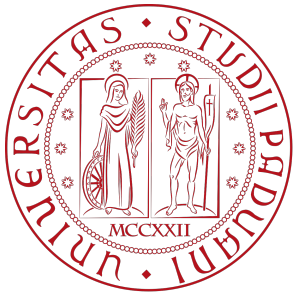
UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI MATEMATICA "TULLIO LEVI-CIVITA"
DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE



Corso di Laurea Triennale in Matematica

Anelli di polinomi in più variabili e basi di Gröbner

Relatrice:
Prof.ssa Eloisa M. Detomi

Laureanda:
Bianca Pigato

Matricola:
1151202

ANNO ACCADEMICO 2021/2022

23 giugno 2022

Indice

Introduzione

Gli anelli di polinomi rappresentano una delle maggiori e prolifiche branche dell'Algebra e, in generale, della Matematica. In particolare, la loro spiccata applicabilità dalle scienze pure a quelle applicate li rende oggetti matematici di notevole interesse. Lo studio della loro struttura e delle loro proprietà occupa un ruolo fondamentale nella scienza moderna.

Lo scopo di questa tesi è studiare gli anelli di polinomi in più variabili con coefficienti su campi e introdurre la teoria delle basi di Gröbner. Il nostro obiettivo è affrontare tale teoria attraverso teoremi ed algoritmi per il calcolo delle basi di Gröbner. Sottolineiamo infatti come questo argomento sia aperto ad una trattazione algoritmica ed eventualmente ad un'implementazione computazionale [1]. I contenuti presentati sono organizzati nella maniera che segue.

In primo luogo andremo a ricordare brevemente alcuni aspetti salienti degli anelli di polinomi in una variabile. Successivamente estenderemo tale discussione ad un contesto in più variabili. Come verrà discusso in dettaglio, gli anelli di polinomi in più variabili su un campo, rispetto ai loro analoghi in una variabile, soffriranno la perdita di importanti proprietà: ad esempio, non avremo più a che fare con domini euclidei, né con domini ad ideali principali, ma con i più generali domini a fattorizzazione unica. Inoltre, tali anelli richiederanno l'introduzione di nuovi concetti e nuovi oggetti di studio: in particolare, come vedremo, sarà necessario introdurre un nuovo modo di definire il grado un polinomio basato sulla scelta di un *ordinamento monomiale*. Fissato tale ordinamento, sarà possibile parlare di *termini direttori* di polinomi, in analogia con i termini di grado massimo in una variabile, e costruire un nuovo e più generale algoritmo di divisione polinomiale.

Facendo uso di tale algoritmo di divisione, ci accorgeremo di un'ulteriore problematica propria dei polinomi multivariati: il resto della divisione di polinomi generalizzata, rispetto un generico insieme di polinomi divisori, perde l'unicità. Questo rappresenta una grave complicazione dal momento che l'unicità del resto della divisione per polinomi in una variabile a coefficienti su un campo garantisce un solido criterio di appartenenza di un

polinomio ad un ideale: sappiamo infatti che dividendo un polinomio per gli elementi di un insieme di generatori di un ideale a cui appartiene si ottiene sempre un resto nullo. In più variabili, in generale, tale proprietà viene persa. In questo contesto si inserisce lo studio delle basi di Gröbner, introdotto da Bruno Buchberger nel 1965 [2]. La terminologia tiene conto dell'influenza di Wolfgang Gröbner sul lavoro di Buchberger. L'idea alla base del lavoro di Buchberger è semplice ma di successo: il suo obiettivo è fornire per ogni ideale un insieme di generatori che permetta di restaurare tale criterio di appartenenza. Un insieme di generatori che permetta ciò è una *base di Gröbner* per l'ideale considerato. La forza del lavoro di Buchberger è tuttavia l'aver presentato un algoritmo in grado di fornire esplicitamente in un numero finito di passi una base di Gröbner per un ideale. A partire da un suo generico insieme di generatori, l'algoritmo aggiorna tale insieme aggiungendo polinomi ottenuti attraverso opportune combinazioni lineari che indicheremo come *S-polinomi*, fino ad ottenere una base di Gröbner. Tali risultati sono validi esclusivamente per polinomi con coefficienti appartenenti ad un campo. Volendo estendere tale trattazione a casi in cui l'anello dei coefficienti presenti una struttura più generale [6], come domini euclidei, incontriamo maggiori difficoltà legate principalmente al calcolo degli S-polinomi.

In seguito, verrà spiegata ed illustrata nel dettaglio l'importanza delle basi di Gröbner sia dal punto di vista prettamente teorico che applicativo. Nell'ultima parte, infatti, andremo a presentare delle applicazioni alla teoria delle basi di Gröbner. In particolare vedremo la *teoria dell'eliminazione* volta alla risoluzione di sistemi di equazioni algebriche. Illustreremo anche come sia possibile sfruttare questa teoria per risolvere problemi di diversa natura; tra questi, il problema di come colorare i vertici di un grafo non orientato in modo che vertici connessi presentino colori differenti e l'interpretazione del gioco del Sudoku in termini di un grafo colorato [5]. Studieremo, inoltre, alcuni metodi per lavorare con ideali di anelli in più variabili usando le basi di Gröbner in concerto con la teoria dell'eliminazione.

Il registro e la notazione scelti in questa tesi vogliono essere in continuità con le scelte didattiche incontrate nel corso di laurea in Matematica, volendo dare la possibilità di approfondire lo studio degli anelli polinomiali in più variabili. Esclusi i casi in cui esplicitamente specificato, abbiamo voluto seguire la trattazione di anelli polinomiali e basi di Gröbner presente in "Abstract Algebra" di David Dummit e Richard Foote [4][cap.9].

Capitolo 1

Anelli di polinomi: definizioni e concetti introduttivi

In questo capitolo introduttivo andremo a presentare le definizioni e nozioni di base riguardanti anelli di polinomi in una e più variabili, in particolare la struttura dei loro elementi e la notazione alla quale verrà fatto riferimento in seguito. Da questo momento, R sarà sempre un anello commutativo con identità $1 \neq 0$.

1.1 Anelli di polinomi in una variabile su un anello

L'anello dei polinomi $R[x]$ di indeterminata x sull'anello R è l'insieme di tutte le somme formali del tipo $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ con $n \geq 0$ e i coefficiente $a_i \in R$.

Se $a_n \neq 0$ allora si dice che il grado del polinomio è n, $a_n x^n$ è detto *termine direttore.* o termine di grado massimo, e a_n, il coefficiente relativo al termine di grado massimo, viene detto *coefficiente direttore* del polinomio.

Il polinomio nullo viene definito come un polinomio il cui coefficiente direttore $a_n = 0$. Un polinomio si dice infine *monico* se il coefficiente di grado massimo $a_n = 1$.

Le operazioni di somma e prodotto dell'anello di polinomi sono definite nel modo seguente; la somma è della seguente tipologia, somma membro a membro:

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i.$$

Il prodotto invece viene definito descrivendo preliminarmente il prodotto tra due generici termini, per poi estendere tale operazione a due polinomi facendo uso della proprietà distributiva. Il prodotto tra due monomi ax^i, $bx^j \in R[x]$ è dato da $(ax^i)(bx^j) = abx^{i+j}$ e in generale per due polinomi:

$$\left(\sum_{i=0}^{n} a_i x^i\right) \times \left(\sum_{j=0}^{m} b_j x^j\right) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} (a_i b_{k-i})\right) x^k.$$

In questi termini, possiamo affermare che $R[x]$ è un anello commutativo con identità, in cui l'identità $1_{R[x]}$ è ereditata dall'anello dei coefficienti R ovvero 1_R; infine identifichiamo R con il sottoanello di $R[x]$ dei polinomi costanti.

Ai fini dello studio dell'anello dei polinomi sulla base delle proprietà dell'anello su cui è costruito, si presenta un'utile proposizione sulle proprietà che eredita $R[x]$ da R, se quest'ultimo è un dominio di integrità.

Proposizione 1. *Sia R un dominio di integrità. Allora, indicando con $deg(p(x)$ il grado del polinomio:*

1. *$deg(p(x)q(x)) = deg(p(x)) + deg(q(x))$ se $p(x)$, $q(x)$ sono polinomi non nulli.*
2. *gli elementi invertibili di $R[x]$ sono solo gli elementi invertibili di R*
3. *$R[x]$ è un dominio di integrità.*

Ricordiamo inoltre un risultato che chiarisce la relazione tra gli ideali dell'anello R e quelli del suo anello di polinomi nella variabile x.

Proposizione 2. *Sia I un ideale dell'anello R e si intenda $(I) = I[x]$, l'ideale di $R[x]$ generato da I, ovvero l'insieme dei polinomi a coefficienti in I. Allora*

$$R[x]/(I) \cong (R/I)[x].$$

In particolare, se I è un ideale primo di R allora (I) è un ideale primo di $R[x]$.

1.2 Anello di polinomi in più variabili su un anello

Concludiamo questa prima parte descrivendo la naturale generalizzazione degli anelli di polinomi in più variabili.

Definizione 1. L'anello dei polinomi nelle variabili $x_1, x_2, \ldots, x_n$ con coefficienti nell'anello R è definito induttivamente come

$$R[x_1, x_2, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$$

Questa definizione mostra come polinomi in n variabili possano essere presentati come polinomi in una sola variabile, in questo caso x_n, ma di coefficienti in $R[x_1, \ldots, x_{n-1}]$, che possono a loro volta essere visti come polinomi nella variabile x_{n-1} e coefficienti in $R[x_1, \ldots, x_{n-2}]$ e così via.

In tal senso ci si riferisce a quest'ultima definizione come *induttiva*. Tale proprietà costitutiva degli anelli di polinomi in più variabili risulterà di fondamentale importanza negli studi successivi.

In altre parole, possiamo definire tali polinomi come somme di termini generali del tipo $ax_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$ con $a \in R$ e $d_1, d_2, \ldots, d_n \geq 0$, numeri naturali opportunamente stabiliti.

Diamo inoltre la definizione di anello di polinomi in un numero arbitrario di variabili.

Definizione 2. L'anello polinomiale in un numero arbitrario di variabili con coefficienti nell'anello R è l'*unione* di tutti gli anelli di polinomi in un numero finito di variabili su R.

Ora ci occupiamo di presentare la notazione di cui verrà fatto uso nei capitoli successivi.

Il termine $x_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$ è un monomio di $R[x_1, \ldots x_n]$ nonché la parte monomiale di $ax_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$.

Successivamente, si indica il *grado del termine individuale* $ax_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$ con $d = d_1 + d_2 + \cdots + d_n$, la somma dei singoli gradi di ogni variabile contenuta nel termine. Un polinomio si dice infine *omogeneo* se ogni suo termine presento il medesimo grado.

Si può poi scrivere un polinomio non nullo come somma di componenti omogenee di grado compreso tra 0 e il grado d del polinomio. La somma di tutti i termini monomiali di f, polinomio in n variabili non nullo di grado k, è chiamata *componente omogenea di f di grado k*. Se f ha grado d, allora f si può scrivere in modo univoco come $f_0 + f_1 + \cdots + f_d$ con f_k la k-esima componente omogenea di f, per $0 \leq k \leq d$ e con la possibilità che qualche componente sia zero.

Introduciamo infine una notazione conveniente per indicare il grado di un termine tenendo conto dei singoli contributi di ogni indeterminata, ovvero il *multigrado*.

Definizione 3 (Multigrado)**.** Sia $ax_1^{d_1}x_2^{d_2}\ldots x_n^{d_n}$ un generico termine di $R[x_1, \ldots x_n]$, allora la $n-$tupla ordinata $(d_1, d_2, \ldots, d_n)$ è il *multigrado* del termine.

Faremo infine riferimento al *multigrado* dell'intero polinomio come al maggiore tra i multigradi dei termini che lo compongono.

Capitolo 2

Anelli di polinomi su campi

Andremo ora a considerare la situazione in cui l'anello dei coefficienti è un *campo* F. In questo ambiente possiamo definire una *norma* N su $F[x]$ definendo $N(p(x))$ pari al grado di $p(x)$, dove poniamo $N(0) = 0$. Il *grado* di un polinomio viene indicato anche con $deg(f)$ (da *degree*) con $f \in F[x]$.

Il teorema che segue mette chiaramente in luce quanto il fatto che F sia campo abbia forti ripercussioni sul suo anello dei polinomi $F[x]$.

Teorema 3. *Sia F un campo. L'anello dei polinomi $F[x]$ è un dominio euclideo. In particolare, se $a(x)$ e $b(x)$ sono due polinomi di $F[x]$ con $b(x)$ non nullo, allora esistono unici due polinomi $q(x)$ e $r(x)$ appartenenti a $F[x]$ tali che*

$$a(x) = q(x)b(x) + r(x) \text{ con } r(x) = 0 \text{ oppure } deg(r(x)) < deg(b(x)).$$

Ricordando inoltre la catena di inclusioni per le strutture algebriche da noi considerata:

$$\text{campo} \subseteq \text{dominio euclideo} \subseteq \text{dominio a ideali principali} \subseteq \text{dominio a fattorizzazione unica} \subseteq \text{dominio di integrità}$$

Possiamo quindi presentare un'ulteriore risultato, immediato dal Teorema 3, ovvero:

Corollario 4. Se F è un campo, allora $F[x]$ è un dominio a ideali principali (PID) e un dominio a fattorizzazione unica (UFD).

Dimostrazione. Segue direttamente dal Teorema (3): F campo implica $F[x]$ dominio euclideo da cui segue PID e UFD. □

2.1 Domini a fattorizzazione unica

Vedremo in dettaglio il ruolo che acquisirà l'immersione di un dominio di integrità nel suo campo delle frazioni associato.

Ricordiamo quindi che, dato R *dominio di integrità*, questo può essere immerso nel *campo delle frazioni* F ovvero $F=\{\frac{a}{b} : a \in R \text{ e } b \in R \text{ con } b \neq 0\}$. Sottolineiamo che se R è dominio di integrità allora F è sicuramente un campo; inoltre $R[x] \subseteq F[x]$ è un sottoanello e per il Teorema (3) $F[x]$ è un dominio euclideo, nonché dominio a Ideali Principali e dominio a fattorizzazione unica.

In tale prospettiva è possibile approcciarsi al calcolo in $R[x]$ facendo uso di $F[x]$. Ciò che maggiormente ci interessa è la fattorizzazione di polinomi: la possibilità di scrivere in maniera unica un polinomio come prodotto di elementi irriducibili del suo ambiente.

