \left(\dfrac{u_i}{\mathrm{MCD}(u_i, v_j)} \ : \ i = 1, \ldots, r \right)$.

Dimostrazione. Preso un qualsiasi elemento $f \in I : J$, per definizione $fv \in I$ per ogni $v \in G(J)$. I monomi di fv appartengono ad I, perché monomiale, ed essi sono dati dai monomi di f per v. Quindi per definizione i monomi di f appartengono ad

[3] vedere l'Esempio 1.15 e il punto 5. dell'Esercizio 1.16 della Lezione 1 di Algebra Commutativa

$I : J$ e per il Corollario 1.4 si ha che il trasportatore è monomiale.
L'uguaglianza $I : J = \bigcap_{j=1}^{s} I : (v_j)$ deriva, in generale, dal fatto che $J = (v_1, \dots, v_s) = (v_1) + \cdots + (v_s)$. Per verificarla basta osservare che preso $f \in I : ((v_1) + (v_2))$ per definizione $f(gv_1 + hv_2) \in I$ per ogni $g, h \in S$ ed in particolare $f(gv_1) \in I$ e $f(hv_2) \in I$ (rispettivamente per $h = 0$ e $g = 0$). Quindi $f \in I : (v_1)$ e $f \in I : (v_2)$, cioè $f \in I : (v_1) \cap I : (v_2)$. D'altra parte, se $f \in I : (v_1) \cap I : (v_2)$ allora $f(gv_1), f(hv_2) \in I$ per ogni $g, h \in S$ e quindi anche la loro somma, così $f \in I : ((v_1) + (v_2))$. L'osservazione può essere estesa per induzione alla somma di più ideali[4].
Per quanto riguarda invece l'uguaglianza $I : (v_j) = \left(\frac{u_i}{\mathrm{MCD}(u_i, v_j)} : i = 1, \dots, r \right)$, è immediata l'inclusione $\supseteq$ poiché $\frac{u_i}{\mathrm{MCD}(u_i, v_j)} v_j = \mathrm{mcm}(u_i, v_j) \in I$ in quanto ideale. Sia quindi $f \in I : (v_j)$, allora $fv_j \in I$ cioè esiste $u_i \in G(I)$ che divide fv_j e questo implica che $\frac{u_i}{\mathrm{MCD}(u_i, v_j)}$ divide f quindi la seconda inclusione $\subseteq$ [5]. $\square$

Esempio 2.6. Dati gli ideali I e J tali che $G(I) = \{x^3, xy, y^4\}$ e $G(J) = \{x^2, xy^2\}$, calcoliamo i sistemi minimali di generatori per il trasportatore di J in I:

$$\begin{aligned}
I : J =& (x^3, xy, y^4) : (x^2) \bigcap (x^3, xy, y^4) : (xy^2) \\
=& \left(\frac{x^3}{\mathrm{MCD}(x^3, x^2)}, \frac{xy}{\mathrm{MCD}(xy, x^2)}, \frac{y^4}{\mathrm{MCD}(y^4, x^2)} \right) \\
& \bigcap \left(\frac{x^3}{\mathrm{MCD}(x^3, xy^2)}, \frac{xy}{\mathrm{MCD}(xy, xy^2)}, \frac{y^4}{\mathrm{MCD}(y^4, xy^2)} \right) \\
=& \left(\frac{x^3}{x^2}, \frac{xy}{x}, \frac{y^4}{1} \right) \bigcap \left(\frac{x^3}{x}, \frac{xy}{xy}, \frac{y^4}{y^2} \right) \\
=& (x, y, y^4) \cap (x^2, 1, y^2) \\
=& (x, y) \cap S \\
=& (x, y); \\
G(I : J) =& \{x, y\}.
\end{aligned}$$

[4] vedere anche il punto 5. dell'Esercizio 1.16 della Lezione 1
[5] vedere anche l'Esempio 1.15 della Lezione 1

3 Radicale di un ideale monomiale

In generale il radicale di un ideale $I \subset S$ è definito come

$$\sqrt{I} = \{f \in S \, : \, f^n \in I \text{ per qualche } n \in \mathbb{N}\}.$$

Inoltre un ideale si dice radicale se coincide con il suo radicale, $I = \sqrt{I}$.

