# Capitolo 1

# Nozioni di Algebra

*Rev. marzo 2011*
*Le parti asteriscate o racchiuse fra parentesi $<< * \quad * >>$ non fanno parte del programma*

In questo capitolo introduttivo esporremo alcune nozioni di algebra che saranno oggetto di applicazione nei diversi capitoli di questa dispensa di Sistemi Multivariabili. La presentazione ha carattere non sistematico e dà per acquisite da corsi precedenti alcune nozioni di Algebra Lineare e di Geometria: in particolare, le proprietà elementari di strutture algebriche quali i numeri interi, i razionali, i polinomi in una o più indeterminate, gli spazi vettoriali. Per approfondimenti si rinvia ai testi citati nella bibliografia.

## 1.1 Anelli e matrici su anelli

**Definizione 1.1.1** [Anello con unità] *Un anello (con unità) $R$ è un insieme nel quale sono definite due operazioni binarie, dette addizione e moltiplicazione (indicate rispettivamente con i simboli $+$ e $\cdot$)* [1].
*e dotato di due particolari elementi distinti 0 e 1, tali che*
- $(R, +, 0)$ *è un gruppo commutativo (in notazione additiva), ovvero per ogni $a, b, c \in R$ valgono le seguenti proprietà*
  - $a_1)$ $(a + b) + c = a + (b + c)$ *(associatività)*
  - $a_2)$ $a + b = b + a$ *(commutatività)*
  - $a_3)$ $a + 0 = 0 + a = a$ *(esistenza dell'elemento neutro)*
  - $a_4)$ *per ogni $a$ in $R$, esiste $b \in R$ tale che $a + b = b + a = 0$.*

*L'elemento $b$ viene detto l'opposto di $a$ e indicato con $-a$.*
- *La moltiplicazione gode delle seguenti proprietà: per ogni $a, b, c \in R$*
  - $m_1)$ $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *(associatività)*
  - $m_2)$ $a \cdot 1 = 1 \cdot a = a$ *(esistenza dell'elemento neutro).*
- *Per ogni $a, b, c \in R$ valgono le proprietà distributive:*
  - $d_1)$ $a \cdot (b + c) = a \cdot b + a \cdot c$
  - $d_2)$ $(a + b) \cdot c = a \cdot c + b \cdot c$.

[1] salvo che in questa definizione, nel seguito per brevità ometteremo il simbolo $\cdot$ per indicare l'operazione di moltiplicazione

Dalla proprietà distributiva segue che $a \cdot 0 = 0 \cdot a = 0$ per ogni $a \in R$. Diremo che un elemento $a \in R$ è *invertibile* se esiste $b \in R$ tale che $a \cdot b = b \cdot a = 1$. L'elemento $b$ è detto un *inverso* (moltiplicativo) di $a$. Quando esiste è unico, diverso da 0 (perchè?) e viene usualmente indicato con $a^{-1}$.
Un anello $R$ è detto *commutativo* se la moltiplicazione gode della proprietà commutativa, ovvero $a \cdot b = b \cdot a$, per ogni $a, b \in R$. **Nel seguito del capitolo, salvo contrario avviso, il termine "anello" denoterà sempre un anello commutativo**

**Definizione 1.1.2** [Domini (di integrità) e Campi] *Un dominio (d'integrità) $D$ è un anello in cui per ogni $a \in D \setminus \{0\}$, si ha $ab = 0 \Rightarrow b = 0$.*
*Un campo* [2] *$\mathbb{F}$ è un anello in cui ogni elemento diverso da 0 è invertibile.*

**Esempio 1.1.1** Rispetto alle usuali operazioni di addizione e moltiplicazione

(*i*) l'insieme dei numeri interi $\mathbb{Z}$ è un dominio i cui unici elementi invertibili sono 1 e -1;

(*ii*) l'insieme $\mathbb{N}$ dei numeri naturali e l'insieme $2\mathbb{Z}$ dei numeri interi pari non sono anelli;

(*iii*) per ogni $n \geq 1$, l'insieme $\mathbb{F}[z_1, z_2, \ldots, z_n]$ dei polinomi nelle indeterminate $z_1, z_2, ..., z_n$ a coefficienti nel campo $\mathbb{F}$ è un dominio. Quali sono i suoi elementi invertibili?

(*iv*) il sottoinsieme di $\mathbb{F}[z]$ costituito dai soli polinomi a potenze pari è un dominio.

(*v*) Se $R$ è un anello e $n$ un intero maggiore di 1, l'insieme $R^{n\times n}$ delle matrici di dimensione $n$ a coefficienti in $R$ è un anello non commutativo.

(*vi*) L'insieme $C[0,1]$ delle funzioni reali a valori reali, continue nell'intervallo [0,1], è un anello rispetto alle operazioni di somma e prodotto definite da

$$(f+g)(x) := f(x) + g(x) \qquad (fg)(x) := f(x)g(x).$$

È un dominio di integrità? Quali sono i suoi elementi invertibili?

- Esercizio 1.1.1 In un anello (non necessariamente commutativo) $ab = b'a = 1$ implica $b = b'$.

- Esercizio 1.1.2 (*i*) Se $a$ e $b$ sono elementi dell'anello $R$ allora $ab$ è invertibile se e solo se lo sono $a$ e $b$.

  (*ii*) Se $a$ è un elemento di un anello $R$ tale che $ab = 0$ per qualche $b \in R$ non nullo, allora $a$ non è invertibile.

  (*iii*) In un dominio di integrità vale la seguente *regola di cancellazione*: se $ac = bc$ e $c \neq 0$, allora $a = b$.

- Esercizio 1.1.3 [Campi e domini] (*i*) Ogni campo è un dominio.

  (*ii*) Ogni dominio finito $D$ è un campo.
  *(Suggerimento: se $a$ è diverso da 0, $\psi_a : D \to D : x \mapsto ax$ è iniettiva e quindi suriettiva).*
  *Osservazione Qui, come sempre in queste dispense, i domini sono intesi commutativi. Esiste un risultato, dovuto a Wedderburn, che asserisce che ogni anello di divisione (un anello - non necessariamente commutativo - in cui ogni elemento non nullo ha un inverso moltiplicativo) finito è un campo. Per una dimostrazione, si rinvia a [4, vol.2.cap.3].*

[2] Tale denominazione, dall'inglese inglese "field", non è l'unica in uso: in letteratura si trovano anche "corpo", dal tedesco "Körper", e "corpo commutativo".

- Esercizio 1.1.4 [Serie formali] (*i*) Con $\mathbb{F}((z))$, $\mathbb{F}$ un campo, denotiamo l'insieme delle serie formali di Laurent nell'indeterminata $z$ a coefficienti in $\mathbb{F}$, ovvero l'insieme delle espressioni formali del tipo $\sum_{i=h}^{+\infty} a_i z^i$, $h \in \mathbb{Z}$. Si dimostri che $\mathbb{F}((z))$ è un campo quando addizione e moltiplicazione vengono definite nel seguente modo:

$$(\sum_i a_i z^i) + (\sum_i b_i z^i) = \sum_i (a_i + b_i) z^i \tag{1.1}$$

$$(\sum_i a_i z^i)(\sum_i b_i z^i) = \sum_i \Big( \sum_{\substack{h,k\in\mathbb{Z} \\ h+k=i}} a_h b_k \Big) z^i. \tag{1.2}$$

(*ii*) L'insieme $\mathbb{F}[[z]] \subset \mathbb{F}((z))$ delle serie formali (a potenze non negative) nell'indeterminata $z$ a coefficienti in $\mathbb{F}$, ovvero l'insieme delle espressioni formali del tipo $\sum_{i=0}^{+\infty} a_i z^i$, è un dominio quando addizione e moltiplicazione vengono definite come al punto precedente. Perchè non è un campo? Quali sono gli elementi invertibili?

<< $*$ **Definizione 1.1.3** [Ordine di un elemento in un dominio] *Dato un dominio $R$, l'ordine di un elemento $a \in R$ è il più piccolo $k \in \mathbb{N}$ (se esiste) per cui si ha*

$$ka = \underbrace{a + a + \ldots + a}_{k \text{ volte}} = 0,$$

*ossia è l'ordine (se finito) del gruppo additivo generato da $a$.*

In un dominio $R$ tutti gli elementi non nulli hanno il medesimo ordine. Infatti, se $k > 1$ è l'ordine finito di $a \in R, a \neq 0$, $0 = ka = \underbrace{1_R \cdot a + \ldots + 1_R \cdot a}_{k \text{ volte}} = (k1_R) \cdot a$ e quindi $k1_R = 0$.
Scelto qualsiasi altro elemento $b \in R$, si ha

$$0 = (k1_R) \cdot b = \underbrace{1_R \cdot b + \ldots + 1_R \cdot b}_{k \text{ volte}} = \underbrace{b + \ldots + b}_{k \text{ volte}} = kb \tag{1.3}$$

In particolare, se $a$ è stato scelto come un elemento non nullo di ordine minimo, si vede da (**??**) che tutti gli elementi non nulli di $R$ hanno il medesimo ordine di $a$.
Tale ordine è un numero primo: se infatti esistesse una fattorizzazione propria $k = k_1 k_2$, con $k_1 k_2 > 1$, da

$$0 = (mn)1_R = \underbrace{1_R + 1_R + \ldots + 1_R}_{k_1 k_2 \text{ volte}} = \underbrace{\overbrace{1_R + \ldots + 1_R}^{k_1 \text{ volte}} + \ldots + \overbrace{1_R + \ldots + 1_R}^{k_1 \text{ volte}}}_{k_2 \text{ volte}} = k_2(k_1 1_R) \tag{1.4}$$

seguirebbe che $k_1 1_R$ è nullo, e quindi $1_R$ avrebbe ordine non superiore a $k_1$, oppure non è nullo, e quindi $(k_1 1_R$, e con lui tutti gli elementi non nulli, e in particolare) $1_R$ avrebbe ordine non superiore a $k_2$. Possiamo concludere con la seguente

**Proposizione 1.1.4** [Caratteristica di un dominio] *In un dominio $R$ tutti gli elementi non nulli hanno il medesimo ordine (finito o infinito). Il dominio $R$ si dirà di "caratteristica zero" se l'ordine dei suoi elementi non nulli è infinito, di "caratteristica $p$" se l'ordine dei suoi elementi non nulli è finito e vale $p$. Il numero $p$ è sempre un numero primo.* $*$ >>

Dato un anello (commutativo) $R$, si possono costruire le matrici $p \times m$ ad elementi in $R$ e definire nel modo consueto le operazioni di somma in $R^{p\times m}$ e di prodotto di una matrice $R^{p\times m}$ per una matrice in $R^{m\times n}$. Rispetto a tali operazioni l'insieme $R^{n\times n}$ delle matrici quadrate di ordine $n$ è un anello *non commutativo*.

**Definizione 1.1.5** [Determinanti] *Sia $R$ un anello (commutativo) e sia $R^{n\times n}$ l'anello (non commutativo) delle matrici $n \times n$ ad elementi in $R$ Una funzione*

$$d : R^{n\times n} \to R : M \mapsto d(M)$$

*degli $n^2$ elementi della matrice $M$ è detta un determinante se soddisfa le seguenti condizioni*

*D.1* *$d$ è una funzione lineare di ciascuna colonna di $M$;*

*D.2* *se due colonne di $M$ sono eguali, allora $d(M) = 0$;*

*D.3* $d(I_n) = 1$.

Se rappresentiamo la matrice $M$ per colonne

$$M = [\, \mathbf{c}_1 \quad \mathbf{c}_2 \quad \dots \quad \mathbf{c}_n \,],$$

e esprimiamo $d$ come funzione delle $n$ colonne della matrice, $d(M) = d(\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n)$, la condizione D.1 significa che

$$d(\lambda \mathbf{c}_1 + \lambda' \mathbf{c'}_1, \mathbf{c}_2, \dots, \mathbf{c}_n) = \lambda d(\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n) + \lambda' d(\mathbf{c'}_1, \mathbf{c}_2, \dots, \mathbf{c}_n)$$

e similmente per le altre colonne. Conseguentemente $d$ è una funzione "bilineare" di ciascuna coppia di colonne, ad esempio per la prima e la seconda colonna si ha

$$\begin{aligned} & d(\lambda \mathbf{c}_1 + \lambda' \mathbf{c'}_1, \mu \mathbf{c}_2 + \mu' \mathbf{c'}_2, \dots, \mathbf{c}_n) \\ = \;& \lambda\, d(\mathbf{c}_1, \mu \mathbf{c}_2 + \mu' \mathbf{c'}_2, \dots, \mathbf{c}_n) + \lambda'\, d(\mathbf{c'}_1, \mu \mathbf{c}_2 + \mu' \mathbf{c'}_2, \dots, \mathbf{c}_n) \\ = \;& \lambda\mu\, d(\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_n) + \lambda\mu'\, d(\mathbf{c}_1, \mathbf{c'}_2, \dots, \mathbf{c}_n) \\ + \;& \lambda'\mu\; d(\mathbf{c'}_1, \mathbf{c}_2, \dots, \mathbf{c}_n) + \lambda\mu'\, d(\mathbf{c}_1, \mathbf{c'}_2, \dots, \mathbf{c}_n), \end{aligned}$$

e, più in generale, è una funzione multilineare delle colonne.

Si dimostra che (cfr [4, vol I, cap 7]) esiste ed è unica la funzione che soddisfa gli assiomi D.1 ÷ D.3. Come di consuetudine, essa sarà denotata con $\det(M)$.

Riassumiamo nella proposizione seguente alcune proprietà dei determinanti, ben note quando $R$ è un campo e che continuano a valere quando $R$ è un anello arbitrario. Si ricorda che il complemento algebrico ("cofactor" nella letteratura anglosassone) di un elemento $m_{ij}$ di $M$ è dato da $(-1)^{i+j} \det M_{ij}$, dove $M_{ij}$ è la sottomatrice ottenuta da $M$ eliminandone la riga $i$-esima e la colonna $j$-esima, e che $\mathrm{adj}(M) = [\det M_{ij}]^T$ è la trasposta della matrice dei complementi algebrici di $M$.

**Proposizione 1.1.6** [Proprietà dei determinanti delle matrici su anelli] *Sia $R$ un anello. Il determinante delle matrici in $R^{n\times n}$ ha le seguenti proprietà:*

*D.4* *Se le colonne di $M$ sono permutate in qualsiasi modo,* $\det(M)$ *è moltiplicato per la segnatura*[3] *della permutazione corrispondente $\sigma$;*

*D.5* *se $M = [m_{i,j}]$, allora* $\det M$ *è espresso nella forma*

$$\det(M) = \sum_{\sigma} \mathrm{sgn}(\sigma) m_{\sigma(1),1} m_{\sigma(2),2} \dots m_{\sigma(n),n}, \tag{1.5}$$

*dove la somma è estesa a tutte le permutazioni $\sigma$ degli interi $1, 2, \dots, n$;*

[3] Con *segnatura di $\sigma$* si intende il numero +1 oppure –1 a seconda che sia pari o dispari il numero di scambi necessari per ottenere da $(1, 2, \dots, n)$ la $n$-pla $(\sigma(1), \sigma(2), \dots, \sigma(n))$.