In $F[x]$ questo sappiamo che avviene poiché è un dominio a fattorizzazione unica. É naturale chiedersi quando questo accada anche per $R[x]$. Il primo passo che dobbiamo compiere per affrontare il problema con precisione è comparare la fattorizzazione di un polinomio in $F[x]$ con quella in $R[x]$. [4][cap.9, p.303]

Proposizione 5 (Lemma di Gauss)**.** *Sia R un dominio a fattorizzazione unica con F il suo campo delle frazioni e sia $p(x) \in R[x]$. Se $p(x)$ è riducibile in $F[x]$ allora $p(x)$ è riducibile in $R[x]$. Più precisamente, se $p(x) = A(x)B(x)$ per polinomi non costanti $A(x), B(x) \in F[x]$, allora esistono due elementi diversi da zero $r, s \in F$ tali che $rA(x) = a(x)$ e $sB(x) = b(x)$ siano polinomi in $R[x]$ e $p(x) = a(x)b(x)$.*

Dimostrazione. I coefficienti del polinomio nella parte destra dell'equazione $p(x) = A(x)B(x)$ sono elementi appartenenti al campo F, pertanto sono frazioni composte da elementi di R che è un dominio a fattorizzazione unica. Sia d un comune denominatore per tutti i coefficienti di $A(x)$ e $B(x)$, moltiplicando entrambi i membri dell'equazione per d otteniamo $dp(x) = a'(x)b'(x)$ dove ora $a'(x)$, $b'(x)$ sono elementi di $R[x]$ e d è un elemento non nullo di R. Se d è un elemento invertibile in R, che ricordiamo essere UFD e non campo, allora, ponendo $a(x) = d^{-1}a'(x)$ e $b(x) = b'(x)$, otteniamo $p(x) = a(x)b(x)$ con $a(x)$, $b(x)$ sono elementi di $R[x]$. In questo modo la proposizione è verificata. Supponiamo invece che d non sia un elemento invertibile in R. Allora poiché R è UFD possiamo scrivere d come prodotto di elementi irriducibili in R, ovvero $d = p_1p_2 \dots p_n$. Poiché p_1 è irriducibile in R, l'ideale (p_1) è *primo* quindi, per la Proposizione 2, $p_1R[x]$ è anch'esso ideale primo e di conseguenza $(R/p_1R)[x]$ è un dominio di integrità. Ora andiamo quindi a ridurre modulo p_1 l'equazione ricavata in precedenza $dp(x) = a'(x)b'(x)$ ed otteniamo $0 = (\overline{a'(x)})(\overline{b'(x)})$ nel dominio di integrità $(R/p_1R)[x]$ (con

le barre abbiamo indicato la riduzione modulo p_1 dei coefficienti dei fattori polinomiali, in particolare sono elementi dell'insieme quoziente $(R/p_1R)[x]$). Se vale $0 = (\overline{a'(x)})(\overline{b'(x)})$, uno dei due fattori deve essere zero. Supponiamo sia $\overline{a'(x)} = 0$. Ma questo significa che tutti i coefficienti di $a'(x)$ sono divisibili per p_1 e che di conseguenza anche $\frac{1}{p_1}a'(x)$ è un elemento di $R[x]$. In altri termini, abbiamo mostrato che nell'equazione $dp(x) = a'(x)b'(x)$ possiamo semplificare a sinistra e destra un fattore, che è p_1, ed ottenere nuovamente un'equazione in $R[x]$. Tale procedimento viene ripetuto per tutti i $p_2, \dots p_n$ ottenendo così $p(x) = a(x)b(x)$ con $a(x), b(x) \in R[x]$ e multipli di $A(x)$ e $B(x)$ di fattori in F, rispettivamente. Si conclude così la dimostrazione. □

Osserviamo che gli elementi di R diventano elementi invertibili nel dominio a fattorizzazione unica $F[x]$, pertanto l'unicità della fattorizzazione di un polinomio, definita a meno di elementi invertibili, cambia tra $R[x]$ e $F[x]$. Questo avviene sostanzialmente nel caso in cui un fattore irriducibile in $R[x]$ diventa invertibile in $F[x]$ come nel caso di tutti i $r \in R$ con $r \neq 0$. Il Corollario seguente chiarisce al meglio questo aspetto e fornisce un criterio di irriducibilità per polinomi su Domini a fattorizzazione unica.

Corollario 6. Sia R un dominio a fattorizzazione unica, sia F il campo delle frazioni a lui associato. Sia poi $p(x) \in R[x]$. Supponiamo che il massimo comun divisore dei coefficienti di $p(x)$ sia 1. Allora $p(x)$ è irriducibile in $R[x]$ *se e solo se* è irriducibile in $F[x]$. In particolare, se $p(x)$ è un polinomio monico che è irriducibile in $R[x]$, allora $p(x)$ è irriducibile in $F[x]$.

Dimostrazione. Usando il Lemma di Gauss dimostrato sopra, se $p(x)$ è riducibile in $F[x]$, allora è riducibile in $R[x]$. Viceversa, l'ipotesi sul massimo comun divisore dei coefficienti di $p(x)$ implica che se questo è riducibile in $R[x]$, allora $p(x) = a(x)b(x)$ dove entrambi $a(x)$ e $b(x)$ sono polinomi non costanti in $R[x]$. Questa stessa fattorizzazione mostra che $p(x)$ è riducibile in $F[x]$ (che contiene $R[x]$), completando la dimostrazione del Corollario. □

Come anticipato, andiamo adesso a trattare le relazioni tra R e l'anello di polinomi $R[x]$. Enunciamo e dimostriamo quindi un importante teorema, di cui faremo uso numerose volte. [4][cap.9, p.304]

Teorema 7. *R è un dominio a fattorizzazione unica se e solo se $R[x]$ è un dominio a fattorizzazione unica.*

Dimostrazione. É facile osservare che se $R[x]$ è dominio a fattorizzazione unica allora forza R stesso, in quanto suo sotto anello, ad essere dominio a fattorizzazione unica.

Viceversa, supponiamo che R sia dominio a fattorizzazione unica, F il suo campo delle frazioni associato e $p(x)$ un elemento non nullo di $R[x]$. Sia

poi d il massimo comun divisore dei coefficienti di $p(x)$, in questo modo $p(x) = dp'(x)$ in cui il massimo comun divisore dei coefficienti di $p'(x)$ è 1. Tale fattorizzazione di $p(x)$ è unica a meno di una variazione in d, ovvero a meno di un elemento invertibile di R. Poiché d può essere fattorizzato in modo unico come prodotto di irriducibili di R, che sono irriducibili anche in $R[x]$, questo è sufficiente per dimostrare che $p'(x)$ può essere fattorizzato solo usando elementi irriducibili in $R[x]$. Pertanto possiamo direttamente assumere che il massimo comun divisore dei coefficienti di $p(x)$ sia 1. Consideriamo inoltre il caso in cui $p(x)$ non sia un elemento invertibile di $R[x]$, ovvero che abbia grado maggiore di zero. Poiché $F[x]$ è un dominio a fattorizzazione unica (dal Corollario 4), $p(x)$ può essere fattorizzato in modo unico in irriducibili di $F[x]$. Come conseguenza del Lemma di Gauss, tale fattorizzazione implica che esiste una fattorizzazione di $p(x)$ in $R[x]$ i cui fattori sono prodotto di elementi di F e dei fattori in $F[x]$. Poiché il massimo comun divisore dei coefficienti di $p(x)$ è 1, il M.C.D. dei coefficienti in ogni fattore in $R[x]$ deve essere 1. Per il Corollario 6, ognuno di questi fattori è irriducibile in $R[x]$. Questo mostra che $p(x)$ può essere scritto come prodotto finito di elementi irriducibili in $R[x]$. Dimostrata così l'esistenza della fattorizzazione finita di $p(x)$ ci occupiamo dell'unicità di tale fattorizzazione. Supponiamo che

$$p(x) = q_1(x) \dots q_r(x) = q'_1(x) \dots q'_s(x)$$

siano due fattorizzazioni di $p(x)$ composte da elementi irriducibili in $R[x]$. Dal momento che il M.C.D. dei coefficienti di $p(x)$ è 1, questo vale anche per ognuno dei fattori di cui sopra, inoltre hanno tutti grado positivo. Per il Corollario 6, ognuno dei $q_i(x)$, $q'_j(x)$ è un irriducibile in $F[x]$. Per l'unicità della fattorizzazione in $F[x]$, $r = s$ e, dopo un opportuno riordino dei termini, possiamo affermare che $q_i(x)$ e $q'_i(x)$ sono associati in $F[x]$ per ogni $i \in \{1, \dots, r\}$. Rimane da dimostrare che sono associati anche in $R[x]$. Considerato che gli elementi invertibili di $F[x]$ sono esattamente gli elementi di $F^\star = F \setminus \{0\}$, dobbiamo prendere in considerazione il caso in cui $q(x) = \frac{a}{b}q'(x)$per certi $q(x)$, $q'(x) \in R[x]$ e a, b elementi non nulli di R, dove il massimo comun divisore dei coefficienti di entrambi i polinomi è 1. In questo caso possiamo riformulare l'equazione come $bq(x) = aq'(x)$; adesso il M.C.D. dei coefficienti del termine destro dell'equazione è a e quello del termine sinistro è b. Dal momento che R è un dominio a fattorizzazione unica, il M.C.D. dei coefficienti di un polinomio non nullo è unico a meno di elementi invertibili, $a = ub$ per un qualche u invertibile di R. In questo modo abbiamo che $q(x) = uq'(x)$ e quindi $q(x)$ e $q'(x)$ sono elementi associati anche in R. Così termina la dimostrazione del teorema. □

Ora possiamo utilizzare questo importante teorema in maniera induttiva e estendere il risultato ad anelli di polinomi in più variabili.

Corollario 8. Se R è un dominio a fattorizzazione unica, allora un anello di polinomi in un numero arbitrario di variabili su R è anch'esso un dominio a fattorizzazione unica.

Dimostrazione. Nel caso di un numero finito di variabili, il risultato segue applicando il Teorema 7 induttivamente seguendo la definizione di anello di polinomi in più variabili data preliminarmente: dal momento che un anello di polinomi in n variabili può essere visto come un anello di polinomi in una variabile con coefficienti appartenenti all'anello di polinomi in $n-1$ variabili , sullo stesso anello R. Il caso generale segue invece dalla definizione di anello di polinomi in un numero arbitrario di variabili come unione di anelli di polinomi in n variabili, al variare di tale n tra i numeri naturali. □

Capitolo 3

Polinomi in più variabili su campi e basi di Gröbner

In questo capitolo andremo a considerare il caso di anelli in più variabili a coefficienti su un campo F. L'obiettivo sarà presentare alcuni risultati teorici concernenti in primo luogo la struttura degli ideali di tali anelli e, successivamente, alcuni strumenti quali le basi di Gröbner. In particolare svilupperemo degli algoritmi per lavorare con ideali in $F[x_1, \ldots, x_n]$.

3.1 Anelli Noetheriani

Nel capitolo precedente abbiamo visto che un anello polinomiale su un campo $F[x]$ è un dominio euclideo, e il Corollario 8 ci ha permesso di notare che $F[x_1, \ldots, x_n]$ è un dominio a fattorizzazione unica (UFD). Tuttavia quest'ultimo anello non è un dominio a ideali principali. Andremo però a dimostrare che gli ideali di $F[x_1, \ldots, x_n]$, sebbene non siano principali, sono sempre finitamente generati. Ad anelli generici che presentano tale proprietà dedichiamo una notazione specifica.

Definizione 4. Un anello commutativo R con l'identità viene detto *Noetheriano* se ogni ideale di R è finitamente generato.

In analogia con la dimostrazione del Corollario 8, possiamo mostrare come $F[x_1, \ldots, x_n]$ sia Noetheriano a partire dal seguente risultato più generale.

Teorema 9 (Teorema della base di Hilbert)**.** *Se R è un anello Noetheriano allora $R[x]$ è anch'esso un anello Noetheriano.*

Dimostrazione. Sia I un ideale di $R[x]$ e sia L l'insieme di tutti i coefficienti direttori degli elementi in I. Per prima cosa andiamo a dimostrare che L è anch'esso ideale di R come segue. Dal momento che I contiene il polinomio

nullo, $0 \in L$. Siano poi $f = ax^d + \dots$ e $g = bx^e + \dots$ due polinomi in I di grado rispettivamente d ed e e coefficienti direttori $a, b \in R$. Allora, per qualsiasi $r \in R$ possono presentarsi due situazioni: o $ra - b = 0$ oppure è il coefficiente direttore del polinomio $rx^e f - x^d g$. Poiché quest'ultimo polinomio appartiene ad I, otteniamo che anche il suo coefficiente direttore appartiene ad L, ovvero che $ra - b \in L$. Considerato poi che R è assunto Noetheriano per ipotesi ne consegue che L, in quanto suo ideale, è finitamente generato ovvero esistono $a_1, a_2, \dots, a_n \in R$ tali che $L = (a_1, a_2, \dots, a_n)$. Per ogni $i = 1, \dots, n$ sia f_i un elemento di I il cui coefficiente direttore sia a_i. Sia poi denotato con e_i il grado di f_i; infine chiamiamo N il massimo tra $e_1, \dots, e_n$.

Per ogni $d \in \{0, 1, \dots, N-1\}$, sia L_d l'insieme contenente 0 e tutti i coefficienti direttori di polinomi in I di grado d. Usando una prova analoga a quella presentata per L, si mostra che L_d è ideale in R, di nuovo finitamente generato in quanto R Noetheriano. Per ogni ideale diverso da zero L_d sia $b_{d,1}, b_{d,2}, \dots, b_{d,n_d}$ un insieme di generatori per L_d, e sia infine, per ogni $i = 1, \dots, n_d$, $f_{d,i}$, un polinomio in I di grado d il cui coefficiente direttore sia $b_{d,i}$.

Il nostro obiettivo adesso è mostrare che i polinomi $f_1, \dots, f_n$ assieme a tutti i polinomi $f_{d,i}$ per tutti gli ideali diversi da zero L_d sono un insieme di generatori per I. Sia:

$$I' = (\{f_1, \dots, f_n\} \cup \{f_{d,i} | 0 \leq d < N, 1 \leq i \leq n_d\})$$

Vogliamo dimostrare che $I = I'$. Per costruzione, I' è contenuto in I dal momento che i suoi generatori sono stati scelti in I. Supponendo che $I \neq I'$, deve esistere un polinomio non nullo $f \in I$ di grado minimo tale per cui $f \notin I'$. Sia ora $d = deg(f)$ e sia a il coefficiente direttore di f.

