

.

Capitolo 7

Prime Proprietá degli Anelli

7.1 Sottoanelli e ideali di un anello

Sia A un anello.

DEFINIZIONE 7.1.1 Un sottoinsieme H di un anello A si chiama *sottoanello* se é una parte stabile e se é un anello rispetto alle operazioni indotte in esso da A . Un sottoanello che risulti un corpo (risp. campo) si chiama *sottocorpo* (risp. *sottocampo*). \diamond

ESERCIZIO 7.1.2 *Nell'anello degli interi trovare una parte stabile che non é un sottoanello.* \diamond

Ogni anello A possiede due sottoanelli *banali*: $\{0\}$ (*sottoanello nullo*) e A . Un sottoanello diverso da A si dice *proprio*.

Elenchiamo alcune proprietá e definizioni relative ai sottoanelli di un anello A .

- H sottoanello di $A \Leftrightarrow a - b \in H$ e $ab \in H$, per ogni $a, b \in H$.
- L'unione di due sottoanelli non é in generale un sottoanello.
- L'intersezione di una famiglia di sottoanelli é un sottoanello.
- La proprietá precedente permette di definire il *sottoanello generato* da un sottoinsieme X di A come l'intersezione di tutti i sottoanelli di A che contengono X . Tale sottoanello é il piú piccolo (rispetto all'inclusione) sottoanello di A che contiene X .
- Un sottoanello H di A é il sottoanello generato da un sottoinsieme X di A se, e solo se, sono verificate le due seguenti proprietá:
 - (1) H é un sottoanello di A contenente X ,
 - (2) ogni sottoanello K di A contenente X contiene H .
- Un elemento $a \in A$ si dice *centrale* se é tale rispetto al prodotto. L'insieme $Z(A)$ degli elementi centrali di A si chiama *centro di A* ed é un sottoanello di A .
- Un sottoanello di un anello unitario puó non essere unitario.
- Un sottoanello unitario di un anello unitario A puó avere unitá diversa da quella di A .

ESEMPI 7.1.3

- Z é sottoanello di Q .
- $2Z$ é un sottoanello non unitario dell'anello unitario Z .
- $H = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} : a \in R \right\}$ é sottoanello unitario di $M_2(R)$ con unitá $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$. Si osservi che l'unitá di H é diversa dall'unitá di $M_2(R)$. \diamond

ESERCIZIO 7.1.4 Siano A_1 e A_2 due anelli e $f: A_1 \rightarrow A_2$ un monomorfismo. Provare che $f(A_1)$ é un sottoanello di A_2 isomorfo a A_1 .

ESERCIZIO 7.1.5 Sia A un anello. Provare che l'intersezione di una famiglia di sottocampi (risp. sottocorpi) di A é un sottocampo (risp. sottocorpo) di A . Nel caso A sia un campo e X un insieme di suoi elementi, definire il sottocampo di A generato da X .

DEFINIZIONE 7.1.6 Un sottoanello H di A prende il nome di *ideale sinistro* (risp. *destro*) se

$$ah \in H \quad (\text{risp. } ha \in H) \quad , \quad \text{per ogni } a \in A \quad , \quad h \in H.$$

Un ideale che sia sinistro e destro si dice *bilatero*. \diamond

OSSERVAZIONE 7.1.7 Un sottoanello di un anello non é necessariamente un ideale. Per esempio, Z é un sottoanello di Q che non é un ideale. \diamond

OSSERVAZIONE 7.1.8 Gli insiemi $\{0\}$ e A sono ideali bilateri dell'anello A e sono detti *ideali banali* di A . Un ideale di A diverso da A si dice *proprio*. Se A é commutativo, tutti i suoi ideali sono bilateri. \diamond

ESERCIZIO 7.1.9 Provare che nell'anello $M_2(Z)$ l'insieme

$$I = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a, b \in Z \right\}$$

é un ideale sinistro ma non é un ideale destro.

ESEMPIO 7.1.10 Sia a un numero reale. L'insieme

$$I = \{f(x) \in R[x] : f(a) = 0\}$$

é un ideale di $R[x]$. \diamond

Riportiamo di seguito alcune proprietà e definizioni relative agli ideali.

- H ideale sinistro di $A \Leftrightarrow a - b \in H$ per ogni $a, b \in H$ e $ah \in H$ per ogni $a \in A, h \in H$.
- L'intersezione di una famiglia di ideali sinistri é un ideale sinistro.
- La proprietà precedente permette di definire l'*ideale sinistro generato* da un sottoinsieme X di A come l'intersezione di tutti gli ideali sinistri di A che contengono X . Tale ideale si denota con $(X)_s$ ed é il piú piccolo (rispetto all'inclusione) ideale sinistro di A contenente X .

• Un ideale sinistro H di A é l'ideale sinistro generato da un sottoinsieme X di G se, e solo se, sono verificate le due seguenti propriet :

- (1) H é un ideale sinistro di A contenente X ,
- (2) ogni ideale sinistro K di A contenente X contiene H .

• Se H, K sono ideali sinistri di A , risulta

$$(H \cup K)_s = \{h + k \quad : \quad h \in H \quad , \quad k \in K\}. \tag{7.1}$$

Tale ideale si denota con $H + K$ e si chiama *somma* degli ideali H e K .

• Se A é unitario ed un suo ideale sinistro H contiene 1, allora risulta $H = A$.

• Se A é unitario ed un suo ideale sinistro H contiene un elemento invertibile, allora risulta $H = A$.

• Se $x \in A$, risulta

$$(x)_s = \{ax + nx \quad : \quad a \in A \quad , \quad n \in \mathbb{Z}\}; \tag{7.2}$$

se A é unitario risulta

$$(x)_s = \{ax \quad : \quad a \in A\}. \tag{7.3}$$

PROPOSIZIONE 7.1.11 *Un anello unitario non nullo A é un corpo se, e soltanto se, i suoi unici ideali sinistri (destri) sono quelli banali.*

DIMOSTRAZIONE. Se A é un corpo, un suo ideale sinistro non nullo contiene elementi invertibili e, quindi, coincide con A . Supponiamo ora che A non posseda ideali sinistri non banali e sia x un suo elemento diverso da zero. Allora abbiamo $(x) = A$ e, di conseguenza, l'unit  1 di A appartiene ad (x) . Ne segue, in forza della (7.3), che esiste in A un elemento $a \neq 0$ tale che $ax = 1$. Analogamente, avendosi $(a) = A$, esiste in A un elemento $b \neq 0$, tale che $ba = 1$ e risulta:

$$xa = 1xa = (ba)(xa) = b(ax)a = ba = 1.$$

Abbiamo cos  che $a = x^{-1}$ e l'asserto é completamente provato. \diamond

DEFINIZIONE 7.1.12 Un ideale sinistro (risp. destro, bilatero) H si dice *principale* se pu  essere generato da un solo elemento, cio  se esiste $x \in H$ tale che $(x)_s = H$ (risp. $(x)_d = H$, $(x) = H$). Un dominio di integrit  unitario A si chiama *anello principale* se tutti i suoi ideali sono principali. \diamond

ESERCIZIO 7.1.13 *Provare che l'unione di una catena (rispetto all'inclusione) di ideali sinistri (risp. destri, bilateri) di un anello é un ideale sinistro (risp. destro, bilatero).*

7.1.1 Ideali massimali e primi

Sia A un anello.

DEFINIZIONE 7.1.14 Un ideale sinistro (risp. destro, bilatero) proprio H di A si dice *massimale* se non é propriamente contenuto in alcun ideale sinistro (risp. destro, bilatero) diverso da A . \diamond

Il teorema che segue é un'altra importante applicazione del lemma di Zorn.

TEOREMA 7.1.15 (teorema di Krull) *Sia A un anello unitario. Allora ogni ideale sinistro proprio H é contenuto in almeno un ideale sinistro massimale.*

DIMOSTRAZIONE. • Sia (\mathcal{L}, \subseteq) l'insieme ordinato degli ideali sinistri propri di A contenenti H e sia \mathcal{E} una catena di \mathcal{L} . Poniamo:

$$L = \bigcup_{K \in \mathcal{E}} K.$$

• L é un ideale sinistro di A contenente H . Poiché $1 \notin L$, L é un ideale proprio¹ e quindi appartiene a \mathcal{L} .

• L é un maggiorante di \mathcal{E} in \mathcal{L} e quindi \mathcal{L} risulta un insieme induttivo.

• Dal lemma di Zorn ricaviamo che esiste in \mathcal{L} un elemento massimale M .

• M é un ideale sinistro massimale contenente H , e l'asserto é dimostrato. \diamond

COROLLARIO 7.1.16 *Ogni anello unitario contiene almeno un ideale sinistro massimale.*

Figura 7.1: W.Krull (1899-1971)

DEFINIZIONE 7.1.17 Sia A un anello commutativo. Un ideale proprio H di A si dice *primo* se:

$$ab \in H \quad \Rightarrow \quad a \in H \quad \text{o} \quad b \in H.$$

\diamond

OSSERVAZIONE 7.1.18 Un anello commutativo A é un dominio di integritá se, e soltanto se, l'ideale nullo é un ideale primo. \diamond

DEFINIZIONE 7.1.19 Sia A un anello commutativo e $H, K \leq A$. Allora l'insieme

$$\{h_1k_1 + h_2k_2 + \cdots + h_s k_s ; h_i \in H, k_i \in K, s \geq 0\}$$

¹Si noti che l'ipotesi che A sia unitario é essenziale per provare che L é un ideale proprio.