*D.6* *il determinante di $M$ è moltiplicato per $\lambda \in R$ se tutti gli elementi di una colonna di $M$ sono moltiplicati per $\lambda$;*

*D.7* *il determinante di $M$ non cambia se ad una colonna si somma il multiplo di un'altra colonna;*

*D.8* $\det(M) = \det(M^T)$

*D.9* *se $M = [m_{ij}]$ è triangolare,* $\det M = m_{11}m_{22}\cdots m_{nn}$*;*

*D.10* *se $M, N \in R^{n\times n}$, allora* $\det(MN) = \det(M)\det(N)$*;*

*D.11* *se $M = [m_{ij}]$, il determinante di $M$ di può "sviluppare" secondo la riga $i$-esima della matrice, combinando linearmente gli elementi della riga $i$-esima con i corrispondenti complementi algebrici*

$$\det(M) = m_{i1}(-1)^{i+1}\det(M_{i1}) + m_{i2}(-1)^{i+2}\det(M_{i2}) + \ldots + m_{in}(-1)^{i+n}\det(M_{in})$$

*D.12* *se $i \neq j$, combinando linearmente gli elementi della riga $i$-esima con i complementi algebrici della riga $j$-esima si ottiene*

$$0 = m_{i1}(-1)^{j+1}\det(M_{j1}) + m_{i2}(-1)^{j+2}\det(M_{j2}) + \ldots + m_{in}(-1)^{j+n}\det(M_{jn});$$

*D.13* $\det(M)I_n = M\mathrm{adj}(M) = \mathrm{adj}(M)\,M$

Poiché D.14 vale per ogni matrice quadrata su un anello commutativo $R$, se $\det(M)$ è invertibile in $R$ si ha

$$M[\det(M)^{-1}\mathrm{adj}(M)] = [\det(M)^{-1}\mathrm{adj}(M)]M = I_n$$

e $M$ ha in $R^{n\times n}$ la matrice $\det(M)^{-1}\mathrm{adj}(M)$ come inversa.
Viceversa, se $M$ ha un'inversa $M^{-1} \in R^{n\times n}$ , allora $\det(M^{-1}) \in R$ e da $1 = \det(I_n) = \det(MM^{-1}) = \det(M)\det(M^{-1})$ segue che $\det(M)$ è un elemento invertibile di $R$, con $\det(M)^{-1} = \det(M^{-1})$. Abbiamo così provato la seguente

**Proposizione 1.1.7** [Invertibilità di una matrice a elementi in un anello] *Sia $M \in R^{n\times n}$ una matrice a elementi nell'anello $R$. Condizione necessaria e sufficiente affinché $M$ abbia un'inversa in $R^{n\times n}$ è che* $\det(M)$ *sia invertibile in $R$.*

Si noti che, quandi $R$ è un campo, la condizione enunciata equivale al fatto che sia $\det(M) \neq 0$, dal momento che ogni elemento non nullo di un campo è invertibile. Su un anello generico $\det(M) \neq 0$ **non** garantisce l'invertibilità di $M$.

## 1.2 Ideali e omomorfismi

**Definizione 1.2.1** [Sottoanello] *Un sottoinsieme $S$ di un anello $R$ è un sottoanello di $R$ se rispetto alle operazioni di $R$ è a sua volta un anello, ovvero se $1 \in S$ e la differenza e il prodotto di due elementi di $S$ appartengono ad $S$.*

**Esempio 1.2.1** (*i*) L'unico sottoanello di $\mathbb{Z}$ è $\mathbb{Z}$ stesso.

(*ii*) Un campo $\mathbb{F}$ è un sottoanello di $\mathbb{F}[z]$, l'anello dei polinomi su $\mathbb{F}$.

(*iii*) In $C[0,1]$ (cfr. Esempio 1.1.1) l'insieme $C^{(1)}[0,1]$ delle funzioni derivabili con derivata prima continua è un sottoanello.

Se $R_i,\ i \in \mathcal{I}$, formano una famiglia arbitraria di sottoanelli dell'anello $A$, è immediato constatare che è un sottoanello di $A$ l'intersezione

$$\bigcap_{i\in\mathcal{I}} R_i \tag{1.6}$$

Se $R$ è un sottoanello dell'anello $A$ ed $a_1, \ldots, \alpha_n$ sono elementi di $A$, indichiamo con $\{R_i,\ i \in \mathcal{I}\}$ la famiglia[4] dei sottoanelli di $A$ che contengono $R$ e gli elementi $\alpha_1, \ldots, \alpha_n$. L'intersezione (**??**) è allora il più piccolo sottoanello di $A$ che contiene sia $R$, sia $\alpha_1, \ldots, \alpha_n$, e sarà chiamata il **sottoanello di $A$ generato su $R$ da** $\alpha_1, \ldots, \alpha_n$. Di tale sottoanello si può dare una descrizione esplicita: è chiaro infatti che ad esso appartengono i prodotti del tipo $\alpha_1^{i_1} \ldots \alpha_n^{i_n},\ i_j \in \mathbb{N}$, quindi le somme finite

$$\sum_{i_1,\ldots,i_n\in\mathbb{N}} r_{i_i\ldots i_n}\alpha_1^{i_1}\ldots\alpha_n^{i_n}, \qquad r_{i_1\ldots i_n} \in R \tag{1.7}$$

Poiché l'insieme degli elementi (**??**) è un sottoanello di $A$ contenente $R$ ed $\alpha_1, \ldots, \alpha_n$, possiamo concludere che esso è il sottoanello cercato. È immediato che gli elementi (**??**) si ottengono formalmente "sostituendo" nell'anello dei polinomi $R[z_1, \ldots z_n]$ gli elementi $\alpha_1, \ldots, \alpha_n$ alle indeterminate $z_1, \ldots, z_n$. Quindi il sottoanello di $A$ generato su $R$ dagli elementi $\alpha_i \in A$ sarà denotato con $R[\alpha_1, \ldots, \alpha_n]$.

**Definizione 1.2.2** [IDEALE] *Sia $R$ un anello. Un sottoinsieme (non vuoto) $I$ di $R$ è un ideale di $R$ se*

($i_1$) *per ogni $a, b \in I,\ a + b \in I$ (chiusura rispetto all'addizione);*

($i_2$) *per ogni $a \in I$ ed $y \in R$, $ay$ appartiene a $I$ (proprietà di assorbimento).*

*Un ideale $I$ è proprio se non coincide con $R$, ed è nullo se $I = \{0\}$.*

**Esempio 1.2.2** (*i*) L'insieme dei numeri interi pari è un ideale di $\mathbb{Z}$. Infatti la somma di due numeri pari è pari ed il prodotto di un intero qualsiasi per un numero pari è pari. Più in generale, l'insieme dei multipli di un dato intero $m$ è un ideale di $\mathbb{Z}$. L'insieme dei numeri dispari, invece, non costituisce un ideale, giacché non è chiuso rispetto alla somma.

(*ii*) In $C[0,1]$ (cfr. Esempio 1.1.1) l'insieme $I_{x_0}$ delle funzioni che si annullano in $x_0 \in [0,1]$ è un ideale.

(*iii*) Sia $M \in \mathbb{R}^{n\times n}$. L'insieme dei polinomi annullatori di $M$, i.e. dei polinomi $\alpha_0+\alpha_1 z+\ldots+\alpha_k z^k$ tali che $\alpha_0 I_n + \alpha_1 M + \ldots + \alpha_k M^k = 0$ è un ideale di $\mathbb{R}[z]$.

- ESERCIZIO 1.2.1 (*i*) L'intersezione di due ideali di un anello $R$ è ancora un ideale di $R$.

  (*ii*) L'insieme delle funzioni di $C[0,1]$ che si annullano in almeno un punto dell'intervallo $[0,1]$ è un ideale?

  (*iii*) Un ideale è proprio se e solo se non contiene elementi invertibili di $R$.

  (*iv*) Sotto quali condizioni un ideale è un sottoanello?

  (*v*) Un anello $R$ è un campo se e solo se l'unico ideale proprio di $R$ è quello nullo.

[4] non vuota, perché contiene almeno $A$

**Definizione 1.2.3** [GENERATORI DI UN IDEALE] *Se $S$ è un sottoinsieme dell'anello $R$, l'***ideale generato da** *$S$ è l'insieme*

$$(S) := \left\{ \sum_{i=1}^{m} s_i r_i : m \in \mathbb{N}, s_i \in S, r_i \in R \right\}. \tag{1.8}$$

*$S$ è detto un "insieme di generatori" per l'ideale $(S)$. Un ideale $I$ di $R$ è*

- **finitamente generato** *se ammette un insieme finito di generatori o, equivalentemente, se esiste un sottoinsieme finito $S$ di $R$ tale che $I = (S)$;*
- **principale** *se ammette un unico generatore. Un anello (dominio) i cui ideali siano tutti principali viene detto anello (dominio) a ideali principali* [5].

**Esempio 1.2.3** L'anello degli interi $\mathbb{Z}$ è un dominio a ideali principali.
La prova ricalca quella svolta, in un contesto più generale, nel paragrafo 1.4 per dimostrare che ogni dominio euclideo è un PID. a) L'ideale nullo è principale. b) Ogni altro ideale $I$ di $\mathbb{Z}$ contiene elementi non nulli e quindi, per la proprietà di assorbimento, elementi positivi. Se $m$ è il più piccolo numero positivo di $I$, per le proprietà $(i_1)$ e $(i_2)$ della Definizione 1.2.2 l'ideale principale $(m)$ è contenuto in $I$. D'altra parte, applicando l'algoritmo di divisione, ogni elemento $n$ di $I$ si esprime come

$$n = qm + r, \quad 0 \leq r < m$$

e $r = n - qm$, poiché appartiene ad $I$, deve essere nullo: altrimenti esisterebbe in $I$ un elemento positivo minore di $m$. Pertanto ogni elemento di $I$ è multiplo di $m$, e $I \subseteq (m)$.

- ESERCIZIO 1.2.2 L'anello dei polinomi in una indeterminata $\mathbb{F}[z]$ sul campo $\mathbb{F}$ è un PID.
*(Suggerimento. La prova si basa sull'algoritmo euclideo di divisione fra polinomi).*

**Esempio 1.2.4** Il passaggio da una a più indeterminate fa perdere all'anello dei polinomi a coefficienti in un campo $\mathbb{F}$ la struttura di PID. Verifichiamo che l'anello $\mathbb{F}[z_1, z_2]$ dei polinomi in due indeterminate a coefficienti in $\mathbb{F}$ non è un PID.

Infatti, l'ideale $I = (z_1, z_2)$, generato dai polinomi $z_1$ e $z_2$, ovvero l'ideale dei i polinomi privi di termine noto, non è principale. Se lo fosse, esisterebbe un polinomio $p(z_1, z_2) \neq 0$ tale che tutti gli elementi di $I$, e in particolare $z_1$ e $z_2$, risultino multipli di $p(z_1, z_2)$. Ponendo

$$p(z_1, z_2) = \sum_h \pi_h(z_1) z_2^h,$$

si ha

$$z_1 = p(z_1, z_2) f(z_1, z_2) = (\sum_h \pi_h(z_1) z_2^h)(\sum_k \phi_k(z_1) z_2^k),$$

da cui segue che $p(z_1, z_2) = \pi_0(z_1)$ è un polinomio non nullo nella sola indeterminata $z_1$. Similmente, dalla relazione $z_2 = p(z_1, z_2)\, g(z_1, z_2)$ segue che $p(z_1, z_2)$ è un polinomio non nullo nella sola indeterminata $z_2$. Ma allora $p(z_1, z_2)$ dovrebbe essere una costante non nulla, e quindi non potrebbe appartenere ad $I$.

- ESERCIZIO 1.2.3 $(i)$ $\mathbb{F}[[z]]$ è un PID e i suoi ideali sono tutti e soli quelli del tipo $(z^k)$, $k \in \mathbb{N}$.
$(ii)$ Sia $D$ un PID, e introduciamo nel prodotto cartesiano $D \times D$ una struttura d'anello ponendo

$$\begin{aligned} (x_1, y_1) + (x_2, y_2) &:= (x_1 + x_2, y_1 + y_2) \\ (x_1, y_1)(x_2, y_2) &:= (x_1 x_2, y_1 y_2), \end{aligned}$$

$x_i, y_i \in D$, $i = 1, 2$. Si verifichi che $D \times D$ è un PID.

[5] Un dominio a ideali principali verrà indicato, per brevità, con l'acronimo (inglese) PID.

<< ∗ **Proposizione 1.2.4** [Catene di ideali in un PID] *Sia $D$ un PID. Una catena strettamente ascendente di ideali (principali!) in $D$*

$$(a_1) \underset{\neq}{\subset} (a_2) \underset{\neq}{\subset} \dots \underset{\neq}{\subset} (a_n) \underset{\neq}{\subset} \dots \tag{1.9}$$

*non può essere infinita.*

Dimostrazione Infatti l'unione insiemistica degli elementi della catena è ancora un ideale, quindi un ideale principale,

$$\cup_{i=1}^{\infty}(a_i) = (a),$$

il cui generatore appartiene necessariamente ad uno degli ideali di (**??**), per esempio ad $(a_n)$. Deve essere allora

$$(a_n) \subseteq (a) \subseteq (a_n)$$

e ciò implica che la catena si fermi ad $(a_n)$. ■

**Definizione 1.2.5** [Ideale massimale e ideale primo] *Sia $I$ un ideale proprio dell'anello $R$. $I$ è*

- *ideale* **massimale** *se per ogni ideale $J$ di $R$, $I \subseteq J$, si ha $J = I$ oppure $J = R$, ovvero $I$ non è contenuto propriamente in nessun ideale proprio di $R$;*
- *ideale* **primo** *se $ab \in I$ implica $a \in I$ o $b \in I$, per ogni $a, b \in R$.*

Si può dimostrare, ricorrendo all'assioma della scelta [3,8], che ogni anello contiene almeno un ideale massimale.

**Esempio 1.2.4** (*i*) Se $p$ è un numero primo, l'ideale $(p)$ in $\mathbb{Z}$ è primo e massimale.
(*ii*) Per ogni $x_0 \in [0,1]$ l'ideale $I_{x_0}$ di $C[0,1]$ è primo e massimale.
(*iii*) L'ideale generato in $\mathbb{F}[z_1, z_2]$ da $z_1$ è primo ma non massimale, in quanto contenuto propriamente nell'ideale (proprio) $(z_1, z_2)$.

- Esercizio 1.2.3 (*i*) In $\mathbb{Z}$ l'ideale (6) non è primo.
  (*ii*) In $\mathbb{F}[z]$, $\mathbb{F}$ un campo, l'insieme dei polinomi che si annullano in $z = 1$ è un ideale massimale.
- Esercizio 1.2.4 Un anello $R$ è un dominio se e solo se l'ideale nullo è primo.
- Esercizio 1.2.5 È vero che se $I$ è ideale massimale di $R$ e $a \notin I$, allora $a$ è invertibile?
- Esercizio 1.2.6 L'unico ideale massimale di $\mathbb{F}[[z]]$ è $(z)$.
- Esercizio 1.2.7 In $R$ l'ideale $I$ è massimale se e solo se nell'anello quoziente gli unici ideali sono $R/I$ e $\{0 + I\}$.

È naturale chiedersi quali relazioni sussistano, in generale, tra ideali massimali ed ideali primi. I precedenti esempi mettono in evidenza che un ideale primo non è necessariamente massimale; ciò, tuttavia, è vero nel caso di domini a ideali principali. Inoltre, gli ideali massimali sono sempre primi, come illustrato dalla seguente proposizione.

**Proposizione 1.2.6** *Sia $R$ un anello.* (*i*) *Ogni ideale massimale di $R$ è primo.*
(*ii*) *Se $R$ è un PID, ogni ideale primo* **non nullo** *è massimale.*

Dimostrazione (*i*) Sia $I$ massimale e sia $ab$ un elemento di $I$. Dimostriamo che $a \notin I$ implica $b \in I$. Se $a$ non appartiene ad $I$, l'ideale $J$, generato dagli elementi di $I$ e da $a$, contiene propriamente $I$ e quindi coincide con $R$. Pertanto risulta $i + ra = 1$, per un'opportuna scelta di $i \in I$ e $r \in R$. Ma allora $b = ib + r(ab)$, in quanto somma di elementi di $I$, sta a sua volta in $I$.

