# Introduzione alle strutture algebriche
# S.I.S.S. Firenze - 2007

Carlo Casolo
Dipartimento di Matematica "Ulisse Dini",
Università di Firenze,
casolo@math.unifi.it

# Indice

# Capitolo 1

# Semigruppi e Gruppi

## 1.1 Operazioni binarie.

Sia $A$ un insieme non vuoto. Una **operazione binaria**, o legge di composizione, su $A$ è un'applicazione

$$A \times A \longrightarrow A.$$

Se $*$ è una operazione su $A$, per ogni $(a, b) \in A \times A$, sciveremo $a * b$ invece di $*((a, b))$.

---

*Nota.* La definizione che abbiamo dato è quella di un'operazione binaria *interna* - ovvero tale che il risultato della composizione di due elementi di $A$ è ancora un elemento di $A$. In matematica sono talvolta chiamate operazioni esterne quelle per cui il risultato delle composizioni appartiene ad un altro insieme: il tipico esempio è, per chi lo conosce, il cosiddetto prodotto scalare di vettori. Un altro tipo di estensione dl concetto di operazione è quello di *operazione n-aria*: dato $n \geq 1$, un'operazione $n$-aria dell'insieme $A$ è una applicazione dall'insieme delle $n$-uple ordinate di $A$ in $A$ (quindi un'operazione 1-aria è una qualsiasi applicazione $A \longrightarrow A$)

---

### 1.1.1 Semigruppi e Monoidi.

Dalla definizione, risulta che su un insieme non vuoto $A$ è possibile definire un gran numero di operazioni. La maggior parte di esse è tuttavia scarsamente importante (secondo il punto di vista delle strutture algebriche). La proprietà fondamentale che, in genere, esclude operazioni poco interessanti, o di difficile studio, è la cosiddetta *associatività*.

Un'operazione $*$ sull'insieme $A$ si dice **associativa** se, per ogni $a, b, c \in A$ risulta: *associatività*

$$(a * b) * c = a * (b * c).$$

**Esempi.** Sono operazioni "interessanti" (oltre che naturali) quelle usuali di - somma e di prodotto sugli insiemi $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. La sottrazione, nel significato usuale, è una operazione su $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ e $\mathbb{C}$, ma non è una operazione su $\mathbb{N}$, dato che la differenza di due numeri interi non è, in genere, un numero intero. Tranne il caso della sottrazione (dove essa è definita), tutte queste operazioni sono associative.

*semigruppi*

Per **semigruppo** si intende una coppia $(A, \cdot)$ dove $A$ è un insieme non vuoto, e $\cdot$ è un'operazione associativa su $A$.

*Osservazione importante.* Se $(A, \cdot)$ è un semigruppo, allora, per ogni $a, b, c \in A$ possiamo scrivere senza ambiguità

$$a \cdot b \cdot c$$

intendendo con ciò l'elemento $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. Questa osservazione si estende ad una stringa finita qualunque di elementi di $A$. Ad esempio se $a_1, a_2, a_3, a_4 \in A$, allora:

$$a_1 \cdot ((a_2 \cdot (a_3 \cdot a_4)) = a_1 \cdot ((a_2 \cdot a_3) \cdot a_4)) = a_1 \cdot (a_2 \cdot a_3 \cdot a_4) = (a_1 \cdot a_2) \cdot (a_3 \cdot a_4) = (a_1 \cdot a_2 \cdot a_3) \cdot a_4 = \text{ etc.}$$

elemento che scriviamo semplicemente: $a_1 \cdot a_2 \cdot a_3 \cdot a_4$ .

Più in generale, per ogni $n \geq 1$ e $a_1, a_2, \ldots, a_n \in A$ , possiamo individuare senza ambiguità l'elemento

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n \ .$$

*commutatività*

Una operazione $*$ sull'insieme $A$ si dice **commutativa** se, per ogni $a, b \in A$ risulta:

$$a * b = b * a.$$

Non si dà un nome particolare ad un insieme dotato di operazione commutativa. Se $(A, \cdot)$ è un semigruppo e l'operazione è commutativa, si dice che $(A, \cdot)$ è un semigruppo commutativo.

**Esempi**. Sono commutative le operazioni di somma e moltiplicazione in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$, mentre (dove è definita) non è commutativa la sottrazione. La composizione di applicazioni o il prodotto righe×colonne tra matrici (vedi §1.3.6) sono gli esempi fondamentali di operazioni associative ma non commutative.

---

*Esercizio.* Su $\mathbb{Z} \times \mathbb{Z}$ si definisca l'operazione $*$ ponendo, per ogni $(x, y), (x_1, y_1) \in \mathbb{Z} \times \mathbb{Z}$, $(x, y) * (x_1, y_1) = (x, y_1)$. Si dica se $(\mathbb{Z} \times \mathbb{Z}, *)$ è un semigruppo. Si dica se è commutativo.

*Soluzione.* Siano $(x, y), (x_1, y_1), (x_2, y_2) \in \mathbb{Z} \times \mathbb{Z}$. Allora

$$\begin{aligned}(x, y) * ((x_1, y_1) * (x_2, y_2)) = (x, y) * (x_1, y_2) = (x, y_2) = \\ = (x, y_1) * (x_2, y_2) = ((x, y) * (x_1, y_1)) * (x_2, y_2)\end{aligned}$$

dunque l'operazione $*$ è associativa e $(\mathbb{Z}\times\mathbb{Z},*)$ è un semigruppo. Non è commutativo perché, ad esempio, $(1,2)*(2,1)=(1,1)\neq(2,2)=(2,1)*(1,2)$.

---

**Caso importante.** Se $X$ è un insieme non vuoto, allora la *composizione* $\circ$ è una operazione sull'insieme $X^X$ di tutte le applicazioni di $X$ in se stesso. La composizione è anche una operazione sull'insieme $Sym(X)$ di tutte le applicazioni biettive di $X$ in se stesso; infatti la composizione di due applicazioni biettive è biettiva. *Sym(X)*

---

*Nota.* Se $|X|\geq 2$ la composizione in $X^X$ non è commutativa. Infatti siano $a,b$ elementi distinti di $X$ e si considerino le applicazioni $f,g:X\to X$ definite da

$$f(x)=a \text{ per ogni } x\in X \quad \text{e} \quad g(x)=b \text{ per ogni } x\in X\ ;$$

allora $(f\circ g)(a)=f(g(a))=f(b)=a$, mentre $(g\circ f)(a)=g(f(a))=g(a)=b$. Quindi $f\circ g\neq g\circ f$.
Se $|X|\geq 3$ la composizione in $Sym(X)$ non è commutativa. Infatti siano $a,b,c$ elementi distinti di $X$; si considerino le permutazioni $\sigma,\tau : X\to X$ definite da

$$\sigma(a)=b\ ,\ \sigma(b)=a\ ,\ \sigma(x)=x \text{ per ogni altro } x\in X$$

$$\tau(a)=c\ ,\ \tau(c)=a\ ,\ \tau(x)=x \text{ per ogni altro } x\in X$$

e si provi che $\sigma\circ\tau\neq\tau\circ\sigma$.

---

Sia $\cdot$ una operazione sull'insieme $A$. Un sottoinsieme $B$ di $A$ si dice **chiuso** (rispetto a $\cdot$) se, per ogni $b,b'\in B$ risulta $b\cdot b'\in B$. *sottoinsiemi chiusi*

Se $B$ è un sottoinsieme chiuso, allora si può definire su $B$ l'operazione $\cdot$ *indotta* da $A$ (cioè quella definita dalla restrizione della operazione $A\times A\longrightarrow A$ ad una operazione $B\times B\longrightarrow B$, dove la regola che determina il prodotto rimane la stessa). Ovviamente se l'operazione su $A$ è associativa (commutativa), anche l'operazione indotta su un sottoinsieme chiuso è tale. Una proprietà elementare ma importante dei sottoinsiemi chiusi è che l'intersezione di due o più di essi è ancora un sottoinsieme chiuso.

**Esempi** L'insieme $2\mathbb{Z}$ dei numeri interi pari è un sottoinsieme chiuso di $(\mathbb{Z},+)$ e di $(\mathbb{Z},\cdot)$, mentre l'insieme dei numeri dispari è chiuso in $(\mathbb{Z},\cdot)$ ma non in $(\mathbb{Z},+)$.

Sia $(A,\cdot)$ un semigruppo. Un elemento $e\in A$ si dice **elemento identico** (o identità, o elemento neutro) se, per ogni $a\in A:\ a\cdot e=a=e\cdot a$. *elem. identico*

**Proposizione 1.1.1.** *Sia $(A,\cdot)$ un semigruppo, e siano $e$, $e'$ elementi identici su $A$. Allora $e=e'$.*

*Dimostrazione.* Se $e$, $e'$ sono elementi identici, si ha:

$$e=e\cdot e'=e'$$

dove la prima uguaglianza sussiste perchè $e'$ è un elemento identico, e la seconda perchè $e$ è un elemento identico. ∎

*monoidi*

Dunque, se un semigruppo $(A, \cdot)$ ha un elemento identico, esso è unico. Lo si denota, in generale, con $1_A$. Un semigruppo dotato di elemento identico si dice **monoide**. Un monoide $(M, \cdot)$ si dice *commutativo* se l'operazione $\cdot$ è commutativa.

**Esempi.** 1) Sono monoidi i semigruppi $(\mathbb{N}, +)$ , $(\mathbb{Z}, +)$ , $(\mathbb{Q}, +)$ , $(\mathbb{R}, +)$ , $(\mathbb{C}, +)$ (l'elemento identico è 0); sono monoidi i semigruppi $(\mathbb{N}, \cdot)$ , $(\mathbb{Z}, \cdot)$ , $(\mathbb{Q}, \cdot)$ , $(\mathbb{R}, \cdot)$ , $(\mathbb{C}, \cdot)$ (l'elemento identico è 1)

2) Se $X$ è un insieme non vuoto, allora $(X^X, \circ)$ è un monoide, con identità l'applicazione identica $\iota_X$.

### 1.1.2 Inversi.

*inversi*

Passiamo ora all'importante questione dell'esistenza di "inversi" rispetto ad una data operazione. Il caso che ci può guidare (ma con un po' di attenzione, perché le operazioni interessanti non sempre sono commutative) è quello familiare delle operazioni di somma e prodotto: se $a$ è un numero (diciamo razionale) allora $-a$ è "l'inverso" di $a$ rispetto all'operazioone $+$ di somma, infatti $a + (-a) = 0$, e 0 è l'elemento neutro per la somma. Se invece consideriamo il prodotto (ovvero lavoriamo nel monoide moltiplicativo $(\mathbb{Q}^*, \cdot)$, dove $\mathbb{Q}^*$ è l'insieme dei numeri razionali non nulli), allora l'inverso di $a \in \mathbb{Q}^*$ è l'usuale innverso razionale $1/a$: infatti $a \cdot (1/a) = 1$, e 1 è l'elemento neutro di $(\mathbb{Q}^*, \cdot)$.

**Proposizione 1.1.2.** *Sia $(M, \cdot)$ un monoide con elemento identico $1_M$, e sia $a \in M$. Se $b, c$ sono elementi di $M$ tali che $ba = 1_M = ac$, allora $b = c$.*

*Dimostrazione.* Siano $a, b, c \in M$ come nelle ipotesi. Allora:

$$b = b \cdot 1_M = b(ac) = (ba)c = 1_M \cdot c = c$$

∎

---

*Nota.* Un elemento $b$ tale che $ba = 1_M$ si dice inverso sinistro di $a$; un elemento $c$ tale che $ac = 1_M$ si dice inverso destro di $a$. Mentre è possibile che un elemento di un monoide abbia diversi inversi sinistri o diversi inversi destri, la proposizione precedente implica che se un elemento $a$ di un monoide ha un inverso sinistro e un inverso destro allora questi coincidono (in tal caso $a$ ha, quindi, un unico inverso sinistro (che è anche l'unico inverso destro).

---

Sia $(M, \cdot)$ un monoide con elemento identico $1_M$. Un elemento $a \in M$ si dice **invertibile** se esiste $b \in M$ tale che

$$a \cdot b = 1_M = b \cdot a..$$

Per la proposizione 1.1.2, un tale $b$ è unico; si denota con $a^{-1}$, e si chiama l'**elemento inverso** di $a$ in $M$.

Osserviamo che l'elemento identico $1_M$ di un monoide $M$ è sempre invertibile, e coincide con il proprio inverso.

**Esempi.** 1) Gli elementi invertibili del monoide $(\mathbb{Z}, \cdot)$ sono 1 e -1, quindi $U(\mathbb{Z}, \cdot) = \{1, -1\}$. Gli elementi invertibili del monoide $(\mathbb{Q}, \cdot)$ sono tutti i numeri razionali diversi da 0, quindi $U(\mathbb{Q}, \cdot) = \mathbb{Q}^* = \mathbb{Q} \setminus \{0, \}$ (e similmente per $\mathbb{R}$ e $\mathbb{C}$).

2) Se $X$ è un insieme non vuoto, gli elementi invertibili di $(X^X, \circ)$ sono precisamente le applicazioni invertibili (ovvero biettive) $f : X \to X$. Quindi l'insieme degli elementi invertibili di $(X^X, \circ)$ è $Sym(X)$.

L'osservazione seguente mostra, in particolare, che l'insieme degli elementi invertibili di un monoide costituisce un sottoinsieme chiuso.

**Proposizione 1.1.3.** *Sia $(M, \cdot)$ un monoide con elemento identico $1_M$, e siano $a, b$ elementi invertibili di $M$. Allora* *proprietà degli inversi*

*(i) $a^{-1}$ è invertibile e $(a^{-1})^{-1} = a$ ;*

*(ii) $ab$ è invertibile e $(ab)^{-1} = b^{-1}a^{-1}$ .*

*Dimostrazione.* (i) Poichè $(a^{-1})a = 1_M = a(a^{-1})$, si ha che $a^{-1}$ è invertibile e, per l'unicità dell'inverso, $(a^{-1})^{-1} = a$.