Per il caso particolare degli ideali monomiali, è utile introdurre alcune definizioni e risultati preliminari su una particolare classe di monomi.

Definizione 3.1. Un monomio $u = \mathrm{x}^{\mathrm{a}}$ di S si dice **squarefree** (o privo di quadrati o ridotto) se $\mathrm{a} \in \mathbb{Z}_2^n$, cioè se $u = x_{i_1} x_{i_2} \cdots x_{i_t}$, con x_{i_k} indeterminate di S a due a due distinte. Si indica con u^{rid} o con $\sqrt{u}$ il monomio squarefree dato dal prodotto delle indeterminate distinte che dividono u (eliminando quindi gli esponenti).
Un ideale generato da monomi squarefree si dice *ideale monomiale squarefree.*

Lemma 3.2. *Ogni ideale monomiale squarefree è radicale.*

Dimostrazione. Sia I un ideale monomiale squarefree con $G(I) = \{u_1, \ldots, u_r\}$. Se $u_1 = x_{i_1} \cdots x_{i_s}$ allora considerando le proprietà dell'intersezione fra ideali vale la seguente scrittura:

$$I = (u_1, \ldots, u_r) = (x_{i_1}, u_2, \ldots, u_r) \cap \cdots \cap (x_{i_s}, u_2, \ldots, u_r).$$

Analogamente, se $u_2 = x_{j_1} \cdots x_{j_t}$ ognuno degli ideali dell'intersezione prima individuata, per $q = 1, \ldots, k$, può essere scritto come:

$$(x_{i_q}, u_2, \ldots, u_r) = (x_{i_q}, x_{j_1}, u_3, \ldots, u_r) \cap \cdots \cap (x_{i_q}, x_{j_t}, u_3, \ldots, u_r).$$

Iterando il procedimento risulterà che I può essere scritto come una intersezione finita di $\overline{r}$ ideali generati da indeterminate, cioè:

$$I = \bigcap_{k=1}^{\overline{r}} P_k = \bigcap_{k=1}^{\overline{r}} (x_{k_1}, x_{k_2}, \ldots, x_{k_p}).$$

Osserviamo che un ideale generato da indeterminate, $P_k = (x_{k_1}, x_{k_2}, \ldots, x_{k_p})$, è radicale; per provarlo basta mostrare che $\sqrt{P_k} \subseteq P_k$ (il viceversa è vero per definizione).

Sia $f \in \sqrt{P_k}$, cioè tale che $f^n \in P_k$ per qualche $n \in \mathbb{N}^*$. Per definizione di ideale generato, ogni monomio di f^n contiene qualche indeterminata fra $x_{k_1}, x_{k_2}, \dots, x_{k_p}$ e di conseguenza le contengono anche i monomi di f (una potenza non cambia le indeterminate) per cui anche f deve essere un polinomio di P_k, dunque $\sqrt{P_k} \subseteq P_k$. Cioè P_k è un ideale radicale: $\sqrt{P_k} = P_k$.
Applichiamo ora le proprietà dei radicali nella scrittura di $\sqrt{I}$:

$$\sqrt{I} = \sqrt{\bigcap_{k=1}^{\bar{r}} P_k} = \bigcap_{k=1}^{\bar{r}} \sqrt{P_k} = \bigcap_{k=1}^{\bar{r}} P_k = I.$$

Quindi I è un ideale radicale. $\square$

Ora è possibile enunciare un risultato sul radicale di un ideale monomiale.

Proposizione 3.3. *Sia $I \subset S$ un ideale monomiale, con $G(I) = \{u_1, \dots, u_r\}$. Allora*