Supponiamo inizialmente che $d \geq N$. Dal momento che $a \in L$, possiamo scrivere a come combinazione lineare con coefficienti in R di generatori di L: $a = r_1 a_1 + r_2 a_2 + \dots + r_n a_n$. Allora il polinomio $g = r_1 x^{x-e_1} f_1 + \dots + r_n x^{d-e_n} f_n$ è un elemento di I' della stesso grado di f e con il medesimo coefficiente direttore a. Consideriamo ora $f - g \in I$: è un polinomio di I con grado minore del grado di F. Per la minimalità del grado di f in I, $f - g = 0$ ovvero $f = g \in I'$, abbiamo trovato così una contraddizione.

Supponiamo poi che $d < N$. In questo caso $a \in L_d$ per qualche $d < N$, di conseguenza possiamo scrivere $a = r_1 b_{d,1} + \dots + r_{n_d} b_{d,n_d}$ per opportuni $r_i \in R$. Allora $g = r_1 f_{d,1} + \dots + r_{n_d} f_{n_d}$ è un polinomio appartenente a I' dello stesso grado e coefficiente direttore a esattamente come prima, pertanto si raggiunge una contraddizione in modo analogo.

Da tali risultati segue che $I = I'$ è finitamente generato, e dal fatto che I era un ideale qualunque, questo dimostra che $R[x]$ è Noetheriano.

□

Poiché un campo F è evidentemente Noetheriano in quanto gli unici ideali di F sono 0 e F stesso, che sono generati rispettivamente da 0 e 1, segue immediatamente il Corollario.

Corollario 10. Ogni ideale dell'anello dei polinomi $F[x_1, \ldots, x_n]$ con coefficienti appartenenti a F campo è finitamente generato.

Questo corollario garantisce così che, dato I ideale di $F[x_1, \ldots, x_n]$, esiste sempre un insieme finito di generatori di I.

3.2 Ordinamenti monomiali

La dimostrazione del Teorema della base di Hilbert è particolarmente importante, oltre al suo stesso significato, anche perché mette in luce l'importanza dei termini direttori degli elementi dell'ideale I, ai fini dello studio della sua stessa struttura. Tale dimostrazione infatti suggerisce di concentrarsi nel dettaglio nello studio di tali termini, associati al grado massimo del polinomio, nell'anello $F[x_1, \ldots, x_n]$. Per fare ciò dobbiamo specificare precisamente cosa significhi essere termine direttore in un contesto multivariato: ciò infatti non è scontato in quanto non esiste a priori un ordine tra le diverse variabili che stabilisca tra due termini chi abbia il grado maggiore, come nel più semplice caso in una sola variabile. É quindi necessario riuscire a confrontare i monomi in base al grado, ovvero conferire un ordine totale sui monomi in $F[x_1, \ldots, x_n]$.

In generale quindi definiamo:

Definizione 5 (Ordinamento monomiale)**.** Un *ordinamento monomiale* è un *buon ordinamento* " $\geq$ " sull'insieme dei monomi che soddisfa la proprietà $m\, m_1 \geq m\, m_2$ per qualsiasi $m_1 \geq m_2$ e m, m_1, m_2 monomi. Un ordinamento monomiale può essere anche descritto definendo un buon ordinamento sulle $n-$tuple $\alpha, \beta, \gamma \in \mathbb{Z}^n$ dei multigradi dei termini monomiali che soddisfi la proprietà di $\alpha + \gamma = \beta + \gamma$ se $\alpha \geq \beta$, per ogni γ.

Mostriamo che queste due definizioni sono equivalenti: siano

$$m_1 = x_1^{a_1} \ldots x_n^{a_n} \quad m_2 = x_1^{b_1} \ldots x_n^{b_n} \quad m = x_1^{c_1} \ldots x_n c_n$$

monomi in $F[x_1, \ldots, x_n]$ e α, β e γ i loro rispettivi multigradi. Osserviamo che se $\alpha \geq \beta$ allora $x_1^{a_1} \ldots x_n^{a_n} \geq x_1^{b_1} \ldots x_n^{b_n}$, ovvero $m_1 \geq m_2$. Supponiamo che $\alpha \geq \beta$ implichi $\alpha + \gamma \geq \beta + \gamma$ ovvero che

$$(a_1, \ldots, a_n) \geq (b_1, \ldots, b_n) \implies (a_1 + c_1, \ldots, a_n + c_n) \geq (b_1 + c_1, \ldots, b_n + c_n)$$

Sapendo che α, β e γ sono i multigradi dei monomi m_1, m_2 e m, scriviamo

$$x_1^{a_1+c_1} \dots x_n^{a_n+c_n} \geq x_1^{b_1+c_1} \dots x_n^{b_n+c_n}$$

da cui, riordinando i termini, otteniamo

$$x_1^{c_1} \dots x_n^{c_n} x_1^{a_1} \dots x_n^{a_n} \geq x_1^{c_1} \dots x_n^{c_n} x_1^{b_1} \dots x_n^{b_n}$$

che equivale a $m\, m_1 \geq m\, m_2$.

A seconda del contesto specifico in cui si intende operare, può essere utile scegliere un ordinamento monomiale adatto alle necessità particolari che si presentino.

Di fatto, fin'ora abbiamo già implicitamente stabilito un ordine tra le variabili semplicemente scegliendo di definire in maniera induttiva l'anello di polinomi in più variabili da noi considerato. Abbiamo infatti visto un polinomio $f \in F[x_1, \dots, x_n]$ come polinomio nella variabile x_n e coefficienti in $F[x_1, \dots, x_{n-1}]$, a loro volta polinomi nella variabile x_{n-1} e coefficienti in $F[x_1, \dots, x_{n-2}]$ e così via; tale ordinamento implicitamente introdotto è un esempio di *ordinamento lessicografico*, che vedremo ora in dettaglio.

Definizione 6. Un ordinamento monomiale *lessicografico* su $F[x_1, \dots, x_n]$ è un ordinamento monomiale che viene costruito anzitutto dichiarando un ordinamento sulle variabili, ovvero per esempio $x_1 > x_2 > \dots > x_n$, e poi dichiarando che il termine monomiale $Ax_1^{a_1} \dots x_n^{a_n}$ di esponenti $(a_1, \dots, a_n)$ è maggiore nell'ordinamento rispetto al termine $Bx_1^{b_1} \dots x_n^{b_n}$ di esponenti $(b_1, \dots, b_n)$ se per la prima componente in cui le $n-$tuple differiscono vale $a_i > b_i$.

Notiamo che questo modo di ordinare i monomi è molto simile all'ordine in cui sono classificate le parole all'interno di un dizionario, da qui il nome di ordine lessicografico.

Un piccolo esempio: sia $F[x_1, x_2]$ e " $\geq$ " ordinamento lessicografico dato da $x_1 > x_2$. Allora $x_1 \geq x_2^n$ per ogni $n \in \mathbb{N}$, $x_1^2 x_2^3 \geq x_1^2 x_2^2$.

3.3 Termini direttori e ideale dei termini direttori

Come introdotto precedentemente, definito un ordinamento tra i monomi che ci possa permettere di confrontarne i multigradi, possiamo definire cosa siano termini e coefficienti direttori, in analogia ai termini di grado massimo in una variabile.

Definizione 7. Fissato un ordinamento monomiale sull'anello dei polinomi $F[x_1, \dots, x_n]$:

1. Il *termine direttore* di un polinomio non nullo f in $F[x_1, \ldots, x_n]$, indicato con $LT(f)$ (dall' inglese *leading term*), è il termine monomiale di ordine massimo in f; inoltre il termine direttore di $f = 0$ è 0.
2. Se I è un ideale di $F[x_1, \ldots, x_n]$, l'*ideale dei termini direttori*, indicato con $LT(I)$, è l'ideale generato dai termini direttori di tutti gli elementi dell'ideale, ovvero $LT(I) = (LT(f)|f \in I)$.

Il termine direttore e il multigrado di un polinomio, che ricordiamo essere il multigrado del suo termine direttore, dipendono evidentemente dall'ordinamento monomiale scelto. In particolare, non è necessariamente vero che il termine direttore sia il termine di grado totale maggiore. Allo stesso modo, anche l'ideale dei termini direttori dipende dalla scelta dell'ordinamento.

L'ideale $LT(I)$ è un *ideale monomiale* ovvero generato da termini esclusivamente monomiali. Tali ideali presentano delle peculiarità che andiamo ad illustrare nella proposizione che segue.

Proposizione 11 (Ideali monomiali)**.** *Sia I ideale monomiale in $R = F[x_1, \ldots, x_n]$. Indichiamo con m_i dei generici monomi appartenenti a R. Allora:*

1. *Un monomio appartiene all'ideale I se, e solo se, è divisibile per uno dei monomi che generano I.*
2. *Un polinomio $f = \sum_i a_i m_i \in I$ se, e solo se, tutti i monomi m_i che lo compongono, con $a_i \neq 0$, appartengono a I.*

Come abbiamo visto nella dimostrazione del Teorema della base di Hilbert, è importante conoscere tutti i termini direttori di tutti i polinomi contenuti nell'ideale I. Se quindi $I = (f_1, \ldots, f_m)$, allora sicuramente $LT(I)$ contiene tutti i termini direttori $LT(f_1), \ldots, LT(f_m)$. Inoltre, essendo $LT(I)$ un ideale, contiene l'ideale generato da tali termini direttori ovvero:

$$(LT(f_1), \ldots, LT(f_m)) \subseteq LT(I).$$

Tuttavia, come sarà chiaro dagli esempi a seguire, l'ideale $LT(I)$ dei termini direttori è, in generale, strettamente maggiore dell'ideale generato dai termini direttori di generatori di I.

Esempio 1. Consideriamo per esempio F campo, l'anello polinomiale $F[x, y]$ e scegliamo l'ordinamento monomiale $x > y$. Siano poi $f_1 = x^3y - xy^2 + 1$ e $f_2 = x^2y^2 - y^3 - 1$, polinomi in $F[x, y]$. I rispettivi termini direttori sono $LT(f_1) = x^3y$ e $LT(f_2) = x^2y^2$, e i loro multigradi sono $\delta(f_1) = (3, 1)$ e $\delta(f_2) = (2, 2)$. Se $I = (f_1, f_2)$ è l'ideale generato da f_1 e f_2 allora l'ideale dei termini direttori $LT(I)$ contiene i termini direttori $LT(f_1)$ e $LT(f_2)$, quindi $(x^3y, x^2y^2) \subseteq LT(I)$. Dal momento che

$$g = yf_1 - xf_2 = y(x^3y - xy^2 + 1) - x(x^2y^2 - y^3 - 1) = x + y.$$

Vediamo che $g = x + y$ è un elemento di I e di conseguenza il suo termine direttore $LT(g) = x \in LT(I)$. Questo mostra che $LT(I)$ è strettamente maggiore di $(LT(f_1), LT(f_2))$: infatti, ogni elemento di $(LT(f_1), LT(f_2)) = (x^3y, x^2y^2)$ deve sempre avere grado totale pari o superiore a 4 e g ha grado totale 1.

Esempio 2. Anche scegliendo l'ordinamento monomiale opposto, $y > x$,vediamo nello stesso esempio che $LT(f_1) = -xy^2$ e $LT(f_2) = -y^3$ e $\delta(f_1) = (2, 1)$ e $\delta(f_2) = (3, 0)$. Sia $I = (f_1, f_2)$ allora $(LT(f_1), LT(f_2)) = (-y^2x, -y^3) \subset LT(I)$: analogamente all'esempio precedente considero:

$$yf_1 - xf_2 = y(x^3y - xy^2 + 1) - x(x^2y^2 - y^3 - 1) = x$$

Allo stesso modo $x \notin (LT(f_1), LT(f_2))$ in quanto ogni elemento in quest'ultimo ideale ha grado totale maggiore o uguale a 3, dimostrando così l'inclusione stretta $(LT(f_1), LT(f_2)) \subset LT(I)$.

3.4 Basi di Gröbner

Ricordiamo ora un'importante proprietà degli anelli di polinomi in una variabile e come questa perda di validità in contesto multivariato: l'unicità del resto della divisione. Per gli anelli di polinomi in una variabile, i termini direttori sono usati nell'algoritmo di divisione tra polinomi per ridurre un polinomio g modulo un altro polinomio f ottenendo un unico resto r. L'unicità di tale resto è garantita dal Teorema 3, in quanto dominio euclideo. In questo caso, tale resto $r = 0$ se e solo se g appartiene all'ideale (f). Dal momento che $F[x_1, \ldots, x_n]$ non è un dominio euclideo se $n \geq 2$, e nemmeno un PID, la situazione è decisamente più complicata rispetto ai polinomi in una variabile.

Facendo riferimento al primo esempio presentato 1, proviamo ad operare in analogia al caso in una variabile. Anzitutto vediamo che nè f_1 nè f_2 dividono g in $F[x, y]$, per considerazioni sul grado per esempio. Provando quindi a dividere g prima per uno tra f_1 e f_2 e poi per l'altro, per provare a ridurre g modulo l'ideale I, si otterrebbe un resto pari a g stesso e quindi diverso da zero. Questo, in particolare, suggerirebbe che l'elemento $g = yf_1 - xf_2$ non sia un elemento di I, quando invece lo è. Il motivo per cui il polinomio g di grado totale 1 può essere composizione lineare dei polinomi f_1 e f_2 di grado totale 4 è che i termini direttori di yf_1 e xf_2 si cancellano nella differenza: questo è il motivo per cui $LT(f_1)$ e $LT(f_2)$, come abbiamo visto sopra, non sono sufficienti per generare l'ideale dei termini direttori $LT(I)$.

Ad un insieme di generatori dell'ideale I in $F[x_1, \ldots, x_n]$ i cui termini direttori generino l'ideale dei termini direttori $LT(I)$ dedichiamo una nome speciale.

