UNIVERSITÀ DEGLI STUDI DI TORINO
Facoltà di Scienze M.F.N.
Corso di Laurea in Matematica

Tesi di Laurea Triennale

L'algebra lineare nello studio delle varietà di punti

Relatore:
Dott. Mario Valenzano

Candidato:
Paolo Saracco

A.A. 2010-2011

Indice

Introduzione

Lo scopo del presente elaborato è l'analisi di un metodo, legato all'algebra lineare, che permette di studiare le *varietà di punti*, cioè varietà affini formate da un numero finito di punti. Tale metodo prende il nome di *metodo degli autovalori e degli autovettori*.
Vedremo come una varietà di punti sia definita da un *sistema di equazioni polinomiali* e vedremo come il metodo degli autovalori e degli autovettori permetta di risolvere tale sistema da un punto di vista algebrico, allo scopo di trovare le coordinate di tali punti.
Questo approccio si propone come alternativa (o come supporto) alla teoria dell'eliminazione e fornisce inoltre un interessante esempio di come la matematica astratta possa celare inattese potenzialità applicative.
A differenza di altri metodi, a volte molto efficienti dal punto di vista dell'implementazione su computer, il metodo in questione, di natura essenzialmente algebrica, può risultare computazionalmente più svantaggioso, ma permette di ottenere informazioni aggiuntive riguardanti la struttura della varietà: esistenza delle soluzioni, numero dei punti e molteplicità delle soluzioni coincidenti.
Dal momento che le varietà di punti sono oggetti geometrici zero-dimensionali (e quindi considerati "semplici" nell'ambito della geometria algebrica), gli strumenti geometrici introdotti saranno relativamente pochi e limitati ai legami che uniscono struttura algebrica e geometrica, come il *Nullstellensatz di Hilbert*. Verrà dedicato invece maggior spazio a quelli più prettamente algebrici e alla risoluzione di sistemi di equazioni polinomiali.
Il primo capitolo richiama concetti e risultati tecnici di base legati ai vari ambiti coinvolti: l'algebra dei polinomi, le varietà affini, l'algebra lineare. Il secondo invece, è interamente riservato allo sviluppo del nucleo centrale. Volendo andare più nel dettaglio, possiamo analizzare lo scritto passo dopo passo dicendo che:
La prima sezione del Capitolo 1 riassume alcuni fatti salienti riguardanti i polinomi e la teoria generale relativa ad anelli e ideali. Partendo dalle prime definizioni e proprietà, si giunge fino al *Teorema della Base di Hilbert* e all'introduzione delle *Basi di Gröbner*. Si tratta di poco più che una rapida presentazione, ma che contiene risultati di importanza cardinale nello sviluppo successivo.
La seconda sezione, invece, presenta gli oggetti matematici che ci siamo riproposti di studiare: le *varietà affini*. Ma non solo: analizza anche il profondo legame che c'è tra queste e gli ideali di polinomi, fino alla dimostrazione del fondamentale *Nullstellensatz di Hilbert* (al quale è dedicata un'intera sottosezione).
La terza sezione introduce la struttura algebrica su cui si innesterà poi il metodo degli autovalori e degli autovettori, cioè quella di *algebra* su di un campo. Grazie alla sua duplice natura di anello e spazio vettoriale, ci permetterà di applicare gli strumenti del-

l'algebra lineare ai sistemi di equazioni algebriche. Si dimostrerà inoltre il *Finiteness Theorem*, che mette in relazione la dimensione dell'algebra in analisi con il numero di punti presenti nella varietà, e si presenterà il concetto di *ideale zero-dimensionale*, cioè il corrispondente algebrico della varietà di punti.
La quarta sezione contiene alcuni richiami di algebra lineare, volti principalmente alla dimostrazione del *Teorema di Cayley-Hamilton* e all'introduzione delle *matrici non-derogatorie*.
Si passa dunque ad affrontare l'argomento centrale della presente trattazione. La prima sezione del Capitolo 2 è dedicata all'introduzione delle *mappe di moltiplicazione* e delle loro proprietà. Queste funzioni sono le mappe lineari a cui applicheremo il metodo degli autovalori e degli autovettori, al fine di ricavare da un sistema di equazioni algebriche, la varietà di punti che esso rappresenta.
La seconda sezione è riservata al teorema che rende possibile questo passaggio: si tratta dell'*Eigenvalue Theorem* o Teorema degli Autovalori. Esso mette in relazione gli autovalori delle mappe di moltiplicazione con i punti della varietà algebrica in esame.
L'ultima sezione approfondisce i risultati ottenuti nella precedente, studiando quali altre informazioni si possono ricavare dall'analisi degli autovettori delle mappe di moltiplicazione nel caso in cui queste siano non-derogatorie.
Vengono citati, ma non trattati in questo lavoro, risultati relativi alla molteplicità dei punti di una varietà. Viene inoltre trattato, solo superficialmente, il caso in cui la matrice sia *derogatoria*. Per approfondimenti riguardanti questi risultati si può far riferimento a [Cox] e [CLO2].

Capitolo 1

Nozioni preliminari

1.1 Polinomi

Definizione 1.1.1. (*successione*)
Sia R un anello commutativo con unità. Una *successione* σ a valori in R è una sequenza infinita

$$\sigma = (s_0, s_1, s_2, \ldots, s_i, \ldots),$$

con $s_i \in R$, per ogni $i \geq 0$. Ossia, una successione σ è una funzione

$$\begin{array}{rccc} \sigma\colon & \mathbb{N} & \to & R \\ & i & \mapsto & \sigma(i) = s_i \end{array}$$

Le entrate $s_i \in R$, per ogni $i \geq 0$, sono chiamate i *coefficienti* di σ.
Inoltre, due successioni $\sigma = (s_0, s_1, s_2, \ldots, s_i, \ldots)$ e $\tau = (t_0, t_1, t_2, \ldots, t_i, \ldots)$ sono uguali se e solo se $s_j = t_j$ per ogni $j \geq 0$.

Definizione 1.1.2. (*polinomio*)
Un *polinomio* a coefficienti in un anello commutativo con unità R è una successione $\sigma = (s_0, s_1, s_2, \ldots, s_i, \ldots)$ di elementi di R, soddisfacenti la condizione $s_i = 0$ per ogni $i > m$, per un certo $m \geq 0$. Cioè

$$\sigma = (s_0, s_1, s_2, \ldots, s_m, 0, 0, \ldots).$$

Il polinomio nullo è la successione $\sigma = (0, 0, 0, \ldots)$ e viene denotato con $\sigma = 0$.

Definizione 1.1.3. Se $\sigma = (s_0, s_1, s_2, \ldots, s_n, 0, 0, \ldots)$ è un polinomio non nullo, allora esiste un $s_n \neq 0$ tale che $s_j = 0$ per ogni $j > n$. Si definisce *coefficiente direttivo* del polinomio l'elemento s_n e il numero n prende il nome di *grado* del polinomio. Tale grado si indica con $\deg(\sigma)$.

Osservazione 1.1.4. Il polinomio nullo non ha grado, perché non ha nessun coefficiente diverso da 0. Per convenzione porremo $\deg(0) = -\infty$.

Indicheremo con $R[x]$ l'insieme di tutti i polinomi a coefficienti in R. Introduciamo in $R[x]$ due operazioni di addizione e moltiplicazione nel seguente modo:

$$(s_0, s_1, \ldots, s_i, \ldots) + (t_0, t_1, \ldots, t_i, \ldots) \stackrel{\text{def}}{=} (s_0 + t_0, s_1 + t_1, \ldots, s_i + t_i, \ldots)$$

e

$$(s_0, s_1, \ldots, s_i, \ldots) \cdot (t_0, t_1, \ldots, t_i, \ldots) \stackrel{\text{def}}{=} (s_0t_0, s_1t_0 + s_0t_1, \ldots, \underbrace{\sum_{k=0}^{i} s_k t_{i-k}}_{\text{pos.}(i+1)\text{-esima}}, \ldots)$$

Proposizione 1.1.5. *Con le operazioni sopra definite* $(R[x], +, \cdot)$ *è un anello commutativo con unità, chiamato* anello dei polinomi in una indeterminata a coefficienti in R.

Dimostrazione. Il fatto che $(R[x], +)$ sia un gruppo abeliano è immediata conseguenza della definizione. Il prodotto $\cdot$ gode della proprietà commutativa perché è definito in funzione del prodotto e della somma in R, che godono di tale proprietà. L'unità è il polinomio $1 = (1, 0, 0, \ldots)$. □

Proposizione 1.1.6. *Se* R *è un dominio di integrità, allora* $(R[x], +, \cdot)$ *è un dominio di integrità.*

Dimostrazione. Siano $\sigma = (s_0, s_1, \ldots, s_n, 0, \ldots)$ e $\tau = (t_0, t_1, \ldots, t_m, 0, \ldots)$ due polinomi non nulli in $R[x]$. Questo significa che almeno s_n e t_m sono elementi non nulli di R. Ma allora vale:

$$\sum_{k=0}^{n+m} s_k t_{n+m-k} = s_n t_m \neq 0,$$

cioè il termine di posto $n + m + 1$ nel polinomio prodotto è non nullo. Quindi in $R[x]$ non si possono avere divisori dello zero e dunque è un dominio di integrità. □

Osservazione 1.1.7. Si noti che solo i polinomi costanti $\sigma = (k, 0, 0, \ldots)$, tali che k sia un elemento invertibile di R, hanno inverso moltiplicativo, dunque $(R[x], +, \cdot)$ non è mai un campo.

Per comodità di notazione, d'ora in avanti indicheremo $(R[x], +, \cdot)$ solo con il simbolo $R[x]$, sottointendendo le due operazioni definite sopra.

Osservazione 1.1.8. Il legame tra una successione definita come sopra e un polinomio nella sua forma tradizionale è dato dalla corrispondenza biunivoca:

$$(a_0, a_1, a_2, a_3, \ldots, a_n, \underbrace{0, 0, \ldots}_{\text{tutti } 0}) \longleftrightarrow \sum_{i=0}^{n} a_i x^i.$$

In particolare abbiamo le seguenti identificazioni:

$$\begin{array}{rcl} (1, 0, 0, 0, 0, \ldots) & \equiv & 1 \\ (0, 1, 0, 0, 0, \ldots) & \equiv & x \\ (0, 0, 1, 0, 0, \ldots) & \equiv & x^2 \\ \vdots & & \vdots \\ (0, 0, \ldots, \underbrace{1}_{(i+1)\text{-ma}}, 0, \ldots) & \equiv & x^i, \end{array}$$

da cui si vede come l'indeterminata x e le sue potenze svolgano una funzione analoga a quella di un segnaposto. D'ora in avanti, per comodità, rappresenteremo i polinomi nella loro forma tradizionale.

Nota 1.1.9. L'addendo $a_i x^i$ prende il nome di *termine* del polinomio f. a_n viene chiamato il *coefficiente direttivo* del polinomio, il numero n è il suo *grado* e $a_n x^n$ viene detto *termine iniziale* o *termine di grado massimo* di f e si indica con $\mathrm{lt}(f)$ (lt è l'abbreviazione della locuzione inglese: 'leading term').

Osservazione 1.1.10. Se R è un anello commutativo con unità, allora ogni polinomio $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x]$ definisce una *funzione polinomiale* da R in sé data da:

$$\begin{array}{rccc} f\colon & R & \to & R \\ & r & \mapsto & \sum_{i=0}^{n} a_i r^i \end{array}$$

Resta quindi definita un'applicazione

$$\begin{array}{rccccc} \Psi: & R[x] & \longrightarrow & \mathcal{F} & & \\ & \displaystyle\sum_{i=0}^{n} a_i x^i & \longmapsto & f: & R & \to & R \\ & & & & r & \mapsto & \sum_{i=0}^{n} a_i r^i \end{array}$$

dove $\mathcal{F}$ rappresenta l'insieme delle funzioni polinomiali $\varphi\colon R \to R$.
Tale applicazione è suriettiva, ma non necessariamente iniettiva. Se l'anello R è finito, allora c'è solo un numero finito di funzioni da R in sé. Tuttavia i polinomi in $R[x]$ sono sempre infiniti: infatti, è sufficiente considerare le potenze $1, x, x^2, \ldots$, che sappiamo essere polinomi distinti.

Passiamo ora a definire induttivamente l'anello dei polinomi in n indeterminate, estendendo anche i concetti sopra riportati a questo caso.

Definizione 1.1.11. L'anello $R_n = R[x_1, \ldots, x_n]$ dei polinomi in n indeterminate a coefficienti in R si definisce induttivamente nel modo seguente:

$$R_1 \stackrel{\text{def}}{=} R[x], \qquad R_n \stackrel{\text{def}}{=} R_{n-1}[x_n] = R[x_1, \ldots, x_{n-1}][x_n].$$

Definizione 1.1.12. Un *monomio* nelle indeterminate $x_1, x_2, \ldots, x_n$ è un prodotto

$$x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \tag{1.1}$$

dove gli α_i sono interi non negativi. Per abbreviare riscriveremo a volte la (1.1) come x^α, dove $\alpha = (\alpha_1, \ldots, \alpha_n)$ è il vettore degli esponenti del monomio e $x = (x_1, \ldots, x_n)$ il vettore delle indeterminate.
Il *grado totale* di un monomio x^α è la somma degli esponenti: $\alpha_1 + \cdots + \alpha_n$. Sovente lo denoteremo con $|\alpha|$.
Indicheremo con T_n l'insieme di tutti i monomi nelle n indeterminate, cioè:

$$\mathrm{T}_n = \{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} : \alpha_i \in \mathbb{N},\ i = 1, \ldots, n\}$$

Definizione 1.1.13. Un *polinomio* nelle indeterminate x_i, per $i \in \{1, \ldots, n\}$, a coefficienti in un anello commutativo con unità R assume allora la forma:

$$f = \sum_{\alpha} c_\alpha x^\alpha$$

dove $c_\alpha \in R$ per ogni α e c'è solamente un numero finito di addendi non nulli nella sommatoria.
Denoteremo con *termine* il prodotto di un elemento diverso da zero di R per un monomio.
Il *grado* di un polinomio nell'indeterminata x_i è l'esponente più alto con cui compare la x_i nel polinomio f.
Il *grado totale* del polinomio f è il grado più alto dei suoi monomi.

Nota 1.1.14. Due polinomi in n indeterminate sono *uguali* se e solo se hanno gli stessi coefficienti.

In $R[x_1, \ldots, x_n]$ si possono introdurre l'addizione e la moltiplicazione di polinomi, ricordandosi la Definizione 1.1.11. Cioè, un elemento di $R[x_1, \ldots, x_n]$ si può pensare come un polinomio nell'indeterminata x_n a coefficienti nell'anello $R[x_1, \ldots, x_{n-1}]$; valgono allora le definizioni di somma e prodotto date per i polinomi in una indeterminata. Con tali operazioni $R[x_1, \ldots, x_n]$ ha la struttura di anello commutativo con unità. Si può provare per induzione che se R è un dominio di integrità, allora anche $R[x_1, \ldots, x_n]$ è un dominio di integrità (è sufficiente ricalcare i passi della dimostrazione della Proposizione 1.1.6). Tuttavia solo i polinomi costanti $f = k$ tali che k appartenga all'insieme degli elementi invertibili di R hanno inverso moltiplicativo, dunque $R[x_1, \ldots, x_n]$ non è mai un campo.

1.1.1 Ideali

Dato un insieme finito di polinomi $\{f_1, \ldots, f_s\}$ contenuto in $R[x_1, \ldots, x_n]$, possiamo considerare l'insieme di tutte le combinazioni finite a coefficienti in $R[x_1, \ldots, x_n]$:

$$\{p_1 f_1 + \cdots + p_s f_s : p_i \in R[x_1, \ldots, x_n] \, \forall \, i = 1, \ldots, s\}. \tag{1.2}$$

Indicheremo tale insieme con $\langle f_1, \ldots, f_s \rangle$.

Definizione 1.1.15. (*ideale*)
Sia $I \subseteq R[x_1, \ldots, x_n]$ un sottoinsieme non vuoto. Diremo che I è un *ideale* se:

I1: per ogni $f, g \in I$, $f + g \in I$;

I2: per ogni $f \in I$ e per ogni $p \in R[x_1, \ldots, x_n]$, $fp \in I$.

Proposizione 1.1.16. *L'insieme* (1.2) *dei polinomi costruiti a partire da un insieme finito* $\{f_1, \ldots, f_s\} \subset R[x_1, \ldots, x_n]$ *tramite somma e prodotto è un ideale di* $R[x_1, \ldots, x_n]$ *ed è il più piccolo ideale contenente* $\{f_1, \ldots, f_s\}$. *Di conseguenza lo chiameremo* ideale generato da $f_1, \ldots, f_s$ *e diremo che l'insieme* $\{f_1, \ldots, f_s\}$ *è un* sistema di generatori *o una* base *per tale ideale.*

Dimostrazione. Proviamo innanzitutto che si tratta di un ideale. Siano

$$p = \sum_{i=1}^{s} p_i f_i \qquad \text{e} \qquad q = \sum_{i=1}^{s} q_i f_i$$

due polinomi in $I = \langle f_1, \ldots, f_s \rangle$.

$$p + q = \sum_{i=1}^{s} p_i f_i + \sum_{i=1}^{s} q_i f_i = \sum_{i=1}^{s} (p_i + q_i) f_i \in I$$

Sia anche $r \in R[x_1, \ldots, x_n]$

$$rp = r \left(\sum_{i=1}^{s} p_i f_i \right) = \sum_{i=1}^{s} (r p_i) f_i \in I$$

Proviamo ora che si tratta del più piccolo ideale (rispetto all'inclusione) contenente $\{f_1, \ldots, f_s\}$. Supponiamo che J sia un ideale contenente $\{f_1, \ldots, f_s\}$, per definizione di ideale J contiene pf_i per ogni $p \in R[x_1, \ldots, x_n]$, $f_i \in \{f_1, \ldots, f_s\}$ e somme finite di questi, quindi contiene anche I. □

Teorema 1.1.17. (Teorema della Base di Hilbert)
Sia R un anello commutativo con unità. In $R[x_1, \ldots, x_n]$ valgono le seguenti proprietà:

1. *se I è un ideale di $R[x_1, \ldots, x_n]$, allora esistono dei polinomi $f_1, \ldots, f_s$ appartenenti a $R[x_1, \ldots, x_n]$ tali che $I = \langle f_1, \ldots, f_s \rangle$;*

2. *se $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$ è una catena ascendente di ideali, allora esiste un N tale che $I_n = I_N$ per ogni $n \geq N$.*

Definizione 1.1.18. (*ideale finitamente generato*)
Un ideale I di un qualsiasi anello commutativo con unità R che soddisfi alla condizione (1) del Teorema 1.1.17 si dice *finitamente generato.*

Definizione 1.1.19. (*anello Noetheriano*)
La condizione (2) del Teorema 1.1.17 viene generalmente indicata col nome di *condizione della catena ascendente* e un qualunque anello commutativo con unità R che soddisfi questa condizione viene detto *Noetheriano.*

Per un anello commutativo con unità risulta che le due condizioni del Teorema 1.1.17 sono equivalenti, cioè se vale la (1) vale anche la (2) e viceversa, come afferma il seguente:

Teorema 1.1.20. *Le seguenti condizioni sono equivalenti per un anello commutativo con unità R:*

1. *se I è un ideale di R, allora esistono degli elementi $r_1, \ldots, r_s \in R$ tali che $I = \langle r_1, \ldots, r_s \rangle$;*

2. *se $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$ è una catena ascendente di ideali, allora esiste un N tale che $I_n = I_N$ per ogni $n \geq N$.*

Equivalentemente, l'anello R è Noetheriano se e solo se ogni ideale in R è finitamente generato.

Dimostrazione. Assumiamo prima che valga la condizione (1), cioè ogni ideale in R sia finitamente generato, e sia

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \subseteq I_n \subseteq \ldots$$

una catena ascendente di ideali di R. Consideriamo l'insieme $I = \bigcup_{i=1}^{\infty} I_i$. Dal momento che gli ideali I_i sono incapsulati, è evidente che I è un ideale di R. Per la condizione (1) allora $I = \langle r_1, \ldots, r_s \rangle$ per certi $r_1, \ldots, r_s \in R$. Poiché $r_i \in I$, esiste un N_i tale che $r_i \in I_{N_i}$. Sia $N = \max_{1 \leq i \leq s} N_i$; allora $r_i \in I_N$ per ogni $i = 1, \ldots, s$ e quindi $I \subseteq I_N$. Segue che $I = I_N$ e vale la condizione (2).
Viceversa, supponiamo per assurdo che non valga (1) pur valendo (2). Esiste allora un ideale I in R che non è generato da un numero finito di elementi di R. Sia $r_1 \in I$. Esiste un r_2 in I tale che $r_2 \notin \langle r_1 \rangle$. Allora $\langle r_1 \rangle \subsetneq \langle r_1, r_2 \rangle$. Continuando alla stessa maniera troviamo una catena strettamente ascendente di ideali di R, contraddicendo l'ipotesi di Noetherianità. □

Sfruttando questi risultati, proviamo ora una versione più generale del Teorema della Base di Hilbert:

Teorema 1.1.21. *Se R è un anello Noetheriano, allora anche $R[x]$ è Noetheriano.*

Dimostrazione. Sia R un anello Noetheriano e J un ideale di $R[x]$. Per il Teorema 1.1.20 è sufficiente provare che J è finitamente generato. Per ogni $n \geq 0$, definiamo I_n come l'insieme:

$$\{r \in R : r \text{ è il coefficiente direttivo di un polinomio in } J \text{ di grado n}\} \cup \{0\}.$$

I_n è un ideale di R: se $r, s \in I_n$, $r + s$ è il coefficiente direttivo della somma dei due polinomi. Questa sta ancora in J perché è un ideale e dunque $r + s \in I_n$. Allo stesso modo se $a \in R$, $a \cdot r$ è il coefficiente direttivo del polinomio ottenuto moltiplicando il polinomio costante a per il polinomio di cui r è il coefficiente direttivo. Sta ancora in J perché ideale e allora $a \cdot r \in I_n$.
Risulta evidente che $I_n \subseteq I_{n+1}$. Dal momento che R è Noetheriano esiste un N tale che $I_n = I_N$ per ogni $n \geq N$. Sempre per il Teorema 1.1.20, ogni I_i è finitamente generato; poniamo $I_i = \langle r_{i1}, \ldots, r_{it_i} \rangle$. Ora, per $i = 1, \ldots, N$ e per $j = 1, \ldots, t_i$, sia f_{ij} un polinomio in J di grado i con coefficiente direttivo r_{ij}. Per terminare la dimostrazione è sufficiente provare che

$$J = \langle f_{ij} : 1 \leq i \leq N,\ 1 \leq j \leq t_i \rangle$$

Sia allora $J^* = \langle f_{ij} : 1 \leq i \leq N,\ 1 \leq j \leq t_i \rangle$. Chiaramente $J^* \subseteq J$. Viceversa sia $f \in J$ e sia n il grado di f.
Proviamo per induzione su n che $f \in J^*$. Se $f = 0$ o $n = 0$, allora $f \in I_0$ e quindi $f \in J^*$. Sia ora $n > 0$ e supponiamo che tutti gli elementi di J di grado al più $n - 1$ stiano in J^*. Sia r il coefficiente direttivo di f. Abbiamo due possibilità:
Se $n \leq N$, dal momento che $r \in I_n$, abbiamo che $r = \sum_{j=1}^{t_n} s_j \cdot r_{nj}$, per qualche $s_j \in R$. Allora il polinomio $g = \sum_{j=1}^{t_n} s_j \cdot f_{nj}$ è di grado n, ha coefficiente direttivo r, e sta in J^*. Quindi $f - g$ ha grado al più $n - 1$ e sta in J. Per induzione $f - g$ sta in J^* e

dunque anche f sta in J^*.
Se $n > N$ allora $r \in I_n = I_N$ e abbiamo che $r = \sum_{j=1}^{t_N} s_j \cdot r_{Nj}$, per qualche $s_j \in R$. Il polinomio $g = \sum_{j=1}^{t_N} s_j \cdot x^{n-N} \cdot f_{Nj}$ è di grado n, ha coefficiente direttivo r, e sta in J^*. Quindi $f - g$ ha grado al più $n-1$ e, per induzione, sta in J^*. Dunque anche f sta in J^*. □

Proposizione 1.1.22. *Sia R un anello Noetheriano. L'anello $R[x_1, \ldots, x_n]$ è Noetheriano.*

Dimostrazione. Per induzione su n.
Caso $n = 1$: per ipotesi abbiamo che R è Noetheriano, allora $R_1 = R[x_1]$ è Noetheriano per il Teorema 1.1.21. Supponiamo che la proprietà valga per ogni $k \leq n$, cioè supponiamo che $R_n = R[x_1, \ldots, x_n]$ sia Noetheriano. Allora, ancora per il Teorema 1.1.21, $R_{n+1} = R_n[x_{n+1}] = R[x_1, \ldots, x_n, x_{n+1}]$ è Noetheriano. Questo conclude la dimostrazione. □

Corollario 1.1.23. *Vale il Teorema della Base di Hilbert.*

Osservazione 1.1.24. Ogni campo $\mathbb{K}$ è banalmente Noetheriano: infatti gli unici ideali di $\mathbb{K}$ sono $\langle 0 \rangle$ e $\mathbb{K} = \langle 1 \rangle$, che sono finitamente generati. Per il Teorema 1.1.20 $\mathbb{K}$ è Noetheriano.