(*ii*) Sia $(a)$, $a \neq 0$, un ideale primo e supponiamo che $(b)$ sia un ideale che contiene propriamente $(a)$. Allora $a$ appartiene a $(b)$ e quindi $a = bc$, per qualche $c \in R$. Essendo $(a)$ ideale primo, almeno uno tra $b$ e $c$ appartiene ad $(a)$; $b$, però, non può appartenere ad $(a)$, altrimenti $(b)$ sarebbe contenuto in $(a)$, contro l'ipotesi. Quindi $c$ sta in $(a)$, ovvero $c = da$, e pertanto

$$a = bc = b(da) = (bd)a.$$

Dalla regola di cancellazione segue $1 = bd$, e quindi $(b) = (1) = R$. ■ >>

**Definizione 1.2.7** [Omomorfismo] *Siano $R$ e $S$ anelli e $\phi : R \to S$ una mappa. $\phi$ è un omomorfismo (di anelli) se valgono le seguenti condizioni:*
*(i)* $\phi(a+b) = \phi(a) + \phi(b)$ *per ogni* $a, b \in R$*;*
*(ii)* $\phi(ab) = \phi(a)\phi(b)$ *per ogni* $a, b \in R$*;*
*(iii)* $\phi(1_R) = 1_S$*, dove* $1_R$ *e* $1_S$ *sono rispettivamente l'unità di* $R$ *e di* $S$*.*

- Esercizio 1.2.8 [Nucleo e immagine] Se $\phi : R \to S$ è un omomorfismo d'anelli, allora
  *(i)* $\phi(0_R) = 0_S$ e $\phi(-r) = -\phi(r)$ per ogni $r \in R$;
  *(ii)* il *nucleo di* $\phi$
  $$\ker\phi := \{r \in R : \phi(r) = 0\}$$
  è un ideale di $R$, ed è l'ideale nullo se e solo se $\phi$ è iniettivo;
  *(iii)* l'*immagine di* $\phi$
  $$\mathrm{im}\phi := \{s \in S : s = \phi(r), \exists r \in R\}$$
  è un sottoanello di $S$.

Se $R$ è un anello e $I$ è un ideale proprio di $R$, possiamo definire in $R$ una relazione di equivalenza $\equiv$ ponendo, per ogni coppia di elementi $r$ ed $s$ in $R$

$$r \equiv s \Leftrightarrow r - s \in I$$

Si lascia come esercizio verificare che la relazione introdotta è riflessiva, simmetrica e transitiva e che la classe di equivalenza che contiene l'elemento $r$ e' data dall'insieme

$$r + I := \{v : v = r + i,\ i \in I\}$$

L'insieme delle classi di equivalenza può essere dotato a sua volta di struttura di anello definendovi le operazioni di somma e prodotto come segue:

$$(a+I) + (b+I) = (a+b) + I; \qquad (a+I) \cdot (b+I) = (a \cdot b) + I$$

Le operazioni sono ben definite (nel senso che il risultato non dipende dal particolare rappresentante scelto a designare una classe), la classe nulla è $0 + I$ e l'unità è $1 + I$. L'anello così ottenuto si dice *anello quoziente* e si indica col simbolo $R/I$.

- Esercizio 1.2.9* [Anelli quoziente, campi e domini] Sia $I$ un ideale proprio di $R$. Allora
  *(i)* $R/I$ è un campo se e solo se $I$ è ideale massimale;
  *(ii)* $R/I$ è un dominio se e solo se $I$ è ideale primo.
  *Suggerimento: Per (i), si vedano gli esercizi 1.2.1(v) e 1.2.7. Per (ii) se $I$ è primo e $(a+I)(b+I) = ab+I = 0$ allora $ab \in I$, quindi $a$ o $b$ appartiene ad $I$, quindi nell'anello quoziente $a+I$ oppure $b+I$ è l'elemento nullo; viceversa, se $R/I$ è un dominio e $ab \in I$, da $ab = 0$ segue $0 = ab+I = (a+I)(b+I)$, quindi $a + I = 0$ o $b + I = 0$, quindi $a \in I$ o $b \in I$.*

## 1.3 Cenni alla fattorizzazione nei domini di integrità

In questo paragrafo discuteremo brevemente alcuni concetti connessi con la struttura moltiplicativa di un dominio $D$: l'esistenza di divisori non banali di un elemento, i divisori comuni di due elementi, la fattorizzazione di un elemento in fattori non ulteriormente "fattorizzabili". L'obiettivo che ci proponiamo è duplice: vogliamo anzitutto definire alcuni

termini (irriducibile, primo, massimo comune divisore etc.) che utilizzeremo costantemente nel seguito, ma intendiamo anche accennare a come varie nozioni, note per lo più dall'algebra degli interi o dei polinomi in una indeterminata, e in quegli ambienti dotate di connessioni e proprietà familiari per lunga consuetudine di studio, richiedano invece una discussione approfondita quando ci si ponga in un ambiente più generale.
Per la comprensione del seguito di queste dispense, se si eccettua il capitolo sui sistemi multidimensionali per i quali ricorreremo ad anelli di polinomi in più indeterminate, è sufficiente concentrarsi sulle proprietà della fattorizzazione nei domini a ideali principali.

**Definizione 1.3.1** [Divisori e associati] *Se $a$ e $b$ sono elementi del dominio $D$, diciamo che un elemento non nullo $a$ "divide" $b$ ($a$ è "un divisore di" $b$ o $b$ è "un multiplo di" $a$) e scriviamo $a|b$, se esiste $c \in R$ tale che $b = ac$.*
*Se $c$ è un elemento invertibile di $D$, allora $a$ e $b$ sono detti* **associati** *e si ha anche $b|a$.*

Si noti che, se $a|b$ e $b|a$ allora $a = bc$, $b = ac'$ e

$$a(1 - cc') = 0.$$

Poiché $D$ è un dominio, si può applicare la legge di cancellazione, ottenendo $1 = cc'$. Si conclude che due elementi non nulli $a$ e $b$ sono associati se e solo se $a|b$ e $b|a$.

**Definizione 1.3.2** [Elementi irriducibili e elementi primi] *In un dominio $D$, un elemento $a$ non invertibile e non nullo è detto*
*($i$)* **irriducibile** *se quando fattorizza nella forma $a = bc$, $b, c \in D$, allora uno dei fattori $b$ e $c$ è un elemento invertibile;*
*($ii$)* **primo** *se quando divide un prodotto, ovvero $a|bc$, $b, c \in D$, allora divide uno almeno dei fattori, ossia $a|b$ oppure $a|c$.*

Si noti che la definizione di irriducibilità può essere data, in modo equivalente, dicendo che $a = bc$ implica che uno tra $b$ e $c$ è associato ad $a$.

**Definizione 1.3.3** [Massimo comun divisore] *Se $a$ e $b$ sono elementi, non entrambi nulli, di un dominio $D$, un elemento $d \in D$ è massimo comun divisore di $a$ e $b$ ($d = \mathrm{MCD}(a, b)$) se*
*($i$) $d|a$ e $d|b$, ovvero $d$ è un divisore comune di $a$ e $b$,*
*($ii$) per ogni altro divisore comune $d'$ di $a$ e $b$ si ha $d'|d$.*
*$a$ e $b$ sono detti* **coprimi** *(o relativamente primi) se 1 è un loro massimo comun divisore.*

- Esercizio 1.3.1 Si provi che in ogni dominio
  (i) esiste il MCD di una coppia in cui un elemento sia nullo oppure invertibile;
  (ii) se $d$ e $d'$ sono due MCD della coppia non nulla $(a, b)$ allora $d$ e $d'$ sono associati. (*Suggerimento: $d|d'$ e $d'|d$*)

**Definizione 1.3.4** [Dominio a fattorizzazione unica] *Un dominio $D$ è detto a fattorizzazione unica (per brevità UFD) o dominio fattoriale se valgono simultaneamente le seguenti condizioni:*

*(i) ogni elemento non nullo e non invertibile $a \in D$ può essere espresso come prodotto di elementi irriducibili*

$$a = p_1 p_2 \cdots p_k$$

*(ii) la precedente fattorizzazione è essenzialmente unica, nel senso che, per ogni altra fattorizzazione in elementi irriducibili*

$$a = p'_1 p'_2 \cdots p'_h,$$

*abbiamo $h = k$ e, eventualmente dopo una permutazione dei pedici dei $p'_i$,*

$$p'_i = u_i p_i, \ i = 1, 2, \ldots k$$

*con $u_i$ elementi invertibili di $D$.*

La seguente proposizione fornisce un quadro sufficientemente indicativo delle interconnessioni fra le nozioni che abbiamo introdotto. In particolare, essa mostra come siano collegate fra loro proprietà quali l'esistenza di una fattorizzazione unica di ogni elemento, l'esistenza del massimo comun divisore di ogni coppia, la prinipalità di ogni ideale, l'equivalenza fra primalità e irriducibilità.

**Proposizione 1.3.5** *Sia $D$ un dominio. Valgono allora i seguenti fatti:*

*(i) ogni elemento primo è anche irriducibile;*

*(ii) se ogni coppia non nulla di elementi ammette MCD, allora ogni elemento irriducibile è anche primo;*

*(iii) se $D$ è a fattorizzazione unica allora ogni coppia non nulla di elementi ammette MCD;*

*(iv) se $D$ è un PID, allora $D$ è a fattorizzazione unica.*

Dimostrazione (i) Supponiamo che $a \in D$ sia un elemento primo, e sia $a = bc$ una sua fattorizzazione, $b$ e $c$ elementi di $D$. Da $a = bc$ segue $a|bc$ e quindi $a$ divide almeno uno tra $b$ e $c$, ad esempio $a|b$. Allora $b = ad$, per qualche $d \in D$, e si ha $a = bc = a(dc)$, da cui $1 = dc$. Quindi $c$ è invertibile e $a$ irriducibile.

$<<$ $*(ii)$ Supponiamo che in $D$ ogni coppia non nulla ammetta MCD e che $d$ sia irriducibile. Per verificare che $d$ è primo, proviamo che se $d \not| a$, $d \not| b$, con $a, b$ elementi non nulli, allora $d \not| ab$. Infatti, posto $m := \mathrm{MCD}(a, d)$, si ha $d = mx$ e se $m$ non fosse invertibile, dovrebbe esserlo $x$ (per l'irriducibilità di $d$) e $a = my = dx^{-1}y$ avrebbe $d$ come divisore. Possiamo quindi supporre, ripetendo il medesimo ragionamento anche sulla coppia $(b, d)$,

$$\mathrm{MCD}(a, d) = \mathrm{MCD}(b, d) = 1.$$

Per concludere, basterà provare che

$$\mathrm{MCD}(ab, d) = 1, \tag{1.10}$$

perché allora $d|ab$ è incompatibile con (**??**). Ma (**??**) segue a sua volta dalle relazioni generali

$$\mathrm{MCD}\Big(\mathrm{MCD}(x, y), z\Big) = \mathrm{MCD}\Big(x, \mathrm{MCD}(y, z)\Big)$$

$$z\mathrm{MCD}(x, y) = \mathrm{MCD}(zx, zy)$$

e da

$$1 = \mathrm{MCD}(d, a) = \mathrm{MCD}\Big(d, \mathrm{MCD}(ad, ab)\Big) = \mathrm{MCD}\Big(\mathrm{MCD}(d, ad), ab\Big) = \mathrm{MCD}(d, ad).$$

(iii) Per l'Esercizio 1.3.1 possiamo limitarci a verificare l'esistenza del MCD per ogni coppia $a, b$ in cui entrambi gli elementi siano non nulli e non invertibili.

Consideriamo una fattorizzazione di $a$ nel prodotto di elementi irriducibili e in tale rappresentazione sostituiamo i fattori irriducibili associati con un singolo rappresentante moltiplicato per elementi invertibili di $D$. Otteniamo così una fattorizzazione

$$a = up_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}, \tag{1.11}$$

in cui $u \in D$ è invertibile, $p_i \in D$ sono irriducibili, non associati tra di loro, e gli $e_i \in \mathbb{N}$ sono interi positivi. È chiaro che i fattori di $a$ sono tutti e soli gli elementi di $D$ della forma $u' p_1^{e'_1} p_2^{e'_2} \cdots p_r^{e'_r}$ con $u'$ invertibile in $D$ e con $0 \leq e'_i \leq e_i$. È anche facile vedere che $a$ e $b$ possono essere espressi mediante i medesimi elementi irriducibili non associati, nella forma

$$a = up_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}, \qquad b = vp_1^{f_1} p_2^{f_2} \cdots p_s^{f_s} \tag{1.12}$$

con $u, v \in D$ elementi invertibili, pur di consentire a $e_i$ e a $f_i$ di assumere valori non negativi (e non solo positivi come in (**??**)). Consideriamo ora l'elemento

$$d = p_1^{g_1} p_2^{g_2} \cdots p_s^{g_s}, \quad g_i = \min\{e_i, f_i\},\ i = 1, 2, \ldots, s \tag{1.13}$$

e verifichiamo che esso è un MCD di $a$ e $b$. Chiaramente $d|a$ e $d|b$. Inoltre, ogni divisore comune di $a$ e di $b$, dovendo avere la struttura $d' = wp_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}$ con $w$ invertibile e $h_i \leq g_i,\ i = 1, 2, \ldots, s$, soddisfa $d'|d$. Pertanto la parte (iii) è provata.

(iv) Dimostriamo anzitutto che ogni elemento non nullo del dominio a ideali principali $D$ ammette una fattorizzazione in elementi irriducibili. Indichiamo con $\mathcal{S}$ l'insieme degli elementi $\neq 0$ di $D$ che non ammettono una fattorizzazione in elementi irriducibili e supponiamo che esso non sia vuoto. Allora esiste in $\mathcal{S}$ almeno un elemento $\bar{a}$ tale che nessun altro ideale $(a)$ sia generato da un elemento di $a \in \mathcal{S}$ e contenga propriamente $(\bar{a})$. Altrimenti, potemmo costruire una catena infinita strettamente ascendente di ideali principali generati da elementi $a_i \in \mathcal{S}$

$$(a_1) \underset{\neq}{\subset} (a_2) \underset{\neq}{\subset} \ldots \underset{\neq}{\subset} (a_n) \underset{\neq}{\subset} \ldots \tag{1.14}$$

e ciò contraddice la Proposizione 1.2.4.
Notiamo che $\bar{a} \in \mathcal{S}$ non può essere irriducibile, (altrimenti avrebbe una fattorizzazione, quella banale, in elementi irriducubili). Quindi può essere espresso nella forma $\bar{a} = bc$, con $b$ e $c$ non invertibili. Ma allora

$$(b) \supset (\bar{a}), \quad (c) \supset (\bar{a})$$

implica che $b$ e $c$ ammettono entrambi fattorizzazioni in fattori irriducibili , e il prodotto di tali fattorizzazioni è una fattorizzazione di $\bar{a}$, il che è manifestamente assurdo.

Per provare l'unicità della fattorizzazione, verifichiamo anzitutto che in un PID ogni elemento irriducibile $a$ è primo (e quindi, per il punto (i), in un PID irriducibili e primi coincidono). Infatti, supponiamo che $a|bc$ e $a \not| b$. L'ideale $(a, b)$ è generato da un elemento $u$, quindi $a = ux$, $b = uy$ e $x$ non può essere invertibile, altrimenti $b = uy = ax^{-1}y$ implicherebbe $a|b$. Poiché $a$ è irriducibile, $a = ux$ non è una fattorizzazione propria e $u$ è invertibile in $D$. Allora si ha

$$1 = ha + kb$$

per opportuni $h$ e $k$ in $D$, e $c = (hc)a + k(bc) = (hc)a + k(ta)$. Quindi $a|c$.
Supponiamo ora che $d \in D$ abbia due fattorizzazioni in elementi irriducibili:

$$d = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s \tag{1.15}$$

Poichè l'elemento $p_1$ è primo e divide il prodotto $q_1 q_2 \ldots q_s$, esso deve dividerne uno dei fattori, ad esempio (eventualmente renumerandoli) $q_1$. Esiste allora un invertibile $u$ per cui risulta $q_1 = up_1$ e quindi, cancellando il fattore $p_1$ in (**??**), $p_2 \ldots p_r = uq_2 \ldots q_s$. Si conclude ragionando per induzione sul numero dei fattori irriducibili. $* >>$ ■

Si può verificare l'esistenza di

- domini a fattorizzazione unica che non sono a ideali principali (basta pensare a $\mathbb{F}[z_1, z_2]$),

- domini in cui ogni coppia non nulla ammette un MCD ma che non sono a fattorizzazione unica,
- domini in cui ogni elemento irriducibile è primo ma non tutte le coppie non nulle di elementi ammettono MCD,
- domini in cui ci sono elementi irriducibili che non sono primi.