Definizione 8 (Base di Gröbner)**.** Una *base di Gröbener* per un ideale I nell'anello dei polinomi $F[x_1, \ldots, x_n]$ sul campo F è un insieme finito di generatori $\{g_1, \ldots, g_m\}$ per l'ideale I i cui termini direttori generano l'ideale di tutti i termini direttori, ovvero:

$$I = (g_1, \ldots, g_m) \quad e \quad LT(I) = (LT(g_1), \ldots, LT(g_m))$$

Per ogni ideale in $F[x_1, \ldots, x_n]$ esiste una base di Gröbner ed è possibile calcolarla seguendo un preciso algoritmo, l'algoritmo di Buchberger, come vedremo in seguito. Per ogni ideale I possono esistere molteplici basi di Gröbner

Esempio 3. Considero l'ideale $I = (f_1, f_2)$ dell'esempio 1. Come calcoleremo in seguito

$$G = \{x^3y - xy^2 + 1, x^2y^2 - y^3 - 1, x + y, y^4 - y^3 - 1\} \quad e \quad G' = \{x + y, y^4 - y^3 - 1\}$$

sono due distinte basi di Gröbner per I in $F[x, y]$ rispetto l'ordinamento $x > y$.

Si osservi che la notazione di *base* di Gröbner si riferisce ad un insieme di generatori per I, ovvero ogni elemento in I è combinazione lineare dei generatori e non nell'accezione di base di spazio vettoriale.

Una delle proprietà più importanti di una base di Gröbner, che proveremo nel teorema a seguire, è che ogni polinomio g appartenente all'anello $F[x_1, \ldots, x_n]$ può essere scritto in modo unico come somma di un elemento in I e un resto r, ottenuti da un algoritmo di divisione generale che presenteremo in dettaglio. Inoltre, vedremo che g è un elemento di I se, e solo se, il resto $r = 0$. Vedremo poi che, nonostante si trovi in generale una simile decomposizione, non usando una base di Gröbner l'unicità viene persa.

3.5 Divisione di polinomi generalizzata

Ora estenderemo l'algoritmo di divisione in una variabile ad una divisione polinomiale non canonica in più variabili: per fare ciò, fissato un ordinamento monomiale, useremo i termini direttori dei polinomi coinvolti.

Algoritmo di divisione in una variabile

Ricordiamo preliminarmente il funzionamento dell'algoritmo di divisione polinomiale canonico in una variabile. Consideriamo l'anello dei polinomi $F[x]$ sul campo F; siano poi $f(x)$ e $g(x)$ due polinomi in $F[x]$. Dividendo $f(x)$ per $g(x)$ secondo tale algoritmo di divisione, si ottengono due polinomi $q(x)$, detto *quoziente*, e $r(x)$, detto *resto* della divisione che soddisfano l'equazione

$f(x) = q(x)g(x) + r(x)$. Tale decomposizione si ottiene verificando successivamente se il termine direttore di $f(x)$ sia divisibile o meno per il termine direttore di $g(x)$: se $LT(f) = a(x)LT(g(x))$, il termine monomiale $a(x)$ viene sommato al quoziente e il procedimento viene iterato sostituendo a $f(x)$ il nuovo dividendo $f(x) - a(x)g(x)$, che è di grado inferiore poiché i termini direttori si cancellano, per la scelta di $a(x)$. Tale processo termina quando il termine direttore del divisore $g(x)$ non divide più il termine direttore del dividendo; ciò che rimane è il resto $r(x)$ della divisione.

Possiamo estendere questo procedimento alla divisione usando un numero finito di polinomi divisori in più variabili operando divisioni successive. Lo vediamo in dettaglio qui di seguito.

Algoritmo di divisione generalizzato

Algoritmo (Algoritmo di divisione polinomiale generalizzata)**.** Fissato un ordinamento monomiale sull'anello $R = F[x_1, \ldots, x_n]$, consideriamo $G = \{g_1, \ldots, g_n\}$ un insieme di polinomi appartenenti a $F[x_1, \ldots, x_n]$ non nulli. Ci riferiremo a G come all'*insieme dei divisori*. Fissiamo inoltre un ordine tra i polinomi in G, da g_1 a g_n. Sia $f \in R$. L'algoritmo di divisione generalizzato produce n polinomi $q_1, \ldots, q_n$, che indicheremo come *polinomi quozienti* e un *polinomio resto* r; inizializziamo

$$q_1 = q_2 = \cdots = q_n = 0 \quad e \quad r = 0$$

. Sia $i = 1$. L'algoritmo procede nel modo seguente:

1. Considero $LT(g_i)$: se $LT(g_i)$ divide $LT(f)$, ovvero esiste $a_i \in R$ tale che $LT(f) = a_i LT(g_i)$, sostituiamo q_i con $q_i + a_i$ e f con $f - a_i g_i$ e ripetiamo il punto 1. Osserviamo che il multigrado di $f - a_i g_i$ è inferiore al multigrado di f.

   Se invece $LT(g_i)$ non divide $LT(f)$, sostituiamo $i+1$ ad i e ripetiamo il punto 1: andiamo così a ripetere la stessa procedura ma considerando g_{i+1}, il polinomio successivo nella lista dei divisori G.

2. Se invece $LT(f)$ non è divisibile per alcun $LT(g_i)$ per ogni $1 \leq i \leq n$, sostituiamo al polinomio resto r il polinomio $r + LT(f)$ e sostituiamo a f il polinomio $f - LT(f)$. A questo punto reiteriamo il procedimento dal punto 1.

L'algoritmo termina quando il polinomio dividendo corrente f è pari a 0. Osserviamo che il processo termina in un numero finito di passi perché, ad ogni iterazione, il multigrado del termine direttore del polinomio dividendo f cala; dal momento che il minimo grado di un polinomio è 0, la procedura si arresta quando $LT(f)$ arriva ad avere multigrado pari a 0.

Alla terminazione dell'algoritmo, otteniamo un insieme di polinomi quozienti $q_1, \ldots, q_n$ e un polinomio resto r che mi permettono di scrivere il polinomio f come

$$f = q_1 g_1 + \cdots + q_n g_n + r$$

Presentiamo alcuni esempi per comprendere l'algoritmo presentato. Fissiamo l'ordinamento monomiale lessicografico $x > y$ su $F[x, y]$.

Esempio 4. Consideriamo i polinomi $f = x^3y^3 + 3x^2y^4$ e $g = xy^4$. Il termine direttore di f è $LT(f) = x^3y^3$ e non è divisibile per il termine direttore di g, che in questo caso coincide con g stesso. Andiamo quindi a sommare $LT(f)$ al resto r e reiteriamo il procedimento a $f - LT(f) = 3x^2y^4$. In questo caso il suo termine direttore è divisibile per g e vale $3x^2y^4 = (3x)LT(g)$.I due polinomi risultanti sono quindi $q = 3x$ e $r = LT(f) = x^3y^3$. Il polinomio f si può quindi scrivere come $f = qg + r = (3x)(xy^4) + x^3y^3$.

In questo esempio possiamo notare l'importanza del secondo passo dell'algoritmo di divisione generalizzato: se ci fossimo fermati dopo aver verificato che $LT(f)$ non fosse divisibile per $LT(g)$, in analogia alla divisione polinomiale in una variabile, avremmo avuto come resto della divisione l'intero polinomio f, nonostante ci fossero dei termini monomiali di f, come $3x^2y^4$, divisibili per $LT(g)$. Notiamo infine che nel caso in una variabile non è possibile incontrare un caso simile, pertanto non risulta necessario procedere con il secondo passo dell'algoritmo introdotto.

Ora andiamo a presentare un secondo esempio che sarà utile per notare un'altra criticità in cui è possibile incorrere usando la divisione generalizzata: i quozienti e il resto della divisione in generale non sono unici.

Esempio 5. Sia $f = x^2 + x - y^2 + y$, supponiamo poi $g_1 = xy + 1$ e $g_2 = x + y$. Applichiamo l'algoritmo di divisione generalizzata a f rispetto i divisiori g_1 e g_2. Nella prima iterazione, $LT(f) = x^2$ non è divisibile per $LT(g_1) = xy$ ma è divisibile per $LT(g_2) = x$. Il quoziente q_2 in questa iterazione è x e sostituiamo f con il nuovo dividendo $f - xg_2 = -xy + x - y^2 + y$. Procedendo con la seconda iterazione, $LT(f - xg_2) = -xy$ che è divisibile per $LT(g_1) = xy$ ma anche per $LT(g_2)$. Aggiornando i quozienti, otteniamo $q_1 = -1$ e $q_2 = x$ e sostituiamo nuovamente il dividendo con $(f - xg_2) - (-1)g_1 = x - y^2 + y + 1$. Alla terza iterazione, il termine direttore del dividendo non è divisibile per il termine direttore di g_1 ma è nuovamente divisibile per quello di g_2; otteniamo così i seguenti quozienti aggiornati: $q_1 = -1$ e $q_2 = x + 1$. Sostituendo per l'ultima volta il dividendo, otteniamo il nuovo dividendo $(x - y^2 + y + 1) - (1)g_2 = -y^2 + 1$. Il termine direttore di quest'ultimo dividendo non è divisibile né per $LT(g_1)$ né per $LT(g_2)$ pertanto viene aggiunto al resto r. Considerando poi $-y^2 + 1 - (-y^2) = 1$, seguendo il secondo passo dell'algoritmo, 1 non è divisibile per i termini direttori dei divisori pertanto viene aggiunto al resto r. L'algoritmo termina in quanto il

nuovo dividendo è $1 - 1 = 0$ e i risultati trovati sono: $q_1 = -1$, $q_2 = x + 1$ e $r = -y^2 + 1$. Si può quindi scrivere:

$$f = q_1 g_1 + q_2 g_2 + r = (-1)(xy + 1) + (x + 1)(x + y) + (-y^2 + 1)$$

Se invece, nello stesso esempio, scambiamo l'ordine dei divisori ovvero $g_1 = x + y$ e $g_2 = xy + 1$, cambiano anche i quozienti e il resto. In particolare, otteniamo $q_1 = x - y + 1$, $q_2 = 0$ e $r = 0$. Possiamo quindi trovare una diversa scomposizione del polinomio f come:

$$f = q_1 g_1 + q_2 g_2 + r = (x - y + 1)(x + y)$$

In questo caso è immediato notare che il polinomio $f = x^2 + x - y^2 + y$ è un elemento dell'ideale $I = (x + y, xy + 1)$ poiché il resto della divisione è $r = 0$. Tuttavia, nella prima decomposizione trovata non era affatto evidente che appartenesse all'ideale, e non avremmo potuto a priori trarre alcuna conclusione a riguardo.

Sottolineiamo che, ogni volta che otteniamo resto pari a 0, possiamo concludere che l'elemento appartenga all'ideale generato dai divisori ma in generale non possiamo affermare il viceversa: l'algoritmo di divisione generalizzato, infatti, non garantisce di ottenere resto $r = 0$, come si vede nel primo caso presentato nell'esempio.

Il teorema che andiamo ad enunciare e dimostrare di seguito mostra come queste difficoltà non si presentino se consideriamo come insieme di generatori per l'ideale I una base di Gröbner. Otterremo un unico resto r della divisione generalizzata, che potrà essere usato all'occorrenza per stabilire l'appartenenza o meno di un polinomio all'ideale I.

Teorema 12. *Fissiamo un ordinamento monomiale su $R = F[x_1, \ldots, x_n]$ e supponiamo $\{g_1, \ldots, g_m\}$ sia una base di Gröbner per l'ideale non nullo I di R. Allora:*

1. *Ogni polinomio $f \in R$ può essere scritto in modo unico nella forma*

   $$f = f_I + r$$

   dove $f_I \in I$ e nessun termine monomiale diverso da zero del resto r è divisibile per alcun termine direttore tra $LT(g_1), \ldots, LT(g_m)$.

2. *Sia f_I che r possono essere calcolati usando la divisione tra polinomi generalizzata per $g_1, \ldots, g_m$ e sono indipendenti dall'ordine in cui questi polinomi vengono usati nella divisione.*

3. *Il resto r fornisce un unico rappresentante per la classe di equivalenza di f nell'anello quoziente $F[x_1, \ldots, x_n]/I$. In particolare, $f \in I$ se e solo se $r = 0$.*

Dimostrazione. Consideriamo il risultato della divisione tra polinomi generalizzata con dividendo f e divisori $g_1, \ldots, g_m$: possiamo scrivere quindi $f = \sum_{i=1}^{m} q_i g_i + r$, con $q_1, \ldots, q_m$ quozienti e r resto della divisione. Ponendo $f_I = \sum_{i=1}^{m} q_i g_i \in I$, si fornisce direttamente una decomposizione $f = f_I + r$, per ogni insieme di generatori $g_1, \ldots, g_m$.

Viceversa, consideriamo due decomposizioni di f nella forma descritta precedentemente: $f = f_I + r = f'_I + r'$. Allora $r - r' = f_I - f'_I \in I$, quindi il suo termine direttore $LT(r - r')$ è un elemento appartenente a $LT(I) = (LT(g_1), \ldots, LT(g_m))$. Ogni elemento contenuto in questo ideale è somma di multipli dei termini monomiali $LT(g_1), \ldots, LT(g_m)$, quindi è somma di termini ognuno dei quali è divisibile per un qualche termine direttore $LT(g_i)$. Tuttavia sia r che r' sono somme di termini monomiali nessuno dei quali è divisibile per alcun termine direttore dei divisori; questa è una contraddizione a meno che $r - r' = 0$. Da ciò segue che r è unico e di conseguenza lo è anche $f_I = f - r$. Abbiamo provato così il primo asserto.

Come abbiamo appena visto, f_I e r possono essere calcolati in modo algoritmico tramite divisione polinomiale generalizzata. Dall'unicità di f_I e r dimostrata nel punto precedente, possiamo affermare che r sia indipendente dall'ordine con cui i polinomi $g_1, \ldots, g_m$ sono usati nella divisione. Analogamente $f_I = \sum_{i=1}^{m} q_i g_i$ è univocamente determinato, nonostante i quozienti q_i no siano in generale unici. Abbiamo dimostrato la seconda parte dell'enunciato del teorema.

La prima frase della terza parte dell'enunciato, dove si afferma che r è l'unico rappresentate di f nella classe di equivalenza di $F[x_1, \ldots, x_n]/I$, segue direttamente da ciò che abbiamo dimostrato fin'ora. Se poi supponiamo $r = 0$ allora $f = f_I \in I$. Viceversa, sia $f \in I$, allora $f = f + 0$ che, assieme alla unicità di r, implica $r = 0$. □

Osserviamo che, dato un ideale I di $F[x_1, \ldots, x_n]$, esistono diverse basi di Gröbner per I. Vediamo un esempio

In questa proposizione dimostriamo l'esistenza di una base di Gröbner per ogni ideale non nullo e ne diamo una caratterizzazione alternativa.