Corollario 1.1.25. *Sia $\mathbb{K}$ un campo. L'anello $\mathbb{K}[x_1, \ldots, x_n]$ è Noetheriano.*

Riportiamo un ultimo risultato di teoria degli anelli che tornerà utile più avanti.

Definizione 1.1.26. (*classi di equivalenza, anello quoziente*)
Sia R un anello commutativo con unità e ρ una relazione di equivalenza in R. Sia $r \in R$ un elemento; definiamo *classe di equivalenza di r* l'insieme:

$$[r]_\rho = \{t \in R : t \ \rho \ r\}.$$

Sia ora I un ideale proprio di R e ρ la relazione di equivalenza così definita:

$$t \ \rho \ r \iff t - r \in I.$$

Indichiamo con $r + I$ la classe di equivalenza di r modulo I e definiamo l'*anello quoziente*[1] di R modulo I come l'insieme:

$$R/I = \{r + I : r \in R\}.$$

Definizione 1.1.27. (*ideale massimale*)
Un ideale I di un anello commutativo con unità R è un *ideale massimale* se è un ideale proprio tale che non esiste nessun altro ideale J per cui valga $I \subsetneq J \subsetneq R$.

Teorema 1.1.28. *Un ideale proprio I di un anello commutativo con unità R è un ideale massimale se e solo se R/I è un campo.*

[1] Si verifica che si tratta effettivamente di un anello commutativo con unità.

Dimostrazione. ($\Leftarrow$): Supponiamo che R/I sia un campo. Sia J un ideale tale per cui $I \subseteq J \subseteq R$ e proviamo che o $I = J$ o $J = R$. Consideriamo la proiezione canonica sul quoziente $\pi\colon R \to R/I$ che manda l'elemento r nella classe $r + I$. Poiché l'immagine tramite π di un ideale è ancora un ideale, abbiamo che $\pi(J) = J/I \subseteq R/I$. Ma un campo contiene solo ideali banali e dunque o $J/I = \langle 0 \rangle$ o $J/I = R/I$. Se $J/I = \langle 0 \rangle$, allora $J = I$. Se invece $J/I = R/I$ allora, per ogni $r \in R$, si ha che $r + I \in J/I$, cioè esiste un $j \in J$ tale che $r + I = j + I$; questo implica che $r - j \in I \subseteq J$ e quindi che $R \subseteq J$, da cui $J = R$.
($\Rightarrow$): Sia ora I un ideale massimale e proviamo che R/I è un campo. Sia J^* un ideale di R/I; questo implica che $J = \pi^{-1}(J^*)$ è un ideale di R tale che $I \subseteq J \subseteq R$. Ma I è massimale, quindi o $I = J$ o $J = R$. Di conseguenza, abbiamo che R/I ammette solo gli ideali banali ed è dunque un campo. □

1.1.2 Ordini monomiali, Algoritmo di Divisione e basi di Gröbner

Definizione 1.1.29. (*ordine monomiale*)
Un *ordine monomiale* in $R[x_1, \ldots, x_n]$ è una relazione d'ordine $<$ nell'insieme T_n dei monomi x^α nelle indeterminate $x_1, \ldots, x_n$ (o, equivalentemente, sui vettori degli esponenti α in $\mathbb{N}^n$) tale che soddisfi le seguenti proprietà:

1. $<$ è una relazione di ordine totale;
2. $<$ è compatibile con la moltiplicazione in $R[x_1, \ldots, x_n]$, cioè, se $x^\alpha < x^\beta$ e x^γ è un altro monomio, allora
$$x^\alpha \cdot x^\gamma = x^{\alpha+\gamma} < x^{\beta+\gamma} = x^\beta \cdot x^\gamma;$$
3. $<$ è un buon ordinamento, cioè, ogni insieme non vuoto di monomi ammette un elemento minimo rispetto a $<$.

Nota 1.1.30. Affermiamo qui (ma lo proveremo solo in seguito) che se valgono le proprietà 1 e 2 di sopra, allora le seguenti affermazioni sono tra loro equivalenti:

a. $<$ è un buon ordinamento;
b. $1 < x^\alpha$ per ogni α in $\mathbb{N}^n$, $\alpha \neq (0, \ldots, 0)$;
c. $1 < x_i$ per ogni $i = 1, \ldots, n$.

Gli ordini monomiali che si possono definire sono molti. Qui riportiamo solo alcuni tra i principali[2].

Definizione 1.1.31. (*ordine lessicografico* o *lex*)
Siano x^α e x^β due monomi in $R[x_1, \ldots, x_n]$. Diremo che $x^\alpha <_{\text{lex}} x^\beta$ se, nella differenza $\beta - \alpha \in \mathbb{Z}^n$ l'elemento non nullo più a sinistra è positivo.

Definizione 1.1.32. (*ordine lessicografico graduato inverso* o *grevlex*)
Siano x^α e x^β due monomi in $R[x_1, \ldots, x_n]$. Diremo che $x^\alpha <_{\text{grevlex}} x^\beta$ se $|\alpha| < |\beta|$ o se $|\alpha| = |\beta|$ e nella differenza $\beta - \alpha \in \mathbb{Z}^n$ l'elemento non nullo più a destra è negativo.

[2]Per la dimostrazione del fatto che si tratti effettivamente di ordini monomiali si veda [CLO1], pagina 56 e seguenti.

Osservazione 1.1.33. Nelle definizioni degli ordini lessicografici, scrivendo i vettori degli esponenti come n-uple di numeri naturali, abbiamo implicitamente ordinato le indeterminate in $R[x_1, \ldots, x_n]$ considerando:

$$x_n < x_{n-1} < \cdots < x_2 < x_1.$$

D'ora in poi, a meno di esplicite variazioni, considereremo sempre questo ordine.

L'introduzione di un ordine monomiale ci permette di definire, anche per polinomi in più di una indeterminata, concetti familiari come il coefficiente direttivo o il termine di grado massimo.

Definizione 1.1.34. Siano $<$ un ordine monomiale in $R[x_1, \ldots, x_n]$ ed $f = \sum_\alpha c_\alpha x^\alpha$ un polinomio.
Il *termine iniziale* di f (rispetto a $<$) è il prodotto $c_\alpha x^\alpha$ dove x^α è il monomio maggiore in f rispetto a $<$. Lo denoteremo con $\mathrm{lt}_<(f)$ o con $\mathrm{lt}(f)$, qualora non vi sia possibilità di confusione.
Se inoltre $\mathrm{lt}(f) = cx^\alpha$, allora diremo che c è il *coefficiente direttivo* di f e che α è il suo *multigrado*. Li indicheremo rispettivamente con $\mathrm{lc}(f)$ e con $\mathrm{multideg}(f)$.

Esempio 1.1.35. Consideriamo i seguenti monomi in $\mathbb{Z}[x, y, z]$: $x^4y^2z^5$ e $x^3y^4z^4$. I corrispondenti vettori degli esponenti sono $(4, 2, 5)$ e $(3, 4, 4)$ e il grado totale è 11 per entrambi. Se introduciamo l'ordine *lex* con $x > y > z$ abbiamo che $(4, 2, 5) - (3, 4, 4) = (1, -2, 1)$ e dunque

$$x^4y^2z^5 >_{\mathrm{lex}} x^3y^4z^4.$$

Se invece introduciamo l'ordine *grevlex* avremmo che $(3, 4, 4) - (4, 2, 5) = (-1, 2, -1)$ e, poiché l'elemento non nullo più a destra è -1, si ha

$$x^3y^4z^4 >_{\mathrm{grevlex}} x^4y^2z^5.$$

Questo esempio mostra come le cose cambiano radicalmente a seconda di quale ordine monomiale si sceglie. Consideriamo infatti il polinomio $f = 2x^4y^2z^5 + 3x^3y^4z^4 \in \mathbb{Z}[x, y, z]$. Per quanto visto sopra, tale polinomio ha coefficiente direttivo 2 se l'ordinamento introdotto in T_3 è il *lex*, ha invece coefficiente direttivo 3 se è stato scelto il *grevlex*.

Vediamo ora un altro motivo per cui si introduce un ordine sui monomi: trovare un algoritmo di divisione per polinomi in più indeterminate. Diamo prima alcune definizioni.

Nota 1.1.36. Per una questione di comodità, d'ora in avanti faremo conto di lavorare in $\mathbb{K}[x_1, \ldots, x_n]$ con $\mathbb{K}$ campo. Tuttavia è necessario precisare che questa condizione non è restrittiva: buona parte dei risultati che seguiranno risultano essere validi anche se si considera R, anello commutativo con unità, al posto di $\mathbb{K}$.[3]

Definizione 1.1.37. (*riduzione modulo s*)
Sia $<$ un ordine monomiale e siano $f, h, s \in \mathbb{K}[x_1, \ldots, x_n]$, con $s \neq 0$. Diciamo che f *si*

[3]Per una trattazione più generale di questa sezione si faccia riferimento a [AdLo], pagina 201 e seguenti.

riduce ad h modulo s in un passo (in simboli $f \xrightarrow{s} h$), se e solo se il termine iniziale di s divide un termine non nullo $c_\beta x^\beta$ di f e

$$h = f - \frac{c_\beta x^\beta}{\mathrm{lt}(s)} s.$$

Allora la *riduzione* $f \xrightarrow{s} h$ consiste nel sostituire h a f.

Esempio 1.1.38. Sia $f = x^2y^2 - z^2$ e sia $s = x - y^2z$. Consideriamo l'ordine *lex* con $x > y > z$ e proviamo che $f \xrightarrow{s} h$, dove $h = xy^4z - z^2$. Il termine iniziale di s, $\mathrm{lt}(s) = x$, divide il termine x^2y^2 di f, poniamo allora:

$$\begin{aligned} h &= f - \frac{x^2y^2}{x} s \\ &= x^2y^2 - z^2 - xy^2(x - y^2z) \\ &= xy^4z - z^2 \end{aligned}$$

e la prova è terminata. Osserviamo che l'operazione può essere iterata, perché ora x divide il termine xy^4z di h. Se proseguiamo, otteniamo:

$$\begin{aligned} h' &= h - \frac{xy^4z}{x} s \\ &= xy^4z - z^2 - xy^4z + y^6z^2 \\ &= y^6z^2 - z^2. \end{aligned}$$

La riduzione però termina qui, dal momento che $\mathrm{lt}(s) = x$ non divide più nessun termine di h'.

Definizione 1.1.39. (*riduzione modulo S*)
Sia $<$ un ordine monomiale e siano $f, h, s_1, \ldots, s_m \in \mathbb{K}[x_1, \ldots, x_n]$, con $s_i \neq 0$ per ogni $i = 1, \ldots, m$. Poniamo $S = \{s_1, \ldots, s_m\}$. Diciamo che f *si riduce ad h modulo S* (in simboli $f \xrightarrow{S}_+ h$), se e solo se esiste una sequenza di indici $i_1, \ldots, i_t \in \{1, \ldots, m\}$ e una sequenza di polinomi $h_1, \ldots, h_{t-1} \in \mathbb{K}[x_1, \ldots, x_n]$ tali che

$$f \xrightarrow{s_{i_1}} h_1 \xrightarrow{s_{i_2}} h_2 \xrightarrow{s_{i_3}} \cdots \xrightarrow{s_{i_{t-1}}} h_{t-1} \xrightarrow{s_{i_t}} h.$$

Definizione 1.1.40. Un polinomio $r \in \mathbb{K}[x_1, \ldots, x_n]$ si dice *ridotto* rispetto a $S = \{s_1, \ldots, s_m\}$ se $r = 0$ oppure nessun termine che occorre in r è divisibile per alcuno dei $\mathrm{lt}(s_i)$, $i = 1, \ldots, m$. Cioè, se r non può essere ridotto modulo S.

Definizione 1.1.41. Se $f \xrightarrow{S}_+ r$ e r è ridotto modulo S, allora diremo che r è un *resto* di f nella riduzione modulo S.

Algoritmo di Divisione

Possiamo ora introdurre l'Algoritmo di Divisione per polinomi in più indeterminate. A differenza di quanto accadeva per i polinomi in una sola indeterminata in $\mathbb{K}[x]$, si noti che ora è prevista la possibilità di dividere un polinomio per un insieme di polinomi, oltre che per uno soltanto.

Teorema 1.1.42. (Divisione in $\mathbb{K}[x_1, \ldots, x_n]$)
Sia $<$ un ordine monomiale in $\mathbb{K}[x_1, \ldots, x_n]$. Sia $f \in \mathbb{K}[x_1, \ldots, x_n]$ un polinomio in n indeterminate e $S = (s_1, \ldots, s_m)$ una m-upla ordinata di polinomi in $\mathbb{K}[x_1, \ldots, x_n]$. Allora f può essere scritto come

$$f = a_1 s_1 + \cdots + a_m s_m + r, \tag{1.3}$$

dove $a_i, r \in \mathbb{K}[x_1, \ldots, x_n]$, per ogni $i = 1, \ldots, m$. Inoltre, $a_i s_i = 0$ oppure $lt(f) \geq lt(a_i s_i)$ e analogamente $r = 0$ oppure r è una combinazione lineare di monomi, nessuno dei quali è divisibile per alcuno tra i $lt(s_i)$.

Osservazione 1.1.43. Prima di riportare l'algoritmo però, osserviamo due cose. Innanzitutto, nella definizione di resto, abbiamo parlato di *un* resto e non *del* resto. Abbiamo poi richiesto, tra le ipotesi del teorema, che S sia una m-upla *ordinata* di polinomi. Il motivo è che l'algoritmo dato di seguito non produce un'unica espressione della forma (1.3): essa dipende dall'ordine con cui si effettuano le divisioni e dall'ordine monomiale scelto. Per convincersene, si consideri l'esempio che segue l'algoritmo.

Algoritmo di Divisione in $\mathbb{K}[x_1, \ldots, x_n]$[4]

INPUT $s_1, \ldots, s_m, f \in \mathbb{K}[x_1, \ldots, x_n]$ con $s_i \neq 0$ $(1 \leq i \leq m)$
OUTPUT $a_1, \ldots, a_m, r$ tali che $f = a_1 s_1 + \cdots + a_m s_m + r$ e r è ridotto modulo $\{s_1, \ldots, s_m\}$
INIZIALIZZAZIONE $a_1 := 0$
$a_2 := 0$
$\vdots$
$a_m := 0$
$r := 0$
$h := f$
WHILE $h \neq 0$ **DO**
IF esiste un i tale che $\mathrm{lt}(s_i)$ divide $\mathrm{lt}(f)$ **THEN**
si scelga l'i minore per cui vale e
$a_i = a_i + \frac{\mathrm{lt}(f)}{\mathrm{lt}(s_i)}$
$h = h - \frac{\mathrm{lt}(f)}{\mathrm{lt}(s_i)} s_i$
ELSE $r = r + \mathrm{lt}(h)$
$h = h - \mathrm{lt}(h)$

Esempio 1.1.44. Introduciamo in $\mathrm{T}_2 \subset \mathbb{Q}[x, y]$ l'ordine *grevlex* con $x > y$. Sia $S = \{s_1, s_2\}$, con $s_1 = y^4 + xy^2$ e $s_2 = x^2 - xy$ in $\mathbb{Q}[x, y]$, e consideriamo $f = x^3y^3 + 2y^2 \in \mathbb{Q}[x, y]$.
Cominciamo considerando la coppia $S = (s_1, s_2)$ e dividiamo f per S seguendo i passi dell'algoritmo.

[4]Per la dimostrazione del fatto che l'algoritmo effettivamente fornisce un'espressione del tipo (1.3) si faccia riferimento a [AdLo], pagina 28 e seguenti.

1. Inizializziamo le variabili: $a_1 = 0$, $a_2 = 0$, $r = 0$, $h = x^3y^3 + 2y^2$ e segnamo a parte che $\mathrm{lt}(s_1) = y^4$ e $\mathrm{lt}(s_2) = x^2$.

2. Il $\mathrm{lt}(s_1)$ non divide x^3y^3, ma $\mathrm{lt}(s_2)$ sì, dunque:
$$\begin{aligned} a_2 &= \frac{x^3y^3}{x^2} = xy^3 \\ h &= x^3y^3 + 2y^2 - xy^3(x^2 - xy) \\ &= 2y^2 + x^2y^4 = x^2y^4 + 2y^2. \end{aligned}$$

3. $\mathrm{lt}(s_1)$ divide x^2y^4:
$$\begin{aligned} a_1 &= x^2 \\ h &= x^2y^4 + 2y^2 - x^2(y^4 + xy^2) \\ &= 2y^2 - x^3y^2 = -x^3y^2 + 2y^2. \end{aligned}$$

4. $\mathrm{lt}(s_1)$ non divide x^3y^2, ma $\mathrm{lt}(s_2)$ sì:
$$\begin{aligned} a_2 &= xy^3 - xy^2 \\ h &= -x^3y^2 + 2y^2 + xy^2(x^2 - xy) \\ &= 2y^2 - x^2y^3 = -x^2y^3 + 2y^2. \end{aligned}$$

5. $\mathrm{lt}(s_2)$ divide $-x^2y^3$:
$$\begin{aligned} a_2 &= xy^3 - xy^2 - y^3 \\ h &= -x^2y^3 + 2y^2 + y^3(x^2 - xy) \\ &= 2y^2 - xy^4 = -xy^4 + 2y^2. \end{aligned}$$

6. $\mathrm{lt}(s_1)$ divide $-xy^4$:
$$\begin{aligned} a_1 &= x^2 - x \\ h &= -xy^4 + 2y^2 + x(y^4 + xy^2) \\ &= 2y^2 + x^2y^2 = x^2y^2 + 2y^2. \end{aligned}$$

7. $\mathrm{lt}(s_2)$ divide x^2y^2:
$$\begin{aligned} a_2 &= xy^3 - xy^2 - y^3 + y^2 \\ h &= x^2y^2 + 2y^2 - y^2(x^2 - xy) \\ &= 2y^2 + xy^3 = xy^3 + 2y^2. \end{aligned}$$

8. Osserviamo subito che $h = xy^3 + 2y^2$ è ridotto rispetto a S, quindi possiamo concludere aggiungendolo al resto r:
$$\begin{aligned} r &= xy^3 + 2y^2 \\ h &= 0 \\ a_1 &= x^2 - x \\ a_2 &= xy^3 - xy^2 - y^3 + y^2 \end{aligned}$$

Come c'era da aspettarsi, nessuno dei monomi che compongo il resto è divisibile per $\mathrm{lt}(s_1)$ o $\mathrm{lt}(s_2)$: il resto r è ridotto rispetto a $S = (s_1, s_2)$. Abbiamo così trovato la seguente espressione per f:

$$f = (x^2 - x) \cdot s_1 + (xy^3 - xy^2 - y^3 + y^2) \cdot s_2 + (xy^3 + 2y^2).$$

Mostriamo ora come questa espressione *non sia unica*.
Se consideriamo, invece che il *grevlex*, l'ordine *lex* con $x > y$ il polinomio s_1 diventa $s_1 = xy^2 + y^4$, mentre gli altri due restano tali e quali. Svolgendo i calcoli in questa situazione otteniamo quest'altra espressione:

$$f = (x^2y - xy^3 + y^5) \cdot s_1 + 0 \cdot s_2 + (-y^9 + 2y^2).$$

Nella stessa situazione, consideriamo ora la coppia $S = (x^2 - xy, xy^2 + y^4)$, cioè poniamo $s_1 = x^2 - xy$ e $s_2 = xy^2 + y^4$. Se si svolgessero i calcoli come abbiamo fatto sopra, si troverebbe la seguente espressione per f:

$$f = (xy^3 + y^4) \cdot s_1 + y^3 \cdot s_2 + (-y^7 + 2y^2).$$

A titolo d'esempio, svolgiamo ancora i calcoli espliciti per il caso in cui l'ordine sia il *lex*, ma con $y > x$. I polinomi sono: $f = y^3x^3 + 2y^2$, $s_1 = y^4 + y^2x$, $s_2 = -yx + x^2$.

1. Inizializziamo le variabili: $u_1 = 0$, $u_2 = 0$, $r = 0$, $h = y^3x^3 + 2y^2$ e segnamo a parte che $\mathrm{lt}(s_1) = y^4$ e $\mathrm{lt}(s_2) = -yx$.

2. Il $\mathrm{lt}(s_1)$ non divide y^3x^3, ma $\mathrm{lt}(s_2)$ sì, dunque:
$$\begin{aligned} a_2 &= -y^2x^2 \\ h &= y^2x^4 + 2y^2. \end{aligned}$$

3. $\mathrm{lt}(s_2)$ divide y^2x^4:
$$\begin{aligned} a_2 &= -y^2x^2 - yx^3 \\ h &= 2y^2 + yx^5. \end{aligned}$$

4. Né $\mathrm{lt}(s_1)$, né $\mathrm{lt}(s_2)$ dividono $2y^2$:
$$\begin{aligned} r &= 2y^2 \\ h &= yx^5. \end{aligned}$$

5. $\mathrm{lt}(s_2)$ divide yx^5:
$$\begin{aligned} a_2 &= -y^2x^2 - yx^3 - x^4 \\ h &= x^6. \end{aligned}$$

6. x^6 è ridotto rispetto a S, dunque:
$$\begin{aligned} r &= 2y^2 + x^6 \\ h &= 0 \\ a_1 &= 0 \\ a_2 &= -y^2x^2 - yx^3 - x^4 \end{aligned}$$

Abbiamo così trovato che:

$$f = (0) \cdot s_1 + (-y^2x^2 - yx^3 - x^4) \cdot s_2 + (2y^2 + x^6).$$

È immediato notare come non solo le espressioni di f cambino radicalmente, ma anche il resto non sia lo stesso.

Questo esempio mostra come l'ordine con cui si effettuano le operazioni, l'ordine monomiale e l'ordine con cui si considerano le indeterminate influisca sia sui coefficienti a_i sia sul resto r. In quanto affronteremo più avanti, tuttavia, ci tornerà utile che almeno il resto sia indipendente dall'ordine con cui si effettuano le divisioni, in modo da poter definire quella che chiameremo una 'forma normale' per ogni polinomio in $\mathbb{K}[x_1, \ldots, x_n]$. Per raggiungere questo obiettivo, introduciamo il concetto di 'base di Gröbner'.

Basi di Gröbner

Nota 1.1.45. D'ora in avanti daremo per scontato di aver introdotto un ordine in $\mathrm{T}_n \subset \mathbb{K}[x_1, \ldots, x_n]$, anche quando non sarà specificato esplicitamente.

Definizione 1.1.46. (*base di Gröbner*)
Un insieme di polinomi non nulli $G = \{g_1, \ldots, g_t\}$ contenuto in un ideale I, è detto una *base di Gröbner per* I se e solo se, per ogni polinomio non nullo $f \in I$, esiste un $i \in \{1, \ldots, t\}$ tale che $\mathrm{lt}(g_i)$ divide $\mathrm{lt}(f)$.

Osservazione 1.1.47. Dalla definizione è subito chiaro che, se G è una base di Gröbner per I, allora non ci sono polinomi non nulli in I ridotti rispetto a G.

Vediamo ora le principali proprietà di una base di Gröbner.

Teorema 1.1.48. *Sia I un ideale di $\mathbb{K}[x_1, \ldots, x_n]$. Le seguenti affermazioni sono equivalenti per un insieme di polinomi non nulli $G = \{g_1, \ldots, g_t\} \subset I$:*

1. *G è una base di Gröbner per I;*
2. *$f \in I$ se e solo se $f \xrightarrow{G}_+ 0$.*

Dimostrazione. ($1 \Rightarrow 2$) Sia $f \in \mathbb{K}[x_1, \ldots, x_n]$. Per il Teorema 1.1.42 esiste un $r \in \mathbb{K}[x_1, \ldots, x_n]$, ridotto rispetto a G, tale che $f \xrightarrow{G}_+ r$. Di conseguenza, $f - r \in I$ e quindi $f \in I$ se e solo se $r \in I$.
Chiaramente, se $r = 0$, allora $f \in I$. Viceversa, se $f \in I$ e per assurdo fosse $r \neq 0$, allora r apparterrebbe a I e per (1) esisterebbe un $i \in \{1, \ldots, t\}$ tale che $\mathrm{lt}(g_i)$ divide $\mathrm{lt}(r)$. Questo contraddice l'ipotesi che r sia ridotto rispetto a G. Dunque, $r = 0$ e $f \xrightarrow{G}_+ 0$.
($1 \Leftarrow 2$) Supponiamo per assurdo che G non sia una base di Gröbner per I. Questo significa che esiste un f in I tale che, per ogni $i \in \{1, \ldots, t\}$, $\mathrm{lt}(g_i)$ non divide $\mathrm{lt}(f)$. Se applicassimo allora l'Algoritmo di Divisione per ridurre f modulo G, avremmo che

$$f = a_1g_1 + \cdots + a_tg_t + r$$

con $r \neq 0$, perché almeno $\mathrm{lt}(f)$ comparirebbe in r. Ma quindi $f \xrightarrow{G}_+ r$, contro l'ipotesi che $f \xrightarrow{G}_+ 0$ per ogni $f \in I$. □

Corollario 1.1.49. *Se $G = \{g_1, \ldots, g_t\}$ è una base di Gröbner per I, allora $I = \langle g_1, \ldots, g_t \rangle$.*

Dimostrazione. Indubbiamente $\langle g_1, \ldots, g_t \rangle \subseteq I$, dal momento che ogni g_i appartiene a I. Viceversa, sia $f \in I$. Per il Teorema 1.1.48, $f \xrightarrow{G}_+ 0$ e quindi $f \in \langle g_1, \ldots, g_t \rangle$. □

Definizione 1.1.50. Diciamo che un sottoinsieme $G = \{g_1, \ldots, g_t\}$ di polinomi in $\mathbb{K}[x_1, \ldots, x_n]$ è una *base di Gröbner* se e solo se è una base di Gröbner per l'ideale $\langle G \rangle$ che genera.

