



UNIVERSITÀ DI PISA

DIPARTIMENTO DI MATEMATICA

Corso di Laurea Triennale in Matematica

Metodi Computazionali per il Calcolo della Decomposizione Primaria

Relatore:

Prof. Enrico Sbarra

Candidato:

Ludovico Piazza

ANNO ACCADEMICO 2022/2023

Indice

1	Prerequisiti	1
2	L'algoritmo GTZ	5
2.1	Decomposizione primaria di ideali 0-dimensionali	5
2.2	Il caso generale	16
3	L'algoritmo SY	23
3.1	Decomposizione primaria	23
3.1.1	Decomposizione pseudo-primaria	23
3.1.2	Estrazione	27
3.1.3	Calcolo di una decomposizione primaria	28
3.2	Decomposizione primaria minimale	29
3.2.1	Identificazione di componenti ridondanti	29
3.2.2	Albero di decomposizione	33
3.2.3	Calcolo di una decomposizione primaria minimale	37
	Bibliografia	39

Introduzione

Una delle proprietà più importanti dell'anello degli interi è l'esistenza e unicità, a meno dell'ordine, della fattorizzazione in potenze di primi di un qualsiasi suo elemento non nullo e non invertibile. I domini che soddisfano questa proprietà sono detti a fattorizzazione unica, e costituiscono una classe di anelli particolarmente significativa. Proprietà di fattorizzazione analoghe si possono riscontrare anche in altre classi di anelli, ancora più ampie. Una di queste è la classe degli anelli noetheriani, in cui ogni ideale proprio ammette una decomposizione nota come *decomposizione primaria*.

Definizione. Dati un anello R e un ideale $I \subsetneq R$, chiamiamo *decomposizione primaria* di I una sua scrittura come intersezione finita di ideali primari

$$I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_s.$$

Diciamo inoltre che tale decomposizione è *minimale* se:

1. per ogni $i \neq j$ abbiamo $\sqrt{\mathfrak{q}_i} \neq \sqrt{\mathfrak{q}_j}$;
2. per ogni i abbiamo che $\mathfrak{q}_i$ non è *ridondante*, ovvero $\bigcap_{j \neq i} \mathfrak{q}_j \not\subseteq \mathfrak{q}_i$.

Nel 1905, lo scacchista e matematico Emanuel Lasker dimostra in [9] che gli ideali propri degli anelli polinomiali e delle serie di potenze convergenti a coefficienti interi o complessi possiedono una decomposizione primaria.

In seguito, nel 1913, Francis Sowerby Macaulay pubblica alcuni risultati relativi alle proprietà della decomposizione primaria in [10], fornendo anche un primo algoritmo per il suo calcolo; nel medesimo articolo, dimostra due teoremi di unicità, i cui enunciati affermano l'unicità sia dell'insieme dei radicali delle componenti di una decomposizione primaria minimale - noto come insieme dei *primi associati* dell'ideale - che dell'insieme delle componenti di una decomposizione primaria minimale i cui radicali sono minimali tra i primi associati, in quanto essi non dipendono dalla decomposizione scelta.

Nel 1921, Emmy Noether dimostra che tutti gli ideali propri di un anello noetheriano sono dotati di una decomposizione primaria minimale, e che esse soddisfano le proprietà di unicità formulate da Macaulay.

Questa tesi tratta gli aspetti computazionali del calcolo della decomposizione primaria di ideali polinomiali: le dimostrazioni classiche del celebre Teorema di Lasker-Noether non sono infatti costruttive. Lo sviluppo di un metodo costruttivo per la determinazione di una decomposizione primaria di un ideale consente di implementare tale calcolo nei sistemi di algebra computazionale, ma anche di sviluppare una teoria più articolata che ci permette di comprendere meglio la natura di tale decomposizione e il suo comportamento.

Come già menzionato, il primo algoritmo per il calcolo della decomposizione primaria viene descritto da Macaulay nel 1913, ma la sua applicazione è limitata agli anelli polinomiali con coefficienti interi o complessi. Il primo algoritmo che calcola la decomposizione primaria di ideali in anelli polinomiali a coefficienti in un qualsiasi campo a caratteristica 0 viene presentato da Grete Hermann, studentessa di Emmy Noether, nella sua tesi di dottorato [7] del 1926; si tratta inoltre del primo algoritmo per il calcolo della decomposizione primaria di cui viene stimata la complessità computazionale.

In seguito ai risultati prodotti da Hermann, vi sono state numerose proposte di algoritmi alternativi nel corso degli anni, tuttavia miglioramenti significativi relativi alla complessità computazionale sono stati raggiunti soltanto negli anni '80, dopo l'introduzione di procedure che sfruttano le basi di Gröbner.

Uno tra i primi algoritmi per il calcolo della decomposizione primaria a fare uso di questo strumento è l'algoritmo GTZ, presentato per la prima volta nel 1984 e pubblicato nel 1988 in [5] da Patrizia Gianni, Barry Trager e Gail Zacharias. Nel 1992, anche David Eisenbud, Craig Huneke e Wolmer Vasconcelos presentano un algoritmo facente uso delle basi di Gröbner in [4] - noto oggi come algoritmo EHV - la cui peculiarità è l'uso di tecniche di algebra omologica e di localizzazione che mantengono un'eventuale struttura sparsa dei generatori dell'ideale. Nel 1996, Takeshi Shimoyama e Kazuhiro Yokoyama presentano in [12] l'algoritmo SY, che mediante le basi di Gröbner ottiene un algoritmo che calcola direttamente una decomposizione primaria minimale; tale algoritmo risulta particolarmente efficiente sotto il punto di vista computazionale nella decomposizione di ideali con un numero elevato di primi associati non minimali. Attualmente, questi ultimi tre algoritmi sono i più usati nei sistemi di algebra computazionale.

	GTZ	EHV	SY
Singular	✓	X	✓
CoCoA	✓	X	✓
Macaulay2	✓	✓	✓
Sage ¹	✓	X	✓

Tabella 1: Algoritmi implementati dai principali sistemi di algebra computazionale

Questa tesi discute nel dettaglio il funzionamento degli algoritmi GTZ e SY.

Nel primo capitolo, introdurremo brevemente alcuni strumenti teorici e definizioni basilari che useremo nel resto della trattazione.

Nel secondo capitolo, esporremo l'algoritmo GTZ rifacendoci alla trattazione di [6]: dimostreremo inizialmente lo *Shape Lemma* nel Teorema 2.5, il quale ci permette di ottenere nel Teorema 2.6 la decomposizione primaria di un ideale 0-dimensionale tramite la fattorizzazione del generatore di un ideale di eliminazione. In seguito generalizzeremo l'algoritmo agli ideali di dimensione positiva, introducendo la nozione di *insieme di variabili indipendente massimale*, per la quale verrà fornito un metodo per il relativo calcolo nell'Algoritmo 2.15. Mostreremo poi nel Teorema 2.18 che è possibile ricondurre il calcolo delle componenti al caso 0-dimensionale già risolto, usando lo *Splitting Tool* enunciato nel Lemma 1.9.

Nel terzo capitolo, partendo dalla teoria sviluppata per l'algoritmo GTZ, esporremo l'algoritmo SY seguendo la trattazione dell'articolo [12]. All'inizio del capitolo mostreremo gli elementi costitutivi fondamentali dell'algoritmo, la *decomposizione pseudo-primaria* e l'*estrazione*, il cui funzionamento verrà mostrato rispettivamente nei Teoremi 3.5 e 3.10. Successivamente dimostreremo nel Teorema 3.19 un criterio per il riconoscimento di componenti ridondanti valido in contesti più generali: esso ci permetterà di formulare l'Algoritmo 3.21, una variante dell'algoritmo GTZ che calcola direttamente una decomposizione primaria minimale dell'ideale. Infine, mediante lo studio delle proprietà dell'*albero di decomposizione* dell'ideale, mostreremo un'applicazione del suddetto criterio all'algoritmo SY che ci porterà alla formulazione dell'Algoritmo 3.34.

¹Implementati tramite un'interfaccia all'interprete di Singular

1 Prerequisiti

Nei capitoli di questa tesi faremo frequente uso di risultati e nozioni concernenti la teoria della dimensione. Ricordiamone intanto le definizioni principali.

Definizione 1.1 (*Altezza di un ideale*). Dato un anello R e un ideale primo $\mathfrak{p} \subsetneq R$, chiamiamo *altezza* di $\mathfrak{p}$ la quantità, anche infinita

$$\text{ht}(\mathfrak{p}) := \sup\{k \in \mathbb{N} \mid \exists \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \dots \subsetneq \mathfrak{p}_k = \mathfrak{p}, \mathfrak{p}_i \text{ primo per ogni } i\}.$$

Dato un anello R e un ideale $I \subsetneq R$, chiamiamo *altezza* di I la quantità, anche infinita

$$\text{ht}(I) := \inf\{\mathfrak{p} \in \text{minAss}(I) \mid \text{ht}(\mathfrak{p})\},$$

indicando con la scrittura $\text{minAss}(I)$ gli elementi minimali rispetto all'inclusione nell'insieme dei primi associati ad I .

Definizione 1.2 (*Dimensione di Krull*). Dato un anello R non banale, chiamiamo *dimensione di Krull* di R la quantità, anche infinita

$$\dim(R) := \sup\{\text{ht}(\mathfrak{p}) \mid \mathfrak{p} \subsetneq R \text{ ideale primo}\}.$$

Dato un ideale $I \subsetneq R$, chiamiamo *dimensione di Krull* di I la quantità, anche infinita

$$\dim(I) := \dim(R/I).$$

In particolare, i risultati della sezione 3.2 avranno a fondamento un'applicazione del seguente risultato di teoria della dimensione.

Teorema 1.3 ([6], Corollario 7.5.5). Sia $<$ un ordinamento monomiale su $\mathbb{K}[\mathbf{x}]$ e sia $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale. Abbiamo:

$$\dim(I) = \dim(\text{Lt}_{<}(I)).$$

Il principale anello con cui lavoreremo nella tesi è l'anello polinomiale in più variabili a coefficienti in un campo. Tale anello possiede alcune proprietà che ricordiamo qui di seguito, e che possono essere dimostrate tramite il Lemma di Normalizzazione di Noether.

Teorema 1.4 ([6], Teorema 3.5.1). Sia $\mathbb{K}$ un campo e $R = \mathbb{K}[\mathbf{x}]$ con $\mathbf{x} = \{x_1, \dots, x_n\}$ insieme di variabili, valgono le seguenti proprietà.

1. Dato un ideale $\mathfrak{m} \subsetneq R$ massimale, $\mathbb{K} \subseteq R/\mathfrak{m}$ è un'estensione di campi finita.
2. Dato un ideale primo $\mathfrak{p} \subsetneq R$, vale la seguente identità

$$\dim(\mathfrak{p}) + \text{ht}(\mathfrak{p}) = \dim(R).$$

3. Dato un ideale $I \subsetneq R$ e la sua base di Gröbner ridotta G rispetto a un ordinamento $<$, $\dim(I) = 0$ se e soltanto se

$$\text{Lt}_{<}(G) \text{ contiene potenze pure di } x_i \text{ per ogni } i = 1, \dots, n.$$

4. Dato un ideale primo $\mathfrak{p} \subsetneq R$, il grado di trascendenza dell'estensione di campi $\mathbb{K} \subseteq \text{Frac}(R/\mathfrak{p})$ è $\text{trdeg}_{\mathbb{K}}(\text{Frac}(R/\mathfrak{p})) = \dim(R/\mathfrak{p})$.
5. Dato un ideale $I \subsetneq R$ e un sottoinsieme di variabili $\mathbf{u} \subseteq \mathbf{x}$ tali che $I \cap \mathbb{K}[\mathbf{u}] = 0$, allora abbiamo $\dim(I) \geq \#\mathbf{u}$.

Inoltre esiste sempre $\mathbf{w} \subseteq \mathbf{x}$ tale che $I \cap \mathbb{K}[\mathbf{w}] = 0$ e $\dim(I) = \#\mathbf{w}$.

Dimostrazione. Dato che 1., 2., 3. e 4. sono risultati molto noti che possono essere trovati in molti manuali di algebra commutativa, non li dimostreremo. Procediamo a dimostrare l'enunciato 5.

Dato un sottoinsieme di variabili $\mathbf{u} \subseteq \mathbf{x}$ tale che $I \cap \mathbb{K}[\mathbf{u}] = 0$, sappiamo che $\bigcap_{\mathfrak{p} \in \min \text{Ass}(I)} (\mathfrak{p} \cap \mathbb{K}[\mathbf{u}]) = \sqrt{I} \cap \mathbb{K}[\mathbf{u}] = 0$. Di conseguenza, esiste un primo minimale $\hat{\mathfrak{p}}$ di I per cui $\hat{\mathfrak{p}} \cap \mathbb{K}[\mathbf{u}] = 0$, e quindi che $\mathbb{K}(\mathbf{u}) \subseteq \text{Frac}(\mathbb{K}[\mathbf{x}]/\hat{\mathfrak{p}})$. Perciò

$$\#\mathbf{u} = \text{trdeg}_{\mathbb{K}}(\mathbb{K}(\mathbf{u})) \leq \text{trdeg}_{\mathbb{K}}(\text{Frac}(\mathbb{K}[\mathbf{x}]/\hat{\mathfrak{p}})).$$

Poiché per l'enunciato 4. vale $\dim(\hat{\mathfrak{p}}) = \text{trdeg}_{\mathbb{K}}(\text{Frac}(\mathbb{K}[\mathbf{x}]/\hat{\mathfrak{p}}))$, abbiamo la seguente disuguaglianza

$$\#\mathbf{u} \leq \text{trdeg}_{\mathbb{K}}(\text{Frac}(\mathbb{K}[\mathbf{x}]/\hat{\mathfrak{p}})) = \dim(\hat{\mathfrak{p}}) \leq \dim(I),$$

e questo dimostra la prima parte dell'enunciato.

Sia ora $\mathfrak{p} \in \min \text{Ass}(I)$ tale che $\dim(\mathfrak{p}) = \dim(I)$.

Dato che $\dim(I) = \text{trdeg}_{\mathbb{K}}(\text{Frac}(\mathbb{K}[\mathbf{x}]/\mathfrak{p}))$, esistono $x_{i_1}, \dots, x_{i_{\dim(\mathfrak{p})}}$ algebricamente indipendenti modulo $\mathfrak{p}$. Di conseguenza, se prendiamo $\mathbf{w} = \{x_{i_1}, \dots, x_{i_{\dim(\mathfrak{p})}}\}$ abbiamo $\mathfrak{p} \cap \mathbb{K}[\mathbf{w}] = 0$, e quindi anche $I \cap \mathbb{K}[\mathbf{w}] = 0$. $\square$

Ricordiamo inoltre il seguente risultato classico sulle proprietà degli ideali primari.

Lemma 1.5 ([1], Lemma 4.4). Sia $\mathfrak{q}$ un ideale $\mathfrak{p}$ -primario di un anello noetheriano A . Valgono le seguenti proprietà:

1. se $x \in \mathfrak{q}$ allora $(\mathfrak{q} : x) = (1)$;
2. se $x \notin \mathfrak{q}$ allora $(\mathfrak{q} : x)$ è $\mathfrak{p}$ -primario;
3. se $x \notin \mathfrak{p}$ allora $(\mathfrak{q} : x) = \mathfrak{q}$.

Nella discussione della tesi sarà molto frequente l'uso di *saturazioni* di ideali.

Definizione 1.6. Siano R un anello, $I \subsetneq R$ un ideale e $S \subsetneq R$ un sottoinsieme moltiplicativo. Consideriamo estensioni e contrazioni di ideali rispetto all'omomorfismo di anelli $i : R \rightarrow R_S$ tale che $i(r) = r/1$ per ogni $r \in R$. Chiamiamo *saturazione* di I rispetto a S l'ideale

$$I^{ec}.$$

Talvolta nella tesi useremo impropriamente la seguente notazione: se S è un insieme finito, indicheremo con R_S la localizzazione rispetto all'insieme moltiplicativo generato da S .

Proposizione 1.7 ([2], Teorema 138.1). Siano R un anello, $I \subsetneq R$ un ideale e $s \in R$, la saturazione di un ideale rispetto all'insieme moltiplicativo generato da s è

$$I^{ec} = I : (s)^\infty.$$

Nella discussione della tesi sarà ampiamente utilizzate saturazioni rispetto a un insieme moltiplicativo. L'utilità di tale strumento è messa in mostra dal seguente teorema, che descrive le proprietà della decomposizione primaria della saturazione di un ideale.

Teorema 1.8 ([1], Proposizioni 4.8, 4.9). Siano $\mathfrak{q}$ un ideale $\mathfrak{p}$ -primario di un anello noetheriano R e $S \subseteq R$ un sottoinsieme moltiplicativo. Consideriamo estensioni e contrazioni di ideali rispetto all'omomorfismo di anelli $i : R \rightarrow R_S$ tale che $i(r) = r/1$ per ogni $r \in R$. Valgono i seguenti enunciati.

1. Se $S \cap \mathfrak{p} = \emptyset$ allora $\mathfrak{q}^e$ è $\mathfrak{p}^e$ -primario e $\mathfrak{q}^{ec} = \mathfrak{q}$.

Se invece $S \cap \mathfrak{p} \neq \emptyset$ allora $\mathfrak{q}^e = R_S$.

2. Sia $I = \bigcap_{i=1}^n \mathfrak{q}_i$ una decomposizione primaria minimale di I con $\sqrt{\mathfrak{q}_i} = \mathfrak{p}_i$. Sia inoltre $k \in \mathbb{N}$ con $k \leq n$ tale che $\mathfrak{p}_i \cap S = \emptyset$ per ogni $i = 1, \dots, k$ e $\mathfrak{p}_i \cap S \neq \emptyset$ altrimenti. Allora

$$I^{ec} = \bigcap_{i=1}^k \mathfrak{q}_i.$$

Vi è inoltre un'ulteriore decomposizione che viene frequentemente usata all'interno della tesi, ed è la seguente.

Lemma 1.9 (Splitting Tool, [6], Lemma 3.3). Siano R un anello e $I \subsetneq R$ un ideale. Sia inoltre $a \in R$ tale che $I : (a) = I : (a^2)$. Allora abbiamo la seguente decomposizione

$$I = I : (a) \cap (I, a).$$

Dimostrazione. Si osserva facilmente che $I : (a) \cap (I, a) \subseteq I$, dimostriamo quindi l'inclusione opposta. Sia $f \in I : (a) \cap (I, a)$, esso si può scrivere come $f = g + ka$ con $g \in I$ e $k \in R$. Dato che $af = ag + a^2k \in I$ allora $a^2k \in I$. Di conseguenza abbiamo $k \in I : (a)^2 = I : (a)$, ovvero $k \in I$, che dimostra che $f \in I$. $\square$

Essendo la discussione di questa tesi di carattere computazionale, ricordiamo inoltre che molte operazioni tra ideali polinomiali sono calcolabili, avendo a disposizione i generatori degli ideali su cui si opera.

Siano $\mathbb{K}$ un campo e $I = (f_1, \dots, f_l)$, $J = (g_1, \dots, g_h)$ una coppia di ideali dell'anello $\mathbb{K}[\mathbf{x}] = \mathbb{K}[x_1, \dots, x_n]$. È possibile calcolare:

- l'intersezione $I \cap J$, poichè è noto che $I \cap J = (tI, (1-t)J) \cap \mathbb{K}[\mathbf{x}]$ dove t è una nuova indeterminata, pertanto prendendo una base di Gröbner G di $(tI, (1-t)J)$ rispetto a un ordinamento lessicografico in cui $\mathbf{x} > t$ possiamo calcolare $I \cap J = (G \cap \mathbb{K}[\mathbf{x}])$;
- il quoziente $I : J$, dato che $I : J = \bigcap_{i=1}^h (I : g_i) = \bigcap_{i=1}^h \frac{1}{g_i} (I \cap g_i)$, e pertanto ci è sufficiente calcolare tali intersezioni tramite il metodo al punto precedente;
- l'ideale $I : J^\infty := \bigcap_{i=1}^\infty I : J^i$, infatti $\mathbb{K}[\mathbf{x}]$ è noetheriano e quindi esiste un naturale s per cui $I : J^s = I : J^\infty$, di conseguenza possiamo ripetere il calcolo dei quozienti $I : J$, $I : J^2$, $I : J^3, \dots$ e restituire l'ideale in cui la catena si stabilizza.

2 L'algoritmo GTZ

L'algoritmo introdotto da Patrizia Gianni, Barry Trager e Gail Zacharias in [5] - conosciuto come algoritmo GTZ dalle iniziali dei suoi autori - è uno dei più noti e usati algoritmi per il calcolo della decomposizione primaria di un ideale polinomiale, nel caso di campi di caratteristica 0 - o perlomeno *sufficientemente grande*. Da un'analisi condotta nel 1999 [3], è emerso essere il più efficiente nella maggior parte dei casi. Nel frattempo, non si sono riscontrati significativi avanzamenti nella letteratura riguardo al calcolo della decomposizione primaria di un qualsiasi ideale polinomiale a scalari in un campo di caratteristica 0.