La figura 1.3.1 illustra le inclusioni (proprie) fra le varie strutture. Per una dimostrazione, si veda p.es. [1, vol.I, cap IV]

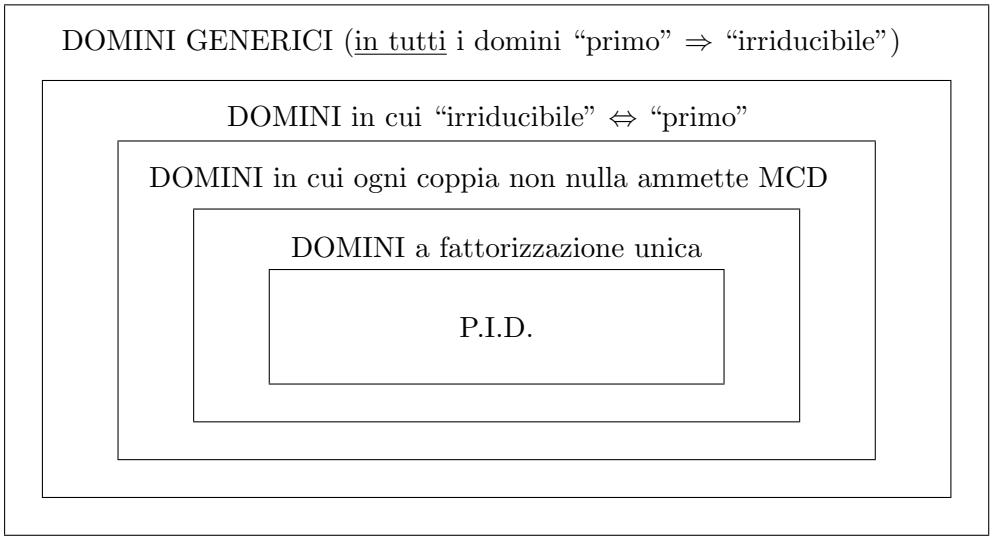


Figura 1.3.1

**Esempio 1.3.1*** [IRRIDUCIBLE $\not\Rightarrow$ PRIMO] Sia $D \subset \mathbb{C}$ l'insieme dei numeri complessi del tipo $a + ib\sqrt{5}$, dove $i$ è l'unità immaginaria e $a, b$ sono interi arbitrari. E' facile verificare che $D$ è un sottoanello di $\mathbb{C}$, quidi un dominio. Per studiarne le proprietà di fattorizzazione, introduciamo la funzione "norma"

$$N : D \to \mathbb{N} : a + ib\sqrt{5} \mapsto a^2 + 5b^2.$$

La norma è moltiplicativa: $N(rs) = N(r)N(s)$, e i suoi valori sono positivi per ogni elemento non nullo di $D$.

i) Gli elementi invertibili di $D$ sono tutti e soli quelli per cui $N$ vale 1 (quindi $+1$ e $-1$). Infatti $rs = 1$ implica $N(r)N(s) = N(1) = 1$, quindi $N(r) = N(s) = 1$. Viceversa, se $r = a + ib\sqrt{5}$ ha norma unitaria, dev'essere $a = \pm 1$ e $b = 0$. e quindi $r$ è invertibile in $D$. Perciò i soli associati di un elemento sono l'elemento stesso e il suo opposto.

ii) L'elemento $3 + 0i\sqrt{5}$ è irriducibile, ma non primo. Infatti, supponiamo sia $3 = rs$, $r, s \in D$. Allora $N(r)N(s) = 9$ implica $N(r) = 1, 3$ o $9$. Ma $N(r) = 3$ è impossibile perché nessun elemento di $D$ ha norma 3, mentre $N(r) = 9$ implica $N(s) = 1$ e $N(s) = 9$ implica $N(r) = 1$. Poiché la sua fattorizzazione in ogni caso non è propria, 3 è irriducibile. D'altra parte, abbiamo

$$3 | (2 + i\sqrt{5})(2 - i\sqrt{5}) = 9,$$

ma

$$3 \not| (2 + i\sqrt{5}) \text{ e } 3 \not| (2 - i\sqrt{5})$$

perché sia $(2 + i\sqrt{5}) = (a + ib\sqrt{5})3$, sia $(2 - i\sqrt{5}) = (a + ib\sqrt{5})3$ sono impossibili per valori interi di $a$ e $b$. Quindi 3 non é primo.

- ESERCIZIO 1.3.2* [COPPIE DI ELEMENTI PRIVE DI MCD] Si consideri il dominio $D$ dell'Esempio 1.3.1 e si ponga $a = -15 + i6\sqrt{5}$, $b = 9$.
  ($i$) si verifichi che in $D$ non esistono elementi a norma 3 o 27 e quindi ogni fattore comune $d$ di $a$ e $b$ deve avere norma $N(d)$ eguale a uno dei numeri 1,9,81.
  ($ii$) ricordando che elementi di egual norma differiscono per un fattore invertibile, si provi che gli unici divisori di $b$ con norma 81 sono $\pm 9$ e che di conseguenza $a$ e $b$ non hanno fattori comuni a norma 81.
  ($iii$) si verifichi che $r = 3$ e $s = 2 + i\sqrt{5}$ sono entrambi divisori comuni di $a$ e $b$, a norma 9
  ($iv$) se $d$ fosse un MCD di $a$ e $b$, dovrebbero valere sia $r|d$ che $s|d$. Ma da $N(r) = N(s) = N(d) = 9$ seguirebbe che $r$ ed $s$ differiscono entrambi da $d$, e quindi l'uno dall'altro, per un fattore invertibile di $D$. Perciò si avrebbe $r = \pm s$, che è manifestamente falsa. Conclusione: $a$ e $b$ non hanno MCD.

La seguente proposizione pone in relazione l'ideale generato da una coppia di elementi $a$ e $b$ e l'ideale generato dal loro eventuale MCD.

**Proposizione 1.3.6** [COPRIMALITÀ E ZERO-COPRIMALITÀ] *Sia $D$ un dominio in cui ogni coppia non nulla ammette MCD e siano $a, b, d$ elementi di $D$.*
*(i) l'ideale generato da $a$ e $b$ e quello generato da $d$ coincidono se e solo se $d$ è esprimibile come combinazione lineare su $D$ degli elementi $a$ e $b$ e se $d = \mathrm{MCD}(a, b)$:*

$$(d) = (a, b) \quad \Leftrightarrow \quad \begin{cases} d \in (a, b) \\ d = \mathrm{MCD}(a, b) \end{cases} \quad \Leftrightarrow \quad \begin{cases} d = xa + yb, \ \exists\, x, y \in D \\ d = \mathrm{MCD}(a, b) \end{cases} \tag{1.16}$$

*(ii) la condizione di* **zero coprimalità** *di $a, b$, ossia $(1) = (a, b)$ equivale all'esistenza di $x, y \in D$ per i quali vale l'identità di Bézout $1 = xa + yb$ :*

$$(1) = (a, b) \quad \Leftrightarrow \quad 1 = xa + yb \quad \text{per opportuni } x, y \in D \tag{1.17}$$

*(iii) la condizione di zero coprimalità implica, ma in generale non è implicata da, la condizione di* **coprimalità** *(talvolta , in inglese, "factor coprimeness") di $a, b$*

$$(1) = (a, b) \quad \begin{matrix} \Rightarrow \\ \not\Leftarrow \end{matrix} \quad 1 = \mathrm{MCD}(a, b) \tag{1.18}$$

*($iv$) se $d = \mathrm{MCD}(a, b)$ e se $a = \bar{a}d$, $b = \bar{b}d$, allora*

$$1 = \mathrm{MCD}(\bar{a}, \bar{b});$$

*($v$) se $p$ è irriducibile e $p \not| a$, allora*

$$1 = \mathrm{MCD}(a, p).$$

DIMOSTRAZIONE È chiaro che $d \in (a, b)$ equivale dire che $d$ è esprimibile nella forma $xa + yb$ per opportuni $x, y \in D$.
(i) Se vale $(d) = (a, b)$, allora $d \in (a, b)$, e da $a \in (d)$, $b \in (d)$ segue che $a$ e $b$ sono entrambi multipli di $d$, ovvero che $d$ è un loro divisore comune.
Inoltre, se $d'$ è un divisore comune di $a$ e $b$, allora

$$a = d'x' \text{ e } b = d'y' \Rightarrow (a, b) \subseteq (d') \ \Rightarrow \ (d) \subseteq (d') \ \Rightarrow \ d = rd',$$

quindi $d'|d$ e $d$ è un MCD di $a$ e $b$.
Viceversa, se $d = \mathrm{MCD}(a,b)$ e $d \in (a,b)$, dalla prima condizione segue $d|a$, $d|b$ e quindi $(a,b) \subseteq (d)$, mentre dalla seconda segue $(d) \subseteq (a,b)$.

(ii) $1 = xa + yb$ implica $1 \in (a,b)$, quindi $(1) \subseteq (a,b)$. D'altra parte, è certamente vero che $(1) = D \supseteq (a,b)$.

(iii) l'implicazione asserita si ottiene da (i) ponendo $d = 1$. Un controesempio che disprova l'implicazione opposta è fornito nell'Esercizio 1.3.5.

$<< *$ Per (iv), si noti che, se $d'$ è un divisore di $\bar{a}$ e di $\bar{b}$, allora $\bar{a} = d'\tilde{a}$ e $\bar{b} = d'\tilde{b}$ implica $a = dd'\tilde{a}$ e $b = dd'\tilde{b}$ e $dd'$, in quanto divisore comune di $a$ e di $b$, divide $d = \mathrm{MCD}(a,b)$. Quindi per qualche $x \in D$ si ha $dd'x = d$, ovvero $d(1 - d'x) = 0$ ed essendo $d \neq 0$ si ha che $d'$ e' invertibile in $D$. Quindi i divisori comuni di $\bar{a}$ e $\bar{b}$ sono tutti invertibili e 1 è un MCD.

Per (v), sia $d$ un divisore comune di $a$ e $p$. Allora $a = \bar{a}d$ e $p = \bar{p}d$ e se $d$ non fosse inveribile lo sarebbe $\bar{p}$, per definizione di irriducibilità. Ciò implicherebbe $d = p\bar{p}^{-1}$ e quindi $a = \bar{a}\bar{p}^{-1}p$ avrebbe $p$ come fattore, contro l'ipotesi $p \not| a$. Si conclude che tutti i divisori comuni di $a$ e $p$ sono invertibili in $D$. $* >>$ ■

- Esercizio 1.3.3* Si dimostri che
  (i) $d = \mathrm{MCD}(a,b)$ se e solo se $(d) \supseteq (a,b)$ e se $(d') \supseteq (a,b)$ implica $(d') \supseteq (d)$. Quindi $d$ è un MCD di $a$ e $b$ se l'insieme degli ideali principali contenenti $(a,b)$ ha un minimo $(d)$ rispetto all'ordine indotto dall'inclusione, ovvero se
  $$\bigcap_{(d')\supseteq(a,b)} (d') = (d) \supseteq (a,b)$$
  (ii) $a$ e $b$ sono coprimi se l'unico ideale principale che contiene $(a,b)$ è $(1)$
  (iii) nell'esercizio 1.3.2 ciascuno degli ideali principali $(r) = (3)$ e $(s) = (2 + i\sqrt{5})$ contiene l'ideale $(a,b) = (-15 + i6\sqrt{5}, 9)$. Ma $(r) \cap (s) \not\supseteq (a,b)$, infatti $9 \notin (r) \cap (s)$.

Nei domini a ideali principali la situazione descritta nella precedente Proposizione si semplifica alquanto:

**Corollario 1.3.7** [Coprimalità e MCD nei PID] *Se $D$ è un PID, allora*
*(i) Il MCD di due elementi $a$ e $b$ non entrambi nulli è il generatore dell'ideale principale generato da $a$ e $b$:*
$$d = \mathrm{MCD}(a,b) \quad \Leftrightarrow \quad (d) = (a,b); \tag{1.19}$$
*(ii) se $d$ è il MCD di due elementi non nulli $a, b$, ammette soluzione l'equazione diofantea $xa + yb = d$:*
$$d = \mathrm{MCD}(a,b) \quad \Rightarrow \quad xa + yb = d \text{ per opportuni } x, y \in D \tag{1.20}$$
*(iii) coprimalità e zero-coprimalità sono equivalenti.*

Dimostrazione (i) Della (**??**) basta provare l'implicazione $d = \mathrm{MCD}(a,b) \Rightarrow (d) = (a,b)$. Dal momento che $D$ è un PID, esiste un elemento $d'$ per cui risulta $(d') = (a,b)$. Per la Proposizione 1.3.6.(i), $d'$ è un $\mathrm{MCD}(a,b)$. Ma due MCD $d$ e $d'$ della medesima coppia di elementi differiscono per un fattore invertibile, quindi $(d) = (d')$.
(ii) $d = \mathrm{MCD}(a,b)$ implica, per il punto precedente, $(d) = (a,b)$ che a sua volta implica, per il punto (i) della Proposizione 1.3.6, l'esistenza di $x$ e $y$ in $D$ che risolvono l'equazione
$$xa + yb = d$$

.
(iii) Se $a$ e $b$ sono coprimi, ossia $\mathrm{MCD}(a,b)=1$, per il punto (i) si ha $(a,b)=(1)$, quindi appunto la zero coprimalità di $a$ e $b$. ■

- ESERCIZIO 1.3.4 In un dominio $D$ a ideali principali risulta $\mathrm{MCD}(a_1,a_2,\ldots,a_n)=1$ se e solo se l'equazione $a_1x_1+a_2x_2+\ldots+a_nx_n=1$ nelle incognite $x_1,x_2,\ldots,x_n$ ammette soluzione in $D$.

- ESERCIZIO 1.3.5 [COPRIMALITÀ $\not\Rightarrow$ ZERO-COPRIMALITÀ] Si verifichi che in $\mathbb{F}[z_1,z_2]$ il MCD dei polinomi $a(z_1,z_2)=z_1$ e $b(z_1,z_2)=z_2$ è 1, ma l'equazione $xa+yb=1$ non è risolubile per nessuna coppia di polinomi $(x(z_1,z_2),y(z_1,z_2))$.

**Definizione 1.3.8** [MINIMO COMUNE MULTIPLO] *Sia $D$ un dominio e siano $a$ e $b$ due suoi elementi. $c\in D$ è un minimo comune multiplo (mcm) di $a$ e $b$ se*
*(i) $a|c$ e $b|c$, ovvero $c$ è un multiplo comune di $a$ e $b$,*
*(ii) per ogni altro multiplo comune $c'$ di $a$ e $b$ si ha $c|c'$.*

- ESERCIZIO 1.3.6 Sia $D$ un dominio in cui ogni coppia non nulla ammette MCD e siano $a$ e $b$ due suoi elementi. Allora
  (i) esiste $\mathrm{mcm}(a,b)$;
  (ii) $\mathrm{mcm}\ (a,b)=a'b$, dove $a'\mathrm{MCD}(a,b)=a$;
  (iii) se $a$ e $b$ sono coprimi allora $\mathrm{mcm}(a,b)=ab$ e $(ab)=(a)\cap(b)$.

## 1.4 Domini euclidei

**Definizione 1.4.1** [DOMINIO EUCLIDEO] *Un dominio $D$ è detto "euclideo" se in esso è definita una funzione* **grado**

$$\delta : D\setminus\{0\}\to\mathbb{N} \tag{1.21}$$

*che soddisfa le seguenti proprietà:*
*(i) se $a\mid b$, $a,b\neq 0$, allora $\delta(b)\leq\delta(a)$;*
*(ii) per ogni $a$ e $b$ in $D$, $b\neq 0$, esiste $q\in D$ tale che l'elemento $r:=a-bq$ è zero oppure ha grado $\delta(r)<\delta(b)$.*

In generale, gli elementi $q$ ed $r$, noti come **quoziente** e **resto** della divisione di $a$ per $b$, non sono univocamente determinati dalle condizioni sulla funzione grado contenute negli assiomi $(i)$ e $(ii)$.

- ESERCIZIO 1.4.1 Siano $a$ e $b$ elementi di un dominio euclideo $D$. Si dimostri che
  (i) $a\neq 0$ implica $\delta(1)\leq\delta(a)$;
  (ii) se $a$ e $b$ sono associati, $\delta(a)=\delta(b)$. In particolare, $\delta(a)=\delta(-a)$ per ogni $a\in D$;
  (iii) se $b\neq 0$, $a\in(b)$ se e solo se 0 è un resto della divisione di $a$ per $b$.

  **Esempio 1.4.1** (i) Gli interi sono un dominio euclideo rispetto alla funzione $\delta(n)=|n|$. Quoziente e resto sono univocamente determinati?