Proposizione 13. *Fissato su $R = F[x_1, \ldots, x_n]$ un ordinamento monomiale, sia I un ideale non nullo di R.*

1. *Se $g_1, \ldots, g_m$, elementi di I t.c. $LT(I) = (LT(g_1), \ldots, LT(g_m))$, allora l'insieme $\{g_1, \ldots, g_m\}$ è una base di Gröbner per I.*
2. *Esiste una base di Gröbner per I.*

Dimostrazione. Supponiamo che $g_1, \ldots, g_m$ siano elementi con la proprietà che

$$LT(I) = (LT(g_1), \ldots, LT(g_m))$$

Dobbiamo dimostrare che $g_1, \ldots, g_m$ generano l'ideale I. Possiamo scrivere $f \in I$ usando la divisione polinomiale generalizzata come

$$f = \sum_{i=1}^{m} q_i g_i + r$$

dove nessun termine monomiale contenuto in r è divisibile per $LT(g_i)$ per ogni $1 \leq i \leq m$. Dal momento che $f \in I$, abbiamo anche che $r \in I$, pertanto $LT(r) \in LT(I)$. Ma allora $LT(r)$ dovrebbe essere divisibile per almeno un $LT(g_i)$, $i \in \{1, \ldots, m\}$; questa è una contraddizione a meno che $r = 0$. Di conseguenza,

$$f = \sum_{i=1}^{m} q_i g_i$$

ovvero $\{g_1, \ldots, g_m\}$ è un insieme di generatori per I e sono quindi una base di Gröbner per I. Abbiamo provato la prima parte dell'enunciato.

Per dimostrare il secondo punto del teorema, ricordiamo anzitutto che $LT(I)$ è un ideale monomiale di $R = F[x_1, \ldots, x_n]$, in particolare

$$LT(I) = (LT(f) | f \in I)$$

Sia $S = \{LT(f) | f \in I\}$ l'insieme di generatori di I. Dal momento che $LT(I)$ è un ideale di R, anello Noetheriano, esiste un insieme finito di generatori per $LT(I)$ 4 che indichiamo con $\{p_1, \ldots, p_k\} \subset R$ tali che $I = (p_1, \ldots, p_k)$.

Dal momento che, per ogni $1 \leq i \leq k$, $p_i \in LT(I)$, esistono $a_1, \ldots, a_{q_i} \in R$ tali che

$$p_i = \sum_{j=1}^{q_i} a_j \, LT(f_j)$$

Riscrivendo tutti i p_i in questo modo abbiamo coinvolto un numero finito di elementi di S che sono sufficienti per generare tutto $LT(I)$, siano $\{LT(f_1), \ldots, LT(f_h)\}$. Vale che

$$LT(I) = (p_1, \ldots, p_k) = (LT(f_1), \ldots, LT(f_h))$$

Per il primo punto della proposizione che stiamo dimostrando, l'insieme $G = \{f_1, \ldots, f_h\}$, i cui corrispondenti termini direttori generano $LT(I)$, è una base di Gröbner per I. □

3.6 Algoritmo di Buchberger

Grazie alla Proposizione 13, abbiamo dimostrato l'esistenza di una base di Gröbner per ogni ideale I di $F[x_1, \ldots, x_n]$. Il nostro obiettivo ora diventa esibire una base di Gröbner di un dato ideale a partire da un insieme di generatori.

Presenteremo dunque un criterio che ci permetta di determinare se un dato insieme di generatori di un ideale I sia o meno una base di Gröbner; successivamente useremo tale criterio per fornire un algoritmo per determinare esplicitamente una base di Gröbner per I. Tale approccio è stato presentato per la prima volta da Bruno Buchberger nel 1965 [3, p. 535]; parleremo quindi rispettivamente di *criterio di Buchberger* e di *algoritmo di Buchberger*.

L'idea alla base è molto semplice: come abbiamo visto negli esempi precedenti, il motivo per cui vale l'inclusione stretta $(LT(f_1), \ldots, LT(f_m)) \subset LT(I)$ per certi insiemi di generatori $f_1, \ldots, f_m$ è che ci sono termini direttori in $LT(I)$ che hanno origine dalle combinazioni lineari di generatori che cancellano i termini direttori. Nelle pagine successive vedremo che i termini direttori generati in questa maniera sono l'unico ostacolo al fatto che un insieme di generatori sia base di Gröbner.

Criterio di Buchberger

Dati f_i e f_j due polinomi in $F[x_1, \ldots, x_n]$ e M il minimo comune multiplo monico tra i termini direttori $LT(f_i)$ e $LT(f_j)$, possiamo cancellare i termini direttori nel modo seguente.

Definizione 9 (S-Polinomi)**.** Dati $f_1,\ f_j \in F[x_1, \ldots, x_n]$, definiamo l'*$S$-polinomio* di f_i e f_j:

$$S(f_i, f_j) = \frac{M}{LT(f_i)} f_i - \frac{M}{LT(f_j)} f_j$$

Le combinazione lineari come quella appena introdotta sono di fondamentale importanza: da tali combinazioni infatti hanno origine tutte le possibili cancellazioni di termini direttori e saranno lo strumento principale nella costruzione delle basi cercate.

Nel lemma seguente, andremo a vedere che tali elementari combinazioni lineari, indicate con $S(f_i, f_j)$, rappresentano tutte le possibili cancellazioni di termini direttori tra polinomi dello stesso multigrado.

Lemma 14. *Supponiamo che $f_1, \ldots, f_m \in F[x_1, \ldots, x_n]$ siano polinomi con lo stesso multigrado α. Inoltre, supponiamo che la combinazione lineare*

$h = a_1 f_1 + \cdots + a_m f_m$ di costanti $a_i \in F$ abbia multigrado strettamente minore. Allora

$$h = \sum_{i=2}^{m} b_i S(f_{i-1}, f_i)$$

per alcune costanti $b_i \in F$.

Dimostrazione. Per prima cosa scriviamo tutti i polinomi come $f_i = c_i f_i'$ con $c_i \in F$ e f_i' polinomio monico di multigrado α. Abbiamo quindi

$$\begin{aligned} h = \sum_{i=1}^{m} a_i c_i f_i' &= a_1 c_1 (f_1' - f_2') + (a_1 c_1 + a_2 c_2)(f_2' - f_3') + \dots \\ &+ (a_1 c_1 + \cdots + a_{m-1} c_{m-1})(f_{m-1}' - f_m') + (a_1 c_1 + \cdots + a_m c_m) f_m'. \end{aligned}$$

Ora osserviamo che, $f_{i-1}' - f_i' = S(f_{i-1}, f_i)$. Allora, dal momento che ogni $f_{i-1}' - f_i'$, come anche h stesso, ha multigrado strettamente minore di α, segue che $a_1 c_1 + \cdots + a_m c_m = 0$, di conseguenza l'ultimo termine nella parte destra dell'equazione è 0. In questo modo possiamo riscrivere h come combinazione lineare dei polinomi f_i e f_j. □

Abbiamo gli elementi per enunciare e dimostrare il criterio di Buchberger [4][cap.9, p.324] Fissato un ordinamento monomiale su $R = F[x_1, \dots, x_n]$ e dato un insieme ordinato di polinomi $G = \{g_1, \dots, g_m\}$ in R, scriviamo che $f \equiv r \bmod G$ se r è il resto della divisione polinomiale generalizzata di $f \in R$ per $g_1, \dots, g_m$, in quest'ordine.

Proposizione 15 (Criterio di Buchberger)**.** *Sia $R = F[x_1, \dots, x_n]$ e si fissi un ordinamento monomiale su R. Se $I = (g_1, \dots, g_m)$ è un ideale non nullo di R, allora $G = \{g_1, \dots, g_m\}$ è una base di Gröbner per I se, e solo se,*

$$S(g_i, g_j) \equiv 0 \ mod\ G \quad \forall 1 \le i < j \le m$$

Dimostrazione. Dimostrare il primo verso della doppia implicazione è immediato: se infatti supponiamo $G = \{g_1, \dots, g_m\}$ sia base di Gröbner per I, allora $S(g_i, g_j) \equiv 0 \bmod G$ semplicemente perché combinazioni lineari di $g_i \in G$, elementi dell'insieme di generatori per I.

Viceversa, supponiamo che $S(g_i, g_j) \equiv 0 \bmod G$ per ogni $1 \le i < j \le m$ e consideriamo un elemento $f \in I$. Per dimostrare che G sia una base di Gröbner dobbiamo mostrare che $LT(f) \in (LT(g_1), \dots, LT(g_m))$.

Dal momento che $f \in I$, esistono m polinomi $h_1, \dots, h_m \in R$ tali che

$$f = \sum_{i=1}^{m} h_i g_i$$

Tale scrittura, ricordiamo, non è unica. Tra le varie possibili rappresentazioni, scegliamone una tale che il più grande multigrado dei termini $h_i g_i$ sia minimo, lo indicheremo con α. Osserviamo quindi che il multigrado di f è, nel caso peggiore, pari al maggiore dei multigradi dei termini della somma, ovvero $\delta(f) \leq \alpha$. Riscriviamo la somma decomponendola nel modo seguente:

$$f = \sum_{i=1}^{m} h_i g_i = \sum_{\delta(h_i g_i)=\alpha} h_i g_i + \sum_{\delta(h_i g_i)<\alpha} h_i g_i = \\ = \sum_{\delta(h_i g_i)=\alpha} LT(h_i) g_i + \sum_{\delta(h_i g_i)=\alpha} (h_i - LT(h_i)) g_i + \sum_{\delta(h_i g_i)<\alpha} h_i g_i. \quad (3.1)$$

Supponiamo ora che $\delta(f) < \alpha$. Dal momento che anche i multigradi delle ultime due somme nell'espressione 3.1 sono minori di α, anche il multigrado della prima somma deve essere minore di α. Se indichiamo con $a_i \in F$ i coefficienti dei termini monomiali $LT(h_i)$, possiamo scrivere $LT(h_i) = a_i h_i'$ con h_i' un monomio. Possiamo ora applicare il Lemma 14 alla somma $\sum a_i (h_i' g_i)$ per riscrivere la prima somma come

$$\sum_{\delta(h_i g_i)=\alpha} LT(h_i) g_i \quad = \quad \sum_{\delta(h_i g_i)=\alpha} a_i h_i' g_i \quad = \quad \sum b_i S(h_{i-1}' g_{i-1}, h_i' g_i) \quad (3.2)$$

al variare dei termini tali che $\delta(h_{i-1}' g_{i-1}) = \delta(h_i' g_i) = \alpha$.

Indichiamo ora con $\beta_{i-1,i}$ il multigrado del minimo comune multiplo monico tra $LT(g_{i-1})$ e $LT(g_i)$. Con un conto diretto si vede che $S(h_{i-1}' g_{i-1}, h_i' g_i)$ è semplicemente $S(g_{i-1}, g_i)$ moltiplicato per il monomio di multigrado $\alpha - \beta_{i-1,i}$. Il polinomio $S(g_{i-1}, g_i)$ ha multigrado minore di $\beta_{i-1,i}$ e, per ipotesi, $S(g_{i-1}, g_i) \equiv 0 \bmod G$. Questo significa che dopo aver operato la divisione polinomiale generalizzata di $S(g_{i-1}, g_i)$ per gli elementi di G, ogni $S(g_{i-1}, g_i)$ può essere scritto come somma di elementi di G e resto 0, ovvero

$$S(g_{i-1}, g_i) = \sum q_j g_j \quad con \quad \delta(q_j g_j) < \beta_{i-1,i}$$

Da questo segue che anche ogni $S(h_{i-1}' g_{i-1})$ è una somma $\sum q_j' g_j$ con $\delta(q_j' g_j) < \alpha$. Ma allora tutte le somma nel lato destro dell'espressione presentata possono essere scritte come una somma di termini nella forma $p_i g_i$ con p_i polinomi che soddisfano la condizione $\delta(p_i g_i) < \alpha$. Questo però contraddice la condizione di minimalità di α e mostra così che in realtà che $\delta(f) = \alpha$.

Se ora quindi consideriamo i termini nell'equazione 3.1 di multigrado esattamente α troviamo che

$$LT(f) = \sum_{\delta(h_i g_i)=\alpha} LT(h_i) LT(g_i)$$

Abbiamo così dimostrato che $LT(f) \in (LT(g_1), \ldots, LT(g_m))$, quindi che $G = \{g_1, \ldots, g_m\}$ è una base di Gröbner per I. □

Esempio 6. Sia $I = (x+y, y^4-y^3-1)$. $G = \{x+y, y^4-y^3-1\}$ soddisfa il criterio di Buchberger ed è una base di Gröbner per I. Vediamo infatti che

$$S(x+y, y^4-y^3-1) = \frac{xy^4}{x}(x+y) - \frac{xy^4}{y^4}(y^4-y^3-1) = xy^3 + x + y^5$$

Dividendo $xy^3 + x + y^5$ per $\{x+y, y^4-y^3-1\}$ otteniamo che

$$S(x+y, y^4-y^3-1) \equiv y(y^4-y^3-1) \equiv 0 \ mod\ G$$

pertanto G è una base di Gröbner per I.

Algoritmo di Buchberger

Come preannunciato, andiamo ora a trattare l'algoritmo di Buchberger per la costruzione di una base di Gröbner, basato sul criterio appena dimostrato.

Algoritmo (Algoritmo di Buchberger)**.** Sia I ideale di $R = F[x_1, \ldots, x_n]$ e $G = \{g_1, \ldots, g_m\}$ insieme di generatori di I.

1. Se dividendo $S(g_i, g_j)$ per $G = \{g_1, \ldots, g_m\}$ si ottiene un resto pari a 0, per ogni $1 \leq i < j \leq m$, allora G è base di Gröbner per I.
2. Se invece esiste un $S(g_i, g_j)$ che presenta un resto $r \neq 0$ della divisione per gli elementi di G, aggiungiamo a G il polinomio $g_{m+1} = r$ e reiteriamo la procedura dal primo punto.

Osserviamo che, ogni volta che aggiungiamo un nuovo elemento a G rimane comunque un insieme di generatori per I dal momento che $g_{m+1} \in I$. Tale procedura termina dopo un numero finito di passi perché ogni nuovo elemento aggiunto a G ha multigrado inferiore agli elementi da cui è stato ottenuto. Otteniamo quindi un insieme G di generatori per I che soddisfa il criterio di Buchberger, quindi una base di Gröbner.