é un ideale che si chiama *prodotto* di H e K e si denota con HK .² Inoltre, per ogni intero $n > 1$, l'ideale definito per induzione da

$$H^n = \underbrace{HH \cdots H}_{{(n-1)} \text{ volte}} H$$

si chiama *potenza n -ma* di H . ◇

ESERCIZIO 7.1.20 *Provare che, se H, K, L sono ideali di un anello unitario, risulta:*

$$HK \subseteq H \cap K \quad e \quad (HK)L = H(KL).$$

PROPOSIZIONE 7.1.21 *Siano A un anello commutativo, H un ideale primo e H_1, H_2, \dots, H_n ideali tali che $H_1 H_2 \cdots H_n \subseteq H$. Allora risulta $H_i \subseteq H$, per almeno un indice i .*

DIMOSTRAZIONE. Supponiamo $n = 2$, $H_2 \not\subseteq H$ e $b \in H_2 \setminus H$. Allora si ha

$$a \in H_1 \Rightarrow ab \in H_1 H_2 \Rightarrow ab \in H, \quad b \notin H \Rightarrow a \in H,$$

cioé $H_1 \subseteq H$. A questo punto basta procedere per induzione su $n > 2$. ◇

7.1.2 Ideali di $(Z, +, \cdot)$ e $(Z_n, +, \cdot)$

Usando i risultati del paragrafo 6.1.2 si possono caratterizzare senza difficoltà gli ideali dell'anello degli interi e dell'anello degli interi modulo n .

PROPOSIZIONE 7.1.22 *Ogni ideale H di $(Z, +, \cdot)$ é del tipo mZ , ove m é il minimo fra gli interi non negativi contenuti in H . Ne segue che Z é un anello principale.*

DIMOSTRAZIONE. Osserviamo che mZ é un ideale e che ogni ideale é un sottogruppo di $(Z, +)$. Allora l'asserto segue dalla prop.6.1.27. ◇

ESERCIZIO 7.1.23 *Sia mZ un ideale dell'anello Z degli interi. Provare che mZ é un ideale primo se, e solo se, m é un primo. Provare inoltre che un ideale di Z é primo se, e solo se, é massimale.*

PROPOSIZIONE 7.1.24 *Ogni ideale H di $(Z_n, +, \cdot)$ é del tipo*

$$\langle h \rangle = \{0, h, 2h, \dots, (k-1)h\},$$

ove h e k sono interi tali che $n = hk$.

DIMOSTRAZIONE. Osserviamo che $\langle h \rangle$ é un ideale e che ogni ideale é un sottogruppo di $(Z_n, +)$. Allora l'asserto segue dalle 6.1.32 e 6.1.33. ◇

²Attenzione, in questo caso il simbolo HK non denota l'insieme $\{hk : h \in H, k \in K\}$.

7.2 Il campo dei quozienti di un dominio d'integritá

Sia D un dominio d'integritá e ricordiamo esplicitamente che stiamo supponendo non nulli tutti gli anelli che prendiamo in considerazione.

DEFINIZIONE 7.2.1 La relazione \sim su $D \times D^*$ definita da

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

risulta d'equivalenza ed il relativo insieme quoziente si denota con $Q(D)$. La classe d'equivalenza $[(a, b)]$ di una coppia (a, b) , che si denota con

$$\frac{a}{b} \quad \text{o con} \quad a/b,$$

si chiama *frazione di numeratore a e denominatore b* . ◇

Le seguenti proprietá sono di facile verifica:

- $\frac{a}{b} = \frac{c}{d} \Leftrightarrow (a, b) \sim (c, d) \Leftrightarrow ad = bc$;
- $\frac{ac}{bc} = \frac{a}{b}$, per ogni elemento $c \in D^*$;
- $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'} \Rightarrow \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$;
- $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'} \Rightarrow \frac{ac}{bd} = \frac{a'c'}{b'd'}$.

Risultano, pertanto, ben definite in $Q(D)$ le seguenti operazioni di addizione e moltiplicazione:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \frac{c}{d} = \frac{ac}{bd}.$$

La struttura $(Q(D), +)$ é un gruppo abeliano additivo nel quale lo zero é dato dalla frazione $\frac{0}{d}$, con $d \in D^*$, e l'opposto di un elemento $\frac{a}{b}$ é $\frac{-a}{b}$. La moltiplicazione é associativa, commutativa, distributiva rispetto all'addizione ed eredita dalla moltiplicazione di D anche la validitá della legge di annullamento del prodotto, cioé

$$\frac{a}{b} \frac{c}{d} = 0 \Leftrightarrow \frac{a}{b} = 0 \quad \text{o} \quad \frac{c}{d} = 0.$$

Ne segue che $Q(D)^* = Q(D) \setminus \{0\}$ é stabile rispetto alla moltiplicazione. La struttura $(Q(D)^*, \cdot)$ é un gruppo abeliano moltiplicativo nel quale l'unitá é data dalla frazione $\frac{a}{a}$, con $a \in D \setminus \{0\}$, e l'inverso di un elemento non nullo $\frac{a}{b}$ é $\frac{b}{a}$.

Quanto finora detto prova il seguente teorema.

TEOREMA 7.2.2 *La struttura algebrica $(Q(D), +, \cdot)$ é un campo.*

DEFINIZIONE 7.2.3 Il campo $(Q(D), +, \cdot)$ prende il nome di *campo dei quozienti* del dominio d'integritá D e sará denotato semplicemente con $Q(D)$. ◇

OSSERVAZIONE 7.2.4 *Il campo $(Q(\mathbb{Z}), +, \cdot)$ dei quozienti di \mathbb{Z} é il campo Q dei razionali.*

Fissato un elemento $b \in D^*$, definiamo l'applicazione

$$i : a \in D \rightarrow \frac{ab}{b} \in Q(D)$$

e osserviamo che essa non dipende dalla scelta di b in D^* perché é

$$\frac{ab}{b} = \frac{ac}{c},$$

per ogni $c \in D^*$. Inoltre, risultando

$$\begin{aligned} i(x+y) &= \frac{(x+y)b}{b} = \frac{xb+yb}{b} = \frac{xb}{b} + \frac{yb}{b} \\ &= \frac{xb^2 + byb}{b^2} = \frac{xb}{b} + \frac{yb}{b} = i(x) + i(y), \\ i(xy) &= \frac{xyb}{b} = \frac{xyb}{b} \frac{b}{b} = \frac{xb yb}{b^2} = \frac{xb}{b} \frac{yb}{b} = i(x)i(y), \end{aligned}$$

la funzione i é un omomorfismo con nucleo nullo

$$\text{Ker } i = \{a \in D : \frac{ab}{b} = 0\} = \{0\}.$$

Ne segue che i é un monomorfismo canonico, nel senso che é indipendente dalla scelta dell'elemento b in D^* , e quindi

$$D \sim i(D) = \left\{ \frac{ab}{b} : a \in D \right\} \subseteq Q(D).$$

Abbiamo cosí che $Q(D)$ contiene il sottoanello $i(D)$ canonicamente isomorfo ad D .

Nel seguito, con abuso di linguaggio e di notazione, identificheremo D e $i(D)$, cioè penseremo D come sottoanello di $Q(D)$, e scriveremo $a = i(a)$, per ogni $a \in D$. Con questa notazione, per ogni $\frac{x}{y} \in Q(D)^*$, abbiamo

$$\frac{x}{y} = \frac{xb}{b} \frac{b}{yb} = \frac{xb}{b} \left(\frac{yb}{b} \right)^{-1} = i(x)i(y)^{-1} = xy^{-1}$$

e cosí possiamo scrivere

$$Q(D) = \{ab^{-1} : a, b \in D, b \neq 0\}.$$

ESERCIZIO 7.2.5 *Provare che l'unitá di $Q(D)$ appartiene a $i(D)$ se, e solo se, D é unitario.*

ESEMPIO 7.2.6 $Z[x]$ é un dominio d'integritá e quindi possiamo considerare il suo campo dei quozienti

$$Q(Z[x]) = \left\{ \frac{f(x)}{g(x)} : f, g \in Z[x], f \neq 0 \right\}.$$

Gli elementi di $Q(Z[x])$ si chiamano *funzioni razionali* su Z .

◇

ESEMPIO 7.2.7 Se F é un campo, il campo dei quozienti di $F[x]$ si denota con $F(x)$. Gli elementi di $F(x)$ si chiamano *funzioni razionali* su F . \diamond

ESERCIZIO 7.2.8 Siano D_1, D_2 domini d'integritá isomorfi e $f : D_1 \rightarrow D_2$ un isomorfismo. Provare che l'applicazione

$$\varphi : \frac{a}{b} \in Q(D_1) \rightarrow \frac{f(a)}{f(b)} \in Q(D_2)$$

é ben definita e risulta un isomorfismo fra $Q(D_1)$ e $Q(D_2)$.