  (ii) L'anello $\mathbb{F}[z]$ dei polinomi in una sola indeterminata a coefficienti nel campo $\mathbb{F}$ è un dominio euclideo rispetto alla funzione $\delta(p(z))=\deg p$, in cui $\deg p$ è, come di consueto, il massimo esponente di $z$ nei monomi non nulli di $p(z)$.

**Esempio 1.4.2** [Polinomi di Laurent] L'anello $\mathbb{F}[z, z^{-1}]$ dei *polinomi di Laurent* nell'indeterminata $z$, ovvero il sottoanello delle serie formali a supporto compatto con le operazioni definite come in (1.1) e (1.2), è un dominio euclideo rispetto alla funzione grado definita per un polinomio non nullo $p(z, z^{-1}) = \sum_{i=m}^{M} p_i z^i$, $p_m, p_M \neq 0$, come

$$\delta(p(z, z^{-1})) := M - m. \tag{1.22}$$

In questo caso, però, quoziente e resto della divisione non sono univocamente determinati.

**Proposizione 1.4.2** *Ogni dominio euclideo $D$ è un PID.*

Dimostrazione Sia $I$ un ideale di $D$. Se $I = \{0\}$, ovviamente $I$ è principale. Se $I$ non è l'ideale nullo, chiamiamo $m$ l'elemento minimo dell'insieme $\Delta := \{\delta(a) : a \in I, a \neq 0\} \subseteq \mathbb{N}$, e $a_m$ un elemento di $I$ tale che $\delta(a_m) = m$. Vogliamo provare che $I = (a_m)$.
Poichè $(a_m) \subseteq I$, è sufficiente verificare che ogni $a \in I$ è un multiplo di $a_m$. Dal momento che $D$ è un dominio euclideo, esistono $r$ e $q$ tali che $a - qa_m = r$, e se $r$ è diverso da zero vale $\delta(r) < \delta(a_m)$. Ma quest'ultima possibilità va esclusa, dal momento che $r$ sarebbe un elemento non nullo di $I$ con grado minore di $m$. Pertanto vale $a = qa_m$. ■

Va sottolineato che il risultato della precedente proposizione non si inverte, nel senso che esistono PID sui quali non è definibile una funzione grado che li renda euclidei [7].

**Definizione 1.4.3** [Dominio euclideo proprio] *Un dominio euclideo si dice proprio se non è un campo e per ogni $a$ e $b$ non nulli si ha*

$$\delta(ab) = \delta(a) + \delta(b). \tag{1.23}$$

- Esercizio 1.4.2 (*i*) Si verifichi che $\mathbb{F}[z]$ e $\mathbb{F}[z, z^{-1}]$ sono domini euclidei propri rispetto alle funzioni grado considerate nell'Esempio 1.4.1.
  (*ii*) Si verifichi che rispetto alla funzione grado $\delta(n) = |n|$, $\mathbb{Z}$ non è un dominio euclideo proprio.
  (*iii*) Si verifichi che in un dominio $D$ la (i) della definizione 1.4.1 è implicata da (**??**). Quindi un dominio è euclideo proprio se vi valgono (**??**) e la condizione (ii) della definizione 1.4.1.

In un dominio euclideo proprio non è garantita l'unicità di quoziente e resto nella divisione, come si verifica considerando, ad esempio, l'anello dei polinomi di Laurent (che è un dominio euclideo proprio rispetto alla funzione grado (**??**)). La seguente proposizione fornisce una condizione per l'unicità di quoziente e resto.

**Proposizione 1.4.4** [Unicità di quoziente e resto] *Se $D$ è un dominio euclideo, sono equivalenti i seguenti fatti:*
*(i) per ogni $a, b \in D$, entrambi non nulli e tali che $a + b \neq 0$*

$$\delta(a + b) \leq \max\{\delta(a), \delta(b)\}, \tag{1.24}$$

*(ii) per ogni $a, b \in D$, $b \neq 0$ esiste un'unica coppia $(q, r) \in D \times D$ con $r = 0$ oppure $\delta(r) < \delta(b)$ tale che*

$$a = qb + r. \tag{1.25}$$

DIMOSTRAZIONE Supponiamo valga la (**??**) Poiché $D$ è un dominio euclideo, esiste una coppia $(q, r)$ che soddisfa la (**??**) e il vincolo sul grado. Se $(q', r')$ è un'altra coppia che rispetta i vincoli di grado, allora

$$qb + r = a = q'b + r'$$

e quindi $(q - q')b = r' - r$. Poichè $b$ non è nullo, $r = r'$ se e solo se $q = q'$. Supponiamo allora $q \neq q'$, e quindi $r \neq r'$. Se $r = 0$, si ha $r' = (q - q')b$ e da (i) della Definizione 1.4.1 segue l'assurdo $\delta(b) \leq \delta(r')$. Se $r$ e $r'$ sono entrambi diversi da zero, si perviene all'assurdo

$$\delta(b) \leq \delta(r' - r) \leq \max\{\delta(r'), \delta(r)\} < \delta(b)$$

Viceversa, supponiamo che la (**??**) non valga per due elementi non nulli $a, b$ in $D$, con $a + b \neq 0$. Da

$$a = (a + b)1 + (-b) = (a + b)0 + a,$$

e da $\delta(a + b) > \max\{\delta(a), \delta(b)\}$ si ha che nella divisione euclidea di $a$ per $a + b$ le coppie $(1, -b)$ e $(0, a)$ sono entrambe interpretabili come quoziente e resto. ■

**Esempio 1.4.2 - continuazione** [POLINOMI DI LAURENT] Mentre i polinomi in una indeterminata a coefficienti in un campo, con la definizione di grado data nell'Esempio 1.4.1, soddisfano le ipotesi della Proposizione 1.4.2., la condizione (**??**) non è soddisfatta dai polinomi di Laurent. Ciò può essere verificato direttamente a partire dalla definizione di funzione grado data in (**??**), o, equivalentemente, determinando due polinomi $a(z)$ e $b(z)$, $b(z) \neq 0$, per i quali la scrittura (**??**) non è unica.
Ad esempio, per $a(z) = z^3 + z^2 + z + 2$ e $b(z) = z^2 + z - 1$ in $\mathbb{R}[z, z^{-1}]$, si ha $a(z) = b(z)q_1(z) + r_1(z)$ con $q_1(z) = z$ e $r_1(z) = 2z + 2$, $\delta(r_1) = 1 < 2 = \delta(b)$, ma anche $a(z) = b(z)q_2(z) + r_2(z)$ con $q_2(z) = z + 2z^{-1}$ e $r_2(z) = 2z^{-1}$, $\delta(r_2) = 0 < 2 = \delta(b)$.

## 1.5 Polinomi - parte I

Nelle pagine precedenti siamo ricorsi in vari esempi all'anello dei polinomi e al corrispondente campo delle funzioni razionali, assumendo per note, almeno da un punto di vista operativo, alcune loro proprietà. In questo paragrafo ci proponiamo, senza pretesa di completezza, di precisare alcune definizioni e i risultati più elementari ai quali faremo riferimento nel seguito.

### 1.5.1 Polinomi in una indeterminata

Sia $R$ un anello; con il simbolo $z$, non appartenente a $R$, formiamo le espressioni del tipo

$$p(z) = \sum_i p_i z^i, \tag{1.26}$$

dove l'indice $i$ varia su un sottoinsieme finito di $\mathbb{N}$ e i *coefficienti* $p_i$ sono elementi dell'anello $R$. Ciascuno degli addendi in (**??**) viene chiamato *monomio*, mentre il simbolo $z^i$ è detto *termine*. Queste espressioni sono note come *polinomi* e il simbolo $z$ rappresenta l'*indeterminata*. È importante sottolineare che un'indeterminata è solamente un simbolo, una lettera e null'altro.
Due polinomi sono detti *uguali* se contengono esattamente gli stessi monomi, ad eccezione dei monomi a coefficiente nullo, che possono essere inclusi o omessi a piacere. Se sommiamo

o moltiplichiamo due polinomi $p(z)$ e $q(z)$ secondo le regole ben note, assumendo che tutte le potenze di $z$ commutino con gli elementi di $R$, e riuniamo termini relativi alla medesima potenza di $z$, otteniamo un nuovo polinomio. Se $p(z) = \sum_i p_i z^i$ e $q(z) = \sum_i q_i z^i$, infatti, abbiamo

$$p(z) + q(z) := \sum_i (p_i + q_i) z^i, \tag{1.27}$$

dove $p_i$ e $q_i$ vanno assunti nulli ogniqualvolta non compaiano esplicitamente nelle espressioni di $p(z)$ e $q(z)$. Similmente si definisce il loro prodotto come

$$p(z) \cdot q(z) := \sum_i \sum_h (p_{i-h}\ q_h) z^i. \tag{1.28}$$

Con queste due operazioni l'insieme $R[z]$ dei polinomi a coefficienti in $R$ diventa un anello avente come zero il polinomio nullo, i.e. il polinomio a coefficienti tutti nulli, e come unità l'unità di $R$.

Il *grado*, $\deg p$, di un polinomio $p(z)$ non nullo è il più grande intero $m$ tale che $p_m \neq 0$; nel caso di polinomio nullo faremo la convenzione che il suo grado sia $-\infty$. Il coefficiente $p_m$ è noto come *coefficiente conduttore* e quando esso è unitario si parla di polinomio *monico*. Il coefficiente $p_0$ viene detto *termine noto*. Un polinomio di grado zero è del tipo $p_0 z^0$, $p_0 \neq 0$, e può essere identificato con l'elemento $p_0$ di $R$. Questa identificazione fa sì che $R$ sia un sottoanello di $R[z]$.

Un polinomio $p(z) \in R[z]$ si dice *irriducibile* (in $R[z]$) se in ogni sua fattorizzazione $p(z) = p_1(z)p_2(z)$ uno dei due fattori è un elemento invertibile in $R[z]$.

La ragione per cui i polinomi risultano così utili è che possiamo sostituire all'indeterminata $z$ un arbitrario elemento di $R$, o perfino di un anello più grande, senza distruggere la validità delle relazioni di somma e prodotto espresse dalle (**??**) e (**??**). Ciò segue dal fatto che somma e prodotto sono state definite nel modo più naturale, e restano pertanto valide se alla $z$ viene sostituito un arbitrario elemento $\alpha \in R$.

- Esercizio 1.5.1 (*i*) Sia $D$ un dominio; quali sono gli elementi invertibili di $D[z]$?

  (*ii*) Se $R$ non è un dominio possono esistere polinomi invertibili in $R[z]$ di grado strettamente positivo.
  *(Suggerimento: si consideri il polinomio $2z + 1$ a coefficienti nell'anello degli interi modulo 4)*

  (*iii*) Sia $D$ un dominio e siano $a(z)$ e $b(z)$ due polinomi in $D[z]$, il secondo dei quali monico. Dimostrare che esistono $q(z)$ ed $r(z)$ in $D[z]$ tali che

  $$a(z) = b(z)q(z) + r(z) \qquad \deg r < \deg b.$$

  Perchè questo risultato non prova che $D[z]$ è un dominio euclideo?

  (*iv*) in un campo $\mathbb{F}$ un polinomio $p(z)$ è irriducibile se e solo se non è esprimibile come prodotto di due polinomi di grado positivo.

Molte proprietà di $R$ (ma non tutte!) sono ereditate da $R[z]$; in particolare, vale il seguente risultato.

**Proposizione 1.5.1** *$D$ è un dominio se e solo se $D[z]$ lo è.*

DIMOSTRAZIONE Supponiamo che $D$ sia un dominio. Se $p(z)$ e $q(z)$ sono polinomi non nulli in $D[z]$, con coefficienti conduttori rispettivamente $p_m$ e $q_r$, il coefficiente del termine $z^{m+r}$ in $p(z)q(z)$ è $p_m q_r$. Perciò $p(z)q(z)$ non è il polinomio nullo.
Il viceversa è ovvio, avendo identificato $D$ con un sottoanello di $D[z]$. ■

- ESERCIZIO 1.5.2 È vero che se $D$ è un PID allora lo è anche $D[z]$?

Come si è avuto modo di osservare in precedenza, se $\mathbb{F}$ è un campo, $\mathbb{F}[z]$ è un dominio euclideo, quindi a ideali principali. Di conseguenza, per ogni coppia di polinomi non nulli $a(z)$ e $b(z)$, esiste un loro MCD, $d(z)$, ed esso è esprimibile nella forma

$$d(z) = x(z)a(z) + y(z)b(z), \tag{1.29}$$

per opportuni $x(z)$ e $y(z)$ in $\mathbb{F}[z]$. L'applicazione iterata dell'algoritmo di divisione di polinomi consente di calcolare $d(z)$ e fornisce allo stesso tempo una coppia di polinomi $(x(z), y(z))$ che soddisfa la (**??**). In particolare, questo algoritmo fornisce una procedura costruttiva per verificare se una coppia di polinomi è coprima e, in caso affermativo, una soluzione all'identità di Bézout $1 = x(z)a(z) + y(z)b(z)$.

### 1.5.2 Algoritmo Euclideo per l'estrazione del MCD

Siano $a(z)$ e $b(z)$ una coppia di polinomi non nulli in $\mathbb{F}[z]$, $\mathbb{F}$ un campo.
1. [DIVISIONI SUCCESSIVE] Poniamo $p_0(z) = a(z)$ e $p_1(z) = b(z)$ e per $k \geq 2$ definiamo ricorsivamente la successione di polinomi

$$p_k(z) = p_{k-2}(z) - q_{k-1}(z)p_{k-1}(z), \qquad q_{k-1}(z) \in \mathbb{F}[z],\ \deg p_k < \deg p_{k-1}, \tag{1.30}$$

in cui $p_k(z)$ rappresenta il resto della divisione euclidea di $p_{k-2}(z)$ per $p_{k-1}(z)$.
Poiché la successione dei gradi dei polinomi $p_k(z)$ è strettamente decrescente, esiste $\bar{k} \in \mathbb{N}$ tale che $p_{\bar{k}+1}(z) = 0$ e $p_{\bar{k}}(z) \neq 0$. Esplicitamente si ha

$$\begin{aligned}
p_0(z) - q_1(z)p_1(z) &= p_2(z) && (1.31)\\
p_1(z) - q_2(z)p_2(z) &= p_3(z) && (1.32)\\
\dots &\quad \dots\\
p_{\bar{k}-4}(z) - q_{\bar{k}-3}(z)p_{\bar{k}-3}(z) &= p_{\bar{k}-2}(z) && (1.33)\\
p_{\bar{k}-3}(z) - q_{\bar{k}-2}(z)p_{\bar{k}-2}(z) &= p_{\bar{k}-1}(z) && (1.34)\\
p_{\bar{k}-2}(z) - q_{\bar{k}-1}(z)p_{\bar{k}-1}(z) &= p_{\bar{k}}(z) && (1.35)\\
p_{\bar{k}-1}(z) - q_{\bar{k}}(z)p_{\bar{k}}(z) &= 0. && (1.36)
\end{aligned}$$

Vogliamo provare che $p_{\bar{k}}(z)$ è un MCD di $a(z)$ e $b(z)$ ed è esprimibile come in (**??**).

2. [$p_{\bar{k}(z)}$ È DIVISORE COMUNE DI $a(z)$ E $b(z)$] È chiaro da (**??**) e (**??**) che $p_{\bar{k}}(z)$ divide sia $p_{\bar{k}-1}(z)$ che $p_{\bar{k}-2}(z)$. Induttivamente si dimostra che se $p_{\bar{k}}(z)$ divide $p_{k-1}(z)$ e $p_{k-2}(z)$, allora divide anche $p_{k-2}(z)$ e $p_{k-3}(z)$, e infine $a(z)$ e $b(z)$. Quindi $p_{\bar{k}}(z)$ è un divisore comune di $a(z)$ e $b(z)$.