$$\sqrt{I} = (\sqrt{u_1}, \dots, \sqrt{u_r})$$

Dimostrazione. Proviamo la doppia inclusione, dapprima $(\sqrt{u_1}, \dots, \sqrt{u_r}) \subseteq \sqrt{I}$. Siano in generale $u_i = x_{i1}^{c_{i1}} x_{i2}^{c_{i2}} \cdots x_{ik_i}^{c_{ik_i}}$ e sia $c_i = \max\{c_{ik} : k = 1, \dots, k_i\}$ per $i = 1, \dots, r$, allora $u_i \mid \sqrt{u_i}^{\,c_i}$ quindi $\sqrt{u_i}^{\,c_i} \in I$ e di conseguenza $\sqrt{u_i} \in \sqrt{I}$. Poiché ciò avviene per tutti i generatori, allora vale per l'intero ideale o, in alternativa, si può considerare $c = \sum_{i=1}^{r} c_i$ e si ottiene che $\left(f_1\sqrt{u_1} + \cdots + f_r\sqrt{u_r}\right)^c \in I$ e quindi $f_1\sqrt{u_1} + \cdots + f_r\sqrt{u_r} \in \sqrt{I}$ da cui la tesi.
D'altra parte, sicuramente $I \subseteq (\sqrt{u_1}, \dots, \sqrt{u_r})$ poiché ogni u_i (generatore di I) è diviso dal proprio ridotto. Passando ai radicali si ottiene:

$$\sqrt{I} \subseteq \sqrt{(\sqrt{u_1}, \dots, \sqrt{u_r})} = (\sqrt{u_1}, \dots, \sqrt{u_r})$$

per il Lemma 3.2, poiché $(\sqrt{u_1}, \dots, \sqrt{u_r})$ è un ideale monomiale squarefree.
È quindi provata la proposizione. $\square$

Mettendo assieme i risultati finora ottenuti si può enunciare il seguente risultato che caratterizza gli ideali monomiali radicali.

Corollario 3.4. *Un ideale monomiale $I \subset S$ è radicale, cioè $I = \sqrt{I}$, se e solo se I è un ideale monomiale squarefree.*

Esempio 3.5. Calcolare il radicale dell'ideale monomiale $I = (x_1^3, x_2^2x_3^3, x_2^3x_3^2, x_2^2x_4, x_4^3)$:

$$\begin{aligned}\sqrt{I} =& \left(\sqrt{x_1^3}, \sqrt{x_2^2x_3^3}, \sqrt{x_2^3x_3^2}, \sqrt{x_2^2x_4}, \sqrt{x_4^3}\right)\\ =&(x_1, x_2x_3, x_2x_3, x_2x_4, x_4);\\ G(\sqrt{I}) =&\{x_1, x_2x_3, x_4\}.\end{aligned}$$

4 Ideali monomiali Primi e Massimali

Le definizioni di ideale *primo* e *massimale* valgono in particolare per la classe degli ideali monomiali. In questo caso è possibile caratterizzare gli ideali primi e massimali in modo abbastanza semplice.

Proposizione 4.1. *Sia $S = K[x_1, \dots, x_n]$. Valgono le seguenti proposizioni:*

i) Tutti e soli gli ideali monomiali **primi** *sono quelli della forma $(x_{i_1}, \dots, x_{i_r})$ con indici $i_j \in \{1, \dots, n\}$, $j = 1, \dots, r$ a due a due distinti.*

ii) L'unico ideale **massimale** *è $(x_1, \dots, x_n)$.*

Dimostrazione.

i) Sia I un ideale monomiale primo con $G(I) = \{u_1, \dots, u_r\}$. Se un qualsiasi suo generatore minimale u_i avesse grado maggiore di 1, allora si potrebbe scrivere come $u_i = x_j u_i'$ con $x_j, u_i' \notin I$ per via della minimalità di u_i (in base alla relazione di divisibilità) ma ciò è assurdo poiché il loro prodotto appartiene ad I che è primo. Quindi il grado dei monomi u_i deve essere 1, cioè i generatori minimali possono soltanto essere le singole indeterminate.
D'altra parte, se l'ideale è della forma $I = (x_{i_1}, \dots, x_{i_r})$, allora il quoziente S/I è generato dalle classi i cui rappresentanti sono le indeterminate di S che non generano I, quindi isomorfo all'anello dei polinomi in dette indeterminate, quindi un dominio di integrità. Questo permette di affermare che I è primo.

ii) Poiché gli ideali monomiali massimali devono essere ricercati tra gli ideali monomiali primi, per la caratterizzazione in i) l'unico ideale massimale può essere soltanto $M = (x_1, \dots, x_n)$. Infatti tutti gli altri ideali primi che non contengono una qualche indeterminata sono propriamente contenuti in M e quindi non massimali. Si può anche osservare che $S/M = K$ è un campo.