Nella prima sezione di questo capitolo dimostreremo come è possibile calcolare la decomposizione primaria di un'ideale polinomiale 0-dimensionale tramite un algoritmo per il calcolo della fattorizzazione dei polinomi in una variabile.

Nella seconda sezione mostreremo invece che è sempre possibile ridurre il problema della decomposizione primaria di un ideale proprio qualsiasi al caso 0-dimensionale. Scegliendo un'opportuna estensione dell'ideale in un altro anello polinomiale otteniamo un ideale 0-dimensionale di cui possiamo calcolare le componenti primarie; le contrazioni all'anello polinomiale di partenza di tali componenti restituiscono alcune delle componenti primarie cercate, mentre eventuali componenti rimanenti si possono recuperare applicando ricorsivamente l'algoritmo.

L'uso degli *insiemi di variabili indipendenti rispetto ad un ideale massimale*, congiuntamente con alcuni risultati di teoria della dimensione, sarà fondamentale per la trattazione di quest'ultima parte.

§2.1 Decomposizione primaria di ideali 0-dimensionali

Per iniziare la trattazione del caso 0-dimensionale, introduciamo le seguenti definizioni.

Definizione 2.1. Un ideale massimale $\mathfrak{m} \subsetneq \mathbb{K}[x_1, \dots, x_n]$ si dice in *posizione generale* rispetto all'ordinamento lessicografico dato da $x_1 > \dots > x_n$ se esistono dei polinomi $g_1, \dots, g_n \in \mathbb{K}[x_n]$ tali che $\mathfrak{m} = (x_1 - g_1(x_n), \dots, x_{n-1} - g_{n-1}(x_n), g_n(x_n))$.

Generalizzando, un ideale 0-dimensionale $I \subsetneq \mathbb{K}[x_1, \dots, x_n]$ si dice in *posizione generale* rispetto all'ordinamento lessicografico dato da $x_1 > \dots > x_n$ se tutti i suoi primi associati $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ sono in posizione generale e tali che per ogni $i \neq j$ vale $\mathfrak{p}_i \cap \mathbb{K}[x_n] \neq \mathfrak{p}_j \cap \mathbb{K}[x_n]$.

Notiamo che la definizione appena data è ben posta, infatti i primi associati ad un ideale 0-dimensionale sono massimali.

Nel resto della trattazione, se un ideale è in posizione generale rispetto all'ordinamento lessicografico dato da $x_1 > \dots > x_n$ diremo semplicemente che è in posizione generale, omettendo l'ordine.

Osservazione 2.2. Dato un ideale massimale in posizione generale I , un insieme di generatori di I del tipo $\{x_1 - g_1(x_n), \dots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)\}$ è una base di Gröbner minimale rispetto all'ordinamento lessicografico dato da $x_1 > \dots > x_n$. A meno di riduzioni modulo $g_n(x_n)$, possiamo assumere senza perdita di generalità che sia ridotta.

Notiamo che non tutti gli ideali 0-dimensionali sono in posizione generale: per mostrarlo è sufficiente prendere un qualsiasi ideale massimale la cui base di Gröbner ridotta

rispetto a un ordinamento lessicografico non è della forma voluta, ad esempio l'ideale $(x, y^2 + y + 1) \subseteq \mathbb{K}[x, y]$ con $\mathbb{K} = \mathbb{Q}$ oppure $\mathbb{K} = \mathbb{F}_p$, con $p \in \mathbb{N}$ primo, non è in posizione generale rispetto all'ordinamento $x > y$.

Come vedremo nelle proposizioni successive, è possibile ricondurre con facilità lo studio degli ideali 0-dimensionali a quello degli ideali in posizione generale.

Quasi tutti gli ideali 0-dimensionali sono in posizione generale, infatti se si effettua un cambio di variabili *casuale*, la probabilità che si ottenga un ideale che non è in posizione generale è nulla. La formalizzazione di questo fatto verrà vista tra poco. Preliminarmente, dimostriamo alcuni lemmi che ci serviranno per dimostrare le successive proposizioni.

Lemma 2.3. Siano R un anello commutativo e I un ideale di R . Siano inoltre $f_1, \dots, f_r \in R$ elementi non invertibili di R tali che $f = f_1 \cdots f_r \in I$ e tali che $(f_i, f_j) = R$ per ogni $i \neq j$. Allora l'ideale I si può scrivere come

$$I = \bigcap_{i=1}^r (I, f_i).$$

Dimostrazione. Dato che gli ideali (I, f_i) sono a coppie comassimali, infatti $(I, f_i) + (I, f_j) = I + (f_i, f_j) = R$. Inoltre l'intersezione di ideali comassimali è sempre uguale al loro prodotto, e quindi vale

$$(I, f_i) \cap (I, f_j) = (I, f_i)(I, f_j) = (I^2, (f_i, f_j)I, f_i f_j).$$

Poiché $I^2 \subseteq I$ e $(f_i, f_j) = R$ abbiamo anche

$$(I, f_i) \cap (I, f_j) = (I^2, I, f_i f_j) = (I, f_i f_j).$$

Per il caso base $r = 2$, visto che $f \in I$, ci basta specializzare l'identità appena ottenuta

$$(I, f_1) \cap (I, f_2) = (I, f) = I.$$

Sia dunque $r > 2$, per dimostrare il passo induttivo osserviamo che

$$\bigcap_{i=1}^r (I, f_i) = \prod_{i=1}^r (I, f_i) = (I, f_1)(I, f_2) \prod_{i=3}^r (I, f_i) = (I, f_1 f_2) \prod_{i=3}^r (I, f_i).$$

Consideriamo gli elementi $g_1 := f_1 f_2$ e $g_i := f_{i+1}$ per $i = 2, \dots, r-1$. Chiaramente essi non sono invertibili, e inoltre gli ideali (g_i) sono a coppie comassimali. Questo è vero in quanto per ogni $j = 3, \dots, r$ esistono $a, b, a', b' \in R$ tali che

$$a f_1 + b f_j = 1, \quad a' f_2 + b' f_j = 1.$$

Moltiplicando la prima delle due identità per $a' f_2$ otteniamo $aa' f_1 f_2 + a' b f_2 f_j = a' f_2 = 1 - b' f_j$. Di conseguenza, per ogni $j > 1$, gli ideali (g_1) e (g_j) sono comassimali in quanto $(aa') f_1 f_2 + (a' b f_2 + b') f_j = 1$. In conclusione, gli elementi soddisfano le ipotesi del lemma, e quindi possiamo applicare l'ipotesi induttiva per concludere che

$$\bigcap_{i=1}^r (I, f_i) = (I, f_1 f_2) \prod_{i=3}^r (I, f_i) = \prod_{i=1}^{r-1} (I, g_i) = \bigcap_{i=1}^{r-1} (I, g_i) = I. \quad \square$$

Ricordiamo che un polinomio $f \in \mathbb{K}[\mathbf{x}]$ si dice *libero da quadrati* in $\mathbb{K}[\mathbf{x}]$ se non è divisibile per alcun quadrato di un polinomio irriducibile di $\mathbb{K}[\mathbf{x}]$.

Lemma 2.4. Siano $\mathbb{K}$ un campo di caratteristica 0, $\bar{\mathbb{K}}$ la sua chiusura algebrica e $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale. Allora:

1. $I\bar{\mathbb{K}}[\mathbf{x}] \cap \mathbb{K}[\mathbf{x}] = I$;
2. se p è libero da quadrati in $\mathbb{K}[\mathbf{x}]$ allora è anche libero da quadrati in $\bar{\mathbb{K}}[\mathbf{x}]$.

Dimostrazione. 1. Dato un polinomio $p(\mathbf{x}) \in I\bar{\mathbb{K}}[\mathbf{x}] \cap \mathbb{K}[\mathbf{x}]$, esistono $i(\mathbf{x}) \in I$ e $q(\mathbf{x}) \in \bar{\mathbb{K}}[\mathbf{x}]$ per cui $p(\mathbf{x}) = i(\mathbf{x}) \cdot q(\mathbf{x})$. Dato un qualsiasi ordinamento monomiale, dividendo $p(\mathbf{x})$ per $i(\mathbf{x})$ in $\bar{\mathbb{K}}[\mathbf{x}]$ otteniamo una scrittura $p(\mathbf{x}) = u(\mathbf{x})i(\mathbf{x}) + r(\mathbf{x})$ con $u(\mathbf{x}), r(\mathbf{x}) \in \bar{\mathbb{K}}[\mathbf{x}]$. Visto che l'algoritmo di divisione è stato fatto tra polinomi in $\mathbb{K}[\mathbf{x}]$, allora anche $u(\mathbf{x})$ appartiene a $\mathbb{K}[\mathbf{x}]$. Dato che abbiamo diviso per un solo polinomio il resto è unico, e quindi $r = 0$ e $u(\mathbf{x}) = q(\mathbf{x}) \in \mathbb{K}[\mathbf{x}]$. Questo fatto implica $p(\mathbf{x}) \in I\mathbb{K}[\mathbf{x}] = I$ e perciò $I\bar{\mathbb{K}}[\mathbf{x}] \cap \mathbb{K}[\mathbf{x}] \subseteq I$. Poiché vale anche l'inclusione opposta, abbiamo dimostrato l'uguaglianza voluta.

2. Per il criterio della derivata, un polinomio $p(\mathbf{x})$ è libero da quadrati se e solo se vale $(p(\mathbf{x}), p'(\mathbf{x})) = (1)$. Questo implica che $(p(\mathbf{x}), p'(\mathbf{x}))_{\bar{\mathbb{K}}[\mathbf{x}]} = (1)_{\bar{\mathbb{K}}[\mathbf{x}]}$ e quindi $p(\mathbf{x})$ è libero da quadrati anche quando è visto come polinomio in $\bar{\mathbb{K}}$. $\square$

Dimostriamo ora un teorema nota in letteratura con il nome di *Shape Lemma*, risultato centrale per lo studio dei sistemi 0-dimensionali da un punto di vista computazionale.

Teorema 2.5 (Shape Lemma)

Sia $\mathbb{K}$ un campo di caratteristica 0 e $I \subseteq \mathbb{K}[\mathbf{x}]$ un ideale 0-dimensionale. Per ogni $a = (a_1, \dots, a_{n-1}) \in \mathbb{K}^{n-1}$, definiamo un cambio di variabili

$$\begin{aligned} \phi_a : \mathbb{K}[\mathbf{x}] &\longrightarrow \mathbb{K}[\mathbf{x}] \\ x_i &\longmapsto x_i \quad \text{per } i < n, \\ x_n &\longmapsto x_n + \sum_{i=1}^{n-1} a_i x_i. \end{aligned}$$

Allora esiste un aperto di Zariski non vuoto $U \subseteq \mathbb{K}^{n-1}$ tale che per ogni $a \in U$ l'ideale $\phi_a(I)$ è in posizione generale.

Dimostrazione. Per dimostrare questo teorema, distinguiamo due casi.

I massimale: Sappiamo dal Teorema 1.4.1 che $\mathbb{K}[\mathbf{x}]/I$ è un'estensione finita di $\mathbb{K}$. Dato che ogni estensione finita è algebrica, possiamo applicare il Teorema dell'Elemento Primitivo. Seguendo una dimostrazione costruttiva del teorema, come ad esempio quella descritta in [13] che usa il *metodo delle indeterminate* di Kronecker, possiamo osservare che esiste un aperto di Zariski non vuoto $U \subseteq \mathbb{K}^{n-1}$ tale che, per ogni $a = (a_1, \dots, a_{n-1}) \in U$, l'elemento

$$z_a := x_n + \sum_{i=1}^{n-1} a_i x_i$$

è primitivo per l'estensione di campo $\mathbb{K}[\mathbf{x}]/I$. Tale dimostrazione necessita che $\mathbb{K}$ sia perfetto ed infinito, e tali caratteristiche sono verificate in quanto $\mathbb{K}$ è di caratteristica 0.

Senza perdita di generalità, si può assumere che 0 sia un elemento di U . Questo è possibile in quanto per ogni $b, c \in \mathbb{K}^{n-1}$ è facile verificare che $\phi_{b+c} = \phi_b \circ \phi_c$, perciò per ogni $a = (a_1, \dots, a_{n-1}) \in U$ possiamo sostituire l'ideale I e l'insieme U rispettivamente con $\tilde{I} := \phi_a(I)$ e $\tilde{U} := \{b \in \mathbb{K}^{n-1} \mid b + a \in U\}$: per ogni $b \in \tilde{U}$ l'ideale $\phi_b(\tilde{I}) = \phi_{b+a}(I)$ è in posizione generale se e solo se per ogni $c \in U$ l'ideale $\phi_c(I)$ è in posizione generale.

Sia pertanto $0 \in U$; l'elemento $z_0 = x_n + \sum_{i=1}^{n-1} 0 \cdot x_i = x_n$ è primitivo per l'estensione $\mathbb{K} \subsetneq \mathbb{K}[\mathbf{x}]/I$. Abbiamo dunque un isomorfismo di $\mathbb{K}$ -algebre

$$\begin{aligned} \phi : \mathbb{K}[\mathbf{x}]/I &\longrightarrow \mathbb{K}[x_n]/(g_n(x_n)) \\ x_i + I &\longmapsto g_i(x_n) + (g_n(x_n)) \quad \text{per } i < n, \\ x_n + I &\longmapsto x_n + (g_n(x_n)), \end{aligned}$$

con $g_1(x_n), \dots, g_n(x_n) \in \mathbb{K}[x_n]$ e $g_n(x_n)$ irriducibile.

Sia $\pi : \mathbb{K}[\mathbf{x}] \rightarrow \mathbb{K}[\mathbf{x}]/I$ la proiezione naturale al quoziente. Se consideriamo la composizione $\pi \circ \phi : \mathbb{K}[\mathbf{x}] \rightarrow \mathbb{K}[x_n]/(g_n(x_n))$ possiamo osservare che $p(\mathbf{x})$ appartiene ad I se e soltanto se $p(g_1(x_n), \dots, g_{n-1}(x_n), x_n) + (g_n(x_n)) = (g_n(x_n))$, ovvero se e soltanto se $p(g_1(x_n), \dots, g_{n-1}(x_n), x_n)$ appartiene a $(g_n(x_n))$. Questo ci permette di osservare che vale il contenimento

$$(x_1 - g_1(x_n), \dots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)) \subseteq I.$$

Tuttavia, essendo $g_n(x_n)$ irriducibile, l'ideale appena definito è massimale, e quindi è esattamente I . Concludiamo che I è un ideale in posizione generale.

I non massimale: Siano $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ i primi associati ad I . Per ogni primo $\mathfrak{p}_i$ esiste un aperto di Zariski non vuoto U_i tale che se $a \in U_i$, l'ideale $\phi_a(\mathfrak{p}_i)$ è in posizione generale. Considerando $U = \cap_{i=1}^s U_i$, che è aperto e non vuoto, e $a \in U$, allora tutti i $\phi_a(\mathfrak{p}_i)$ sono in posizione generale. A meno di un cambio di variabili, possiamo assumere senza perdita di generalità che $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ sono in posizione generale.

L'unica proprietà che rimane da controllare è che per ogni $i \neq j$ valga la disuguaglianza $\mathfrak{p}_i \cap \mathbb{K}[x_n] \neq \mathfrak{p}_j \cap \mathbb{K}[x_n]$.

Sia $J = (x_1 - g_1(x_n), \dots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)) \subseteq \mathbb{K}[\mathbf{x}]$ un ideale massimale in posizione generale qualunque, e studiamo l' $(n-1)$ -simo ideale di eliminazione di $\phi_a(J)$. A meno di intersecare U con un aperto di Zariski non vuoto, possiamo assumere che anche $\phi_a(J)$ sia in posizione generale, e che quindi si possa scrivere come $\phi_a(J) = (x_1 - g'_{a1}(x_n), \dots, x_{n-1} - g'_{a(n-1)}(x_n), g'_{an}(x_n))$ con $g'_{a1}(x_n), \dots, g'_{an}(x_n) \in \mathbb{K}[x_n]$ e $g'_{an}(x_n)$ irriducibile di grado $r = \dim_{\mathbb{K}} \mathbb{K}[x_n]/(g'_{an}(x_n))$.

L'omomorfismo di $\mathbb{K}$ -algebre

$$\begin{aligned} \mathbb{K}[\mathbf{x}] &\longrightarrow \mathbb{K}[x_n]/(g'_{an}(x_n)) \\ x_i &\longmapsto g'_{ai}(x_n) + (g'_{an}(x_n)) \quad \text{per } i < n, \\ x_n &\longmapsto x_n + (g'_{an}(x_n)), \end{aligned}$$

ha un nucleo che contiene $(x_1 - g'_{a1}(x_n), \dots, x_{n-1} - g'_{a(n-1)}(x_n), g'_{an}(x_n)) = \phi_a(J)$. Dato che $\phi_a(J)$ è un ideale massimale e che l'omomorfismo non è nullo, il suo nucleo coincide con $\phi_a(J)$. Abbiamo quindi che $\mathbb{K}[\mathbf{x}]/\phi_a(J)$ è isomorfo a $\mathbb{K}[x_n]/(g'_{an}(x_n))$ come $\mathbb{K}$ -algebre, e quindi anche come $\mathbb{K}$ -spazi vettoriali. Di conseguenza

$$r = \dim_{\mathbb{K}} \mathbb{K}[x_n]/(g'_{an}(x_n)) = \dim_{\mathbb{K}} \mathbb{K}[\mathbf{x}]/\phi_a(J) = \dim_{\mathbb{K}} \mathbb{K}[\mathbf{x}]/J = \deg(g_n).$$

Dato che $g_n(x_n)$ è irriducibile, esso è libero da quadrati in $\mathbb{K}[\mathbf{x}]$, e per il Lemma 2.4.2 anche in $\bar{\mathbb{K}}[\mathbf{x}]$. Siano allora $\alpha_1, \dots, \alpha_r$ le r radici distinte di g_n in $\bar{\mathbb{K}}$. Per quanto visto nel Lemma 2.3 sappiamo che

$$J\bar{\mathbb{K}}[\mathbf{x}] = \bigcap_{i=1}^r (x_1 - g_1(x_n), \dots, x_{n-1} - g_{n-1}(x_n), g_n(x_n), x_n - \alpha_i)_{\bar{\mathbb{K}}[\mathbf{x}]}.$$

Consideriamo l'unica estensione a $\bar{\mathbb{K}}[\mathbf{x}] \rightarrow \bar{\mathbb{K}}[\mathbf{x}]$ dell'isomorfismo di $\mathbb{K}$ -algebre ϕ_a , che per comodità continuiamo a chiamare ϕ_a . Se applichiamo questo cambio di variabili a $J\bar{\mathbb{K}}[\mathbf{x}]$ otteniamo

$$\begin{aligned} \phi_a(J\bar{\mathbb{K}}[\mathbf{x}]) &= \phi_a \left(\bigcap_{i=1}^r (x_1 - g_1(x_n), \dots, x_{n-1} - g_{n-1}(x_n), g_n(x_n)x_n - \alpha_i)_{\bar{\mathbb{K}}[\mathbf{x}]} \right) \\ &= \bigcap_{i=1}^r \left(x_1 - g'_{a1}(x_n), \dots, x_{n-1} - g'_{a(n-1)}(x_n), g'_{an}(x_n), x_n - \alpha_i + \sum_{h=1}^{n-1} a_h x_h \right)_{\bar{\mathbb{K}}[\mathbf{x}]} \\ &= \bigcap_{i=1}^r \left(x_1 - g'_{a1}(x_n), \dots, x_{n-1} - g'_{a(n-1)}(x_n), x_n - \alpha_i + \sum_{h=1}^{n-1} a_h g'_{ah}(\alpha_i) \right)_{\bar{\mathbb{K}}[\mathbf{x}]}, \end{aligned}$$

e pertanto

$$\begin{aligned} &\left(\prod_{i=1}^r \left(x_n - \alpha_i + \sum_{h=1}^{n-1} a_h g'_{ah}(\alpha_i) \right) \right)_{\bar{\mathbb{K}}[\mathbf{x}]} \subseteq \bigcap_{i=1}^r \left(x_n - \alpha_i + \sum_{h=1}^{n-1} a_h g'_{ah}(\alpha_i) \right)_{\bar{\mathbb{K}}[\mathbf{x}]} \\ &\subseteq \bigcap_{i=1}^r \left(x_1 - g_1(x_n), \dots, x_{n-1} - g_{n-1}(x_n), x_n - \alpha_i + \sum_{h=1}^{n-1} a_h g'_{ah}(\alpha_i) \right)_{\bar{\mathbb{K}}[\mathbf{x}]} \cap \bar{\mathbb{K}}[x_n] \\ &= \phi_a(J\bar{\mathbb{K}}[\mathbf{x}]) \cap \bar{\mathbb{K}}[x_n]. \end{aligned}$$

Per il Lemma 2.4.1, sappiamo anche che

$$\begin{aligned} (g'_{an}(x_n)) &= \phi_a(J) \cap \bar{\mathbb{K}}[x_n] = \phi_a(J)\bar{\mathbb{K}}[\mathbf{x}] \cap \bar{\mathbb{K}}[\mathbf{x}] \cap \bar{\mathbb{K}}[x_n] \\ &= \phi_a(J)\bar{\mathbb{K}}[\mathbf{x}] \cap \bar{\mathbb{K}}[x_n] = \phi_a(J\bar{\mathbb{K}}[\mathbf{x}]) \cap \bar{\mathbb{K}}[x_n]. \end{aligned}$$

Sia ora

$$f_a(x_n) := \prod_{i=1}^r \left(x_n - \alpha_i + \sum_{h=1}^{n-1} a_h g'_{ah}(\alpha_i) \right) \in \mathbb{K}(\alpha_1, \dots, \alpha_r)[x_n].$$

Visto che f_a è invariante sotto l'azione del gruppo $\text{Gal}(\mathbb{K}(\alpha_1, \dots, \alpha_r)/\mathbb{K})$, deduciamo che è un polinomio a coefficienti in $\mathbb{K}$. Inoltre, dal momento che $f_a \in \phi_a(J\bar{\mathbb{K}}[\mathbf{x}]) \cap \bar{\mathbb{K}}[x_n]$, abbiamo $f_a \in \phi_a(J\bar{\mathbb{K}}[\mathbf{x}]) \cap \bar{\mathbb{K}}[x_n] = (g'_{an}(x_n))$. Poiché sia f_a che g'_{an} sono polinomi monici di grado r appartenenti allo stesso ideale principale, abbiamo $f_a = g'_{an}$.