Esempio 7. Consideriamo lo stesso esempio 1: calcoliamo una base di Gröbner per $I = (f_1, f_2)$ usando l'algoritmo di Buchberger. Abbiamo

$$f_1 = x^3y - xy^2 + 1 \quad e \quad f_2 = x^2y^2 - y^3 - 1 \in F[x,y] \quad con \quad x > y$$

Anzitutto applichiamo il criterio di Buchberger per verificare se G sia o meno base di Gröbner per I. Il minimo comune multiplo monico tra f_1 e f_2 è $M = x^3y^2$. Abbiamo quindi

$$S(f_1, f_2) = \frac{x^3y^2}{x^3y}(x^3y - xy^2 + 1) - \frac{x^3y^2}{x^2y^2}(x^2y^2 - y^3 - 1) = x + y \not\equiv 0 \ mod\ G$$

Per il criterio di Buchberger, G non è base di Gröbner; aggiorniamo quindi G aggiungendo $f_3 = x + y$ ed otteniamo

$$G' = \{f_1, f_2, f_3\}$$

Reiteriamo il procedimento dal primo passo. Osserviamo che ora non è necessario ricalcolare il primo S-polinomio dal momento che non varia aggiungendo f_3 a G. Abbiamo quindi $S(f_1, f_2) = f_3 \equiv 0 \ mod \ G'$.

$$S(f_1, f_3) = -x^2y^2 - xy^2 + 1 \equiv x^3y - xy^2 + 1 = f_1 \equiv 0 \ mod \ G'$$

$$S(f_2, f_3) = -xy^3 - y^3 - 1 \equiv y^4 - y^3 - 1 \ mod \ G'$$

Aggiorniamo nuovamente G' aggiungendo il quarto polinomio

$$f_4 = y^4 - y^3 - 1$$

. Otteniamo quindi

$$G'' = \{f_1, f_2, f_3, f_4\}$$

Calcoliamo nuovamente gli S-polinomi per G''; gli unici che dobbiamo calcolare sono quelli che coinvolgono f_4. Con brevi conti si ottiene che

$$S(f_1, f_4) \equiv 0 \ mod \ G \quad S(f_2, f_4) \equiv 0 \ mod \ G \quad S(f_3, f_4) \equiv 0 \ mod \ G$$

Per il Criterio di Buchberger possiamo concludere che G'' è una base di Gröbner per I.

Osserviamo ora che se $G = \{g_1, \ldots, g_m\}$ è una base di Gröbner per I ed esiste i tale che $LT(g_i)$ è divisibile per $LT(g_j)$ per un $j \neq i$, allora vale che

$$LT(I) = (LT(g_k) \,|\, 1 \leq k \leq m, \, k \neq i)$$

Di conseguenza grazie alla Proposizione 13 posso escludere g_i dall'insieme G ed ottenere ugualmente una base di Gröbner per I.

Inoltre, assumiamo senza perdita di generalità che per ogni $1 \leq i \leq m$ i $LT(g_i)$ siano monici, dal momento che stiamo lavorando con coefficienti sul campo F. Di conseguenza possiamo definire una base di Gröbner con tali caratteristiche.

Definizione 10 (Base minimale di Gröbner)**.** Una base di Gröbner per I $\{g_1, \ldots, g_m\}$ in cui ogni $LT(g_i)$ è monico e ogni $LT(g_i)$ non è divisibile per nessun $LT(g_j)$ per $i \neq j$ è detta *base minimale di Gröbner*.

Esempio 8. Riferendoci ai risultati dell'ultimo esempio 7, ricaviamo da G'' una base minimale di Gröbner eliminando gli elementi nell'insieme di generatori G'' il cui termine direttore è divisibile per altri termini direttori. Otteniamo una base minimale

$$G = \{f_3, f_4\} = \{x + y, y^4 - y^3 - 1\}$$

Una base minimale di Gröbner non è unica. Vediamo infatti la seguente proposizione.

Proposizione 16. *Una base di Gröbner $G = \{g_1, \dots, g_m\}$ per I è minimale se, e solo se, non esiste un sottoinsieme proprio di $\{LT(g_1), \dots, LT(g_m)\}$ che possa generare $LT(I)$, ovvero $\{LT(g_1), \dots, LT(g_m)\}$ è un insieme minimale di generatori per $LT(I)$ rispetto l'inclusione insiemistica.*

Inoltre, due basi minimali di Gröbner per uno stesso ideale I hanno lo stesso numero di elementi.

Dimostrazione. Sia $G = \{g_1, \dots, g_m\}$ una base minimale di Gröbner per I. Supponiamo per assurdo che esista un sottoinsieme proprio dell'insieme di generatori $\{LT(g_1), \dots, LT(g_m)\}$ capace di generare $LT(I)$. In particolare, esiste un $i \in \{1, \dots, m\}$ tale che

$$LT(I) = (LT(g_j) \,|\, 1 \leq j \leq m,\, j \neq i)$$

Poiché $g_i \in I$, $LT(g_i) \in LT(I)$. Di conseguenza, $LT(g_i) = \sum_{j \neq i} a_j LT(g_j)$: vediamo quindi che $LT(g_i)$ è divisibile per almeno un $LT(g_j)$ con $j \neq i$. Questo è assurdo dal momento che stiamo assumendo G base minimale di Gröbner per I.

Viceversa, sia $\{LT(g_1), \dots, LT(g_m)\}$ un insieme di generatori minimale per $LT(I)$ rispetto l'inclusione insiemistica. Supponiamo per assurdo che $G = \{g_1, \dots, g_m\}$ non sia una base di Gröbner minimale ovvero che esista un elemento $LT(g_i) \in \{LT(g_1), \dots, LT(g_m)\}$ divisibile per un altro elemento $LT(g_j)$ nello stesso insieme di generatori per $LT(I)$. Allora varrebbe che

$$LT(I) = (LT(g_j) \,|\, j \neq i)$$

Avremmo ottenuto un insieme di generatori per $LT(I)$ incluso strettamente in $\{LT(g_1), \dots, LT(g_m)\}$. Questo sarebbe assurdo avendo supposto tale insieme di generatori per $LT(I)$ minimale rispetto l'inclusione.

Infine, date $G = \{g_1, \dots, g_m\}$ e $H = \{h_1, \dots, h_k\}$ due basi minimali di Gröbner per I abbiamo che

$$LT(I) = (LT(g_1), \dots, LT(g_m)) = (LT(h_1), \dots, LT(h_k))$$

Usando ciò che abbiamo appena visto, sappiamo che $\{LT(g_1), \dots, LT(g_m)\}$ e $\{LT(h_1), \dots, LT(h_k)\}$ sono insiemi minimali di generatori per $LT(I)$ pertanto sono uguali e presentano lo stesso numero di elementi. □

Capiamo quindi che, potendo trovare polinomi diversi con lo stesso termine direttore, possiamo allo stesso modo avere anche diverse basi minimali di Gröbner per lo stesso ideale.

Esempio 9. Sia $G = \{x^2+xy^2, x^2-y^3, y^3-y^2, xy^2+y^2\}$ una base di Gröbner per $I = (x^2 + xy^2, x^2 - y^3, y^3 - y^2)$. Ricaviamo da G una base di Gröbner minimale per I: notiamo che $LT(x^2 + xy^2)$ è divisibile per $LT(x^2 - y^3)$, pertanto possiamo scartare x^2+xy^2 dall'insieme di generatori G. Otteniamo una base minimale

$$G' = \{x^2 - y^3, y^3 - y^2, xy^2 + y^2\}$$

Se invece decidiamo di eliminare il secondo elemento di G, otteniamo una diversa base minimale per I

$$G'' = \{x^2 + xy^2, y^3 - y^2, xy^2 + y^2\}$$

G' e G'' sono due distinte basi minimale di Gröbner per l'ideale I rispetto all'ordinamento monomiale $x > y$.

Vediamo ora che rafforzando ulteriormente alcune condizioni possiamo ottenere un'importante proprietà di unicità.

Definizione 11 (Base di Gröbner ridotta)**.** Fissiamo un ordinamento monomiale su $R = F[x_1, \ldots, x_n]$. Una base di Gröbner $\{g_1, \ldots, g_m\}$ per l'ideale non nullo I di R è detta *base di Gröbner ridotta* se:

1. ogni g_i ha termine direttore monico, ovvero $LT(g_i)$ è monico, per ogni $i = 1, \ldots, m$
2. nessun termine in g_i è divisibile per alcun $LT(g_j)$ con $i \neq j$.

Si osservi che una base di Gröbner ridotta è anche una base minimale per I.

Ora proviamo a trovare un modo per ricavare una base ridotta da una data base minimale di Gröbner per un ideale I. Osserviamo che, usando la divisione polinomiale generalizzata, possiamo raggiungere tale scopo. Sia $G = \{g_1, \ldots, g_m\}$ una base minimale di Gröbner per I e i tale che $1 \leq i \leq m$, per ogni $j \neq i$ dividiamo g_i per g_j: abbiamo ottenuto un polinomio r_i, resto della divisione polinomiale generalizzata. Dal momento che G è base di Gröbner minimale, sappiamo che $LT(r_i) = LT(g_i)$ e che nessun termine monomiale in r_i è divisibile per nessun altro $LT(g_j)$, $j \neq i$. Procedendo in questo modo per tutti gli elementi $g_i \in G$, l'insieme

$$G' = \{r_i \,|\, 1 \leq i \leq m\}$$

è una base ridotta di Gröbner per lo stesso ideale I. Infatti, grazie alla Proposizione 13 sappiamo che

$$LT(I) = (LT(g_1), \ldots, LT(g_m)) = (LT(r_1), \ldots, LT(r_m))$$

e da questo segue che G' è base di Gröbner per I. Inoltre tale base G' è ridotta per le proprietà che presentano i polinomi resto della divisione polinomiale.

Vediamo ora un importante teorema che garantisce l'unicità di una base di Gröbner ridotta per un ideale.

Teorema 17. *Fissiamo un ordinamento monomiale su $R = F[x_1, \ldots, x_n]$. Sia I ideale non nullo in R. Allora esiste un unica base di Gröbner ridotta per I.*

Dimostrazione. Come visto nella proposizione 16, due basi ridotte per I hanno lo stesso numero di elementi e stessi termini direttori, dal momento che sono anche basi minimali di Gröbner. Consideriamo quindi due basi ridotte $G = \{g_1, \ldots, g_m\}$ e $G' = \{g'_1, \ldots, g'_m\}$ per lo stesso ideale non nullo I. Dopo aver operato opportuni scambi, possiamo affermare che $LT(g_i) = LT(g'_i) = h_i$ per $i = 1, \ldots, m$. Per ogni i possiamo considerare il polinomio $f_i = g_i - g'_i$. Se $f_i \neq 0$ allora, poiché $f_i \in I$, il suo termine direttore deve essere divisibile per qualche h_j. Per definizione di base ridotta, h_j, per $j \neq i$, non divide alcun termine né in g_i né in g'_i, pertanto non divide anche $LT(f_i)$. Inoltre, nemmeno h_i stesso divide $LT(f_i)$ poiché tutti i termini di f_i hanno multigrado strettamente minore. Concludiamo quindi che può essere solamente $f_i = g_i - g'_i = 0$; di conseguenza $g_i = g'_i$ per tutti $i = 1, \ldots, m$ ovvero $G = G'$. □

Esempio 10. Nell'esempio 7 $G = \{f_3, f_4\} = \{x + y, y^4 - y^3 - 1\}$ è la base ridotta di Gröbner per l'ideale I rispetto l'ordinamento monomiale $x > y$: ogni termine monomiale di f_3 non è divisibile per $LT(f_4) = y^4$ e ogni termine di f_4 non è divisibile per $LT(f_3) = x$.

Esempio 11. Riprendendo l'esempio 9 consideriamo

$$G' = \{x^2 - y^3, y^3 - y^2, xy^2 + y^2\}$$

base minimale di Gröbner per $I = (x^2 + xy^2, x^2 - y^3, y^3 - y^2)$.

Ricaviamo da G' la base ridotta di Gröbner per I rispetto all'ordinamento $x > y$: osserviamo che $x^2 - y^3$ presenta un termine monomiale divisibile per $LT(y^3 - y^2) = y^3$. Dividiamo $x^2 - y^3$ per $\{y^3 - y^2, xy^2 + y^2\}$

$$x^2 - y^3 = y^3 - y^2 + x^2 + y^2 \equiv x^2y^2 \ mod\ G$$

Sottolineiamo che $x^2 + y^2$ è il resto della divisione polinomiale generalizzata. Sostituiamo il polinomio $x^2 - y^3$ con il resto della divisione e otteniamo la base ridotta di Gröbner per I

$$G'' = \{x^2 + y^2, y^3 - y^2, xy^2 + y^2\}$$

Capitolo 4

Basi di Gröbner: applicazioni

In quest'ultimo capitolo vedremo alcune applicazioni delle basi di Gröbner. Il primo argomento che introdurremo sarà un metodo per la risoluzione di sistemi di equazioni algebriche basato sul principio di eliminazione; successivamente porremo l'accento su alcuni metodi computazionali per operare con gli ideali.

4.1 Teoria dell'eliminazione

Uno dei principali utilizzi della teoria delle basi di Gröbner è la risoluzione esplicita di sistemi di equazioni algebriche: rappresenta un importante strumento di calcolo e costituisce le fondamenta dei programmi di risoluzione di sistemi di equazioni algebriche implementati nei calcolatori [1][cap.6, p.243].

Supponiamo che $S = \{f_1, \ldots, f_m\}$ sia un insieme di polinomi nelle variabili $x_1, \ldots, x_n$ e che stiamo cercando la soluzione del sistema di equazioni

$$f_1 = 0,\ f_2 = 0, \ldots,\ f_m = 0$$

Una soluzione del sistema dato è una $n-$tupla $(a_1, \ldots, a_n)$ tale che

$$f_i(a_1, \ldots, a_n) = 0 \quad \textit{per ogni} \quad i = 1, \ldots, m$$

Osserviamo che se $(a_1, \ldots, a_n)$ è una generica soluzione del sistema in esame, allora $f(a_1, \ldots, a_n) = 0$ per ogni $f \in I$, con I ideale generato dagli elementi in S. Inoltre, dato $S' = \{g_1, \ldots, g_s\}$, un *qualsiasi* insieme di generatori per I, allora l'insieme delle soluzioni del sistema dato dalle equazioni algebriche $g_1 = 0, \ldots, g_s = 0$ presenta il medesimo insieme di soluzioni associato ad S.