□

5 Decomposizione Primaria di ideali monomiali

Trovare una decomposizione primaria di un ideale significa trovarne una scrittura (o presentazione) come intersezione di ideali primari[6]. Tale operazione risulta utile nelle applicazioni alla geometria algebrica, infatti è possibile associare ad ogni ideale di polinomi una varietà algebrica (i cui punti sono le radici del sistema di polinomi). I punti associati ad un ideale coincidono con quelli associati al radicale dell'ideale (il teorema degli zeri di Hilbert stabilisce la corrispondenza biunivoca fra ideali radicali e varietà se il campo è algebricamente chiuso), gli ideali primi rappresentano varietà irriducibili e gli ideali primari rappresentano la varietà associata al loro radicale ma conservando informazioni sulla molteplicità della componente. Una decomposizione primaria di un ideale permette quindi di classificare la varietà da esso individuata.

Ricordiamo alcune definizioni valide in generale per gli ideali.
Un ideale si dice **irriducibile**[7] se non può essere espresso come intersezione di ideali che lo contengono propriamente.
Un ideale $I \subset S$ si dice **primario**[8] se per ogni $f, g \in S$ si ha $fg \in I \Rightarrow f \in I$ oppure $g \in \sqrt{I}$.

Poiché consideriamo ideali monomiali di anelli di polinomi, ci troviamo quindi in un dominio di integrità a fattorizzazione unica che è anche noetheriano; valgono quindi i risultati già dimostrati a lezione[9], in particolare che ogni ideale è **decomponibile**, cioè ammette una decomposizione primaria, e valgono le seguenti relazioni

[6] Lezione 4
[7] Definizione 2.11 della Lezione 2
[8] Definizione 2.34 della Lezione 3
[9] Lezione 4 e Lezione 5

fra classi di ideali:

Ideali massimali $\Longrightarrow$ Ideali primi $\Longrightarrow$ Ideali irriducibili $\Longrightarrow$ Ideali primari.

Procedendo similmente a quanto fatto nella dimostrazione del Lemma 3.2, è possibile operare un analogo procedimento nel caso di ideali monomiali non necessariamente squarefree, per poterli presentare come un'intersezione. Tale decomposizione, data la particolare natura degli ideali che intervengono, si proverà essere quella cercata.

Osservazione 5.1. Sia I un ideale monomiale con $G(I) = \{u_1, \ldots, u_r\}$. Se $u_1 = x_{i_1}^{a_1} \cdots x_{i_s}^{a_s}$, per indici a due a due distinti, allora considerando il Corollario 2.4 vale la seguente scrittura:

$$I = (u_1, \ldots, u_r) = (x_{i_1}^{a_1}, u_2, \ldots, u_r) \cap \cdots \cap (x_{i_s}^{a_s}, u_2, \ldots, u_r).$$

Osserviamo che sicuramente I è contenuto nell'intersezione e l'altra inclusione vale poiché un monomio dell'intersezione o è divisibile per qualche u_t, $t = 2, \ldots, r$, oppure per tutte le potenze (poiché coprime) $x_{i_j}^{a_j}$, $i = 1, \ldots, s$, e quindi per u_1; in ogni caso appartiene ad I.
Analogamente, se $u_2 = x_{j_1}^{b_1} \cdots x_{j_t}^{b_t}$ ognuno degli ideali dell'intersezione prima individuata, per $q = 1, \ldots, k$, può essere scritto come:

$$(x_{i_q}^{a_q}, u_2, \ldots, u_r) = (x_{i_q}^{a_q}, x_{j_1}^{b_1}, u_3, \ldots, u_r) \cap \cdots \cap (x_{i_q}^{a_q}, x_{j_t}^{b_t}, u_3, \ldots, u_r).$$

Iterando il procedimento risulterà che I può essere scritto come una intersezione finita di $\overline{r}$ ideali generati da potenze di indeterminate, cioè:

$$I = \bigcap_{k=1}^{\overline{r}} Q_k = \bigcap_{k=1}^{\overline{r}} (x_{k_1}^{c_1}, x_{k_2}^{c_2}, \ldots, x_{k_p}^{c_p}),$$

con indici a due a due distinti ed esponenti positivi.

Quindi è possibile enunciare il seguente risultato.