(ii) Se $a$ e $b$ sono invertibili:

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}1_M b = b^{-1}b = 1_M \ ;$$

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1_M a^{-1} = aa^{-1} = 1_M$$

dunque $ab$ è invertibile e, per l'unicità dell'inverso, $(ab)^{-1} = b^{-1}a^{-1}$. ∎

---

*Esercizio.* Sull'insieme $\mathbb{Z}$ dei numeri interi si definisca l'operazione $*$ ponendo, per ogni $n, m \in \mathbb{Z}$ : $n * m = n + m - nm$. Si dimostri che $(\mathbb{Z}, *)$ è un monoide e si determinino gli elementi invertibili.

*Soluzione.* Verifichiamo che l'oerazione $*$ è associativa: siano $n, m, t \in \mathbb{Z}$, allora

$$\begin{aligned} n * (m * t) = n + (m * t) - n(m * t) = n + (m + t - mt) - n(m + t - mt) = \\ = (n + m - nm) + t - (n + m - nm)t = (n * m) * t. \end{aligned}$$

Proviamo ora che $0$ è l'elemento identico di $(\mathbb{Z}, *)$.Infatti, per ogni $n \in \mathbb{Z}$

$$n * 0 = n + 0 - n \cdot 0 = n = 0 * n.$$

Quindi $(\mathbb{Z}, *)$ è un monoide (commutativo). Supponiamo ora che $n \in \mathbb{Z}$ sia invertibile in $(\mathbb{Z}, *)$, allora esiste $n' \in \mathbb{Z}$ tale che

$$0 = n * n' = n + n' - nn'.$$

Quindi, deve essere che $n' = \frac{n}{n-1}$ appartiene a $\mathbb{Z}$; ciò si verifica solo per $n = 0, 2$. Pertanto, gli invertibili di $(\mathbb{Z}, *)$ sono 0 e 2, e (come si verifica immediatamente), coincidono con i loro inversi.

---

### 1.1.3 Esercizi.



**Esercizio 1.1.** Sia $S$ un insieme non vuoto. Si provi che l'operazione definita su $S$ da $(a, b) \mapsto a$ è associativa.

**Esercizio 1.2.** Siano $(A, \cdot)$, $(B, *)$ semigruppi. Sul prodotto diretto $A \times B$ si definisca una operazione ponendo, per ogni $(a, b), (a_1, b_1) \in A \times B$ :

$$(a, b)(a_1, b_1) = (a \cdot a_1, b * b_1) \ .$$

Si dimostri che, con tale operazione, $A \times B$ è un semigruppo. Si provi che se $A$ e $B$ sono monoidi (gruppi), allora $A \times B$ è un monoide (gruppo).

**Esercizio 1.3.** Sull'insieme $\mathbb{N}^*$ dei numeri naturali diversi da zero si definisca l'operazione $\tau$ ponendo, per ogni $n, m \in \mathbb{N}^* : \ n \tau m = MCD(n, m)$. Si dica se tale operazione è associativa e se esiste un elemento identico.

**Esercizio 1.4.** Sia $(S, \cdot)$ un semigruppo e siano $T, V$ sottoinsiemi chiusi di $S$. Sia $TV = \{ \ x \cdot y \mid x \in T \ \text{ e } \ y \in V \ \}$. Si dimostri che se $x \cdot y = y \cdot x$ per ogni $x \in T$ e $y \in V$, allora $TV$ è un sottoinsieme chiuso di $S$.

**Esercizio 1.5.** Sia $M$ un monoide che soddisfa la legge di cancellazione. Si provi che se $M$ è finito allora è un gruppo. [sugg.: per ogni $a \in M$ si consideri la applicazione da $M$ in se stesso definita da $x \mapsto ax$; usando la proprietà di cancellazione si provi che è iniettiva e quindi ...] Si dica se la stessa affermazione vale se $M$ è infinito.

## 1.2 Gruppi.

### 1.2.1 Prime proprietà.

**Definizione.** Un **gruppo** è un *monoide in cui ogni elemento è invertibile.* *gruppi*

Quindi un insieme con operazione $(G, \cdot)$ è un gruppo se e solo se sono soddisfatte le seguenti condizioni:

1. *Per ogni* $a, b, c \in G$ : $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ .
2. *Esiste* $1_G \in G$ *tale che, per ogni* $a \in G$ : $a1_G = a = 1_G a$ .
3. *Per ogni* $a \in G$ *esiste* $b \in G$ *tale che* $a \cdot b = 1_G = b \cdot a$ (tale $b$ è unico e si denota con $a^{-1}$).

**Esempi.** 1) Sono gruppi i monoidi additivi $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, e quelli moltiplicativi $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$, dove $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ , $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ , $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

2) Se $X$ è un insieme non vuoto, allora $(Sym(X), \circ)$ è un gruppo, detto il *Gruppo Simmetrico* su $X$.

3) Se $(M, \cdot)$ è un monoide, allora, per la Proposizione 1.1.3, l'insieme $U(M)$ degli elementi invertibili di $M$ è un gruppo rispetto alla operazione indotta da $M$.

Un gruppo si dice **commutativo** (o **abeliano**) se l'operazione è commutativa. Per i gruppi (o monoidi) commutativi, a volte è conveniente utilizzare la cosiddetta *notazione additiva* in cui l'operazione si denota con il simbolo $+$ (mentre la notazione che usiamo in generale, in cui il simbolo dell'operazione è un puntino oppure viene omesso, si dice moltiplicativa). In notazione additiva il simbolo per l'elemento neutro è $0_M$ (o, semplicemente, $0$); se $(A, +)$ è un monoide commutativo, un elemento $a \in A$ è invertibile se esiste $b \in A$ tale che $a + b = 0$, in tal caso si scrive $b = -a$ (invece di $b = a^{-1}$) e $-a$ si chiama *l'opposto* di $a$. L'enunciato della Proposizione 4 diventa : se $a, b$ sono invertibli, $-(-a) = a$ e $-(a+b) = -b+(-a) = -a+(-b)$ (perchè $M$ è commutativo). Infine, se $(A, +)$ è un gruppo, e $x, y \in A$ , si adotta la convenzione di scrivere $x + (-y) = x - y$ . *gruppi abeliani*

---

*Esercizio.* Sia $G$ un gruppo, e sia $g^{-1} = g$ per ogni $g \in G$. Si dimostri che $G$ è commutativo.

*Soluzione.* Siano $g, h \in G$. Allora $hg = h^{-1}g^{-1} = (gh)^{-1} = gh$.

---

Sia $G$ un gruppo e sia $g \in G$ e $z \in \mathbb{Z}$. La *potenza* z-esima $g^z$ di $g$ si definisce *potenze*

"induttivamente" nella maniera seguente:

$$g^0 = 1_G \ ;$$

$$\text{se } z \geq 0 \ , \quad g^{z+1} = g^z g \ ;$$

$$\text{se } z \leq -1 \ , \quad g^z = (g^{-1})^{-z}.$$

In pratica, se $z \geq 0$ ,

$$g^z = \underbrace{g \cdot g \cdot \ldots \cdot g}_{\text{z volte}}$$

Dalla definizione, tenendo conto che $(g^{-1})^{-1} = g$ segue in particolare che, per ogni $z \in \mathbb{Z}$, $g^{-z} = (g^{-1})^z$. Osserviamo anche che, se $n < 0$,

$$g^n g = (g^{-1})^{-n} g = (g^{-1})^{-n-1+1} g = (g^{-1})^{-n-1} g^{-1} g = (g^{-1})^{-n-1} = g^{n+1}.$$

E in generale, valgono per le potenze di un elemento di un gruppo le regole che ci sono familiari per le potenze intere di numeri reali:

**Proposizione 1.2.1.** *Sia $G$ un gruppo, $g \in G$ e siano $n, m \in \mathbb{Z}$. Allora*

*proprietà potenze*

*(i)* $g^{n+m} = g^n g^m$ ;

*(ii)* $g^{nm} = (g^n)^m$ .

---

*Nota.* Abbiamo dato la definizione di potenze in un gruppo, ma le stesse definizioni valgono, limitando opportunamente gli esponenti, ad elementi in un semigruppo o in un monoide. Così, in un semigruppo le potenze di un elemento sono definite come sopra per esponenti $z \geq 1$, e nel caso di un monoide per esponenti $z \geq 0$. Similmente, la Proposizione 1.2.1, che abbiamo enunciato per i gruppi, sussiste, restringendo il dominio degli esponenti, anche per semigruppi e monoidi.

---

*Notazione additiva.* In notazione additiva è preferibile adottare una diversa notazione per le potenze di un elemento, sotto forma di multipli. Se $(A, +)$ è un gruppo additivo, $a \in A$ e $n \in \mathbb{N}$, si scrive

$$0a = 0_A \ ;$$
$$na = a + a + \ \ldots \ + a \qquad \text{(n volte)};$$
$$(-n)a = n(-a) = -(na) \ .$$

e la Proposizione 1.2.1 diventa: per ogni $a \in A$ e $m, n \in \mathbb{Z}$,

$$(n+m)a = na + ma \qquad (nm)a = n(ma).$$

*Attenzione:* in generale, in un gruppo $G$, se $x, y \in G$ e $z \in \mathbb{Z}$ allora $(xy)^z \neq x^z y^z$. Infatti,

$$(xy)^2 = x^2y^2 \;\Leftrightarrow\; xyxy = xxyy \;\Leftrightarrow\; x^{-1}xyxyy^{-1} = x^{-1}xxyyy^{-1} \;\Leftrightarrow\; yx = xy.$$

Ciò che si può dire è il seguente fatto (la facile dimostrazione è un esercizio).

**Proposizione 1.2.2.** *Sia $G$ un gruppo, $g, h \in G$, con $gh = hg$. Allora, per ogni $z \in \mathbb{Z}$, $(gh)^z = g^z h^z$.*

---

*Esercizio.* Sia $M$ un monoide commutativo e sia $a \in M$. Si provi che se, per qualche $n \geq 1$, $a^n$ è invertibile allora $a$ è invertibile.

*Soluzione.* Siano $a \in M$ e $n \geq 1$ tali che $a^n$ sia invertibile. Allora esiste $b \in M$ tale che $a^n b = 1$. Da ciò segue (poiché $n \geq 1$ ed $M$ è commutativo), $(a^{n-1}b)a = a(a^{n-1}b) = 1$. Quindi $a$ è invertibile e $a^{n-1}b$ è il suo inverso.

---

*cancellazione*

Un semigruppo $S$ soddisfa la legge di *cancellazione* se, per ogni $a, b, c \in S$, da $ab = ac$ segue $b = c$, e da $ba = ca$ segue $b = c$. Ad esempio, il monoide $(\mathbb{Z}^*, \cdot)$ soddisfa la legge di cancellazione, mentre, in generale, il monoide $(X^X, \circ)$ non la soddisfa (lo si verifichi con un esempio). Una proprietà elementare ma fondamentale di un gruppo è che esso soddisfa la legge di cancellazione.

**Proposizione 1.2.3. (Legge di cancellazione).** *Sia $G$ un gruppo, e siano $a, b, c \in G$. Se $ab = ac$ allora $b = c$. Se $ba = ca$ allora $b = c$.*

*Dimostrazione.* . Sia $G$ un gruppo, e siano $a, b, c \in G$ tali che $ab = ac$. Allora, moltiplicando a sinistra per $a^{-1}$ si ha

$$b = 1_G b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}(ac) = (a^{-1}a)c = 1_G c = c\ .$$

La dimostrazione che $ba = ca \;\Rightarrow\; b = c$ si fa allo stesso modo moltiplicando a destra per $a^{-1}$. ∎

---

*Esercizio.* Sia $G$ un gruppo, e siano $g, h \in G$ tali che $g^2h^2 = h^2g^2$ e $(gh)^3 = g^3h^3$. Si provi che $gh = hg$.

*Soluzione.* Per le ipotesi su $g, h$ si ha $(gh)^3 = g^3h^3 = (gg^2)(h^2h) = g(g^2h^2)h = gh^2g^2h$; cioè $(gh)(gh)(gh) = (gh)(hg)(gh)$ e quindi, per la legge di cancellazione, $gh = hg$.

---

*tabelle di moltiplicazione*

*Nota.* Per un un semigruppo $(G, \cdot)$ è finito (cioè contiene un numero finito di elementi), può essere utile fare riferimento alla sua *tabella di moltiplicazione*. Si tratta di una tabella in cui ogni riga e ogni colonna è associata ad un diverso elemento di $G$; all'incrocio della

riga assegnata a un certo $g \in G$ con la colonna assegnata a $h \in G$ si scrive il prodotto $g \cdot h$.
Nel caso in cui $(G, \cdot)$ è un gruppo, la legge di cancellazione implica che in ogni riga (ed in ogni colonna) della tabella compaiono una ed una sola volta tutti gli elementi di $G$ (la tabella è, cioè, quello che viene chiamato un quadrato latino - come avviene, ad esempio, per un diagramma di sudoku).