Dimostriamo adesso la proprietà per cui abbiamo introdotto le basi di Gröbner.

Teorema 1.1.51. *Se $G = \{g_1, \ldots, g_t\}$ è una base di Gröbner allora, per ogni $f \in \mathbb{K}[x_1, \ldots, x_n]$, il resto nella divisione di f per G è unico, indipendentemente dall'ordine scelto per gli elementi di G nella divisione.*

Dimostrazione. Sia G una base di Gröbner e sia $f \in \mathbb{K}[x_1, \ldots, x_n]$. Assumiamo che valgano:

$$f \xrightarrow{G}_+ r_1 \quad \text{e} \quad f \xrightarrow{G}_+ r_2,$$

con r_1 e r_2 ridotti rispetto a G. Questo significa che $f - r_1$ e $f - r_2$ appartengono a $\langle G \rangle$, e dunque anche $r_1 - r_2$ appartiene a $\langle G \rangle$. Inoltre $r_1 - r_2$ è ridotto modulo G. Quindi, per il Teorema 1.1.48 punto 2, $r_1 - r_2 = 0$. □

Esempio 1.1.52. Abbiamo visto, nell'Esempio 1.1.44, che il resto nella divisione di $f = x^3y^3 + 2y^2$ per $\{xy^2 + y^4, x^2 - xy\}$ (rispetto all'ordine *lex* con $x > y$) non è unico, nel senso che dipende dall'ordine in cui sono state svolte le divisioni. Questo perché, nel nostro caso, $S = \{xy^2 + y^4, x^2 - xy\}$ non è una base di Gröbner per $I = \langle S \rangle$. Per rendersene conto basta considerare il polinomio $y^6 + y^5 = (-x + y^2 + y) \cdot (xy^2 + y^4) + y^2 \cdot (x^2 - xy)$: questo appartiene all'ideale $\langle xy^2 + y^4, x^2 - xy \rangle$, ma è già ridotto modulo S contro quanto affermato nel Teorema 1.1.48 punto 2.
Ricorrendo al comando Maple *Basis* del pacchetto *Groebner*, ricaviamo che una base di Gröbner per $\langle S \rangle$ rispetto all'ordine *lex*, è data dall'insieme

$$G = \left\{ xy^2 + y^4, x^2 - xy, y^6 + y^5 \right\}.$$

Riduciamo allora f modulo G e otteniamo:

$$f = (x^2y - xy^3 + y^5) \cdot (xy^2 + y^4) + 0 \cdot (x^2 - xy) + (-y^3 + y^2 - y + 1) \cdot (y^6 + y^5) - y^5 + 2y^2$$

e $-y^5 + 2y^2$ è l'unico resto di f nella divisione per G. Per verificarlo basta riprendere l'Esempio 1.1.44, quando abbiamo invertito la coppia (s_2, s_1). In quel caso avevamo ottenuto $r = -y^7 + 2y^2$ e, proseguendo con la divisione per $y^6 + y^5$, otteniamo ancora:

$$f = (xy^3 + y^4) \cdot (x^2 - xy) + y^3 \cdot (xy^2 + y^4) + (-y + 1) \cdot (y^6 + y^5) - y^5 + 2y^2.$$

Osservazione 1.1.53. L'esempio precedente mostra che, benché il resto r sia indipendente dall'ordine, i singoli a_i non lo sono.

Osservazione 1.1.54. Il Teorema 1.1.51 garantisce che il resto nella divisione di un certo polinomio f per una base di Gröbner non dipende dall'ordine con cui si sono effettuate le divisioni. Tuttavia tale resto dipende ancora dall'ordine monomiale scelto, perché la base di Gröbner stessa dipende dall'ordine monomiale. L'esempio seguente è significativo in tal senso.

Esempio 1.1.55. Si considerino i polinomi $g_1 = z + x$ e $g_2 = y - x$ in $\mathbb{Q}[x, y, z]$. Sia $G = \{g_1, g_2\}$ e $I = \langle g_1, g_2 \rangle$. Assumiamo di utilizzare l'ordine *lex* con $x < y < z$ e proviamo che G è una base di Gröbner.
Per assurdo non lo sia. Questo significa che esiste un $f \neq 0$ in I tale che $\mathrm{lt}(f)$ non è divisibile né per $\mathrm{lt}(g_1) = z$ né per $\mathrm{lt}(g_2) = y$, cioè il termine iniziale di f è una potenza della sola x. Come conseguenza dell'ordine scelto sulle indeterminate, f deve appartenere a $\mathbb{Q}[x]$. D'altro canto, però, $f \in \langle g_1, g_2 \rangle$ e dunque $f = h_1(x, y, z) \cdot (z + x) + h_2(x, y, z) \cdot (y - x)$ con $h_1, h_2 \in \mathbb{Q}[x, y, z]$. Siccome y e z non compaiono nell'espressione di f deve necessariamente essere $h_1(x, y, z) = 0$ e $h_2(x, y, z) = 0$, ma allora $f = 0$. Assurdo.
Se invece assumessimo come ordine delle indeterminate $x > y > z$, allora G non sarebbe più una base di Gröbner. Infatti $y + z \in \langle G \rangle$, ma $\mathrm{lt}(g_1) = \mathrm{lt}(g_2) = x$ non divide né $\mathrm{lt}(y + z) = y$ né $\mathrm{lt}((y + z) - y) = z$; cioè $y + z \in \langle G \rangle$ ed è contemporaneamente ridotto modulo G.

Esempio 1.1.56. Come ulteriore conferma si consideri nuovamente l'Esempio 1.1.44. Rispetto all'ordinamento *grevlex*, $\{y^4 + xy^2, x^2 - xy\}$ è una base di Gröbner per l'ideale $\langle y^4 + xy^2, x^2 - xy \rangle$, mentre è risultato evidente che non lo fosse rispetto all'ordinamento *lex*.

Tuttavia, giunti a questo punto, è doveroso osservare che dalla definizione non è immediatamente chiaro se ogni ideale ammetta o meno una base di Gröbner. La Proposizione 1.1.65 proverà proprio questo risultato, ma prima è necessario sviluppare ancora un po' di teoria.

Definizione 1.1.57. (*ideale monomiale*)
Un ideale $I \subset \mathbb{K}[x_1, \ldots, x_n]$ è detto essere un *ideale monomiale* se esiste un sottoinsieme $A \subset \mathbb{N}^n$ tale che I è composto da tutti i polinomi che sono somme finite della forma

$$\sum_{\alpha \in A} h_\alpha x^\alpha,$$

dove $h_\alpha \in \mathbb{K}[x_1, \ldots, x_n]$. Ossia, se I è generato dai monomi dell'insieme $\{x^\alpha : \alpha \in A\}$.

Proposizione 1.1.58. *Sia $I = \langle x^\alpha : \alpha \in A \rangle$ un ideale monomiale. Allora un monomio x^β sta in I se e solo se x^β è divisibile per x^α per un certo $\alpha \in A$.*

Dimostrazione. Se x^β è divisibile per x^α, per un certo $\alpha \in A$, allora x^β sta in I per definizione di ideale.
Viceversa, se x^β sta in I, allora:

$$x^\beta = \sum_{i=1}^{s} h_i x^{\alpha_i},$$

dove $h_i \in \mathbb{K}[x_1, \ldots, x_n]$ e $\alpha_i \in A$. Se ora espandiamo il membro di destra come combinazione lineare di monomi, osserviamo che ogni termine è divisibile per qualche x^{α_i}. Per la definizione di uguaglianza tra polinomi la stessa cosa deve accadere al membro di sinistra e dunque x^β deve essere divisibile per almeno un x^{α_i}. □

Proposizione 1.1.59. *Siano $I = \langle x^\alpha : \alpha \in A \rangle$ un ideale monomiale ed f appartenente a $\mathbb{K}[x_1, \ldots, x_n]$. Allora le seguenti proprietà sono equivalenti:*

1. *$f \in I$;*
2. *ogni termine di f sta in I;*
3. *f è una combinazione lineare a coefficienti in $\mathbb{K}$ dei monomi contenuti in I.*

Dimostrazione. Il fatto che $3 \Rightarrow 2 \Rightarrow 1$ è banale. Proviamo allora che $1 \Rightarrow 3$.
Dire che f sta in I implica che f sia della forma

$$f = \sum_{\alpha \in A} h_\alpha x^\alpha.$$

Fissiamo l'attenzione su un $\alpha \in A$, consideriamo il polinomio $h_\alpha x^\alpha$ e lo espandiamo come combinazione lineare di monomi a coefficienti in $\mathbb{K}$. Ciascuno di questi monomi è divisibile per x^α e quindi, per la Proposizione 1.1.58, sta in I. Per la generalità di α abbiamo che ciascun $h_\alpha x^\alpha$ è combinazione lineare a coefficienti in $\mathbb{K}$ dei monomi di I, e dunque lo è anche f. □

Teorema 1.1.60. (Lemma di Dickson)
Sia $I = \langle x^\alpha : \alpha \in A \rangle$ un ideale monomiale. Allora I può essere scritto nella forma $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, dove $\alpha_1, \ldots, \alpha_s \in A$. In particolare, I ammette una base finita.

Dimostrazione. Cominciamo a provare che I ammette una base finita formata da soli monomi, cioè che $I = \langle x^{\beta_1}, \ldots, x^{\beta_l} \rangle$. Per il Teorema della Base di Hilbert (Teorema 1.1.17), $I = \langle f_1, \ldots, f_t \rangle$ per certi $f_i \in \mathbb{K}[x_1, \ldots, x_n]$, $i \in \{1, \ldots, t\}$. Poiché ciascun f_i sta anche in I, per la Proposizione 1.1.59 abbiamo che:

$$f_i = \sum_{\alpha \in A} c_\alpha x^\alpha$$

per ogni $i \in \{1, \ldots, t\}$, $c_\alpha \in \mathbb{K}$, e ci sono solo un numero finito di addendi non nulli nella sommatoria. L'insieme di tutti i monomi che compaiono nelle espressioni degli f_i genera I e tali monomi sono in numero finito. Questo conclude la prima parte della dimostrazione.
Proviamo ora che I può essere scritto nella forma $I = \langle x^{\alpha_1}, \ldots, x^{\alpha_s} \rangle$, dove $\alpha_1, \ldots, \alpha_s \in A$. Sappiamo, per la parte precedente, che possiamo scrivere $I = \langle x^{\beta_1}, \ldots, x^{\beta_l} \rangle$. Dal momento che x^{β_i} sta in I per ogni $i \in \{1, \ldots, l\}$, per la Proposizione 1.1.58 è divisibile per un qualche x^α tale che $\alpha \in A$. Ma allora è sufficiente considerare, al posto di ogni x^{β_i}, il monomio x^{α_i} che lo divide e abbiamo provato che gli elementi della base finita possono essere scelti tra i monomi che formano l'insieme di generatori dato. □

Giunti a questo punto abbiamo anche gli strumenti per dimostrare quanto affermato nella Nota 1.1.30, cioè:

Proposizione 1.1.61. *Sia $<$ una relazione sull'insieme T_n di tutti i monomi x^α in $\mathbb{K}[x_1, \ldots, x_n]$, tale che soddisfi le seguenti proprietà:*

1. *$<$ è una relazione di ordine totale;*
2. *$<$ è compatibile con la moltiplicazione in $\mathbb{K}[x_1, \ldots, x_n]$.*

Allora le seguenti affermazioni sono equivalenti tra di loro:

a. *$<$ è un buon ordinamento;*

b. *$1 < x^\alpha$ per ogni $\alpha \in \mathbb{N}^n$, $\alpha \neq (0, \ldots, 0)$;*

c. *$1 < x_i$ per ogni $i = 1, \ldots, n$.*

Dimostrazione. (a. $\Rightarrow$ b.) Supponiamo che ogni insieme non vuoto di monomi ammetta minimo. In particolare T_n deve ammetterlo e supponiamo che tale minimo sia x^α per un certo $\alpha \in \mathbb{N}^n$. Per la proprietà (1) deve essere $x^\alpha \leq 1$ e per la proprietà (2) questo vuol dire che $x^\alpha \cdot x^\alpha \leq x^\alpha$. Ma, per minimalità di x^α, si deve avere $x^{2\alpha} = x^\alpha$. Per l'uguaglianza tra polinomi questo è equivalente a chiedere che $2\alpha_i = \alpha_i$ per ogni $1 \leq i \leq n$, cioè $\alpha_i = 0$ per ogni i e quindi $x^\alpha = 1$.
(a. $\Leftarrow$ b.) Sia $S \subseteq \mathrm{T}_n$ un sottoinsieme dell'insieme di tutti i monomi. Posso considerare l'ideale $I = \langle S \rangle$ generato da tutti gli elementi di S. Tale ideale è un ideale monomiale e, per il Lemma di Dickson (Teorema 1.1.60), ammette una base finita. Cioè, $I = \langle x^{\alpha_1}, x^{\alpha_2}, \ldots, x^{\alpha_m} \rangle$ per certi $x^{\alpha_1}, x^{\alpha_2}, \ldots, x^{\alpha_m} \in S$ che posso supporre così ordinati:

$$x^{\alpha_1} < x^{\alpha_2} < \cdots < x^{\alpha_m}.$$

Affermo e provo che x^{α_1} è l'elemento minimo in S. Sia x^β in S; allora $x^\beta \in I$ e, per la Proposizione 1.1.58, questo significa che x^β è divisibile per un qualche x^{α_i}. Cioè, esiste un $x^\gamma \in \mathrm{T}_n$ tale che $x^\beta = x^{\alpha_i} \cdot x^\gamma$. Poiché, per ipotesi, $1 < x^\gamma$, abbiamo che:

$$x^\beta = x^{\alpha_i} \cdot x^\gamma > x^{\alpha_i} \cdot 1 = x^{\alpha_i} \geq x^{\alpha_1}.$$

(b. $\Rightarrow$ c.) Ovvio. Infatti, per ogni $i \in \{1, \ldots, n\}$, risulta che $x_i = x^\alpha$ dove $\alpha = (0, \ldots, \underbrace{1}_{i\text{-esima}}, \ldots, 0)$.
(b. $\Leftarrow$ c.) Dal momento che $<$ è compatibile col prodotto in $\mathbb{K}[x_1, \ldots, x_n]$ e che $1 < x_i$, risulta $1 < x_i^{\alpha_i}$ per ogni $i = 1, \ldots, n$ e per ogni $\alpha_i \in \mathbb{N}$: vale infatti la catena

$$1 < x_i < x_i^2 < \cdots < x_i^{\alpha_i}.$$

Sia ora x^α un monomio in $\mathbb{K}[x_1, \ldots, x_n]$, $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Poiché $<$ è compatibile col prodotto e $1 < x_i^{\alpha_i}$ per ogni $i \in \{1, \ldots, n\}$, vale:

$$1 < x_1^{\alpha_1} < x_1^{\alpha_1} x_2^{\alpha_2} < \cdots < x_1^{\alpha_1} \cdots x_n^{\alpha_n} = x^\alpha$$

per ogni $\alpha \in \mathbb{N}^n$ e questo conclude la dimostrazione. □

Definizione 1.1.62. Sia S un sottoinsieme di $\mathbb{K}[x_1, \ldots, x_n]$, indichiamo con $\mathrm{lt}(S)$ l'insieme

$$\mathrm{lt}(S) = \{\mathrm{lt}(f) : f \in S\}$$

e definiamo *ideale dei termini iniziali di* S l'ideale

$$\langle \mathrm{lt}(S) \rangle = \langle \mathrm{lt}(f) : f \in S \rangle$$

Osservazione 1.1.63. L'ideale $\langle \mathrm{lt}(S) \rangle = \langle \mathrm{lt}(f) : f \in S \rangle$ è un ideale monomiale.

Lemma 1.1.64. *Se* $\langle lt(G) \rangle = \langle lt(I) \rangle$*, dove* $G = \{g_1, \ldots, g_t\}$*, allora* G *è una base di Gröbner per* I *(e viceversa).*

Dimostrazione. Sia $f \in I$. Per ipotesi $\mathrm{lt}(f) \in \langle \mathrm{lt}(G) \rangle$ e dunque, per la Proposizione 1.1.58, $\mathrm{lt}(f)$ deve essere divisibile per almeno uno tra i $\mathrm{lt}(g_i)$. Ciò prova che G è una base di Gröbner per definizione.
Il viceversa è banale. □

Proposizione 1.1.65. *Ogni ideale* I *di* $\mathbb{K}[x_1, \ldots, x_n]$ *ammette una base di Gröbner.*

Dimostrazione. Poiché $\langle \mathrm{lt}(I) \rangle$ è un ideale di $\mathbb{K}[x_1, \ldots, x_n]$, per il Teorema della Base di Hilbert (Teorema 1.1.17) ammette un insieme finito di generatori. Per il Lemma di Dickson (Teorema 1.1.60) possiamo assumere che tale insieme di generatori sia della forma $\{\mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t)\}$, con $g_1, \ldots, g_t \in I$. Se poniamo $G = \{g_1, \ldots, g_t\}$, allora abbiamo che $\langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(I) \rangle$ e quindi G è una base di Gröbner per il Lemma 1.1.64. □

Riportiamo un ultimo lemma tecnico che può tornare utile.

Lemma 1.1.66. *Sia* G *una base di Gröbner per l'ideale* I*. Sia* $p \in G$ *un polinomio tale che* $lt(p) \in \langle lt(G - \{p\}) \rangle$*. Allora* $G - \{p\}$ *è ancora una base di Gröbner per* I*.*

Dimostrazione. Per il Lemma 1.1.64 sappiamo che $\langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(I) \rangle$. Se $\mathrm{lt}(p) \in \langle \mathrm{lt}(G - \{p\}) \rangle$, allora abbiamo che $\langle \mathrm{lt}(G - \{p\}) \rangle = \langle \mathrm{lt}(G) \rangle$ e dunque anche $G - \{p\}$ è una base di Gröbner per I. □

1.2 Varietà affini

Definizione 1.2.1. Dati un campo $\mathbb{K}$ e un numero naturale $n \in \mathbb{N}$, definiamo lo *spazio affine* n*-dimensionale* su $\mathbb{K}$ come l'insieme delle n-uple:

$$\mathbb{K}^n = \{(a_1, \ldots, a_n) : a_i \in \mathbb{K}, \ \forall\, i = 1, \ldots, n\}$$

Definizione 1.2.2. (*varietà affine*)
Sia $\mathbb{K}$ un campo e siano $f_1, \ldots, f_s$ polinomi in $\mathbb{K}[x_1, \ldots, x_n]$. Chiamiamo *varietà affine* definita da $f_1, \ldots, f_s$ l'insieme di tutte le soluzioni $(a_1, \ldots, a_n) \in \mathbb{K}^n$ del sistema di equazioni polinomiali:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ f_2(x_1, \ldots, x_n) = 0 \\ \qquad \vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases} \tag{1.4}$$

e la denotiamo con $\mathbf{V}(f_1, \ldots, f_s)$. Un sottoinsieme V di $\mathbb{K}^n$ è una *varietà affine* se $V = \mathbf{V}(f_1, \ldots, f_s)$ per qualche insieme di polinomi $f_i \in \mathbb{K}[x_1, \ldots, x_n]$.

Esempio 1.2.3. Consideriamo il polinomio $x^4 - y^2 \in \mathbb{R}[x, y]$. La varietà affine $V = \mathbf{V}(x^4 - y^2)$ è un insieme infinito di punti della forma $(t, \pm t^2)$ (graficamente si tratta dell'unione delle due parabole $y = x^2$ e $y = -x^2$).
Se consideriamo invece i polinomi $xy - 1$ e $x^2 + 4y^2 - 5$ in $\mathbb{R}[x, y]$, questi generano una varietà finita:

$$\mathbf{V}(xy - 1, x^2 + 4y^2 - 5) = \left\{(1, 1), (-1, -1), \left(2, \tfrac{1}{2}\right), \left(-2, -\tfrac{1}{2}\right)\right\},$$

come si può facilmente verificare svolgendo i calcoli (graficamente si tratta dell'intersezione dell'ellisse di equazione $x^2 + 4y^2 - 5 = 0$ con l'iperbole $xy = 1$).

Preso un qualunque elemento g in $\langle f_1, \ldots, f_s\rangle$, si vede che $g(a_1, \ldots, a_n) = 0$, per ogni $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s)$. Questa semplice osservazione, insieme al Teorema della Base di Hilbert, ci permette di pensare alle varietà affini come definite da ideali di $\mathbb{K}[x_1, \ldots, x_n]$, invece che da particolari insiemi di polinomi.

Definizione 1.2.4. Sia I un ideale di $\mathbb{K}[x_1, \ldots, x_n]$. Indichiamo con $\mathbf{V}(I)$ l'insieme:

$$\mathbf{V}(I) = \{(a_1, \ldots, a_n) \in \mathbb{K}^n : f(a_1, \ldots, a_n) = 0 \text{ per ogni } f \in I\}$$

Proposizione 1.2.5. *Sia I un ideale di $\mathbb{K}[x_1, \ldots, x_n]$, allora $\mathbf{V}(I)$ è una varietà affine. In particolare, se $I = \langle f_1, \ldots, f_s\rangle$, allora $\mathbf{V}(I) = \mathbf{V}(f_1, \ldots, f_s)$.*

Dimostrazione. Per il Teorema della Base di Hilbert sappiamo che $I = \langle f_1, \ldots, f_s\rangle$, per un certo insieme finito di generatori. Procediamo allora per doppia inclusione.
$\mathbf{V}(I) \subseteq \mathbf{V}(f_1, \ldots, f_s)$: Sia $(a_1, \ldots, a_n) \in \mathbf{V}(I)$. Dal momento che $f_i \in I$ per ogni $i = 1, \ldots, s$, e poiché $f(a_1, \ldots, a_n) = 0$ per ogni $f \in I$, risulta che $f_i(a_1, \ldots, a_n) = 0$. Per definizione, allora, $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s)$.
$\mathbf{V}(I) \supseteq \mathbf{V}(f_1, \ldots, f_s)$: Sia $(a_1, \ldots, a_n) \in \mathbf{V}(f_1, \ldots, f_s)$ e sia $f \in I$. Possiamo scrivere che

$$f = \sum_{i=1}^{s} h_i f_i$$

per certi $h_i \in \mathbb{K}[x_1, \ldots, x_n]$. Ma allora:

$$\begin{aligned} f(a_1, \ldots, a_n) &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot f_i(a_1, \ldots, a_n) \\ &= \sum_{i=1}^{s} h_i(a_1, \ldots, a_n) \cdot 0 = 0. \end{aligned}$$

E dunque $(a_1, \ldots, a_n) \in \mathbf{V}(I)$. □

Corollario 1.2.6. *Siano $\{f_1, \ldots, f_s\}$ e $\{g_1, \ldots, g_t\}$ due insiemi di generatori dello stesso ideale di $\mathbb{K}[x_1, \ldots, x_n]$, cioè $\langle f_1, \ldots, f_s\rangle = \langle g_1, \ldots, g_t\rangle$. Allora $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}(g_1, \ldots, g_t)$.*

Dunque, una varietà dipende solo dall'ideale I generato dai polinomi associati alle equazioni che la definiscono e non dai particolari polinomi presi in considerazione. Vale inoltre la seguente proprietà:

Proposizione 1.2.7. *Siano $I, J \subseteq \mathbb{K}[x_1, \ldots, x_n]$ due ideali tali che $I \subseteq J$, allora $\mathbf{V}(I) \supseteq \mathbf{V}(J)$.*

Dimostrazione. Sia $a = (a_1, \ldots, a_n) \in \mathbf{V}(J)$. Questo implica che $g(a) = 0$, per ogni $g \in J$. In particolare, $f(a) = 0$ per tutti gli $f \in I \subseteq J$, e dunque $a \in \mathbf{V}(I)$. □

Osservazione 1.2.8. Sappiamo che se $V = \mathbf{V}(f_1, \ldots, f_s)$ è una varietà affine, allora tutti i polinomi in $\langle f_1, \ldots, f_s \rangle$ si annullano su ogni punto di V. La domanda che sorge ora è: Questi polinomi sono *tutti* i polinomi che si annullano su ogni punto di V? La risposta è no, come mostra l'esempio seguente.