Teorema 5.2. *Sia $I \subset S = K[x_1, \ldots, x_n]$ un ideale monomiale. Allora $I = \bigcap_{i=1}^{s} Q_i$, con $Q_i = \left(x_{i_1}^{a_1}, \ldots, x_{i_r}^{a_r}\right)$. Inoltre è sempre possibile ricondursi ad una forma* **irridondante** *di tale decomposizione e questa è unica.*

Dimostrazione. Utilizzando l'Osservazione 5.1, l'ideale I può essere scritto nella forma

$$I = \bigcap_{k=1}^{\overline{r}} Q_k = \bigcap_{k=1}^{\overline{r}} (x_{k_1}^{c_1}, x_{k_2}^{c_2}, \dots, x_{k_p}^{c_p}),$$

per qualche $\overline{r} \in \mathbb{N}^*$. È possibile eliminare da tale presentazione quegli ideali che contengano l'intersezione di altri ideali. Così facendo si ottiene una presentazione irridondante che è unica. Infatti se esistessero due presentazioni minimali $I = \bigcap_{i=1}^{s} Q_i = \bigcap_{j=1}^{t} Q'_j$ del tipo prima descritto, tali che $Q'_j \not\subset Q_i$ per ogni $j = 1, \dots, t$ allora sarebbe possibile individuare le potenze $x_{\ell_j}^{b_j} \in Q'_j \setminus Q_i$ che vuol dire o che l'indeterminata x_{ℓ_j} non appare in alcun Q_i oppure che l'esponente b_j è minore di quello con cui vi appare. Consideriamo allora il monomio $w = \text{mcm}\{x_{\ell_1}^{b_1}, \dots, x_{\ell_t}^{b_t}\}$. Si osserva subito che $w \in \bigcap_{j=1}^{t} Q'_j \subset Q_i$ per i in $\{1, \dots, s\}$, per l'assunzione sull'uguaglianza delle due scritture. Quindi deve esistere un $x_i^{a_i}$ che divide w (per l'appartenenenza) ma ciò è assurdo poiché essendo le indeterminate coprime dovrebbe dividerne una di queste, contraddizione alla scelta effettuata.
Questo implica che per qualche j si ha che $Q'_j \subset Q_i$ per ogni $i = 1, \dots, s$. Per analogia vale anche la relazione simmetrica e questa è una contraddizione all'irridondanza delle due presentazioni (perché se così fosse una delle due potrebbe essere ridotta ulteriormente). Quindi si ha che $s = t$ e che $\{Q_1, \dots, Q_s\} = \{Q'_1, \dots, Q'_t\}$. □

Esempio 5.3. Calcolare una decomposizione (irridondante) dell'ideale monomiale $I = (x_1^2 x_2, x_1^2 x_3^2, x_2^2, x_2 x_3^2)$ dell'anello $S = K[x_1, x_2, x_3]$:

$$\begin{aligned}
I &= \left(x_1^2, x_1^2 x_3^2, x_2^2, x_2 x_3^2\right) \cap \left(x_2, x_1^2 x_3^2, x_2^2, x_2 x_3^2\right) \\
&= \left(x_1^2, x_2^2, x_2 x_3^2\right) \cap \left(x_2, x_1^2 x_3^2\right) \\
&= \left(x_1^2, x_2^2, x_2\right) \cap \left(x_1^2, x_2^2, x_3^2\right) \cap \left(x_2, x_1^2\right) \cap \left(x_2, x_3^2\right) \\
&= \left(x_1^2, x_2\right) \cap \left(x_1^2, x_2^2, x_3^2\right) \cap \left(x_1^2, x_2\right) \cap \left(x_2, x_3^2\right) \\
&= \left(x_1^2, x_2\right) \cap \left(x_1^2, x_2^2, x_3^2\right) \cap \left(x_2, x_3^2\right).
\end{aligned}$$

Si può verificare che ognuno di questi ideali non è contenuto negli altri.

Analizzando tale teorema e alcune informazioni sugli ideali squarefree, si può enunciare un primo corollario al Teorema 5.2.