*gruppo di Klein*

**Esempio** (*Il gruppo di Klein*). Il gruppo di Klein $K$ è composto da 4 elementi:

$$1_K = (1,1),\ \mathrm{a} = (1,-1),\ \mathrm{b} = (-1,1),\ \mathrm{c} = (-1,-1)$$

e l'operazione è data dal normale prodotto eseguito separatamente sulle due componenti, ovvero $(i,j)(r,s) = (ir, js)$. La tebella di moltiplicazione del gruppo $K$ è

| | 1 | a | b | c |
|---|---|---|---|---|
| 1 | 1 | a | b | c |
| a | a | 1 | c | b |
| b | b | c | 1 | a |
| c | c | b | a | 1 |

---

### 1.2.2 Sottogruppi.

*sottogruppi*

Un sottoinsieme non vuoto $H$ di un gruppo $G$ si dice **sottogruppo** (e si scrive $H \leq G$) se soddisfa alle seguenti proprietà

**(1)** $H$ è chiuso; cioè, per ogni $x, y \in H,\ xy \in H$;

**(2)** $1_G \in H$;

**(3)** per ogni $x \in H,\ x^{-1} \in H$.

È chiaro (e da ciò viene il termine sotto-gruppo) che un sottogruppo $H$ di un gruppo $G$ è esso stesso un gruppo rispetto all'operazione indotta da $G$.
Dalla definizione segue immediatamente che se $S \leq H$ e $H \leq G$, allora $S \leq G$. Inolotre, se $H$ e $K$ sono sottogruppi del gruppo $G$, allora $H \cap K \leq G$ (esercizio). Osserviamo anche che ogni gruppo $G$ ha almeno due sottogruppi: $G$ stesso e $\{1_G\}$. $\{1_G\}$ è detto il *sottogruppo banale* di $G$, mentre un sottogruppo $H$ si dice *proprio* se $H \neq G$.

**Esempio.** Sia $1 \leq n \in \mathbb{N}$. Nell'insieme $\mathbb{C}^*$ dei numeri complessi diversi dallo zero, consideriamo il sottoinsieme delle radici n-esime dell'unità:

$$U_n = \{z \in \mathbb{C}^* \mid z^n = 1\}.$$

Allora $U_n$ è un sottogruppo del gruppo moltiplicativo $(\mathbb{C}^*, \cdot)$. Infatti $1 \in U_n$ e, per ogni $z_1, z_2 \in U_n$, si ha $(z_1 z_2)^n = z_1^n z_2^n = 1 \cdot 1 = 1$ e $(z_1^{-1})^n = (z_1^n)^{-1} = 1$; dunque sia $z_1 z_2$ che $z_1^{-1}$ appartengono a $U_n$. Quindi $U_n \leq \mathbb{C}^*$.

In notazione additiva le condizioni affinchè un sottoinsieme $H$ di un gruppo additivo $A$ sia un sottogruppo si scrivono:

$$(1)\ \forall x, y \in H,\ x + y \in H \qquad (2)\ 0_A \in H \qquad (3)\ \forall x \in H,\ -x \in H\ .$$

*sottogruppi di $\mathbb{Z}$*

**Esempio importante** Sia $n \in \mathbb{N}$ e indichiamo con $n\mathbb{Z}$ l'insieme di tutti i multipli interi di $n$; cioè

$$n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}.$$

Allora $n\mathbb{Z}$ è un sottogruppo del gruppo $(\mathbb{Z}, +)$. Infatti,
(1) $0 = n0 \in n\mathbb{Z}$ ;
(2) se $x, y \in n\mathbb{Z}$, esistono $z, z_1 \in \mathbb{Z}$ tali che $x = nz,\ y = nz_1$; quindi $x + y = nz + nz_1 = n(z + z_1) \in n\mathbb{Z}$ ;
(3) se $x = nz \in n\mathbb{Z}$, allora $-x = -(nz) = n(-z) \in n\mathbb{Z}$.
Un fatto importante che si può provare (vedi Teorema 1.3.1) è che tutti i sottogruppi del gruppo $(\mathbb{Z}, +)$ sono di questo tipo.

---

*Esercizio. Siano $A, B$ sottogruppi del gruppo $G$. Si provi che se $G = A \cup B$, allora $G = A$ oppure $G = B$.*

*Soluzione.* Siano $A, B$ sottogruppi propri del gruppo $G$ e supponiamo per assurdo $G = A \cup B$. Ora, $B \not\subseteq A$ perchè se cosi fosse sarebbe $G = A \cup B = A$ (contro l'ipotesi che $A$ sia un sottogruppo proprio); e similmente $A \not\subseteq B$. Dunque esistono $a \in A \setminus B$ e $b \in B \setminus A$. Considero $ab$. Se $ab \in A$ allora $b = a^{-1}(ab) \in A$ contro la scelta di $b$; quindi $ab \notin A$. Similmente $ab \notin B$. Quindi $ab \notin A \cup B$, assurdo.

---

*Teorema di Lagrange*

A conclusione di questo breve paragrafo sui sottogruppi, riportiamo, senza dimostrarlo, un risultato che è alla base della teoria dei gruppi finiti.

**Teorema 1.2.4.** (Lagrange). *Sia $H$ un sottogruppo del gruppo finito $G$. Allora, l'ordine di $H$ divide l'ordine di $G$.*

### 1.2.3 Isomorfismi.

La nozione di isomorfismo e quella, più debole, di omomorfismo, servono a formalizzare la situazione in cui gruppi di diversa estrazione si comportano, dal punto di vista formale dell'operazione in modo simile o anche allo stesso modo .

*omomorfismi e isomorfismi*

Siano $(G, \cdot)$ e $(G', *)$ due gruppi (o semigruppi). Una applicazione $\phi : G \longrightarrow G'$, tale che, per ogni $x, y \in M$,

$$\phi(x \cdot y) = \phi(x) * \phi(y)$$

si chiama un **omomorfismo** di $G$ in $G'$. Se, inoltre, $\phi$ è un'applicazione biettiva, allora è detta un **isomorfismo** di $G$ in $G'$.
Osserviamo che se $G$ è un (semi)gruppo l'applicazione identica $\iota_G$ è un isomorfismo di $G$ in se stesso.

**Proposizione 1.2.5.** *Siano $(G,\cdot)$, $(G',*)$ gruppi, e sia $\phi : G \longrightarrow G'$ un omomorfismo. Allora $\phi(1_G) = 1_{G'}$ e, per ogni $g \in G$, $\phi(g^{-1}) = (\phi(g))^{-1}$.*

*Dimostrazione.* Sia $b = \phi(1_G)$. Allora

$$b * b = \phi(1_G) * \phi(1_G) = \phi(1_G \cdot 1_G) = \phi(1_G) = b$$

moltiplicando a destra per $b^{-1}$ si ottiene $b = b * b * b^{-1} = b * b^{-1} = 1_{G'}$ .
Sia ora $g \in G$, allora

$$\phi(g^{-1}) * \phi(g) = \phi(g^{-1} \cdot g) = \phi(1_G) = 1_{G'}$$

e quindi $\phi(g^{-1}) = (\phi(g))^{-1}$ . ■

---

*Esercizio.* Sia $G$ un gruppo. Si dimostri che l'applicazione $f : G \longrightarrow G$, definita da, per ogni $g \in G$, $f(g) = g^{-1}$ è un isomorfismo se e solo se $G$ è commutativo.

*Soluzione.* Sia $G$ un gruppo, e supponiamo che l'applicazione $f$ sia un omomorfismo, allora per ogni $g, h \in G$,

$$g^{-1}h^{-1} = f(g)f(h) = f(gh) = (gh)^{-1} ,$$

dunque $gh = ((gh)^{-1})^{-1} = (g^{-1}h^{-1})^{-1} = (h^{-1})^{-1}(g^{-1})^{-1} = hg$, e quindi $G$ è commutativo.
Viceversa, sia $G$ commutativo. Allora, per ogni $g, h \in G$,

$$f(gh) = (gh)^{-1} = (hg)^{-1} = g^{-1}h^{-1} = f(g)f(h)$$

dunque $f$ è un omomorfismo. Poichè $f$ è una applicazione biettiva (coincide con la propria inversa), essa è un automorfismo.

---

*composiz. di omomorfismi*

Una proprietà importante degli omomorfismi e isomorfismi è che la composizione di due di essi è ancora un omomorfismo.

**Proposizione 1.2.6.** *Siano $(A,\cdot), (B,\cdot)$ e $(C\cdot)$ (semi)gruppi, e siano $\phi : A \longrightarrow B$ e $\psi : B \longrightarrow C$ due omomorfismi. Allora $\psi \circ \phi : A \longrightarrow C$ è un omomorfismo. Se $\phi$ e $\psi$ sono isomorfismi, $\psi \circ \phi$ è un isomorfismo.*

*Dimostrazione.* Siano $a, b \in A$. Allora, poichè $\phi$ e $\psi$ sono omomorfismi

$$\psi \circ \phi(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)) = (\psi \circ \phi(a))(\psi \circ \phi(b))$$

dunque $\psi \circ \phi$ è un omomorfismo. Se $\phi$ e $\psi$ sono isomorfismi, allora sono biettive e quindi $\psi \circ \phi$ è biettiva e pertanto è un isomorfismo. ∎

---

*Nota.* Per diversi tipi di strutture matematiche il concetto di isomorfismo richiede l'esistenza di un'applicazione invertibile tale che sia essa *che la sua inversa* conservino la struttura (questo è, ad esempio, il caso degli spazi topologici). Per i gruppi non è necessario richiedere esplicitamente che l'inversa conservi l'operazione, perché tale condizione è comunque soddisfatta da un omomorfismo biettivo. Infatti, sia $\phi : (G, \cdot) \longrightarrow (G', *)$ un omomorfismo biettivo di gruppi, e siano $a, b \in G'$. Poichè $\phi$ è un omomorfismo, si ha

$$\phi(\phi^{-1}(a) \cdot \phi^{-1}(b)) = \phi(\phi^{-1}(a)) * \phi(\phi^{-1}(b)) = a * b = \phi(\phi^{-1}(a * b))$$

e, quindi poichè $\phi$ è iniettiva,

$$\phi^{-1}(a) \cdot \phi^{-1}(b) = \phi^{-1}(a * b).$$

Dunque $\phi^{-1} : G' \longrightarrow G$ è un omomorfismo.

---

Due gruppi $G$ , $G'$ si dicono **isomorfi** se esiste un isomorfismo da $G$ in $G'$. Si scrive in tal caso $G \simeq G'$. Dalle proposizioni e osservazioni precedenti segue che $G \simeq G$ (mediante l'applicazione identica), se $G \simeq G'$ allora $G' \simeq G$, e che se $G \simeq G'$ e $G' \simeq G''$ allora $G \simeq G''$. (si osservi che una applicazione tra due gruppi $G, G'$ è un omomorfismo (isomorfismo) di gruppi se e solo se è un omomorfismo (isomorfismo) di $G$ in $G'$ considerati come semigruppi).

---

*Nota.* Come già suggerisce la Proposizione 1.2.5, se due gruppi sono isomorfi allora soddisfano le stesse proprietà strutturali come gruppi. Tutto ciò che, relativamente all'operazione, si può affermare per uno dei due gruppi vale, passando attraverso la corrispondenza biunivoca stabilita dall'isomorfismo, anche per l'altro gruppo. Parlando informalmente, si giunge a dire che due gruppi isomorfi sono lo stesso gruppo.

---

**Esempi.** 1) Sia $P$ l'insieme dei numeri reali strettamente maggiori di zero. Allora $P$ è un gruppo con l'operazione di moltiplicazione. L'applicazione logaritmo naturale $P \longrightarrow \mathbb{R}$ definita da, per ogni $x \in P$, $x \mapsto log_e(x)$, è un isomorfismo del gruppo moltiplicativo $(P, \cdot)$ nel gruppo additivo $(\mathbb{R}, +)$. Infatti, è biettiva e per ogni $x, y \in P$, $log_e(xy) = log_e(x) + log_e(y)$. L'applicazione inversa è la funzione esponenziale, ed è un isomorfismo da $(\mathbb{R}, +)$ in $(P, \cdot)$ (naturalmente si ottiene un isomorfismo anche considerando il logaritmo in una qualsiasi base positiva $\neq 1$ fissata).

2) Sia $G$ un gruppo, e sia $g \in G$. La Proposizione 1.2.1 implica che la applicazione $\gamma : \mathbb{Z} \to G$, definita da, per ogni $z \in \mathbb{Z}$, $\gamma(z) = g^z$, è un omomorfismo del gruppo $(\mathbb{Z}, +)$ nel gruppo $G$.

### 1.2.4 Esercizi.



**Esercizio 1.6.** Sia $G$ un gruppo. Si dimostri che per ogni coppia di elementi $a, b \in G$ esiste uno e un solo $x \in G$ tale che $ax = b$.

**Esercizio 1.7.** Sull'insieme $\mathbb{Q}^2 = \{(x, y) \mid x, y \in \mathbb{Q}\}$ si definisca l'operazione $*$ ponendo, per ogni $(\mathrm{a}, \mathrm{b}), (\mathrm{a}_1, \mathrm{b}_1) \in \mathbb{Q}^2$,

$$(\mathrm{a}, \mathrm{b}) * (\mathrm{a}_1, \mathrm{b}_1) = (\mathrm{aa}_1, \mathrm{ab}_1 + \mathrm{b}).$$

Si dica se tale operazione è associativa e se esiste un elemento identico in $\mathbb{Q}^2$. Per ogni $b \in \mathbb{Q}$ e ogni $n \in \mathbb{N}$ si determini, procedendo per induzione su $n$, la potenza $(1, b)^n$.

**Esercizio 1.8.** Si provi che l'insieme

$$\left\{ \frac{m}{2^i} \mid m \in \mathbb{Z},\ i \in \mathbb{N} \right\}$$

è un sottogruppo del gruppo $(\mathbb{Q}, +)$.

**Esercizio 1.9.** Per ogni coppia $(a, b)$ di numeri reali con $a \neq 0$ sia $\sigma_{a,b} : \mathbb{R} \to \mathbb{R}$, l'applicazione definita da $\sigma_{a,b}(x) = ax + b$ per ogni $x \in \mathbb{R}$. Sia $G = \{\sigma_{a,b} \mid a, b \in \mathbb{R}\ \ a \neq 0\}$.
Si dimostri che $G$ dotato della operazione di composizione di applicazioni è un gruppo e si verifichi che il sottoinsieme $T = \{\sigma_{1,b} \mid b \in \mathbb{R}\}$ è un suo sottogruppo.