ESERCIZIO 7.2.9 Provare che il campo dei quozienti del dominio d'integritá $(2Z, +, \cdot)$ é isomorfo al campo razionale.

OSSERVAZIONE 7.2.10 Due domini d'integritá non isomorfi possono avere campi dei quozienti isomorfi. Abbiamo, infatti, visto che $(Z, +, \cdot)$ e $(2Z, +, \cdot)$, che non sono isomorfi, hanno entrambi campo dei quozienti isomorfo al campo razionale. \diamond

PROPOSIZIONE 7.2.11 Siano K un corpo e A un sottoanello commutativo di K . Allora A é un dominio d'integritá, l'insieme

$$F = \{ab^{-1} : a, b \in A, b \neq 0\}$$

é un sottocampo di K isomorfo a $Q(A)$ e coincide col sottocampo di K generato da A . In particolare, se A é un campo, abbiamo $F = A$ e, quindi, ogni campo é isomorfo al proprio campo dei quozienti.

DIMOSTRAZIONE. L'applicazione

$$f : \frac{a}{b} \in Q(A) \rightarrow ab^{-1} \in K$$

é un monomorfismo di anelli e risulta $f(Q(A)) = F$. Ne segue che $Q(A)$ ed F sono isomorfi, cioè l'asserto. \diamond

PROPOSIZIONE 7.2.12 Se D é un dominio d'integritá, $Q(D)$ non contiene sottocampi propri contenenti D .

DIMOSTRAZIONE. Sia K un sottocampo di $Q(D)$ contenente D . Allora

$$K \supseteq D \Rightarrow ab^{-1} \in K, \forall a, b \in D, b \neq 0 \Rightarrow K \supseteq Q(D).$$

\diamond

PROPOSIZIONE 7.2.13 Sia D un dominio d'integritá. Sia K un campo contenente D come sottoanello e privo di sottocampi propri contenenti D . Allora K é isomorfo a $Q(D)$.

DIMOSTRAZIONE. La prop.7.2.11 assicura che $F = \{ab^{-1} : a, b \in D, b \neq 0\}$ é un sottocampo di K contenente D e isomorfo a $Q(D)$. Ne segue che $K = F \sim Q(D)$. \diamond

Le ultime due proposizioni hanno il seguente corollario di immediata dimostrazione.

COROLLARIO 7.2.14 Siano K un campo ed A un sottoanello di K . Allora il sottocampo di K generato da A é isomorfo al campo dei quozienti di A .

Avvertiamo il Lettore che nel seguito, se K é un campo e A un suo sottoanello, con abuso di notazione, identificheremo spesso $Q(A)$ col sottocampo di K generato da A ; porremo cioè

$$Q(A) = \{ab^{-1} : a, b \in A, b \neq 0\}. \quad (7.4)$$

7.3 Esempi notevoli di anelli

7.3.1 Anelli di polinomi

Sia A un anello commutativo unitario.

DEFINIZIONE 7.3.1 Si chiama *polinomio a coefficienti in A nella indeterminata x* un'espressione formale del tipo

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

ove $a_0, a_1, a_2, \dots, a_n$ sono elementi di A e si dicono *coefficienti*³ di $a(x)$. Il coefficiente a_0 si chiama anche *termine noto* di $a(x)$. Se a_n è diverso da zero, l'intero n prende il nome di *grado* di $a(x)$ e si denota con $\deg(a(x))$ o $\deg(a)$. Nel caso in cui il polinomio $a(x)$ ha grado n , l'elemento a_n si chiama *coefficiente* o *parametro direttore* di $a(x)$ e, se $a_n = 1$, il polinomio si dice *monico*. L'insieme di tutti i polinomi a coefficienti in A si denota con $A[x]$. \diamond

Osserviamo che:

- gli elementi non nulli dell'anello A sono polinomi di grado zero;
- lo zero dell'anello A è un polinomio (*polinomio nullo*) e risulta l'unico polinomio per cui non è definito il grado;
- due polinomi

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n, \quad b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m$$

sono uguali se, e solo se,

$$n = m \quad \text{e} \quad a_0 = b_0, a_1 = b_1, a_2 = b_2, \dots, a_n = b_n,$$

in particolare un polinomio è il polinomio nullo se, e solo se, tutti i suoi coefficienti sono uguali a zero.

DEFINIZIONE 7.3.2 Se $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ è un polinomio a coefficienti in A , la funzione

$$\bar{a} : A \rightarrow A$$

definita da

$$\bar{a}(c) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n, \quad \text{per ogni } c \in A,$$

si chiama *funzione polinomiale di $a(x)$* . Di solito, se $a(x)$ è un polinomio e c un elemento di A , con abuso di notazione, si scrive $a(c)$ in luogo di $\bar{a}(c)$ e si dice che l'elemento $a(c)$ è il *valore* di $a(x)$ su c . Si dice, poi, che in $A[x]$ vale il *principio di identità dei polinomi* se accade che due polinomi di $A[x]$ sono uguali se, e solo se, sono uguali le loro funzioni polinomiali. \diamond

OSSERVAZIONE 7.3.3 Il Lettore ricorderà dal corso di *Analisi matematica I* che in $Z[x], Q[x], R[x], C[x]$ vale il principio di identità dei polinomi. Proveremo nel seguito che tale principio vale in $A[x]$, per ogni dominio d'integritá unitario infinito K . \diamond

³Per convenzione si usa porre $0 = a_{n+1} = a_{n+2} = \cdots$

OSSERVAZIONE 7.3.4 Il polinomio $x^2 - x$ a coefficienti in Z_2 ha funzione polinomiale nulla, pur non essendo il polinomio nullo. Abbiamo cosí che in $Z_2[x]$ non vale il principio di identitá dei polinomi. \diamond

Nell'insieme $A[x]$ dei polinomi a coefficienti in A si possono definire un'operazione di *addizione* e una di *moltiplicazione* nel seguente modo. Se

$$a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \quad \text{e} \quad b(x) = b_0 + b_1x + b_2x^2 + \cdots + b_mx^m,$$

poniamo

$$a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots + (a_t + b_t)x^t,$$

ove t é il piú grande fra gli interi n e m , e

$$a(x)b(x) = \sum_{h=0}^{n+m} \left(\sum_{i+j=h} a_i b_j \right) x^h.$$

La struttura algebrica $A[x] = (A[x], +, \cdot)$ é un anello commutativo unitario, che si chiama *l'anello dei polinomi nell'indeterminata x a coefficienti in A* . E' facile verificare che A é sottoanello unitario di $A[x]$ e che A e $A[x]$ hanno la stessa unitá. Gli elementi di A si chiamano *polinomi costanti* o semplicemente *costanti*.

ESERCIZIO 7.3.5 *Provare che l'anello $A[x]$ é generato da A e da x .*

Osserviamo esplicitamente che la scelta del simbolo x usato per denotare l'indeterminata con cui abbiamo costruito $A[x]$ é del tutto arbitraria nel senso della seguente proposizione la cui dimostrazione lasciamo per esercizio al Lettore.

PROPOSIZIONE 7.3.6 *Siano $A[x]$ e $A[y]$ gli anelli dei polinomi a coefficienti in A nelle indeterminate x e y , rispettivamente. Allora l'applicazione*

$$\varphi : a_0 + a_1x + \cdots + a_nx^n \in A[x] \rightarrow a_0 + a_1y + \cdots + a_ny^n \in A[y]$$

é l'unico isomorfismo tra $A[x]$ e $A[y]$ tale che

$$\varphi(c) = c \quad \text{per ogni } c \in A \quad \text{e} \quad \varphi(x) = y.$$

Sia dunque A un anello commutativo unitario e $A[x]$ l'anello dei polinomi a coefficienti in A nell'indeterminata x . Le seguenti proprietá sono di facile verifica:

- $\deg(f) = \deg(-f)$.
- $f \neq -g \Rightarrow \deg(f + g) \leq \max\{\deg(f), \deg(g)\}$.
- $fg \neq 0 \Rightarrow \deg(fg) \leq \deg(f) + \deg(g)$.
- Siano f, g polinomi non nulli i cui parametri direttori non siano entrambi divisori dello zero. Allora é $fg \neq 0$ e

$$\deg(fg) = \deg(f) + \deg(g).$$

- Se A é un dominio di integritá, allora $A[x]$ é un dominio di integritá.

L'anello dei polinomi su A , specilmente quando A é un campo, presenta molte analogie con l'anello Z degli interi; alcune di queste sono evidenti nelle definizioni e nei risultati che seguono.