Queste osservazioni permettono di capire quale sia quindi la tecnica di risoluzione verso cui siamo diretti: usare le basi di Gröbner per dare un insieme di generatori conveniente ai fini del calcolo, dal momento che l'insieme delle soluzioni rimane invariato.

Eliminazione di Gauss-Jordan: sistemi lineari

Ricordiamo ora brevemente la tecnica di risoluzione nel caso *lineare*: nella situazione in cui $f_1, \ldots, f_m$ sono polinomi lineari, una soluzione del sistema di equazioni può essere ottenuta eliminando una ad una le variabili coinvolte tramite semplici combinazioni lineari delle equazioni, generando un sistema di equazioni di facile risoluzioni in forma triangolare.

Tale metodo viene indicato in algebra lineare come *eliminazione di Gauss-Jordan.*

Eliminazione: sistemi algebrici

Andando ora ad affrontare il medesimo problema ma in cui $S = \{f_1, \ldots, f_m\}$ è composto da polinomi algebrici, non più lineari, la situazione intuitivamente si complica, tuttavia il principio di eliminazione alla base rimane il medesimo.

Infatti, se è possibile determinare un polinomio, $p(x_n) \in I$ dipendente esclusivamente da una variabile, in questo caso stiamo supponendo senza perdita di generalità x_n, possiamo calcolare esplicitamente la soluzione relativa all'ultima variabile, ovvero l'ultima coordinata a_n della $n-$upla soluzione: questa è infatti soluzione dell'equazione $p(x_n) = 0$. Se poi esiste un polinomio nelle variabili x_{n-1} e x_n che indichiamo con $q(x_{n-1}, x_n)$, allora troviamo le soluzioni relative alla penultima variabile come soluzione dell'equazione $q(x_{n-1}, a_n) = 0$ nella sola variabile x_{n-1}, in cui utilizziamo le soluzioni trovate precedentemente.

In questo modo possiamo successivamente determinare polinomi in I che vadano ad eliminare le variabili $x_1, \ldots, x_n$ determinando esplicitamente tutte le soluzioni del sistema considerato. Tale approccio alla risoluzione di sistemi algebrici viene indicato come *teoria dell'eliminazione.*

Nel procedimento di eliminazione descritto è evidente l'importanza di determinare elementi dell'ideale I che non coinvolgano determinate variabili. Introduciamo una notazione specifica.

Definizione 12 (i-esimo ideale di eliminazione di I)**.** Se I è un ideale di $F[x_1, \ldots, x_n]$ allora

$$I_i = I \cap F[x_{i+1}, \ldots, x_n]$$

è detto l'*i-esimo ideale di eliminazione* di I rispetto all'ordinamento monomiale $x_1 > x_2 > \cdots > x_n$

Appare chiaro a questo punto che la convenienza di usare il metodo di eliminazione per risolvere sistemi algebrici dipende dalla capacità di determinare tali ideali di eliminazione.

Le basi di Gröbner acquisiscono così un ruolo fondamentale, come vediamo nella proposizione seguente.[4][cap.9, p.328]

Proposizione 18 (Eliminazione)**.** *Supponiamo che $G = \{g_1, \ldots, g_m\}$ sia una base di Gröbner per l'ideale I di $F[x_1 \ldots, x_n]$, fissato l'ordinamento monomiale lessicografico $x_1 > \cdots > x_n$. Allora*

1. *$G \cap F[x_{i+1}, \ldots, x_n]$ è base di Gröbner dell'i-esimo ideale di eliminazione di I, $I_i = I \cap F[x_{i+1}, \ldots, x_n]$.*
2. *$I \cap F[x_{i+1}, \ldots, x_n] = 0$ se, e solo se, $G \cap F[x_{i+1}, \ldots, x_n] = \emptyset$.*

Dimostrazione. Indichiamo con $G_i = G \cap F[x_{i+1}, \ldots, x_n]$. Certamente $G_i \subseteq I_i$, per dimostrare che G_i sia base di Gröbner per I_i utilizziamo la Proposizione 13: sarà sufficiente dimostrare che $LT(I_i)$ sia generato dai termini direttori degli elementi in G_i.

Di sicuro $(LT(G_i)) \subseteq LT(I_i)$. Per dimostrare l'inclusione opposta, consideriamo anzitutto un elemento $f \in I_i$; di certo $f \in I$ e, dal momento che G è base di Gröbner per I, è possibile scrivere $LT(f)$ nel modo seguente

$$LT(f) = a_1(x_1, \ldots, x_n)LT(g_1) + \cdots + a_m(x_1, \ldots, x_n)LT(g_m)$$

per $a_1, \ldots, a_m \in F[x_1, \ldots, x_n]$. Se poi scriviamo ogni polinomio a_i come somma dei suoi termini monomiali, possiamo vedere $LT(f)$ come una somma di elementi del tipo

$$\sum_i a x_1^{d_{i_1}} \ldots x_n^{d_{i_n}} LT(g_i)$$

scomponendolo quindi in una combinazione di certi $LT(g_i)$. Dal momento che $f \in F[x_{i+1}, \ldots, x_n]$, la somma dei suoi termini contenenti le variabili $x_1, \ldots, x_i$ deve essere 0, quindi $LT(f)$ è somma di termini monomiali contenenti solo le ultime $n - i$ variabili, $x_{i+1}, \ldots, x_n$. Ciò implica che $LT(f)$ può essere scritto come combinazione lineare, con coefficienti in $F[x_{i+1}, \ldots, x_n]$, di alcuni termini monomiali $LT(g_j)$, dove tali $LT(g_j)$ non coinvolgono le variabili $x_1, \ldots, x_i$. Ora ricordiamo però che avendo fissato l' ordinamento monomiale lessicografico, se i $LT(g_j)$ non coinvolgono le prime i variabili, allora anche tutti i termini di multigrado inferiore devono necessariamente non contenere $x_1, \ldots, x_i$. Di conseguenza, anche $LT(f)$ può essere scritto come combinazione lineare di elementi in $LT(G_i)$ a coefficienti in $F[x_{i+1}, \ldots, x_n]$, dimostrando la proposizione. □

Di seguito presentiamo alcuni esempio esplicativi del metodo di eliminazione.

Esempio 12 (Ricerca esplicita di punti di intersezione)**.** Sia $I = (x^2 + xy + y^2 - 1, x^2 + 4y^2 - 4)$ un ideale di $F[x, y]$, fissato l'ordinamento monomiale $x > y$. Dopo aver calcolato una base di Gröbner per l'ideale I, andiamo a

cercare i punti di intersezione tra l'ellisse di equazione $f_1 : x^2+xy+y^2-1 = 0$ e l'ellisse di equazione $f_2 : x^2 + 4y^2 - 4 = 0$, nel piano $\mathbb{R}^2$, sfruttando la base appena ottenuta.

Il nostro obiettivo è cercare l'ideale di eliminazione di x in modo da ottenere una base in cui non compaia la prima variabile, avendo modo così di calcolare esplicitamente le soluzioni rispetto a y.

Anzitutto, applichiamo l'algoritmo di Buchberger a $G = \{f_1, f_2\}$: vediamo subito che $S(f_1, f_2) = f_1 - f_2 \equiv xy - 3y^2 + 3 \bmod \{f_1, f_2\}$. Aggiungiamo quindi $f_3 = xy - 3y^2 + 3$ alla lista di generatori: $G = \{f_1, f_2, f_3\}$.

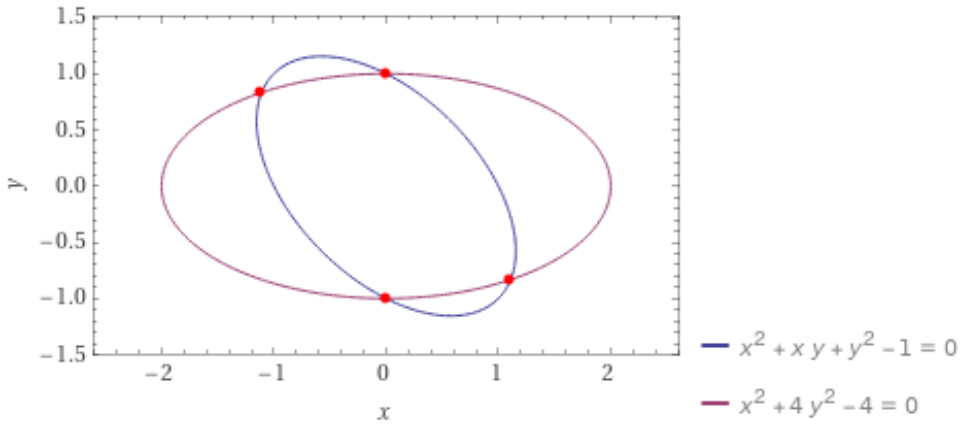
Ora, calcoliamo $S(f_1, f_3) = 4xy^2 - 3x + y^3 - y$ e lo riduciamo modulo G: dopo aver applicato la divisione generalizzata, otteniamo $S(f_1, f_3) \equiv f_4 = -3x+13y^3-13y \bmod G$. Denominiamo $f_4' = x-\frac{13}{3}y^3+\frac{13}{3}y$ e lo aggiungiamo a G in quanto nessun termine di f_4 è divisibile per alcun termine direttore degli elementi in G. A questo punto, pertanto, $G = \{f_1, f_2, f_3, f_4\}$.

Calcoliamo infine $S(f_1, f_4) = 13xy^3 - 10xy + 3y^2 - 3 \equiv 13y^4 - 22y^2 + 9 \bmod G$. Indichiamo con $f_5 = 13y^4 - 22y^2 + 9$. Con brevi conti, vediamo che $G' = \{f_1, f_2, f_3, f_4, f_5\}$ è una base di Gröbner per I dal momento che $S(f_i, f_j) \equiv 0 \bmod G'$ per $1 \leq i < j \leq 5$. Inoltre, posso eliminare alcuni elementi di G' in modo da ottenere la base di Gröbner ridotta per I che indicheremo con $G = \{f_4', f_5'\}$, in cui f_4' e f_5' sono monici: abbiamo tolto f_1, f_2, f_3 perché i loro termini direttori sono divisibili per il termine direttore $LT(f_4') = x$. Abbiamo così che $I = (-3x + 13y^3 - 13y, 13y^4 - 22y^2 + 9)$ e il primo ideale di eliminazione di I per x è $I_1 = (f_5)$ in virtù della Proposizione 18, essendo elementi di una base di Grb̈ner in cui non compare la prima variabile.

Possiamo quindi calcolare le soluzioni del sistema $f_1 = 0$, $f_2 = 0$ usando il primo ideale di eliminazione per I, I_1, ideale di eliminazione per x. Da $f_5 = 13y^4 - 22y^2 + 9 = 0$ otteniamo quattro soluzioni per y: $y_1 = 1$, $y_2 = -1$, $y_3 = \frac{3\sqrt{13}}{13}$ e $y_4 = \frac{-3\sqrt{13}}{13}$. Sostituendo le y_i ottenute nell'equazione $f_4 = -3x + 13y^3 - 13y = 0$, abbiamo determinato le coordinate dei quattro punti di intersezione tra le due ellissi: rispettivamente,

$$P_1 = (0, 1) \quad P_2 = (0, -1) \quad P_3 = (\frac{-4\sqrt{13}}{13}, \frac{3\sqrt{13}}{13}) \quad e\ P_4 = (\frac{4\sqrt{13}}{13}, \frac{-3\sqrt{13}}{13})$$

come in figura.



Esempio 13 (Colorare grafi con n colori)**.** Un altro esempio di applicazione della teoria delle basi di Gröbner è il problema di colorare un grafo Γ a N vertici non orientato usando n colori: ci chiediamo se sia possibile colorare i vertici del grafo considerato in modo che ogni coppia di vertici connessi da un arco abbia tra loro colorazioni differenti. Tale problema può avere una soluzione esplicita, nessuna, ma anche molteplici a seconda del grafo e dal numero di colori considerato.

Iniziamo a modellizzare il problema [4][cap.9 p.335]: sia F un campo con almeno n elementi, introduciamo una variabile x_i per ogni vertice i e rappresentiamo gli n colori scegliendo un insieme S di n elementi distinti nel campo F. Una colorazione ammissibile del grafo sarà quindi composta dalle assegnazioni $x_i = \alpha_i$ per ogni $i = 1, \dots, N$ in cui $\alpha_i \in S$ e $\alpha_i \neq \alpha_j$ se i vertici i e j sono connessi da un arco del grafo Γ, che indicheremo con $(i, j) \in \Gamma$.

Sia ora $f(x) = \prod_{\alpha \in S}(x - \alpha_i)$: questo polinomio ha grado n in $F[x]$ e le sue radici sono tutti e soli gli elementi di S. Dal momento che $x_i = \alpha_i$ per qualche $\alpha_i \in S$, $f(x_i) = 0$ per ogni $i = 1, \dots, N$. Scrivere poi che $\alpha_i \neq \alpha_j$ è equivalente a richiedere che $f(x_i) = f(x_j)$ con $x_i \neq x_j$. In altri termini, richiedere che due vertici connessi da un arco siano colorati in modo diverso equivale a porre che, per ogni coppia di vertici connessi (i, j), x_i e x_j soddisfino l'equazione $g(x_i, x_j) = 0$, con $g(x_i, x_j) = \frac{f(x_i) - f(x_j)}{x_i - x_j} \in F[x_i, x_j]$.

Di conseguenza, risolvere il problema di colorare i vertici del grafo Γ con n colori equivale a risolvere il sistema di equazioni seguente:

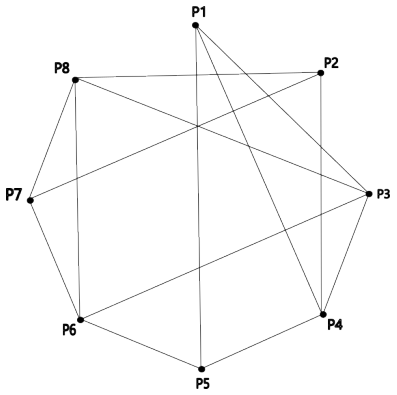
$$\begin{cases} f(x_i) = 0, \quad per\, i = 1, \dots, N \\ g(x_i, x_j) = 0, \forall\, (i, j) \in \Gamma \end{cases}$$

Possiamo a questo punto risolvere questo sistema con la teoria dell'eliminazione, sfruttando le basi di Gröbner.