**Esercizio 1.10.** Sia $\phi : G \to G'$ un omomorfismo di gruppi. Procedendo per induzione su $n$, si provi che, per ogni $x_1,\ x_2, \ldots,\ x_n \in G :\ \phi(x_1 x_2 \cdots x_n) = \phi(x_1)\phi(x_2)\cdots\phi(x_n)$.

**Esercizio 1.11.** Sia $(G, \cdot)$ un gruppo e sia $a \in G$ tale che $ag = ga$ per ogni $g \in G$. Su $G$ si definisca una nuova operazione $*$, ponendo, per ogni $x, y \in G :\ x * y = x \cdot a \cdot y$. Si provi che $(G, *)$ è un gruppo. Si dimostri quindi che l'applicazione

$$\begin{array}{ccc} G & \to & G \\ x & \mapsto & a^{-1}x \end{array}$$

è un isomorfismo del gruppo $(G, \cdot)$ nel gruppo $(G, *)$.

**Esercizio 1.12.** Si scrivano le tabelle di moltiplicazione di due gruppi con 4 elementi che non siano tra loro isomorfi .

## 1.3 Esempi.

### 1.3.1 Operazioni tra insiemi.

*unione e inetersezione*

Esaminiamo rapidamente, dal punto di vista generale, il comportamento delle principali operazioni tra insiemi, unione e intersezione e. Per farlo, dobbiamo considerare gli insiemi su cui operiamo come oggetti di un insieme più ampio. Il modo più semplice e sicuro è quello di considerare un insieme (non vuoto) $X$, e l'insieme delle sue parti $\mathcal{P}(X)$. Sull'insieme $\mathcal{P}(X)$ sono dunque definite le operazioni di unione e intersezione: per ogni $Y, Z \in \mathcal{P}(\mathcal{X})$ (cioè per ogni coppia $Y, Z$ di sottoinsiemi di $X$) sono definiti nel modo usuale $Y \cap Z$ e $Y \cup Z$. Quidni $\cap$ e $\cup$ sono operazioni definite su $\mathcal{P}(X)$. È facile verificare che entrambe queste operazioni sono *associative* (e anche commutative); inoltre, per ogni $Y \in (X)$ si ha

$$Y \cup \emptyset = Y = \emptyset \cup Y \qquad \text{e} \qquad Y \cap X = Y = X \cap Y.$$

Quindi, l'insieme vuoto $\emptyset$ è un elemento neutro (e l'unico) per l'operazione di unione, mentre l'insieme ambiente $X$ è l'elemento neutro per l'operazione di intersezione. Pertanto, $\mathcal{P}(X)$ è sempre un monoide (commutativo) sia rispetto all'unione che all'intersezione. Osserviamo che, per $Y, Z \in \mathcal{P}(X)$ si ha

$$Y \cup Z = \emptyset \quad \Leftrightarrow \quad Y = Z = \emptyset$$

$$Y \cap Z = X \quad \Leftrightarrow \quad Y = Z = X;$$

dunque, in $\mathcal{P}(X)$ il solo elemento invertibile rispetto all'unione è $\emptyset$, ed il solo elemento invertibiule rispetto all'intersezione è $X$. Quindi, con le operazioni $\cup$ o $\cap$, $\mathcal{P}(X)$ non è mai un gruppo (tranne il caso in cui $\mathcal{P}(X)$ contiene un solo elemento, il che avviene se e solo se $X = \emptyset$).

---

*diff simmetrica*

*Nota.* Sull'insieme $\mathcal{P}(X)$ è possibile definire un'operazione, la *differenza simmetrica* $\Delta$, che assegna una struttura di gruppo. Per ogni $Y, Z \in \mathcal{P}(X)$ si pone

$$Y \Delta Z = (Y \setminus Z) \cup (Z \setminus Y)$$

(quindi, $Y \Delta Z$ è l'insieme degli elementi che appartengono ad uno *e uno solo* tra $Y$ e $Z$). Si può provare (in modo elementare ma un po' laborioso) che tale operazione è associativa (oltre che commutativa); si verifichi per esercizio che $\emptyset$ è l'elemento neutro, e che ogni elemento di $\mathcal{P}(X)$ ha un inverso rispetto alla differenza simmetrica (si osserverà che, per ogni $Y \in \mathcal{P}(X)$, $Y$ coincide con il suo inverso). Quindi, per ogni insieme ambiente $X$, $(\mathcal{P}(X), \Delta)$ è un gruppo (commutativo).

---

*dualità tra $\cup$ e $\cap$*

Sia $X$ un insieme. Allora l'applicazione di complementazione: $\mathcal{C} : \mathcal{P}(X) \longrightarrow \mathcal{P}(X)$,

definita da, per ogni $Y \in \mathcal{P}(X)$, $\mathcal{C}(Y) = X \setminus Y$, è un isomorfismo del monoide $(\mathcal{P}(X), \cap)$ nel monoide $(\mathcal{P}(X), \cup)$. Infatti, $\mathcal{C}$ è biettiva (coincide con la propria inversa), e per ogni $X, Z \in \mathcal{P}(X)$ si ha, per la legge di De Morgan, $\mathcal{C}(Y \cup Z) = X \setminus (Y \cup Z) = (X \setminus Y) \cap (X \setminus Z) = \mathcal{C}(Y) \cap \mathcal{C}(Z)$.

### 1.3.2 Parole.

*parole*

Uno degli esempio più semplici (ma, forse, anche più astratti) di semigruppo è quello dell *parole* in un dato alfabeto $X$.
L'*alfabeto* è un insieme (non necessariamente finito) non vuoto fissato (ad esempio, l'insieme $\{a, b, c, \ldots, , z\}$, oppure l'insieme $\{0, 1\}$, o anche l'insieme $\{A, G, C, T\}$). Gli elementi di $X$ sono detti *lettere*; una *parola* nell'alfabeto $X$ è una sequenza finita $x_1 x|_2 \ldots x_n$ di lettere $x_1, x_2, \ldots$ non necessariamente distinte. L'insieme $P_X$ di tutte le parole finite in $X$ ammette una operazione naturale, che consiste semplicemente nel giustapporre le parole nell'ordine dato; detto più chiaramente, se $\bar{x} = x_1 x_2 \ldots x_n$ e $\bar{y} = y_1 y_2 \ldots y_m$ sono due parole in $X$, si pone

$$\bar{x} \cdot \bar{y} = x_1 x_2 \ldots x_n y_1 y_2 \ldots y_m.$$

Si comprende facilmente che, con tale operazione, l'insieme $P_X$ è un semigruppo. Se, inoltre, tra le possibili parole in $X$ si ammette (come di solito si fa) anche la parola vuota, che si denota con !, allora $P_X$ diventa un monoide, il cui elemento identico è la parola vuota.

### 1.3.3 Gruppi ciclici.

*sottogruppi ciclici*

Sia $g$ un fissato (ma generico) elemento di un gruppo $G$. Le proprietà delle potenze implicano che l'insieme di tutte le potenze intere di $g$,

$$< g >= \{\ g^z \mid z \in \mathbb{Z}\ \}$$

è un sottogruppo di $G$. Si chiama il **sottogruppo ciclico generato** da $g$. Se $H$ è un qualche sottogruppo di $G$ che contiene $g$, allora, per la chiusura rispetto a prodotti ed inversi, $H$ deve contenere tutte le potenze intere di $g$; cioè $H \supseteq < g >$. Quindi $< g >$ è il minimo sottogruppo di $G$ che contiene l'elemento $g$.
Osserviamo che un sottogruppo ciclico è commutativo. Infatti per ogni $g \in G$ e ogni $n, m \in \mathbb{Z}$, $g^n g^m = g^{n+m} = g^{m+n} = g^m g^n$ .

In *notazione additiva*, il sottogruppo ciclico generato da un elemento $a$ è l'insieme dei multipli interi di $a$; ovvero $< a >= \{\ za \mid z \in \mathbb{Z}\ \}$. Dimostriamo ora l'importante fatto che tutti i sottogruppi del gruppo additivo $(\mathbb{Z}, +)$ sono ciclici. Per quanto appena osservato, se $a \in \mathbb{Z}$ allora il sottogruppo ciclico generato da $a$ è $a\mathbb{Z} = \{\ az \mid z \in \mathbb{Z}\ \}$.

**Teorema 1.3.1.** *Sia $H$ un sottogruppo del gruppo additivo $\mathbb{Z}$. Allora esiste $n \in \mathbb{N}$ tale che $H = n\mathbb{Z}$.* *sottogruppi di $(\mathbb{Z}, +)$*

Un gruppo $G$ si dice **ciclico** se esiste un elemento $g \in G$ tale che $G$ è il sottogruppo generato da $g$; cioè *gruppi ciclici*

$$G =< g >= \{\ g^z \mid z \in \mathbb{Z}\ \}\ .$$

In tal caso, $g$ si dice un **generatore** di $G$.

(In notazione additiva, un gruppo $A$ è ciclico se esiste $a \in A$ tale che $A = \{za \mid z \in \mathbb{Z}\}$).

**Esempi.** 1) $(\mathbb{Z}, +)$ è un gruppo ciclico con generatore 1 (un altro possibile generatore è -1 ; si verifichi che questi sono i soli possibili generatori di $\mathbb{Z}$).

Abbiamo già osservato che un gruppo ciclico è abeliano. Il gruppo $\mathbb{Z}$ è il modello fondamentale per i gruppi ciclici. Vediamo ad esempio che, così come avviene per $\mathbb{Z}$, ogni sottogruppo di un gruppo ciclico è ciclico. Ne diamo quindi una esposizione rapida. Si cerchi di completarla e di scriverne una specificatamente per $\mathbb{Z}$.

**Proposizione 1.3.2.** *Ogni sottogruppo di un gruppo ciclico è ciclico.*

*Dimostrazione.* Sia $G =< g >$ un gruppo ciclico con generatore $g$, e sia $H \leq G$. Se $H = \{1_G\}$ allora $H =< 1_G >$. Sia quindi $H \neq \{1_G\}$; allora esiste $0 \neq z \in \mathbb{Z}$ tale che $g^z \in H$. Poichè $H$ è un sottogruppo si ha anche $g^{-z} \in H$. Quindi non è vuoto l'insieme $\{0 \neq m \in \mathbb{N} \mid g^m \in H\}$. Sia $n$ il minimo di tale insieme. Allora $g^n \in H$ e quindi $< g^n > \leq H$. Viceversa, se $h = g^z \in H$, si divide $z$ per $n$ : $z = nq + r$ con $0 \leq r \leq n-1$. Quindi $g^r = g^{z-nq} = g^z(g^n)^{-q} \in H$, da cui segue, per la scelta di $n$, $r = 0$. Quindi $h = g^z = g^{nq} = (g^n)^q \in < g^n >$ e dunque $H \leq < g^n >$. Quindi $H =< g^n >$ è ciclico. ∎

---

*Nota.* I due esempi seguenti illustrano come la classe dei gruppi ciclici si suddivida naturalmente in due tipologie; quelli infiniti e quelli finiti. Agli esempi seguirà una proposizione che descrive in generale la differenza tra il caso finito e quello infinito.

*Esempi.* 1) Consideriamo il gruppo moltiplicativo $(\mathbb{R}^*, \cdot)$, dei numeri reali diversi da 0, e consideriamo l'insieme

$$G = \{\ 2^z \mid z \in \mathbb{Z}\ \}.$$

Allora $G$ è un sottogruppo di $\mathbb{R}^*$, ed è un gruppo ciclico generato da $g = 2$. Osserviamo che se $z, z'$ sono numeri interi diversi allo $2^z \neq 2^{z'}$ (cioè $g^z \neq g^{z'}$). Quindi il gruppo ciclico $G$ è infinito, e c'è un'ovvia corrispondenza biunivoca tra esso e l'insieme $\mathbb{Z}$ dei numeri interi.

2) Consideriamo il gruppo simmetrico su $\mathbb{R}^2$ (cioè il gruppo delle permutazioni dei punti del piano cartesiano), e il suo elemento $\rho$ che consiste nella rotazione di $\pi/3$ radianti (ovvero $60^o$) in senso antiorario e centro l'origine. Allora $\rho^6$ è la permutazione che consiste

nel ruotare di un angolo giro attorno all'origine; quindi $\rho^6$ è l'identità $I = \iota_{\mathbb{R}^2}$. Ora, per ogni intero $z$, si può dividere $z$ per 6: $z = 6q + r$, con un resto $0 \leq r \leq 5$. Applicando le regole sulle potenze si ricava:

$$\rho^z = \rho^{6q+r} = \rho^{6q} \circ \rho^r = (\rho^6)^q \circ \rho^r = I^q \circ \rho^r = I \circ \rho^r = \rho^r.$$

Dunque il gruppo ciclico $\langle \rho \rangle$ consiste nei sei elementi

$$\rho^0 = I \quad \rho = \rho^1 \quad \rho^2 \quad \rho^3 \quad \rho^4 \quad \rho^5;$$

(si osservi che $\rho^3$ è la rotazione di un angolo piatto, e che $\rho^5 = \rho^{-1}$ è una rotazione di $\frac{5}{3}\pi$ radianti – cioè 270° – in senso antiorario, che equivale ad una rotazione di $\frac{\pi}{3}$ in senso orario). Quindi il gruppo ciclico genarato da $\rho$ ha ordine 6.

Gli esempi di sopra illustrano i due tipi fondamentali di gruppi ciclici, che la seguentre Proposizione (che non proviamo) descrive in modo esatto.