DEFINIZIONE 7.3.7 Siano $f, g \in A[x]$ con $g \neq 0$. Si dice che per la coppia (f, g) vale l'*algoritmo della divisione* se esiste in $A[x]$ un'unica coppia di polinomi (q, r) tali che

$$f = gq + r, \quad \text{con } r = 0 \text{ oppure } \deg(r) < \deg(g).$$

In queste ipotesi, q si dice *quoziente* e r *resto* della divisione fra f e g . ◇

PROPOSIZIONE 7.3.8 Siano $f, g \in A[x]$, $g \neq 0$ e il parametro direttore di g sia invertibile. Supponiamo che

$$f = gq + r, \quad \text{con } r = 0 \text{ oppure } \deg(r) < \deg(g)$$

e

$$f = gq' + r', \quad \text{con } r' = 0 \text{ oppure } \deg(r') < \deg(g).$$

Allora risulta $q = q'$ e $r = r'$.

DIMOSTRAZIONE. • $gq + r = gq' + r' \Rightarrow g(q - q') = r' - r$.

- $r \neq r' \Rightarrow q \neq q' \Rightarrow \deg(r' - r) = \deg(g) + \deg(q - q') \geq \deg(g)$ e $\deg(r' - r) \leq \max\{\deg(r'), \deg(r)\} < \deg(g)$, assurdo.
- $r = r' \Rightarrow g(q - q') = 0 \Rightarrow q - q' = 0 \Rightarrow q = q'$. ◇

TEOREMA 7.3.9 Siano $f, g \in A[x]$, $g \neq 0$ e il parametro direttore di g sia invertibile. Allora per la coppia (f, g) vale l'*algoritmo della divisione*.

DIMOSTRAZIONE. Supponiamo $\deg(f) = n$, $\deg(g) = m$ e poniamo

$$f = a_0 + a_1x + \dots + a_nx^n, \quad g = b_0 + b_1x + \dots + b_mx^m.$$

- I casi $f = 0$; $f \neq 0$ e $n < m$; $n = m = 0$ sono banali.
- Se supponiamo $n \geq m$ e $n > 0$, possiamo procedere per induzione su n ; abbiamo cosí :

$$\deg(a_nb_m^{-1}x^{n-m}g) = n \text{ e il parametro direttore di } (a_nb_m^{-1}x^{n-m}g) \text{ é } a_n$$

$$\Rightarrow f_1 = f - a_nb_m^{-1}x^{n-m}g \text{ ha grado minore di } n \text{ o é nullo}$$

$$\Rightarrow \text{per } (f_1, g) \text{ vale l'algoritmo della divisione}$$

$$\Rightarrow f_1 = gq_1 + r_1 \text{ con } \deg(r_1) < \deg(g) \text{ o } r_1 = 0 \Rightarrow$$

$$f = gq_1 + r_1 + a_nb_m^{-1}x^{n-m}g = g \underbrace{(q_1 + a_nb_m^{-1}x^{n-m})}_q + \underbrace{r_1}_r.$$

A questo punto l'asserto segue dalla proposizione precedente. ◇

COROLLARIO 7.3.10 Se K é un campo, l'*algoritmo della divisione* vale per ogni coppia di polinomi (f, g) con $g \neq 0$.

OSSERVAZIONE 7.3.11 Notiamo che, nel corso della dimostrazione della proposizione precedente, il procedimento usato per trovare il quoziente e il resto della divisione tra f e g non é altro che l' usuale *algoritmo della divisione*, noto al Lettore dalle scuole medie. Per esempio, la procedura per il calcolo del quoziente $q(x)$ e del resto $r(x)$ della divisione in $Q[x]$ tra i polinomi $f(x) = 3x^4 + x^3 + 2x^2 + 1$ e $g(x) = 2x^2 + 2x + 1$ puó essere sintetizzata nello schema della figura 7.2, dal quale ricaviamo

$$q(x) = \frac{3}{2}x^2 - x + \frac{5}{4}, \quad r(x) = -\frac{3}{2}x - \frac{1}{4}.$$

◇

Figura 7.2: Divisione tra polinomi

OSSERVAZIONE 7.3.12 L'algoritmo e lo schema ricordati nell' esempio precedente, in forza del teorema 7.3.9 valgono su un campo arbitrario. Per esempio, la procedura per il calcolo del quoziente $q(x)$ e del resto $r(x)$ della divisione in $Z_5[x]$ di $3x^4 + x^3 + 2x^2 + 1$ per $2x^2 + 2x + 1$ é formalmente la stessa che abbiamo usato in $Q[x]$; bisogna solo tener presente che questa volta

le operazioni sono quelle di Z_5 . Abbiamo così

$$\begin{array}{r} 3x^4 + x^3 + 2x^2 + 1 \\ \underline{3x^4 + 3x^3 + 4x^2} \\ 3x^3 + 3x^2 + 1 \\ \underline{3x^3 + 3x^2 + 4x} \\ x + 1 \end{array} : \frac{2x^2 + 2x + 1}{4x^2 + 4x}$$

e quindi

$$q(x) = 4x^2 + 4x, \quad r(x) = x + 1.$$

◇

TEOREMA 7.3.13 *Sia K un campo. Allora tutti gli ideali di $K[x]$ sono principali. Ne segue che $K[x]$ è un anello principale.*

DIMOSTRAZIONE. Sia I un ideale non nullo di $K[x]$ e sia g un polinomio di grado minimo in I . Se g è una costante, risulta $I = K[x] = (g)$ e quindi possiamo supporre $\deg(g) > 0$. Ovviamente, abbiamo

$$(g) \subseteq I.$$

D'altra parte, se $f \in I$, possiamo scrivere

$$f = gq + r, \quad \text{con } \deg(r) < \deg(g) \text{ o } r = 0 \text{ e } gq \in I.$$

Ne segue che

$$f - gq = r \in I,$$

e, essendo g di grado minimo in I , deve essere $r = 0$. Otteniamo così $f = gq \in (g)$, cioè

$$I \subseteq (g),$$

che è il nostro asserto.

◇

COROLLARIO 7.3.14 *Siano K un campo, I un ideale non banale di $K[x]$ e g un elemento di I . Allora risulta $I = (g)$ se, e soltanto se, g è un polinomio non nullo di grado minimo in I . Inoltre, i generatori di $I = (g)$ sono tutti e soli i polinomi del tipo kg , al variare di k in K^* .*

DEFINIZIONE 7.3.15 Il corollario precedente garantisce che, se K è un campo e I un ideale non banale di $K[x]$, allora esiste un unico polinomio monico che genera I . Tale polinomio si chiama *polinomio minimo* di I .

◇

ESERCIZIO 7.3.16 *Siano A e B anelli commutativi unitari isomorfi. Provare che $A[x]$ e $B[x]$ sono isomorfi.*

ESERCIZIO 7.3.17 *Sia A un anello commutativo unitario. Provare che $A[x]$ ha la stessa caratteristica di A .*

ESERCIZIO 7.3.18 *Provare che in $Z[x]$ i polinomi del tipo*

$$2a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

costituiscono un ideale.

ESERCIZIO 7.3.19 *Provare che in $Z[x]$ l'ideale (x) generato da x é primo ma non massimale.*

ESERCIZIO 7.3.20 *Provare che in $Q[x]$ l'ideale (x) generato da x é primo e massimale.*

ESERCIZIO 7.3.21 *Sia K un campo e si consideri l'insieme I di polinomi a coefficienti in K definito da*

$$I = \{a_0 + a_1x + \cdots + a_nx^n : a_0 + a_1 + \cdots + a_n = 0\}.$$

Provare che I é un ideale di $K[x]$ e trovare un generatore di I .

OSSERVAZIONE 7.3.22 Sia A un anello commutativo unitario. Poiché $A[x]$ é a sua volta un anello commutativo unitario, possiamo considerare l'anello $A[x][y]$ dei polinomi nell'indeterminata y a coefficienti in $A[x]$ e, analogamente, $A[y][x]$. Si prova senza difficoltà che la funzione

$$\varphi : \sum_{i=1}^n a_i(x)y^i \in A[x][y] \rightarrow \sum_{i=1}^n a_i(y)x^i \in A[y][x]$$

é l'unico isomorfismo di $A[x][y]$ su $A[y][x]$ tale che

$$\varphi(a(x)) = a(y) \text{ per ogni } a(x) \in A[x] \text{ e } \varphi(x) = y, \varphi(y) = x.$$

Gli anelli $A[x][y]$ e $A[y][x]$ possono dunque identificarsi mediante l'isomorfismo φ e, per tale motivo, si pone $A[x, y] := A[x][y]$. Tale anello si chiama *anello dei polinomi nelle indeterminate x, y a coefficienti in A* e un suo elemento generico può scriversi nella forma

$$\sum_{0 \leq i+j \leq m} a_{ij}x^i y^j,$$

con $a_{ij} \in A$ ed $m \in N_0$. ◇

L'osservazione appena fatta giustifica la seguente definizione.