Sia I l'ideale generato da $f(x_i)$ per $i = 1, \ldots, N$ e da $g(x_i, x_j)$ per ogni arco $(i, j) \in \Gamma$. Per il Teorema degli zeri di Hilbert [4][p.701], se I non è un ideale proprio di $F[x_1, \ldots, x_N]$, ovvero se la base di Gröbner ridotta di I è $\{1\}$, il problema non ammette alcuna soluzione. Quando invece I è un ideale proprio, esiste almeno una colorazione dei vertici conforme alle richieste del problema

Consideriamo un esempio esplicito. Sia Γ il grafo in figura; presenta 8 vertici e 14 archi : $(1,3), (1,4), (1,5), (2,4), (2,7), (2,8), (3,4), (3,6), (3,8), (4,5), (5,6), (6,7), (6,8), (7,8)$. Vogliamo colorarne i vertici con tre colori, rosso, verde e blu. Attribuiamo ai colori gli elementi del campo su 3 elementi $\mathbb{F}_3 = \{0, 1, 2\}$ nel modo seguente: rosso= 0, verde= 1 e blu= 2.

Figura 4.1: Il grafo Γ



Costruiamo il sistema di equazioni per risolvere il problema. Anzitutto, non è restrittivo assumere che il primo vertice sia colorato di rosso, ovvero $x_1 = 0$. Sia poi

$$f(x) = \prod_{\alpha_i \in \mathbb{F}_3} (x - \alpha_i) = x(x-1)(x-2) = x^3 + 2x = x^3 - x$$

dal momento che $f(x) \in \mathbb{F}_3[x]$. Calcoliamo ora

$$\begin{aligned} g(x_i, x_j) &= \frac{f(x_i) - f(x_j)}{x_i - x_j} = \frac{x_i^3 - x_i - x_j^3 + x_j}{x_i - x_j} = \frac{x_i^3 - x_j^3}{x_i - x_j} - \frac{x_i - x_j}{x_i - x_j} \\ &= \frac{(x_i - x_j)^3}{x_i - x_j} - 1 = x_i^2 + x_i x_j + x_j^2 - 1 \end{aligned}$$

ricordando che $x_i^3 - x_j^3 = (x_i - x_j)^3$ in $\mathbb{F}_3[x_i, x_j]$. Il sistema di equazioni che dobbiamo risolvere è quindi:

$$\begin{cases} x_1 = 0 \\ x_i^3 - x_i = 0, \quad \forall\, i \quad 2 \leq i \leq 8 \\ x_i^2 + x_i x_j + x_j^2 - 1 = 0, \quad \forall\, (i,j) \in \Gamma \end{cases}$$

Calcoliamo nel modo descritto dall'algoritmo di Buchberger una base di Gröbner per I, ideale generato dai polinomi x_1, $f(x_i)$ e $g(x_i, x_j)$, per ogni $2 \leq i \leq 8$ e per tutti gli archi $(i, j) \in \Gamma$, nel rispetto dell'ordinamento $x_1 > x_2 > \cdots > x_8$ e poi ne ricaviamo la base ridotta

$$G = \{x_1, x_2, x_3 + x_8, x_4 + 2x_8, x_5 + x_8, x_6, x_7 + x_8, x_8^2 + 2\}$$

Le soluzioni del sistema sono quindi due: dall'ultimo elemento di G otteniamo l'equazione $x_8^2 + 2 = 0$ da cui $x_8 = 1$ oppure $x_8 = -1 = 2$ in $\mathbb{F}_3[x_8]$. Scriviamo quindi le due soluzioni. Se $x_8 = 1$ allora la soluzione è:

$$x_1 = x_2 = x_6 = 0,\ x_3 = 2,\ x_4 = 1,\ x_5 = 2,\ x_7 = 2,\ x_8 = 1$$

Nell'altro caso invece:

$$x_1 = x_2 = x_6 = 0,\ x_3 = 1,\ x_4 = 2,\ x_5 = 1,\ x_7 = 1,\ x_8 = 2$$

Figura 4.2: La prima colorazione di Γ

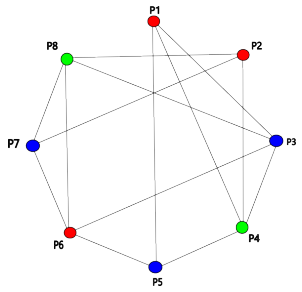
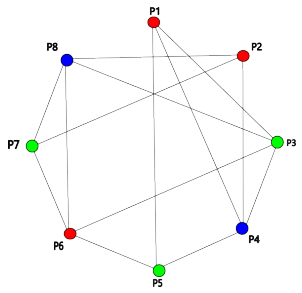


Figura 4.3: La seconda colorazione di Γ



Esempio 14 (Sudoku come grafo)**.** Mostriamo adesso come si possa usare la risoluzione del problema appena descritto di come colorare i vertici di un grafo, per interpretare e risolvere altri quesiti.

Nell'esempio che presentiamo diamo un'interpretazione del gioco del Sudoku come grafo ed impostiamo la sua risoluzione in termini adatti all'uso della

teoria dell'eliminazione [5]. Sudoku è un rompicapo molto noto e diffuso che consiste in una griglia di caselle 9×9 divisa in 9 regioni 3×3. L'obiettivo del gioco è riempire ogni riga, colonna e sotto tabella 3×3 con i numeri da 1 a 9, senza ripetizioni. Se un Sudoku è elaborato in maniera corretta ammette un unica soluzione possibile. Possiamo esprimere il gioco del Sudoku come un problema di colorazione di grafo non orientato nel modo seguente:

1. Il grafo ha 81 vertici, uno per ogni cella, a cui vengono associate le variabili $x_1, \ldots, x_{81}$ seguendo l'ordine per righe della tabella del gioco. Nella prima riga le variabile da x_1 a x_9, nella seconda da x_{10} a x_{18} e così via.
2. I colori necessari sono 9, tanti quanti i numeri da inserire.
3. La relazione di adiacenza dei vertici del grafo è definita in base alle proprietà del gioco: due vertici i e j sono adiacenti, ovvero l'arco (i, j) appartiene al grafo, se le relative celle appartengono alla stessa riga, alla stessa colonna o alla stessa sotto tabella 3×3.

Il grafo che otteniamo è un grafo in cui ogni vertice ha grado 20, quindi un grafo *regolare*. Questo perché ogni vertice è adiacente nel senso sopra descritto ad altri 20: ogni cella, infatti, è collegata alle 8 celle nella sua stessa riga, 8 nella stessa colonna e le rimanenti 4 celle nella stessa regione 3×3. Possiamo quindi calcolare il numero di archi del grafo che è pari a $\frac{81 \cdot 20}{2} = 810$. Abbiamo tutti gli elementi per ricavare il sistema di equazioni algebriche per la risoluzione: tale sistema è descritto dall'ideale I in $\mathbb{Q}[x_1, \ldots, x_{81}]$ generato dai polinomi $f(x_i)$ per ogni $i \in \{1, \ldots, 81\}$ e $g(x_i, x_j)$, se i vertici i e j sono adiacenti, con

$$f(x_i) = \prod_{k=1}^{9} (x_i - k) \qquad g(x_i, x_j) = \frac{f(x_i) - f(x_j)}{x_i - x_j}$$

Infine dobbiamo tenere conto delle informazioni iniziali date dal problema inserendo nell'insieme dei generatori dell'ideale I i polinomi $x_i - \alpha_i$ con $\alpha_i \in \{1, \ldots, 9\}$ il valore della casella fornito dal gioco.

Giunti a questo punto si risolve il sistema cercando una base di Gröbner ridotta per I e procedendo come nei casi descritti fin'ora.

4.2 Operare con ideali

In questa ultima parte andremo ad analizzare alcuni semplici metodi per operare con gli ideali di $F[x_1, \ldots, x_n]$ seguendo un approccio computazionale, basato sulla teoria delle basi di Gröbner.

Anzitutto, dall'unicità della base ridotta di Gröbner per un dato ideale I (Teorema 17) segue immediatamente un criterio per stabilire l'uguaglianza tra due ideali.

Proposizione 19 (Uguaglianza di ideali)**.** *Sia $F[x_1, \ldots, x_n]$ con un fissato ordinamento monomiale e I, J ideali di $F[x_1, \ldots, x_n]$, allora*

$I = J$ se, e solo se, I e J presentano la stessa base ridotta di Gröbner.

Vediamo inoltre un uso della Teoria dell'eliminazione, in particolare degli ideali di eliminazione, per calcolare l'intersezione tra ideali in $F[x_1, \ldots, x_n]$.

Proposizione 20 (Intersezione di ideali)**.** *Se I e J sono due ideali di $F[x_1, \ldots, x_n]$allora $tI + (1-t)J$ è un ideale di $F[t, x_1, \ldots, x_n]$ e $I \cap J = (tI + (1-t)J) \cap F[x_1, \ldots, x_n]$. In particolare, $I \cap J$ è il primo ideale di eliminazione di $tI + (1-t)J$, coerentemente all'ordinamento monomiale $t > x_1 > \cdots > x_n$ in $F[t, x_1, \ldots, x_n]$.*

Dimostrazione. Vogliamo dimostrare che $I \cap J = (tI + (1-t)J) \cap F[x_1, \ldots, x_n]$ usando la doppia inclusione. Anzitutto, tI e $(1-t)J$ sono sicuramente ideali di $F[t, x_1, \ldots, x_n]$. Sia poi $f \in I \cap J \subseteq F[x_1, \ldots, x_n]$, allora lo possiamo scrivere come

$$f = tf - (1-t)f \in (tI + (1-t)J)$$

e questo mostra che $I \cap J \subseteq (tI + (1-t)J) \cap F[x_1, \ldots, x_n]$.

Viceversa sia $f = tf_1 + (1-t)f_2$ un elemento di $F[x_1, \ldots, x_n]$ con $f_1 \in I$ e $f_2 \in J$. Possiamo scrivere $t(f_1 - f_2) = f - f_2 \in F[x_1, \ldots, x_n]$ dal momento che sia f che f_2 sono polinomi nelle sole variabili $x_1, \ldots, x_n$. Poiché l'unico modo in cui $t(f_1 - f_2) \in F[x_1, \ldots, x_n]$ è che $t(f_1 - f_2) = 0$, segue che $f_1 - f_2 = 0$ e $f_1 = f_2$; possiamo quindi concludere che $f = f_1 = f_2 \in I \cap J$.

Abbiamo mostrato che $I \cap J = (tI + (1-t)J) \cap F[x_1, \ldots, x_n]$, in cui riconosciamo la definizione di ideale di eliminazione per $(tI + (1-t)J)$ rispetto alla variabile t, nell'ordinamento monomiale $t > x_1 > \cdots > x_n$. □

Dati quindi due ideali I e J di $F[x_1, \ldots, x_n]$ e delle basi di Gröbner rispettive $G = \{f_1, \ldots, f_s\}$ per I e $H = \{h_1, \ldots, h_t\}$ per J, calcoliamo $I \cap J$ nel modo indicato della Proposizione 20. Sapendo che $I \cap J$ è il primo ideale di eliminazione di

$$tI + (1-t)J = (tf_1, \ldots, tf_s, (1-t)h_1, \ldots, (1-t)h_t)$$

rispetto all'ordinamento $t > x_1 > \cdots > x_n$, calcoliamo, usando l'algoritmo di Buchberger, una base di Gröbner per $tI + (1-t)J$ a partire dai generatori elencati. I polinomi appartenenti alla base trovata che non presentano la dipendenza da t sono quindi un insieme di generatori, nonché base di Gröbner, per $I \cap J$.

Illustriamo a seguire un esempio esplicito.

Esempio 15 (Calcolo intersezione ideali)**.** Un facile esempio è il seguente: siano $I = (x^2, xy, y^2)$ e $J = (x)$ ideali in $F[x, y]$. Determiniamo $I \cap J$. Per la Proposizione 20, $I \cap J$ è il primo ideale di eliminazione di $tI + (1-t)J$ nel rispetto dell'ordinamento monomiale $t > x > y$.

Ora, $tI + (1-t)J = (tx^2, txy, ty^2, (1-t)x)$. Siano $f_1 = tx^2$, $f_2 = txy$, $f_3 = ty^2$ e $f_4 = -tx + x$, calcoliamo una base di Gröbner per $tI + (1-t)J$ usando l'algoritmo di Buchberger. Si vede immediatamente che

$$S(f_1, f_2) \equiv S(f_1, f_3) \equiv S(f_2, f_3) \equiv 0 \ mod \ \{f_1, \ldots, f_4\}$$
$$S(f_1, f_4) \equiv x^2 \ mod \ \{f_1, \ldots, f_4\}$$
$$S(f_2, f_4) \equiv xy \ mod \ \{f_1, \ldots, f_4\}$$
$$S(f_3, f_4) \equiv xy^2 \ mod \ \{f_1, \ldots, f_4\}$$

Aggiungendo questi tre monomi alla lista di generatori, si verifica senza sforzi che

$$G = \{f_1, \ldots, f_4, x^2, xy, xy^2\}$$

è una base di Gröbner per $tI + (1-t)J$ dal momento che soddisfa il criterio di Buchberger. Ricaviamo poi la base ridotta

$$G' = \{ty^2, tx - x, x^2, xy\}$$

ed infine l'ideale di eliminazione di $tI + (1-t)J$ rispetto alla variabile t,

$$(tI + (1-t)J)_1 = G' \cap F[x, y] = (x^2, xy) = I \cap J$$

Bibliografia

[1] Thomas Becker. *Gröbner bases : a computational approach to commutative algebra / Thomas Becker, Volker Weispfenning ; in cooperation with Heinz Kredel*. Graduate texts in mathematics. Springer, New York, 1993.

[2] Bruno Buchberger. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. PhD thesis, Universitat Insbruck*, 1965.

[3] Bruno Buchberger and Franz Winkler. *Gröbner bases and applications*, volume 17. Cambridge University Press Cambridge, 1998.

[4] David S Dummit and Richard M Foote. *Abstract algebra*. Prentice Hall Englewood Cliffs, NJ, 2004.

[5] Jesús Gago-Vargas, Isabel Hartillo-Hermoso, Jorge Martín-Morales, and José María Ucha-Enríquez. *Sudokus and Gröbner bases: not only a divertimento. Lecture Notes in Comput. Sci., 4194, Springer, Berlin*, 2006.

[6] Daniel Lichtblau. *Effective computation of strong Gröbner bases over Euclidean domains. Illinois J. Math.*, 2012.