Corollario 5.4. *Ogni ideale monomiale squarefree si decompone nell'intersezione di ideali monomiali primi.*

Dimostrazione. Seguendo l'Osservazione 5.1 e il Teorema 5.2 si ottiene una decomposizione irridondante. Inoltre per la dimostrazione del Lemma 3.2 e la Proposizione 4.1, sappiamo che gli ideali che formano la presentazione sono primi.
Quindi nel caso di ideali monomiali squarefree tale decomposizione è primaria ed i suoi primi associati sono quelli che intervengono nella decomposizione. □

Nel caso di ideali monomiali, avendo caratterizzato gli ideali primi (Proposizione 4.1), è possibile fare delle considerazioni sugli ideali irriducibili e quindi sui primari.

Proposizione 5.5. *Gli ideali monomiali* **irriducibili** *sono tutti e soli quelli della forma*

$$\left(x_{i_1}^{a_1}, \ldots, x_{i_r}^{a_r}\right)$$

con indici $i_j \in \{1, \ldots, n\}$, $j = 1, \ldots, r$ *a due a due distinti.*

Dimostrazione. Mostriamo prima che qualsiasi ideale Q di questa forma è irriducibile. Se così non fosse, allora esisterebbero almeno due ideali monomiali contenenti propriamente Q per i quali $Q = \left(x_{i_1}^{a_1}, \ldots, x_{i_r}^{a_r}\right) = I \cap J$. Per il Teorema 5.2, entrambi questi ideali ammettono decomposizioni irridondanti uniche $I = \bigcap_{i=1}^{s} Q_i$ e $J = \bigcap_{j=1}^{t} Q'_j$. Si ottiene così la seguente scrittura: $Q = \left(\bigcap_{i=1}^{s} Q_i\right) \cap \left(\bigcap_{j=1}^{t} Q'_j\right)$.
L'unicità della decomposizione implica quindi che $Q = Q_i$ o che $Q = Q'_j$ (poiché Q rappresenta già la sua decomposizione irridondante), ma questo contraddice l'ipotesi che I e J contengono propriamente Q.
D'altra parte, se un ideale monomiale è irriducibile allora avrà unica decomposizione irridondante banale, in cui interviene soltanto esso stesso. Sarà quindi della forma $\left(x_{i_1}^{a_1}, \ldots, x_{i_r}^{a_r}\right)$. Infatti se vi fosse un monomio divisibile per due indeterminate distinte, allora Q si scriverebbe come intersezione di due ideali che lo contengono propriamente, per l'Osservazione 5.1, contraddicendo la sua irriducibilità. □

Quindi vale il seguente risultato.

Corollario 5.6. *Gli ideali monomiali della forma*

$$\left(x_{i_1}^{a_1}, \dots, x_{i_r}^{a_r}\right)$$

con indici $i_j \in \{1, \dots, n\}$, $j = 1, \dots, r$ *a due a due distinti sono* $(x_{i_1}, \dots, x_{i_r})$-**primari**.

Dimostrazione. Per la Proposizione 5.5, l'ideale I è irriducibile quindi primario[10]. Inoltre il radicale di I è l'ideale primo $\sqrt{I} = (x_{i_1}, \dots, x_{i_r})$, che sicuramente è il più piccolo ideale primo che lo contiene[11]. Quindi l'ideale I è $(x_{i_1}, \dots, x_{i_r})$-primario. □

Osserviamo che non tutti gli ideali monomiali primari hanno la forma della Proposizione 5.6. Infatti sia I un ideale monomiale con $G(I) = \{u_1, \dots, u_r\}$. Se I è primario, sicuramente il suo radicale è il più piccolo ideale primo che lo contiene[12]. Per la Proposizione 3.3 sappiamo calcolare il suo radicale $\sqrt{I} = (\sqrt{u_1}, \dots, \sqrt{u_r})$ e per la caratterizzazione nella Proposizione 4.1, questo radicale deve essere della forma $(x_{i_1}, \dots, x_{i_r})$. Quindi

$$\sqrt{I} = (\sqrt{u_1}, \dots, \sqrt{u_r}) = (x_{i_1}, \dots, x_{i_r})\,.$$

I monomi $\sqrt{u_j}$, però non sono univocamente determinati infatti esistono monomi che hanno lo stesso ridotto ma non sono confrontabili (secondo divisibilità). Quindi, eliminando gli esponenti, potrebbero venire cancellate delle informazioni e ciò non ci permette di asserire che $u_j = x_{i_j}^{a_j}$ per qualche esponente positivo a_j.
Il successivo esempio mostra proprio quest'eventualità.