DEFINIZIONE 7.3.23 Siano A un anello commutativo unitario ed $n > 1$ un intero. Si chiama *anello dei polinomi nelle indeterminate x_1, x_2, \dots, x_n a coefficienti in A* , e si denota con

$$A[x_1, x_2, \dots, x_n],$$

l'anello definito per induzione da

$$A[x_1, x_2, \dots, x_n] = A[x_1, x_2, \dots, x_{n-1}][x_n].$$

Un elemento generico di tale anello é del tipo

$$f(x_1, x_2, \dots, x_n) = \sum_{0 \leq j_1 + j_2 + \cdots + j_n \leq m} a_{j_1 j_2 \dots j_n} x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n}, \quad (7.5)$$

con $a_{j_1 j_2 \dots j_n} \in A$ ed $m \in N_o$. I polinomi del tipo

$$a_{j_1 j_2 \dots j_n} x_1^{j_1} x_2^{j_2} \dots x_n^{j_n}$$

si chiamano *monomi* e, se $a_{j_1 j_2 \dots j_n} \neq 0$, l'intero $j_1 + j_2 + \dots + j_n$ si dice *grado* del monomio. Il grado massimo dei monomi che compaiono nell'espressione (7.5) si chiama *grado* del polinomio $f(x_1, x_2, \dots, x_n)$ ⁴ e si denota con $deg(f)$. \diamond

ESERCIZIO 7.3.24 Sia A un dominio di integritá unitario. Provare che $A[x_1, x_2, \dots, x_n]$ é un dominio di integritá e che

$$f, g \in A[x_1, x_2, \dots, x_n], fg \neq 0 \Rightarrow deg(fg) = deg(f) + deg(g).$$

DEFINIZIONE 7.3.25 Siano K un campo e $f(x_1, x_2, \dots, x_n)$ un polinomio in n indeterminate a coefficienti in K . Possiamo allora considerare l'insieme

$$G_f = \{ \sigma \in S_n : f(x_1, x_2, \dots, x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) \},$$

che, come subito si prova, risulta un gruppo di permutazioni su N_n . Tale gruppo si chiama *gruppo delle simmetrie* di f ; si dice inoltre che f é *simmetrico*, o *invariante*, rispetto ad un gruppo di permutazioni G su N_n se risulta $G \leq G_f$. Quando accade che $G_f = S_n$, il polinomio f si dice *simmetrico*. \diamond

ESEMPIO 7.3.26 Il polinomio $x_1^2 + x_1 x_2 + x_2^2$ é simmetrico. Il polinomio

$$f(x_1, x_2, x_3, x_4) = x_1 x_2 + x_3 x_4$$

non é simmetrico e il suo gruppo delle simmetrie é

$$G_f = \{ 1, (1, 2), (3, 4), (1, 2)(3, 4), (1, 3)(2, 4), (1, 4)(2, 3), (1, 3, 2, 4), (1, 4, 2, 3) \}.$$

\diamond

ESEMPIO 7.3.27 I seguenti polinomi in n indeterminate a coefficienti in un campo K sono simmetrici:

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + \dots + x_n &= \sum_{i=1}^n x_i, \\ \sigma_2 &= x_1 x_2 + x_1 x_3 + \dots + x_{n-1} x_n &= \sum_{1 \leq i < j \leq n} x_i x_j, \\ \sigma_3 &= x_1 x_2 x_3 + x_1 x_2 x_4 + \dots + x_{n-2} x_{n-1} x_n &= \sum_{1 \leq i < j < k \leq n} x_i x_j x_k, \\ &\dots\dots\dots \\ \sigma_n &= x_1 x_2 \dots x_n; \end{aligned}$$

essi prendono il nome di *polinomi simmetrici elementari*. \diamond

⁴Si osservi che, a differenza di quanto accade per i polinomi in una sola indeterminata, può accadere che nella (7.5) vi sia piú di un monomio di grado massimo.

Riportiamo senza dimostrazione la proprietà fondamentale dei polinomi simmetrici elementari che, tra l'altro, giustifica anche l'aggettivo *elementare* usato per questi polinomi.

TEOREMA 7.3.28 *Siano K un campo e $f(x_1, x_2, \dots, x_n)$ un polinomio simmetrico a coefficienti in K . Allora esiste un unico polinomio*

$$f_s(x_1, x_2, \dots, x_n) \in K[x_1, x_2, \dots, x_n]$$

tale che

$$f(x_1, x_2, \dots, x_n) = f_s(\sigma_1, \sigma_2, \dots, \sigma_n).$$

ESEMPIO 7.3.29 Assegnato il polinomio simmetrico $f(x) = x_1^2 + x_1x_2 + x_2^2$, risulta

$$f_s(x_1, x_2) = x_1^2 - x_2;$$

infatti si ha:

$$f_s(\sigma_1, \sigma_2) = f_s(x_1 + x_2, x_1x_2) = (x_1 + x_2)^2 - x_1x_2 = x_1^2 + x_1x_2 + x_2^2 = f(x_1, x_2).$$

◇

ESERCIZIO 7.3.30 *Siano K un campo e $K_s[x_1, x_2, \dots, x_n]$ l'insieme dei polinomi simmetrici a coefficienti in K nelle indeterminate x_1, x_2, \dots, x_n . Provare che $K_s[x_1, x_2, \dots, x_n]$ è un sottoanello di $K[x_1, x_2, \dots, x_n]$ e che risulta*

$$K_s[x_1, x_2, \dots, x_n] = K[\sigma_1, \sigma_2, \dots, \sigma_n].$$

Provare, inoltre, che $K_s[x_1, x_2, \dots, x_n]$ non è un ideale di $K[x_1, x_2, \dots, x_n]$.

7.3.2 Estensioni quadratiche di Z

Sia A un sottoanello unitario del campo C dei numeri complessi e osserviamo che A è un dominio di integrità. Sia inoltre u un elemento non quadrato di A , cioè un elemento per cui non esiste alcun $x \in A$ tale che $x^2 = u$.

DEFINIZIONE 7.3.31 Sia \sqrt{u} un numero complesso il cui quadrato sia u . Si chiama *estensione quadratica di A ottenuta aggiungendo una radice quadrata \sqrt{u} di u* , e si denota con $A[\sqrt{u}]$, il sottoanello di C generato da $A \cup \{\sqrt{u}\}$, cioè

$$A[\sqrt{u}] = \{a + b\sqrt{u} \quad : \quad a, b \in A\}.$$

◇

DEFINIZIONE 7.3.32 Se $z = a + b\sqrt{u}$ è un elemento di $A[\sqrt{u}]$, l'elemento $\bar{z} = a - b\sqrt{u}$ si chiama *coniugato* di z . Il prodotto $n(z) = z\bar{z}$ si chiama *norma* di z .

◇

Poiché risulta

$$n(a + b\sqrt{u}) = (a + b\sqrt{u})(a - b\sqrt{u}) = a^2 - ub^2,$$

la norma di un elemento di $A[\sqrt{u}]$ è un elemento di A . Inoltre si ha:

- $\bar{a} = a \Leftrightarrow a \in A$;
- $n(a) = a^2 \Leftrightarrow a \in A$;
- $n(0) = 0$ e $n(1) = 1$;
- $n(z_1 z_2) = n(z_1)n(z_2)$.

PROPOSIZIONE 7.3.33 *Un elemento $z \in A[\sqrt{u}]$ è invertibile in $A[\sqrt{u}]$ se, e solo se, la norma $n(z)$ è invertibile di A . Inoltre, se A è un campo, allora $A[\sqrt{u}]$ è un campo.*

DIMOSTRAZIONE. Se z è invertibile in $A[\sqrt{u}]$, risulta

$$1 = n(1) = n(z z^{-1}) = n(z)n(z)^{-1},$$

cioè $n(z)$ è invertibile in A . Se $n(z)$ è invertibile in A , risulta

$$1 = n(z)n(z)^{-1} = z \bar{z} n(z)^{-1} = z (\bar{z} n(z)^{-1}),$$

cioè z è invertibile in $A[\sqrt{u}]$.