Ricordando che gli ideali $\phi_a(\mathfrak{p}_i)$ sono in posizione generale, chiamiamo $f_{ia} \in \bar{\mathbb{K}}[x_n]$ i polinomi monici tali che $\phi_a(\mathfrak{p}_i) \cap \bar{\mathbb{K}}[x_n] = (f_{ia}(x_n))$.

Nel caso in cui avessimo $\phi_a(\mathfrak{p}_i) \cap \bar{\mathbb{K}}[x_n] = \phi_a(\mathfrak{p}_j) \cap \bar{\mathbb{K}}[x_n]$ per qualche coppia di i, j distinti, avremmo che $f_{ia} = f_{ja}$. Quest'ultima identità definisce un sistema di equazioni polinomiali non nulle che dipende anche da $a \in \mathbb{K}^{n-1}$ visto che $\mathfrak{p}_i \neq \mathfrak{p}_j$. A meno di intersecare ulteriormente l'aperto U con un aperto, possiamo perciò assumere che per ogni $a \in U$ e per ogni $i \neq j$ vale $f_{ia} \neq f_{ja}$, che è quanto volevamo. $\square$

Procediamo quindi dimostrando in che modo sia possibile calcolare una decomposizione primaria nel caso di ideali in posizione generale.

Teorema 2.6

Siano $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale 0-dimensionale e $g = g_1^{\nu_1} \dots g_s^{\nu_s} \in \mathbb{K}[x_n]$, con g_i polinomi monici irriducibili distinti, tale che $(g) = I \cap \mathbb{K}[x_n]$. Allora

$$1. \quad I = \bigcap_{i=1}^s (I, g_i^{\nu_i}).$$

Inoltre, se I è in posizione generale:

2. $(I, g_i^{\nu_i})$ è primario per ogni $i = 1, \dots, s$;
3. $(I, g_i^{\nu_i})$ è in posizione generale per ogni $i = 1, \dots, s$.

Dimostrazione. 1. Sappiamo già che $I \subseteq \bigcap_{i=1}^s (I, g_i^{\nu_i})$, per cui verifichiamo che vale l'inclusione opposta. Posto $g_i := g/g_i^{\nu_i}$, abbiamo che $(g_1, \dots, g_s)\mathbb{K}[x_n] = (1)\mathbb{K}[x_n]$, perciò esistono dei polinomi $a_1, \dots, a_s \in \mathbb{K}[x_n]$ tali che $\sum_{i=1}^s a_i g_i = 1$.

Sia $f \in \bigcap_{i=1}^s (I, g_i^{\nu_i})$. Per ogni $i = 1, \dots, s$ esistono $f_i \in I$, $\xi_i \in \mathbb{K}[\mathbf{x}]$ per cui $f = f_i + \xi_i g_i^{\nu_i}$. Di conseguenza

$$f = \sum_{i=1}^s a_i g_i (f_i + \xi_i g_i^{\nu_i}) = \sum_{i=1}^s (a_i g_i f_i + a_i \xi_i g) \in I.$$

2. Osserviamo che per ogni $i = 1, \dots, s$, l'ideale $(I, g_i^{\nu_i}) \subseteq \mathbb{K}[\mathbf{x}]$ è proprio. Questo è vero in quanto, se fosse tutto $\mathbb{K}[\mathbf{x}]$, esisterebbero dei polinomi $f \in I$, $a \in \mathbb{K}[\mathbf{x}]$ per cui $f + a g_i^{\nu_i} = 1$, tuttavia moltiplicando entrambi i membri di questa identità per $g_i := g/g_i^{\nu_i}$ otteniamo $g_i f + a g = g_i$, e quindi g_i appartiene a $(f, g) \subseteq I$. Questo ci fornisce un assurdo, in quanto avremmo $I \cap \mathbb{K}[x_n] = (g) \subsetneq (g_i) \subseteq I \cap \mathbb{K}[x_n]$.

Mostriamo anche che $\text{Ass}((I, g_i^{\nu_i})) \subseteq \text{Ass}(I)$: questo è vero perché i primi associati sono tutti massimali, e quindi comassimali, perciò per le proprietà del radicale

$$\sqrt{(I, g_i^{\nu_i})} = \sqrt{(\sqrt{I}, g_i)} = \sqrt{\left(\bigcap_{\mathfrak{p} \in \text{Ass}(I)} \mathfrak{p}, g_i \right)} = \sqrt{\left(\prod_{\mathfrak{p} \in \text{Ass}(I)} \mathfrak{p}, g_i \right)} = \bigcap_{\mathfrak{p} \in \text{Ass}(I)} \sqrt{(\mathfrak{p}, g_i)}.$$

Di conseguenza

$$\begin{aligned} \bigcap_{\mathfrak{p} \in \text{Ass}((I, g_i^{\nu_i}))} \mathfrak{p} &= \sqrt{(I, g_i^{\nu_i})} = \bigcap_{\mathfrak{p} \in \text{Ass}(I)} \sqrt{(\mathfrak{p}, g_i)} \\ &= \left(\bigcap_{\mathfrak{p} \in \text{Ass}(I), g_i \in \mathfrak{p}} \mathfrak{p} \right) \cap \left(\bigcap_{\mathfrak{p} \in \text{Ass}(I), g_i \notin \mathfrak{p}} \mathbb{K}[\mathbf{x}] \right) = \bigcap_{\mathfrak{p} \in \text{Ass}(I), g_i \in \mathfrak{p}} \mathfrak{p}, \end{aligned}$$

da cui segue che $\text{Ass}((I, g_i^{\nu_i})) = \{\mathfrak{p} \in \text{Ass}(I) \mid g_i \in \mathfrak{p}\} \subseteq \text{Ass}(I)$.

Siano $\mathfrak{p}_1, \dots, \mathfrak{p}_k$ i primi associati ad I e siano $p_i \in \mathbb{K}[x_n]$ polinomi tali che $\mathfrak{p}_i \cap \mathbb{K}[x_n] = (p_i)$. Essendo I in posizione generale, i p_i sono tutti polinomi irriducibili distinti, e quindi a coppie comassimali. Come conseguenza abbiamo che

$$\left(\prod_{i=1}^k p_i \right) = \bigcap_{i=1}^k (p_i) = \bigcap_{i=1}^k (\mathfrak{p}_i \cap \mathbb{K}[x_n]) = \bigcap_{i=1}^k \mathfrak{p}_i \cap \mathbb{K}[x_n] = \sqrt{I} \cap \mathbb{K}[x_n].$$

Dato che $\mathbb{K}[\mathbf{x}]$ è noetheriano, esiste un intero m per cui

$$\left(\prod_{i=1}^k p_i \right)^m = \left(\sqrt{I} \cap \mathbb{K}[x_n] \right)^m \subseteq (g) = I \cap \mathbb{K}[x_n] \subseteq \sqrt{I} \cap \mathbb{K}[x_n] = \left(\prod_{i=1}^k p_i \right)$$

e quindi abbiamo che $\prod_{i=1}^k p_i \mid g \mid \prod_{i=1}^k p_i^m$; questo ci dice che i divisori irriducibili di g sono proprio $p_1, \dots, p_k$ con $l = s$.

Senza perdita di generalità assumiamo che $p_i = g_i$, quindi $\mathfrak{p}_i$ è l'unico primo associato ad I che contiene $g_i^{\nu_i}$ e perciò per il Teorema 1.8.1 concludiamo $\text{Ass}((I, g_i^{\nu_i})) = \{\mathfrak{p} \in \text{Ass}(I) \mid g_i^{\nu_i} \in \mathfrak{p}\} = \{\mathfrak{p}_i\}$ e quindi $(I, g_i^{\nu_i})$ è primario.

3. Come abbiamo precedentemente visto

$$\sqrt{(I, g_i^{\nu_i})} = \bigcap_{\mathfrak{p} \in \text{Ass}(I), g_i \in \mathfrak{p}} \sqrt{\mathfrak{p}}.$$

Poiché ogni $\mathfrak{p} \in \text{Ass}(I)$ è in posizione generale, lo è anche $(I, g_i^{\nu_i})$. □

Corollario 2.7. Sia $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale in posizione generale. La decomposizione $I = \cap_{i=1}^s (I, g_i^{\nu_i})$ descritta nel Teorema 2.6 è una decomposizione primaria minimale.

Dimostrazione. Si tratta di una decomposizione primaria per definizione; è anche minimale in quanto, come visto nella dimostrazione del Teorema 2.6, il numero di componenti s è pari al numero di primi associati di I . □

Fissato un ideale I , l'insieme di parametri a per cui $\phi_a(I)$ non è in posizione generale è un chiuso di Zariski di $\mathbb{K}^{n-1}$. Non possiamo dunque essere certi che prendendo un parametro questo non appartenga a tale chiuso. Nel caso in cui il campo sia $\mathbb{Q}$, possiamo ad esempio prendere a con distribuzione uniforme sulla palla unitaria; la probabilità che $\phi_a(I)$ non sia in posizione generale è 0, ma non è impossibile che ciò avvenga.

Dunque, per certificare che la decomposizione ottenuta sia una decomposizione primaria, individuiamo un criterio algoritmico che ci permette di verificare, tra l'altro, se gli ideali del Teorema 2.6 sono in posizione generale.

Teorema 2.8

Sia $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale. Le seguenti condizioni sono equivalenti.

1. I è un ideale 0-dimensionale, primario e in posizione generale.
2. Esistono dei polinomi $g_1, \dots, g_n \in \mathbb{K}[x_n]$ e degli interi positivi $\mu_1, \dots, \mu_n$ tali che:
 - $I \cap \mathbb{K}[x_n] = (g_n^{\mu_n})$ con g_n irriducibile;
 - $(x_j - g_j)^{\mu_j} \in I$, per ogni $j < n$.
3. Sia G la base di Gröbner ridotta di I rispetto all'ordine lessicografico dato da $x_1 > \dots > x_n$. Esistono dei polinomi $g_1, \dots, g_n \in \mathbb{K}[x_n]$ e degli interi positivi $\nu_1, \dots, \nu_n$ tali che:
 - $g_n^{\nu_n} \in G$ con g_n irriducibile;
 - $(x_j - g_j)^{\nu_j}$ è congruente a un elemento in $G \cap \mathbb{K}[x_j, \dots, x_n]$ modulo l'ideale $(x_{j+1} - g_{j+1}, \dots, x_{n-1} - g_{n-1}, g_n) \subseteq \mathbb{K}[\mathbf{x}]$ per ogni $j = 1, \dots, n-1$.

Dimostrazione. In questa dimostrazione useremo più volt il seguente fatto: per ogni $j = 1, \dots, n$, vale $I \cap \mathbb{K}[x_j] \neq (0)$. Infatti, dato che I è un ideale 0-dimensionale, per il Teorema 1.4.3 la base di Gröbner ridotta contiene un polinomio il cui monomio di testa è una potenza pura di x_j , e quindi è un polinomio in $\mathbb{K}[x_j]$ per ogni j . Procediamo a dimostrare questo criterio mostrando le implicazioni $3. \Rightarrow 2. \Rightarrow 1. \Rightarrow 3.$

3. $\Rightarrow$ 2. Dato che G è una base di Gröbner ridotta, non può contenere due elementi distinti di $\mathbb{K}[x_n]$. Per il teorema di eliminazione delle variabili, $I \cap \mathbb{K}[x_n] = (G \cap \mathbb{K}[x_n]) = (g_n^{\mu_n})$. Per induzione si dimostra anche che esiste una potenza di $x_i - g_i$ che appartiene a I per $i < n$, o equivalentemente che $x_i - g_i$ appartiene a $\sqrt{I}$ per ogni $i < n$. Ipotizzando che per ogni j tale che $i < j \leq n$ si abbia $x_j - g_j \in \sqrt{I}$, sappiamo per la seconda proprietà del punto 3. che esiste una potenza di $x_i - g_i$ congrua ad un elemento di I modulo un ideale generato da elementi di $\sqrt{I}$. Ne consegue che $x_i - g_i$ appartiene a $\sqrt{I + (x_{j+1} - g_{j+1}, \dots, x_{n-1} - g_{n-1}, g_n)} = \sqrt{I}$.
2. $\Rightarrow$ 1. Essendo g_n irriducibile, l'ideale $J := (x_1 - g_1, \dots, x_{n-1} - g_{n-1}, g_n)$ è massimale. Il fatto che J sia contenuto in $\sqrt{I}$ implica $\sqrt{I} = J$. Inoltre, un ideale il cui radicale è massimale è sempre primario e 0-dimensionale. Concludiamo che I è in posizione generale perché il suo unico primo associato J è in posizione generale.
1. $\Rightarrow$ 3. Poiché I è in posizione generale, lo è anche $\sqrt{I}$. Esistono quindi dei polinomi $g_1, \dots, g_n \in \mathbb{K}[x_n]$ con g_n monico e irriducibile tali che $\sqrt{I} = (x_1 - g_1, \dots, x_{n-1} - g_{n-1}, g_n)$.

Chiamiamo G la base di Gröbner ridotta di I rispetto all'ordinamento lessicografico dato da $x_1 > \dots > x_n$ e sia $G \cap \mathbb{K}[x_n] = \{g\}$. Per il Teorema di eliminazione delle variabili, sappiamo che l'ideale $I \cap \mathbb{K}[x_n] = (g)$. Poiché $\sqrt{I \cap \mathbb{K}[x_n]} = (g_n)$ con g_n irriducibile, avremo necessariamente $g = g_n^{\nu_n}$ per un qualche $\nu_n \in \mathbb{N}$. Questo dimostra la prima proprietà del punto 3.

Per dimostrare la seconda proprietà del punto 3. facciamo la seguente osservazione.

Per il Teorema 1.4.3, per ogni $j = 1, \dots, n$ esiste un elemento $h^{(j)} \in G$ ed un intero positivo m_j tali che $\text{LM}(h^{(j)}) = x_j^{m_j}$; una conseguenza immediata di quest'ultimo fatto è che $h^{(j)}$ è un elemento di $\mathbb{K}[x_j, \dots, x_n]$.

Poniamo $\mathbf{x}' := \{x_{j+1}, \dots, x_n\}$, $\mathbf{m}' := \sqrt{I} \cap \mathbb{K}[\mathbf{x}'] = (x_{j+1} - g_{j+1}, \dots, x_{n-1} - g_{n-1}, g_n)_{\mathbb{K}[\mathbf{x}]}$ e $\mathbb{K}' := \mathbb{K}[\mathbf{x}']/\mathbf{m}'$. Fissato j , consideriamo la proiezione al quoziente per $\mathbf{m}'$ dei coefficienti in $\mathbb{K}[\mathbf{x}']$

$$\pi : \mathbb{K}[x_1, \dots, x_n] = (\mathbb{K}[\mathbf{x}'])(x_1, \dots, x_j) \longrightarrow \mathbb{K}'[x_1, \dots, x_j].$$

Valgono allora i seguenti fatti:

- (1) $\pi(G \cap \mathbb{K}[x_j, \mathbf{x}']) = \{\pi(h^{(j)}), 0\}$;
- (2) esiste $l_j \in \mathbb{Z}_+$ tale che $\pi(I) \cap \mathbb{K}'[x_j] = ((x_j - \bar{g}_j)^{l_j})_{\mathbb{K}'[x_j]}$, dove $\bar{g}_j$ denota la proiezione al quoziente per $\mathbf{m}'$ di g_j .

Supponiamo che (1) e (2) siano vere. Dalla proprietà (1) consegue che tutti gli elementi di $G \cap \mathbb{K}[x_j, \mathbf{x}']$ diversi da $h^{(j)}$ sono polinomi in x_j con coefficienti appartenenti a $\mathbf{m}'$. Per il Teorema di eliminazione delle variabili sappiamo inoltre che $\pi(I \cap \mathbb{K}[x_j, \mathbf{x}']) = (\pi(G \cap \mathbb{K}[x_j, \mathbf{x}']))_{\mathbb{K}'[x_1, \dots, x_j]} = (\pi(h^{(j)}))_{\mathbb{K}'[x_1, \dots, x_j]}$.

Vista la proprietà (2) e dato che $h^{(j)}$ è monico, abbiamo che $\pi(h^{(j)}) = (x_j - \bar{g}_j)^{l_j}$ e

$$l_j = m_j.$$

Perciò abbiamo dimostrato che $h^{(j)}$ è congruo a $(x_j - g_j)^{m_j}$ modulo $\mathfrak{m}'\mathbb{K}[x_j, \mathbf{x}']$, e quindi anche modulo $\mathfrak{m}'\mathbb{K}[\mathbf{x}]$; abbiamo quindi ottenuto la seconda proprietà del punto 3.

Concludiamo dunque dimostrando questi due fatti.

(1): Come sopra, sia $\mathbf{x}' = \{x_{j+1}, \dots, x_n\}$ e consideriamo l'ideale

$$L_j := \left(f_s \in \mathbb{K}[\mathbf{x}'] \mid \exists s < m_j, \exists f_0, \dots, f_{s-1} \in \mathbb{K}[\mathbf{x}'] : \sum_{i=0}^s f_i x_j^i \in I \right)_{\mathbb{K}[\mathbf{x}']}.$$

Abbiamo allora $I \cap \mathbb{K}[\mathbf{x}'] \subseteq L_j \subsetneq \mathbb{K}[\mathbf{x}']$.

La prima inclusione è chiaramente vera, in quanto per ogni $f_0 \in I \cap \mathbb{K}[\mathbf{x}]$ abbiamo $f_0 x_j^0 \in I$.

La seconda inclusione invece è stretta in quanto se 1 appartenesse a L_j allora esisterebbe un polinomio monico di grado $\bar{s} < m_j$ in x_j e coefficienti in $\mathbb{K}[\mathbf{x}']$ che appartiene ad I , il che è assurdo per la minimalità di G , in quanto il suo monomio di testa è una potenza di x_j non divisibile per $x_j^{m_j}$.

Osserviamo che $\mathfrak{m}'$ è un ideale massimale e quindi che $\sqrt{L_j} = \mathfrak{m}'$ poiché $I \cap \mathbb{K}[\mathbf{x}'] \subseteq L_j$. Dimostriamo quindi che ogni elemento di $G \cap \mathbb{K}[x_j, \mathbf{x}']$ diverso da $h^{(j)}$ si può scrivere come un polinomio in x_j e coefficienti in $\mathfrak{m}'$.

Dato un polinomio $p = \sum_{h=0}^s p_h x_j^h \in G \cap \mathbb{K}[x_j, \mathbf{x}'] \setminus \{h^{(j)}(x_j)\}$ con $p_h \in \mathbb{K}[\mathbf{x}']$, dimostriamo che i tutti i suoi coefficienti appartengono a L_j . Dal momento che G è la base di Gröbner ridotta, abbiamo che $s < m_j$ e questo implica per definizione che $p_s \in L_j$. Consideriamo la seguente successione di polinomi in $I \cap \mathbb{K}[x_j, \mathbf{x}']$

$$\begin{aligned} p^{(0)} &:= p, & p^{(1)} &:= x_j^{m_j-s} p^{(0)} - p_s^{(0)} h^{(j)}, \\ p^{(i)} &:= x_j p^{(i-1)} - p_{m_j-1}^{(i-1)} h_j^{(j)} & \text{per } i > 1. \end{aligned}$$

Si può osservare con semplici calcoli che per ogni $i \geq 0$ i polinomi $p^{(i)}$ hanno grado al più $m_j - 1$, pertanto il loro $(m_j - 1)$ -simo coefficiente appartiene ad L_j . Esplicitando $p_{m_j-1}^{(i)}$ osserviamo

$$p_{m_j-1}^{(1)} = p_{s-1}^{(0)} - p_s h_{m_j-1}^{(j)}, \quad p_{m_j-1}^{(i)} = p_{m_j-2}^{(i-1)} - p_{m_j-1}^{(i-1)} h_{m_j-1}^{(j)} \quad \text{per } i > 1.$$

Mettendo insieme le identità precedenti abbiamo

$$p_{s-1}^{(0)} + L_j = p_s^{(0)} h_{m_j-1}^{(j)} + L_j = L_j, \quad p_{m_j-2}^{(i)} + L_j = p_{m_j-1}^{(i-1)} h_{m_j-1}^{(j)} + L_j = L_j \quad \text{per } i > 0.$$

Si osserva però anche che per ogni indice ammissibile l abbiamo

$$p_l^{(1)} + L_j = p_{l-m_j+s}^{(0)} + L_j, \quad p_l^{(i-1)} + L_j = p_{l-1}^{(i-1)} + L_j \quad \text{per } i > 1$$

e quindi per ogni $0 \leq k \leq s$ vale la seguente catena di identità

$$p_{s-k}^{(0)} + L_j = p_{m_j-k}^{(1)} + L_j = \dots = p_{m_j-1}^{(k)} + L_j = L_j,$$

che è quanto volevamo.