3. [$p_{\bar{k}(z)}$ APPARTIENE ALL'IDEALE $(a(z), b(z))$] Sostituendo nella (**??**) l'espressione di $p_{\bar{k}-1}(z)$ data dalla (**??**), si ottiene per $p_{\bar{k}}(z)$ un'espressione del tipo

$$p_{\bar{k}}(z) = m_{\bar{k}-3}(z)p_{\bar{k}-3}(z) + m_{\bar{k}-2}(z)p_{\bar{k}-2}(z), \tag{1.37}$$

sostituendo $p_{\bar{k}-2}(z)$ in (**??**) con la sua espressione fornita da (**??**) e così via, procedendo a ritroso si giunge, infine, all'espressione

$$p_{\bar{k}}(z) = x(z)a(z) + y(z)b(z).$$

4. [Ogni divisore comune di $a(z)$ e $b(z)$ divide $p_{\bar{k}(z)}$] Se $d'(z)$ è un divisore comune di $a(z)$ e $b(z)$, allora dalla relazione precedente è anche un divisore di $p_{\bar{k}}(z)$, il che dimostra che $p_{\bar{k}}(z)$ è un MCD.

Il precedente algoritmo ha permesso il calcolo di un MCD, $d(z)$, di una coppia di polinomi ed ha portato all'espressione di $d(z)$ fornita dalla (**??**). Adottando un'ottica diversa, $d(z)$ può essere interpretato come termine noto di una particolare equazione diofantea nei polinomi incogniti $x(z)$ e $y(z)$ che, per quanto visto, ammette soluzione. Questo punto di vista ci introduce al problema più generale di trovare sotto quali condizioni, dati tre polinomi $a(z), b(z)$ e $c(z)$ in $\mathbb{F}[z]$, l'equazione diofantea

$$c(z) = x(z)a(z) + y(z)b(z), \tag{1.38}$$

nelle incognite $x(z)$ e $y(z)$, è risolubile in $\mathbb{F}[z]$, e di determinare qual è la struttura dell'insieme delle sue soluzioni. Nella teoria del controllo lineare l'interesse per questo tipo di equazioni è motivato dal fatto che molte procedure di sintesi di controllori, osservatori, etc., possono essere ricondotte, come vedremo, alla soluzione di equazioni diofantee del tipo (**??**) o, nel caso multivariabile, di equazioni polinomiali a coefficienti matriciali.

**Proposizione 1.5.3** [Risolubilità e soluzione generale dell'equazione diofantea] *Sia $d(z)$ un MCD dei polinomi $a(z)$ e $b(z)$. L' equazione (**??**) è risolubile se e solo se $d(z)|c(z)$.*
*Inoltre, se $(\bar{x}(z), \bar{y}(z))$ è una soluzione particolare, posto $\bar{a}(z) = a(z)/d(z)$ e $\bar{b}(z) = b(z)/d(z)$, la soluzione generale di (**??**) è data da*

$$(x(z), y(z)) = (\bar{x}(z), \bar{y}(z)) + q(z)(-\bar{b}(z), \bar{a}(z)) \tag{1.39}$$

*al variare di $q(z)$ in $\mathbb{F}[z]$.*

Dimostrazione Chiaramente l'equazione (**??**) è risolubile se e solo se $c(z)$ appartiene all'ideale generato da $a(z)$ e $b(z)$, ma in un PID tale ideale coincide con quello generato dal MCD di $a(z)$ e $b(z)$. Da ciò segue il risultato.
È immediato verificare che tutte le coppie $(x(z), y(z))$ fornite dalla (**??**) sono soluzioni della (**??**). D'altra parte, se $(x(z), y(z))$ è un'arbitraria soluzione, si ha

$$(x(z) - \bar{x}(z))a(z) = -(y(z) - \bar{y}(z))b(z), \tag{1.40}$$

da cui

$$(x(z) - \bar{x}(z))\bar{a}(z) = -(y(z) - \bar{y}(z))\bar{b}(z). \tag{1.41}$$

Poiché $\bar{a}(z)$ e $\bar{b}(z)$ sono coprimi, da $\bar{a}(z)|(y(z) - \bar{y}(z))\bar{b}(z)$ segue $\bar{a}(z)q(z) = (y(z) - \bar{y}(z))$ e, sostituendo in (**??**), si prova subito la (**??**). ■

**Osservazione** Se l'equazione diofantea (**??**) è risolubile, ovvero se $c(z) = h(z)d(z)$ per un opportuno polinomio $h(z)$, è immediato ottenere una soluzione particolare ricorrendo

all'algoritmo di estrazione del MCD di $a(z)$ e $b(z)$. Da esso, infatti, si ricavano $\tilde{x}(z)$ e $\tilde{y}(z)$ in $\mathbb{F}[z]$ tali che

$$d(z) = \tilde{x}(z)a(z) + \tilde{y}(z)b(z).$$

e la coppia $\Big(h(z)\tilde{x}(z), (h(z)\tilde{y}(z)\Big)$ è una soluzione particolare di (**??**).

**Proposizione 1.5.4** *Se l'equazione (**??**) è risolubile, essa ammette una soluzione* $(x_1(z), y_1(z))$ *con* $\deg x_1 < \deg b$*, ed una soluzione* $(x_2(z), y_2(z))$ *con* $\deg y_2 < \deg a$*.*

DIMOSTRAZIONE Se $(\bar{x}(z), \bar{y}(z))$ è una soluzione particolare dell'equazione, e $\deg \bar{x} \geq \deg b$, applicando l'algoritmo di divisione si ottiene

$$\bar{x}(z) = q(z)b(z) + x_1(z), \qquad \deg x_1 < \deg b.$$

Dalla (**??**) è immediato verificare che $(x_1(z), y_1(z)) = (\bar{x}(z) - q(z)b(z), \bar{y}(z) + q(z)a(z))$ è la soluzione cercata.
Per $(x_2(z), y_2(z))$ si procede in modo analogo. ■

- ESERCIZIO 1.5.3 Siano $a(z) = z^3 - 2z^2 - z + 2$, $b(z) = z^2 - 2z$ e $c(z) = z^5 - 4z^4 + 4z^3 + z - 2$ polinomi in $\mathbb{R}[z]$.
  (*i*) Si provi che $\mathrm{MCD}(a(z), b(z)) = z - 2$.
  (*ii*) Si dimostri che la soluzione generale dell'equazione (**??**), in corrispondenza ai polinomi $a(z)$ e $b(z)$ assegnati, è data da

$$\begin{aligned} x(z) &= (-z^4 + 2z^3 - 1) - q(z)z \\ y(z) &= (z^5 - 2z^4 + z) + q(z)(z^2 - 1) \end{aligned}$$

  (*iii*) Dimostrare che una soluzione $(x_1(z), y_1(z))$ con $\deg x_1 < \deg b$, è data da

$$x(z) = -1 \qquad y(z) = z^3 - 2z^2 + z.$$

- ESERCIZIO 1.5.4 Si provi che nella Proposizione 1.5.4 si puo' assumere $\deg x_1 < \deg \bar{b}$ con $\bar{b}(z) = b(z)/d(z)$, $d(z) = \mathrm{MCD}(a(z), b(z))$.

Ogni polinomio in $p(z) = a_0 + a_1 z + \ldots + a_k z^k \in \mathbb{F}[z]$ individua la funzione $f_p : \mathbb{F} \to \mathbb{F} : c \mapsto a_0 + a_1 c + \ldots + a_k c^k$, che associa ad ogni valore della variabile $c \in \mathbb{F}$ il valore che la "funzione polinomiale" $f_p(\cdot)$ assume in $c$. Di solito, la funzione $f_p$ viene denotata con il medesimo simbolo del polinomio, e con il simbolo $p(c)$ si intende il valore che la funzione polinomiale $p(\cdot)$ assume nel punto $c \in \mathbb{F}$.
Non è sempre vero che polinomi diversi individuino funzioni polinomiali diverse. Se $\mathbb{F}$ è il campo a due elementi, i polinomi $z^k + z^{k+1} \in \mathbb{F}[z]$ individuano, per ogni $k \geq 0$, la funzione polinomiale identicamente nulla.
In ogni caso, fissato $c$ in $\mathbb{F}$, la mappa

$$\phi_c : \mathbb{F}[z] \to \mathbb{F} : p(z) \mapsto p(c)$$

è un omomorfismo suriettivo d'anello.

**Definizione 1.5.5** [ZERO DI UN POLINOMIO] *Sia $c$ un elemento del campo $\mathbb{F}$ e sia $p(z) = \sum_i a_i z^i$ un polinomio in $\mathbb{F}[z]$. Con $p(c)$ indichiamo l'elemento $\sum_i a_i c^i \in \mathbb{F}$. Diciamo che $c$ è uno zero del polinomio $p(z)$ se $p(c) = 0$.*

**Proposizione 1.5.6** *Sia $c$ un elemento del campo $\mathbb{F}$ e sia $p(z)$ un polinomio in $\mathbb{F}[z]$, allora il resto della divisione euclidea di $p(z)$ per $z-c$ coincide con $p(c)$. Di conseguenza, $z-c$ divide $p(z)$ se e solo se $p(c)=0$.*

DIMOSTRAZIONE Dall'algoritmo di divisione euclidea segue

$$p(z) = q(z)(z-c) + r(z), \tag{1.42}$$

con $\deg r < \deg(z-c) = 1$, e quindi $r(z)$ è una costante $r$. Sostituendo $c$ a $z$ in ambo i membri di **??** (in termini più formali, applicando l'omomorfismo $\phi_c$ ad entrambi i membri) si trova $p(c) = q(c)\ 0 + r$.
Se $p(c)=0$, allora $r=0$ e quindi $p(z)=q(z)(z-c)$. Viceversa, se $z-c$ divide $p(z)$ allora il resto della divisione $r=a(c)$ è nullo. ■

- ESERCIZIO 1.5.5 (i) Utilizzando la precedente proposizione si dimostri che se un polinomio $p(z) \in \mathbb{F}[z]$ ha $k$ zeri distinti $c_1, c_2, \ldots, c_k$, allora $\deg p \geq k$
  *(Suggerimento : dividendo $p(z)$ per $z-c_1$ si trova $p(z) = p_1(z)(z-c_1)$, quindi $p_1(z)$ ha zeri $c_2, c_3, \ldots, c_k$).*
  (ii) Se $\mathbb{F}$ è un campo infinito, allora polinomi distinti determinano funzioni polinomiali distinte
  *(Suggerimento: basta osservare che solo il polinomio nullo individua la funzione polinomiale nulla. Infatti, per motivi di grado, solo il polinomio nullo può avere infiniti zeri distinti.)*

<< ∗ **Proposizione 1.5.7** [POLINOMIO INTERPOLATORE DI LAGRANGE] *Sia $\mathbb{F}$ un campo. Dati $n$ elementi distinti $c_1, c_2, \ldots, c_n \in \mathbb{F}$ ed $n$ altri elementi, non necessariamente distinti, $\lambda_1, \lambda_2, \ldots, \lambda_n \in \mathbb{F}$, esiste in $\mathbb{F}[z]$ un polinomio, unico se di grado non superiore a $n-1$, che assume in $c_i$ il valore $\lambda_i$, per $i = 1, 2., \ldots, n$.*

PROVA Si ponga $p_i(z) = \prod_{j \neq i}(z - c_i)$. Allora il polinomio

$$p(z) = \sum_{i=1}^{n} \frac{\lambda_i}{p_i(c_i)} p_i(z) \tag{1.43}$$

ha grado non superiore a $n-1$ e soddisfa la condizione richiesta. Se un altro polinomio $q(z)$ di grado minore di $n$ soddisfa la medesima condizione, allora $p(z) - q(z)$ è identicamente nullo, avendo $n$ zeri distinti $c_1, c_2, \ldots, c_n$ e grado minore di $n$, quindi $q(z) = p(z)$.∗ >> ■

**Definizione 1.5.8** [ZERO MULTIPLO DI UN POLINOMIO] *Un elemento $c \in \mathbb{F}$ è uno zero di $p(z) \in \mathbb{F}[z]$ con* **molteplicità** *$m$ se $(z-c)^m \mid p(z)$ ma $(z-c)^{m+1} \nmid p(z)$.*
*In particolare $c$ ci dirà zero multiplo di $p(z)$ se $m > 1$.*

Dato un polinomio $p(z) = a_0 + a_1 z + \ldots + a_n z^n$ a coefficienti nell'anello $R$ si definisce polinomio derivato di $p$ il polinomio come

$$Dp(z) = a_1 + 2a_2 z + \ldots + n a_{n-1} z^{n-1}.$$

È un facile esercizio verificare che la mappa $D : R[z] \to R[z] : p \mapsto Dp$ che associa ad un polinomio il suo derivato soddisfa in $R[z]$ le proprietà dell'operatore di derivazione definito sulle funzioni reali di variabile reale:

**D**.1 $D(p(z) + q(z)) = Dp(z) + Dq(z)$
**D**.2 $D(p(z)q(z)) = (Dp(z))q(z) + p(z)(Dq(z))$

**D**.3 $D(ap(z)) = aDp(z), \quad a \in R$
**D**.4 $D(z) = 1$

**Proposizione 1.5.9** [Zero multiplo di un polinomio] *Un elemento $c$ in un campo $\mathbb{F}$ è uno zero multiplo di $p(z) \in \mathbb{F}[z]$ se e solo se $p(c) = Dp(c) = 0$.*

Prova Per definizione, $c$ è zero multiplo di $p(z)$ se e solo se $(z-c)^2 | p(z)$.
La divisione euclidea di $p(z)$ per $(z-c)^2$ dà

$$p(z) = (z-c)^2 q(z) + r(z), \quad \text{con } r(z) = (z-c)r_1 + r_0, \quad r_0, r_1 \in \mathbb{F} \tag{1.44}$$

e la derivata di $p(z)$ è

$$Dp(z) = 2(z-c)q(z) + (z-c)^2 Dq(z) + Dr(z) \tag{1.45}$$

Ponendo $z = c$ otteniamo da (**??**) e da (**??**)

$$p(c) = r(c) = r_0, \quad Dp(c) = Dr(c) = r_1$$

e quindi

$$p(z) = (z-c)^2 q(z) + (z-c)Dp(c) + p(c). \tag{1.46}$$

Pertanto $(z-c)^2$ divide $p(z)$ se e solo se $p(c) = Dp(c) = 0$. ■

Un polinomio a coefficienti in un generico campo $\mathbb{F}$ può esser privo di zeri in $\mathbb{F}$ pur avendo grado positivo.

**Definizione 1.5.10** [Campi algebricamente chiusi] *Diciamo che un campo $\mathbb{F}$ è* **algebricamente chiuso** *se ogni polinomio in $\mathbb{F}[z]$ di grado maggiore o uguale a 1 ha almeno uno zero in $\mathbb{F}$.*

È immediato verificare che $\mathbb{F}$ è algebricamente chiuso se e solo se ogni polinomio di grado $n$ fattorizza in $\mathbb{F}[z]$ nel prodotto di $n$ polinomi del primo grado.
È possibile dimostrare [2,6] che comunque scelto un campo $\mathbb{F}$ esiste un campo algebricamente chiuso che lo contiene e i cui elementi sono zeri di opportuni polinomi a coefficienti in $\mathbb{F}$. Il più piccolo campo algebricamente chiuso contenente $\mathbb{F}$ è unico a meno di isomorfismi, viene chiamato **chiusura algebrica di** $\mathbb{F}$ e viene indicato con il simbolo $\bar{\mathbb{F}}$.
Nel seguito, quando parleremo di zeri di un polinomio $p(z) \in \mathbb{F}[z]$ penseremo $p(z)$ come elemento di $\bar{\mathbb{F}}[z]$ e i suoi zeri come elementi di $\bar{\mathbb{F}}$. Pertanto gli zeri di ogni polinomio di grado positivo in $\mathbb{F}[z]$, contati con la rispettiva molteplicità, sono in numero pari al grado.
Ulteriori complementi sui polinomi sono presentati in un paragrafo successivo.