Per la seconda parte, basta osservare che, se A è un campo, la norma di un suo elemento $\neq 0$ non è nulla, altrimenti u sarebbe un quadrato in A . \diamond

OSSERVAZIONE 7.3.34 Il campo dei numeri complessi è l'estensione quadratica del campo reale ottenuta aggiungendo una radice quadrata di -1 . \diamond

OSSERVAZIONE 7.3.35 L'applicazione

$$c : z \in A[\sqrt{u}] \rightarrow \bar{z} \in A[\sqrt{u}]$$

è un automorfismo di $A[\sqrt{u}]$, che si chiama *coniugio*. È immediato verificare che c^2 è l'identità e che c fissa tutti gli elementi di A . \diamond

PROPOSIZIONE 7.3.36 *Gli unici automorfismi di $A[\sqrt{u}]$ che fissano ogni elemento di A sono il coniugio e l'automorfismo identico.*

DIMOSTRAZIONE. Se f è un automorfismo del tipo richiesto e poniamo $v = \sqrt{u}$, abbiamo $u = v^2 = f(v^2) = f(v)^2$ e quindi

$$0 = v^2 - f(v)^2 = (v - f(v))(v + f(v)).$$

Ne segue che $v - f(v) = 0$ oppure $v + f(v) = 0$. Nel primo caso si ha subito che f è l'identità. Nel secondo caso abbiamo $f(v) = -v$ e quindi, per ogni $z = a + bv \in A[\sqrt{u}]$,

$$f(z) = f(a + bv) = f(a) + f(b)f(v) = a - bv = \bar{z};$$

ne segue che f è il coniugio. \diamond

COROLLARIO 7.3.37 *Gli unici automorfismi del campo complesso che fissano ogni elemento del campo reale sono il coniugio e l'automorfismo identico.*

DEFINIZIONE 7.3.38 Denotata con $i = \sqrt{-1}$ l'unità immaginaria di C , la estensione quadratica

$$Z[i] = \{a + bi \quad : \quad a, b \in Z\}$$

si chiama *anello degli interi di Gauss*. ◇

7.3.3 L'anello degli endomorfismi di un gruppo abeliano

Sia G un gruppo abeliano additivo e si denoti con $End(G)$ l'insieme di tutti gli endomorfismi di G . In $End(G)$ si definiscono una operazione di addizione e una di moltiplicazione nel seguente modo:

$$(f + g)(a) = f(a) + g(a) \quad e \quad (fg)(a) = f(g(a)),$$

per ogni $f, g \in End(G)$ e per ogni $a \in G$. Rispetto a tali operazioni $End(G)$ risulta un anello unitario che si chiama *l'anello degli endomorfismi di G* . L'unità di $End(G)$ é la permutazione identica su G .

ESERCIZIO 7.3.39 *Verificare se $End(G)$ é commutativo.*

7.3.4 Il corpo dei quaternioni

Nell'anello delle matrici $M_4(R)$ si consideri l'insieme

$$H = \{a + bi + cj + dk \quad : \quad a, b, c, d \in R\},$$

con

$$1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, i = \begin{bmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{bmatrix},$$

$$j = \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}, k = \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Un elemento di H si chiama *quaternione* ed é una matrice del tipo

$$\begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix},$$

ove a, b, c, d sono numeri reali.

Si verifica che H é un sottoanello non commutativo di $M_4(R)$. Tale sottoanello risulta un sottocorpo e prende il nome di *corpo dei quaternioni*.

In H valgono le seguenti proprietà :

$$i^2 = j^2 = k^2 = -1,$$

$$ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j.$$

OSSERVAZIONI 7.3.40 • La regola per moltiplicare due quaternioni é la seguente:

$$(a + ib + jc + kd)(a' + ib' + jc' + kd') =$$

$$(aa' - bb' - cc' - dd') + i(ab' + ba' + cd' - dc') +$$

$$j(ac' - bd' + ca' + db') + k(ad' + bc' - cb' + da').$$

- Si chiama *coniugato* di $\alpha = a + ib + jc + kd$ il quaternione $\bar{\alpha} = a - ib - jc - kd$.
- Sia $\alpha = a + ib + jc + kd$. Il prodotto $\alpha\bar{\alpha}$, che si denota con $\|\alpha\|$, si chiama la *norma* di α e risulta $\|\alpha\| = a^2 + b^2 + c^2 + d^2$.
- Il corpo dei quaternioni H contiene il campo C dei numeri complessi e quindi il campo R dei numeri reali. Precisamente si ha:

$$C = \{a + ib + jc + kd \in H : c = d = 0\},$$

$$R = \{a + ib + jc + kd \in H : b = c = d = 0\}.$$

- Nel corpo H dei quaternioni, ogni numero reale é permutabile (rispetto al prodotto) con ciascuno dei quaternioni i, j, k .

- Il corpo dei quaternioni é isomorfo a $(R^4, +, \cdot)$, ove l'addizione é definita componente per componente e la moltiplicazione é definita da

$$(a, b, c, d)(a', b', c', d') =$$

$$(aa' - bb' - cc' - dd', ab' + ba' + cd' - dc', ac' - bd' + ca' + db', ad' + bc' - cb' + da').$$

◇

OSSERVAZIONE 7.3.41 Storicamente il corpo dei quaternioni é stato il primo esempio di corpo *non commutativo*. Esso fu scoperto nel 1843 dal matematico irlandese William R. Hamilton dopo che lo stesso aveva cercato invano di definire un campo sulle terne ordinate di numeri reali (*ternioni*) che contenesse il campo complesso. In effetti un tale campo non esiste, come é provato dalla proposizione che segue. ◇

PROPOSIZIONE 7.3.42 (il campo dei ternioni non esiste!) *Non esiste un corpo avente come sostegno l'insieme*

$$\{a + ib + jc \quad : \quad a, b, c \in R\}$$

nel quale l'addizione é definita da

$$(a + ib + jc) + (a' + ib' + jc') = a + a' + i(b + b') + j(c + c')$$

e la moltiplicazione gode delle seguenti propriet a:

$$i^2 = j^2 = -1, \quad ai = ia, \quad aj = ja, \quad \text{per ogni } a \in R.$$

DIMOSTRAZIONE. Se un tale corpo esistesse avremmo:

- $ij = r + si + tj$ con $r, s, t \in R$.
- $i(ij) = (ii)j = -j$.
- $-j = i(r + si + tj) = ri - s + tij$
 $= -s + ri + t(r + si + tj) = -s + ri + tr + tsi + t^2j$
 $= (tr - s) + (r + ts)i + t^2j \Rightarrow$
 $tr - s = 0, \quad r + ts = 0, \quad t^2 = -1,$

l'ultima uguaglianza dá un assurdo perch e t é un numero reale. ◊

Figura 7.3: W.R.Hamilton (1805-1865)

7.3.5 Anelli di funzioni

Se A é un anello e X un insieme non vuoto, denotiamo con $H(X, A)$ l'insieme di tutte le funzioni di X in A . Si definiscano in $H(X, A)$ una operazione di *addizione* e una di *moltiplicazione* nel seguente modo:

$$(f + g)(x) = f(x) + g(x) \quad \text{e} \quad (fg)(x) = f(x)g(x),$$

per ogni $f, g \in H(X, A)$ e $x \in X$. La struttura algebrica $H(X, A) = (H(X, A), +, \cdot)$ é un anello che si chiama *anello delle funzioni* di X in A .

ESERCIZIO 7.3.43 *Provare che $H(X, A)$ é commutativo (risp. unitario) se, e solo se, A é commutativo (risp. unitario). Nel caso A sia unitario, dire qual é l'unitá di $\text{Hom}(X, A)$.*

DEFINIZIONE 7.3.44 Nel caso $A = Z_2$, si chiama *supporto* di una funzione $f \in H(X, Z_2)$ il sottoinsieme di X definito da

$$\text{supp}(f) = \{a \in X : f(a) = 1\}$$

e la funzione

$$f \in H(X, Z_2) \rightarrow \text{supp}(f) \in P(X)$$

risulta biunivoca. Se Y é un sottoinsieme di X , l' unica funzione $f \in H(X, Z_2)$ tale che $Y = \text{supp}(f)$ si chiama *funzione caratteristica* di Y . \diamond

ESERCIZIO 7.3.45 *Sia A un anello. Provare che, per ogni $a \in A$, l'applicazione*

$$\Phi_a : f \in H(A, A) \rightarrow f(a) \in A$$

é un omomorfismo (omomorfismo di valutazione) fra gli anelli $H(A, A)$ e A .

7.3.6 Somma diretta di anelli

Siano A_1, A_2, \dots, A_m anelli e si consideri il prodotto cartesiano A dei loro sostegni, cioè

$$A = A_1 \times A_2 \times \dots \times A_m.$$

Si definiscano in A le seguenti operazioni di *addizione* e *moltiplicazione*:

$$(a_1, a_2, \dots, a_m) + (b_1, b_2, \dots, b_m) = (a_1 + b_1, a_2 + b_2, \dots, a_m + b_m),$$

$$(a_1, a_2, \dots, a_m)(b_1, b_2, \dots, b_m) = (a_1 b_1, a_2 b_2, \dots, a_m b_m),$$

per ogni $(a_1, a_2, \dots, a_m), (b_1, b_2, \dots, b_m) \in A$. La struttura algebrica $A = (A, +, \cdot)$ é un anello che si chiama *somma diretta* di A_1, A_2, \dots, A_m e si denota con

$$A_1 \oplus A_2 \oplus \dots \oplus A_m.$$

A volte, invece di somma diretta di anelli, si parla di *prodotto diretto*. In questo caso, invece di usare la notazione $A_1 \oplus A_2 \oplus \dots \oplus A_m$, si usa $A_1 \times A_2 \times \dots \times A_m$.

ESERCIZIO 7.3.46 *Siano A un anello unitario e f l'applicazione di A in $A \oplus A$ definita da $f(a) = (a, 0)$, per ogni $a \in A$. Provare che f é un omomorfismo. Provare inoltre che l'anello $A \oplus A$ é unitario e che f non trasforma l'unitá di A nell'unitá di $A \oplus A$.*

ESERCIZIO 7.3.47 *Sia $A = A_1 \oplus A_2 \oplus \dots \oplus A_m$ la somma diretta degli anelli A_1, A_2, \dots, A_m . Provare che valgono le seguenti proprietá:*

- A é commutativo \Leftrightarrow Ogni A_j é commutativo.
- A é unitario \Leftrightarrow Ogni A_j é unitario.