Esempio 1.2.9. La varietà $\mathbf{V}(x^2) \subset \mathbb{C}^2$ è formata da tutti i punti per i quali risulta $x = 0$, cioè tutto l'asse y. Il polinomio $f = x \in \mathbb{C}[x, y]$ è tale che $f(0, t) = 0$ per ogni $(0, t) \in \mathbf{V}(x^2)$. Tuttavia $x \notin \langle x^2 \rangle$. Questo conduce allora a dare la seguente definizione.

Definizione 1.2.10. (*vanishing ideal*)
Sia $V \subset \mathbb{K}^n$ una varietà affine. Definiamo *vanishing ideal* di V l'insieme

$$\mathbf{I}(V) = \{f \in \mathbb{K}[x_1, \ldots, x_n] : f(a_1, \ldots, a_n) = 0 \text{ per ogni } (a_1, \ldots, a_n) \in V\}$$

Il nome 'vanishing ideal' non è dato caso, come conferma la seguente:

Proposizione 1.2.11. *Se $V \subseteq \mathbb{K}^n$ una varietà affine, allora $\mathbf{I}(V)$ è un ideale di $\mathbb{K}[x_1, \ldots, x_n]$.*

Dimostrazione. Siano $f, g \in \mathbf{I}(V)$, $h \in \mathbb{K}[x_1, \ldots, x_n]$ e $(a_1, \ldots, a_n)$ un punto qualsiasi di V. Allora abbiamo che:

$$(f + g)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0,$$

$$(h \cdot f)(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot f(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot 0 = 0$$

e dunque $\mathbf{I}(V)$ è un ideale. □

Dati $f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$, possiamo allora costruire:

$$\begin{array}{ccccc} \text{ideale} & & \text{varietà} & & \text{ideale} \\ \langle f_1, \ldots, f_s \rangle & \rightarrow & \mathbf{V}(f_1, \ldots, f_s) & \rightarrow & \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s)) \end{array}$$

Questo fa però sorgere una domanda: quand'è che vale $\langle f_1, \ldots, f_s \rangle = \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$? Ovviamente non sempre, come abbiamo già visto nell'Esempio 1.2.9. La risposta sarà fornita dal celebre *Nullstellensatz*, o *Teorema degli zeri*, di Hilbert.

1.2.1 Il Nullstellensatz di Hilbert

Quelle trattate in questo scritto sono particolari varietà affini, formate da un numero finito di punti. Per quanto visto nel paragrafo precedente una varietà è definita da un sistema di equazioni polinomiali. Una prima informazione fondamentale dunque, è sapere quando un dato sistema di equazioni polinomiali ammetta o meno una soluzione. Il Nullstellensatz fornisce anche una risposta a questo interrogativo ed è quindi un primo passo concreto verso lo studio delle varietà di punti. Vedremo infatti che fornisce un criterio per decidere quando $\mathbf{V}(f_1, \ldots, f_s) = \emptyset$.
Del Nullstellensatz esistono più versioni, riportiamo qui solo quelle che ci serviranno. Prima però occorre dimostrare alcune proprietà indispensabili.

Lemma 1.2.12. *Sia $\mathbb{K}$ un campo algebricamente chiuso e non numerabile e sia M un ideale massimale di $\mathbb{K}[x_1, \ldots, x_n]$. Allora $\mathbb{K}[x_1, \ldots, x_n]/M \cong \mathbb{K}$.*

Dimostrazione. Sappiamo che $\mathbb{K}[x_1, \ldots, x_n]/M = \mathbb{F}$ è un campo (vedi Teorema 1.1.28). Ovviamente, la proiezione canonica sul quoziente:

$$\pi \colon \mathbb{K}[x_1, \ldots, x_n] \to \mathbb{K}[x_1, \ldots, x_n]/M$$

mappa $\mathbb{K}$ in se stesso; dunque abbiamo che $\mathbb{F}$ è un'estensione di $\mathbb{K}$ e possiamo vedere $\mathbb{F}$ come $\mathbb{K}$-spazio vettoriale. Ora, $\mathbb{K}[x_1, \ldots, x_n]$ ha dimensione al più numerabile come $\mathbb{K}$-spazio vettoriale, perché è generato dai monomi di T_n. Allora $\dim_{\mathbb{K}}(\mathbb{F})$ è sicuramente al più numerabile, perché $\mathbb{F}$ è ottenuto come quoziente di $\mathbb{K}[x_1, \ldots, x_n]$.
Supponiamo, per assurdo, che $\mathbb{F}$ sia un'estensione propria di $\mathbb{K}$, cioè che esista un $t \in \mathbb{F}$ tale che $t \notin \mathbb{K}$. Dal momento che $\mathbb{K}$ è algebricamente chiuso, si deve necessariamente avere che t è trascendente su $\mathbb{K}$. Consideriamo allora il seguente sottoinsieme di $\mathbb{F}$:

$$U = \left\{ \frac{1}{t - c} : c \in \mathbb{K} \right\}.$$

U è non numerabile, perché indicizzato dall'insieme $\mathbb{K}$ (che è supposto non numerabile), e andiamo a provare che è formato da elementi linearmente indipendenti su $\mathbb{K}$. Se gli elementi di U fossero linearmente dipendenti, esisterebbero degli $a_1, \ldots, a_r \in \mathbb{K}$ non nulli e dei $c_1, \ldots, c_r \in \mathbb{K}$ distinti, tali che

$$\sum_{i=1}^{r} \frac{a_i}{t - c_i} = 0.$$

Eliminando i denominatori, otteniamo un polinomio $h(t) \in \mathbb{K}[t]$:

$$h(t) = \sum_{i=1}^{r} a_i (t - c_1)(t - c_2) \cdots \widehat{(t - c_i)} \cdots (t - c_n) = 0$$

(Il simbolo $\widehat{(t - c_i)}$ sta a indicare che quel fattore non compare). Ma, poiché $h(c_1) = a_1(c_1 - c_2)(c_1 - c_3) \cdots (c_1 - c_n) \neq 0$, $h(t)$ non è il polinomio nullo e ammette t come radice, contro l'ipotesi di trascendenza di t. Quindi U è un insieme di cardinalità non numerabile di elementi linearmente indipendenti dentro a uno spazio vettoriale di dimensione al più numerabile. Assurdo.
Allora $\mathbb{F} = \mathbb{K}$ e abbiamo concluso. □

Proposizione 1.2.13. *Sia $\mathbb{K}$ un campo algebricamente chiuso (e non numerabile), allora ogni ideale massimale M in $\mathbb{K}[x_1, \ldots, x_n]$ è della forma*

$$M = \langle x_1 - a_1, \ldots, x_n - a_n \rangle,$$

dove $a = (a_1, \ldots, a_n) \in \mathbb{K}^n$.

Dimostrazione. Sia M un ideale massimale di $\mathbb{K}[x_1, \ldots, x_n]$: per il Lemma 1.2.12 sappiamo che $\mathbb{K}[x_1, \ldots, x_n]/M$ e $\mathbb{K}$ sono isomorfi. Siano allora

$$\varphi \colon \mathbb{K}[x_1, \ldots, x_n]/M \to \mathbb{K}$$

un tale isomorfismo,

$$\pi\colon \mathbb{K}[x_1,\dots,x_n] \to \mathbb{K}[x_1,\dots,x_n]/M$$

la proiezione canonica e consideriamo $\psi = \varphi \circ \pi : \mathbb{K}[x_1,\dots,x_n] \to \mathbb{K}$.
ψ è un epimorfismo di anelli, dunque esistono degli $a_i \in \mathbb{K}$ $(1 \leq i \leq n)$ tali che $\psi(x_i) = a_i$, da cui:

$$\begin{aligned}\psi(x_i) &= (\varphi \circ \pi)(x_i) = \varphi(\pi(x_i)) \\ &= \varphi(x_i + M) = a_i.\end{aligned}$$

Pertanto, esistono costanti $a_i \in \mathbb{K}$ tali che $x_i + M = a_i + M$ per ogni $i = 1,\dots,n$, ma allora $x_i - a_i \in M$ e dunque

$$\langle x_1 - a_1, \dots, x_n - a_n\rangle \subseteq M.$$

Proviamo ora che $\langle x_1 - a_1, \dots, x_n - a_n\rangle$ è massimale. Sia $a = (a_1,\dots,a_n) \in \mathbb{K}^n$ e consideriamo l'epimorfismo di anelli

$$\begin{array}{rccc}\eta\colon & \mathbb{K}[x_1,\dots,x_n] & \to & \mathbb{K} \\ & f & \mapsto & f(a)\end{array}.$$

Osserviamo che

$$\begin{aligned}\ker(\eta) = \mathbf{I}(a) &= \{f \in \mathbb{K}[x_1,\dots,x_n] : f(a) = 0\} \\ &= \{f = g_1(x_1 - a_1) + \cdots + g_n(x_n - a_n) : g_i \in \mathbb{K}[x_1,\dots,x_n]\} \\ &= \langle x_1 - a_1, \dots, x_n - a_n\rangle\end{aligned}$$

Questo implica che $\mathbb{K}[x_1,\dots,x_n]/\mathbf{I}(a)$ è un campo, e dunque che $\mathbf{I}(a)$ è massimale. Ma allora, per massimalità, $M = \langle x_1 - a_1, \dots, x_n - a_n\rangle$. □

Teorema 1.2.14. (Nullstellensatz (debole))
Sia $\mathbb{K}$ un campo algebricamente chiuso e sia $I \subseteq \mathbb{K}[x_1,\dots,x_n]$ un ideale tale che $\mathbf{V}(I) = \emptyset$, allora $I = \mathbb{K}[x_1,\dots,x_n]$. Equivalentemente, se I è un ideale proprio di $\mathbb{K}[x_1,\dots,x_n]$, allora $\mathbf{V}(I) \neq \emptyset$.

Nota 1.2.15. Ne daremo ora la dimostrazione nel caso in cui $\mathbb{K}$ sia non numerabile. Questo perché ricorreremo al risultato della Proposizione 1.2.13, dove abbiamo supposto che $\mathbb{K}$ lo sia. In realtà il Teorema 1.2.14 vale anche qualora non lo sia e lo stesso vale per la Proposizione 1.2.13; la dimostrazione in quel caso, però, richiede ulteriori strumenti teorici e esula dagli scopi di questa trattazione[5].

Dimostrazione. Se I è un ideale proprio di $\mathbb{K}[x_1,\dots,x_n]$ allora, dal momento che $\mathbb{K}[x_1,\dots,x_n]$ è Noetheriano, esiste un ideale massimale M che lo contiene (se così non fosse, potrei costruire una catena ascendente infinita di ideali contenenti I). Per la Proposizione 1.2.13, esiste un $(a_1,\dots,a_n) \in \mathbb{K}^n$ tale che $M = \langle x_1 - a_1, \dots, x_n - a_n\rangle$. Ora, per la Proposizione 1.2.7, $I \subseteq M$ implica che $\mathbf{V}(I) \supseteq \mathbf{V}(M) \ni (a_1,\dots,a_n)$, e quindi $\mathbf{V}(I) \neq \emptyset$. □

[5]Per la dimostrazione del caso generale si faccia riferimento a [Rot], pagina 931 e seguenti.

Osservazione 1.2.16. Nel caso in cui $\mathbb{K} = \mathbb{C}$, il Nullstellensatz può essere riletto come una sorta di generalizzazione del Teorema Fondamentale dell'Algebra per polinomi in più indeterminate: ogni insieme di polinomi che genera un ideale strettamente contenuto in $\mathbb{K}[x_1, \ldots, x_n]$, ha una radice comune in $\mathbb{K}^n$.

Corollario 1.2.17. *Sia*

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ f_2(x_1, \ldots, x_n) = 0 \\ \qquad \vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases}$$

un sistema di equazioni polinomiali. Tale sistema ammette almeno una soluzione se e solo se $\mathbf{V}(f_1, \ldots, f_s) \neq \emptyset$*, cioè se e solo se* $1 \notin \langle f_1, \ldots, f_s \rangle$.

Osservazione 1.2.18. Come conseguenza del precedente Corollario, per decidere se il sistema di equazioni ammetta o no una soluzione è sufficiente calcolare una base di Gröbner per $\langle f_1, \ldots, f_s \rangle$ rispetto a un qualsiasi ordine monomiale. Se tale base risulta essere $\{1\}$, allora il sistema non ammette soluzioni. Vale infatti la seguente proprietà.

Proposizione 1.2.19. *Siano* I *un ideale di* $\mathbb{K}[x_1, \ldots, x_n]$ *e* G *una base di Gröbner per* I*.* $G = \{1\}$ *se e solo se* $I = \langle 1 \rangle = \mathbb{K}[x_1, \ldots, x_n]$.

Dimostrazione. ($\Leftarrow$): Sia $G = \{g_1, \ldots, g_t\}$ una base di Gröbner per $I = \langle 1 \rangle$. Di conseguenza, $1 \in \langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_t) \rangle$. Allora, per la Proposizione 1.1.58, 1 è divisibile per un qualche $\mathrm{lt}(g_i)$ $(i = 1, \ldots, t)$; supponiamo, senza perdere in generalità, che sia g_1. Questo forza $\mathrm{lt}(g_1)$ a essere una costante; dunque $\mathrm{lt}(g_2), \ldots, \mathrm{lt}(g_t)$ sono tutti divisibili per $\mathrm{lt}(g_1)$ e, per il Lemma 1.1.66, possono essere rimossi da G. Inoltre, poiché $\mathrm{lt}(g_1)$ è una costante, g_1 stesso è un polinomio costante (dato un qualsiasi ordine monomiale $<$, per la Proposizione 1.1.61 risulta $1 < x^\alpha$, per ogni monomio non costante x^α). Possiamo allora riscalare g_1 per un'opportuna costante di modo che $g_1 = 1$ e $G = \{1\}$.
($\Rightarrow$): Sia $G = \{1\}$ una base di Gröbner per I rispetto a un ordine monomiale $<$. Poiché $1 \in \langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(I) \rangle$ abbiamo che esiste un $f \in I$ tale che $\mathrm{lt}(f)$ divide 1. Per un discorso analogo a quello precedente, questo implica che $f = 1 \in I$ e dunque $I = \mathbb{K}[x_1, \ldots, x_n]$. □

Esempio 1.2.20. Abbiamo visto, nell'Esempio 1.2.3, che il sistema:

$$\begin{cases} xy - 1 = 0 \\ x^2 + 4y^2 - 5 = 0 \end{cases}$$

ammette 4 soluzioni in $\mathbb{C}[x, y]$.
Se calcolassimo una base di Gröbner per $I = \langle xy - 1, x^2 + 4y^2 - 5 \rangle$ rispetto all'ordinamento *lex*, otterremmo $\{4y^4 - 5y^2 + 1, x + 4y^3 - 5y\} \neq \{1\}$.
Se invece consideriamo il sistema:

$$\begin{cases} x^2y - 2x + y = 0 \\ x^2 + 1 = 0 \end{cases}$$

questo non ammette soluzione, come si può facilmente verificare, e infatti l'ideale generato dai due polinomi ammette $\{1\}$ come base di Gröbner.

Teorema 1.2.21. (Nullstellensatz di Hilbert)
Sia $\mathbb{K}$ un campo algebricamente chiuso. Se $f, f_1, \ldots, f_s \in \mathbb{K}[x_1, \ldots, x_n]$ sono polinomi tali che $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$, allora esiste un intero $m \geq 1$ tale che

$$f^m \in \langle f_1, \ldots, f_s \rangle$$

(e viceversa).

Dimostrazione. Dato un polinomio f che si annulla ogniqualvolta viene valutato su una radice comune ai polinomi $f_1, \ldots, f_s$, dobbiamo provare che esiste un intero $m \geq 1$ e polinomi $p_1, \ldots, p_s \in \mathbb{K}[x_1, \ldots, x_n]$ tali che

$$f^m = \sum_{i=1}^{s} p_i f_i.$$

Consideriamo allora l'ideale

$$J = \langle f_1, \ldots, f_s, 1 - yf \rangle \subset \mathbb{K}[x_1, \ldots, x_n, y],$$

dove f e gli f_i sono tali che $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$ e proviamo che $\mathbf{V}(J) = \emptyset$.
Sia $(a_1, \ldots, a_n, a_{n+1}) \in \mathbb{K}^{n+1}$; abbiamo due possibilità:

1. $(a_1, \ldots, a_n)$ è una radice comune a tutti gli f_i, oppure
2. $(a_1, \ldots, a_n)$ non è una radice comune a tutti gli f_i.

Nel primo caso, poiché $f \in \mathbf{I}(\mathbf{V}(f_1, \ldots, f_s))$, abbiamo che $f(a_1, \ldots, a_n) = 0$ e allora il polinomio $1 - yf$ assume in $(a_1, \ldots, a_n, a_{n+1})$ il valore: $1 - a_{n+1} f(a_1, \ldots, a_n) = 1 \neq 0$. In particolare $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(J)$.
Nel secondo caso esiste un i, $1 \leq i \leq s$, tale per cui $f_i(a_1, \ldots, a_n) \neq 0$. In particolare, abbiamo nuovamente che $(a_1, \ldots, a_n, a_{n+1}) \notin \mathbf{V}(J)$. Per la generalità di $(a_1, \ldots, a_n, a_{n+1})$, concludiamo che $\mathbf{V}(J) = \emptyset$.
Ora, per il Nullstellensatz nella formulazione debole, abbiamo che $1 \in J$, cioè:

$$1 = \sum_{i=1}^{s} q_i(x_1, \ldots, x_n, y) f_i + q(x_1, \ldots, x_n, y)(1 - yf)$$

per certi $q_i, q \in \mathbb{K}[x_1, \ldots, x_n, y]$. Se adesso poniamo $y = \frac{1}{f}$, otteniamo

$$1 = \sum_{i=1}^{s} q_i \left(x_1, \ldots, x_n, \tfrac{1}{f} \right) f_i \tag{1.5}$$

e, moltiplicando entrambi i membri di (1.5) per una potenza f^m, dove m è sufficientemente grande da eliminare tutti i denominatori, risulta:

$$f^m = \sum_{i=1}^{s} p_i(x_1, \ldots, x_n) f_i,$$

per certi polinomi $p_i \in \mathbb{K}[x_1, \ldots, x_n]$, che è proprio ciò che volevamo ottenere. □

Giungiamo ora all'ultima formulazione del Nullstellensatz, cioè l'analogo del Nullstellensatz di Hilbert riletto in termini di ideali. Prima però servono ancora un paio di definizioni.

Definizione 1.2.22. (*ideale radicale*)
Un ideale I si dice *radicale* se, ogniqualvolta f^m appartiene a I per un certo intero $m \geq 1$, si ha che f appartiene a I.

Definizione 1.2.23. (*radicale di un ideale*)
Sia I un ideale di $\mathbb{K}[x_1, \ldots, x_n]$. Il *radicale di* I, indicato con $\sqrt{I}$, è l'insieme:

$$\sqrt{I} = \{f \in K[x_1, \ldots, x_n] : f^m \in I \text{ per qualche intero } m \geq 1\}$$

Proposizione 1.2.24. *Se I è un ideale di $\mathbb{K}[x_1, \ldots, x_n]$, allora $\sqrt{I}$ è un ideale di $\mathbb{K}[x_1, \ldots, x_n]$ che contiene I. Inoltre, $\sqrt{I}$ è radicale.*

Dimostrazione. Ovviamente $I \subseteq \sqrt{I}$: basta infatti osservare che dire che $f \in I$ è equivalente a dire che $f^1 \in I$ e dunque $f \in \sqrt{I}$ per definizione.
Proviamo che si tratta di un ideale. Siano $f, g \in \mathbb{K}[x_1, \ldots, x_n]$ tali che $f^m, g^l \in I$ e consideriamo

$$(f+g)^{m+l} = \sum_{k=0}^{m+l} \binom{m+l}{k} f^k g^{m+l-k}.$$

Per ogni $k = 0, \ldots, m+l$, o f^k o g^{m+l-k} stanno in I, quindi $f^k g^{m+l-k}$ sta in I e allora $(f+g)^{m+l}$ sta in I. Questo implica che $f + g \in \sqrt{I}$.
Sia ora, inoltre, $h \in K[x_1, \ldots, x_n]$. Poiché I è un ideale, $(hf)^m = h^m f^m \in I$ e quindi $hf \in \sqrt{I}$, come volevasi dimostrare.
Resta solo più da provare che si tratta di un ideale radicale. Sia $f \in \mathbb{K}[x_1, \ldots, x_n]$ tale che $f^m \in \sqrt{I}$ per un certo intero $m \geq 1$. Questo vuol dire che esiste un intero $n \geq 1$ tale per cui $(f^m)^n = f^{mn} \in I$. Ma allora, per definizione di radicale di I, $f \in \sqrt{I}$ e abbiamo concluso. □

Teorema 1.2.25. (Nullstellensatz (forte))
Sia $\mathbb{K}$ un campo algebricamente chiuso. Se I è un ideale di $\mathbb{K}[x_1, \ldots, x_n]$, allora

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

Dimostrazione. Ovviamente abbiamo che $\sqrt{I} \subseteq \mathbf{I}(\mathbf{V}(I))$: se $f \in \sqrt{I}$ allora esiste un intero $m \geq 1$ tale per cui $f^m \in I$; quindi f^m si annulla in ogni punto di $\mathbf{V}(I)$ e, di conseguenza, anche f si annulla in ogni punto di $\mathbf{V}(I)$, da cui: $f \in \mathbf{I}(\mathbf{V}(I))$.
Viceversa, supponiamo che $f \in \mathbf{I}(\mathbf{V}(I))$. Allora, per definizione, f si annulla in ogni punto di $\mathbf{V}(I)$. Per il Nullstellensatz di Hilbert (Teorema 1.2.21), questo è equivalente a dire che esiste un intero $m \geq 1$ tale per cui $f^m \in I$. Ma allora, per definizione, $f \in \sqrt{I}$ e, per l'arbitrarietà di f, abbiamo che $\mathbf{I}(\mathbf{V}(I)) \subseteq \sqrt{I}$. □

Nota 1.2.26. D'ora in avanti ci riferiremo alla formulazione forte del Nullstellensatz come *al Nullstellensatz*, senza altre aggiunte.
Nonostante la dimostrazione che ne abbiamo dato valga per il caso in cui $\mathbb{K}$ è non numerabile, ricordiamo che questa ipotesi non è vincolante e può essere rimossa.
L'ipotesi $\mathbb{K}$ algebricamente chiuso invece è imprescindibile, come mostra l'esempio seguente.

Esempio 1.2.27. Sia $f = x^2 + y^2 + 1 \in \mathbb{R}[x, y]$. Si vede immediatamente che $\mathbb{R}^2 \supset \mathbf{V}(f) = \emptyset$, tuttavia $x \notin \langle f \rangle$ e dunque $\langle f \rangle \subset \mathbb{R}[x, y]$. Inoltre, $x^4 + y^4 + 1$ appartiene a $\mathbf{I}(\mathbf{V}(f))$, ma non esiste un $m \in \mathbb{N}$ tale che $(x^4 + y^4 + 1)^m \in \langle f \rangle$ e, d'altro canto, $\mathbf{I}(\mathbf{V}(f)) = \mathbb{R}[x, y] \supset \sqrt{\langle f \rangle}$.
Quindi, su $\mathbb{R}$ (non algebricamente chiuso) non valgono né la formulazione debole, né la formulazione forte del Nullstellensatz, né il Nullstellensatz di Hilbert.

1.3 Algebre e ideali zero-dimensionali

Definizione 1.3.1. (*algebra*)
Un'*algebra* su un campo $\mathbb{K}$ è un insieme A su cui sono definite una somma $+$, un prodotto $*$ e un prodotto per scalari $\cdot$ tali che $(A, +, *)$ sia un anello, $(A, +, \cdot)$ sia uno spazio vettoriale, e valga la proprietà associativa $(\lambda \cdot f) * g = \lambda \cdot (f * g) = f * (\lambda \cdot g)$ per ogni $\lambda \in \mathbb{K}$ e $f, g \in A$.

Sia I un ideale di $\mathbb{K}[x_1, \ldots, x_n]$. Consideriamo l'anello quoziente:

$$\mathbb{K}[x_1, \ldots, x_n]/I = \{[f] : f \in \mathbb{K}[x_1, \ldots, x_n]\},$$

dove $[f] = f + I = \{f + g \in \mathbb{K}[x_1, \ldots, x_n] : g \in I\}$.