- (2): Poiché π è surgettivo vale il seguente fatto $\pi(\sqrt{I + \ker \pi}) = \sqrt{\pi(I + \ker \pi)} = \sqrt{\pi(I)}$.
 Dato che $\ker \pi = \mathfrak{m}'\mathbb{K}[\mathbf{x}] = (\sqrt{I} \cap \mathbb{K}[\mathbf{x}'])_{\mathbb{K}[\mathbf{x}]}$, abbiamo

$$\sqrt{I + \ker \pi} = \sqrt{\sqrt{I} + \ker \pi} = \sqrt{\sqrt{I} + (\sqrt{I} \cap \mathbb{K}[\mathbf{x}'])_{\mathbb{K}[\mathbf{x}]}} = \sqrt{\sqrt{I}} = \sqrt{I}.$$

Pertanto $\pi(\sqrt{I}) = \sqrt{\pi(I)}$, da cui deduciamo

$$\begin{aligned} \sqrt{\pi(I)} \cap \mathbb{K}'[x_j] &= \pi((x_1 - g_1, \dots, x_{n-1} - g_{n-1}, g_n)) \cap \mathbb{K}'[x_j] = \\ &= (x_1 - \bar{g}_1, \dots, x_j - \bar{g}_j)_{\mathbb{K}'[x_1, \dots, x_j]} \cap \mathbb{K}'[x_j] = (x_j - \bar{g}_j)_{\mathbb{K}'[x_j]}. \end{aligned}$$

Possiamo quindi concludere che

$$\pi(I \cap \mathbb{K}[x_j, \mathbf{x}']) \cap \mathbb{K}'[x_j] = \pi(I) \cap \mathbb{K}'[x_j] = ((x_j - \bar{g}_j)^{l_j})_{\mathbb{K}'[x_j]}$$

per un certo $l_j \in \mathbb{Z}_+$. □

Basandoci sul Teorema 2.8, possiamo quindi definire il seguente algoritmo.

Algoritmo 2.9 — TestPrimario(I)

Input: Un ideale $I = (f_1, \dots, f_k) \subsetneq \mathbb{K}[\mathbf{x}]$ 0-dimensionale.

Output: $\sqrt{I}$ se I è un ideale primario in posizione generale, (0) altrimenti.

```

1:  $S \leftarrow$  base di Gröbner ridotta di  $I$  rispetto all'ordine lessicografico dato da
    $x_1 > \dots > x_n$ ;
2:  $g \leftarrow$  elemento con monomio di testa minimale di  $S$ ;
3: Fattorizzo  $g$ :
4:  $g_1^{\nu_1} \dots g_s^{\nu_s} = g$ ;
5: if  $s = 1$  then
6:    $\mathfrak{p} \leftarrow (g_s)$ ;
7: else
8:   return (0);
9: if  $n = 1$  then
10:  return  $\mathfrak{p}$ ;
11: for  $i = n, \dots, 2$  do
12:   $f \leftarrow$  elemento di  $S$  con  $\text{lm}(f) = x_i^m$  con  $m$  intero positivo;
13:   $b \leftarrow$  il coefficiente del monomio  $x_i^{m-1}$  di  $f$  visto come polinomio in  $x_i$ ;
14:   $q \leftarrow x_i - \frac{b}{m}$ ;
15:  if  $q^m \equiv f \pmod{\mathfrak{p}}$  then
16:     $\mathfrak{p} \leftarrow \mathfrak{p} + (q)$ ;
17:  else
18:    return (0);
19: return  $\mathfrak{p}$ ;
```

Lo scheletro dell'algoritmo può essere diviso in tre passi:

- righe 1-4 prendiamo la base di Gröbner ridotta G di I e ne estraiamo l'elemento con monomio di testa minimale g rispetto all'ordinamento lessicografico, poi lo fattorizziamo;
- righe 5-8 verifichiamo che $G \cap \mathbb{K}[x_n] = \{g\}$ sia la potenza di un polinomio irriducibile, e in caso aggiungo il suo fattore irriducibile ai generatori del radicale di I ;

righe 9-18 otteniamo che i polinomi $x_j - g_j$ abbiano una potenza congruente ad un elemento di $G \cap \mathbb{K}[x_j, \mathbf{x}']$ modulo $(g_n, x_{n-1} - g_{n-1}, \dots, x_{j+1} - g_{j+1})$ seguendo la costruzione della dimostrazione di $1. \Rightarrow 3.$ della proposizione precedente. In particolare, dato $h^{(j)}$ definito come in tale dimostrazione che ha monomio di testa $\text{LM}(h^{(j)}) = x_j^{m_j}$, abbiamo $\pi(h^{(j)}) = (x_j - \bar{g}_j)^{m_j}$. Sviluppando quest'ultima potenza notiamo che il coefficiente di $x_j^{m_j-1}$ in $\pi(h^{(j)})$ è $m_j \bar{g}_j$, pertanto possiamo ricavare g_j prendendo il coefficiente di $x_j^{m_j-1}$ di $h^{(j)}$ visto come polinomio a coefficienti in $\mathbb{K}[\mathbf{x}']$ e dividendolo per m_j .

L'Algoritmo 2.9 funziona correttamente, infatti

- I è primario ed in posizione generale se e soltanto se vale l'enunciato 3. del Teorema 2.8; l'esistenza di un polinomio $g_n \in \mathbb{K}[x_n]$ irriducibile tale che $g_n^{\nu_n} \in G$ viene testato alle righe 5 – 8; l'esistenza di polinomi irriducibili $g_1, \dots, g_{n-1} \in \mathbb{K}[x_n]$ tali che per ogni $j = 1, \dots, n-1$ si ha che $(x_j - g_j)^{\nu_j}$ è congruente a un elemento in $G \cap \mathbb{K}[x_j, \dots, x_n]$ modulo l'ideale $(x_{j+1} - g_{j+1}, \dots, x_{n-1} - g_{n-1}, g_n) \subseteq \mathbb{K}[\mathbf{x}]$ viene testato nelle righe 9 – 18;
- se I è primario ed in posizione generale si ha che il suo radicale è $(g_n, x_{n-1} - g_{n-1}, \dots, x_1 - g_1)$; dato che il termine q aggiunto alla riga 16 ai generatori del radicale all' i -esima iterazione del ciclo for è $x_i - g_i$, per quanto sopra, al termine dell'esecuzione viene quindi restituito il radicale dell'ideale.

In conclusione, possiamo riassumere tutti i precedenti risultati in un unico algoritmo per calcolare la decomposizione primaria minimale di un qualsiasi ideale di dimensione 0 in un anello polinomiale $\mathbb{K}[\mathbf{x}]$ con $\mathbb{K}$ campo di caratteristica 0.

Algoritmo 2.10 — DecomposizioneZeroDimensionale(I)

Input: Un ideale 0-dimensionale $I = (f_1, \dots, f_k) \subsetneq \mathbb{K}[\mathbf{x}]$.

Output: Un insieme di coppie di ideali $(\mathbf{q}_i, \mathbf{p}_i)$ in cui i $\mathbf{q}_i$ sono le componenti di della decomposizione primaria minimale di I e i $\mathbf{p}_i$ sono i relativi primi associati.

```

1:  $DecPrim \leftarrow \emptyset$ ;
2:  $a \leftarrow$  elemento di  $\mathbb{K}^{n-1}$  preso in maniera casuale;
3:  $\phi_a \leftarrow$  cambio di coordinate come definito nello Shape Lemma;
4:  $I' \leftarrow \phi_a(I)$ ;
5:  $G \leftarrow$  base di Gröbner ridotta di  $I'$  rispetto all'ordine lessicografico dato da
    $x_1 > \dots > x_n$ ;
6:  $g \leftarrow$  elemento con monomio di testa minimo di  $G$ ;
7: Fattorizzo  $g$ ;
8:  $g_1^{\nu_1} \dots g_n^{\nu_n} = g$ ;
9: for  $i = 1, \dots, s$  do
10:    $\mathbf{q}'_i \leftarrow (I', g_i^{\nu_i})$ ;
11:    $\mathbf{q}_i \leftarrow (I, \phi_a^{-1}(g_i^{\nu_i}))$ ;
12:    $\mathbf{p}'_i \leftarrow \text{TestPrimario}(\mathbf{q}'_i)$ ;
13:   if  $\mathbf{p}'_i \neq (0)$  then
14:      $\mathbf{p}_i \leftarrow \phi_a^{-1}(\mathbf{p}'_i)$ ;
15:      $DecPrim \leftarrow DecPrim \cup \{(\mathbf{q}_i, \mathbf{p}_i)\}$ ;
16:   else
```

```

17:       $DecPrim \leftarrow DecPrim \cup \text{DecomposizioneZeroDimensionale}(\mathbf{q}_i);$ 
18: return  $DecPrim$ ;

```

L'algoritmo esegue i seguenti passi:

- righe 1-4 effettua il cambio di coordinate definito nello Shape Lemma all'ideale I ;
- righe 5-8 calcola il generatore g dell' $(n-1)$ -simo ideale di eliminazione di I ;
- righe 10-12 per ogni g_i fattore irriducibile di g calcola ognuno degli ideali della decomposizione del Teorema 2.6 e verifica che sono primari;
- righe 13-17 se l'ideale ottenuto nelle righe precedenti era primario lo aggiunge alla decomposizione, altrimenti ne calcola ricorsivamente la decomposizione primaria.

L'Algoritmo 2.10 non è certo che termini, in quanto potrebbe accadere che ad ogni chiamata dell'algoritmo un ideale I venga traslato in un ideale $\phi_a(I)$ che non è in posizione generale. Tuttavia, per lo Shape Lemma sappiamo che l'insieme di parametri a per cui $\phi_a(I)$ non è in posizione generale è un chiuso di Zariski, perciò risulta improbabile.

Esso restituisce una decomposizione primaria minimale, ammettendo che gli ideali $\phi_a(I)$ sia in posizione generale, gli ideali primari calcolati corrispondono a quelli dell'enunciato del Teorema 2.6.

§2.2 Il caso generale

È possibile usare l'Algoritmo DecomposizioneZeroDimensionale come parte di una strategia per calcolare la decomposizione primaria di un ideale con dimensione positiva. Nella trattazione del caso generale useremo la nozione di *insieme di variabili indipendente* e l'estensione di un ideale $I \subseteq \mathbb{K}[\mathbf{x}]$ all'anello $\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]$ con $\mathbf{u}$ sottoinsieme di variabili indipendente massimale di $\mathbf{x}$.

Definizione 2.11. Sia $I \subsetneq \mathbb{K}[\mathbf{x}]$. Un sottoinsieme di variabili $\mathbf{u} \subseteq \mathbf{x}$ si dice *indipendente* rispetto a I se $I \cap \mathbb{K}[\mathbf{u}] = 0$. Un insieme di variabili indipendente $\mathbf{u} \subseteq \mathbf{x}$ rispetto a I si dice *massimale* se $\dim(I) = \#\mathbf{u}$.

Osservazione 2.12. Un insieme indipendente $\mathbf{u} \subseteq \mathbf{x}$ massimale rispetto ad un ideale I è effettivamente massimale rispetto all'ordinamento indotto dall'inclusione, in quanto non può essere esteso per il Teorema 1.4.5.

Un'altra applicazione del Teorema 1.4.5 mostra che esiste sempre un insieme di variabili indipendente $\mathbf{u} \subseteq \mathbf{x}$ massimale rispetto ad un qualsiasi ideale $I \subsetneq \mathbb{K}[\mathbf{x}]$. Per costruirne esplicitamente uno, potremmo ad esempio verificare l'indipendenza di tutti i sottoinsiemi di variabili di $\mathbf{u} \subseteq \mathbf{x}$ ed estrarne uno massimale tra quelli per cui vale la proprietà $I \cap \mathbb{K}[\mathbf{u}] = 0$; tale algoritmo è tuttavia computazionalmente inefficiente in quanto richiede il calcolo di $O(2^n)$ intersezioni di ideali, e risulta quindi non adatto alla nostra trattazione. Mostriamo perciò alcuni risultati nella direzione di un algoritmo con complessità inferiore.

Osserviamo intanto che è possibile ricondurre il calcolo di un insieme di variabili indipendente massimale al caso degli ideali monomiali.

Osservazione 2.13. Sia $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale e sia $>$ un ordinamento monomiale. Sia $\mathbf{u} \subseteq \mathbf{x}$ un insieme di variabili indipendente rispetto a $\text{Lt}(I)$. Allora $\mathbf{u}$ è un insieme di variabili indipendente anche rispetto ad I . Se per assurdo non fosse così, esisterebbe un polinomio non nullo $p \in I \cap \mathbb{K}[\mathbf{u}]$, e di conseguenza $0 \neq \text{lt}(p) \in \text{Lt}(I) \cap \mathbb{K}[\mathbf{u}]$. Inoltre, un insieme di

variabili indipendente massimale rispetto a $\text{Lt}(I)$ è un insieme di variabili indipendente massimale anche rispetto ad I , in quanto per il Teorema 1.3 gli ideali I e $\text{Lt}(I)$ hanno la stessa dimensione.

Proposizione 2.14. Dato $I = (m_1, \dots, m_s) \subseteq \mathbb{K}[\mathbf{x}]$ un ideale monomiale, allora

$$\dim(\mathbb{K}[\mathbf{x}]/I) = \begin{cases} d(I, \mathbf{x}) & \text{se } I \neq 0 \text{ e } n > 0, \\ n & \text{altrimenti,} \end{cases}$$

con $d(I, \mathbf{x}) := \max \{ \dim(\mathbb{K}[\mathbf{x} \setminus \{x_i\}]/I_{x_i=0}) : x_i \mid m_1 \}$.

Dimostrazione. Osserviamo che se $I = 0$, la dimensione di $\mathbb{K}[\mathbf{x}]/I = \mathbb{K}[\mathbf{x}]$ è noto che sia n , e che se $n = 0$ la dimensione è nulla.

Sia dunque $I \neq 0$ e $n > 0$, e sia $\mathfrak{p}$ un primo minimale associato ad I . Poiché m_1 appartiene ad $I \subseteq \mathfrak{p}$, esiste una variabile $x_i \mid m_1$ che appartiene a $\mathfrak{p}$. Per questa ragione, $\mathfrak{p}$ si può scrivere come $\mathfrak{p} = (\mathfrak{p}, x_i) = (\mathfrak{p}_{x_i=0}, x_i)$. Poiché evidentemente $I_{x_i=0} \subseteq \mathfrak{p}_{x_i=0}$, si verifica la seguente disuguaglianza

$$\begin{aligned} \dim(\mathbb{K}[\mathbf{x} \setminus \{x_i\}]/I_{x_i=0}) &\geq \dim(\mathbb{K}[\mathbf{x} \setminus \{x_i\}]/\mathfrak{p}_{x_i=0}) \\ &= \dim(\mathbb{K}[\mathbf{x}]/(\mathfrak{p}_{x_i=0}, x_i)) \\ &= \dim(\mathbb{K}[\mathbf{x}]/\mathfrak{p}). \end{aligned}$$

Abbiamo quindi mostrato che

$$d(I, \mathbf{x}) \geq \max_{\mathfrak{p} \in \min \text{Ass}(I)} \{ \dim(\mathbb{K}[\mathbf{x}]/\mathfrak{p}) \} = \dim(\mathbb{K}[\mathbf{x}]/I).$$

Supponiamo per assurdo che la disuguaglianza sia stretta. Allora esiste un $x_j \mid m_1$ tale che

$$\dim(\mathbb{K}[\mathbf{x} \setminus \{x_j\}]/I_{x_j=0}) > \dim(\mathbb{K}[\mathbf{x}]/I),$$

e questo contraddice il fatto che

$$\dim(\mathbb{K}[\mathbf{x} \setminus \{x_j\}]/I_{x_j=0}) = \dim(\mathbb{K}[\mathbf{x}]/(I, x_j)) \leq \dim(\mathbb{K}[\mathbf{x}]/I). \quad \square$$

La proposizione precedente fornisce una formula ricorsiva per il calcolo della dimensione di un ideale monomiale. Questo risultato, assieme all'Osservazione 2.13, può essere usato per costruire un algoritmo che restituisce un insieme di variabili indipendente massimale.

Algoritmo 2.15 — $\text{InsiemeMassimale}(I, \mathbf{x} = \{x_1, \dots, x_n\})$

Input: Un ideale $I = (f_1, \dots, f_k) \subseteq \mathbb{K}[\mathbf{x}]$ e un insieme di variabili $\mathbf{x}$ dotato di un certo ordinamento $<$.

Output: Un insieme $\mathbf{u} \subseteq \mathbf{x}$ indipendente rispetto ad I massimale.

- 1: $f_1', \dots, f_{k'}' \leftarrow f_1, \dots, f_k$ tranne i generatori nulli;
- 2: $\mathbf{u} \leftarrow \emptyset$;
- 3: **if** $k' = 0 \vee \#\mathbf{x} = 0$ **then**
- 4: **return** $\mathbf{x}$;
- 5: **for** $j = 1, \dots, n$ **do**
- 6: **if** $x_j \mid \text{lt}(f_1')$ **then**
- 7: $\mathbf{v} \leftarrow \text{InsiemeMassimale}(I_{|x_j=0}, \mathbf{x} \setminus \{x_j\})$;
- 8: **if** $\#\mathbf{v} > \#\mathbf{u}$ **then**
- 9: $\mathbf{u} \leftarrow \mathbf{v}$;

10: **return** $\mathbf{u}$;

Notiamo che nell'algoritmo che abbiamo descritto stiamo trovando ricorsivamente un insieme massimale di $\text{Lt}(I)$: se x_j divide $\text{lt}(f'_1)$, sicuramente non apparterrà a nessun insieme di variabili indipendente rispetto a $\text{Lt}(I)$; l'insieme di variabili indipendente massimale va quindi ricercato in $\mathbf{x} \setminus \{x_j\}$.

Il motivo per cui ci interessano gli insiemi di variabili indipendenti massimali è il seguente: come vedremo tra poco, dato un insieme di variabili indipendente massimale rispetto ad I , l'ideale $I\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]$ è 0-dimensionale.

D'ora in poi, dopo aver fissato un insieme di variabili $\mathbf{u}$ indipendente massimale rispetto a I , per ogni $J \subsetneq \mathbb{K}[\mathbf{x}]$, $L \subsetneq \mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]$ ideali propri definiamo rispettivamente I^e e J^e come l'estensione di I e la contrazione di J rispetto all'immersione canonica $i : \mathbb{K}[\mathbf{x}] \hookrightarrow \mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]$.

Osservazione 2.16. Per ogni $\mathbf{u} \subseteq \mathbf{x}$ sottoinsieme di variabili e per ogni polinomio non nullo $f \in \mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]$, esiste un polinomio $\alpha \in \mathbb{K}[\mathbf{u}]$ tale che $\alpha f \in \mathbb{K}[\mathbf{x}]$. Possiamo ad esempio prendere come α il minimo comune multiplo dei denominatori dei monomi di f .

Sia $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale, e sia $I^e = \bigcap_{i=1}^r \mathfrak{q}_i^e$ una decomposizione primaria minimale, l'insieme dei primari contratti $\mathfrak{q}_i^e$ è la decomposizione primaria minimale di un ideale saturato $I : (h)^\infty = I : (h)$ per un certo $h \in \mathbb{K}[\mathbf{x}] \setminus I$. Per lo Splitting Tool possiamo riscrivere l'ideale I come $I = I : (h) \cap (I, h)$, e riapplicando ricorsivamente l'algoritmo a (I, h) vedremo che si ottiene una decomposizione primaria I .

Procediamo a dimostrare un lemma preliminare per poi proseguire con l'ultimo risultato teorico necessario per completare l'algoritmo.

Lemma 2.17. Siano $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale e $I = \bigcap_{i=1}^r \mathfrak{q}_i$ una sua decomposizione primaria minimale. Sia $\mathbf{u} \subseteq \mathbf{x}$ un sottoinsieme di variabili indipendente rispetto ad I . Se esiste un s intero tale che $\mathfrak{q}_i \cap \mathbb{K}[\mathbf{u}] = (0)$ per $i = 1, \dots, s$ e $\mathfrak{q}_i \cap \mathbb{K}[\mathbf{u}] \neq (0)$ per $i = s+1, \dots, r$ allora

$$I^e = \bigcap_{i=1}^s \mathfrak{q}_i^e \text{ è una decomposizione primaria minimale.}$$

Dimostrazione. Poiché per $i = s+1, \dots, r$ si ha $I\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}] = (\mathbb{K}[\mathbf{u}] \setminus \{0\})^{-1}I$ e $\mathfrak{q}_i \cap \mathbb{K}[\mathbf{u}] \neq (0)$, per il Teorema 1.8.1 otteniamo la seguente decomposizione primaria di I^e

$$I^e = \bigcap_{i=1}^s \mathfrak{q}_i^e.$$

Dimostriamo che tale decomposizione è minimale.