### 1.5.2 Polinomi in più indeterminate

Il procedimento seguito per ottenere da un anello $R$ un anello di polinomi è consistito essenzialmente nella aggiunzione ad $R$ di una indeterminata (di un simbolo) $z \notin R$, con la quale costruire espressioni (i "polinomi") del tipo $b_0 + b_1 z + \ldots b_k z^k$, $\underline{\ } i \in R$ e nella definizione delle operazioni di somma e di moltiplicazione fra le espressioni predette. L'anello $R[z]$ così ottenuto è isomorfo ad ogni altro anello $R[z']$ al quale si perviene aggiungendo ad $R$ una diversa indeterminata $z' \notin R$ e costruendo i polinomi in $z'$.
Poiché il procedimento di aggiungere una indeterminata può essere applicato a qualsiasi

anello, può essere applicato in particolare all'anello $R[z]$. Naturalmente dovremo chiamare la nuova indeterminata con un nome diverso da $z$, p.es. $y$. In questo caso otteniamo l'anello dei polinomi $R[z][y]$, il cui elemento generico ha la forma

$$p(z,y) = \sum_{ij} b_{ij} z^i y^j, \quad b_{ij} \in R$$

e la somma è estesa a un numero finito di coppie $(i,j) \in \mathbb{N} \times \mathbb{N}$. È chiaro che alle stesse espressioni si perviene estendendo dapprima $R$ con $y$ e poi $R[y]$ con $z$, per cui poniamo $R[z,y] := R[z][y] = R[y][z]$.
Più in generale, definiamo l'anello dei polinomi nelle indeterminate $z_1, \ldots, z_n$ in via induttiva, mediante la regola

$$R[z_1, \ldots, z_n] = R[z_1, \ldots, z_{n-1}][z_n]$$

I suoi elementi sono le espressioni formali

$$p(z_1, \ldots, z_n) = \sum_{i_1, \ldots, i_n} b_{i_1 \ldots i_n} z_1^{i_1} \cdots z_n^{i_n}, \quad b_{i_1 \ldots i_n} \in R$$

dove la somma è estesa ad $n$-uple finite di elementi di $\mathbb{N}$.
Gli elementi $b_{i_1 \ldots i_n}$ sono i **coefficienti** del polinomio, ciascuno degli addendi $b_{i_1 \ldots i_n} z_{i_1 \ldots z_n^{i_n}}$ è un **monomio** di grado $i_1 + \ldots + i_n$, e il **grado del polinomio** $p(z_1, \ldots, z_n)$ è il massimo dei gradi dei monomi non nulli che vi figurano.
Un polinomio i cui monomi non nulli hanno tutti il medesimo grado $k$ si dice **omogeneo** (o una forma) di grado $k$. Un polinomio $\mathrm{p}(\mathrm{z}_1, \ldots z_n)$ è una forma di grado $k$ se e solo se, introdotta un'ulteriore indeterminata $t$, si ha

$$p(tz_1, \ldots, tz_n) = t^k p(z_1, \ldots, z_n).$$

## 1.6 Funzioni razionali in una indeterminata

In questo paragrafo costruiremo, a partire dal dominio $\mathbb{F}[z]$, il campo $\mathbb{F}(z)$ delle funzioni razionali nell'indeterminata $z$ a coefficienti in $\mathbb{F}$ e ne studieremo alcune proprietà. La tecnica di costruzione impiegata ha validità generale, nel senso che permette di ottenere, a partire da un arbitrario dominio di integrità $D$, il "campo delle frazioni (o dei quozienti) di $D$", ovvero il più piccolo campo di cui $D$ risulti sottoanello; in particolare, nell'aritmetica elementare essa consente di passare dall'anello degli interi al campo dei numeri razionali.

### 1.6.1 Il campo delle frazioni

Introduciamo nell'insieme $\mathbb{F}[z] \times (\mathbb{F}[z] \setminus \{0\})$ delle coppie ordinate di polinomi $(p(z), q(z))$, con $q(z) \neq 0$, una relazione di equivalenza $\sim$ ponendo

$$(p(z), q(z)) \sim (n(z), d(z)) \quad \Leftrightarrow \quad n(z)q(z) = p(z)d(z), \tag{1.47}$$

e denotiamo la classe di equivalenza individuata dalla coppia $(p(z), q(z))$ con $p(z)/q(z)$. Sull'insieme $\mathbb{F}[z] \times (\mathbb{F}[z] \setminus \{0\})/\sim$ delle classi di equivalenza si definiscono le operazioni di addizione e moltiplicazione ponendo

$$p \,/\, q + n \,/\, d := (pd + nq) \,/\, qd \qquad p/q \cdot n/d := pn \,/\, qd.$$

Rispetto a queste operazioni l'insieme assume struttura di campo, il *campo delle funzioni razionali* in una indeterminata, e viene denotato con $\mathbb{F}(z)$.

- Esercizio 1.6.1 Dimostrare i seguenti fatti :

  $(i)$ $\sim$ è una relazione di equivalenza.

  $(ii)$ Le operazioni di addizione e moltiplicazione prima introdotte sono ben definite, nel senso che somma e prodotto non dipendono dalle particolari coppie di elementi scelte per rappresentare le classi.

  $(iii)$ Ogni classe di equivalenza contiene una coppia $(p(z), q(z))$ con $p$ e $q$ coprimi cui rimane associata una *rappresentazione irriducibile* $p(z)/q(z)$ della funzione razionale. È unica tale coppia?

  $(iv)$ $0/1$ e $1/1$ sono rispettivamente l'elemento neutro rispetto all'addizione ed alla moltiplicazione.

  $(v)$ L'inverso di $p/q$, $p \neq 0$, è $q/p$.

  $(vi)$ Se $(p(z), q(z)) \sim (n(z), d(z))$ e $p(z)/q(z)$ è una rappresentazione irriducibile, allora esiste un $c(z)$ tale che $n(z) = p(z)c(z)$ e $d(z) = q(z)c(z)$.

### 1.6.2 Valutazioni

Sia

$$f(z) = \frac{p(z)}{q(z)} \in \mathbb{F}(z)$$

una funzione razionale non nulla, e sia $\bar{\mathbb{F}}$ la chiusura algebrica di $\mathbb{F}$. Come conseguenza dell'immersione di $\mathbb{F}[z]$ in $\bar{\mathbb{F}}[z]$, ogni polinomio di grado $n$ in $\mathbb{F}[z]$ ha esattamente $n$ zeri (eventualmente coincidenti) in $\bar{\mathbb{F}}$ e fattorizza quindi nel prodotto di $n$ fattori di primo grado. Pertanto, se $\alpha$ è un arbitrario elemento di $\bar{\mathbb{F}}$, è sempre possibile giungere alla scrittura

$$f(z) = \frac{n(z)}{d(z)}(z - \alpha)^{\nu}, \tag{1.48}$$

con $\nu$ un intero e $n(z)$ e $d(z)$ polinomi in $\bar{\mathbb{F}}[z]$, entrambi diversi da zero in $\alpha$.
L'esponente intero $\nu$ che compare nella (**??**) sarà chiamato *valutazione di* $f(z)$ *in* $\alpha$ e indicato con la scrittura $v_\alpha(f)$. La *valutazione di* $f(z)$ *all'infinito* è invece definita da

$$v_\infty(f) := \deg q(z) - \deg p(z).$$

Se $f(z)$ è la funzione nulla, la sua valutazione è per definizione $+\infty$ ovunque.
Se la valutazione $v_\alpha(f)$ è negativa, diremo che $\alpha \in \bar{\mathbb{F}}$ è un *polo di* $f(z)$ *di molteplicità* $-v_\alpha(f)$, se è positiva diremo che $\alpha$ è uno *zero di* $f(z)$ *di molteplicità* $v_\alpha(f)$. La definizione di zero e polo all'infinito è del tutto analoga.

È immediato riconoscere il legame esistente tra zeri e poli di una funzione $f(z)$ e gli zeri dei polinomi che compaiono al *numeratore* $p(z)$ e al *denominatore* $q(z)$ di una sua arbitraria rappresentazione $p(z)/q(z)$. In generale, gli zeri di $f(z)$ sono un sottoinsieme

degli zeri di $p(z)$ ed i poli di $f(z)$ un sottoinsieme degli zeri di $q(z)$; nell'ipotesi in cui $p(z)/q(z)$ sia una rappresentazione irriducibile, invece, zeri e poli di $f(z)$ coincidono con gli zeri di $p(z)$ e $q(z)$, rispettivamente.

- ESERCIZIO 1.6.2 Dimostrare che se $\alpha$ appartiene ad $\bar{\mathbb{F}}$ oppure è il simbolo $+\infty$

  $(i)$ le valutazioni non dipendono dalla particolare rappresentazione $p(z)/q(z)$ utilizzata per la funzione razionale;

  $(ii)$ $v_\alpha(fg) = v_\alpha(f) + v_\alpha(g)$;

  $(iii)$ se $g(z) \neq 0$, allora $v_\alpha(1/g) = -v_\alpha(g)$ e quindi $v_\alpha(f/g) = v_\alpha(f) - v_\alpha(g)$ per ogni $f(z),, g(z) \in \mathbb{F}(z)$;

  $(iv)$ $v_\alpha(f+g) \geq \min(v_\alpha(f), v_\alpha(g))$; in particolare, se $v_\alpha(f) \neq v_\alpha(g)$ allora $v_\alpha(f+g) = \min(v_\alpha(f), v_\alpha(g))$.

  $(v)$ È vero che $v_\alpha(f+g) \leq \max(v_\alpha(f), v_\alpha(g))$?

  $(vi)$ Data $f(z)$ una funzione in $\mathbb{F}(z)$ si effettui la sostituzione $d = 1/z$ ottenendo così una funzione razionale $\tilde{f}(d) \in \mathbb{F}(d)$. Assumendo, per convenzione, $1/0 = \infty$ e $1/\infty = 0$, si verifichi che $v_\alpha(f) = v_{1/\alpha}(\tilde{f})$, per ogni $\alpha \in \bar{\mathbb{F}} \cup \{+\infty\}$.

Una funzione razionale $f(z) \in \mathbb{F}(z)$ è detta *propria* se la sua valutazione all'infinito è maggiore o uguale a zero. In particolare, $f(z)$ è *strettamente propria* se $v_\infty(f) > 0$.

- ESERCIZIO 1.6.3 (i) Si verifichi che le funzioni razionali proprie formano un dominio di integritá, che denoteremo con $\mathbb{F}_p(z)$. Esso è un dominio euclideo proprio rispetto alla funzione grado $\delta(f) := v_\infty(f)$, ma in esso non vale la condizione $\delta(f+g) \leq \max\{\delta(f), \delta(g)\}$ (si considerino, p.es., $f(z) = -2/z$ e $g(z) = (2z+1)/z^2$). Quindi quoziente e resto della divisione euclidea non sono unici. Si fornisca un esempio di tale situazione.

  (ii) Con riferimento alla notazione dell'esercizio 1.6.2 (vi), si dimostri che $f(z)$ è propria se e solo se $\tilde{f}(d)$ ammette una rappresentazione in cui il polinomio a denominatore ha termine noto non nullo, ed è strettamente propria se nella medesima rappresentazione il polinomio a numeratore ha nullo il termine noto.

  (iii) Si dimostri che una funzione razionale $f(z)$ è propria se e solo se può essere sviluppata in serie nell'anello $\mathbb{F}[[z^{-1}]]$.

### 1.6.3 Funzioni razionali stabili

Nel seguito di questo paragrafo assumeremo che $\mathbb{F}$ sia il campo dei reali $\mathbb{R}$ e perciò $\bar{\mathbb{F}}$ coincida con $\mathbb{C}$. Indicheremo inoltre con $\mathbb{C}_e$ l'insieme dei numeri complessi esteso, ovvero il piano complesso compreso il punto improprio $\infty$, e con $\mathbb{D}$ il disco unitario aperto in $\mathbb{C}$, ovvero l'insieme dei numeri complessi di modulo strettamente minore di 1.

**Definizione 1.6.1** [FUNZIONI RAZIONALI STABILI] *Una funzione razionale $f(z)$ in $\mathbb{R}(z)$ è detta stabile*[6] *se i suoi poli sono tutti in $\mathbb{D}$ o, equivalentemente, se $v_\alpha(f) \geq 0$ per ogni $\alpha \in \mathbb{C}_e \setminus \mathbb{D}$.*

Per brevità, quando ci riferiremo ad una generica funzione razionale, ne chiameremo stabili i poli e gli zeri in $\mathbb{D}$, instabili quelli in $\mathbb{C}_e \setminus \mathbb{D}$. Diremo, inoltre, che $p(z) \in \mathbb{R}[z]$ è un *polinomio a zeri stabili* se tutti i suoi zeri appartengono a $\mathbb{D}$. Detto

$$\mathcal{S} := \{f(z) \in \mathbb{R}(z) : v_\alpha(f) \geq 0 \quad \forall \alpha \in \mathbb{C}_e \setminus \mathbb{D}\},$$

[6] Questa definizione di stabilità è giustificata dal fatto che nel seguito prenderemo in considerazione soltanto sistemi a tempo discreto. Una definizione analoga per i sistemi a tempo continuo fa riferimento a funzioni razionali con poli a parte reale strettamente negativa.

l'insieme delle *funzioni razionali (proprie e) stabili*, è immediato verificare che $\mathcal{S}$ è un sottoanello di $\mathbb{R}(z)$. Gli elementi invertibili di $\mathcal{S}$ sono le funzioni razionali la cui valutazione è nulla in ogni punto di $\mathbb{C}_e \setminus \mathbb{D}$, ovvero le funzioni razionali con denominatore e numeratore del medesimo grado e con poli e zeri in $\mathbb{D}$. Tali elementi verranno chiamati **funzioni a fase minima**.

<< * Se $f(z)$ e $g(z)$ sono elementi di $\mathcal{S}$, $g(z)$ divide $f(z)$ in $\mathcal{S}$ se esiste una funzione $h(z) \in \mathcal{S}$ tale che $f(z) = g(z)h(z)$. Dal momento che $\mathbb{R}(z)$ è un campo, l'equazione $f(z) = g(z)h(z)$ nell'incognita $h(z)$ ammette sempre una ed una sola soluzione $h(z) = f(z)/g(z)$ in $\mathbb{R}(z)$, salvo nel caso in cui $g(z)$ sia nullo e $f(z)$ non lo sia; tale soluzione però può non appartenere ad $\mathcal{S}$.

<< * **Proposizione 1.6.2** [Divisori e MCD in $\mathcal{S}$] *Se $f(z)$ e $g(z)$ sono elementi di $\mathcal{S}$ e $g(z) \neq 0$,*

*i) $g(z)$ divide $f(z)$ in $\mathcal{S}$ se e solo se per ogni $\alpha$ in $\mathbb{C}_e \setminus \mathbb{D}$ si ha*

$$v_\alpha(f) \geq v_\alpha(g). \tag{1.49}$$

*ii) $f(z)$ e $g(z)$ non a fase minima sono coprimi se e solo se sono privi di zeri comuni in $\mathbb{C}_e \setminus \mathbb{D}$, ovvero $v_\alpha(f) > 0$ implica $v_\alpha(g) = 0$ per ogni $\alpha \in \mathbb{C}_e \setminus \mathbb{D}$.*

Dimostrazione *(i)* Supponiamo sia $f(z) = g(z)h(z)$ per qualche $h(z) \in \mathcal{S}$. Allora per ogni $\alpha \in \mathbb{C}_e$ si ha $v_\alpha(f) = v_\alpha(g) + v_\alpha(h)$, e per ogni $\alpha \in \mathbb{C}_e \setminus \mathbb{D}$ risulta $v_\alpha(f) \geq v_\alpha(g)$, dal momento che $v_\alpha(h)$ è non negativa.

Viceversa, se vale la (**??**), allora la funzione razionale $h(z) := f(z)/g(z)$ soddisfa $f(z) = g(z)h(z)$ e vale $v_\alpha(h) = v_\alpha(f) - v_\alpha(g) \geq 0$ per ogni $\alpha \in \mathbb{C}_e \setminus \mathbb{D}$. Ciò garantisce che $h(z)$ sia in $\mathcal{S}$.