Proposizione 1.3.2. *$\mathbb{K}[x_1, \ldots, x_n]/I$ ha la struttura di spazio vettoriale su $\mathbb{K}$.*

Dimostrazione. La verifica del fatto che la somma di laterali e il prodotto di un laterale per un elemento di $\mathbb{K}$ soddisfino le proprietà richieste per essere spazio vettoriale segue dalle proprietà dei laterali in $\mathbb{K}[x_1, \ldots, x_n]/I$ e di $\mathbb{K}[x_1, \ldots, x_n]$ stesso. □

Corollario 1.3.3. *$\mathbb{K}[x_1, \ldots, x_n]/I$ è un'algebra sul campo $\mathbb{K}$.*

Dimostrazione. È sufficiente verificare che valga la proprietà associativa, ma questa segue immediatamente dalle proprietà dei laterali in $\mathbb{K}[x_1, \ldots, x_n]/I$ e del prodotto di polinomi in $\mathbb{K}[x_1, \ldots, x_n]$. □

Sia inoltre $I = \langle g_1, \ldots, g_n \rangle$, con $G = \{g_1, \ldots, g_n\}$ base di Gröbner per I. Sappiamo che, per ogni elemento $f \in \mathbb{K}[x_1, \ldots, x_n]$, esiste un unico $r \in \mathbb{K}[x_1, \ldots, x_n]$ tale che $f \xrightarrow{G}_+ r$.

Definizione 1.3.4. (*forma normale*)
L'elemento r come sopra prende il nome di *forma normale di f* rispetto a G, e viene indicato con $N_G(f)$.

Definizione 1.3.5. (*insieme normale*)
Sia I un ideale in $\mathbb{K}[x_1, \ldots, x_n]$ e sia $<$ un ordine monomiale definito in $\mathbb{K}[x_1, \ldots, x_n]$. Sia $\langle \mathrm{lt}(I) \rangle$ l'ideale generato dai termini iniziali di tutti gli elementi di I. L'insieme N di tutti i monomi che non appartengono a $\langle \mathrm{lt}(I) \rangle$, cioè

$$N := \{t \in \mathrm{T}_n : t \notin \langle \mathrm{lt}(I) \rangle\},$$

viene chiamato *insieme normale* di I rispetto a $<$.

Osservazione 1.3.6. Per quanto provato nel Lemma 1.1.64, sappiamo che se I è un ideale proprio di $\mathbb{K}[x_1, \ldots, x_n]$, $<$ è un ordine monomiale e G è una base di Gröbner per I rispetto a $<$, allora $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(G) \rangle$. In tal caso trovare l'insieme normale di I rispetto a $<$ si riduce a cercare l'insieme:

$$\{t \in \mathrm{T}_n : t \notin \langle \mathrm{lt}(G) \rangle\} = \{t \in \mathrm{T}_n : t \notin \langle \mathrm{lt}(g_1), \ldots, \mathrm{lt}(g_s) \rangle\},$$

che risulta assai più semplice, come mostra l'esempio seguente.

Esempio 1.3.7. Consideriamo ancora l'ideale $I = \langle xy^2 + y^4, x^2 - xy \rangle$ dell'Esempio 1.1.52. Sappiamo che, introdotto l'ordinamento *lex*, una base di Gröbner per I è data da $G = \{xy^2 + y^4, x^2 - xy, y^6 + y^5\}$. Vogliamo trovare l'insieme normale N di I rispetto all'ordine $<_{\mathrm{lex}}$.
Cominciamo a osservare il seguente fatto: la Proposizione 1.1.58 ci assicura che se $\langle x^\alpha : \alpha \in A \rangle$ è un ideale monomiale, allora x^β vi appartiene se e solo se è divisibile per un qualche x^α. Questo significa che x^β sta in $\langle x^\alpha : \alpha \in A \rangle$ se e solo se soddisfa la relazione:

$$x^\beta = x^\alpha \cdot x^\gamma$$

per qualche $\gamma \in \mathbb{N}^n$, cioè $\beta = \alpha + \gamma$. Ma allora, l'insieme

$$\alpha + \mathbb{N}^n = \{\alpha + \gamma : \gamma \in \mathbb{N}^n\}$$

è formato dagli esponenti di tutti i monomi divisibili per x^α e dunque stanno in $\langle x^\alpha : \alpha \in A \rangle$ tutti quei monomi il cui vettore degli esponenti appartiene all'insieme

$$U = \bigcup_{\alpha \in A} (\alpha + \mathbb{N}^n).$$

Questa osservazione ci facilita notevolmente il compito, perché ora sappiamo che i monomi che non stanno in $\langle x^\alpha : \alpha \in A \rangle$ sono tutti quei monomi il cui vettore degli esponenti appartiene al complementare in $\mathbb{N}^n$ di U, cioè appartiene all'insieme

$$\bigcap_{\alpha \in A} (\mathbb{N}^n - (\alpha + \mathbb{N}^n)).$$

Vediamo sull'esempio come questo ci aiuta. Abbiamo che $\mathrm{lt}(G) = \{xy^2, x^2, y^6\}$; i vettori appartenenti a $\mathbb{N}^n - ((1,2) + \mathbb{N}^n)$ sono tutti i vettori $(\alpha, \beta) \in \mathbb{N}^n$ tali che $\alpha = 0$ oppure $\beta \leq 1$. Analogamente appartengono a $\mathbb{N}^n - ((2,0) + \mathbb{N}^n)$ tutti i vettori tali che $\alpha \leq 1$ e a $\mathbb{N}^n - ((0,6) + \mathbb{N}^n)$ tutti quelli tali che $\beta \leq 5$. Se ora prendiamo in considerazione l'intersezione dei tre insiemi ottenuti abbiamo trovato gli esponenti (e quindi i monomi) dell'insieme normale N:

$$N = \left\{1, x, y, xy, y^2, y^3, y^4, y^5\right\}$$

Se volessimo visualizzarli, potremmo procedere in questo modo: rappresentiamo sul piano cartesiano il reticolo dei punti a coordinate intere, di cui però consideriamo solo il primo quadrante; segnamo il punto $(1,2)$ e evidenziamo l'area di piano tale per cui $x \geq 1$ e $y \geq 2$, segnamo il punto $(2,0)$ e evidenziamo l'area per cui $x \geq 2$ e $y \geq 0$ e ripetiamo la stessa operazione anche per $(0,6)$; terminato ciò, i punti a coordinate intere del primo quadrante non evidenziati saranno proprio i vettori degli esponenti che stavamo cercando.

Proposizione 1.3.8. *Sia I un ideale di $\mathbb{K}[x_1, \ldots, x_n]$ come sopra e $<$ un ordine monomiale. I laterali dei monomi appartenenti all'insieme normale di I rispetto a $<$ formano una base di $\mathbb{K}[x_1, \ldots, x_n]/I$ come $\mathbb{K}$-spazio vettoriale.*

Dimostrazione. Proviamo che tali elementi generano $\mathbb{K}[x_1, \ldots, x_n]/I$. Sappiamo che ogni polinomio $f \in \mathbb{K}[x_1, \ldots, x_n]$ ammette un'unica forma normale $N_G(f)$, che è ridotta rispetto a G. Dal momento che, per l'Algoritmo di Divisione, possiamo scrivere $f = f_I + N_G(f)$, con $f_I \in I$, abbiamo che

$$f \equiv N_G(f) \mathrm{mod} I.$$

Quindi $[f] = [N_G(f)]$ e $\mathbb{K}[x_1, \ldots, x_n]/I = \{[N_G(f)] : f \in \mathbb{K}[x_1, \ldots, x_n]\}$. D'altro canto, per definizione di *ridotto rispetto a G*, $N_G(f)$ è una combinazione lineare a coefficienti in $\mathbb{K}$ di monomi $x^\alpha \in \mathrm{T}_n$ tali che $\mathrm{lt}(g_i)$ non divide x^α, per ogni $i = 1, \ldots, n$. Cioè, per la Proposizione 1.1.58, x^α non appartiene a $\langle \mathrm{lt}(G) \rangle$. Poiché G è una base di Gröbner, per il Lemma 1.1.64 abbiamo che $\langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(G) \rangle$ e dunque $x^\alpha \in N$ per definizione. Proviamo ora che sono linearmente indipendenti. Sia, per assurdo,

$$\sum_{x^\alpha \in N} c_\alpha \, [x^\alpha] = [0] \in \mathbb{K}[x_1, \ldots, x_n]/I$$

con $c_\alpha \in \mathbb{K}$ non tutti nulli. Questo equivale a dire che $\sum_{x^\alpha \in N} c_\alpha x^\alpha \in I$, cioè, per il Teorema 1.1.48: $\sum_{x^\alpha \in N} c_\alpha x^\alpha \xrightarrow{G}_+ 0$. Ma $\sum_{x^\alpha \in N} c_\alpha x^\alpha$ è già ridotto modulo G per ipotesi. Assurdo per il Teorema 1.1.51. □

1.3.1 Finiteness Theorem

Abbiamo analizzato, nel paragrafo precedente, un metodo per capire quando una varietà sia vuota e quando invece non lo sia. Supponiamo di aver appurato che non lo è. Gli interrogativi che ora ci si può porre sono se sia una varietà di punti e, qualora lo fosse, da quanti punti sia composta. Questa sezione è dedicata ai risultati teorici che rispondono a questi quesiti: il *Finiteness Theorem* fornisce due condizioni necessarie e sufficienti affinché una varietà algebrica sia formata da soli punti, mentre la Proposizione che lo segue fornisce una stima del numero di tali punti.

Teorema 1.3.9. (Finiteness Theorem)
Sia $\mathbb{K}$ un campo algebricamente chiuso e sia $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideale. Allora le seguenti condizioni sono equivalenti:

1. *l'algebra $A = \mathbb{K}[x_1, \ldots, x_n]/I$ è di dimensione finita su $\mathbb{K}$;*
2. *la varietà $\mathbf{V}(I) \subset \mathbb{K}^n$ è un insieme finito;*
3. *se G è una base di Gröbner per I, allora per ogni i, $1 \leq i \leq n$, esiste un $m_i \geq 0$ tale che $x_i^{m_i} = lt(g)$ per qualche $g \in G$.*

Dimostrazione. ($1 \Rightarrow 2$) Per provare che $\mathbf{V}(I)$ è un insieme finito è sufficiente provare che, per ogni $i = 1, \ldots, n$, i punti di $\mathbf{V}(I)$ hanno solo un numero finito di coordinate i-esime distinte. Per ogni i, consideriamo allora il seguente insieme:

$$X = \left\{[1], [x_i], [x_i]^2, \ldots, [x_i]^k, \ldots\right\}$$

Dal momento che $\mathbb{K}[x_1, \ldots, x_n]/I$ ha dimensione finita, X deve essere formato da elementi linearmente dipendenti, cioè esistono coefficienti $c_k \in \mathbb{K}$ non tutti nulli e un intero $t \in \mathbb{N}$ tali che

$$[0] = \sum_{k=0}^{t} c_k [x_i]^k = \left[\sum_{k=0}^{t} c_k x_i^k\right] = [f],$$

e quindi $f \in I$. Poiché f è un polinomio non nullo di grado t in $\mathbb{K}[x_i]$, ammette al più un numero finito di radici distinte, dunque i punti di $\mathbf{V}(I)$ hanno solo un numero finito di coordinate i-esime distinte.
($2 \Rightarrow 3$) Se $\mathbf{V}(I) = \emptyset$, sappiamo dal Nullstellensatz (debole) che $I = \mathbb{K}[x_1, \ldots, x_n] = \langle 1 \rangle$ e, per la Proposizione 1.2.19, che $G = \{1\}$. Basta allora porre $m_i = 0$ per ogni $i = 1, \ldots, n$ e l'implicazione è provata.
Supponiamo allora che $\mathbf{V}(I) \neq \emptyset$. Sia $G = \{g_1, \ldots, g_s\}$ una base di Gröbner per I, fissiamo $i \in \{1, \ldots, n\}$ e siano $a_j \in \mathbb{K}$, $1 \leq j \leq t$, gli elementi distinti che compaiono come i-esima coordinata dei punti di $\mathbf{V}(I)$. Il polinomio

$$f = \prod_{j=1}^{t} (x_i - a_j)$$

si annulla in ogni punto di $\mathbf{V}(I)$ (per costruzione) e dunque, per il Nullstellensatz, esiste un $m \in \mathbb{N}$ tale che f^m sta in I. Da questo segue che $\mathrm{lt}(f^m) = x_i^{mt} \in \langle \mathrm{lt}(I) \rangle = \langle \mathrm{lt}(G) \rangle$, perché G è una base di Gröbner. Ma allora, per la Proposizione 1.1.58, esiste un $k \in \{1, \ldots, s\}$ tale che $\mathrm{lt}(g_k)$ divide x_i^{mt} e quindi $\mathrm{lt}(g_k) = x_i^{m_i}$ per un certo $1 \leq m_i \leq mt$.
($3 \Rightarrow 1$) Poiché per ogni i, $1 \leq i \leq n$, esiste un m_i tale che $x_i^{m_i} \in \langle \mathrm{lt}(G) \rangle = \langle \mathrm{lt}(I) \rangle$, tutti i monomi $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ con almeno un α_i maggiore di m_i stanno in $\langle \mathrm{lt}(I) \rangle$. Dunque, gli elementi che appartengono all'insieme normale di I devono essere della forma $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, con $\alpha_i \leq m_i - 1$ per ogni $i = 1, \ldots, n$, e sono al più $m_1 \cdot m_2 \cdot \cdots \cdot m_n$. Per la Proposizione 1.3.8 sappiamo che i laterali di tali monomi formano una base dello spazio vettoriale $\mathbb{K}[x_1, \ldots, x_n]/I$, che quindi ha dimensione finita. □

Definizione 1.3.10. (*ideale zero-dimensionale*)
Un ideale I che soddisfi alle condizioni equivalenti del Teorema 1.3.9 si dice *zero-dimensionale*.

Osservazione 1.3.11. L'unico punto in cui usiamo l'ipotesi $\mathbb{K}$ algebricamente chiuso è nel provare che $2 \Rightarrow 3$, le altre implicazioni valgono anche nel caso di $\mathbb{K}$ campo qualunque.

Proviamo ora una proprietà che ci permette di sapere quante possono essere (al più) le soluzioni di un sistema di equazioni polinomiali, quando sono in numero finito; prima però dobbiamo introdurre un lemma tecnico.

Lemma 1.3.12. *Sia $S = \{p_1, \ldots, p_m\}$ un sottoinsieme finito di $\mathbb{K}^n$. Esistono dei polinomi $g_i \in \mathbb{K}[x_1, \ldots, x_n]$, $i = 1, \ldots, m$, tali che*

$$g_i(p_j) = \begin{cases} 0 & \text{se } i \neq j \\ 1 & \text{se } i = j \end{cases}$$

Dimostrazione. (*Costruttiva*) Supponiamo, senza perdere in generalità, che i p_i siano tutti distinti. Fissiamo p_1 e proviamo che esiste un $g_1 \in \mathbb{K}[x_1, \ldots, x_n]$ tale che:

$$g_1(p_j) = \begin{cases} 0 & \text{se } j = 2, \ldots, m \\ 1 & \text{se } j = 1 \end{cases}$$

Innanzitutto osserviamo che se $a \neq b$ in $\mathbb{K}^n$, esiste un $k \in \{1, \ldots, n\}$ tale che $a_k \neq b_k$. Di conseguenza il polinomio

$$q = \frac{x_k - b_k}{a_k - b_k}$$

soddisfa $q(a) = 1$ e $q(b) = 0$.
Possiamo allora costruire, per ogni $i = 2, \ldots, m$, q_i come sopra, in modo che $q_i(p_1) = 1$ e $q_i(p_i) = 0$. Questo implica che il polinomio

$$g_1 = \prod_{i=2}^{m} q_i$$

soddisfa la proprietà richiesta.
Osserviamo ora che, in quanto detto sopra, p_1 può essere sostituito da un qualsiasi p_i, per $i = 1, \ldots, m$. Ciò ci permette di costruire i g_i e terminare la dimostrazione. □

Proposizione 1.3.13. *Sia I un ideale zero-dimensionale di $\mathbb{K}[x_1, \ldots, x_n]$, con $\mathbb{K}$ algebricamente chiuso. Allora:*

1. *il numero di punti in $\mathbf{V}(I)$ è al più pari a $\dim(\mathbb{K}[x_1, \ldots, x_n]/I)$, dove $\dim$ è la dimensione di $\mathbb{K}[x_1, \ldots, x_n]/I$ come spazio vettoriale su $\mathbb{K}$;*
2. *se inoltre I è radicale, tale numero uguaglia $\dim(\mathbb{K}[x_1, \ldots, x_n]/I)$.*

Dimostrazione. 1) Supponiamo che $\mathbf{V}(I) = \{p_1, \ldots, p_m\}$, con i p_i tutti distinti; possiamo allora costruire m polinomi $f_1, \ldots, f_m$ come nel Lemma 1.3.12. Proviamo che i vettori dell'insieme $\{[f_1], \ldots, [f_m]\}$ sono linearmente indipendenti in $A = \mathbb{K}[x_1, \ldots, x_n]/I$. Supponiamo che

$$\sum_{i=1}^{m} a_i [f_i] = [0]$$

in A. Questo significa che $g = \sum_{i=1}^{m} a_i f_i \in \mathbb{K}[x_1, \ldots, x_n]$ appartiene a I e dunque si annulla in ogni punto di $\mathbf{V}(I)$. Ma allora

$$0 = g(p_k) = \sum_{i=1}^{m} a_i f_i(p_k) = a_k f_k(p_k) = a_k$$

per ogni $k = 1, \ldots, m$, che ci garantisce l'indipendenza lineare. Questo prova che la dimensione di A è sicuramente maggiore o uguale a m.

2) Supponiamo ora che I sia anche radicale e proviamo che $\{[f_1], \ldots, [f_m]\}$ è un insieme di generatori di A. Sia allora $[g] \in \mathbb{K}[x_1, \ldots, x_n]/I$ e siano $a_i = g(p_i)$, per ogni $i = 1, \ldots, m$, i valori assunti da g sui punti di $\mathbf{V}(I)$. Consideriamo il polinomio

$$h = g - \sum_{k=1}^{m} a_k f_k;$$

risulta:

$$\begin{aligned} h(p_i) &= g(p_i) - \sum_{k=1}^{m} a_k f_k(p_i) \\ &= g(p_i) - a_i f_i(p_i) \\ &= g(p_i) - a_i = 0 \end{aligned}$$

per ogni $i = 1, \ldots, m$. Dunque, h appartiene a $\mathbf{I}(\mathbf{V}(I))$ e, per il Nullstellensatz, h appartiene a $\sqrt{I} = I$. Ma allora $[h] = [0]$ in A e $[g] = \sum_{k=1}^{m} a_k[f_k]$, come volevasi dimostrare. □

1.4 Elementi di Algebra Lineare

Riportiamo qui solo alcuni risultati di algebra lineare a cui faremo riferimento nella trattazione. Sia R un anello commutativo con unità, ricordiamo che il *polinomio caratteristico* di una matrice $M \in \mathcal{M}_{n\times n}(R)$ è, per definizione:

$$p_M(\lambda) = \det(M - \lambda I_n) \in R[\lambda]$$

e le sue radici (in R) sono gli *autovalori* della matrice (I_n è la matrice identità di ordine n).

Definizione 1.4.1. (*cofattore, matrice aggiunta*)
Sia R un anello commutativo con unità. Se $M = (m_{ij}) \in \mathcal{M}_{n\times n}(R)$ è una matrice quadrata di ordine n, allora si definisce *minore complementare dell'elemento* m_{ij} il determinante della sottomatrice ottenuta rimuovendo la i-esima riga e la j-esima colonna da M, e si indica con M_{ij}. Il numero $C_{ij} = (-1)^{i+j} M_{ij}$ è detto *cofattore* dell'elemento m_{ij}.
La matrice $C = (C_{ij})$ $(1 \leq i, j \leq n)$ è detta *matrice dei cofattori*. La sua trasposta $(C_{ij})^T$ è detta *matrice aggiunta* di M e si indica con $\mathrm{Adj}(M)$.

Osservazione 1.4.2. Come conseguenza dei teoremi di Laplace sullo sviluppo del determinante di una matrice abbiamo che:

$$\begin{aligned} \det(M) &= \sum_{i=1}^{n} m_{ij} C_{ij} \quad \text{sviluppo secondo la } j\text{-esima colonna}, \\ \det(M) &= \sum_{j=1}^{n} m_{ij} C_{ij} \quad \text{sviluppo secondo la } i\text{-esima riga}, \\ 0 &= \sum_{i=1}^{n} m_{ij} C_{ik} \quad j \neq k, \\ 0 &= \sum_{j=1}^{n} m_{ij} C_{kj} \quad i \neq k. \end{aligned}$$

Proposizione 1.4.3. *Siano R un anello commutativo con unità, M una matrice quadrata di ordine n e sia $Adj(M)$ la sua matrice aggiunta, allora:*

$$M \cdot Adj(M) = \det(M) I_n = Adj(M) \cdot M.$$

Dimostrazione. Consideriamo il prodotto

$$M \cdot \mathrm{Adj}(M) = \begin{pmatrix} m_{11} & m_{12} & \dots & m_{1n} \\ m_{21} & m_{22} & \dots & m_{2n} \\ \vdots & \vdots & \dots & \vdots \\ m_{n1} & m_{n2} & \dots & m_{nn} \end{pmatrix} \cdot \begin{pmatrix} C_{11} & C_{21} & \dots & C_{n1} \\ C_{12} & C_{22} & \dots & C_{n2} \\ \vdots & \vdots & \dots & \vdots \\ C_{1n} & C_{2n} & \dots & C_{nn} \end{pmatrix}.$$

L'elemento nella riga i-esima e colonna j-esima della matrice prodotto $B = M \cdot \mathrm{Adj}(M)$ è dato da:

$$b_{ij} = m_{i1}C_{j1} + m_{i2}C_{j2} + \cdots + m_{in}C_{jn}.$$

Per l'Osservazione 1.4.2 tale elemento è 0 se $i \neq j$, è $\det(M)$ se $i = j$. Quindi:

$$M \cdot \mathrm{Adj}(M) = \det(M) I_n$$

e questo prova la prima uguaglianza. Per provare la seconda uguaglianza è sufficiente osservare che al posto degli sviluppi per riga si considerano quelli per colonna. □

Teorema 1.4.4. (Teorema di Cayley-Hamilton)
Sia $M \in \mathcal{M}_{n\times n}(R)$ una matrice $n \times n$ con polinomio caratteristico

$$p_M(\lambda) = \lambda^n + c_{n-1}\lambda^{n-1} + \cdots + c_1\lambda + c_0.$$

Allora $p_M(M) = 0$, cioè

$$M^n + c_{n-1}M^{n-1} + \cdots + c_1 M + c_0 I_n = 0.$$

Dimostrazione. Consideriamo la matrice $M - \lambda I_n$, questa è a entrate nell'anello $R[\lambda]$ e dunque possiamo considerare la matrice $A = \mathrm{Adj}(M - \lambda I)$ (per comodità scriveremo solo più I al posto di I_n). Per la Proposizione 1.4.3 abbiamo che:

$$(M - \lambda I) \cdot A = \det(M - \lambda I) I = p_M(\lambda) I.$$

Osserviamo che sia A che $p_M(\lambda)I$ sono matrici che hanno come entrate polinomi in λ. Possiamo allora riscriverle nel seguente modo:

$$A = \sum_{i=0}^{n-1} \lambda^i A_i,$$

$$p_M(\lambda) I = \lambda^n I + \sum_{i=0}^{n-1} \lambda^i c_i I,$$

dove le matrici A_i sono 'costanti' (nel senso che le loro entrate sono elementi di R). Sfruttiamo ora la proprietà distributiva:

$$\begin{aligned}\lambda^n I + \sum_{i=0}^{n-1} \lambda^i c_i I &= (M - \lambda I) \cdot A = (M - \lambda I) \cdot \sum_{i=0}^{n-1} \lambda^i A_i \\ &= \sum_{i=0}^{n-1} M \cdot \lambda^i A_i - \sum_{i=0}^{n-1} \lambda I \cdot \lambda^i A_i = \sum_{i=0}^{n-1} \lambda^i M \cdot A_i - \sum_{i=0}^{n-1} \lambda^{i+1} A_i \\ &= -\lambda^n A_{n-1} + \sum_{i=1}^{n-1} \lambda^i (M \cdot A_i - A_{i-1}) + M \cdot A_0.\end{aligned}$$

Tale uguaglianza vale se e solo se:

$$\begin{cases} c_0 I &= M \cdot A_0 \\ c_1 I &= M \cdot A_1 - A_0 \\ &\vdots \\ c_{n-1} I &= M \cdot A_{n-1} - A_{n-2} \\ I &= -A_{n-1} \end{cases}$$

Adesso moltiplichiamo a sinistra la riga i-esima per la matrice M^i, per ogni $i = 0, \ldots, n$, e poi sommiamo sulle righe:

$$\begin{aligned}M^n + c_{n-1} M^{n-1} + \cdots + c_1 M + c_0 I = \\ = -M^n \cdot A_{n-1} + M^{n-1} \cdot (M \cdot A_{n-1} - A_{n-2}) + \cdots \\ \cdots + M \cdot (M \cdot A_1 - A_0) + M \cdot A_0 = 0\end{aligned}$$

e, poiché il membro di sinistra dell'equazione è proprio $p_M(M)$, abbiamo che il teorema è dimostrato. □

Definizione 1.4.5. (*polinomio minimo*)
Il *polinomio minimo* $m_M(t)$ di una matrice $M \in \mathcal{M}_{n\times n}(R)$ è il polinomio $f \in R[t]$ monico di grado minimo tale che $f(M) = 0$.