Esempio 5.7. L'ideale monomiale $I = (x_1^3, x_1^2x_2, x_1x_2^3, x_2^5) \subset S = K[x_1, x_2]$ è primario ma non è irriducibile. Infatti è possibile esprimerlo come un'intersezione di ideali

[10]proposizione 4.5 Lezione 5
[11]Proposizione 2.42 Lezione 4
[12]Proposizione 2.42 Lezione 4

che lo contengono propriamente, utilizzando il metodo descritto nell'Osservazione 5.1:

$$\begin{aligned} I &= \left(x_1^3, x_1^2x_2, x_1x_2^3, x_2^5\right) \\ &= \left(x_1^3, x_1^2, x_1x_2^3, x_2^5\right) \cap \left(x_1^3, x_2, x_1x_2^3, x_2^5\right) \\ &= \left(x_1^2, x_1x_2^3, x_2^5\right) \cap \left(x_1^3, x_2\right) \\ &= \left(x_1^2, x_1, x_2^5\right) \cap \left(x_1^2, x_2^3, x_2^5\right) \cap \left(x_1^3, x_2\right) \\ &= \left(x_1, x_2^5\right) \cap \left(x_1^2, x_2^3\right) \cap \left(x_1^3, x_2\right) \end{aligned}$$

Per verificare che sia primario si può osservare che è intersezione di ideali (x_1, x_2)-primari o si può osservare che il radicale è massimale in S:

$$\sqrt{I} = (x_1, x_1x_2, x_1x_2, x_2) = (x_1, x_2)\,.$$

Quindi I è primario[13].

La proposizione seguente caratterizza gli ideali monomiali primari. Una dimostrazione può essere trovata in [3, Proposition 6.1.7].

Proposizione 5.8. *Gli ideali monomiali* **primari** *sono tutti e soli quelli della forma*

$$Q = \left(x_{i_1}^{a_1}, \dots, x_{i_r}^{a_r}, \mathrm{x}^{\mathrm{b}_1}, \dots, \mathrm{x}^{\mathrm{b}_s}\right)$$

con indici $i_j \in \{1, \dots, n\}$ a due a due distinti e $a_j \geq 0$ per $j = 1, \dots, r$ e dove nei monomi $\mathrm{x}^{\mathrm{b}_i}$, per $i = 1, \dots, s$, compaiono soltanto le indeterminate x_{i_j}, $j = 1, \dots, r$.

Dimostrazione. Può essere utile osservare che dalle ipotesi si ottiene subito che $\sqrt{\left(x_{i_1}^{a_1}, \dots, x_{i_r}^{a_r}, \mathrm{x}^{\mathrm{b}_1}, \dots, \mathrm{x}^{\mathrm{b}_s}\right)} = (x_{i_1}, \dots, x_{i_r})$, per la Proposizione 3.3.
Supponiamo che Q sia primario e quelli indicati i suoi generatori minimali, allora presa una indeterminata x_t che divide un monomio $\mathrm{x}^{\mathrm{b}_i}$ si può scrivere $\mathrm{x}^{\mathrm{b}_i} = x_t\mathrm{x}^{\mathrm{c}}$ per una opportuna n-upla c, con x^{c} monomio non appartenente a Q. Poiché tale ideale è stato supposto primario, allora per definizione una potenza di x_t dovrà appartenere ad esso. Ciò può accadere soltanto se x_t coincide con una delle indeterminate x_{i_j}, per $j = 1, \dots, r$. L'ideale avrà quindi la forma ipotizzata.

[13]per la Proposizione 2.46 Lezione 4

Per provare invece che Q sia primario, si può procedere in diversi modi. Applicando l'Osservazione 5.1 per determinare una decomposizione in irriducibili, e quindi primari, si osserva che tutti gli ideali che si otterranno sono $(x_{i_1}, \dots, x_{i_r})$-primari. L'ideale Q è la loro intersezione e, per il Lemma 3.3 della Lezione 4, è dunque anch'esso un ideale $(x_{i_1}, \dots, x_{i_r})$-primario. In alternativa, si può osservare che Q ha un unico primo associato ed è dunque primario per l'Osservazione 3.11 della Lezione 4 di Algebra Commutativa, che afferma che un ideale è primario se e solo se possiede un unico ideale primo associato. □

Considerando i risultati finora ottenuti, possiamo enunciare un corollario al Teorema sulla decomposizione di un ideale monomiale.