Fissati due indici distinti $i, j \leq s$, mostriamo che $\sqrt{\mathfrak{q}_i^e} \neq \sqrt{\mathfrak{q}_j^e}$. Ipotizziamo per assurdo il contrario, e prendiamo un polinomio non nullo $f \in \sqrt{\mathfrak{q}_i^e} \subseteq \sqrt{\mathfrak{q}_i^e} = \sqrt{\mathfrak{q}_j^e}$. Per l'Osservazione 2.16, sappiamo che esiste un polinomio non nullo $\alpha \in \mathbb{K}[\mathbf{u}]$ per cui $\alpha f \in \mathbb{K}[\mathbf{x}]$, di conseguenza $\alpha f \in \sqrt{\mathfrak{q}_j^e} \cap \mathbb{K}[\mathbf{x}] = \sqrt{\mathfrak{q}_j^{ec}} = \sqrt{\mathfrak{q}_j}$. Ipotizziamo per assurdo che $f \notin \sqrt{\mathfrak{q}_j}$. Per primalità di $\sqrt{\mathfrak{q}_j}$ allora abbiamo che esiste un intero n tale che $\alpha^n \in \mathfrak{q}_j$, ma ciò è assurdo in quanto $\alpha \in \mathbb{K}[\mathbf{u}]$ e $\mathfrak{q}_j \cap \mathbb{K}[\mathbf{u}] = (0)$. Pertanto abbiamo che $\sqrt{\mathfrak{q}_i} \subseteq \sqrt{\mathfrak{q}_j}$. Analogamente, si dimostra anche l'inclusione opposta, e quindi $\sqrt{\mathfrak{q}_i} = \sqrt{\mathfrak{q}_j}$ che è assurdo.

Mostriamo infine che nessun ideale $\mathfrak{q}_i^e$ può essere omesso dalla decomposizione. Dato che la decomposizione di I è minimale, esiste un polinomio non nullo $f \in (\bigcap_{j \neq i, j \leq s} \mathfrak{q}_j) \setminus \mathfrak{q}_i \subseteq (\bigcap_{j \neq i, j \leq s} \mathfrak{q}_j^e) \setminus \mathfrak{q}_i$.

Ipotizziamo per assurdo che $f \in \mathfrak{q}_i^e$. Esiste di conseguenza un polinomio non nullo $\alpha \in \mathbb{K}[\mathbf{u}]$ tale che $\alpha f \in \mathfrak{q}_i$. Questo è assurdo in quanto $f \notin \mathfrak{q}_i$ per cui $\alpha \in \sqrt{\mathfrak{q}_i}$. Essendo $\mathbf{u}$ indipendente rispetto a $\mathfrak{q}_i$, abbiamo $\alpha \in \sqrt{\mathfrak{q}_i} \cap \mathbb{K}[\mathbf{u}] = 0$. Di conseguenza $f \in \left(\bigcap_{j \neq i, j \leq s} \mathfrak{q}_j^e \right) \setminus \mathfrak{q}_i^e$ e perciò $\mathfrak{q}_i^e$ non è ridondante. $\square$

Ricordiamo che un ideale proprio I di un anello noetheriano si dice *equidimensionale* se ogni suo primo associato $\mathfrak{p}$ è tale che $\dim(\mathfrak{p}) = \dim(I)$.

Teorema 2.18

Sia $I \subseteq \mathbb{K}[\mathbf{x}]$ un ideale $\mathbf{u} \subseteq \mathbf{x}$ un insieme di variabili indipendente massimale rispetto ad I .

1. $I^e \subseteq \mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]$ è un ideale 0-dimensionale;
2. Sia $G' := \{g'_1, \dots, g'_s\} \subseteq \mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]$ la base di Gröbner ridotta di I^e . Prendiamo $G := \{g_1, \dots, g_s\} \subseteq \mathbb{K}[\mathbf{x}]$ la base di Gröbner di I^e ottenuta moltiplicando ogni g'_i per il minimo comune multiplo dei denominatori dei suoi coefficienti. Sia $h := \text{lcm}(\text{lc}(g_1), \dots, \text{lc}(g_s)) \in \mathbb{K}[\mathbf{u}]$, allora

$$I^{ec} = I : (h^\infty).$$

3. L'ideale $I : (h^\infty)$ è un ideale equidimensionale di dimensione $\dim(I)$;
4. Sia $I^e = \mathfrak{q}_1 \cap \dots \cap \mathfrak{q}_s$ una decomposizione primaria minimale, allora anche $I^{ec} = \mathfrak{q}_1^c \cap \dots \cap \mathfrak{q}_s^c$ è una decomposizione primaria minimale.

Dimostrazione. 1. È una conseguenza diretta della definizione di $\mathbf{u}$ e del Teorema 1.4.5.

2. Per dimostrare questo fatto osserviamo che valgono entrambe le inclusioni.

Prendiamo un elemento $a \in I : (h^\infty)$, per definizione sappiamo che esiste un naturale k per cui $ah^k \in I$. Questo implica che $a \in I\mathbb{K}(\mathbf{u})$ e quindi $a \in I^e$. Quindi vale $I : (h^\infty) \subseteq I^{ec}$.

Prendiamo un elemento $f \in I^{ec}$. Poiché $f \in I^e$, se prendiamo il resto della divisione per G' del polinomio f otteniamo 0, di conseguenza possiamo scrivere f come combinazione lineare degli elementi della base di Gröbner, in particolare esistono $\xi_i \in \mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]$ per cui $f = \sum_{i=1}^s \xi_i g_i$. Poiché $g_i \in \mathbb{K}[\mathbf{x}]$ per ogni i e nel processo di divisione per G' al più stiamo dividendo per i termini di testa della base, sappiamo che $\xi_i \in \mathbb{K}[\mathbf{x}]_h$. Questo ha come conseguenza che esiste un intero N tale che $h^N f \in I$. Abbiamo quindi provato che $f \in I : (h^N) \subseteq I : (h^\infty)$, dunque $I^{ec} \subseteq I : (h^\infty)$.

3. Data una decomposizione primaria minimale $I = \bigcap_{i=1}^r \mathfrak{q}_i$, supponiamo senza perdita di generalità che $\mathfrak{q}_i \cap \mathbb{K}[\mathbf{u}] = (0)$ per $i = 1, \dots, s$ e $\mathfrak{q}_i \cap \mathbb{K}[\mathbf{u}] \neq (0)$ per $i = s+1, \dots, r$.

Come conseguenza del Lemma 2.17, $I^e = \bigcap_{i=1}^s \mathfrak{q}_i^e$ è una decomposizione primaria minimale.

Poiché $\mathbf{u}$ è un sottoinsieme di variabili indipendente rispetto a tutti i $\mathfrak{q}_i$ con $i = 1, \dots, s$, lo è anche per $\mathfrak{q}_i^e$, e inoltre anche per $\mathfrak{q}_i^{ec}$ e per $\sqrt{\mathfrak{q}_i^{ec}}$. Per il Teorema 1.8.1 sappiamo che per $i = 1, \dots, s$ abbiamo $\mathfrak{q}_i^{ec} = \mathfrak{q}_i$.

Per il Teorema 1.4.5, sappiamo anche che la dimensione dei primi associati di I^{ec} è maggiore o uguale a $\#\mathbf{u} = \dim(I) \geq \dim(I^{ec})$, e visto che i primi associati ad un

ideale hanno dimensione sempre minore o uguale a quella dell'ideale stesso, per ogni $i = 1, \dots, s$ abbiamo $\dim(\sqrt{\mathfrak{q}_i^{ec}}) = \dim(I)$ per $i = 1, \dots, s$.

4. È una conseguenza diretta del Teorema 1.8.2. $\square$

Possiamo applicare quanto dimostrato nel precedente teorema per costruire due algoritmi. Il primo ci riporta al caso 0-dimensionale, il secondo è quello finale che utilizza tutti i risultati visti finora per calcolare la decomposizione primaria di un qualsiasi ideale.

Algoritmo 2.19 — RiduzioneZeroDimensionale(I)

Input: Un ideale $I = (f_1, \dots, f_k) \subseteq \mathbb{K}[\mathbf{x}]$.

Output: Se I ha dimensione positiva, restituisce la terna $(\mathbf{u}, G, h)$ in cui $\mathbf{u} \subseteq \mathbf{x}$ è un sottoinsieme di variabili indipendente massimale, $G \subseteq \mathbb{K}[\mathbf{x}]$ è la base di Gröbner ridotta di $I\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]$ a meno di moltiplicazione di ogni elemento per scalari. Infine, $h \in \mathbb{K}[\mathbf{u}]$ è il polinomio tale che $I\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}] = I : (h) = I : (h^\infty)$. Se I ha dimensione nulla, restituisce $(\emptyset, \emptyset, 0)$.

```

1:  $\mathbf{u} \leftarrow \text{InsiemeMassimale}(I, \mathbf{x});$ 
2: if  $\#\mathbf{u} = 0$  then
3:   return  $(\emptyset, \emptyset, 0);$ 
4:  $G = \{g_1, \dots, g_s\} \leftarrow$  base di Gröbner di  $I$  relativa ad un ordine lessicografico in cui  $\mathbf{x} \setminus \mathbf{u} > \mathbf{u};$ 
5:  $h \leftarrow \prod_{i=1}^s \text{lc}(g_i)$  con i  $g_i$  visti come polinomi a coefficienti in  $\mathbb{K}(\mathbf{u})$  nelle variabili  $\mathbf{x} \setminus \mathbf{u};$ 
6: Calcolo la saturazione di  $I$  rispetto a  $(h)$ :
7:  $I_0 := I;$ 
8:  $I_1 \leftarrow I_0 : (h);$ 
9:  $m \leftarrow 1;$ 
10: while  $I_m \not\subseteq I_{m-1}$  do
11:    $m \leftarrow m + 1;$ 
12:    $I_m \leftarrow I_{m-1} : (h);$ 
13: return  $(\mathbf{u}, \{g_1, \dots, g_s\}, h^m);$ 
```

Algoritmo 2.20 — DecomposizionePrimaria(I)

Input: Un ideale $I = (f_1, \dots, f_k) \subseteq \mathbb{K}[\mathbf{x}]$.

Output: Se I non è l'intero anello restituisce un insieme di coppie di ideali $(\mathfrak{q}_i, \mathfrak{p}_i)$ in cui $\mathfrak{q}_i$ sono gli ideali primari della decomposizione primaria di I e i $\mathfrak{p}_i$ sono i relativi primi associati. Se $I = \mathbb{K}[\mathbf{x}]$ invece restituisce l'insieme vuoto.

```

1: if  $1 \in I$  then
2:   return  $\emptyset;$ 
3:  $(\mathbf{u}, G, h) \leftarrow \text{RiduzioneZeroDimensionale}(I);$ 
4: if  $\#\mathbf{u} = 0$  then
5:   return  $\text{DecomposizioneZeroDim}(I);$ 
6:  $\text{primariEstesi} \leftarrow \text{DecomposizioneZeroDim}((G)_{\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]});$ 
7:  $\text{primari} \leftarrow \{(\mathfrak{q}_i \cap \mathbb{K}[\mathbf{x}], \mathfrak{p}_i \cap \mathbb{K}[\mathbf{x}]) \mid (\mathfrak{q}_i, \mathfrak{p}_i) \in \text{primariEstesi}\};$ 
8:  $\text{primari} \leftarrow \text{primari} \cup \text{DecomposizionePrimaria}((I, h));$ 
9: return  $\text{primari};$ 
```

Entrambi gli algoritmi funzionano in quanto seguono le costruzioni ottenute nelle dimostrazioni dei teoremi di questa sezione. Ricordiamo comunque che tutte le operazioni che abbiamo individuato su ideali sono calcolabili. Vanno fatte però alcune precisazioni su `DecomposizionePrimaria`, esso infatti:

- **termina:** poiché ad ogni passo ottengo tramite `RiduzioneZeroDimensionale` un polinomio $h \in \mathbb{K}[\mathbf{u}]$ con $\mathbf{u}$ indipendente rispetto a I , ho che $h \notin I$; non potendo costruire una catena ascendente infinita di ideali del tipo $I \subsetneq (I, h_1) \subsetneq (I, h_1, h_2) \subsetneq \dots$ visto che $\mathbb{K}[\mathbf{x}]$ è noetheriano, l'algoritmo può essere richiamato soltanto un numero finito di volte, finché non raggiungo il caso $I = \mathbb{K}[\mathbf{x}]$;
- **è corretto:** poiché segue la costruzione del Teorema precedente, nella riga 6 otteniamo la decomposizione primaria minimale dell'ideale $I : (h)$, mentre alla riga 7 uniamo tali componenti primarie a quelle di (I, h) ; per lo `Splitting Tool` sappiamo che $I = I : (h) \cap (I, h)$, quindi abbiamo ottenuto una decomposizione primaria per I , anche se non necessariamente minimale.

Notiamo che, a differenza dell'algoritmo di decomposizione primaria per ideali 0-dimensionali, non abbiamo garanzie sulla minimalità della decomposizione.

3 L'algoritmo SY

Un ulteriore algoritmo per il calcolo della decomposizione primaria di ideali polinomiali a coefficienti in un campo di caratteristica 0 è l'algoritmo SY. Esso è stato introdotto nel 1996 da Takeshi Shimoyama e Kazuhiro Yokoyama in [12], servendosi della teoria già sviluppata per l'algoritmo GTZ, allo scopo di ottimizzare il calcolo della decomposizione primaria degli ideali con un elevato numero di primi associati non minimali. Come osservato in [3], nelle implementazioni presenti nei sistemi di algebra computazionale, questa caratteristica può comportare un guadagno notevole, sebbene non sia sempre garantito.

L'algoritmo SY è strutturato nel seguente modo:

- calcola i primi minimali dell'ideale, usando uno tra gli algoritmi noti in letteratura che lo permettono, come ad esempio [8];
- calcola una decomposizione dell'ideale chiamata *decomposizione pseudo-primaria*, più rapida da calcolare rispetto ad una decomposizione primaria;
- ricava da essa alcune componenti primarie tramite una tecnica chiamata *estrazione*;
- ricava le eventuali componenti primarie mancanti applicando ricorsivamente l'algoritmo su ideali di dimensione inferiore a quello di partenza.

Nella prima sezione del capitolo descriveremo nel dettaglio ognuno di questi passi, eccetto il primo, poiché esiste una vasta letteratura a riguardo.

Nella seconda sezione del capitolo, discuteremo alcuni criteri di ridondanza di componenti primarie, che ci consentiranno di apportare delle modifiche all'algoritmo SY, riducendo il numero di componenti primarie ridondanti calcolate e restituendo infine una decomposizione primaria minimale. Inizieremo dimostrando un criterio generale applicabile anche ad altri algoritmi, tra cui l'algoritmo GTZ; successivamente, mostreremo un criterio più specifico per l'algoritmo SY che ci permetterà di ottimizzarlo.

§3.1 Decomposizione primaria

Come già osservato, alla base di questo algoritmo vi sono due elementi: il calcolo della *decomposizione pseudo-primaria* di un ideale, e il calcolo dell'*estrazione* di un ideale primario. Qui di seguito li trattiamo nel dettaglio, mostrandone i relativi algoritmi e dimostrando i risultati teorici che vi stanno a fondamento; nell'ultima parte di questa sezione mostriamo in che modo è possibile comporre queste due procedure per ottenere un algoritmo che, dato un ideale proprio in input, ne produce una decomposizione primaria.

§3.1.1 Decomposizione pseudo-primaria

Definiamo innanzitutto cos'è un ideale pseudo-primario.

Definizione 3.1. Un ideale $J \subsetneq \mathbb{K}[x]$ si dice *pseudo-primario* se e soltanto se $\sqrt{J}$ è un ideale primo.

Prima di introdurre la definizione di decomposizione pseudo-primaria, descriviamo le caratteristiche essenziali del tipo di decomposizione che vogliamo ottenere: vogliamo poter

scrivere un qualsiasi ideale $I \subsetneq \mathbb{K}[\mathbf{x}]$ come intersezione finita di ideali pseudo-primari e di un eventuale ideale di dimensione strettamente minore. Dimostriamo intanto una prima proposizione.

Definizione 3.2. Sia $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale con $\min\text{Ass}(I) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$. Un insieme finito S_i si dice *separatore* di I rispetto a $\mathfrak{p}_i$ se

$$S_i \cap \mathfrak{p}_i = \emptyset, \quad S_i \cap \mathfrak{p}_j \neq \emptyset \text{ per } i \neq j$$

Chiamiamo invece *sistema di separatori* di I un insieme $\{S_1, \dots, S_r\}$ in cui per ogni $i = 1, \dots, r$ l'insieme S_i è separatore rispetto a $\mathfrak{p}_i$.

Proposizione 3.3. Sia $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale con $\min\text{Ass}(I) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$. Sia inoltre $I = \cap_{i=1}^l \mathfrak{q}_i$ una decomposizione primaria minimale di I . Se esiste un sistema di separatori $\{S_1, \dots, S_r\}$ di I allora per ogni $i = 1, \dots, r$

1. $\bigcap_{\sqrt{\mathfrak{q}_i} \cap S_i = \emptyset} \mathfrak{q}_i$ è una decomposizione primaria minimale di $I\mathbb{K}[\mathbf{x}]_{S_i} \cap \mathbb{K}[\mathbf{x}]$;
2. $I\mathbb{K}[\mathbf{x}]_{S_i} \cap \mathbb{K}[\mathbf{x}]$ è un ideale pseudo-primario con radicale $\mathfrak{p}_i$.

Dimostrazione. Per il Teorema 1.8.2, abbiamo la seguente decomposizione

$$I\mathbb{K}[\mathbf{x}]_{S_i} \cap \mathbb{K}[\mathbf{x}] = \bigcap_{\sqrt{\mathfrak{q}_i} \cap S_i = \emptyset} \mathfrak{q}_i.$$

Dalla minimalità della decomposizione di I discende subito anche la minimalità di quest'ultima. Abbiamo quindi mostrato l'enunciato 1.

Per dimostrare l'enunciato 2., osserviamo che tutte le componenti primarie $\mathfrak{q}$ di I per cui $\sqrt{\mathfrak{q}} \cap S_i = \emptyset$ sono tali che $\sqrt{\mathfrak{q}}$ non contiene nessuno tra i primi minimi $\mathfrak{p}_j$ con $j \neq i$. Dovendo contenere almeno un primo minimale, abbiamo $\mathfrak{p}_i \subseteq \sqrt{\mathfrak{q}}$. Perciò

$$\sqrt{I\mathbb{K}[\mathbf{x}]_{S_i} \cap \mathbb{K}[\mathbf{x}]} = \bigcap_{\substack{\sqrt{\mathfrak{q}_j} \cap S_i = \emptyset \\ \mathfrak{p}_i \subseteq \sqrt{\mathfrak{q}_j}}} \sqrt{\mathfrak{q}_j} = \mathfrak{p}_i. \quad \square$$

Osserviamo che esistono insiemi di separatori calcolabili per ogni ideale $I \subsetneq \mathbb{K}[\mathbf{x}]$. Sia $\min\text{Ass}(I) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ e, fissato un ordinamento monomiale arbitrario, indichiamo con G_i una base di Gröbner di $\mathfrak{p}_i$ per ogni $i = 1, \dots, r$. Per ogni $i \neq j$, esiste $t_{ij} \in G_i \setminus \mathfrak{p}_j$, pertanto possiamo costruire

$$S_i := \{t_{i1}, \dots, t_{ii-1}, t_{ii+1}, \dots, t_{ir}\} \text{ e } S'_i := \left\{ \prod_{j \neq i} t_{ij} \right\} \text{ per ogni } i = 1, \dots, r.$$

È immediato verificare che gli insiemi $\{S_1, \dots, S_r\}$ e $\{S'_1, \dots, S'_r\}$ sono insiemi di separatori di I .

Osserviamo che, per un qualsiasi sistema moltiplicativo generato da un insieme finito $S := \{s_1, \dots, s_r\}$, calcolare la localizzazione di un anello in nell'insieme moltiplicativo generato da S o in $s := \prod_{i=1}^r s_i$ è equivalente.

Inoltre, abbiamo la seguente conseguenza della Proposizione 3.3.