1.4.1 Autovettori generalizzati

Un concetto che servirà nel secondo capitolo è quello di *matrice non-derogatoria*. Dal momento che esistono due definizioni equivalenti di questo particolare tipo di matrice, e le useremo entrambe, dimostriamo in questa sezione l'equivalenza tra le due.
(Quasi tutti i risultati sono riportati senza dimostrazione; per le dimostrazioni mancanti e eventuali approfondimenti si faccia riferimento a [Cand].)

Definizione 1.4.6. (*matrice non-derogatoria*)
Una matrice $M \in \mathcal{M}_{n\times n}(R)$ quadrata di ordine n a entrate in un anello commutativo con unità R è *non-derogatoria* se

D1: il suo polinomio minimo è uguale al suo polinomio caratteristico, cioè se $m_M(x) = p_M(x)$.

D2: tutti i suoi autospazi hanno dimensione 1.

Nota 1.4.7. La definizione data è quella generale. Tuttavia il contesto in cui la useremo prevede che $R = \mathbb{K}$, campo algebricamente chiuso. Quindi, in ciò che rimane della sezione, faremo conto di lavorare con un endomorfismo $\phi\colon V \to V$, dove V è uno spazio vettoriale di dimensione n, finita, su un campo $\mathbb{K}$ algebricamente chiuso. Fissata una base B di V, l'endomorfismo sarà rappresentato dalla matrice M rispetto a tale base. Viceversa, ogni matrice M quadrata di ordine n a entrate in $\mathbb{K}$ sarà associata ad un endomorfismo $\phi\colon V \to V$ rispetto a una certa base di V.

Definizione 1.4.8. (*autovettore generalizzato*)
Un vettore v di V è un *autovettore generalizzato* della matrice M se $(M - \lambda I)^m \cdot v = 0$ per qualche autovalore $\lambda \in \mathbb{K}$ di M e per qualche intero positivo m. Si chiama *periodo* dell'autovettore generalizzato v il minimo intero s tale che $v \in \ker[(M - \lambda I)^s]$, ovvero l'intero s per cui $(M - \lambda I)^s \cdot v = 0$ ma $(M - \lambda I)^{s-1} \cdot v \neq 0$.

Nota 1.4.9. Con un piccolo abuso di notazione indicherò con $\ker(M)$ il nullspace della matrice M, pensandolo come nucleo dell'endomorfismo rappresentato da M. L'operazione $\cdot$ indicherà il prodotto righe per colonne di una matrice per un vettore colonna.

Osservazione 1.4.10. Sia v un autovettore generalizzato di M relativo all'autovalore λ e sia k il suo periodo. Allora i vettori

$$\left\{v, (M - \lambda I) \cdot v, \ldots, (M - \lambda I)^{k-1} \cdot v\right\}$$

sono linearmente indipendenti.

Proposizione 1.4.11. *Sia $p_M(x) = (x-\lambda_1)^{m_1} \cdots (x-\lambda_r)^{m_r}$ il polinomio caratteristico di M, con $\lambda_1, \ldots, \lambda_r$ a due a due distinti. Per $k = 1, \ldots, r$ indichiamo con c_k il massimo periodo di un autovettore generalizzato relativo all'autovalore λ_k. Allora il polinomio minimo di M è dato da:*

$$m_M(x) = (x - \lambda_1)^{c_1} \cdots (x - \lambda_r)^{c_r}.$$

Teorema 1.4.12. *Sia M una matrice quadrata di ordine n, a entrate in un campo $\mathbb{K}$ algebricamente chiuso, con polinomio caratteristico $p_M(x) = (x - \lambda_1)^{m_1} \cdots (x - \lambda_r)^{m_r}$ dove i λ_i sono a due a due distinti. Allora*

$$V = \ker[(M - \lambda_1 I)^{m_1}] \oplus \ker[(M - \lambda_2 I)^{m_2}] \oplus \cdots \oplus \ker[(M - \lambda_r I)^{m_r}]$$

e inoltre $\dim_{\mathbb{K}}(\ker[(M - \lambda_i I)^{m_i}]) = m_i$.

Lemma 1.4.13. *Sia M una matrice quadrata di ordine n, a entrate in un campo $\mathbb{K}$ algebricamente chiuso, tale che*

$$p_M(x) = m_M(x) = (x - \lambda_1)^{m_1} \cdots (x - \lambda_r)^{m_r},$$

dove gli autovalori $\lambda_1, \ldots, \lambda_r$ sono a due a due distinti. Allora, per ogni $k = 1, \ldots, r$, esiste un autovettore generalizzato $w_k \in \ker[(M - \lambda I)^{m_k}]$ di periodo esattamente m_k.

Corollario 1.4.14. *Sia M una matrice quadrata di ordine n, a entrate in un campo $\mathbb{K}$ algebricamente chiuso, tale che il suo polinomio minimo e quello caratteristico coincidano. Allora esiste un vettore $v \in V$ tale che $\{v, M \cdot v, \dots, M^{n-1} \cdot v\}$ è un insieme di vettori linearmente indipendenti.*
In particolare ciò significa che se

$$p_M(x) = m_M(x) = x^n - a_1 x^{n-1} - \cdots - a_n,$$

allora la matrice M è simile alla matrice

$$C = \begin{pmatrix} 0 & 0 & \dots & 0 & a_n \\ 1 & 0 & \dots & 0 & a_{n-1} \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & a_1 \end{pmatrix}.$$

Possiamo dimostrare ora l'equivalenza delle due definizioni date all'inizio del paragrafo:

Proposizione 1.4.15. *Una matrice M, quadrata di ordine n, a entrate in un campo algebricamente chiuso $\mathbb{K}$, ha polinomio minimo e caratteristico coincidenti se e solo se tutti i suoi autospazi hanno dimensione 1.*

Dimostrazione. ($\Rightarrow$) : Sia data una matrice M tale che il suo polinomio minimo e quello caratteristico coincidono. Per il Corollario 1.4.14 questo significa che esiste $P \in GL_n(\mathbb{K})$ tale che $M = P^{-1} \cdot C \cdot P$ e

$$C = \begin{pmatrix} 0 & 0 & \dots & 0 & a_n \\ 1 & 0 & \dots & 0 & a_{n-1} \\ 0 & \ddots & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & a_1 \end{pmatrix}.$$

Questo implica che $(M - \lambda I) = P^{-1} \cdot (C - \lambda I) \cdot P$ e allora, poiché la relazione di similitudine tra matrici conserva il rango, abbiamo che la dimensione degli autospazi di M è uguale alla dimensione degli autospazi di C. Ma si osserva facilmente che C ha tutti autospazi di dimensione 1, come volevasi dimostrare.
($\Leftarrow$) : Viceversa, supponiamo che tutti gli autospazi di M abbiano dimensione 1. Come conseguenza della Proposizione 1.4.11, abbiamo che $p_M(x) = m_M(x)$ se e solo se, per ogni autovalore di M, esiste un autovettore generalizzato di periodo pari alla molteplicità algebrica dell'autovalore stesso. Proviamo allora il seguente fatto: Sia M come da ipotesi e siano $\lambda_1, \dots, \lambda_r$ gli autovalori della matrice M, a due a due distinti. Per ogni $k = 1, \dots, r$ esiste un autovettore generalizzato $z \in V$, relativo all'autovalore λ_k, il cui periodo vale m_k.
Per comodità poniamo $\lambda_k = \lambda$ e $m_k = m$ e supponiamo, per assurdo, che non esista un autovettore generalizzato relativo all'autovalore λ di periodo m. Allora, ogni autovettore generalizzato w relativo a λ avrebbe periodo $c < m$. Sia z quello di periodo massimo:

t. Per l'Osservazione 1.4.10 l'insieme $Z = \{z, (M-\lambda I)\cdot z, \ldots, (M-\lambda I)^{t-1}\cdot z\}$ è libero in $\ker[(M-\lambda I)^m]$. Provo che ne è anche una base.
Per assurdo non lo sia. Siano y_i $(i = t, \ldots, m-1)$ $m-t$ vettori linearmente indipendenti che completano Z a una base di $\ker[(M-\lambda I)^m]$ e sia $0 \neq a \in \ker[(M-\lambda I)^m]$. Per ipotesi possiamo scrivere

$$a = \sum_{i=0}^{t-1} a_i (M-\lambda I)^i \cdot z + \sum_{j=t}^{m-1} a_j y_j$$

con gli a_i e a_j non tutti nulli (in particolare supponiamo $a_0 \neq 0$). Applico allora $(M-\lambda I)^{t-1}$ a entrambi i membri e ottengo

$$(M-\lambda I)^{t-1}\cdot a = a_0 (M-\lambda I)^{t-1}\cdot z + \sum_{j=t}^{m-1} a_j (M-\lambda I)^{t-1}\cdot y_j. \tag{1.6}$$

Ora, ricordando che t è il periodo massimo degli elementi di $\ker[(M-\lambda I)^m]$, si presentano le seguenti possibilità:
1. $(M-\lambda I)^{t-1}\cdot a = 0$ e $(M-\lambda I)^{t-1}\cdot y_j = 0$ per ogni $j = t, \ldots, m-1$. Ma questo è impossibile, perché significherebbe che $a_0(M-\lambda I)^{t-1}\cdot z = 0$.
2. $(M-\lambda I)^{t-1}\cdot a = 0$, ma esiste almeno un $(M-\lambda I)^{t-1}\cdot y_j$ diverso da 0. Allora (1.6) implica che

$$(M-\lambda I)^{t-1}\cdot z = -\sum_{j=t}^{m-1} \frac{a_j}{a_0}(M-\lambda I)^{t-1}\cdot y_j,$$

cioè che $(M-\lambda I)^{t-1}\cdot z$ è linearmente dipendente dagli y_j. Assurdo.
3. $(M-\lambda I)^{t-1}\cdot a \neq 0$ ed esiste almeno un $(M-\lambda I)^{t-1}\cdot y_j$ diverso da 0. A questo punto sfruttiamo l'ipotesi che ogni autospazio di M abbia dimensione 1: poiché t è, per ipotesi assurda, il massimo periodo degli elementi di $\ker[(M-\lambda I)^m]$, abbiamo che $(M-\lambda I)^{t-1}\cdot a$ è un autovettore tradizionale di M rispetto all'autovalore λ. Ma anche $(M-\lambda I)^{t-1}\cdot z$ gode della stessa proprietà (per lo stesso motivo) e dunque $(M-\lambda I)^{t-1}\cdot a = c(M-\lambda I)^{t-1}\cdot z$ per un certo scalare $c \in \mathbb{K}$. Osservato ciò, succede che: se $c - a_0 = 0$, abbiamo che gli y_j sono linearmente dipendenti; se $c - a_0 \neq 0$, siamo di nuovo nel caso 2.
In tutti i casi siamo giunti ad un assurdo, nato dall'aver supposto che Z non fosse una base. Ma allora, dal momento che Z è una base, $\dim(\ker[(M-\lambda I)^m]) = t < m$. Assurdo per il Teorema 1.4.12. E questo conclude la dimostrazione. □

Capitolo 2

Sulla risoluzione di equazioni via autovalori e autovettori

Sappiamo, a questo punto, che una varietà algebrica è l'insieme delle soluzioni di un sistema di equazioni polinomiali del tipo:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ f_2(x_1, \ldots, x_n) = 0 \\ \qquad \vdots \\ f_s(x_1, \ldots, x_n) = 0 \end{cases} \tag{2.1}$$

Sappiamo inoltre che, se l'ideale è zero-dimensionale, la varietà è formata da un numero finito di punti e sappiamo dire se è vuota, se non lo è, e in questo secondo caso sappiamo stimare quanti punti può contenere. Per procedere nello studio di tali varietà, dobbiamo allora sviluppare un metodo per trovarne i punti, dato un sistema del tipo (2.1). Lo scopo di questo capitolo e l'argomento principale di questo scritto è proprio descrivere un metodo che sfrutta l'algebra lineare per risolvere il sistema (2.1): il cosiddetto *metodo degli autovalori e degli autovettori*.

2.1 Mappe di moltiplicazione

Introduciamo qui le applicazioni lineari che stanno alla base del metodo degli autovalori e degli autovettori, insieme alle loro proprietà.

Nota 2.1.1. Sia dato un sistema di equazioni polinomiali come (2.1), dove f_i appartiene a $\mathbb{K}[x_1, \ldots, x_n]$ per ogni $i = 1, \ldots, s$. D'ora in avanti useremo la seguente notazione:

- $I = \langle f_1, \ldots, f_s \rangle$ è l'ideale di $\mathbb{K}[x_1, \ldots, x_n]$ generato da $f_1, \ldots, f_s$.
- $[f] = f + I = \{f + g \in \mathbb{K}[x_1, \ldots, x_n] : g \in I\}$ è il laterale di $f \in \mathbb{K}[x_1, \ldots, x_n]$ in A modulo I.

Definizione 2.1.2. (*mappa di moltiplicazione*)
Sia f un polinomio qualsiasi in $\mathbb{K}[x_1, \ldots, x_n]$, fissato. Risulta definito il laterale $[f]$ di

f in $A = \mathbb{K}[x_1, \ldots, x_n]/I$. Consideriamo la seguente applicazione, definita da A in se stesso:

$$\begin{array}{rccc} m_f\colon & A & \to & A \\ & [g] & \mapsto & [f]\cdot[g] = [fg] \end{array} \tag{2.2}$$

Essa prende il nome di *mappa di moltiplicazione* per f.

Tale applicazione gode delle seguenti proprietà di base:

Proposizione 2.1.3. *Sia $f \in \mathbb{K}[x_1, \ldots, x_n]$. Allora*

1. *l'applicazione m_f sopra definita è un'applicazione lineare da A in A;*
2. *risulta $m_f = m_g$ se e solo se $f - g \in I$. Cioè due polinomi definiscono la stessa applicazione lineare se e solo se differiscono per un elemento di I. In particolare, m_f è l'applicazione nulla se e solo se $f \in I$.*

Dimostrazione. 1. Per verificare che si tratta di un'applicazione lineare dobbiamo provare che

$$m_f(\lambda[g] + \mu[h]) = \lambda \cdot m_f([g]) + \mu \cdot m_f([h])$$

per ogni $[g], [h] \in A$ e per ogni $\lambda, \mu \in \mathbb{K}$. Ricorriamo alla definizione:

$$m_f(\lambda[g] + \mu[h]) = [f] \cdot (\lambda[g] + \mu[h])$$

Poiché il prodotto in A gode della proprietà distributiva rispetto alla somma ed è $\mathbb{K}$-lineare:

$$[f] \cdot (\lambda[g] + \mu[h]) = \lambda[f] \cdot [g] + \mu[f] \cdot [h] = \lambda m_f([g]) + \mu m_f([h])$$

per definizione e abbiamo concluso.
2. Supponiamo sia $m_f = m_g$. Dal momento che $[1] \in A$ è l'identità rispetto al prodotto in A abbiamo che:

$$[f] = [f] \cdot [1] = m_f([1]) = m_g([1]) = [g] \cdot [1] = [g]$$

e per come abbiamo definito il quoziente A questo significa che $f - g \in I$. Viceversa, se $f - g \in I$, allora $[f] = [g]$ e dunque $m_f = m_g$ per come sono state definite m_f e m_g. □

Dal momento che A è uno spazio vettoriale di dimensione finita su $\mathbb{K}$, possiamo rappresentare m_f tramite la sua matrice rispetto a una base fissata.
Introduciamo quindi un ordine monomiale in $\mathbb{K}[x_1, \ldots, x_n]$ e usiamolo per calcolare una base di Gröbner G di I. Da questa ricaviamo i monomi appartenenti all'insieme normale N, i cui laterali formano una base B dello spazio vettoriale $A = \mathbb{K}[x_1, \ldots, x_n]/I$ (vedi paragrafo 1.1.2). Questa scelta si rivela particolarmente comoda perché, una volta nota la tavola di moltiplicazione per gli elementi di B, la matrice dell'applicazione m_f può essere letta direttamente dalla tavola. Denoteremo tale matrice col simbolo M_f.

Esempio 2.1.4. Consideriamo:

$$G = \left\{ x^2 + \frac{3}{2}xy + \frac{1}{2}y^2 - \frac{3}{2}x - \frac{3}{2}y, xy^2 - x, y^3 - y \right\}.$$

Usando l'ordine *grevlex* si vede che G è una base di Gröbner per l'ideale $I = \langle G \rangle \subset \mathbb{C}[x, y]$. Esaminando i monomi iniziali di G, si vede che $\langle LT(I) \rangle = \langle x^2, xy^2, y^3 \rangle$. Gli unici monomi che non appartengono a questo ideale sono quelli dell'insieme:

$$N = \left\{ 1, x, y, xy, y^2 \right\}.$$

Quindi i laterali di questi cinque monomi formano una base dello spazio vettoriale $A = \mathbb{C}[x, y]/I$ su $\mathbb{C}$:

$$B = \left\{ [1], [x], [y], [xy], [y^2] \right\}.$$

Ricaviamo ora la tavola di moltiplicazione per gli elementi della base B.
Ovviamente $[1] \cdot [x^\alpha] = [x^\alpha]$, $[x] \cdot [y] = [xy]$ e $[y] \cdot [y] = [y^2]$. Ricordiamo inoltre che:

$$\begin{aligned} [x^2] &= \left[\frac{3}{2}x + \frac{3}{2}y - \frac{3}{2}xy - \frac{1}{2}y^2 \right], \\ [xy^2] &= [x], \\ [y^3] &= [y], \end{aligned}$$

le quali si possono facilmente ricavare dagli elementi di G. Calcoliamo allora i restanti prodotti non immediati:

$$\begin{aligned} [x] \cdot [xy] &= [x^2 y] \\ &= [x^2] \cdot [y] \\ &= \left[\frac{3}{2}x + \frac{3}{2}y - \frac{3}{2}xy - \frac{1}{2}y^2 \right] \cdot [y] \\ &= \frac{3}{2}[x] \cdot [y] + \frac{3}{2}[y] \cdot [y] - \frac{3}{2}[xy] \cdot [y] - \frac{1}{2}[y^2] \cdot [y] \\ &= \left[-\frac{3}{2}x - \frac{1}{2}y + \frac{3}{2}xy + \frac{3}{2}y^2 \right] \end{aligned}$$

e inoltre:

$$\begin{aligned} [xy] \cdot [y^2] &= [xy^3] = [x] \cdot [y^3] \\ &= [xy], \\ [y^2] \cdot [y^2] &= [y^4] = [y] \cdot [y^3] \\ &= [y^2], \\ [xy] \cdot [xy] &= [x^2 y^2] = [x] \cdot [xy^2] = [x] \cdot [x] \\ &= \left[\frac{3}{2}x + \frac{3}{2}y - \frac{3}{2}xy - \frac{1}{2}y^2 \right] \end{aligned}$$

Quindi, ponendo:

$$\alpha = \frac{3}{2}x + \frac{3}{2}y - \frac{3}{2}xy - \frac{1}{2}y^2$$

e

$$\beta = -\frac{3}{2}x - \frac{1}{2}y + \frac{3}{2}xy + \frac{3}{2}y^2,$$

otteniamo che la tavola di moltiplicazione risulta essere:

$\cdot$	$[1]$	$[x]$	$[y]$	$[xy]$	$[y^2]$
$[1]$	$[1]$	$[x]$	$[y]$	$[xy]$	$[y^2]$
$[x]$	$[x]$	$[\alpha]$	$[xy]$	$[\beta]$	$[x]$
$[y]$	$[y]$	$[xy]$	$[y^2]$	$[x]$	$[y]$
$[xy]$	$[xy]$	$[\beta]$	$[x]$	$[\alpha]$	$[xy]$
$[y^2]$	$[y^2]$	$[x]$	$[y]$	$[xy]$	$[y^2]$

Nota questa, possiamo facilmente ricavare la matrice M_f con $f \in N$: costruiamo una matrice quadrata di ordine 5 la cui j-esima colonna è formata dalle componenti, rispetto alla base B, dell'immagine del j-esimo elemento della base stessa mediante m_f.
Consideriamo ad esempio $f = x$ e otteniamo:

$$\begin{aligned} m_x([1]) &= [x] \\ m_x([x]) &= [x^2] = [\alpha] \\ m_x([y]) &= [xy] \\ m_x([xy]) &= [x^2y] = [\beta] \\ m_x([y^2]) &= [xy^2] = [x] \end{aligned}$$

da cui:

$$M_x = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 3/2 & 0 & -3/2 & 1 \\ 0 & 3/2 & 0 & -1/2 & 0 \\ 0 & -3/2 & 1 & 3/2 & 0 \\ 0 & -1/2 & 0 & 3/2 & 0 \end{pmatrix}$$

Come osservato sopra, le colonne di M_x sono formate dai coefficienti dei vettori presenti nella seconda riga della tavola di moltiplicazione, espressi in termini di B.
Analogamente otteniamo:

$$M_1 = I_5$$

dove I_5 è la matrice identità 5×5 e:

$$M_y = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$$

$$M_{xy} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & -3/2 & 1 & 3/2 & 0 \\ 0 & -1/2 & 0 & 3/2 & 0 \\ 1 & 3/2 & 0 & -3/2 & 1 \\ 0 & 3/2 & 0 & -1/2 & 0 \end{pmatrix}$$

$$M_{y^2} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Nota 2.1.5. Si osservi che $M_{xy} = M_x\, M_y$ e $M_{y^2} = M_y\, M_y$. Vedremo come questa sia una proprietà delle matrici M_f.

Osservazione 2.1.6. In generale, una volta costruita una base di Gröbner G per I rispetto a un certo ordine monomiale $<$, risulta facile ricavare la matrice M_f. Si costruisce l'insieme normale N di I rispetto a $<$:

$$N = \{t \in \mathrm{T}_n : \nexists\, g \in G \text{ per il quale accada che } \mathrm{lt}(g) \text{ divide } t\}$$

e poi, per ogni $x^\alpha \in N$, si calcola $N_G(x^\alpha \cdot f)$ usando l'Algoritmo di Divisione, che è fondamentalmente ciò che è stato fatto nell'Esempio 2.1.4.

Passiamo ora ad indagare le proprietà delle matrici M_f:

Proposizione 2.1.7. *Siano $[f]$, $[g]$ due elementi dell'algebra A. Allora:*

1. $M_{f+g} = M_f + M_g$;
2. $M_{fg} = M_f\, M_g = M_g\, M_f$.

Equivalentemente, in termini di mappe di moltiplicazione:

1. $m_{f+g} = m_f + m_g$;
2. $m_{fg} = m_f \circ m_g = m_g \circ m_f$.

Dimostrazione. La dimostrazione è immediata se la pensiamo in termini di applicazioni lineari:
1. Per ogni $[h] \in A$:

$$\begin{aligned} m_{f+g}([h]) &= [f+g]\cdot[h] = ([f]+[g])\cdot[h] \\ &= ([f]\cdot[h]) + ([g]\cdot[h]) \\ &= m_f([h]) + m_g([h]) \end{aligned}$$

2. Per ogni $[h] \in A$:

$$\begin{aligned} m_{fg}([h]) &= [fg]\cdot[h] = ([f]\cdot[g])\cdot[h] \\ &= [f]\cdot([g]\cdot[h]) = [f]\cdot m_g([h]) \\ &= m_f(m_g([h])) \\ &= (m_f \circ m_g)([h]) \end{aligned}$$

Inoltre risulta, per ogni $[h] \in A$:

$$(m_f \circ m_g)([h]) = ([f] \cdot [g]) \cdot [h] = ([g] \cdot [f]) \cdot [h] = (m_g \circ m_f)([h])$$

e abbiamo usato solo la definizione di m_f e le proprietà dei laterali. □

Nota 2.1.8. Sia $h(t) = \sum_{i=0}^{m} c_i t^i \in \mathbb{K}[t]$ un polinomio in una indeterminata, $f \in \mathbb{K}[x_1, \ldots, x_n]$ un polinomio in n indeterminate e M una matrice nell'anello $\mathcal{M}_{d\times d}(\mathbb{K})$ delle matrici quadrate di ordine d a coefficienti in $\mathbb{K}$. L'espressione $h(f) = \sum_{i=0}^{m} c_i f^i$ è ancora un elemento di $\mathbb{K}[x_1, \ldots, x_n]$. Similmente $h(M) = \sum_{i=0}^{m} c_i M^i$ è una matrice ben definita in $\mathcal{M}_{d\times d}(\mathbb{K})$ (a patto di interpretare il termine c_0 come $c_0\, I_d$).