Corollario 5.9. *Sia $I \subset S = K[x_1, \dots, x_n]$ un ideale monomiale. Allora I ammette una decomposizione primaria irridondante.*

Dimostrazione. Seguendo le operazioni dell'Osservazione 5.1 è sempre possibile costruire una decomposizione di I. Inoltre il Teorema 5.2 sottolinea che è sempre possibile ricondursi ad un'unica decomposizione irridondante di I. Gli ideali che intervengono in tale decomposizione sono generati da potenze di indeterminate, cioè irriducibili e quindi per il Corollario 5.6 si tratta di ideali primari. Da una decomposizione primaria siffatta, associando opportunamenti i primari associati allo stesso ideale primo, ci si può sempre ricondurre ad una decomposizione primaria irridondante. □

Esempio 5.10. Calcolare una decomposizione primaria irridondante dell'ideale monomiale $I = (x_1^3, x_1^2 x_2, x_1 x_2^2 x_3)$ dell'anello $S = K[x_1, x_2, x_3]$:

$$\begin{aligned}
I &= \left(x_1^3, x_1^2, x_1 x_2^2 x_3\right) \cap \left(x_1^3, x_2, x_1 x_2^2 x_3\right) \\
&= \left(x_1^3, x_1^2, x_1\right) \cap \left(x_1^3, x_1^2, x_2^2\right) \cap \left(x_1^3, x_1^2, x_3\right) \cap \left(x_1^3, x_2, x_1\right) \cap \left(x_1^3, x_2, x_2^2\right) \cap \left(x_1^3, x_2, x_3\right) \\
&= (x_1) \cap \left(x_1^2, x_2^2\right) \cap \left(x_1^2, x_3\right) \cap (x_1, x_2) \cap \left(x_1^3, x_2\right) \cap \left(x_1^3, x_2, x_3\right)
\end{aligned}$$

Osserviamo che $(x_1^3, x_2) \subseteq (x_1^3, x_2, x_3)$ e $(x_1^2, x_2^2) \subseteq (x_1, x_2)$, quindi è possibile eliminare (x_1^3, x_2, x_3) e (x_1, x_2) dalla scrittura della decomposizione:

$$I = (x_1) \cap \left(x_1^2, x_2^2\right) \cap \left(x_1^2, x_3\right) \cap \left(x_1^3, x_2\right)$$

Si può inoltre osservare che $\sqrt{(x_1^2, x_2^2)} = (x_1, x_2) = \sqrt{(x_1^3, x_2)}$, si tratta quindi di ideali (x_1, x_2)-primari. Se ne può calcolare l'intersezione $(x_1^2, x_2^2) \cap (x_1^3, x_2) = (x_1^3, x_1^2x_2, x_1^3x_2^2, x_2^2) = (x_1^3, x_1^2x_2, x_2^2)$ ed utilizzarla come unica componente (x_1, x_2)-primaria della decomposizione:

$$I = (x_1) \cap \left(x_1^3, x_1^2x_2, x_2^2\right) \cap \left(x_1^2, x_3\right).$$

La decomposizione primaria così ottenuta è irridondante e i primi associati ad I sono dunque:

$$\operatorname{Ass}(I) = \{(x_1), (x_1, x_2), (x_1, x_3)\}$$

Osserviamo che (x_1) è un primo isolato, mentre (x_1, x_2) e (x_1, x_3) sono primi immersi, di conseguenza saranno tali le rispettive componenti primarie.

Riferimenti bibliografici

[1] J. Herzog and T. Hibi, *Monomial ideals*, vol. 260 of *Graduate texts in mathematics*. Springer-Verlag London, 1 ed., 2011.

[2] R. Fröberg, "An introduction to Gröbner bases," in *Pure and applied mathematics*, John Wiley & Sons Inc, 1997.

[3] R. Villarreal, *Monomial Algebras.* Chapman & Hall/CRC Monographs and Research Notes in Mathematics, CRC Press, 2018.