Corollario 3.4. Siano $I \subsetneq \mathbb{K}[\mathbf{x}]$, $\min\text{Ass}(I) = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ e $I = \bigcap_{i=1}^l \mathfrak{q}_i$ una decomposizione primaria minimale di I . Sia inoltre $\{S_1, \dots, S_r\}$ un sistema di separatori di I . Per ogni $i = 1, \dots, r$ definiamo

$$\mathcal{F}_i := \{\mathfrak{q}_i \mid \sqrt{\mathfrak{q}_i} \cap S_i = \emptyset\} \text{ e } \mathcal{P}_i := \{\sqrt{\mathfrak{q}} \mid \mathfrak{q} \in \mathcal{F}_i\}.$$

Allora $\{\mathcal{F}_1, \dots, \mathcal{F}_r\}$ e $\{\mathcal{P}_1, \dots, \mathcal{P}_r\}$ sono famiglie di insiemi a coppie disgiunti.

Dimostrazione. Sia $\mathfrak{q}$ una componente primaria di I che appartiene a $\mathcal{F}_i \cap \mathcal{F}_j$. Dato che $\sqrt{\mathfrak{q}} \cap S_i = \sqrt{\mathfrak{q}} \cap S_j = \emptyset$ si ha che $\sqrt{\mathfrak{q}}$ contiene i primi minimali $\mathfrak{p}_i$ e $\mathfrak{p}_j$. Tuttavia, se $i \neq j$, per definizione di sistema di separatori si ha anche che $\mathfrak{p}_i \cap S_j \neq \emptyset$ e $\mathfrak{p}_j \cap S_i \neq \emptyset$, che è assurdo. Pertanto, gli insiemi $\mathcal{F}_1, \dots, \mathcal{F}_r$ sono tutti a coppie disgiunti.

Dato che la decomposizione $I = \bigcap_{i=1}^l \mathfrak{q}_i$ è minimale, le sue componenti primarie hanno radicali distinti, e visto che gli insiemi $\mathcal{F}_1, \dots, \mathcal{F}_r \subseteq \{\mathfrak{q}_1, \dots, \mathfrak{q}_l\}$ sono a coppie disgiunti allora anche gli insiemi $\mathcal{P}_1, \dots, \mathcal{P}_r$ sono a coppie disgiunti dato che per ogni $i = 1, \dots, r$ abbiamo $\mathcal{P}_i = \text{Ass}(I\mathbb{K}[\mathbf{x}]_{S_i} \cap \mathbb{K}[\mathbf{x}])$ per la Proposizione 3.3.1. $\square$

Dimostriamo ora la validità della seguente decomposizione.

Teorema 3.5

Siano $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale, $\{S_1, \dots, S_r\}$ un sistema di separatori rispetto ad I e

$$\overline{\mathfrak{q}}_i := I\mathbb{K}[\mathbf{x}]_{S_i} \cap \mathbb{K}[\mathbf{x}] \text{ con } s_i = \prod_{s \in S_i} s.$$

Per ogni $i = 1, \dots, r$, sia k_i un intero tale che $I : (s_i^{k_i}) = \overline{\mathfrak{q}}_i$. Allora, posto $I' = (I, s_1^{k_1}, \dots, s_r^{k_r})$, si ha la seguente decomposizione

$$I = \bigcap_{i=1}^r \overline{\mathfrak{q}}_i \cap I'. \quad (3.1)$$

Inoltre, se $I' \neq \mathbb{K}[\mathbf{x}]$, vale $\dim(I') < \dim(I)$.

Dimostrazione. Supponendo che $s_j^{k_j} \in I : (s_i^{k_i})$ per $j \neq i$, l'identità (3.1) è una diretta conseguenza dello Splitting Tool. Per $r = 1$

$$I = I : (s_1^{k_1}) \cap (I, s_1^{k_1}) = \overline{\mathfrak{q}}_1 \cap I'.$$

Se $r > 1$, applicando più volte lo Splitting Tool abbiamo

$$\begin{aligned} I &= I : (s_1^{k_1}) \cap (I, s_1^{k_1}) \\ &= I : (s_1^{k_1}) \cap (I : (s_2^{k_2}) \cap (I, s_2^{k_2}), s_1^{k_1}) \\ &= I : (s_1^{k_1}) \cap I : (s_2^{k_2}) \cap (I, s_1^{k_1}, s_2^{k_2}) \\ &= \dots = \bigcap_{i=1}^r I : (s_1^{k_1}) \cap (I, s_1^{k_1}, \dots, s_r^{k_r}) = \bigcap_{i=1}^r \overline{\mathfrak{q}}_i \cap I'. \end{aligned}$$

Verifichiamo dunque che vale $s_j^{k_j} \in \overline{\mathfrak{q}}_i$ per $j \neq i$.

Sia $I = \bigcap_{i=1}^l \mathfrak{q}_i$ una decomposizione primaria minimale di I e sia

$$\overline{\mathfrak{q}}_i = \bigcap_{\sqrt{\mathfrak{q}_i} \cap S_i = \emptyset} \mathfrak{q}_i$$

la decomposizione primaria di $\bar{q}_i$ descritta nella Proposizione 3.3. Dimostriamo che $s_j^{k_j}$ appartiene ad ogni componente primaria di $\bar{q}_i$.

Ipotizziamo per assurdo che $s_j^{k_j} \notin \mathfrak{q}$ per qualche componente $\mathfrak{q}$ della decomposizione di $\bar{q}_i$, e consideriamo l'ideale $L_j := \mathfrak{q} : (s_j^{k_j})$. Osserviamo che, dal momento che $I \subseteq \mathfrak{q}$, si ha il contenimento $\bar{q}_j = I : (s_j^{k_j}) \subseteq L_j$.

Dato che $s_j^{k_j} \notin \mathfrak{q}$, per il Lemma 1.5 l'ideale L_j è $\sqrt{\mathfrak{q}}$ -primario. Tuttavia, $\sqrt{L_j} = \sqrt{\mathfrak{q}}$ contiene $\bar{q}_j$ che per definizione ha intersezione non banale con S_i . Questo è un assurdo in quanto, per come è stato scelto $\mathfrak{q}$, il suo radicale ha intersezione vuota con S_i .

Dimostriamo ora che se $I' \neq \mathbb{K}[\mathbf{x}]$ allora $\dim(I') < \dim(I)$.

Prendiamo un primo minimale $\mathfrak{p}'$ di I' . Poiché $\sqrt{I} \subseteq \sqrt{I'}$, esiste un primo $\mathfrak{p}_i$ contenuto in $\mathfrak{p}'$. Dal momento che $s_i \in I' \setminus \mathfrak{p}_i \subseteq \mathfrak{p}' \setminus \mathfrak{p}_i$ deduciamo che l'inclusione tra i due primi è stretta. Ne consegue quindi $\dim(\mathfrak{p}') < \dim(\mathfrak{p}_i) \leq \dim(I)$ per ogni primo minimale $\mathfrak{p}'$ di I' , e quindi concludiamo $\dim(I') < \dim(I)$. $\square$

Definizione 3.6. Una decomposizione di I come quella appena individuata nel Teorema 3.5 si chiama *decomposizione pseudo-primaria*. Ogni ideale $\bar{q}_i$ viene detto *componente pseudo-primaria* di I , mentre I' viene chiamata *componente restante* della decomposizione pseudo-primaria di I .

Riscrivendo in forma algoritmica gli ultimi enunciati, otteniamo il seguente algoritmo per il calcolo di una decomposizione pseudo-primaria di un ideale I .

Algoritmo 3.7 — DecomposizionePseudoPrimaria(I, minAss)

Input: Un ideale $I = (f_1, \dots, f_k) \subsetneq \mathbb{K}[\mathbf{x}]$ e il suo insieme di primi minimali minAss .

Output: Se $I = \mathbb{K}[\mathbf{x}]$ restituisce $(\emptyset, \mathbb{K}[\mathbf{x}])$. Se $I \neq \mathbb{K}[\mathbf{x}]$ restituisce una coppia $(\text{compPseudoPrimarie}, I')$ in cui il primo elemento $\text{compPseudoPrimarie}$ è l'insieme delle coppie $(\bar{q}_i, \mathfrak{p}_i)$ con $\bar{q}_i$ componenti pseudo-primarie di I e $\mathfrak{p}_i$ i relativi primi minimali; I' è la componente restante della decomposizione.

```

1: if  $1 \in I$  then
2:   return  $(\emptyset, \mathbb{K}[\mathbf{x}])$ ;
3: if  $\text{minAss} = \{\mathfrak{p}\}$  then
4:   return  $(\{(I, \mathfrak{p})\}, \mathbb{K}[\mathbf{x}])$ ;
5:  $\text{compPseudoPrimarie} \leftarrow \emptyset$ ,  $I' \leftarrow I$ ;
6: for  $\mathfrak{p} \in \text{minAss}$  do
7:    $S \leftarrow$  separatore di  $I$  rispetto a  $\mathfrak{p}$ ;
8:    $\text{compPseudoPrimarie} \leftarrow \{(I\mathbb{K}[\mathbf{x}]_S \cap \mathbb{K}[\mathbf{x}], \mathfrak{p})\}$ ;
9:    $s \leftarrow \prod_{t \in S} t$ ;
10:   $k \leftarrow$  intero tale che  $I : (s^k) = I\mathbb{K}[\mathbf{x}]_S \cap \mathbb{K}[\mathbf{x}]$ ;
11:   $I' \leftarrow I' + (s^k)$ ;
12: return  $(\text{compPseudoPrimarie}, I')$ ;
```

Osserviamo inoltre il seguente fatto, che useremo successivamente.

Corollario 3.8. Con la stessa notazione del Teorema 3.5, vale

$$\sqrt{I'} = \bigcap_{i=1}^r \sqrt{(\mathfrak{p}_i, s_i)}.$$

Dimostrazione. È sufficiente osservare

$$\begin{aligned}\sqrt{I'} &= \sqrt{(I, s_1^{k_1}, \dots, s_r^{k_r})} = \sqrt{(\sqrt{I}, s_1, \dots, s_r)} = \\ &= \sqrt{(\cap_{i=1}^r \mathfrak{p}_i, s_1, \dots, s_r)} = \sqrt{\cap_{i=1}^r (\mathfrak{p}_i, s_1, \dots, s_r)}.\end{aligned}$$

Poiché per ogni $j \neq i$ abbiamo $s_i \notin \mathfrak{p}_i$, $s_j \in \mathfrak{p}_i$ concludiamo

$$\sqrt{I'} = \sqrt{\cap_{i=1}^r (\mathfrak{p}_i, s_1, \dots, s_r)} = \bigcap_{i=1}^r \sqrt{(\mathfrak{p}_i, s_1)}.$$

□

§3.1.2 Estrazione

Conoscendo una decomposizione pseudo-primaria di un ideale, è desiderabile poter estrarre da essa informazioni su una decomposizione primaria dell'ideale.

Nella seguente proposizione mostriamo un metodo per calcolare la componente primaria associata all'unico primo minimale di un ideale pseudo-primario.

Proposizione 3.9. Sia $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale pseudo-primario tale che $\sqrt{I} = \mathfrak{p}$, e sia $\mathfrak{q}$ la componente primaria associata a $\mathfrak{p}$. Dato $\mathbf{u} \subseteq \mathbf{x}$ un insieme di variabili indipendente massimale rispetto a $\mathfrak{p}$, vale $\mathfrak{q} = I\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}] \cap \mathbb{K}[\mathbf{x}]$.

Dimostrazione. Dato un ideale $J \subsetneq \mathbb{K}[\mathbf{x}]$, osserviamo che $J\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}] \cap \mathbb{K}[\mathbf{x}]$ può essere riscritto come saturazione $J\mathbb{K}[\mathbf{x}]_{\mathbb{K}[\mathbf{u}] \setminus \{0\}} \cap \mathbb{K}[\mathbf{x}]$. Notiamo che $\mathfrak{p} \cap \mathbb{K}[\mathbf{u}] = \emptyset$, e quindi a maggior ragione $\mathfrak{p} \cap (\mathbb{K}[\mathbf{u}] \setminus \{0\}) = \emptyset$.

Dimostriamo che ogni primo associato di I ha intersezione non vuota con $\mathbb{K}[\mathbf{u}] \setminus \{0\}$.

Sia $I = \cap_{i=1}^r \mathfrak{q}_i$ una decomposizione primaria minimale di I ; senza perdita di generalità poniamo $\mathfrak{q} = \mathfrak{q}_1$. Visto che $\sqrt{I} = \mathfrak{p}$, tutti gli ideali primi $\sqrt{\mathfrak{q}_i}$ con $i > 1$ contengono strettamente $\mathfrak{p}$, che è minimale, e pertanto la loro dimensione è strettamente minore di $\dim(\mathfrak{p})$. Ricordando che $\#\mathbf{u} = \dim(\mathfrak{p})$, deduciamo che $\mathbf{u}$ è necessariamente dipendente rispetto a $\sqrt{\mathfrak{q}_i}$ per $i > 1$, e quindi $\sqrt{\mathfrak{q}_i} \cap (\mathbb{K}[\mathbf{u}] \setminus \{0\}) \neq \emptyset$ per ogni $i > 1$. Dal Teorema 1.8.2 sappiamo allora che $I\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}] \cap \mathbb{K}[\mathbf{x}] = \mathfrak{q}_1 = \mathfrak{q}$. □

Possiamo ora quindi definire cos'è l'*estrazione* di un ideale pseudo-primario.

Teorema 3.10

Siano $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale pseudo-primario, G una sua base di Gröbner ed f il minimo comune multiplo di tutti i coefficienti di testa dei polinomi di G visti come polinomi a coefficienti in $\mathbb{K}(\mathbf{u})$.

Dato un intero k tale che $I\mathbb{K}[\mathbf{x}]_f \cap \mathbb{K}[\mathbf{x}] = I : (f^k)$ e $I' = (I, f^k)$, la componente primaria associata a $\sqrt{I}$ è $\mathfrak{q} = I\mathbb{K}[\mathbf{x}]_f \cap \mathbb{K}[\mathbf{x}]$. Quindi

$$I = \mathfrak{q} \cap I'.$$

Inoltre, se $I' \neq \mathbb{K}[\mathbf{x}]$ si ha $\dim(I') < \dim(I)$.

Dimostrazione. Grazie al Teorema 2.18.2, sappiamo che il polinomio $f \in \mathbb{K}[\mathbf{u}]$ è tale che $I\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}] \cap \mathbb{K}[\mathbf{x}] = I : (f^k)$. Ricordandoci anche della Proposizione 3.9, sappiamo che $\mathfrak{q} = I\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}] \cap \mathbb{K}[\mathbf{x}]$ con $\mathfrak{q}$ ideale primario associato a $\sqrt{I}$. Usando lo Splitting Tool, possiamo quindi decomporre I come $I = I : (f^k) \cap (I, f^k) = \mathfrak{q} \cap I'$.

Dimostriamo quindi che se $I' \neq \mathbb{K}[\mathbf{x}]$ allora $\dim(I') < \dim(I)$. Poiché f^k non appartiene a $\sqrt{I}$, abbiamo $\sqrt{I} \subsetneq \sqrt{I'}$ e perciò $\dim(I') < \dim(I)$. □

Definizione 3.11. Sia $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale pseudo-primario con radicale $\mathfrak{p}$. Usando la stessa notazione del Teorema 3.10, l'elemento f definito nel Teorema 3.10 è detto *estrattore* associato a $\mathfrak{p}$.

Riutilizzando l'algoritmo RiduzioneZeroDimensionale, Algoritmo 2.19, possiamo calcolare l'estrazione di un ideale come segue.

Algoritmo 3.12 — Estrazione($I, \mathfrak{p}$)

Input: Un ideale pseudo-primario $I = (f_1, \dots, f_k) \subsetneq \mathbb{K}[\mathbf{x}]$ e il suo radicale $\mathfrak{p}$.

Output: Restituisce la coppia $(\mathfrak{q}, I')$ in cui $\mathfrak{q}$ è la componente primaria di I associata al suo unico primo minimale $\mathfrak{p}$, mentre I' è la componente restante dell'estrazione.

- 1: $(\mathbf{u}, G, f) \leftarrow \text{RiduzioneZeroDimensionale}(I)$;
- 2: $I' \leftarrow (I, f)$;
- 3: **return** $((G) \cap \mathbb{K}[\mathbf{x}], I')$;

Dimostriamo infine una caratterizzazione del radicale della componente restante dell'estrazione, che useremo in seguito.

Corollario 3.13. Usando la notazione del Teorema 3.10, vale la seguente identità

$$\sqrt{I'} = \sqrt{(I, f^k)} = \sqrt{(\sqrt{I}, \sqrt{f^k})} = \sqrt{(\mathfrak{p}, f)}.$$

§3.1.3 Calcolo di una decomposizione primaria

Abbiamo ora a disposizione tutti gli strumenti teorici necessari per il calcolo della decomposizione primaria di un ideale.

Algoritmo 3.14 — DecomposizionePrimariaSY(I)

Input: Un ideale $I = (f_1, \dots, f_k) \subseteq \mathbb{K}[\mathbf{x}]$.

Output: Se $I = \mathbb{K}[\mathbf{x}]$ restituisce $\emptyset$. Se $I \neq \mathbb{K}[\mathbf{x}]$ restituisce un insieme di coppie $(\mathfrak{q}_i, \mathfrak{p}_i)$ in cui i $\mathfrak{q}_i$ sono gli ideali primari di una decomposizione primaria di I e i $\mathfrak{p}_i$ sono i relativi primi associati.

- 1: **if** $1 \in I$ **then**
- 2: **return** $\emptyset$;
- 3: $\mathcal{U} \leftarrow \emptyset$;
- 4: $\text{minAss} = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\} \leftarrow$ primi minimali di I ;
- 5: $(\text{compPseudoPrimarie}, I') \leftarrow \text{DecomposizionePseudoPrimaria}(I, \text{minAss})$;
- 6: **for** $(\bar{\mathfrak{q}}, \mathfrak{p}) \in \text{compPseudoPrimarie}$ **do**:
- 7: $(\mathfrak{q}, \bar{\mathfrak{q}}') \leftarrow \text{Estrazione}(\bar{\mathfrak{q}}, \mathfrak{p})$;
- 8: $\mathcal{U} \leftarrow \mathcal{U} \cup \{(\mathfrak{q}, \mathfrak{p})\}$;
- 9: **if** $\bar{\mathfrak{q}}' \neq \mathbb{K}[\mathbf{x}]$ **then**
- 10: $\mathcal{U} \leftarrow \mathcal{U} \cup \text{DecomposizionePrimariaSY}(\bar{\mathfrak{q}}')$;
- 11: **if** $1 \notin I'$ **then**
- 12: $\mathcal{U} \leftarrow \mathcal{U} \cup \text{DecomposizionePrimariaSY}(I')$;
- 13: **return** $\mathcal{U}$;

L'Algoritmo 3.14 svolge i seguenti passi:

righe 1-2 controlla che I non sia l'intero anello;

- righe 4-5 dopo aver calcolato i primi minimali di I , calcola tramite essi una decomposizione pseudo-primaria dell'ideale;
- righe 6-10 per ogni componente pseudo-primaria, ne calcola l'estrazione e tramite ricorsione ottiene tutte le altre componenti della sua decomposizione pseudo-primaria, infine le aggiunge alla variabile $\mathcal{U}$;
- righe 11-12 calcola la decomposizione primaria della eventuale componente restante della decomposizione pseudo-primaria e aggiunge le sue componenti a $\mathcal{U}$, ottenendo quindi che l'intersezione di tutti gli elementi di $\mathcal{U}$ costituisce una decomposizione primaria di I .

Sappiamo inoltre che certamente termina: poiché la ricorsione nelle righe 10 e 12 viene applicata esclusivamente alle componenti restanti, ci è sufficiente ricordare che esse sono (1) oppure hanno dimensione strettamente minore di $\dim(I)$; per la finitezza della dimensione degli ideali di $\mathbb{K}[\mathbf{x}]$, l'algoritmo termina necessariamente in tempo finito.

§3.2 Decomposizione primaria minimale

In questa sezione introduciamo due criteri distinti per il riconoscimento di componenti ridondanti nell'algoritmo descritto nella sezione precedente, per evitare calcoli superflui e per ottimizzare la procedura. Otterremo grazie ad essi delle varianti degli algoritmi GTZ e SY che calcolano in maniera diretta una decomposizione primaria minimale dell'ideale dato in input.

§3.2.1 Identificazione di componenti ridondanti

Il criterio che mostriamo di seguito ha un'applicabilità che va oltre il contesto dell'algoritmo SY. In particolare, vedremo al termine di questa discussione come esso possa essere applicato all'algoritmo GTZ.

Ricordiamo la definizione di componente ridondante. Sia $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale e $I = \cap_{i=1}^r \mathfrak{q}_i$ una sua decomposizione primaria. Una componente $\mathfrak{q}$ della decomposizione si dice *ridondante* se

$$\bigcap_{\mathfrak{q}_i \neq \mathfrak{q}} \mathfrak{q}_i \subseteq \mathfrak{q}.$$

In questa prima proposizione esplicitiamo la relazione tra una decomposizione primaria minimale di un ideale e le decomposizioni primarie minimali delle sue componenti pseudo-primarie.