Nell'ipotesi che A sia unitario, caratterizzare gli elementi invertibili di A .

7.3.7 Tabella riassuntiva di anelli

PROPRIETA' DI ALCUNI ANELLI

Anello	Forma degli elementi	Unitá	Commutativo	Dominio di integritá	Campo	Caratteristica
Z	n	1	si	si	no	0
Z_m , m non primo	n	1	si	no	no	m
Z_p , p primo	n	1	si	si	si	p
$Z[x]$	$a_0 + a_1x + \dots + a_nx^n$	1	si	si	no	0
mZ , $m > 1$	mn	nessuna	si	no	no	0
$M_2(Z)$	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	no	no	no	0
$M_2(2Z)$	$\begin{bmatrix} 2a & 2b \\ 2c & 2d \end{bmatrix}$	nessuna	no	no	no	0
$Z[i] = Z[\sqrt{-1}]$	$a + ib$	1	si	si	no	0
$Q[\sqrt{2}]$	$a + b\sqrt{2}$	1	si	si	si	0
H	$a + bi + jc + kd$	1	no	si	no	0
$Z \oplus Z$	(a, b)	$(1, 1)$	si	no	no	0

7.4 Esercizi

7.4.1 Provare che le matrici

$$a = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

sono elementi nilpotenti dell'anello $M_2(R)$ e che $a+b$ non é nilpotente. Dedurne che gli elementi nilpotenti di un anello non formano, in generale, un ideale.

7.4.2 Sia A un anello commutativo e siano a, b due suoi elementi nilpotenti tali che $a^n = b^m = 0$, con n, m interi positivi. Provare che $(a-b)^{n+m} = 0$ e che $(ca)^n = 0$, per ogni $c \in A$. Dedurne che gli elementi nilpotenti di un anello commutativo formano un ideale.

7.4.3 Provare che, se il gruppo additivo di un anello é ciclico, allora l'anello é commutativo.

7.4.4 Provare che l'insieme delle matrici diagonali di $M_n(Z)$ é un sottoanello di $M_n(Z)$.

7.4.5 Provare che l'insieme

$$\left\{ \begin{pmatrix} a & a-b \\ a-b & b \end{pmatrix} : a, b \in Z \right\}$$

é un sottoanello di $M_2(Z)$.

7.4.6 Siano K un campo e $S_2(K)$ l'insieme delle matrici su K del tipo

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Provare che $S_2(K)$ é un sottoanello di $M_2(K)$. Provare inoltre che, nel caso $K = R$, $S_2(R)$ é un sottocampo di $M_2(R)$ isomorfo al campo dei numeri complessi.

7.4.7 Siano $K = Z_3$ e $S_2(K)$ il campo definito nell'esercizio precedente. Provare che $S_2(K)$ ha ordine 9, che il suo gruppo additivo non é ciclico e che il suo gruppo moltiplicativo é ciclico.

7.4.8 Nell'anello $M_2(R)$ si consideri il seguente sottoinsieme:

$$K = \left\{ a \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + b \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} : a, b \in R \right\}.$$

Provare che K é un sottocampo di $M_2(R)$.

7.4.9 Sull'insieme $A = R \times R$ si definiscano un'operazione di addizione "+" e una di moltiplicazione "·" nel seguente modo:

$$(a, b) + (c, d) = (a + c, b + d), \quad (a, b) \cdot (c, d) = (ac, bd),$$

per ogni $a, b, c, d \in R$. Provare che $(A, +, \cdot)$ é un anello commutativo unitario e trovare gli elementi invertibili di A .

7.4.10 Sull'insieme $H(R, R)$ di tutte le funzioni di R in R si definiscano un'operazione di addizione "+" e una di moltiplicazione "." nel seguente modo:

$$(f + g)(a) = f(a) + g(a), \quad (f \cdot g)(a) = f(a)g(a),$$

per ogni $f, g \in \text{Hom}(R, R)$ e $a \in R$. Provare che $(H(R, R), +, \cdot)$ é un anello commutativo unitario.

7.4.11 Per ogni numero reale t , si consideri in $M_2(R)$ il sottoinsieme $M_2(t)$ costituito da tutte le matrici del tipo

$$\begin{pmatrix} a + b & b \\ tb & a \end{pmatrix},$$

con $a, b \in R$. Provare che, per ogni t , $M_2(t)$ é un sottoanello unitario di $M_2(R)$ avente la stessa unita di $M_2(R)$. Calcolare, inoltre, i valori di t per cui ogni elemento non nullo di $M_2(t)$ é invertibile.

7.4.12 In $M_2(R)$ si consideri il sottoinsieme A costituito da tutte le matrici del tipo

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix},$$

con $a \in R$. Provare che A é un sottoanello unitario di $M_2(R)$ avente unita diversa da quella di $M_2(R)$. Provare, inoltre, che ogni elemento non nullo di A non é invertibile in $M_2(R)$ ed é invertibile in A .

7.4.13 Siano A un anello unitario ed a un suo elemento tale che $a^2 = 1$. Provare che $X = \{axa : x \in A\}$ é un sottoanello di A e che $1 \in X$.

7.4.14 Trovare una condizione necessaria e sufficiente affinché risulti

$$a^2 - b^2 = (a + b)(a - b),$$

ove a, b sono elementi di un anello.

7.4.15 Controllare la correttezza delle seguenti implicazioni in un anello unitario:

$$a^2 = 1 \Rightarrow (a^2 - 1) = (a + 1)(a - 1) = 0 \Rightarrow a = 1 \text{ o } a = -1.$$

7.4.16 Trovare tutti gli elementi invertibili dell'anello $M_2(\mathbb{Z}_2)$.

7.4.17 Trovare un esempio di anello contenente due divisori dello zero, a e b , tali che $a + b$ non é un divisore dello zero.

7.4.18 Sia A un anello commutativo tale che $aA = A$, per ogni elemento $a \in A$. Provare che A é un campo.

7.4.19 Provare mediante qualche esempio che l'intersezione di due ideali primi in un anello non é necessariamente un ideale primo.

7.4.20 Siano H, K ideali bilateri di un anello A . Provare che $ab \in H \cap K$, per ogni $a \in H$ e $b \in K$.

7.4.21 Calcolare il coefficiente e il grado di $36x^2$ considerato come polinomio in y nei seguenti casi:

$$y = 2x, \quad y = x^2, \quad y = 3x^2, \quad y^2 = x, \quad y^3 = 2x.$$

7.4.22 Trovare una classe infinita di anelli di polinomi che non sono domini di integritá.

7.4.23 Trovare il quoziente e il resto della divisione di $f(x)$ per $g(x)$, $f, g \in R[x]$, nei seguenti casi:

$$\begin{array}{ll} f(x) = 2x^2 - 3x + 4, & g(x) = 3x - 2; \\ f(x) = x^2 - 3x + 4, & g(x) = x - 2; \\ f(x) = x^3 - 5x^2 + 7x + 11, & g(x) = x^2 - x + 1; \\ f(x) = x^4 + 3x^2 - 2x^2 + 2x - 1, & g(x) = 3x^2 - 2x + 5; \\ f(x) = (1 - \sqrt{2})x^3 + (1 + \sqrt{2})x^2 + \sqrt{2}, & g(x) = (1 + \sqrt{2})x^2 + (2 - \sqrt{2}). \end{array}$$

7.4.24 Siano A, B anelli commutativi unitari e $f : A \rightarrow B$ un isomorfismo di A su B . Provare che l' applicazione

$$\varphi : \sum a_i x^i \in A[x] \rightarrow \sum f(a_i) y^i \in A[y]$$

é l' unico isomorfismo di $A[x]$ su $B[y]$ tale che

$$\varphi(c) = f(c) \text{ per ogni } c \in A \text{ e } \varphi(x) = y.$$

7.4.25 Determinare il gruppo degli elementi invertibili dell'anello $Z[i]$ degli interi di Gauss.

7.4.26 Siano $A = Z \oplus Z \oplus Z$ e $X = \{(a, b, c) \in A : a + b = c\}$. Verificare se X é un sottoanello di A .

7.4.27 Provare che la somma diretta di due domini di integritá non é un dominio di integritá.

7.4.28 Provare che nell'anello $Z \oplus Z$ l'insieme

$$I = \{(n, 0) : n \in Z\}$$

é un ideale primo, ma non massimale.

7.5 Appendice

7.5.1 Polinomi e serie formali

Nel paragrafo 7.3.1 abbiamo definito i polinomi nella indeterminata x come delle espressioni formali del tipo

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

ove gli a_j sono elementi di un anello commutativo unitario, senza preoccuparci di precisare la natura di x . In effetti l'indeterminata x e le sue potenze giocano un ruolo del tutto inessenziale; il loro uso nella definizione di polinomio serve soltanto ad assegnare un ordine lineare ai coefficienti del polinomio stesso. Questo significa che una definizione rigorosa di polinomio deve poter prescindere dalla indeterminata ed é appunto questo quello che mostreremo nel presente paragrafo.