**Proposizione 1.3.3.** *Sia $G =< g >$ un gruppo ciclico; allora si verifica uno dei casi seguenti.*

*(1) $\forall n \geq 1,\ g^n \neq 1_G$. In tal caso $|G| = \infty$ e $g^z = g^w$ se e solo se $z = w$.*

*(2) $\exists n \geq 1,\ g^n = 1_G$. In tal caso, se $n$ è il minimo numero naturale non nullo tale che $g^n = 1_G$ allora $|G| = n$ e $G = \{\ g^0 = 1_G,\ g,\ g^2,\ \ldots,\ g^{n-1}\}$.*

---

### 1.3.4 Permutazioni.

Gruppo simmetrico

Sia $X$ un insieme (per esempio, e per rimanere nel finito, si pensi alli'nsieme $\{1, 2, \ldots, n\}$); sappiamo che se $f.g : X \to X$ sono applicazioni biettive, allora è possibile comporre $f$ con $g$ e viceversa, ottenendo in tal modo ancora applicazioni biettive da $X$ in sé. Ciò significa che la composizione è un'operazione binaria nell'iinsieme di tutte le applicazioni biettive da $X$ in se stesso: insieme che denotiamo con $Sym(X)$, e chiamiamo anche 'permutazioni' di $X$ i suoi elementi (ovvero le biezioni di $X$ in sé). L'operazione di composizione è, come sappiamo, associativa, ed ammette un elemento neutro, che mnon è altro che l'applicazione identica $\iota_X$ su $X$; infine ogni applicazione biettiva ammette un'inversa, tale inversa è anche l'inversa nel senso dell'oparzione. La conclusione è che $Sym(X)$ dotato dell'operazione di composizione **è un gruppo**; esso viene chiamato *il gruppo simmetrico (o delle permutazioni)* di $X$.

Dalla teoria generale delle permutazioni, sappiamo che se $|X| = n$ (con $n$ finito), allora $|Sym(X)| = n!$.

*Esempio.* Sia $X$ un insieme e sia $Y \subseteq X$. Allora

$$S_Y = \{\ f \in Sym(X) \mid f(Y) = Y\ \}$$

è un sottogruppo del gruppo $Sym(X)$. Infatti
(1) $\iota_X \in S_Y$ ;
(2) se $f, g \in S_Y$, allora $(f \circ g)(Y) = f(g(Y)) = f(Y) = Y$, dunque $(f \circ g) \in S_Y$
(3) se $f \in S_Y$, allora $f^{-1}(Y) = f^{-1}(f(Y)) = (f^{-1} \circ f)(Y) = \iota_X(Y) = Y$, e dunque $f^{-1} \in S_Y$ .

### 1.3.5 Il Gruppo $S_3$.

Illustriamo nei dettagli il gruppo simmetrico su un insieme di ordine 3. gruppo $S_3$

Sia $S_3$ il gruppo simmetrico sull'insieme $\{1, 2, 3\}$, cioè il gruppo di tutte le permutazioni dell'insieme $\{1, 2, 3\}$. Come sappiamo, $S_3$ contiene 6 elementi. Ogni elemento $\sigma \in S_3$ può essere descritto mediante la tabella

$$\begin{pmatrix} 1 & 2 & 3 \\ \sigma(1) & \sigma(2) & \sigma(3) \end{pmatrix}$$

(osserviamo che, essendo $\sigma$ una applicazione biettiva, la seconda riga della tabella contiene tutti gli elementi $\{1, 2, 3\}$). Allora

$$\iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

Poniamo quindi

$$\gamma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

allora

$$\gamma^2 = \gamma \circ \gamma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

componendo ancora con $\gamma$ si trova $\gamma^3 = \gamma^2 \circ \gamma = \iota$. Quindi $\gamma^2 = \gamma^{-1}$. Se consideriamo un qualunque numero intero $z$ possiamo scrivere $z = 3q + r$ con $r \in \{0, 1, 2\}$ , dunque

$$\gamma^z = \gamma^{3q+r} = \gamma^{3q} \circ \gamma^r = (\gamma^3)^q \circ \gamma^r = \iota^q \circ \gamma^r = \iota \circ \gamma^r = \gamma^r \ ;$$

il sottogruppo ciclico generato da $\gamma$ (che denotiamo con $A$) è quindi composto dai tre elementi

$$\iota = \gamma^0 \ , \quad \gamma \ , \quad \gamma^2 \ .$$

$\gamma$ si dice un **ciclo** di ordine 3, o un 3-ciclo (perchè permuta ciclicamente i tre elementi 1,2,3). Chiaramente, il gruppo ciclico generato da $\gamma^2 = \gamma^{-1}$ coincide con $A =< \gamma >$.

Poniamo ora

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \qquad \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \qquad \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

queste applicazioni scambiano due elementi e fissano i rimanenti; si chiamano **trasposizioni**. Allora, per ogni $i = 1, 2, 3$ , $\tau_i^2 = \iota$ e quindi, ragionando come abbiamo fatto con $\gamma$ , il sottogruppo $T_i$ generato da $\tau_i$ è

$$T_i =< \tau_i >= \{ \iota \ , \ \tau_i \} \ .$$

Abbiamo quindi elencato tutti gli elementi di $S_3$. Sono

$$\iota \ , \ \gamma \ , \gamma^2 \ , \ \tau_1 \ , \ \tau_2 \ , \ \tau_3 \ ;$$

ed abbiamo determinato tutti i sottogruppi ciclici di $S_3$ che sono

$$\{\iota\} \ , \ A \ , \ T_1 \ , \ T_2 \ , \ T_3 \ .$$

In particolare, $S_3$ non coincide con alcuno dei suoi sottogruppi ciclici; cosa che poteva essere anche stabilita osservando che $S_3$ non è abeliano, ad esempio

$$\tau_1 \circ \tau_2 = \gamma \neq \gamma^2 = \tau_2 \circ \tau_1$$

(si può dimostrare che ogni gruppo non commutativo di ordine 6 è isomorfo a $S_3$ e che i gruppi di ordine minore o uguale a 5 sono commutativi. Quindi $S_3$ è il più piccolo gruppo non commutativo).

Vediamo ora che i sottogruppi elencati costituiscono l'insieme di tutti i sottogruppi propri di $S_3$. Sia $H \leq S_3$ e supponiamo che $H$ contenga due distinte trasposizioni, diciamo $\tau_1$ e $\tau_2$ ; allora $H$ contiene $\tau_2 \circ \tau_1 = \gamma^2$ e $\tau_1 \circ \tau_2 = \gamma$ e quindi contiene anche $\gamma \circ \tau_1 = \tau_3$ ; dunque $H = S_3$. Similmente si ragiona a partire dalla altre coppie di trasposizioni.

Supponiamo allora che $H$ contenga un'unica trasposizione $\tau_i$; se $H \neq < \tau_i >= T_i$ , $H$ contiene o $\gamma$ o $\gamma^2$. Se $\gamma \in H$ allora $H$ contiene $\tau_i \circ \gamma = \tau_{\gamma(i)}$ contro l'assunzione che $H$ contenga un'unica trasposizione. Allo stesso modo, se $\gamma^2 \in H$ allora $\tau_{\gamma(i)} = \gamma^2 \circ \tau_i \in H$ contro l'assunzione su $H$. Quindi $H =< \tau_i >= T_i$.

Infine, se $H$ non contiene trasposizioni, allora $H = \{1\}$ o $H =< \gamma >= A$.

In conclusione, i sottogruppi di $S_3$ sono

$$\{\iota\} \ , \ A \ , \ T_1 \ , \ T_2 \ , \ T_3 \ , \ S_3 \ .$$

Dal controllo dei loro elementi si vede che se $H, K$ sono sottogruppi propri e distinti di $S_3$ allora $H \cap K = \{1\} = \{\iota\}$.

Osserviamo che dallo studio dei sottogruppi fatto sopra segue, tra l'altro, che date due distinte trasposizioni, ad esempio $\tau_1,\ \tau_2$, il più piccolo sottogruppo che le contiene è $S_3$; si dice allora che $S_3$ è **generato** dalle trasposizioni $\tau_1,\ \tau_2$ (o che $\{\tau_1,\ \tau_2\}$ è un insieme di generatori di $S_3$), e si scrive $S_3 = \langle \tau_1,\ \tau_2 \rangle$. Ogni elemento di $S_3$ si scrive come un prodotto i cui fattori sono $\tau_1,\ \tau_2$, o loro inversi (che in questo caso coincidono con gli stessi generatori); infatti: $\iota = \tau_1 \circ \tau_2,\ \ \gamma = \tau_1 \circ \tau_2,\ \ \gamma^2 = \tau_2 \circ \tau_1$ e $\tau_3 = \tau_1 \circ \tau_2 \circ \tau_1$.

Osserviamo che gli ordini dei sottogruppi di $S_3$ sono: 1, 2, 3, 6. Ognuno divide l'ordine del gruppo $S_3$. Questo fatto è una proprietà fondamentale (ed una delle prime ad essere stata notata) dei gruppi finiti, e costituisce il cosiddetto **Teorema di Lagrange:** *l'ordine di ogni sottogruppo di un gruppo finito $G$ divide l'ordine di $G$.*

teorema di Lagrange

Il gruppo $S_3$ può anche essere visto (il termine tecnico è *rappresentato*) come il **gruppo delle simmetrie** di un triangolo equilatero. Consideriamo un triangolo equilatero $\Delta$ sul piano, con i vertici numerati con 1, 2, 3; per comodità fissiamo un riferimento cartesiano con origine il centro del triangolo e asse $y$ passante per il vertice 1:

simmetrie di un triangolo

Consideriamo ora l'insieme di tutti i movimenti rigidi del piano che mutano il triangolo $\Delta$ in se stesso. Essi sono:

- *l'identità*;

- *le rotazioni (antiorarie) intorno all'origine di* $\frac{2\pi}{3}$ *e* $\frac{4\pi}{3}$ *radianti* (120 e 240 gradi);

- *le tre riflessioni lungo gli assi del triangolo.*

L'insieme $\gamma$ di queste sei applicazioni (biettive) del piano in se costituisce un gruppo mediante la composizione, che si chiama gruppo delle simmetrie di $\Delta$; ad esempio la composizione della rotazione di $\frac{2\pi}{3}$ radianti con la riflessione lungo l'asse $y$ è la riflessione lungo l'asse passante per il vertice 3, l'inversa della rotazione di $\frac{2\pi}{3}$ radianti è la rotazione di $\frac{4\pi}{3}$ radianti, etc.

Ora, si può definire un isomorfismo da $\Gamma$ in $S_3$ associando ad ogni elemento di $\Gamma$ la permutazione da esso indotta sull'insieme $\{1,\ 2,\ 3\}$ dei vertici di $\Delta$. Ad

esempio, alla rotazione di $\frac{2\pi}{3}$ radianti corrisponde il 3-ciclo $\gamma$, alla riflessione lungo l'asse passante per il vertice 3 corrisponde la trasposizione $\tau_3$, etc. Il sottoinsieme di $\Gamma$ costituito dalle rotazioni (inclusa l'identità, che è la rotazione di un angolo nullo) è un sottogruppo ciclico, e corrisponde in $S_3$ al sottogruppo $<\gamma>$.

Considerazioni simili si possono fare per un qualunque poligono (regolare) o più in generale una qualunque figura piana. Ad esempio il gruppo delle simmetrie di una circonferenza con centro l'origine è un gruppo infinito che contiene tutte le rotazioni e tutte le riflessioni lungo rette passanti per l'origine. Per **esercizio** si studi il caso di un quadrato; si provi che il suo gruppo delle simmetrie contiene 8 elementi e non è commutativo (tale gruppo si chiama *gruppo diedrale* di ordine 8)

### 1.3.6 Matrici.

Un esempio molto importante di operazione, e strettamente legato alla composizione di applicazioni, è il prodotto (righe per colonne) di matrici. Lo studio delle matrici è parte della cosiddetta alggebra lineare. Richiamiamo qui, senza dimostrazione, solo alcuni fatti.

*matrici*

Sia $1 \leq n \in \mathbb{N}$. Una **Matrice quadrata di ordine n** a coefficienti reali è una tabella

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ . & . & \cdots & . \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

dove i coefficienti $a_{ij}$ sono numeri reali. Denoteremo con $M_n(\mathbb{R})$ l'insieme di tutte le matrici quadrate di ordine n a coefficienti reali.
Se $A = (a_{ij}) \in M_n(\mathbb{R})$ , allora, per ogni $i = 1, 2, \ldots, n$ la n-upla di numeri reali

$$(a_{i1}\ a_{i2}\ \cdots\ a_{in})$$

è detta **i-esima riga** della matrice A. Mentre la **i-esima colonna** di A è

$$(a_{1i}\ a_{2i}\ \cdots\ a_{ni}).$$

*prodotto tra matrici*

Il **prodotto** di due matrici quadrate di ordine n, $A = (a_{ij})$, $B = (b_{ij})$ è definito

nella maniera seguente: $(a_{ij})(b_{ij}) = (c_{ij})$ dove, per ogni $i, j = 1, 2, \ldots, n$

$$c_{ij} = \sum_{r=1}^{n} a_{ir} b_{rj} \ .$$

Cioè il coefficiente di posto ij nella matrice prodotto è

$$a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \ldots + a_{in}b_{nj}$$

ovvero il prodotto (scalare) della i-esima riga di A per la j-esima colonna di B.