*(ii)* In base al punto precedente, $h(z) \in \mathcal{S}$ è un divisore comune non banale di $f(z)$ e $g(z)$ se e solo se per ogni $\alpha \in \mathbb{C}_e \setminus \mathbb{D}$ si ha $v_\alpha(h) \leq v_\alpha(f)$ e $v_\alpha(h) \leq v_\alpha(g)$, ed esiste $\bar{\alpha} \in \mathbb{C}_e \setminus \mathbb{D}$ tale che $v_{\bar{\alpha}}(h) > 0$. Ma allora un divisore comune non banale di $f(z)$ e $g(z)$ esiste se e solo se esiste $\bar{\alpha} \in \mathbb{C}_e \setminus \mathbb{D}$ tale che risulti simultaneamente $v_{\bar{\alpha}}(f) > 0$ e $v_{\bar{\alpha}}(g) > 0$. Da ciò segue immediatamente il risultato. ■

**Esempio 1.6.1** Si considerino le funzioni di $\mathcal{S}$

$$g(z) = \frac{z+2}{(z-\frac{1}{2})(z-\frac{1}{4})} \qquad f(z) = \frac{(z+2)^2}{(z-\frac{1}{2})(z-\frac{1}{5})(z+\frac{1}{3})}.$$

Si trova $v_{-2}(g) = 1 < v_{-2}(f) = 2$ e $v_\infty(g) = v_\infty(f) = 1$, mentre per ogni altro $\alpha \in \mathbb{C}_e \setminus \mathbb{D}$ si ha $v_\alpha(g) = v_\alpha(f) = 0$. Essendo soddisfatte le ipotesi della precedente proposizione, si ha che $g(z)$ divide $f(z)$ in $\mathcal{S}$. Di fatto si trova

$$\frac{f(z)}{g(z)} = \frac{(z+2)(z-\frac{1}{4})}{(z-\frac{1}{5})(z+\frac{1}{3})}.$$

- Esercizio 1.6.4 Dimostrare che le seguenti funzioni razionali in $\mathbb{R}(z)$ sono irriducibili in $\mathcal{S}$(ovvero ogni loro fattorizzazione contiene un fattore a fase minima):

$$\frac{1}{z-\alpha} \qquad \frac{z-\beta}{z-\alpha} \qquad \frac{(z-\beta_1)^2+\beta_2^2}{(z-\alpha)^2},$$

con $\alpha \in \mathbb{D} \cap \mathbb{R},\ \beta \in \mathbb{R} \setminus \mathbb{D},\ \beta_1^2 + \beta_2^2 \geq 1$ e $\beta_1\beta_2 \neq 0$

Vogliamo ora introdurre una *funzione grado* $\delta(\cdot) :\ \mathcal{S} \setminus \{0\} \to \mathbb{N}$ rispetto alla quale $\mathcal{S}$ risulti un dominio euclideo proprio (cfr. Definizioni 1.4.1 e 1.4.2). A tale scopo per ogni $f(z) \in \mathcal{S}$ poniamo

$$\delta(f) := \sum_{\alpha \in \mathbb{C}_e \setminus \mathbb{D}} v_\alpha(f), \tag{1.50}$$

ovvero assumiamo come grado di $f(z)$ il numero dei suoi zeri instabili, incluso quello all'infinito, ciascuno contato con la sua molteplicità.

**Esempio 1.6.1 (cont)** Per le funzione dell'esempio 1.6.1 si ha $\delta(g) = 2$ e $\delta(f) = 3$.

- ESERCIZIO 1.6.5 Dimostrare che in $\mathcal{S}$ una funzione $f(z)$ è a fase minima se e solo se $\delta(f) = 0$.

**Lemma 1.6.3** *Se*

$$g(z) = \frac{n_i(z)n_s(z)}{d_s(z)}$$

*è un elemento di $\mathcal{S}$, con $n_s(z)$ e $d_s(z)$ polinomi a zeri stabili e $n_i(z)$ a zeri instabili, allora $\delta(g) = \deg d_s - \deg n_s$.*

DIMOSTRAZIONE Per definizione di $\delta$ si ha

$$\begin{aligned}\delta(g) &= \sum_{\alpha\in\mathbb{C}\setminus\mathbb{D}} v_\alpha(g) + \Big(\deg d_s - \deg(n_i n_s)\Big)\\ &= \sum_{\alpha\in\mathbb{C}\setminus\mathbb{D}} v_\alpha(n_i) + \Big(\deg d_s - \deg n_i - \deg n_s\Big)\\ &= \deg d_s - \deg n_s,\end{aligned}$$

essendo $\deg n_i = \sum_{\alpha\in\mathbb{C}\setminus\mathbb{D}} v_\alpha(n_i)$. ■

**Proposizione 1.6.4** *$\mathcal{S}$ è un dominio euclideo proprio rispetto alla funzione grado* (**??**).

DIMOSTRAZIONE Per provare che $\mathcal{S}$ è un dominio euclideo proprio mostreremo che per ogni $f(z)$ e $g(z)$ in $\mathcal{S}$, $g(z) \neq 0$,

(*i*) $\delta(fg) = \delta(f) + \delta(g)$;

(*ii*) esistono $q(z)$ e $r(z)$ in $\mathcal{S}$, con $r(z)$ nullo o soddisfacente il vincolo $\delta(r) < \delta(g)$, tali che

$$f(z) = q(z)g(z) + r(z);$$

Il punto (*i*) segue dalla definizione di funzione grado e dall'identità $v_\alpha(fg) = v_\alpha(f) + v_\alpha(g)$ (cfr. Esercizio 1.6.2).

Per il punto (*ii*), supponiamo dapprima $\delta(g) = 0$. Per ogni $\alpha \in \mathbb{C}_e \setminus \mathbb{D}$ si ha allora $v_\alpha(g) = 0$, quindi $g(z)$ è invertibile in $\mathcal{S}$ e divide $f(z)$. Di conseguenza

$$q(z) = f(z)g^{-1}(z) \text{ e } r(z) = 0$$

Sia invece $\delta(g) > 0$. Possiamo esprimere $g(z)$ ed $f(z)$ nella forma

$$g(z) = \frac{n_i(z)n_s(z)}{d_s(z)} = \left[\frac{n_s(z)}{d_s(z)} z^{\delta(g)}\right] \frac{n_i(z)}{z^{\delta(g)}}, \qquad f(z) = \frac{a(z)}{b_s(z)},$$

dove $n_s(z), d_s(z)$ e $b_s(z)$ sono polinomi a zeri stabili, $n_i(z)$ ha zeri tutti instabili e $\delta(g)$ è il grado di $g(z)$. Come conseguenza del Lemma 1.6.2 il fattore $n_s(z)z^{\delta(g)}/d_s(z)$ è a fase minima e perciò $n_i(z)/z^{\delta(g)}$è un elemento di $\mathcal{S}$, in quanto prodotto di due elementi di $\mathcal{S}$.
D'altra parte, i polinomi $n_i(z)$ e $b_s(z)$ sono privi di zeri comuni, quindi l'equazione diofantea

$$a(z)z^{\delta(g)-1} = x(z)n_i(z) + y(z)b_s(z) \tag{1.51}$$

è risolubile e (cfr. Proposizione 1.5.4) ammette una soluzione con

$$\deg x < \deg b_s. \tag{1.52}$$

Dividendo entrambi i membri della (**??**) per $b_s(z)z^{\delta(g)-1}$ si perviene all'espressione

$$\begin{aligned}f(z) &= \frac{a(z)}{b_s(z)} = \frac{x(z)}{b_s(z)}\frac{n_i(z)}{z^{\delta(g)-1}} + \frac{y(z)}{z^{\delta(g)-1}}\\ &= \frac{z\ x(z)}{b_s(z)}\left[\frac{n_s(z)}{d_s(z)} z^{\delta(g)}\right]^{-1}\left[\frac{n_s(z)}{d_s(z)} z^{\delta(g)}\right]\frac{n_i(z)}{z^{\delta(g)}} + \frac{y(z)}{z^{\delta(g)-1}}\\ &= \frac{z\ x(z)}{b_s(z)}\left[\frac{n_s(z)}{d_s(z)} z^{\delta(g)}\right]^{-1} g(z) + \frac{y(z)}{z^{\delta(g)-1}}\\ &=: q(z)g(z) + r(z).\end{aligned}$$

nella quale, per (**??**), $z\,x(z)/b_s(z)$ è in $\mathcal{S}$ e quindi $q(z)$, che ne differisce per un fattore a fase minima, è pure in $\mathcal{S}$.
La funzione $r(z)$, in quanto differenza di funzioni di $\mathcal{S}$, appartiene a sua volta a $\mathcal{S}$ e poiché il suo grado soddisfa

$$\delta(r) = \deg z^{\delta(g)-1} - \deg y_s \leq \deg(z^{\delta(g)-1}) < \delta(g),$$

dove con $y_s(z)$ si è indicato la parte stabile di $y(z)$, il punto (ii) è completamente dimostrato ■

**Osservazione** L'operazione di divisione euclidea ora introdotta su $\mathcal{S}$ non assicura l'unicità della coppia quoziente-resto. Ad esempio, per la coppia di funzioni

$$f(z) = \frac{z-1}{z^2} \qquad g(z) = \frac{z-2}{z},$$

valgono entrambe le scomposizioni:

$$f(z) = -\frac{\frac{z}{5} - \frac{1}{2}}{z} g(z) + \frac{\frac{z^2}{5} + \frac{z}{10}}{z^2},$$

e

$$f(z) = -\frac{\frac{z}{4} - \frac{1}{2}}{z} g(z) + \frac{1}{4}.$$

Alternativamente, basta considerare la coppia di funzioni

$$f(z) = \frac{z-1/6}{z} \qquad g(z) = -\frac{z-1/3}{z}$$

per le quali non è soddisfatta la diseguaglianza $\delta(f+g) \leq \max(\delta(f), \delta(g))$: viene quindi a mancare quella che nel paragrafo 1.4 abbiamo evidenziato come condizione necessaria e sufficiente per l'unicità di quoziente e resto.

- Siamo $f(z)$ e $g(z)$ elementi di $\mathcal{S}$. Si dimostri che $f(z)$ e $g(z)$ sono coprimi se e solo se esistono $x(z)$ e $y(z) \in \mathcal{S}$ tali che $x(z)f(z) + y(z)g(z) = 1$.
- Esercizio 1.6.11 Siano $f(z)$ e $g(z)$ elementi di $\mathcal{S}$. Si provi che, come conseguenza dell'Esercizio 1.6.2 $(iv)$, si ha
$$\delta(f+g) = \sum_{\alpha \in \mathbb{C}_e \setminus \mathbb{D}} v_\alpha(f+g) \geq \sum_{\alpha \in \mathbb{C}_e \setminus \mathbb{D}} \min(v_\alpha(f), v_\alpha(g)).$$
- Esercizio 1.6.6 Si interpretino i polinomi di Laurent come funzioni razionali stabili per le quali il dominio di stabilità $\mathbb{D}$ è l'insieme $\{0 \cup \infty\}$.

Vogliamo ora accennare alla possibilità di rappresentare una arbitraria funzione razionale come rapporto di elementi di $\mathcal{S}$.
Come si è avuto modo di sottolineare all'inizio del paragrafo, il procedimento di costruzione del campo delle funzioni razionali $\mathbb{F}(z)$ a partire da $\mathbb{F}[z]$ ha validità generale. L'applicazione di tale procedura al dominio $\mathcal{S}$ conduce ancora al campo delle funzioni razionali $\mathbb{R}(z)$, e dunque $\mathbb{R}(z)$ è il più piccolo campo avente $\mathcal{S}$ come sottoanello (oltre che il più piccolo campo avente come sottoanello $\mathbb{R}[z]$).
Di conseguenza, ogni elemento $w(z)$ di $\mathbb{R}(z)$ è esprimibile come rapporto $f(z)/g(z)$ di due funzioni razionali proprie e stabili e, in particolare, di due funzioni coprime in $\mathcal{S}$, cioè prive di zeri instabili comuni (*rappresentazione irriducibile in* $\mathcal{S}$). Zeri e poli instabili di $w(z)$ possono allora essere interpretati in termini di zeri (instabili) di $f(z)$ e $g(z)$.

**Proposizione 1.6.5** *Sia $w(z)$ una funzione razionale in $\mathbb{R}(z)$.*

*(i) Se $p(z)/q(z)$, con $p(z), q(z) \in \mathbb{R}[z]$, è una rappresentazione di $w(z)$ in $\mathbb{R}[z]$ e se*

$$f(z) := \frac{p(z)}{z^n} \qquad g(z) := \frac{q(z)}{z^n}, \qquad n = \max\{\deg p, \deg q\},$$

*allora $f(z)/g(z)$ è una rappresentazione di $w(z)$ in $\mathcal{S}$, irriducibile in $\mathcal{S}$ se e solo se gli unici fattori comuni a $p(z)$ e $q(z)$ sono polinomi a zeri stabili.*

(*ii*) *Se $f(z)/g(z)$ è una rappresentazione di $w(z)$ irriducibile in $\mathcal{S}$, il punto $\alpha \in \mathbb{C}_e \setminus \mathbb{D}$ è uno zero (polo) di $w(z)$ se e solo se è uno zero di $f(z)$ (di $g(z)$).*

*La sua molteplicità come zero (polo) di $w(z)$ coincide con la sua molteplicità come zero di $f(z)$ (di $g(z)$).*

DIMOSTRAZIONE (*i*) Le funzioni razionali $f(z)$ e $g(z)$ sono elementi di $\mathcal{S}$ dal momento che $z^n$ è un polinomio a zeri stabili il cui grado è non minore di quello di $p(z)$ e $q(z)$. La rappresentazione $f(z)/g(z)$ è irriducibile se e solo se $f(z)$ e $g(z)$ sono privi di zeri comuni in $\mathbb{C}_e \setminus \mathbb{D}$ (vedi Esercizio 1.6.7); come conseguenza della scelta fatta per $n$, certamente $f(z)$ e $g(z)$ non hanno uno zero comune nel punto improprio. Gli eventuali zeri comuni rimangono quindi al finito, da cui segue immediatamente il risultato.

(*ii*) Il risultato è conseguenza della relazione $v_\alpha(w) = v_\alpha(f) - v_\alpha(g)$ e del fatto che, per la coprimalità di $f(z)$ e $g(z)$, per ogni $\alpha \in \mathbb{C}_e \setminus \mathbb{D}$, uno al più tra $v_\alpha(f)$ e $v_\alpha(g)$ può essere positivo.$*$ >> ■

I paragrafi successivi del capitolo sono omessi:

Polinomi - parte II

- Polinomi irriducibili e polinomi primitivi
- Estensioni di un campo
- Zeri di un polinomio in un'estensione del campo dei coefficienti

Moduli

- Definizioni
- Moduli quoziente e omomorfismi
- Generatori
- Annullatori e torsione

Moduli noetheriani
Moduli finitamente generati su un PID
Gruppi abeliani finiti
Campi finiti - Parte I

- Struttura dei campi finiti
- Polinomi su campi finiti
- Elementi coniugati, tracce e norme

Campi Finiti - Parte II

- Basi
- Polinomi ciclotomici

## 1.7 Riferimenti bibliografici

Quasi tutti gli argomenti accennati in questo capitolo sono trattati diffusamente in numerosi manuali di Algebra. Alcuni riferimenti standard, con un'impostazione astratta e sistematica, sono

1. N.Jacobson "Lectures in Abstract Algebra", 3 voll., Van Nostrand, 1951
2. N.Jacobson "Basic Algebra", voll. 1 e 2, Freeman, 1974
3. S.Lang "Algebra" (terza edizione), Addison-Wesley, 1993
4. P.M.Cohn "Algebra" (seconda edizione), voll.1, 2 e 3, Wiley, 1989
5. B.van der Waerden "Algebra", voll.1 e 2, Ungar, 1966.
6. T.W.Hungerfort "Algebra", Springer , 1974

La breve monografia

7. G.Ellis "Rings and Fields", Clarendon Press, 1992

ha un taglio meno sistematico delle opere precedenti ma contiene numerosi spunti applicativi e stimolanti esercizi.

Un ottimo riferimento per l'algebra dei polinomi e per gli aspetti algoritmici connessi è

8. T.Becker, V.Weispfenning "Gröbner Bases", Springer, 1993

Sulle equazioni diofantee possono essere consultati con profitto

9. V.Kucera "Discrete Linear Control: the Polynomial Equation Approach", Wiley, 1979
10. S.Barnett "Polynomials and Linear Control Systems", Dekker, 1983.

Una trattazione approfondita delle funzioni razionali stabili è presentata in

11. M.Vidyasagar "Control System Synthesis: a Factorization Approach", MIT Press, 1985.

Per i campi finiti, un riferimento "enciclopedico" è

12. L.Liedl, H.Niederreiter "Finite Fields", Addison Wesley Pu.Co., 1983