Corollario 2.1.9. *Siano $h \in \mathbb{K}[t]$ e $f \in \mathbb{K}[x_1, \ldots, x_n]$. Allora*

$$M_{h(f)} = h(M_f)$$

Dimostrazione. Sia $h(t) = \sum_{i=0}^{m} c_i t^i$, allora:

$$\begin{aligned} h(M_f) &= \sum_{i=0}^{m} c_i \left(M_f\right)^i = \sum_{i=0}^{m} c_i M_{f^i} \\ &= \sum_{i=0}^{m} M_{c_i f^i} = M_{\sum_{i=0}^{m} c_i f^i} \\ &= M_{h(f)} \end{aligned}$$

e questo conclude la dimostrazione. □

2.2 Eigenvalue Theorem

Il Teorema degli Autovalori o *Eigenvalue Theorem* è il nodo centrale di questo capitolo: il legame tra gli autovalori della matrice M_f e le soluzioni del sistema (2.1).

Osservazione 2.2.1. Sia $f \in \mathbb{K}[x_1, \ldots, x_n]$ e sia $[f] \in A$ il laterale di f in A. Poiché abbiamo supposto A di dimensione finita, l'insieme $\{1, [f], [f]^2, \ldots\}$ deve essere necessariamente formato da vettori linearmente dipendenti in A. Cioè, esiste una combinazione lineare che dà come risultato l'elemento nullo:

$$\sum_{i=0}^{m} c_i [f]^i = [0]$$

in A, per un certo $m \in \mathbb{N}$ e per certi $c_i \in \mathbb{K}$ non tutti nulli. Per definizione di anello quoziente, questo è equivalente a dire che

$$\sum_{i=0}^{m} c_i f^i \in I \tag{2.3}$$

Quindi, per ogni $f \in \mathbb{K}[x_1, \ldots, x_n]$, esiste un polinomio $h(t) = \sum_{i=0}^{m} c_i t^i \in \mathbb{K}[t]$ tale che $h(f)$ si annulla identicamente su ogni punto di $\mathbf{V}(I)$.

Proposizione 2.2.2. *Sia $h(t) \in \mathbb{K}[t]$ e sia $f \in \mathbb{K}[x_1, \ldots, x_n]$. Allora:*

$$h(M_f) = 0 \iff h(f) \in I \tag{2.4}$$

Dimostrazione.

$$\begin{array}{rcll} h(f) \in I & \iff & M_{h(f)} = 0 & \text{(per la Proposizione 2.1.3 parte 2)} \\ & \iff & h(M_f) = 0 & \text{(per il Corollario 2.1.9)} \end{array}$$

□

I polinomi h tali che $h(M_f) = 0$ formano un ideale di $\mathbb{K}[t]$, come afferma la seguente:

Proposizione 2.2.3. *Sia M una matrice quadrata di ordine d con entrate in un campo $\mathbb{K}$. L'insieme I_M di tutti i polinomi $h(t) \in \mathbb{K}[t]$ tali che $h(M) = 0$ (matrice nulla di ordine d) è un ideale non nullo di $\mathbb{K}[t]$.*

Dimostrazione. Il fatto che I_M sia non vuoto è evidente, dal momento che $0 \in I_M$. Per provare che contiene almeno un elemento diverso da 0, è sufficiente ricordare il seguente fatto: l'anello $\mathcal{M}_{d\times d}(\mathbb{K})$ è anche uno spazio vettoriale su $\mathbb{K}$ di dimensione d^2.
Come nell'Osservazione 2.2.1, l'insieme $\{I_d, M, M^2, \ldots\}$ deve necessariamente essere composto da vettori linearmente dipendenti. Da ciò segue che esistono $c_i \in \mathbb{K}$, non tutti nulli, tali che

$$c_0 I_d + c_1 M + c_2 M^2 + \cdots + c_n M^n = 0.$$

Questo è equivalente a dire che $h(t) = \sum_{i=0}^{n} c_i t^i \in I_M$. Proviamo ora che si tratta di un ideale: siano $h, k \in I_M$ e $p(t) \in \mathbb{K}[t]$.
1. $(h + k)(M) = h(M) + k(M) = 0 + 0 = 0$, dunque $h + k \in I_M$;
2. $(p \cdot h)(M) = p(M) \cdot h(M) = p(M) \cdot 0 = 0$, dunque anche $p \cdot h \in I_M$. □

Definizione 2.2.4. (*polinomio minimo*)
Il generatore monico non nullo m_M[1] di I_M è chiamato il *polinomio minimo* di M.

Osservazione 2.2.5. Questa definizione è equivalente a quella che abbiamo dato nel paragrafo 1.4 (vedi Definizione 1.4.5). Infatti, il generatore monico di I_M è banalmente il polinomio monico di grado minimo tale per cui $m_M(M) = 0$.
Viceversa, se $m_M(t)$ è il polinomio monico di grado minimo tale per cui $m_M(M) = 0$, allora divide tutti gli altri polinomi $f(t)$ per i quali vale $f(M) = 0$ e dunque è il generatore monico di I_M. Se per assurdo così non fosse, potrei scrivere che $f(t) = m_M(t)q(t) + r(t)$ con $\deg(r(t)) = 0$ o $\deg(r(t)) < \deg(m_M(t))$, ma allora $f(M) = m_M(M)q(M) + r(M) = 0 + r(M) = 0$ e quindi $r(t)$, di grado strettamente minore del grado di $m_M(t)$, soddisferebbe la proprietà. Assurdo.

Dall'osservazione precedente deduciamo che, se h è un qualunque polinomio tale che $h(M) = 0$, allora il polinomio minimo m_M divide h. In particolare, il polinomio minimo divide il polinomio caratteristico della matrice M. Vale inoltre la seguente proprietà:

[1] Esiste ed è unico perché $\mathbb{K}[t]$ è un PID

Teorema 2.2.6. *Sia $M \in \mathcal{M}_{n\times n}(R)$ una matrice quadrata di ordine n con entrate in un anello commutativo con unità R. Allora il suo polinomio minimo divide il polinomio caratteristico e i due hanno esattamente le stesse radici (a meno della molteplicità). In particolare, le radici del polinomio minimo sono tutti e soli gli autovalori della matrice M.*

Dimostrazione. Siano $m_M(t)$ e $p_M(t)$ in $R[t]$ rispettivamente il polinomio minimo e quello caratteristico di M. La prima affermazione l'abbiamo provata sopra, dimostriamo allora la seconda.
Sia λ un autovalore della matrice M, con corrispondente autovettore $v \neq 0$ e sia

$$m_M(t) = t^d + c_{d-1}t^{d-1} + \cdots + c_1 t + c_0$$

l'espressione estesa di $m_M(t)$. Dal momento che $m_M(M) = 0_n$ (matrice nulla di ordine n), vale la seguente uguaglianza:

$$\begin{aligned} 0 = m_M(M)\cdot v &= M^d \cdot v + c_{d-1}M^{d-1}\cdot v + \cdots + c_1 M\, v + c_0 I \cdot v \\ &= \lambda^d v + c_{d-1}\lambda^{d-1}v + \cdots + c_1\lambda v + c_0 v \\ &= m_M(\lambda)v, \end{aligned}$$

dove il primo membro è il vettore nullo e l'operazione $\cdot$ è il prodotto di matrici. Poiché v è non nullo per ipotesi, questo implica che $m_M(\lambda) = 0$ e dunque tutti gli autovalori della matrice M sono radici del polinomio minimo. Tali autovalori sono anche tutte e sole le radici del polinomio caratteristico, e questo prova l'asserto. □

Corollario 2.2.7. *Se gli autovalori della matrice M sono tutti distinti, allora $m_M(t) = p_M(t)$.*

Denotiamo allora (con un piccolo abuso di notazione) il polinomio minimo dell'applicazione m_f con p_f e consideriamo i seguenti insiemi numerici:

- le *soluzioni* dell'equazione $p_f(t) = 0$,
- gli *autovalori* dell'endomorfismo m_f (o della matrice M_f, se è stata fissata una base),
- i *valori* che la funzione polinomiale f assume sui punti della varietà $\mathbf{V}(I)$.

La tesi dell'Eigenvalue Theorem è che questi tre insiemi coincidono, qualora l'ideale I sia zero-dimensionale.

Teorema 2.2.8. (Eigenvalue Theorem)
Sia $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideale zero-dimensionale, $\mathbb{K}$ algebricamente chiuso, $f \in \mathbb{K}[x_1, \ldots, x_n]$ e sia p_f il polinomio minimo di m_f su $A = \mathbb{K}[x_1, \ldots, x_n]/I$. Allora, per $\lambda \in \mathbb{K}$, le seguenti affermazioni sono equivalenti:

1. *λ è una soluzione dell'equazione $p_f(t) = 0$,*
2. *λ è un autovalore dell'endomorfismo m_f,*
3. *λ è un valore assunto dalla funzione polinomiale f su $\mathbf{V}(I)$.*

Dimostrazione. ($1 \iff 2$): È il Teorema 2.2.6.
($2 \Rightarrow 3$): Sia λ un autovalore di M_f. Allora c'è un corrispondente autovettore $[z] \in A$, $[z] \neq [0]$, tale che $[f][z] = \lambda[z]$, ossia $[f - \lambda][z] = [0]$. Per assurdo, supponiamo che λ non sia un valore assunto da f sui punti di $\mathbf{V}(I)$. Cioè, se $\mathbf{V}(I) = \{p_1, \ldots, p_m\}$, supponiamo che $f(p_i) \neq \lambda$ per ogni $i = 1, \ldots, m$.
Sia $g = f - \lambda$, così che $g(p_i) \neq 0$ per ogni $i = 1, \ldots, m$. Per il Lemma 1.3.12, esistono polinomi g_i tali che $g_i(p_j) = 0$ se $i \neq j$, e $g_i(p_i) = 1$. Consideriamo il polinomio $g' = \sum_{i=1}^{m} \frac{1}{g(p_i)} g_i$. Segue che $g'(p_i)g(p_i) = 1$ per ogni i, e allora $1 - gg' \in \mathbf{I}(\mathbf{V}(I))$. Per il Nullstellensatz (Teorema 1.2.25), $(1 - gg')^l \in I$ per qualche $l \geq 1$. Espandendo con la formula del binomio di Newton e raccogliendo i termini che contengono g come fattore, otteniamo che $1 - \tilde{g}g \in I$ per qualche $\tilde{g} \in \mathbb{K}[x_1, \ldots, x_n]$. In A, ciò implica che $[1] = [\tilde{g}][g]$, quindi $[g]$ ha un inverso moltiplicativo $[\tilde{g}]$ in A.
Ma, per quanto scritto sopra, abbiamo che $[g][z] = [f - \lambda][z] = [0]$ in A. Moltiplicando entrambi i membri per $[\tilde{g}]$, otteniamo che $[z] = [0]$, il che è assurdo. Di conseguenza λ deve essere un valore assunto da f su un punto di $\mathbf{V}(I)$.
($3 \Rightarrow 1$): Sia $\lambda = f(p)$ per qualche $p \in \mathbf{V}(I)$. Dal momento che $p_f(M_f) = 0$, per (2.4) abbiamo che $p_f([f]) = [0]$, e quindi (2.3) implica che $p_f(f) \in I$. Questo significa che $p_f(f)$ si annulla identicamente in ogni punto di $\mathbf{V}(I)$, quindi $p_f(\lambda) = p_f(f(p)) = 0$. $\square$

Riportiamo ora un corollario dell'Eigenvalue Theorem, che consente di calcolare esplicitamente le coordinate delle soluzioni.

Corollario 2.2.9. *Sia $I \subset \mathbb{K}[x_1, \ldots, x_n]$ un ideale zero-dimensionale. Allora gli autovalori della mappa di moltiplicazione m_{x_i}, per $i \in \{1, \ldots, n\}$, coincidono con le coordinate x_i dei punti di $\mathbf{V}(I)$. Inoltre, sostituendo $t = x_i$ nel polinomio minimo p_{x_i} si ottiene l'unico generatore monico dell'ideale di eliminazione $I \cap \mathbb{K}[x_i]$.*

Dimostrazione. La prima affermazione segue direttamente dal punto 3 dell'Eigenvalue Theorem.
Per quanto riguarda la seconda, invece, ricordiamo innanzitutto che, per definizione, il polinomio minimo della matrice M_f è il polinomio monico $p_f \in \mathbb{K}[t]$ di grado minimo tale che $p_f(M_f)$ è la matrice nulla, cioè $p_f(M_f) = 0$.
Per quanto visto nell'Osservazione 2.2.1, questo equivale a dire che p_f è il polinomio monico di grado minimo tale per cui $p_f(f) \in \langle f_1, \ldots, f_s \rangle$. In particolare il polinomio minimo di M_{x_i} è il polinomio monico di grado minimo tale che

$$p_{x_i}(x_i) \in \langle f_1, \ldots, f_s \rangle.$$

Ricordiamo inoltre che $\mathbb{K}[x_i]$ è un dominio a ideali principali, dunque ogni ideale in $\mathbb{K}[x_i]$ è generato da un unico polinomio monico; in particolare vale per $I \cap \mathbb{K}[x_i]$. Supponiamo sia $I \cap \mathbb{K}[x_i] = \langle g \rangle$. Dal momento che $p_{x_i}(x_i) \in I \cap \mathbb{K}[x_i]$, deve accadere che g divide p_{x_i}. Per la minimalità del grado di p_{x_i}, $p_{x_i} = cg$ con $c \in \mathbb{K}$, ma p_{x_i} è anche monico, dunque $c = 1$ e

$$I \cap \mathbb{K}[x_i] = \langle p_{x_i} \rangle \quad \square$$

Osservazione 2.2.10. La seconda affermazione del Corollario 2.2.9 stabilisce inoltre un legame tra le mappe di moltiplicazione e la teoria dell'eliminazione. Infatti dire che $I \cap \mathbb{K}[x_i] = \langle p_{x_i} \rangle$ equivale a dire che $p_{x_i}(x_i) = 0$ è l'equazione ottenuta eliminando tutte le indeterminate, eccetto x_i, dal sistema originale (2.1).

Esempio 2.2.11. Proseguiamo l'Esempio 2.1.4. Eravamo giunti a calcolare le matrici M_x e M_y. Il polinomio minimio di M_x è:

$$p_x(t) = t^4 - 2t^3 - t^2 + 2t = t(t^2 - 1)(t - 2)$$

e le sue radici risultano essere $0, -1, 1, 2$. Quindi queste sono le ascisse dei punti soluzione del sistema:

$$\begin{cases} x^2 + \frac{3}{2}xy + \frac{1}{2}y^2 - \frac{3}{2}x - \frac{3}{2}y = 0 \\ xy^2 - x = 0 \\ y^3 - y = 0 \end{cases} \tag{2.5}$$

Analogamente il polinomio minimo di M_y è:

$$p_y(t) = t^3 - t = t(t^2 - 1)$$

con radici $0, -1, 1$, che sono le ordinate di tali punti.

Osservazione 2.2.12. Osserviamo che il sistema (2.5) può anche essere risolto manualmente, notando che la terza equazione dipende solo dall'indeterminata y. Pertanto, risolvendo $y^3 - y = 0$ e sostituendo nelle altre due, otteniamo i punti

$$(0, 0), (1, 1), (-1, 1), (1, -1), (2, -1).$$

Si vede subito che due punti hanno la stessa ascissa e due coppie di punti hanno invece la stessa ordinata. Questo da un lato spiega la differenza tra i gradi dei due polinomi minimi e il numero effettivo di punti di $\mathbf{V}(I)$, dall'altro apre una nuova questione: formalmente avremmo potuto avere dodici punti in $\mathbf{V}(I)$ (tutte le possibili combinazioni degli autovalori), ma nella realtà ne abbiamo solo cinque: ricordiamo infatti che il numero di soluzioni del sistema può essere al più la dimensione di A, cinque nel nostro caso (Proposizione 1.3.13). Dunque, come accoppiare in maniera corretta i risultati che il metodo degli autovalori fornisce? In generale, provare tutte le possibili combinazioni può essere un metodo, ma si vede già da questo esempio quanto poco efficiente esso sia. Vedremo adesso come gli autovettori della matrice M_f forniscano una risposta più completa.

2.3 Autovettori delle mappe di moltiplicazione

Richiamiamo solo per comodità la definizione di autovettore.

Definizione 2.3.1. (*autovettore*)
Un *autovettore* della matrice $M \in \mathcal{M}_{n\times n}(\mathbb{K})$ è un vettore colonna $v \neq 0$ tale che

$$Mv = \lambda v$$

per qualche $\lambda \in \mathbb{K}$ autovalore di M.

Osservazione 2.3.2. M^T (trasposta di M) ha gli stessi autovalori di M, ma non ha gli stessi autovettori. In alcuni testi, gli autovettori della matrice trasposta vengono chiamati autovettori *sinistri*, per distinguerli dai tradizionali autovettori (detti *destri*). Noi qui non faremo questa distinzione e ci riferiremo a tali autovettori semplicemente come *autovettori della matrice trasposta*.

Proposizione 2.3.3. *Sia $p \in \mathbb{K}^n$ una soluzione del sistema di equazioni polinomiali (2.1) e $I = \langle f_1, \ldots, f_s \rangle$ l'ideale zero-dimensionale generato dai polinomi di (2.1). Siano inoltre $B = \{[x^{\alpha_1}], \ldots, [x^{\alpha_m}]\}$ una base monomiale di $A = \mathbb{K}[x_1, \ldots, x_n]/I$ e M_f la matrice associata all'applicazione m_f rispetto alla base B. Per $j = 1, \ldots, m$, sia p^{α_j} l'elemento di $\mathbb{K}$ ottenuto valutando il monomio x^{α_j} in $p \in \mathbf{V}(I)$. Allora:*

$$M_f^T \, (p^{\alpha_1}, \ldots, p^{\alpha_m})^T = f(p)(p^{\alpha_1}, \ldots, p^{\alpha_m})^T \tag{2.6}$$

e $f(p)$ è un autovalore di M_f.

Dimostrazione. Cominciamo a provare che $f(p)$ è un autovalore di M_f. Questo si può vedere o osservando che $[1] \in B$ (altrimenti non ci sono soluzioni, come abbiamo visto nel Corollario 1.2.17), dunque $(p^{\alpha_1}, \ldots, p^{\alpha_m})^T$ è non nullo e allora $f(p)$ è autovalore per definizione, oppure ricordando l'Eigenvalue Theorem (Teorema 2.2.8).
Per provare (2.6) invece, supponiamo che $M_f = (m_{ij})$. Questo significa che

$$[x^{\alpha_j} f] = m_f([x^{\alpha_j}]) = \sum_{i=1}^{m} m_{ij}[x^{\alpha_i}]$$

per $j = 1, \ldots, m$. Allora $x^{\alpha_j} f \equiv \sum_{i=1}^{m} m_{ij} x^{\alpha_i} \mod I$. Dal momento che tutti gli f_i, per $i = 1, \ldots, m$, si annullano identicamente in p, vale:

$$p^{\alpha_j} f(p) = \sum_{i=1}^{m} m_{ij} p^{\alpha_i} \qquad j = 1, \ldots, m. \tag{2.7}$$

(2.6) è la formulazione matriciale di (2.7) e questo conclude la dimostrazione. □

Corollario 2.3.4. *$(p^{\alpha_1}, \ldots, p^{\alpha_m})^T$ è un autovettore di M_f^T, con $p \in \mathbf{V}(I)$.*

Corollario 2.3.5. *Sia $f \in \mathbb{K}[x_1, \ldots, x_n]$ tale che i valori $f(p)$ siano distinti per ogni $p \in \mathbf{V}(I)$, dove I è un ideale radicale zero-dimensionale proprio. Allora gli autospazi della matrice M_f^T sono di dimensione 1 e sono generati dai vettori riga $(p^{\alpha_1}, \ldots, p^{\alpha_m})$ per $p \in \mathbf{V}(I)$.*

Dimostrazione. Per il Corollario 2.3.4, $(p^{\alpha_1}, \ldots, p^{\alpha_m})$ è un autovettore di M_f^T con autovalore corrispondente $f(p)$. Per ipotesi, gli $f(p)$ sono tutti distinti per ogni $p \in \mathbf{V}(I)$. I è radicale (sempre per ipotesi), quindi $\mathbf{V}(I)$ contiene esattamente $m = \dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I)$ punti (per la Proposizione 1.3.13) e allora la matrice $M_f \in \mathcal{M}_{m \times m}(\mathbb{K})$ ha m autovalori distinti. L'algebra lineare garantisce allora che i corrispondenti autospazi hanno dimensione 1 e sono generati dagli autovettori $(p^{\alpha_1}, \ldots, p^{\alpha_m})$. □

Osservazione 2.3.6. Se l'ideale I non fosse radicale, $\mathbf{V}(I)$ potrebbe avere meno di m punti e dunque il Corollario 2.3.5 potrebbe non valere più. Cioè, gli $f(p)$ potrebbero essere tutti distinti, ma gli autospazi associati avere dimensione strettamente maggiore di 1 (ad esempio nel caso di matrici M_f con autovalori di molteplicità algebrica e geometrica strettamente maggiore di 1). Per quanto studieremo in seguito, però, sarà sufficiente che gli autospazi della matrice M_f^T siano tutti di dimensione 1, indipendentemente dalla molteplicità algebrica dei relativi autovalori[2]. Richiamiamo allora la definizione seguente.

[2]Nel senso che quella che conta è la molteplicità geometrica degli autovalori, e non quella algebrica. Ci possono essere matrici non-derogatorie con autovalori di molteplicità algebrica maggiore di 1, ma geometrica esattamente pari a 1 (ad esempio quella dell'Esempio 2.4.1).

Definizione 2.3.7. (*matrice non-derogatoria*)
Una matrice $M \in \mathcal{M}_{n\times n}(\mathbb{K})$ quadrata di ordine n a entrate in un campo algebricamente chiuso $\mathbb{K}$ è *non-derogatoria* se tutti i suoi autospazi hanno dimensione 1.

Osservazione 2.3.8. Se una matrice quadrata di ordine n ha n autovalori distinti, allora è non-derogatoria (è una conseguenza del Corollario 2.2.7 e della Proposizione 1.4.15).

Vediamo adesso come sfruttare la teoria sviluppata sugli autovettori per trovare le soluzioni del sistema (2.1).

Assumiamo di essere nelle stesse ipotesi della Proposizione 2.3.3 e consideriamo nuovamente l'equazione (2.6):

$$M_f^T\,(p^{\alpha_1},\dots,p^{\alpha_m})^T = f(p)(p^{\alpha_1},\dots,p^{\alpha_m})^T.$$

Supponiamo, inoltre, che la matrice M_f^T sia non-derogatoria (cioè tutti i suoi autospazi abbiano dimensione 1) e che $\lambda \in \mathbb{K}$ sia un autovalore di M_f^T associato all'autovettore

$$\mathbf{v} = (u_1,\dots,u_m)^T.$$

Osservazione 2.3.9. Sappiamo dall'algebra lineare che $\mathbf{v}$ è unico, a meno di uno scalare, e che $\lambda = f(p)$ per un qualche $p \in \mathbf{V}(I)$.
Per trovare quale p, è sufficiente ricordare che anche $(p^{\alpha_1},\dots,p^{\alpha_m})^T$ è un autovettore di M_f^T associato a λ. Per il Corollario 2.3.5, questo significa che

$$\mathbf{v} = c(p^{\alpha_1},\dots,p^{\alpha_m})^T$$

per qualche $c \in \mathbb{K}$. D'altro canto, abbiamo come ipotesi che $1 \notin I$ e possiamo quindi assumere che $x^{\alpha_1} = 1$. Di conseguenza, la prima coordinata p^{α_1} è 1 e, riscalando opportunamente $\mathbf{v}$ in modo che abbia come prima coordinata 1, otteniamo:

$$\mathbf{v} = (1, v_2,\dots,v_m)^T = (1, p^{\alpha_2},\dots,p^{\alpha_m})^T. \tag{2.8}$$

La chiave, a questo punto, sta nel fatto che tra i monomi $x^{\alpha_j} \in B$ compaiono alcune tra le indeterminate $x_1,\dots,x_n$ (se non addirittura tutte). Infatti, il Teorema 1.3.9 (Finiteness Theorem) assicura che, per ogni $i = 1,\dots,n$, esiste un $m_i \geq 1$ tale che $x_i^{m_i}$ è il termine iniziale di un qualche elemento di G (base di Grobner dell'ideale I). Se $m_i > 1$, questo significa che $[x_i] \in B$ e dunque che *si possono leggere le corrispondenti coordinate di p direttamente da* $(1, v_2,\dots,v_m)$.