Proposizione 3.15. Siano $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale e una $I = \cap_{i=1}^r \bar{\mathfrak{q}}_i \cap I'$ decomposizione pseudo-primaria di I . Siano inoltre per ogni $i = 1, \dots, r$

$$\bar{\mathfrak{q}}_i = I : (s_i^{k_i}) = \bigcap_{j=1}^{r_i} \mathfrak{q}_{ij}$$

una decomposizione primaria minimale della componente pseudo-primaria $\bar{\mathfrak{q}}_i$ e

$$I' = (I, s_1^{k_1}, \dots, s_r^{k_r}) = \bigcap_{j=1}^{r_0} \mathfrak{q}_{0j}$$

una decomposizione primaria minimale della componente restante I' .

Allora per ogni $i = 1, \dots, r$ e $j = 1, \dots, r_i$ i primi $\sqrt{\mathfrak{q}_{ij}}$ sono associati ad I e sono a coppie distinti.

Dimostrazione. Sia $0 < i \leq r$ un indice fissato. Usando la stessa notazione del Corollario 3.4, notiamo che $\text{Ass}(\bar{q}_i) = \mathcal{P}_i$. Inoltre, dal momento che I' contiene $s_i^{k_i}$ abbiamo che $\text{Ass}(I') \cap \mathcal{P}_i = \emptyset$. Questo fatto ci permette di concludere: gli insiemi $\mathcal{P}_1, \dots, \mathcal{P}_r$ sono definiti come dei sottoinsiemi di $\text{Ass}(I)$ a coppie disgiunti, e poiché non esistono altre componenti primarie in I' che hanno radicale in $\mathcal{P}_i$, gli ideali $\mathfrak{q}_{ij}$ per $j = 0, \dots, r_i$ sono irridondanti. $\square$

Definiamo i seguenti insiemi che, come vedremo negli enunciati successivi, sono oggetti fondamentali nella formulazione del criterio di ridondanza.

Definizione 3.16. Siano $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale, $\mathfrak{p} \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale primo, s un intero positivo, $\mathcal{U} \subseteq \text{Ass}(I)$ un insieme di primi associati ad I e $I = \bigcap_{i=1}^l \mathfrak{q}_i$ una decomposizione primaria di I . Definiamo i seguenti insiemi:

$$\begin{aligned} \text{Ass}(I, \mathfrak{p}) &:= \{\mathfrak{p}' \in \text{Ass}(I) \mid \mathfrak{p}' \subsetneq \mathfrak{p}\}, \\ \text{Ass}(I, s) &:= \{\mathfrak{p}' \in \text{Ass}(I) \mid \dim(\mathfrak{p}') > s\}, \\ I_{\mathcal{U}} &:= \bigcap_{\substack{\mathfrak{p}' \in \mathcal{U} \\ \sqrt{\mathfrak{q}_i} \subseteq \mathfrak{p}'}} \mathfrak{q}_i. \end{aligned}$$

Denotiamo inoltre con $I_{\mathfrak{p}}$ e I_s rispettivamente gli ideali $I_{\text{Ass}(I, \mathfrak{p})}$ e $I_{\text{Ass}(I, s)}$.

La definizione di $I_{\mathcal{U}}$ è ben posta perché non dipende dalla scelta di una decomposizione primaria di I , come dimostriamo nel seguente lemma.

Lemma 3.17. Siano $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale, $\mathcal{U} \subseteq \text{Ass}(I)$ un insieme di primi associati, $I = \bigcap_{i=1}^l \mathfrak{q}_i = \bigcap_{i=1}^{l'} \mathfrak{q}'_i$ due decomposizioni primarie di I . Allora

$$\bigcap_{\substack{\mathfrak{p}' \in \mathcal{U} \\ \sqrt{\mathfrak{q}_i} \subseteq \mathfrak{p}'}} \mathfrak{q}_i = \bigcap_{\substack{\mathfrak{p}' \in \mathcal{U} \\ \sqrt{\mathfrak{q}'_i} \subseteq \mathfrak{p}'}} \mathfrak{q}'_i.$$

Dimostrazione. Sia S l'insieme moltiplicativo $S = \mathbb{K}[\mathbf{x}] \setminus (\cup_{\mathfrak{p} \in \mathcal{U}} \mathfrak{p})$. Chiaramente, ci basta dimostrare che, per una qualunque decomposizione primaria di $I = \bigcap_{i=1}^r \mathfrak{q}_i$, si ha

$$\bigcap_{\substack{\mathfrak{p}' \in \mathcal{U} \\ \sqrt{\mathfrak{q}'_i} \subseteq \mathfrak{p}'}} \mathfrak{q}_i = I\mathbb{K}[\mathbf{x}]_S \cap \mathbb{K}[\mathbf{x}].$$

Ricordiamo innanzitutto che per il Teorema 1.8.2 si ha $I\mathbb{K}[\mathbf{x}]_S \cap \mathbb{K}[\mathbf{x}] = \bigcap_{\sqrt{\mathfrak{q}_i} \cap S = \emptyset} \mathfrak{q}_i$. Dato che $\sqrt{\mathfrak{q}_i} \subseteq \mathfrak{p}$ per un qualche $\mathfrak{p} \in \mathcal{U}$ implica $\sqrt{\mathfrak{q}_i} \cap S = \emptyset$, abbiamo il contenimento $I_{\mathcal{U}} \subseteq I\mathbb{K}[\mathbf{x}]_S \cap \mathbb{K}[\mathbf{x}]$. Per dimostrare il contenimento opposto, è sufficiente osservare che un ideale che non interseca S è contenuto nel suo complementare $\cup_{\mathfrak{p} \in \mathcal{U}} \mathfrak{p}$, e quindi per il Lemma di Scansamento è contenuto in almeno un primo $\mathfrak{p} \in \mathcal{U}$. $\square$

I due enunciati successivi sono i risultati centrali che ci permettono di formulare il criterio cercato: da essi sarà possibile stabilire se una componente primaria è ridondante o meno mediante un test di inclusione di ideali.

Lemma 3.18. Siano $I \subseteq J$ ideali e

$$\mathcal{U} = \{\mathfrak{p} \in \text{Ass}(I) \mid \mathfrak{p} \not\subseteq \text{Ass}(J) \text{ ed esiste } \mathfrak{p}' \in \text{Ass}(J) \text{ tale che } \mathfrak{p} \subsetneq \mathfrak{p}'\}.$$

Se $\text{Ass}(I) \cap \text{Ass}(J) = \emptyset$ si ha $I_{\mathcal{U}} \subseteq J$.

Dimostrazione. Se I e J hanno insiemi di primi associati disgiunti, allora $\mathcal{U} = \{\mathfrak{p} \in \text{Ass}(I) \mid \exists \mathfrak{p}' \in \text{Ass}(J) : \mathfrak{p} \subsetneq \mathfrak{p}'\}$.

Se consideriamo le saturazioni di I e J rispetto a $S = \mathbb{K}[\mathbf{x}] \setminus (\cup_{\mathfrak{p} \in \mathcal{U}} \mathfrak{p})$, per quanto visto nella dimostrazione del Lemma 3.17, otteniamo

$$I\mathbb{K}[\mathbf{x}]_S \cap \mathbb{K}[\mathbf{x}] = \bigcap_{\substack{\mathfrak{p}' \in \mathcal{U} \\ \sqrt{\mathfrak{q}_i'} \subseteq \mathfrak{p}'}} \mathfrak{q}_i \subseteq J\mathbb{K}[\mathbf{x}]_S \cap \mathbb{K}[\mathbf{x}] = J.$$

Inoltre, abbiamo l'identità $I\mathbb{K}[\mathbf{x}]_S \cap \mathbb{K}[\mathbf{x}] = I_{\mathcal{U}}$, e quindi possiamo concludere che

$$I_{\mathcal{U}} = I\mathbb{K}[\mathbf{x}]_S \cap \mathbb{K}[\mathbf{x}] \subseteq J\mathbb{K}[\mathbf{x}]_S \cap \mathbb{K}[\mathbf{x}] = J. \quad \square$$

Teorema 3.19

Siano $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale e $\mathfrak{q}$ l'unica componente $\mathfrak{p}$ -primaria di una sua decomposizione primaria. Sia inoltre $\mathcal{U} \subseteq \text{Ass}(I) \setminus \{\mathfrak{p}\}$ tale che $\text{Ass}(I, \mathfrak{p}) \subseteq \mathcal{U}$. Le seguenti proprietà sono equivalenti:

1. $\mathfrak{q}$ non è ridondante nella decomposizione primaria di I ;
2. $I_{\mathcal{U}} \not\subseteq \mathfrak{q}$.

Dimostrazione. Ricordiamo che per ogni $\mathcal{U} \subseteq \text{Ass}(I) \setminus \{\mathfrak{p}\}$ l'ideale $I_{\mathcal{U}}$ è intersezione di componenti primarie di I per definizione. Se $\mathfrak{q}$ non è ridondante, $\mathfrak{q}$ non può contenere $I_{\mathcal{U}}$.

Viceversa, notiamo che $\text{Ass}(I, \mathfrak{p}) = \{\mathfrak{p} \in \text{Ass}(I) \mid \mathfrak{p} \not\subseteq \text{Ass}(\mathfrak{q}), \exists \mathfrak{p}' \in \text{Ass}(\mathfrak{q}) : \mathfrak{p} \subsetneq \mathfrak{p}'\}$. Se $I_{\mathfrak{p}} \not\subseteq \mathfrak{q}$ allora $\mathfrak{p} \in \text{Ass}(I)$ per il Lemma 3.18, e quindi $\mathfrak{q}$ non è ridondante. Più in generale, dato che $I_{\mathcal{U}} \subseteq I_{\mathfrak{p}}$ è vero che $I_{\mathcal{U}} \not\subseteq \mathfrak{q}$ implica $I_{\mathfrak{p}} \not\subseteq \mathfrak{q}$, e quindi che $\mathfrak{q}$ non è ridondante. $\square$

Osserviamo che le ipotesi su $\mathcal{U}$ del corollario appena dimostrato sono soddisfatte, ad esempio, dagli insiemi $\text{Ass}(I, \mathfrak{p})$ e $\text{Ass}(I, \dim(\mathfrak{p}))$.

Il criterio del Teorema 3.19 con $\mathcal{U} = \text{Ass}(I, \dim(\mathfrak{p}))$ può essere esteso anche agli ideali equidimensionali. Siano $I = \cap_{i=1}^l \mathfrak{q}_i$ una decomposizione primaria di I , e $J = \cap_{j=1}^s \mathfrak{q}_{i_j}$ un ideale equidimensionale, allora esiste un $\mathfrak{q}_{i_j}$ irridondante nella decomposizione di I se e soltanto se $I_{\dim(J)} \not\subseteq J$. Ciò è vero in quanto se vi è una componente $\mathfrak{q}$ di J che è irridondante allora $I_{\dim(J)} \not\subseteq \mathfrak{q}$, e quindi a maggior ragione che $I_{\dim(J)} \not\subseteq J$. Viceversa, se per ogni $j = 1, \dots, s$ la componente $\mathfrak{q}_{i_j}$ è ridondante allora esistono $\mathfrak{q}_{h_1}, \dots, \mathfrak{q}_{h_r}$ componenti primarie di I diverse da $\mathfrak{q}_{i_j}$ tali che $\cap_{m=1}^r \sqrt{\mathfrak{q}_{h_m}} \subseteq \sqrt{\mathfrak{q}_{i_j}}$. Dimostriamo che, senza perdita di generalità, possiamo supporre che per ogni $m = 1, \dots, r$ l'ideale $\sqrt{\mathfrak{q}_{h_m}}$ abbia dimensione strettamente maggiore di $\dim(J)$. Dato che $\cap_{m=2}^r \sqrt{\mathfrak{q}_{h_m}} \cap \sqrt{\mathfrak{q}_{h_1}} \subseteq \sqrt{\mathfrak{q}_{i_j}}$, conseguenza abbiamo che $\sqrt{\mathfrak{q}_{h_1}} \subseteq \sqrt{\mathfrak{q}_{i_j}}$ oppure $\cap_{m=2}^r \sqrt{\mathfrak{q}_{h_m}} \subseteq \sqrt{\mathfrak{q}_{i_j}}$; se $\dim(\sqrt{\mathfrak{q}_{h_1}}) > \dim(J)$ allora il primo contenimento è impossibile. Possiamo quindi concludere che $I_{\dim(J)} \subseteq \cap_{m=1}^r \mathfrak{q}_{h_m} \subseteq J$.

Possiamo applicare questa osservazione all'Algoritmo GTZ: uno dei suoi passi fondamentali è infatti la decomposizione tramite Splitting Tool $I = I : (f^k) \cap (I, f^k)$ con $I : (f)^k$ equidimensionale per il Teorema 2.18.3.

Specializziamo la discussione all'Algoritmo GTZ, presentando delle varianti degli Algoritmi 2.10 e 2.20 che calcolano una decomposizione primaria minimale.

Algoritmo 3.20 — $\text{DecomposizioneZeroDimensionaleMin}(I[, H = (1)])$

Input: Un ideale $I \subsetneq \mathbb{K}[\mathbf{x}]$ 0-dimensionale. Un ideale $H \subseteq \mathbb{K}[\mathbf{x}]$ che è intersezione di tutte le componenti primarie calcolate nelle precedenti chiamate dell'algoritmo $\text{DecomposizionePrimariaMin}$; se H non è specificato in ingresso, viene posto $H = (1)$.

Output: Se $H = (1)$, restituisce un insieme di coppie di ideali $(\mathbf{q}_i, \mathbf{p}_i)$ in cui i $\mathbf{q}_i$ sono le componenti della decomposizione primaria minimale di I e i $\mathbf{p}_i$ sono i relativi primi associati.

```

1:  $\text{DecPrim} \leftarrow \emptyset$ ;
2: if  $H \subseteq I$  then
3:   return  $\text{DecPrim}$ ;
4:  $a \leftarrow$  elemento di  $\mathbb{K}^{n-1}$  preso in maniera casuale;
5:  $\phi_a \leftarrow$  cambio di coordinate come definito nello Shape Lemma;
6:  $I' \leftarrow \phi_a(I)$ ;
7:  $G \leftarrow$  base di Gröbner ridotta di  $I'$  rispetto all'ordine lessicografico dato da
    $x_1 > \dots > x_n$ ;
8:  $g \leftarrow$  elemento con monomio di testa minimo di  $G$ ;
9: Fattorizzo  $g$ :
10:  $g_1^{\nu_1} \dots g_n^{\nu_n} = g$ ;
11: for  $i = 1, \dots, s$  do
12:    $\mathbf{q}'_i \leftarrow (I', g_i^{\nu_i})$ ;
13:   if  $H \not\subseteq \mathbf{q}'_i$  then
14:      $\mathbf{q}_i \leftarrow (I, \phi_a^{-1}(g_i^{\nu_i}))$ ;
15:      $\mathbf{p}'_i \leftarrow \text{TestPrimario}(\mathbf{q}'_i)$ ;
16:     if  $\mathbf{p}'_i \neq (0)$  then
17:        $\mathbf{p}_i \leftarrow \phi_a^{-1}(\mathbf{p}'_i)$ ;
18:        $\text{DecPrim} \leftarrow \text{DecPrim} \cup \{(\mathbf{q}_i, \mathbf{p}_i)\}$ ;
19:   else
20:      $\text{DecPrim} \leftarrow \text{DecPrim} \cup \text{DecomposizioneZeroDimensionaleMin}(\mathbf{q}_i, H)$ ;
21: return  $\text{DecPrim}$ ;
```

Algoritmo 3.21 — $\text{DecomposizionePrimariaMin}(I[, H = (1)])$

Input: Due ideali $I, H \subseteq \mathbb{K}[\mathbf{x}]$, con H intersezione di tutte le componenti primarie calcolate nelle precedenti chiamate dello stesso algoritmo; se H non è specificato in ingresso, viene posto $H = (1)$.

Output: Se $I = (1)$ restituisce l'insieme vuoto. Se $H = (1)$ e $I \neq (1)$ restituisce un insieme di coppie di ideali $(\mathbf{q}_i, \mathbf{p}_i)$ in cui $\mathbf{q}_i$ sono gli ideali primari di una decomposizione primaria minimale di I e i $\mathbf{p}_i$ sono i relativi primi associati.

```

1: if  $H \subseteq I$  then
2:   return  $\emptyset$ ;
3:  $(\mathbf{u}, G, h) \leftarrow \text{RiduzioneZeroDimensionaleMin}(I)$ ;
4: if  $\#\mathbf{u} = 0$  then
5:   return  $\text{DecomposizioneZeroDim}(I, H)$ ;
6:  $\text{primariEstesi} \leftarrow \text{DecomposizioneZeroDim}((G)_{\mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}]}, H)$ ;
7:  $\text{primari} \leftarrow \{(\mathbf{q}_i \cap \mathbb{K}[\mathbf{x}], \mathbf{p}_i \cap \mathbb{K}[\mathbf{x}]) \mid (\mathbf{q}_i, \mathbf{p}_i) \in \text{primariEstesi}\}$ ;
8:  $H \leftarrow \bigcap_{\mathbf{q} \in \text{primari}} \mathbf{q} \cap H$ ;
```

```

9:  $\text{primari} \leftarrow \text{primari} \cup \text{DecomposizionePrimariaMin}((I, h), H)$ ;
10: return  $\text{primari}$ ;

```

Dato un ideale $I \subsetneq \mathbb{K}[\mathbf{x}]$, l'esecuzione di $\text{DecomposizionePrimariaMin}(I)$ differisce in due modi rispetto all'esecuzione dell'Algoritmo 2.20:

- ogni volta che chiamiamo $\text{DecomposizionePrimariaMin}$ e $\text{DecomposizioneZeroDimensionaleMin}$ su un ideale J , controlliamo se l'intersezione delle componenti primarie già calcolate appartiene a J : se ciò avviene, le componenti primarie di J che calcoleremmo sarebbero tutte ridondanti per I ;
- ogni volta che chiamiamo $\text{DecomposizioneZeroDimensionaleMin}$ su un ideale J , per ogni componente primaria di J controlliamo se le l'intersezione delle componenti primarie già calcolate appartiene a J : se ciò avviene, la sua contrazione sarebbe una componente ridondante per I .

Verifichiamo che restituisce una decomposizione primaria minimale.

Teorema 3.22

Dato $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale, l'Algoritmo 3.21 eseguito sulla coppia $(I, (1))$ restituisce una decomposizione primaria minimale di I .

Dimostrazione. Sia $(J, H) \subseteq \mathbb{K}[\mathbf{x}] \times \mathbb{K}[\mathbf{x}]$ con $H \neq (1)$ una coppia di ideali su cui viene eseguito $\text{DecomposizionePrimariaMin}$. Dato che l'ideale H è l'intersezione di tutte le componenti primaria calcolate in precedenza, se $H \subseteq J$ allora H è contenuto in tutte le componenti primarie di J , e perciò esse sono tutte ridondanti.

Dimostriamo per induzione sulla profondità di ricorsione che l'unione di tutte le componenti primarie calcolate fino a tale momento della ricorsione è costituito da ideali con radicali a coppie distinti. Al prima esecuzione di $\text{DecomposizioneZeroDimensionaleMin}$ al rigo 7 abbiamo una decomposizione primaria minimale dell'ideale $I : (h)$ per un certo $h \in \mathbb{K}[\mathbf{x}]$; al contempo, all' n -esimo passo con $n > 1$ uniamo alle componenti precedenti quelle di una decomposizione primaria minimale di $(I', h') : (l)$ per certi polinomi $h', l \in \mathbb{K}[\mathbf{x}]$. Tutte le componenti primarie di $(I', h') : (l)$ hanno radicali che contengono h' , mentre tutte quelle calcolate in precedenza hanno radicali che non lo contengono.

Sia quindi $(J, H) \subseteq \mathbb{K}(\mathbf{u})[\mathbf{x} \setminus \mathbf{u}] \times \mathbb{K}[\mathbf{x}]$ con $H \neq (1)$ e $\mathbf{u} \subseteq \mathbf{x}$ una coppia di ideali su cui viene eseguito $\text{DecomposizioneZeroDimensionaleMin}$. Osserviamo che $\text{Ass}(H)$ contiene $\text{Ass}(J^c, \dim(J^c))$, mentre per quanto visto al paragrafo precedente non contiene i primi associati delle componenti $(J, g_i)^c$ con (J, g_i) componente primaria di J . Possiamo quindi applicare il Teorema 3.19 e ottenere che ognuna delle componenti primarie $(J, g_i)^c$ di J^c è irridondante se e soltanto se $H \not\subseteq (J, g_i)^c$, o equivalentemente $H \not\subseteq (J, g_i)$. $\square$

§3.2.2 Albero di decomposizione

Per un'applicazione efficiente del criterio descritto precedentemente, è necessario introdurre ulteriori strumenti teorici. Vedremo di seguito come è possibile ottimizzare l'algoritmo SY mediante l'uso dell'*albero di decomposizione*. Esso ci permetterà di analizzare i passi svolti dall'algoritmo $\text{DecomposizionePrimariaSY}$, interrompendo i rami dell'algoritmo che portano a componenti ridondanti. Vediamo innanzitutto le seguenti definizioni.

Definizione 3.23. Sia $I \subsetneq \mathbb{K}[\mathbf{x}]$ un ideale. L'*albero di decomposizione* di I è un albero con radice I tale che ogni nodo V ha come figli tutti e soli gli ideali che si ottengono da V

nell'esecuzione dell'Algoritmo 3.14 mediante decomposizione primaria, pseudo-primaria o estrazione.