---

**Esempi**:

$$\begin{pmatrix} 1 & -\frac{1}{2} \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ \frac{1}{2} & -2 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + (-\frac{1}{2} \cdot \frac{1}{2}) & 1 \cdot (-1) + (-\frac{1}{2}) \cdot (-2) \\ -2 \cdot 0 + 3 \cdot \frac{1}{2} & -2 \cdot (-1) + 3 \cdot (-2) \end{pmatrix} = \begin{pmatrix} -\frac{1}{4} & 0 \\ \frac{3}{2} & -4 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & \frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{2} & 1 \\ 3 & 0 & 1 \\ -2 & \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 1 \\ 5 & \frac{1}{4} & 2 \\ 3 & -\frac{1}{4} & \frac{1}{2} \end{pmatrix}.$$

---

Si verifica che, per ogni $n \geq 1$ il prodotto di matrici quadrate di ordine n è una operazione associativa. Inoltre la **matrice identica** *matrice identica*

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

è l'elemento identico. Quindi $(M_n(\mathbb{R}), \cdot)$ è un monoide. Se $n \geq 2$ il prodotto di matrici non è commutativo, ad esempio:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Ad ogni matrice quadrata reale A è associato un numero reale $|A| = Det(A)$ detto **determinante** di A. La definizione generale di determinante di una matrice e le sue proprietà sono parte del corso di Geometria. Qui ricordo solo il caso di matrici di ordine $n = 2, 3$. (Una matrice di ordine 1 è un numero reale e coincide con il suo determinante) *determinante*

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = Det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \cdot \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} + (-1)a_{12}Det \cdot \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \cdot \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}.$$

Ad esempio

$$\begin{vmatrix} 1 & 0 & -1 \\ 0 & 2 & \frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \end{vmatrix} = 1 \cdot \begin{vmatrix} 2 & \frac{1}{2} \\ 1 & 0 \end{vmatrix} + (-1)0 \cdot \begin{vmatrix} 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 \end{vmatrix} + (-1) \cdot \begin{vmatrix} 0 & 2 \\ -\frac{1}{2} & 1 \end{vmatrix} =$$

$$= 1(2 \cdot 0 - 1\frac{1}{2}) - 0 - 1(0 \cdot 1 - 2(-\frac{1}{2})) = -\frac{1}{2} - 0 - 1 = -\frac{3}{2}.$$

Una proprietà molto importante del determinante è che per ogni $A, B \in M_n(\mathbb{R})$:

$$Det(A \cdot B) = Det(A)Det(B).$$

Inoltre, per ogni $n \geq 1, Det(I_n) = 1$.

*matrici invertibili*

Un altro fatto fondamentale (che qui non proviamo) è che una matrice $A \in M_n(\mathbb{R})$ è **invertibile** se e solo se $Det(A) \neq 0$.
Dunque $\{ A \in M_n(\mathbb{R}) \mid Det(A) \neq 0 \}$ è l'insieme degli elementi invertibili di $M_n(\mathbb{R})$ e quindi, con l'operazione di prodotto righe per colonne, è un **gruppo** che si denota con $GL(n, \mathbb{R})$ e si chiama il gruppo Lineare Generale di ordine n su $\mathbb{R}$.

Rimandiamo ad un testo di Algebra Lineare per le regole generali per determinare la inversa di una matrice invertibile. Qui riporto, al fine di comprendere esempi ed esercizi, il caso $n = 2$.

Sia $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathbb{R})$ (quindi $\Delta = Det(A) \neq 0$ ). Allora

$$A^{-1} = \begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix}.$$

Ha senso considerare matrici quadrate, prodotto di matrici, e determinanti, anche a coefficienti in $\mathbb{Q}$, $\mathbb{C}$, o in $\mathbb{Z}$; o più in generale su ogni insieme R dotato di operazioni di somma e moltiplicazione con determinate proprietà (gli anelli commutativi). L'insieme di esse costituisce un monoide e si denota con $M_n(\mathbb{Q})$, $M_n(\mathbb{Z})$ etc.
Nel caso di coefficienti in $\mathbb{Z}$ risulta che le matrici invertibili in $M_n(\mathbb{Z})$ sono quelle il cui determinante è 1 o -1, e costituiscono un gruppo denotato con $GL(n, \mathbb{Z})$.

**Esempi.** 1) Consideriamo la matrice

$$g = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL(2, \mathbb{R}) .$$

e consideriamo il gruppo ciclico $G =< g >$. L'elemento identico di tale gruppo è la matrice identica di ordine 2. Proviamo per induzione che per ogni $n \in \mathbb{N}$ si ha $g^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Infatti ciò è vero per $n = 0, 1$; supposto vero per $n$ si ha

$$g^{n+1} = g^n g = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+0 & 1+n \\ 0+0 & 0+1 \end{pmatrix} = \begin{pmatrix} 1 & n+1 \\ 0 & 1 \end{pmatrix}$$

dunque l'affermazione è provata. Osserviamo quindi che per $0 > z \in \mathbb{Z}$ si ha

$$g^z = (g^{|z|})^{-1} = \begin{pmatrix} 1 & |z| \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -z \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} .$$

In questo caso quindi, per ogni $0 \neq z \in \mathbb{Z}$ si ha $g^z \neq 1_G$ , e $g^x = g^y$ se e solo se $x = y$. In particolare quindi $|G| = \infty$.
Provate inoltre per esercizio che i soli possibili generatori del gruppo $G$ sono la matrice $g$ e la sua inversa (dimostrate cioè che se $z \neq \pm 1$ allora il sottogruppo generato da $g^z$ non contiene $g$), e che l'omomorfismo $\gamma : \mathbb{Z} \to G$, definito da $\gamma(z) = g^z$, è un isomorfismo.

2) Consideriamo la matrice

$$h = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in GL(2, \mathbb{R}) .$$

e consideriamo il gruppo ciclico $H =< h >$. Facendo i calcoli, si trova

$$h^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \qquad h^3 = h^2 h = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

e così via :

$$h^4 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} \qquad h^5 = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \qquad h^6 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 = 1_H .$$

Abbiamo in particolare trovato un intero strettamente positivo $n = 6$ tale che $h^6 = 1_H$ e 6 è il **più piccolo** naturale non nullo per cui avviene ciò. (Si osservi anche che $h^5 = h^{-1}$ )
Ora, dato $z \in \mathbb{Z}$, lo dividiamo per 6: $z = 6q + r$ con $r \in \{0, 1, 2, 3, 4, 5\}$. Si ha allora:

$$h^z = h^{6q+r} = (h^6)^q h^r = 1^q h^r = h^r .$$

Dunque possiamo concludere che

$$H =< h >= \{ \ h^r \mid 0 \leq r \leq 5 \ \} = \{ \ h^0 = 1, \ h, \ h^2, \ h^3, \ h^4, \ h^5 \ \}$$

e $| < h > | = 6$.

### 1.3.7 Isometrie.

Fissiamo le notazioni. Sia $n$ un numero intero $n \geq 2$; e poniamo $V = \mathbb{R}^n$. Con $V$ intendiamo lo **spazio euclideo** delle $n$-uple di numeri reali; ovvero l'insieme *spazio euclideo*

$$\{(x_1, x_2, \ldots, x_n) \mid x_i \in \mathbb{R}\}$$

provvisto della *distanza euclidea* $d$ definita nel modo corrente: se $\underline{x} = (x_1, x_2, \ldots, x_n)$ e $\underline{y} = (y_1, y_2, \ldots, y_n)$ sono elementi di $\mathbb{R}^n$, allora la loro distanza è il numero reale positivo

$$d(\underline{x}, \underline{y}) = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \ldots + (x_n - y_n)^2}.$$

Una **isometria** di $V$ è un'applicazione $\phi : V \to V$ che conserva le distanze, ovvero tale che, per ogni $\underline{x}, \underline{y} \in V$: *isometrie*

$$d(\phi(\underline{x}), \phi(\underline{y})) = d(\underline{x}, \underline{y}).$$

Indichiamo con $M_n$ l'insieme di tutte le isometrie di $V = \mathbb{R}^n$.

È chiaro che la composizione di due isometrie è un'isometria. Inoltre:

**Teorema 1.3.4.** *Ogni isometria è un'applicazione biettiva. L'inversa di una isometria è un'isometria.*

Da ciò segue f che $M_n$, con l'operazione di composizione, è un gruppo, detto *Gruppo delle isometrie* di $\mathbb{R}^n$.

### 1.3.8 Esercizi.

ESERCIZI

**Esercizio 1.13.** Si scriva la tavola di moltiplicazione di $S_3$.

**Esercizio 1.14.** Nel gruppo moltiplicativo $\mathbb{Q}^*$ si considerino i sottogruppi

$$A = < -\frac{1}{2} >, \qquad B = < \frac{1}{3} >, \qquad C = < -2 >, \qquad D = < 2 > \ .$$

Si determinino $A \cap B$, $A \cap C$, $C \cap D$.

**Esercizio 1.15.** Sia **R** un rettangolo i cui lati adiacenti hanno lunghezza diversa. Si provi che il gruppo delle simmetrie di **R** è commutativo, ha ordine 4, e tutti i suoi elementi hanno ordine 2.

**Esercizio 1.16.** Sia $L$ un alfabeto con almeno due simboli distinti, e sia $X$ l'insieme di tutte le terne ordinate di elementi di $L$. Su $X$ sia definita l'operazione $\#$ ponendo, per ogni $\mathrm{x}, \mathrm{y}, \mathrm{z}, \mathrm{x}', \mathrm{y}', \mathrm{z}' \in L$:

$$\mathrm{xyz} \,\#\, \mathrm{x'y'z'} = \mathrm{xy'z}$$

(a) Si dimostri che $(X, \#)$ è un semigruppo. E' commutativo?

(b) Dati elementi distinti x e y di $L$, si dica, motivando la risposta, se l'elemento xxy appartiene oppure no al sottosemigruppo generato dagli elementi xyx e yxx.

(c) Si dica se $(X, \#)$ è un monoide, determinandone in caso affermativo l'identità.

**Esercizio 1.17.** Si provi che nel monoide $M_2(\mathbb{R})$ non vale la legge di cancellazione.

**Esercizio 1.18.** Si provi che l'insieme

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{R},\ a \neq 0 \neq d \right\}$$

è un sottogruppo del gruppo $GL(2, \mathbb{R})$.

**Esercizio 1.19.** Sia

$$G = \left\{ \begin{pmatrix} x & 0 & y \\ a & x & a \\ 0 & 0 & x-y \end{pmatrix} \mid a, x, y \in \mathbb{R}\ ,\ 0 \neq x \neq y \right\}.$$

Si provi che $G$ è un sottogruppo del gruppo $GL_3(\mathbb{R})$. Si provi quindi che l'applicazione $\phi : G \to \mathbb{R}^*$, definita da:

$$\phi \begin{pmatrix} x & 0 & y \\ a & x & a \\ 0 & 0 & x-y \end{pmatrix} = x$$

è un omomorfismo del gruppo $G$ nel gruppo moltiplicativo dei numeri reali non nulli.

**Esercizio 1.20.** Sia $\mathbb{C}^*$ il gruppo moltiplicativo dei numeri complessi non nulli e sia

$$G = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a, b \in \mathbb{R},\ (a, b) \neq (0, 0) \right\}\ .$$

a) Si provi che $G$ è un sottogruppo del gruppo $GL(2, \mathbb{R})$ delle matrici quadrate invertibili di ordine 2 su $\mathbb{R}$.

b) Si determinino tutte le matrici $A \in G$ tali che $A^3 = 1$.

**Esercizio 1.21.** Sia $M$ un monoide e $X$ un insieme non vuoto. Sull'insieme $M^X$ di tutte la applicazioni di $X$ in $M$ si definisca una operazione $(f, g) \mapsto f \cdot g$ ponendo, per ogni $f, g \in M^X$ e ogni $x \in X$ : $(f \cdot g)(x) = f(x)g(x)$. Si provi che $(M^X, \cdot)$ è un monoide.

**Esercizio 1.22.** Sia $(S, \cdot)$ un semigruppo che gode della seguente proprietá: per ogni $x, y \in S$ : $xyx = y$. Si dimostri che $S$ è un gruppo commutativo tale che $x^2 = 1$ per ogni $x \in S$.

**Esercizio 1.23.** Sia $S = \mathbb{R}^{\mathbb{R}}$ l'insieme di tutte le applicazioni di $\mathbb{R}$ in se stesso. Su $S$ si definisca l'operazione $*$ ponendo, per ogni $f, g \in S$:

$$f * g(x) = \begin{cases} f(x) & \text{se } x \leq 0 \\ g(x) & \text{se } x > 0 \end{cases} \quad \text{per ogni } x \in \mathbb{R}$$

Si dimostri che $(S, *)$ è un semigruppo. E' un monoide ?

# Capitolo 2

# Anelli, Polinomi e Campi

## 2.1 Anelli

*Anello* è il termine usato ad indicare una classe di strutture algebriche dotate di due operazioni, il cui modello fondamentale è l'insieme $\mathbb{Z}$ dei numeri interi con le operazioni usuali di somma e prodotto (moltiplicazione). Infatti, il concetto di anello ha la sua origine dalla teoria di numeri, ed è sorto dall'idea di astrarre le proprietà fondamentali che caratterizzano (per quanto riguarda le due operazioni fondamentali) gli insiemi di numeri (interi, reali o complessi).

### 2.1.1 Definizioni e prime proprietà.

*assiomi d'anello*

Un **anello** è un insieme $A$ dotato di due operazioni $+$ , $\cdot$ (che saranno sempre chiamate somma e prodotto), che soddisfano le seguenti proprietà:

**(S1)** $a + (b + c) = (a + b) + c \quad \forall a, b, c, \in A$ (*associatività* della somma)

**(S2)** $a + b = b + a$ per ogni $a, b \in A$ (*commutatività* della somma)

**(S3)** esiste $0_A \in A$ tale che, per ogni $a \in A$, $a + 0_A = a$ (*elemento neutro* per la somma)

**(S4)** per ogni $a \in A$ esiste $a' \in A$ tale che $a + a' = 0_A$ (esistenza degli *opposti*)

**(P1)** $a(bc) = (ab)c$ per goni $a, b, c, \in A$ (*associatività* del prodotto)

**(P2)** esiste $1_A \in A$ tale che, per ogni $a \in A$, $a1_A = a = 1_A a$ (*elemento neutro* per il prodotto), ed inoltre $1_A \neq 0_A$

**(D)** Valgono le **proprietà distributive** del prodotto rispetto alla somma, ovvero, per ogni $a, b, c \in A$: *distributività*

$$a(b+c) = ab + ac$$

$$(b+c)a = ba + ca \ .$$

**Esempi.** Sono anelli, con le usuali operazioni di somma e prodotto, gli insiemi numerici $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Altri esempi di anelli sono gli anelli di matrici quadrate $M_n(\mathbb{R})$ con le usuali operazioni di somma (per componenti) e prodotto (righe $\times$ colonne) di matrici quadrate.