Esempio 2.3.10. Proseguiamo ancora con l'Esempio 2.1.4. Maple ci dice che le matrici M_x e M_y sono entrambe derogatorie. Tuttavia, se consideriamo $f = 3x+2y$, la matrice

$$M_f^T = 3M_x^T + 2M_y^T$$

risulta essere non-derogatoria e possiamo applicare il metodo degli autovettori (per verificarlo basta controllare che il polinomio minimo e il polinomio caratteristico coincidano[3] o, più semplicemente, controllare che il polinomio caratteristico abbia 5 radici distinte). Ricaviamo allora che:

[3] Per la dimostrazione del fatto che questo è equivalente a richiedere che la matrice sia non-derogatoria si veda la sezione 1.4.1

l'autovalore	-1	ha come autovettore associato	$(1,-1,1,-1,1)$
l'autovalore	0	ha come autovettore associato	$(1,0,0,0,0)$
l'autovalore	1	ha come autovettore associato	$(1,1,-1,-1,1)$
l'autovalore	4	ha come autovettore associato	$(1,2,-1,-2,1)$
l'autovalore	5	ha come autovettore associato	$(1,1,1,1,1)$

Dal momento che avevamo trovato $B = \{[1],[x],[y],[xy],[y^2]\}$, abbiamo che le indeterminate x e y occupano la seconda e terza posizione, rispettivamente. Segue allora dalla (2.8) che le coordinate delle soluzioni sono la seconda e la terza coordinata degli autovettori. Otteniamo dunque:

$$(-1,1),(0,0),(1,-1),(2,-1),(1,1)$$

che sono esattamente le soluzioni che avevamo trovato nell'Esempio 2.2.11.

Giunti a questo punto sorgono spontanee alcune domande, una delle quali ci viene suggerita dall'esempio svolto sopra:

1. Cosa succede quando alcune indeterminate non compaiono in B? Cioè, come si possono trovare le coordinate p_i delle soluzioni quando $m_i = 1$, per qualche $i \in \{1,\dots,n\}$?
2. Come si può trovare un $f \in \mathbb{K}[x_1,\dots,x_n]$ tale che M_f^T sia non derogatoria?

2.3.1 Indeterminate mancanti

Cominciamo a rispondere alla prima domanda.
Sappiamo che, una volta fissato un ordine monomiale, l'ideale $\langle f_1,\dots,f_s\rangle$ ammette una base di Gröbner G. Assumiamo che tale base sia *ridotta*, cioè:

- il coefficiente direttivo di ogni $g \in G$ sia 1;
- per ogni $g \in G$, i termini di g che non sono quello iniziale non siano divisibili per nessuno dei termini inziali degli altri polinomi in G.

Sappiamo anche che G permette di determinare l'insieme normale

$$N = \{x^\alpha : x^\alpha \text{ non è divisibile per nessuno dei termini iniziali dei } g \in G\}$$

da cui ricaviamo B. Sfruttando il metodo degli autovettori, possiamo ricavare tutte le coordinate delle soluzioni di (2.1) corrispondenti alle indeterminate che compaiono in B. Le indeterminate il cui laterale non compare in B sono quelle che possiamo definire *mancanti*.

Osservazione 2.3.11. Per quanto detto poco sopra sappiamo che le indeterminate mancanti sono quelle per cui $m_i = 1$. Tali indeterminate sono evidentemente divisibili per il termine iniziale di qualche $g \in G$. Cioè, se x_i è mancante, allora deve esistere un $g_i \in G$ tale che:

$$g_i = x_i + \text{ termini strettamente minori rispetto all'ordine scelto.}$$

Inoltre, poiché questo è vero per ogni variabile mancante e abbiamo supposto G ridotta, segue che gli altri termini di g_i coinvolgono solo indeterminate che possiamo chiamare *note* (cioè il cui laterale compare in B). Infatti, se una variabile mancante $x_j \neq x_i$ occorresse in uno degli altri termini di g_i, quel termine sarebbe divisibile per il termine iniziale di un certo $g_j \in G$, contro l'ipotesi che G sia ridotta.
Dunque possiamo assumere che, per ogni x_i mancante, esiste un g_i in G tale che:

$$g_i = x_i + \text{ termini che coinvolgono solo indeterminate note}$$

Sia ora p una soluzione del sistema (2.1). Dal momento che $g_i(p) = 0$, per l'Osservazione 2.3.11 possiamo concludere che

$$0 = p_i + \text{ termini che coinvolgono solo coordinate già note.}$$

Questo ci permette di ricavare le coordinate mancanti in funzione di quelle già trovate in precedenza col metodo degli autovettori.

2.3.2 Matrici non-derogatorie

Se l'ideale I risulta essere radicale, allora possiamo considerare un polinomio

$$f = c_1x_1 + c_2x_2 + \cdots + c_nx_n$$

con i coefficienti c_i $(1 \leq i \leq n)$ scelti casualmente. Questo ci garantisce, con una certa sicurezza, che i valori $f(p)$ saranno tutti distinti, per ogni $p \in \mathbf{V}(I)$. In tal caso, la matrice M_f sarà non-derogatoria e potremo applicare il Corollario 2.3.5 e il metodo sviluppato nella Sezione 2.3.1. Vale infatti il seguente risultato:

Proposizione 2.3.12. *Sia $I = \langle f_1, \ldots, f_s \rangle$ un ideale zero-dimensionale e radicale. Allora un polinomio $f \in \mathbb{K}[x_1, \ldots, x_n]$ assume valori distinti sui punti di $\mathbf{V}(I)$ se e solo se il polinomio caratteristico di M_f, $p_{M_f}(\lambda)$, ha tutte radici distinte.*

Dimostrazione. ($\Rightarrow$) : Per ipotesi f assume valori distinti sui punti di $\mathbf{V}(I)$, ma dal momento che I è radicale la Proposizione 1.3.13 ci garantisce che $\mathbf{V}(I)$ ha esattamente n punti distinti, dove $n = \dim_{\mathbb{K}}(\mathbb{K}[x_1, \ldots, x_n]/I)$. La matrice M_f è quadrata di ordine n e ammette gli $f(p)$ come autovalori, dunque ha n autovalori distinti e il suo polinomio caratteristico è prodotto di fattori lineari.
($\Leftarrow$) : Se il polinomio caratteristico ha $n = \dim_{\mathbb{K}} \mathbb{K}[x_1, \ldots, x_n]/I$ radici distinte, allora M_f ha n autovalori distinti, che sono i valori assunti da f sui punti di $\mathbf{V}(I)$. □

Purtroppo, nel caso in cui I non sia radicale, può capitare che la matrice M_f sia derogatoria *per tutti gli* $f \in \mathbb{K}[x_1, \ldots, x_n]$. Si consideri infatti l'esempio significativo seguente:

Esempio 2.3.13. Consideriamo il sistema:

$$\begin{cases} x^2 = 0 \\ y^2 = 0 \end{cases}$$

Esso ha come unica soluzione $p = (0, 0)$, dunque $\mathbf{V}(I) = \{(0, 0)\}$.
Applichiamo adesso la teoria finora sviluppata. Posto $I = \langle x^2, y^2 \rangle$, una base di Gröbner G per I è data da $G = \{x^2, y^2\}$. Si deduce allora facilmente che una base per $A = \mathbb{K}[x, y]/I$ è data da $B = \{[1], [x], [y], [xy]\}$.
Sia $f \in \mathbb{K}[x, y]$ un polinomio qualunque:

$$f = a + bx + cy + dx^2 + exy + fy^2 + \cdots .$$

Sappiamo che $f(p) = a$ e abbiamo che:

$$\begin{aligned} N_G([f] \cdot [1]) &= a[1] + b[x] + c[y] + e[xy] \\ N_G([f] \cdot [x]) &= a[x] + c[xy] \\ N_G([f] \cdot [y]) &= a[y] + b[xy] \\ N_G([f] \cdot [xy]) &= a[xy] \end{aligned}$$

e dunque

$$M_f = \begin{pmatrix} a & 0 & 0 & 0 \\ b & a & 0 & 0 \\ c & 0 & a & 0 \\ e & c & b & a \end{pmatrix}.$$

La matrice $M_f^T - f(p)I_4$ ha chiaramente rango al più 2 e questo vale per ogni polinomio $f \in \mathbb{K}[x, y]$. Ma allora l'autospazio di M_f^T relativo a $f(p) = a$ ha dimensione almeno 2 e quindi la matrice è derogatoria per ogni $f \in \mathbb{K}[x, y]$.

Nel caso in cui l'ideale I non sia radicale le possibilità risultano essere molteplici:

1. Si può costruire il radicale di I: $\sqrt{I}$. Esso fornisce un sistema di equazioni con le stesse soluzioni di quello definito da I, ma con molteplicità minore.

2. Si può dimostrare che, intersecando gli autospazi delle $M_{x_i}^T$ in una opportuna maniera, questi risultano uno-dimensionali e dunque si può applicare il metodo degli autovettori per trovare tutte le soluzioni (per approfondimenti si consulti [Cox] e scritti ivi citati).

3. Si può ricorrere semplicemente al metodo degli autovalori.

Esempio 2.3.14. Mostriamo come la terza via, nel caso dell'Esempio 2.3.13, fornisca la soluzione in pochi passi. È infatti sufficiente calcolare, con poca difficoltà, le matrici:

$$M_x = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad M_y = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

e osservare che entrambe ammettono come unico autovalore 0. Allora, per il Corollario 2.2.9, $\mathbf{V}(I) = \{(0, 0)\}$.

Osservazione 2.3.15. Supponiamo che I non sia radicale. Uno dei motivi per cui $\mathbf{V}(I)$ può avere meno di $m = \dim(A)$ punti è che qualcuno di questi abbia una *molteplicità* maggiore come punto di $\mathbf{V}(I)$, come capita ad esempio quando si interseca la parabola $y = x^2$ con la retta $y = 0$. In alcuni di questi casi la matrice M_f risulta essere derogatoria per ogni polinomio f. Un possibile approccio consiste allora nel determinare (dopo averne definita una) la *molteplicità* dei punti di $\mathbf{V}(I)$ e trovare i punti col metodo degli autovalori. Si può inoltre dimostrare il seguente fatto: se $p_f(t)$ è il polinomio minimo dell'endomorfismo m_f e $p \in \mathbf{V}(I)$, allora la molteplicità di $f(p)$ come radice di $p_f(t)$ è pari alla molteplicità di p come punto di $\mathbf{V}(I)$, a patto che f assuma valori sempre diversi quando valutato sui punti di $\mathbf{V}(I)$[4] (ricordiamo che, per l'Eigenvalue Theorem, i valori assunti da f sui punti di $\mathbf{V}(I)$ coincidono con gli autovalori di m_f).

2.4 Esempi finali

Concludiamo riportando ulteriori esempi di soluzione di sistemi polinomiali sia con il metodo degli autovettori che con quello degli autovalori.

Esempio 2.4.1. Si consideri il seguente sistema di equazioni polinomiali in $\mathbb{C}[x, y]$:

$$\begin{cases} x^2 + 2y^2 - 2y = 0 \\ xy^2 - xy = 0 \\ y^3 - 2y^2 + y = 0 \end{cases}$$

È immediato osservare che tale sistema ammette come uniche soluzioni i punti $(0, 0)$ e $(0, 1)$: basta infatti notare che possiamo riscrivere le equazioni come:

$$\begin{cases} x^2 + 2y(y-1) = 0 \\ xy(y-1) = 0 \\ y(y-1)^2 = 0 \end{cases}$$

Sappiamo dunque che $\mathbf{V}(x^2 + 2y^2 - 2y, xy^2 - xy, y^3 - 2y^2 + y) = \{(0, 0), (0, 1)\}$, ma cerchiamo di giungere a questa stessa conclusione ricorrendo al metodo degli autovalori e a quello degli autovettori.
Consideriamo in T_2 l'ordinamento lessicografico con $x > y$; in tal caso $g_1 = x^2+2y^2-2y$, $g_2 = xy^2 - xy$ e $g_3 = y^3 - 2y^2 + y$ formano una base di Gröbner G per l'ideale $I = \langle g_1, g_2, g_3 \rangle$ da loro generato.
Dal momento che $\mathrm{lt}(G) = \{x^2, xy^2, y^3\}$, ricaviamo $N = \{1, x, xy, y, y^2\}$. Dunque, una base per $A = \mathbb{C}[x, y]/I$ è data da

$$B = \left\{[1], [x], [xy], [y], [y^2]\right\}.$$

Osserviamo rapidamente che $\dim_{\mathbb{C}}(A) = 5$, mentre la varietà è composta solo da due punti; per la Proposizione 1.3.13, questo ci dice che l'ideale I non è radicale. Tuttavia vedremo che, in questo particolare caso, si può applicare anche il metodo degli autovettori e questo fornisce comunque le risposte da noi cercate.

[4] Per approfondire l'argomento si vedano [CLO2], pagina 145 e seguenti, e [Cox].

Per poter applicare il metodo degli autovalori, dobbiamo calcolare le matrici M_x e M_y:

$$\begin{aligned}
[x] \cdot [1] &= [x] \\
[x] \cdot [x] &= [x^2] = 2[y] - 2[y^2] \\
[x] \cdot [xy] &= [x^2 y] = [x^2] \cdot [y] = 2[y^2] - 2[y^3] \\
&= 2[y^2] - 2(-[y] + 2[y^2]) = 2[y] - 2[y^2] \\
[x] \cdot [y] &= [xy] \\
[x] \cdot [y^2] &= [xy^2] = [xy]
\end{aligned}$$

da cui otteniamo:

$$M_x = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 2 & 2 & 0 & 0 \\ 0 & -2 & -2 & 0 & 0 \end{pmatrix}$$

e, analogamente:

$$M_y = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 2 \end{pmatrix}$$

Sviluppando i determinanti $\det(M_x - \lambda I)$ e $\det(M_y - \lambda I)$, troviamo che i polinomi caratteristici sono:

$$\begin{aligned}
p(\lambda, M_x) &= -\lambda^5 \\
p(\lambda, M_y) &= \lambda^2 (1 - \lambda)^3
\end{aligned}$$

e, poiché hanno le stesse radici dei rispettivi polinomi minimi, troviamo conferma al fatto che l'unico valore che assume la prima coordinata è 0, mentre gli unici assunti dalla seconda sono 0 e 1 (come già sapevamo). A questo punto potremmo andare per tentativi e scoprire che effettivamente entrambe le coppie sono punti di $\mathbf{V}(I)$, oppure cambiare approccio e applicare il metodo degli autovettori (come stiamo per fare).
Se calcolassimo i polinomi minimi delle due matrici, troveremmo:

$$\begin{aligned}
p_x(t) &= t^3 \\
p_y(t) &= t(1 - t)^2
\end{aligned}$$

il che ci dice che nessuna delle due è non-derogatoria. Proviamo allora con $f = 2x + 3y$:

$$M_f = 2M_x + 3M_y = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 \\ 0 & 3 & 3 & 2 & 2 \\ 3 & 4 & 4 & 0 & -3 \\ 0 & -4 & -4 & 3 & 6 \end{pmatrix}$$

Calcolando polinomio minimo e caratteristico, scopriamo che coincidono tra loro; in particolare $p(t, M_f) = p_f(t) = t^2(t - 3)^3$ e quindi la matrice M_f è non-derogatoria. Possiamo allora applicare il metodo degli autovettori alla matrice M_f e scoprire che:

l'autovalore	0	ha come autovettore associato	$(1,0,0,0,0)$
l'autovalore	3	ha come autovettore associato	$(1,0,0,1,1)$

Dal momento che le indeterminate x e y compaiono come seconda e quarta nella base B, troviamo i punti $(0,0)$ e $(0,1)$. Siamo così giunti alla stessa conclusione a cui eravamo giunti all'inizio.
Osserviamo inoltre che la condizione di radicalità dell'ideale I non è necessaria; è però sufficiente a garantire che esista un f per cui M_f è non-derogatoria.

Poiché gli esempi svolti finora erano tutti particolarmente semplici da risolvere (anche a mano), riportiamo come ultimo un esempio un po' meno immediato.

Esempio 2.4.2. In $\mathbb{C}[u,x,y,z]$ si introduca l'ordinamento *lex* con $z<y<x<u$ e si consideri il sistema di equazioni polinomiali:

$$\begin{cases} u+y-2z^2=0 \\ 2z^4+z^3-2z^2-z=0 \\ 4x+22z^3+z^2-21z-4=0 \\ 2y+2z^3+3z^2-z-2=0 \end{cases}$$

1. Cerchiamone le soluzioni ricorrendo al metodo degli autovalori.
Sia

$$I=\langle u+y-2z^2, 2z^4+z^3-2z^2-z, 4x+22z^3+z^2-21z-4, 2y+2z^3+3z^2-z-2\rangle$$

l'ideale di $\mathbb{C}[u,x,y,z]$ generato dai polinomi che definiscono la varietà. Una base di Gröbner per I rispetto all'ordinamento *lex* con $z<y<x<u$ è data da $G=\{g_1,g_2,g_3,g_4\}$, dove:

$$\begin{aligned} g_1 &:= u-z^3-\tfrac{7}{2}z^2+\tfrac{1}{2}z+1 \\ g_2 &:= x+\tfrac{11}{2}z^3+\tfrac{1}{4}z^2-\tfrac{21}{4}z-1 \\ g_3 &:= y+z^3+\tfrac{3}{2}z^2-\tfrac{1}{2}z-1 \\ g_4 &:= z^4+\tfrac{1}{2}z^3-z^2-\tfrac{1}{2}z \end{aligned}$$

Da ciò deduciamo che la varietà è non vuota e che l'ideale è zero-dimensionale. Inoltre otteniamo $\mathrm{lt}(G)=\{u,x,y,z^4\}$, da cui segue che $N=\{1,z,z^2,z^3\}$ e

$$B=\left\{[1],[z],[z^2],[z^3]\right\}$$

è una base per $A=\mathbb{C}[u,x,y,z]/I$. Sappiamo allora che la varietà è non vuota, è formata da punti e questi sono in numero di al più 4.
Calcolo adesso le matrici delle moltiplicazioni m_u, m_x, m_y, m_z rispetto alla base B:

$$\begin{aligned} m_u([1]) &= [u]=\left[-1-\frac{1}{2}z+\frac{7}{2}z^2+z^3\right] \\ m_u([z]) &= [u][z]=\left[-z-\frac{1}{2}z^2+\frac{7}{2}z^3+z^4\right] \\ &= \left[-z-\frac{1}{2}z^2+\frac{7}{2}z^3+\frac{1}{2}z+z^2-\frac{1}{2}z^3\right]=\left[-\frac{1}{2}z+\frac{1}{2}z^2+3z^3\right] \\ m_u([z^2]) &= [uz][z]=\left[-\frac{1}{2}z^2+\frac{1}{2}z^3+3z^4\right]=\left[\frac{3}{2}z+\frac{5}{2}z^2-z^3\right] \\ m_u([z^3]) &= [uz^2][z]=\left[\frac{3}{2}z^2+\frac{5}{2}z^3-z^4\right]=\left[-\frac{1}{2}z+\frac{1}{2}z^2+3z^3\right] \end{aligned}$$

da cui segue che:

$$M_u = \begin{pmatrix} -1 & 0 & 0 & 0 \\ -1/2 & -1/2 & 3/2 & -1/2 \\ 7/2 & 1/2 & 5/2 & 1/2 \\ 1 & 3 & -1 & 3 \end{pmatrix} \quad M_x = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 21/4 & -7/4 & 5/4 & -3/4 \\ -1/4 & -1/4 & 3/4 & -1/4 \\ -11/2 & 5/2 & -3/2 & 3/2 \end{pmatrix}$$

$$M_y = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1/2 & 1/2 & -1/2 & 0 \\ -3/2 & -1/2 & -1/2 & -1/2 \\ -1 & -1 & 0 & -1/2 \end{pmatrix} \qquad M_z = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1/2 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & -1/2 \end{pmatrix}$$

e i rispettivi polinomi minimi:

$$\begin{aligned} p_u(t) &= t^4 - 4t^3 + t^2 + 6t = t(t+1)(t-2)(t-3) \\ p_x(t) &= t^3 - \frac{1}{2}t^2 - t + \frac{1}{2} = \frac{1}{2}(t-1)(t+1)(2t-1) \\ p_y(t) &= t^4 - \frac{1}{2}t^3 - t^2 + \frac{1}{2}t = \frac{1}{2}t(t-1)(t+1)(2t-1) \\ p_z(t) &= t^4 + \frac{1}{2}t^3 - t^2 - \frac{1}{2}t = \frac{1}{2}t(t-1)(t+1)(2t+1) \end{aligned}$$

Abbiamo così trovato tutte le possibili coordinate dei punti della varietà, ma abbiamo ancora il problema di determinare le combinazioni giuste. Andare per tentativi è evidentemente troppo lungo: sappiamo che i punti sono al più 4 e abbiamo 4^4 possibili punti. Possiamo però osservare che i punti sono esattamente in numero di 4.
2. Applichiamo allora il metodo degli autovettori.
Osserviamo che evidentemente M_z è non-derogatoria: infatti il polinomio minimo e quello caratteristico hanno lo stesso grado. Possiamo allora cercare gli autospazi di ${M_z}^T$ e troviamo i seguenti autovettori:

l'autovalore	0	ha come autovettore associato	$(1,0,0,0)$
l'autovalore	1	ha come autovettore associato	$(1,1,1,1)$
l'autovalore	-1	ha come autovettore associato	$(-1,1,-1,1)$
l'autovalore	$-\frac{1}{2}$	ha come autovettore associato	$(-8,4,-2,1)$

Ora, la coordinata z compare come seconda nella base B, mentre le altre sono mancanti. Riscalo gli autovettori in modo che la prima coordinata sia 1 e leggo i valori assunti da z sui punti di $\mathbf{V}(I)$: 0, 1, -1, $-\frac{1}{2}$. Adesso applico il procedimento visto nella Sezione 2.3.1 per calcolare le altre coordinate.
Osservo innanzitutto che la base di Gröbner G trovata in precedenza è ridotta. E osservo anche che i polinomi g_1, g_2 e g_3 soddisfano la proprietà

$$g_i = x_i + \{ \text{ termini strettamente minori (nella sola z) } \}$$

che mi permette di ricavare le coordinate mancanti in funzione di quella già nota. Allora, sostituendo il valore $z = 0$ in g_1, g_2 e g_3:

$$\begin{aligned} g_1(\bar{u}, 0) = \bar{u} + 1 = 0 \quad &\iff \quad \bar{u} = -1 \\ g_2(\bar{x}, 0) = \bar{x} - 1 = 0 \quad &\iff \quad \bar{x} = 1 \\ g_3(\bar{y}, 0) = \bar{y} - 1 = 0 \quad &\iff \quad \bar{y} = 1, \end{aligned}$$

da cui deduco che $(-1,1,1,0)$ è un punto di $\mathbf{V}(I)$. Inoltre, con calcoli analoghi al precedente:

$$\begin{array}{lll} g_1(\bar{u},1)=\bar{u}-3=0 & \Longleftrightarrow & \bar{u}=3 \\ g_2(\bar{x},1)=\bar{x}-\frac{1}{2}=0 & \Longleftrightarrow & \bar{x}=\frac{1}{2} \\ g_3(\bar{y},1)=\bar{y}+1=0 & \Longleftrightarrow & \bar{y}=-1, \end{array}$$

$$\begin{array}{lll} g_1(\bar{u},-1)=\bar{u}-2=0 & \Longleftrightarrow & \bar{u}=2 \\ g_2(\bar{x},-1)=\bar{x}-1=0 & \Longleftrightarrow & \bar{x}=1 \\ g_3(\bar{y},-1)=\bar{y}=0 & \Longleftrightarrow & \bar{y}=0, \end{array}$$

$$\begin{array}{lll} g_1(\bar{u},-\frac{1}{2})=\bar{u}=0 & \Longleftrightarrow & \bar{u}=0 \\ g_2(\bar{x},-\frac{1}{2})=\bar{x}+1=0 & \Longleftrightarrow & \bar{x}=-1 \\ g_3(\bar{y},-\frac{1}{2})=\bar{y}-\frac{1}{2}=0 & \Longleftrightarrow & \bar{y}=\frac{1}{2}. \end{array}$$

Ottengo così che i quattro punti della varietà sono:

$$\mathbf{V}(I)=\left\{(-1,1,1,0),\left(3,\frac{1}{2},-1,1\right),(2,1,0,-1),\left(0,-1,\frac{1}{2},-\frac{1}{2}\right)\right\}.$$

Bibliografia

[AdLo] W.W. Adams e P. Loustaunau, *An Introduction to Gröbner Bases*, AMS, Providence RI, 1994.

[BeWe] T. Becker e V. Weispfenning, *Gröbner Bases: A Computational Approach to Commutative Algebra*, Springer Verlag, Berlino e New York, 1993.

[Cand] M. Candilera, *Autovalori ed Autovettori*, reperibile all'indirizzo web: www.math.unipd.it/∼candiler/didafiles/pdf-files/Autoval.pdf.

[Cox] D. Cox, *Solving Equation Via Algebra*, in: *Solving Polynomial Equations: Fundation, Algorithms, and Applications* (A. Dickenstein e I. Z. Emiris, eds.), Springer Verlag, Berlino, 2005.

[CLO1] D. Cox, J. Little e D. O'Shea, *Ideals, Varieties and Algorithms*, 3rd Ed., Springer Verlag, New York, 2007.

[CLO2] D. Cox, J. Little e D. O'Shea, *Using Algebraic Geometry*, 2nd Ed., Springer Verlag, New York, 2004.

[PCat] G.M. Piacentini Cattaneo, *Algebra: un approccio algoritmico*, Decibel-Zanichelli, Padova, 1996.

[Rot] J.J. Rotman, *Advanced Modern Algebra*, 1st Ed., Prentice Hall, 2002.