Per ogni nodo V dell'albero, definiamo la *profondità pesata* di V , denotata con $wtd(V)$, come la somma tra la profondità di V visto come nodo dell'albero e il numero di componenti restanti di decomposizioni pseudo-primarie che si incontrano nel cammino dalla radice I al nodo V .

Un nodo V si dice *nodo componente* se e soltanto se è un ideale primario ottenuto per estrazione dal suo nodo padre; si dice *nodo non-componente* altrimenti.

Dato l'albero di decomposizione di un ideale $I \subseteq \mathbb{K}[\mathbf{x}]$, i nodi componente sono tutte e sole le foglie dell'albero. Inoltre, l'insieme dei nodi componente coincide con l'insieme delle componenti della decomposizione primaria di I ottenuta dall'Algoritmo 3.14.

Dato un sotto-albero $\mathcal{T}'$ dell'albero di decomposizione di un ideale $I \subseteq \mathbb{K}[\mathbf{x}]$, chiamiamo *decomposizione primaria derivata* da $\mathcal{T}'$ l'intersezione di tutti i suoi nodi componente.

Nel resto della trattazione, denoteremo con $\mathcal{T}$ l'albero di decomposizione di un ideale $I \subseteq \mathbb{K}[\mathbf{x}]$ fissato.

Definizione 3.24. Sia (V', V) un arco dell'albero $\mathcal{T}$ tale che V è una componente pseudo-primaria non banale di V' , e sia S l'insieme separatore rispetto a $\sqrt{V}$ che è stato usato per determinare la decomposizione pseudo-primaria di V' .

Un ideale $J \subseteq \mathbb{K}[\mathbf{x}]$ si dice che soddisfa la *condizione di separazione rispetto a* (V', V) se e soltanto se $\sqrt{J}$ non contiene $s := \prod_{t \in S} t$.

Sia V un nodo di $\mathcal{T}$ e sia $I = V_0, \dots, V_r = V$ il cammino dalla radice I al nodo V in $\mathcal{T}$. Si dice che V soddisfa la *condizione di separazione* se e soltanto se V soddisfa la condizione di separazione rispetto a ogni arco (V_i, V_{i+1}) con V_{i+1} componente pseudo-primaria non banale di V_i .

Osservazione 3.25. Sia V un nodo di $\mathcal{T}$, siano $(V_{i_1}, V_{i_1+1}), \dots, (V_{i_l}, V_{i_l+1})$ tutti gli archi nel cammino da I a V in cui il secondo elemento dell'arco è una componente pseudo-primaria non banale del padre e sia s_j il prodotto di tutti gli elementi dell'insieme separatore rispetto a $\sqrt{V_{i_j+1}}$ per ogni j . Il nodo V soddisfa la condizione di separazione se e soltanto se $\sqrt{V}$ non contiene $s := \prod_{j=1}^l s_j$.

Per ogni nodo V di $\mathcal{T}$, chiamiamo *tester* di V l'elemento s definito nell'osservazione.

Mostriamo ora un primo risultato che mette in evidenza in che modo la condizione di separazione e la riducibilità di un vertice sono connesse.

Lemma 3.26. Per ogni nodo non-componente V di $\mathcal{T}$, se V non soddisfa la condizione di separazione allora tutti i nodi componente nel sotto-albero di V sono ridondanti nella decomposizione primaria derivata da $\mathcal{T}$.

Dimostrazione. Sia $I = V_0, \dots, V_r = V$ il cammino dalla radice I a V . Dato che V non soddisfa la condizione di separazione, esiste in particolare un arco (V_i, V_{i+1}) rispetto a cui V non la soddisfa. Per il Teorema 3.5 sappiamo che $V_i \mathbb{K}[\mathbf{x}]_s \cap \mathbb{K}[\mathbf{x}] = V_{i+1}$ con s prodotto di tutti gli elementi dell'insieme separatore rispetto a $\sqrt{V_{i+1}}$ nella decomposizione pseudo-primaria di V_i . Dato che vale $V_{i+1} \mathbb{K}[\mathbf{x}]_s \cap \mathbb{K}[\mathbf{x}] = V_{i+1}$, nessuna componente primaria non ridondante di V_{i+1} può contenere una potenza di s .

Prendiamo quindi un nodo componente Q nel sotto-albero di V . Esso è necessariamente una componente primaria ridondante di V_{i+1} , infatti s appartiene a $\sqrt{V}$ che è contenuto a sua volta in $\sqrt{Q}$, e perciò esiste una potenza di s in Q . Dato che Q è una componente primaria ridondante di V_{i+1} , è anche una componente primaria ridondante di I . $\square$

Introduciamo ora il seguente albero ricavato da $\mathcal{T}$.

Definizione 3.27. Chiamiamo *albero di decomposizione ridotto* di I l'albero ottenuto da $\mathcal{T}$ eliminando ogni sotto-albero la cui radice non soddisfa la condizione di separazione. Denotiamo tale albero con $\mathcal{T}_{\text{red}}$.

Vogliamo dimostrare che la decomposizione primaria derivata da $\mathcal{T}_{\text{red}}$ è una decomposizione primaria minimale di I . Vediamone intanto alcune sue proprietà.

Proposizione 3.28. Tutti i nodi componente di $\mathcal{T}_{\text{red}}$ hanno primi associati distinti.

Dimostrazione. Siano V e V' due distinti nodi componente in $\mathcal{T}_{\text{red}}$ e sia U la radice del più piccolo sotto-albero che contiene sia V che V' . Chiamiamo W e W' i figli di U antenati rispettivamente di V e V' .

Se U è una componente pseudo-primaria del padre, possiamo assumere senza perdita di generalità $W = V$ e che W' sia la componente restante dell'estrazione. Possiamo concludere che le radici di V e V' sono distinte, infatti esiste un estrattore $f \in \sqrt{W'} \setminus \sqrt{V} \subseteq \sqrt{V'} \setminus \sqrt{V}$.

Prendiamo ora il caso in cui U non è una componente pseudo-primaria del padre, ovvero il caso in cui è una componente restante di un'estrazione o di una decomposizione pseudo-primaria. Possiamo assumere senza perdita di generalità che W sia una componente pseudo-primario di U con separatore un insieme S . Sia $s := \prod_{t \in S} t$, allora $s \in \sqrt{W'} \setminus \sqrt{V}$. Dato che $W \subseteq V$ allora $\sqrt{V'} \neq \sqrt{V}$. $\square$

Definizione 3.29. Per ogni $\mathfrak{p} \in \text{Ass}(I)$, esiste un unico nodo componente in $\mathcal{T}_{\text{red}}$ associato a $\mathfrak{p}$. Denotiamo tale componente con $q(\mathfrak{p})$. Inoltre, dato un ideale $J \subsetneq \mathbb{K}[\mathbf{x}]$, se il suo radicale contiene almeno un primo minimale di I , definiamo

$$d(J, I) := \max\{\dim(\mathfrak{p}) \mid \mathfrak{p} \in \min\text{Ass}(I), \mathfrak{p} \subseteq \sqrt{J}\}.$$

Corollario 3.30. L'intersezione degli elementi di $\{q(\mathfrak{p}) \mid \mathfrak{p} \in \text{Ass}(I)\}$ forma una decomposizione primaria minimale di I .

Per concludere questa sezione e ottenere il nostro criterio, ci rimane soltanto da verificare che l'insieme definito nel Corollario 3.30 sopra coincide con quello dei nodi componente di $\mathcal{T}_{\text{red}}$. Dopo aver dimostrato un lemma preparatorio, mostriamo due proprietà dell'albero di decomposizione ridotto, le quali costituiscono degli strumenti utili per dimostrare l'enunciato desiderato.

Lemma 3.31. Per ogni ideale $\mathfrak{p} \in \text{Ass}(\mathbb{K}[\mathbf{x}])$ e per ogni elemento $s \in \mathbb{K}[\mathbf{x}]$ tale che $I = (\mathfrak{p}, s) \neq \mathbb{K}[\mathbf{x}]$, i primi minimali di I hanno dimensione $\dim(\mathfrak{p}) - 1$.

Dimostrazione. Per il Teorema dell'Ideale Principale di Krull sappiamo che i primi minimali di $I/\mathfrak{p} = (s)/\mathfrak{p}$ hanno altezza 1. Di conseguenza, dato che in $\mathbb{K}[\mathbf{x}]$ la somma della dimensione di un primo e della sua altezza è n , i corrispondenti ideali nell'anello $\mathbb{K}[\mathbf{x}]$, ovvero i primi minimali di I , hanno dimensione $\dim(\mathfrak{p}) - 1$. $\square$

Teorema 3.32

Per ogni nodo componente V di $\mathcal{T}_{\text{red}}$, vale la seguente formula $wtd(V) = 2(d(V, I) - \dim(V) + 1)$.

Dimostrazione. Dimostriamo per induzione su $m(V, I) := 2(d(V, I) - \dim(V) + 1)$ che vale l'identità $wtd(V) = m(V, I)$.

Se $m(V, I) = 0$ allora $d(V, I) = \dim(V) - 1$, ma ciò è impossibile in quanto ogni primo $\mathfrak{p}$ contenuto in $\sqrt{V}$ ha dimensione superiore o uguale a quella di V .

Se $m(V, I) = 2$ abbiamo $d(V, I) = \dim(V)$, quindi esiste un primo minimale $\mathfrak{p}$ di I che è contenuto nel primo $\sqrt{V}$ e che ha la stessa dimensione di $\sqrt{V}$. Questo implica l'identità $\mathfrak{p} = \sqrt{V}$, ovvero V è una componente primaria associata ad un primo minimale di I . Di conseguenza si ottiene calcolando l'estrazione di una componente pseudo-primaria di I , ovvero $wtd(V) = 2$.

Consideriamo ora il caso $m(V, I) > 2$. Sia W l'antenato di V con profondità pesata pari a 2: tale nodo del grafo esiste sempre ed è la componente restante della decomposizione pseudo-primaria di I , oppure la componente restante dell'estrazione di un ideale pseudo-primario di I . Per concludere la dimostrazione è sufficiente dimostrare che $d(V, W) = d(V, I) - 1$. Infatti, restringendoci al sottoalbero di W , possiamo applicare l'ipotesi induttiva e ottenere infine la tesi.

Consideriamo il caso in cui W è la componente restante tramite estrazione di un ideale pseudo-primario $\bar{q}$. Prendiamo un primo minimale $\mathfrak{p}_1$ di I contenuto in $\sqrt{V}$ con dimensione $\dim(\mathfrak{p}_1) = d(V, I)$ e sia $\bar{q}_1$ l'ideale pseudo-primario ad esso associato.

Dimostriamo per assurdo che $\bar{q}_1 = \bar{q}$. Se i due ideali fossero distinti, allora lo sarebbero anche i loro radicali $\mathfrak{p}_1$ e $\sqrt{\bar{q}}$. Per questa ragione sappiamo che $\mathfrak{p}_1$ contiene il prodotto di tutti gli elementi dell'insieme separatore associato a $\bar{q}$. Perciò V non soddisfa la condizione di separazione visto che $\sqrt{V} \supseteq \mathfrak{p}_1$, che è assurdo.

Sapendo quindi che $\bar{q}_1 = \bar{q}$, osserviamo che ogni primo minimale di W è per il Corollario 3.13 un primo minimale di $\sqrt{(\mathfrak{p}_1, f)}$ con f estrattore associato a $\mathfrak{p}_1$. Per il Lemma 3.31, ogni primo minimale di W ha quindi dimensione $\dim(\mathfrak{p}_1) - 1$, e ciò ci permette di concludere che $d(V, W) = d(V, I) - 1$.

Consideriamo invece ora il caso in cui W è la componente restante della decomposizione pseudo-primaria di I . Sia $\mathfrak{p}'$ un primo minimale di W di dimensione $d(V, W)$ tale che $\mathfrak{p}' \subseteq \sqrt{V}$. Per il Corollario 3.8,

$$\sqrt{W} = \bigcap_{\mathfrak{p} \in \min \text{Ass}(I)} \sqrt{(\mathfrak{p}, s_{\mathfrak{p}})}$$

dove $s_{\mathfrak{p}}$ è il prodotto di tutti gli elementi dell'insieme separatore di $\mathfrak{p}$. Esiste quindi un primo minimale $\mathfrak{p}_2$ di I tale che

$$\sqrt{(\mathfrak{p}_2, s_{\mathfrak{p}_2})} \subseteq \sqrt{W} \subseteq \mathfrak{p}' \subseteq \sqrt{V}.$$

Da ciò deduciamo che $\dim(\mathfrak{p}_2) \leq d(V, I) = \dim(\mathfrak{p}_1)$ per un certo $\mathfrak{p}_1 \subseteq \sqrt{V}$ primo minimale di W . Per il Lemma 3.31, inoltre, abbiamo che $\dim(\mathfrak{p}') + 1 = \dim(\mathfrak{p}_2) + 1 = d(V, W) + 1 \leq d(V, I)$.

Ci rimane quindi soltanto da dimostrare che $d(V, W) \geq d(V, I) - 1$. Osserviamo infatti che i $\mathfrak{p}_1$ e $s_{\mathfrak{p}_1}$ definiti sopra sono tali che $\mathfrak{p}_1 \subseteq \sqrt{V}$ e $s_{\mathfrak{p}_1} \in \sqrt{W} \subseteq \sqrt{V}$, quindi $\sqrt{(\mathfrak{p}_1, s_{\mathfrak{p}_1})} \subseteq \sqrt{V}$. Visto che per il Lemma 3.31 tutti i primi minimali di $\sqrt{(\mathfrak{p}_1, s_{\mathfrak{p}_1})}$ hanno dimensione $\dim(\mathfrak{p}_1) - 1$. $\square$

Corollario 3.33. Siano V, V' nodi componente di $\mathcal{T}_{\text{red}}$. Se $\sqrt{V} \subsetneq \sqrt{V'}$ allora $wtd(V) < wtd(V')$.

Dimostrazione. Sia $\mathfrak{p}$ un primo minimale di I tale che $\mathfrak{p} \subseteq \sqrt{V}$ di dimensione $d(V, I)$, perciò $\dim(V') < \dim(V)$ e per ipotesi $d(V', I) \geq \dim(\mathfrak{p}) = d(V, I)$. Da questo otteniamo

che $d(V', I) - \dim(V') > d(V', I) - \dim(V) \geq d(V, I) - \dim(V)$. Dal Teorema 3.32 otteniamo la disuguaglianza cercata. $\square$

§3.2.3 Calcolo di una decomposizione primaria minimale

In conclusione a questa sezione, presentiamo una modifica del precedente Algoritmo 3.14. L'algoritmo descritto di seguito calcola una decomposizione primaria minimale di un qualsiasi ideale proprio di $\mathbb{K}[\mathbf{x}]$; più in particolare, restituisce tutte le componenti irridondanti della decomposizione derivata da $\mathcal{T}_{\text{red}}$.

Algoritmo 3.34 — DecomposizionePrimariaMinSY(I)

Input: Un ideale $I = (f_1, \dots, f_k) \subseteq \mathbb{K}[\mathbf{x}]$.

Output: Se $I \neq \mathbb{K}[\mathbf{x}]$ restituisce un insieme di coppie $(\mathfrak{q}_i, \mathfrak{p}_i)$ in cui i $\mathfrak{q}_i$ sono gli ideali primari della decomposizione primaria di I e i $\mathfrak{p}_i$ sono i relativi primi associati. Se $I = \mathbb{K}[\mathbf{x}]$ invece restituisce $(\emptyset, \emptyset)$.

```

1: if  $1 \in I$  then
2:   return  $(\emptyset, \emptyset)$ ;
3:  $H \leftarrow \mathbb{K}[\mathbf{x}]$ ,  $\mathcal{W} \leftarrow \{I\}$ ,  $\mathcal{U} \leftarrow \emptyset$ ;
4: while  $H \neq I$  do
5:    $V \leftarrow$  nodo non-componente di  $\mathcal{W}$  con la profondità pesata più bassa;
6:    $\mathcal{W} \leftarrow \mathcal{W} \setminus \{V\}$ ;
7:    $\mathcal{Y} \leftarrow$  figli del nodo  $V$ ;
8:   if esiste nodo componente  $Q \in \mathcal{Y}$  tale che  $H \not\subseteq Q$  then
9:      $U \leftarrow \{Q\} \cup \mathcal{U}$ ,  $H \leftarrow H \cap Q$ ;
10:   $\mathcal{W} \leftarrow \{V \in \mathcal{Y} \mid V \text{ è un nodo non-componente che soddisfa la condizione di separazione}\} \cup \mathcal{W}$ ;
11: return  $\mathcal{U}$ ;
```

Teorema 3.35

L'Algoritmo 3.34 restituisce una decomposizione primaria minimale di I .

Dimostrazione. Per la Proposizione 3.28 e il Corollario 3.30 sappiamo già che i nodi componente di $\mathcal{T}_{\text{red}}$ formano una decomposizione primaria le cui componenti hanno radicali a coppie distinti. Rimane quindi da dimostrare che nessuno di essi è ridondante. Usando la notazione interna all'algoritmo, dimostriamo che per ogni nodo componente di $\mathcal{T}_{\text{red}}$, la condizione $H \not\subseteq V$ è equivalente all'irridondanza di V . È chiaro per la definizione di ridondanza che se V è irridondante allora non contiene H .

Dimostriamo quindi il viceversa per induzione su $wtd(V)$.

Se $wtd(V) = 2$ allora per il Teorema 3.32 vale $\dim(V) = d(V, I)$, perciò esiste un primo minimale $\mathfrak{p}_0$ di I contenuto in $\sqrt{V}$ che ne ha la stessa dimensione, e quindi $\sqrt{V} = \mathfrak{p}_0$, e quindi V non è ridondante.

Se $wtd(V) > 2$, allora sappiamo che per tutti i nodi componente U che hanno profondità pesata strettamente minore di $wtd(V)$ vale l'ipotesi induttiva. Inoltre, per questa ragione, H è contenuto nell'intersezione di tutte le componenti primarie Q di I tali che $wtd(Q) < wtd(V)$, dato che esse sono ridondanti rispetto alla decomposizione già calcolata a tale punto dell'algoritmo. Per il Corollario 3.33 abbiamo quindi che per ogni

$\mathfrak{p} \in \text{Ass}(I)$, con $\mathfrak{p} \subseteq \sqrt{V}$, si ha $\text{wtd}(q(\mathfrak{p})) < \text{wtd}(V)$. Allora $H \subseteq I_{\sqrt{V}}$. D'altra parte, dato che $V \not\subseteq H$, allora $V \not\subseteq I_{\sqrt{V}}$, e per il Teorema 3.19 abbiamo che V non è ridondante. $\square$

Bibliografia

- [1] M.F. Atiyah e I.G. MacDonald. *Introduction To Commutative Algebra*. Addison-Wesley series in mathematics. Avalon Publishing, 1994. ISBN: 9780813345444.
- [2] A. Bandini, P. Gianni e E. Sbarra. *Esercizi di algebra commutativa*. Pisa University Press, 2023. ISBN: 9788833396798.
- [3] W. Decker, G.M. Greuel e G. Pfister. “Primary decomposition: algorithms and comparisons”. In: *Algorithmic Algebra and Number Theory: Selected Papers From a Conference Held at the University of Heidelberg in October 1997*. Springer. 1999, pp. 187–220.
- [4] D. Eisenbud, C. Huneke e W. Vasconcelos. “Direct methods for primary decomposition”. In: *Inventiones Mathematicae* 110 (dic. 1992), pp. 207–235.
- [5] P. Gianni, B. Trager e G. Zacharias. “Gröbner bases and primary decomposition of polynomial ideals”. In: *Journal of Symbolic Computation* 6.2 (1988), pp. 149–167. ISSN: 0747-7171.
- [6] G.M. Greuel et al. *A Singular Introduction to Commutative Algebra*. Springer Berlin Heidelberg, 2007. ISBN: 9783540735427.
- [7] G. Hermann. “Die Frage der endlich vielen Schritte in der Theorie der Polynomideale. (Unter Benutzung nachgelassener Sätze von K. Hentzelt)”. In: *Mathematische Annalen* 95 (1926), pp. 736–788.
- [8] S. Laplagne. “Computation of the Minimal Associated Primes”. In: *Challenges in Symbolic Computation Software*. A cura di W. Decker et al. Vol. 6271. Dagstuhl Seminar Proceedings (DagSemProc). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2006, pp. 1–6.
- [9] E. Lasker. *Zur Theorie der moduln und Ideale*.
- [10] F.S. Macaulay. “On the Resolution of a given Modular System into Primary Systems including some Properties of Hilbert Numbers.” In: *Mathematische Annalen* 74 (1913), pp. 66–121.
- [11] E. Noether. *Idealtheorie in Ringbereichen*.
- [12] T. Shimoyama e K. Yokoyama. “Localization and Primary Decomposition of Polynomial Ideals”. In: *Journal of Symbolic Computation* 22.3 (1996), pp. 247–277. ISSN: 0747-7171.
- [13] O. Zariski, I.S. Cohen e P. Samuel. *Commutative Algebra I*. Graduate Texts in Mathematics. Springer New York, 1975. ISBN: 9780387900896.