Sia dunque A un anello commutativo unitario e denotiamo con \hat{A} l'insieme di tutte le successioni di elementi di A *definitivamente nulle*, cioè le successioni del tipo

$$\underline{a} = (a_0, a_1, \dots, a_n, \dots) = (a_n)_{n \in N_0}$$

per cui esiste un intero $m \in N_0$ tale che $a_n = 0$, per ogni $n \geq m$.

In \hat{A} si possono definire un'operazione di *addizione* e una di *moltiplicazione* (detta anche *convoluzione*) nel modo seguente. Se

$$\underline{a} = (a_n)_{n \in N_0} \quad \text{e} \quad \underline{b} = (b_n)_{n \in N_0}$$

sono elementi di \hat{A} , poniamo

$$\underline{a} + \underline{b} = (a_n + b_n)_{n \in N_0} \tag{7.6}$$

e

$$\underline{a} \underline{b} = \left(\sum_{i+j=n} a_i b_j \right)_{n \in N_0} = (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots). \tag{7.7}$$

La struttura algebrica $\hat{A} = (\hat{A}, +, \cdot)$ risulta un anello commutativo unitario nel quale lo zero é

$$\underline{0} = (0, 0, \dots, 0, \dots),$$

l'unitá é

$$\underline{1} = (1, 0, 0, \dots, 0, \dots)$$

e l'opposto di un elemento $\underline{a} = (a_n)_{n \in N_0}$ é

$$-\underline{a} = (-a_n)_{n \in N_0}.$$

L'applicazione

$$i : a \in A \rightarrow (a, 0, 0, \dots, 0, \dots) \in \hat{A}$$

é iniettiva e verifica le seguenti proprietà:

- $i(a + b) = i(a) + i(b)$,

- $i(ab) = i(a)i(b)$,
- $i(a) = \underline{0} \Leftrightarrow a = 0$,
- $i(1) = \underline{1}$;

essa é dunque un *monomorfismo* che conserva l'unitá e quindi $i(A)$ é un sottoanello di \hat{A} isomorfo ad A . Possiamo quindi identificare gli elementi di A e di $i(A)$ mediante il monomorfismo i e cosí A puó pensarsi come sottoanello di \hat{A} . In quest' ordine di idee useremo la notazione

$$a = (a, 0, 0, \dots, 0, \dots).$$

Se ora poniamo

$$x = (0, 1, 0, 0, \dots), \tag{7.8}$$

abbiamo:

$$\begin{aligned} x^2 &= xx = (0, 0, 1, 0, 0, \dots), \\ x^3 &= x^2x = (0, 0, 0, 1, 0, 0, \dots), \\ &\dots\dots\dots \\ x^n &= x^{n-1}x = (\underbrace{0, 0, \dots, 0}_n, 1, 0, 0, \dots) \end{aligned}$$

e, per ogni $a \in A$,

$$ax^n = (a, 0, 0, \dots, 0, \dots)(\underbrace{0, 0, \dots, 0}_n, 1, 0, 0, \dots) = (\underbrace{0, 0, \dots, 0}_n, a, 0, 0, \dots). \tag{7.9}$$

Allora, per ogni $\underline{a} \in \hat{A}$, si ha

$$\begin{aligned} &(a_o, a_1, a_2, \dots, a_n, 0, 0, \dots) = \\ &(a_o, 0, 0, \dots) + (0, a_1, 0, 0, \dots) + \dots + (0, \dots, 0, a_n, 0, \dots) = \\ &a_o + a_1x + a_2x^2 + \dots + a_nx^n. \end{aligned}$$

Inoltre, se a_n e b_m sono non nulli ed é $n \leq m$, allora valgono le seguenti implicazioni:

$$\begin{aligned} a_o + a_1x + a_2x^2 + \dots + a_nx^n &= b_o + b_1x + b_2x^2 + \dots + b_mx^m \\ \Rightarrow (a_o, a_1, a_2, \dots, a_n, 0, 0, \dots) &= (b_o, b_1, b_2, \dots, b_m, 0, 0, \dots) \\ \Rightarrow a_o = b_o, a_1 = b_1, \dots, a_n = b_n, &a_i = b_i = 0 \text{ per ogni } i > n. \end{aligned}$$

Ne segue che un elemento $\underline{a} = (a_m) \in \hat{A}$, con $a_n \neq 0$ e $a_m = 0$ per ogni $m > n$, si scrive in un unico modo nella forma

$$\underline{a} = a_o + a_1x + a_2x^2 + \dots + a_nx^n,$$

cióe come combinazione lineare a coefficienti in A di un numero finito di elementi dell'insieme

$$\{1 = x^0, x, x^2, \dots, x^n, \dots\}.$$

A questo punto é chiaro che l'anello \hat{A} é canonicamente isomorfo all'anello dei polinomi $A[x]$ (come costruito nel capitolo precedente) e quindi lo stesso \hat{A} puó assumersi come *definizione* dell'anello dei polinomi su A , eliminando ogni ambiguitá che potrebbe derivare dall' introduzione puramente formale dell' *indeterminata* x .

OSSERVAZIONE 7.5.1 Non dovrebbe essere difficile per il Lettore convincersi che trattare i polinomi come successioni definitivamente nulle, e quindi in qualche modo come successioni di lunghezza finita, é il modo migliore anche per implementare l'algebra polinomiale su una macchina calcolatrice. Per esempio, valutare su un elemento c un polinomio

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$$

equivale a passare dalla successione

$$(a_0, a_1, a_2, \dots, a_n)$$

alla successione

$$(a_0 + a_1c + a_2c^2 + \cdots + a_nc^n, 0, 0, \dots, 0).$$

◇

DEFINIZIONE 7.5.2 Sia A un anello commutativo unitario e denotiamo con \bar{A} l'insieme di tutte le successioni di elementi di A . Allora \bar{A} può strutturarsi ad anello commutativo unitario definendo in esso un'operazione di addizione mediante la (7.6) e una di moltiplicazione mediante la (7.7). Tale anello contiene \hat{A} come sottoanello e l'unità di \bar{A} coincide con quella di \hat{A} . Le (7.8) e (7.9) suggeriscono di porre formalmente

$$(a_0, a_1, \dots, a_n, \dots) = \sum_{n=0}^{\infty} a_n x^n$$

e, per tale motivo, gli elementi di \bar{A} si chiamano *serie formali a coefficienti in A* ⁵. L'anello \bar{A} si dice *anello delle serie formali a coefficienti in A* e si denota con $A[[x]]$. ◇

PROPOSIZIONE 7.5.3 Siano K un campo e

$$A(x) = \sum_{n=0}^{\infty} a_n x^n$$

una serie formale a coefficienti in K . Allora $A(x)$ é invertibile in $K[[x]]$ se, e solo se, a_0 é diverso da zero. In particolare ogni polinomio a coefficienti in K con termine noto diverso da zero é invertibile in $K[[x]]$.

DIMOSTRAZIONE. Se $A(x)$ é invertibile in $K[[x]]$, esiste una serie formale

$$B(x) = \sum_{n=0}^{\infty} b_n x^n$$

tale che $A(x)B(x) = 1$, cioè

$$A(x)B(x) = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \dots) = (1, 0, 0, \dots),$$

⁵Si osservi che l'espressione $\sum_{n=0}^{\infty} a_n x^n$ é soltanto un simbolo e non il risultato di operazioni eseguite in \bar{A} .

da cui segue che $a_o b_o = 1$ e così $a_o \neq 0$.

Se supponiamo $a_o \neq 0$, possiamo considerare la serie formale $B(x)$ definendo i suoi coefficienti mediante la formula ricorrente

$$b_n = a_o^{-1}(-a_1 b_{n-1} - a_2 b_{n-2} - \cdots - a_n b_o)$$

con la condizione iniziale $b_o = a_o^{-1}$. Risulta allora $A(x)B(x) = 1$ e quindi $A(x)$ è invertibile in $K[[x]]$. \diamond

DEFINIZIONE 7.5.4 Se $f(x) \in K[x]$ è un polinomio a coefficienti nel campo K con termine noto diverso da zero, i simboli

$$\frac{1}{f(x)} \quad \text{e} \quad f^{-1}(x)$$

denotano la serie formale inversa di $f(x)$ in $K[[x]]$. \diamond

ESERCIZIO 7.5.5 Calcolare l'inverso $B(x)$ del polinomio $f(x) = 1 - x$ in $Q[[x]]$.

SOLUZIONE. Dobbiamo trovare la serie formale

$$B(x) = \sum_{n=0}^{\infty} b_n x^n$$

tale che

$$(1 - x)(b_o + b_1 x + b_2 x^2 + \cdots) = 1.$$

Allora deve essere $b_o = 1$ e $b_n - b_{n-1} = 0$, per ogni intero $n > 1$. Ne segue che

$$B(x) = \frac{1}{1 - x} = 1 + x + x^2 + x^3 + \cdots = \sum_{n=0}^{\infty} x^n.$$

\diamond