Sarà risultato immediato che gli assiomi di anello relativi alla somma (da (S1) a (S4)) equivalgono alla richiesta che $(A, +)$ sia un gruppo (additivo) commutativo, e che gli assiomi che riguardano il prodotto ((P1) e (P2)), con quella che $(A, \cdot)$ sia un monoide moltiplicativo. Dalla teoria generale dei gruppi e dei monoidi, discendono quindi immediatamente alcune delle proprietà generali e di base degli anelli, che per comodità elenchiamo nella seguente Proposizione. *proprietà elementari*

**Proposizione 2.1.1.** *Sia $A$ un anello. Allora,* *proprietà della somma*

*(1) esiste un unico elemento neutro $0_A$ per la somma (che si chiama* zero *di $A$);*
*(2) per ogni $a \in A$ esiste un unico elemento $-a$ (detto* l'opposto *di $a$) tale che $a + (-a) = 0_A$;*
*(3) vale la legge di cancellazione per la somma; ovvero per ogni $a, b, c \in A$,*

$$a + b = a + c \quad \Rightarrow \quad b = c.$$

*(4) esiste un unico elemento neutro $1_A$ per il prodotto;*

Dagli assiomi che seguono di fatto e direttamente anche molte di quelle proprietà delle operazioni che utilizziamo familiarmente nel caso di anelli numerici. Prima di dimostrarle fissiamo la familiare convenzione che, se $a$ e $b$ sono elementi dell'anello $A$, si adotta la seguente notazione: $a - b = a + (-b)$.

**Proposizione 2.1.2.** *Sia $A$ un anello, e siano $a, b \in A$. Allora* *proprietà del prodotto*

1. $a0_A = 0_A a = 0_A$.
2. $a(-b) = -(ab) = (-a)b$.
3. $(-a)(-b) = ab$.

*Dimostrazione.* 1) Sia $c = a0_A$. Allora, applicando la proprietà distributiva:

$$c = a0_A = a(0_A + 0_A) = a0_A + a0_A = c + c$$

e quindi $c = c + c - c = c - c = 0_A$. Analogamente si dimostra che $0_A a = 0_A$.

2) Proviamo che $a(-b) = -(ab)$. Applicando la proprietà distributiva ed il punto 1):

$$a(-b) + ab = a(-b + b) = a0_A = 0_A$$

e quindi, $a(-b) = -(ab)$. Analogamente si dimostra che $(-a)b = -(ab)$.

3) Per il punto 1) si ha $(-a)(-b) = -(a(-b)) = -(-(ab)) = ab$. ∎

---

*Nota.* In alcuni testi, la definizione di anello viene data senza richiedere l'esistenza dell'elemento neutro per la moltiplicazione (cioè senza inculdere l'assioma (P2)). Da questo punto di vista, un anello nel senso che invece adottiamo noi viene chiamato **anello con unità**. Ribadisco quindi che, secondo la definizione da noi adottata, un anello $A$ ha **sempre** l'unità $1_A$. Un anello $R$ si dice *degenere* se $0_R = 1_R$; in tal caso (lo si dimostri), $R$ è costituito dal solo elemento $0_R$. Con il termine *anello* noi intenderemo **sempre** un *anello non degenere*, quindi tale che $0_R \neq 1_R$.

---

*anelli commutativi*

Un anello $A$ si dice **commutativo** se il prodotto è commutativo, ovvero se, per ogni $a, b \in A$ si ha $ab = ba$.

**Esempi** 1) sono commutativi gli anelli $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, mentre non sono commutativi gli anelli di matrici $M_n(\mathbb{R})$, con $n \geq 2$.

*anello delle funzioni reali*

2) Come altro **esempio (importante)**, consideriamo l'insieme $\mathbb{R}^{\mathbb{R}}$ di tutte le applicazioni dall'insieme dei numeri reali in se stesso, con le abituali operazioni di somma e moltiplicazione di funzioni reali. Quindi, se $f, g \in \mathbb{R}^{\mathbb{R}}$ allora $f + g$ e $fg$ sono definite da, per ogni $x \in \mathbb{R}$,

$$(f + g)(x) = f(x) + g(x)$$
$$(fg)(x) = f(x)g(x)$$

(attenzione: qui il prodotto non è la composizione di applicazioni). Si verifica facilmente che, con tali operazioni, $\mathbb{R}^{\mathbb{R}}$ è un anello commutativo, il cui zero ed uno sono, rispettivamente, le funzioni costanti $c_0$ e $c_1$ definite da, per ogni $x \in \mathbb{R}$,

$$c_0(x) = 0, \qquad c_1(x) = 1.$$

*anelli di Boole*

3) Questo esempio è più curioso (ma ha importanti applicazioni nei sistemi binari). Sia $X$ un insieme non vuoto, e $\mathcal{P}(X)$ l'insieme delle parti di $X$ (si veda il paragrafo 1.31). Allora si vede (con un po' di lavoro di verifica non difficile ma noioso) che, dotato delle operazioni di differenza simmetrica $\Delta$ (come somma) e di intersezione $\cap$ (come prodotto), $\mathcal{P}(X)$ è un anello, il cui zero è l'insieme vuoto $\emptyset$, ed 1 è

l'insieme ambiente $X$. Poiché l'operazione di intersezione è commutativa, l'anello $(\mathcal{P}(X), \Delta, \cap)$ è un anello commutativo.

---

**Potenze.** In un generico anello è possibile definire l'elevazione a potenza per un intero positivo, come visto per i monoidi: se $A$ è un anello, allora per ogni $a \in A$ e per ogni $n \in \mathbb{N}$, la potenza $n$-esima $a^n$ di $a$ si definisce induttivamente nella maniera seguente: *potenze*

$$a^0 = 1_A \qquad \text{e} \qquad a^{n+1} = a^n a.$$

In pratica, se $n \in \mathbb{N}$,

$$a^n = \underbrace{a \cdot a \cdot \ldots \cdot a}_{\text{n volte}}$$

Ricordo le proprietà già osservate per i monoidi:

**Proposizione 2.1.3.** *Sia $A$ un anello, $a \in A$, e siano $n, m \in \mathbb{N}$. Allora*

*(i)* $a^{n+m} = a^n a^m$ ;

*(ii)* $a^{nm} = (a^n)^m$ .

*Dimostrazione.* (i) Procediamo per induzione su $m \in \mathbb{N}$. Se $m = 0$, si ha $a^{n+0} = a^n = a^n \cdot 1_A = a^n a^0$.
Sia ora $m \geq 0$, e per ipotesi induttiva, sia $a^{n+m} = a^n a^m$. Allora,

$$\begin{aligned} a^{n+(m+1)} &= a^{(n+m)+1} = a^{n+m}a \qquad \text{(per definizione)} \\ &= (a^n a^m)a \qquad\qquad \text{(per ipotesi induttiva )} \\ &= a^n(a^m a) = a^n a^{m+1} \qquad \text{(per definizione).} \end{aligned}$$

(ii) La dimostrazione di questo punto è lasciata per esercizio: si proceda ancora per induzione su $m$, utilizzando anche il punto (i). ∎

**Osservazione.** In generale, in un anello non commutativo, non è detto che, dati $a, b \in A$ e $n \in \mathbb{N}$, valga $(ab)^n = a^n b^n$ (si veda l'esercizio 2.11 per un esempio). Tuttavia, non è difficile provare che se $ab = ba$ allora si ha, per ogni $n \geq \mathbb{N}$, $(ab)^n = a^n b^n$.
In particolare, questa ulteriore proprietà delle potenze sussiste negli anelli commutativi, ai quali non è difficile estendere quindi il Teorema del binomio di Newton. Precisamente

**Proposizione 2.1.4.** *Sia $A$ un anello commutativo, e siano $a, b \in A$. Allora per ogni $n \in \mathbb{N}$,* *formula del binomio di Newton*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i \ .$$

Si sarà osservato che, nell'enunciato di questa proposizione, viene dato un senso anche ad una scrittura del tipo $na$ per $a \in A$, e $n \in \mathbb{N}$ (infatti i coefficienti binomiali che compaiono nella formula sono numeri interi). Questo va definito, ed è il corrispondente per la somma di quello che le potenze sono rispetto al prodotto (e si può fare con interi anche negativi).

Se $A$ è un gruppo anello, $a \in A$ e $n \in \mathbb{N}$, si scrive

$$0a = 0_A;$$
$$na = a + a + \ \ldots \ + a \qquad \text{(n volte)};$$
$$(-n)a = n(-a) = -(na).$$

L'elemento $na$ si chiama il multiplo $n$-esimo di $a$.

In modo del tutto analogo a quanto visto per il prodotto, si prova facilmente che, per ogni $a \in A$ ed ogni $m, n \in \mathbb{Z}$,

$$(n+m)a = na + ma \qquad\qquad (nm)a = n(ma)\ .$$

---

*sottoanelli*

Il concetto di sottoanello si presenta in modo naturale.

**Definizione**.Un sottoinsieme non vuoto $S$ di un anello $A$ si dice **sottoanello** di $A$ se soddisfa alle seguenti condizioni

(1) $a - b \in S$, per ogni $a, b \in S$;

(2) $ab \in S$, per ogni $a, b \in S$ e $1_A \in S$.

Se $S$ è un sottoanello di $A$, allora è chiaro che in $S$ sono soddisfatte le proprietà distributive (in quanto casi particolari delle proprietà analoghe di $A$). Quindi $S$ risulta, con le operazioni indotte da $A$, un anello esso stesso, con la stessa unità di $A$ ($1_S = 1_A$). Similmente, un sottoanello di un anello commutativo è un anello commutativo.

**Esempi.** 1) $\mathbb{Z}$ è un sottoanello di $\mathbb{Q}$, il quale, a sua volta, è un sottoanello di $\mathbb{R}$ (che è sottoanello di $\mathbb{C}$).

2) Conviene subito mostrare che l'insieme dei reali $\mathbb{R}$, ammette numerosi sottoanelli. Ad esempio, consideriamo il seguente sottoinsieme di $\mathbb{R}$

$$\mathbb{Q}[\sqrt{2}] = \{\ a + b\sqrt{2} \mid a, b \in \mathbb{Q}\ \}\ ,$$

e verifichiamo che è un sottoanello dell'anello $\mathbb{R}$. Infatti, se $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$ sono due elementi di $\mathbb{Q}[\sqrt{2}]$ (quindi $a, b, c, d \in \mathbb{Q}$), allora $x - y = (a-c) + (b-d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$ , e $xy = (a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2cd)+(ad+bc)\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$; infine $1 = 1 + 0\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$.

3) Se denotiamo con $\mathcal{C}(\mathbb{R})$ il sottoinsieme di $\mathbb{R}^{\mathbb{R}}$ (l'anello delle funzioni reali - esempio a pag. 34) costituito dalle applicazioni **continue**, allora noti teoremi di Analisi assicurano che $\mathcal{C}(\mathbb{R})$ è un sottoanello di $\mathbb{R}^{\mathbb{R}}$.

### 2.1.2 Tipi di anello.

Si sarà osservato che, trattando delle proprietà elementari del prodotto in un anello (Proposizione 2.1.2), non abbiamo enunciato alcuna legge di cancellazione per il prodotto. La ragione di ciò è che in genere essa non è verificata (e quindi *non* discende dagli assiomi di anello). Si consideri ad esempio l'anello $M_2(\mathbb{R})$ delle matrici quadrate di ordine 2 sui numeri reali; in tale anello troviamo, tra i molti esempi:

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

Anche in anelli commutativi si possono verificare casi del genere. Si consideri l'anello delle funzioni reali $\mathbb{R}^{\mathbb{R}}$ (o anche l'anello delle funzioni reali continue $\mathcal{C}(\mathbb{R})$): se, ad esempio, $f, g$ sono le funzioni definite da

$$f(x) = \begin{cases} 0 & \text{se} \quad x \leq 0 \\ x & \text{se} \quad x \geq 0 \end{cases} \qquad g(x) = \begin{cases} x & \text{se} \quad x \leq 0 \\ 0 & \text{se} \quad x \geq 0 \end{cases}$$

allora $f, g$ sono funzioni continue, diverse dalla funzione zero, e tali che

$$f \cdot g = 0 = 0 \cdot g.$$

Dagli esempi precedenti (soprattutto il secondo), si intuisce come, in un certo anello, ci sia una qualche relazione tra il fallire della legge di cancellazione per il prodotto e l'esistenza di elementi non nulli il cui prodotto è zero. Ciò di fatto è vero, e per trattare questo punto, conviene partire dalla seconda possibilità.

*divisori dello zero*

Un elemento $a$ di un anello $A$ si dice **divisore dello zero** se $a \neq 0_A$ ed esiste $b \neq 0_A$ tale che $ab = 0_A$.

Esempi di divosori dello zero (nell'anello $\mathbb{R}^{\mathbb{R}}$) sono quindi le funzioni $f$ e $g$ descritte sopra. Altri facili esempi di divisori dello zero si possono trovare negli anelli di matrici; ad esempio, in $M_2(\mathbb{R})$:

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

*domini di integrità*

Un anello commutativo privo di divisori dello zero si dice un **Dominio d'integrità**. Quindi un anello commutativo è un Dominio d'Integrità se e solo se il prodotto di elementi diversi da zero è diverso da zero.

Quindi, gli anelli $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ sono domini d'integrità, mentre l'anello delle matrici $M_2(\mathbb{R})$o quello delle funzioni reali $\mathbb{R}^{\mathbb{R}}$ non lo sono.

**Proposizione 2.1.5. (Legge di cancellazione)** *Sia $A$ un dominio d'integrità. Allora, per ogni $a, bc \in A$ con $c \neq 0_A$, si ha*

legge di cancellazione

$$ac = bc \qquad \Rightarrow \qquad a = b\ .$$

*Dimostrazione.* Siano $a, b \in A,\ 0_A \neq c \in A$ con $ac = bc$. Allora $0_A = ac - bc = (a-b)c$. Poichè $A$ è privo di divisori dello zero e $c \neq 0_A$, deve essere $a - b = 0_A$, cioè $a = b$. ∎

Un elemento $a$ di un anello $A$ si dice un **invertibile** di $A$ se esiste un elemento $b \in A$ tale che $ab = 1_A = ba$.

elementi invertibili

Come abbiamo dimostrato nel caso delle applicazioni, si prova facilmente che un elemento invertibile $a$ di un anello $A$ ha un unico inverso (che si denota con $a^{-1}$).

**Proposizione 2.1.6.** *Sia $A$ una anello, e sia $a$ un elemento invertibile di $A$. Allora esiste un unico $b \in A$ tale che $ab = 1_A = ba$.*

*Dimostrazione.* Sia $a$ un invertibile di $A$, e siano $b$ e $c$ inversi di $a$. Allora

$$b = b1_A = b(ac) = (ba)c = 1_A c = c.$$

∎

Ad esempio, gli elementi invertibili dell'anello $\mathbb{Z}$ sono 1 e $-1$; gli elementi invertibili dell'anello delle matrici $M_n(\mathbb{R})$ sono le matrici con determinante diverso da 0.

**Esercizio 2.1.** Si provi che gli elementi invertibili dell'anello $\mathbb{R}^{\mathbb{R}}$ sono tutte le funzioni $f \in \mathbb{R}^{\mathbb{R}}$ tali che $f(x) \neq 0$ per ogni $x \in \mathbb{R}$.

A questo punto osserviamo che l'essere un certo elemento invertibile dipende in modo essenziale dall'intero anello che stiamo considerando. Ad esempio, l'anello $\mathbb{Z}$ ha solo due elementi invertibili (1 e $-1$), mentre. quando passiamo all'anello $\mathbb{Q}$ dei numeri razionali, vediamo che ogni numero intero $\neq 0$ ha inverso in $\mathbb{Q}$. In effetti. $\mathbb{Q}$ soddisfa la notevole proprietà che ogni suo elemento diverso da zero è invertibile. Anelli con questa proprietà sono estremamente importanti.

**Definizione**. Un anello commutativo $A$ si dice un **campo** se ogni suo elemento non nullo è un invertibile.

Campi

Ad esempio sono campi gli anelli $\mathbb{Q},\ \mathbb{R},\ \mathbb{C}$.

**Proposizione 2.1.7.** *Ogni campo è un dominio d'integrità.*

*Dimostrazione.* Sia $F$ un campo e $0_F \neq a \in F$. Supponiamo che $b \in F$ sia tale che $ab = 0_F$. Allora $b = 1_F b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0_F = 0_F$, quindi $a$ non è un divisore dello zero. ∎

### 2.1.3 Esercizi.

ESERCIZI

**Esercizio 2.2.** Si completi la dimostrazione della proposizione 2.1.3, e quella della osservazione seguente.

**Esercizio 2.3.** Sia $X$ un insieme non vuoto. Si provi che l'insieme delle parti $\mathcal{P}(X)$ con le operazioni di differenza simmetrica $\Delta$ (come somma) e intersezione $\cap$ (come prodotto) è un anello commutativo. Si osservi che per ogni $Y \in \mathcal{P}(X)$ si ha $Y^2 = Y$. Si provi che, se $|X| \geq 2$, allora l'anello $\mathcal{P}(X)$ non è un dominio d integrità.

**Esercizio 2.4.** Sia $R$ un anello. Si provi che $Z(R) = \{\ a \in R \mid ab = ba \ \ \forall b \in R\ \}$ è un sottoanello di $R$. ($Z(R)$ è detto il centro di $R$).

**Esercizio 2.5.** Si verifichi che l'insieme $\mathbb{Z}[i] = \{\mathrm{a} + \mathrm{ib} \mid \mathrm{a}, \mathrm{b} \in \mathbb{Z}\}$ é un sottoanello dell'anello $\mathbb{C}$ dei numeri complessi ($\mathbb{Z}[i]$ è detto *anello degli interi di Gauss*).

**Esercizio 2.6.** Sia $p$ un numero primo fissato e sia

$$R = \{\ \frac{m}{p^i} \mid m \in \mathbb{Z}\ , i \in \mathbb{N}\ \}.$$

Si provi che $R$ è un sottoanello dell'anello $\mathbb{Q}$ dei numeri razionali.

## 2.2 Esempi

### 2.2.1 Anelli di classi di congruenza.

Sia $n \geq 2$. L'insieme $\mathbb{Z}/n\mathbb{Z}$ di tutte le classi di congruenza modulo $n$ (studiato lo scorso anno), fornisce un importante caso di anello commutativo.
Ovviamente, dobbiamo iniziare con il definire opportune operazioni di somma e di prodotto sull'insieme $\mathbb{Z}/n\mathbb{Z}$.

Sia quindi fissato il modulo $n \geq 2$. Denotando con $\overline{a}$ la classi di congruenza modulo

anelli di classi di resto

$n$ di $a \in \mathbb{Z}$, si ha $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}]|$. Siano $a, b \in \mathbb{Z}$; allora

$$\overline{a} = a + n\mathbb{Z} = \{a + nz \mid z \in \mathbb{Z}\} \qquad \overline{b} = b + n\mathbb{Z} = \{b + nz \mid z \in \mathbb{Z}\}.$$

sono sottoinsiemi non vuoti dell'anello $\mathbb{Z}$, che possiamo quindi sommare secondo la regola

$$\begin{aligned} \overline{a} + \overline{b} &= \{\ x + y \mid x \in \overline{a},\, y \in \overline{b}\ \} = \{\ (a + nz_1) + (b + nz_2) \mid z_1, z_2 \in \mathbb{Z}\ \} = \\ &= \{\ (a + b) + n(z_1 + z_2) \mid z_1, z_2 \in \mathbb{Z}\ \} = \{\ (a + b) + nz \mid z \in \mathbb{Z}\ \} = \\ &= \overline{a + b}. \end{aligned}$$

In pratica, *la somma di classi di congruenza modulo $n$ è ancora una classe di congruenza modulo $n$*, che è descritta dalla regola

$$\overline{a} + \overline{b} = \overline{a + b}.$$

Questo definisce un'operazione di somma sull'insieme $\mathbb{Z}/n\mathbb{Z}$ di tutte le classi di congruenza modulo $n$. In modo simile è possibile definire un prodotto per classi di congruenza. Con gli stessi $n$, $a$ e $b$ di sopra, si pone

$$\overline{a} \cdot \overline{b} = \{\ xy \mid x \in \overline{a},\, y \in \overline{b}\ \}.$$

Quindi,

$$\begin{aligned} \overline{a} \cdot \overline{b} &= \{(a + nz_1)(b + nz_2) \mid z_1, z_2 \in \mathbb{Z}\} = \\ &= \{ab + n(az_2 + bz_1 + nz_1z_2) \mid z_1, z_2 \in \mathbb{Z}\} = \\ &= \{ab + nz \mid z \in \mathbb{Z}\ \} = \overline{ab}. \end{aligned}$$

Dunque, anche in questo caso, *il prodotto di due classi di congruenza modulo $n$ è una classe di congruenza modulo $n$*, ed è descritto da

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

Ciò definisce pertanto un'operazione di prodotto su $\mathbb{Z}/n\mathbb{Z}$.

A questo punto, risulta laborioso ma non difficile provare che l'insieme quoziente $\mathbb{Z}/n\mathbb{Z}$, con le operazioni di somma e prodotto definite sopra, è un anello commutativo, che si chiama **anello delle classi resto modulo n**. Inoltre

$$0_{\mathbb{Z}/n\mathbb{Z}} = \overline{0} = n\mathbb{Z} \qquad \text{e} \qquad 1_{\mathbb{Z}/n\mathbb{Z}} = \overline{1} = 1 + n\mathbb{Z}.$$

Si tratta di verificare proprietà che discendono naturalmente da quelle analoghe in $\mathbb{Z}$, e dalle definizioni delle operazioni. Per esempio verifichiamo la proprietà distributiva.

Siano $\overline{a}, \overline{b}, \overline{c}$, generici elementi di $\mathbb{Z}/n\mathbb{Z}$. Allora

$$\overline{a}(\overline{b}+\overline{c}) = \overline{a}\cdot\overline{(b+c)} = \overline{a(b+c)} = \overline{ab+ac} = \overline{ab}+\overline{ac} = \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}.$$

Le altre verifiche si conducono in modo simile. È altresì immediato verificare che, per ogni $k \in \mathbb{N}$, ed ogni $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$, si ha $\overline{a}^k = \overline{a^k}$.)

---

**Esempio.** 1) Nell'anello $\mathbb{Z}/6\mathbb{Z}$ eseguiamo il calcolo seguente

$$\begin{aligned}
\overline{5}-\overline{2}^3\cdot(\overline{3}+\overline{4}\cdot\overline{5})+(\overline{2}+\overline{3})^3(\overline{3}-\overline{5}) &= \overline{5}-\overline{8}\cdot(\overline{3}+\overline{20})+(\overline{2+3})^3(\overline{3-5}) = \\
&= \overline{5}-\overline{2}\cdot\overline{23}+\overline{5}^3\cdot(\overline{-2}) = \\
&= \overline{5}-\overline{2}\cdot\overline{5}+\overline{(-1)^3}\cdot\overline{4} = \\
&= \overline{5}-\overline{2}\cdot\overline{5}+\overline{(-1)}\cdot\overline{4} = \overline{5-10-4} = \overline{-9} = \overline{3}.
\end{aligned}$$

---

Proprietà di $\mathbb{Z}/n\mathbb{Z}$

Abbiamo già osservato che, per $n \geq 2$, l'anello $\mathbb{Z}/n\mathbb{Z}$ è commutativo. In generale però non è un dominio d'integrità: ad esempio, nell'anello $\mathbb{Z}/12\mathbb{Z}$ delle classi resto modulo 12, $\overline{4} \neq \overline{0}$, $\overline{3} \neq \overline{0}$, ma $\overline{4}\cdot\overline{3} = \overline{12} = \overline{0} = 0_{\mathbb{Z}/6\mathbb{Z}}$, e quindi $\overline{4}$ e $\overline{3}$ sono divisori dello zero. D'altra parte è possibile che $\mathbb{Z}/n\mathbb{Z}$ contenga elementi invertibili che non provengono da invertibili di $\mathbb{Z}$. Ad esempio, sempre in $\mathbb{Z}/12\mathbb{Z}$, l'elemento $\overline{5}$ è diverso sia da $\overline{1}$ che da $\overline{-1}$, e purtuttavia è invertibile. Infatti, in $\mathbb{Z}/12\mathbb{Z}$,

$$\overline{5}\cdot\overline{5} = \overline{25} = \overline{1} = 1_{\mathbb{Z}/12\mathbb{Z}},$$

quindi $\overline{5}$ è un elemento invertibile di $\mathbb{Z}/12\mathbb{Z}$ (e coincide con il proprio inverso). Queste osservazioni sono estese e chiarite dal Teorema seguente (la cui dimostrazione è per i lettori più motivati).

**Teorema 2.2.1.** *Sia $n \geq 2$. Allora*

1. *Un elemento $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ è invertibile in $\mathbb{Z}/n\mathbb{Z}$ se e solo se $(a,n) = 1$. Quindi, l'insieme degli elementi invertibili di $\mathbb{Z}/n\mathbb{Z}$ è $\{\overline{a} \mid 1 \leq a \leq n-1,\ (a,n) = 1\}$.*

2. *$\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se $n$ è un numero primo. Se $n$ non è primo, allora $\mathbb{Z}/n\mathbb{Z}$ non è un dominio d'integrità.*

*Dimostrazione.* 1) Sia $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$. Possiamo prendere $1 \leq a \leq n-1$ (escludiamo $\overline{a} = \overline{0}$ perchè chiaramente lo zero di un anello non è mai un invertibile - e d'altra parte, $(0,n) = n$). Per definizione, $\overline{a}$ è invertibile se e solo se esiste $1 \leq b \leq n-1$ tale che

$$\overline{ab} = \overline{a}\cdot\overline{b} = 1_{\mathbb{Z}/n\mathbb{Z}} = \overline{1}$$

ovvero, $ab \equiv 1 \pmod{n}$. Quindi, $\overline{a}$ è invertibile se e solo se esiste $1 \leq b \leq n-1$ ed un $z \in \mathbb{Z}$ tali che

$$ab + zn = 1$$

cioè se e solo se $(a, n) = 1$.

2) $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo se ogni elemento non nullo è invertibile. Quindi, per il punto 1), $\mathbb{Z}/n\mathbb{Z}$ è un campo se e solo $(a, n) = 1$ per ogni $1 \leq a \leq n-1$, e questo avviene se e solo se $n$ è un numero primo.
Supponiamo, infine, che $n$ non sia un numero primo. Dunque $n$ si fattorizza propriamente, e quindi esistono interi $2 \leq a,\, b \leq n-1$, tali che $ab = n$. Ma allora, nell'anello $\mathbb{Z}/n\mathbb{Z}$, $\overline{a}$ e $\overline{b}$ sono diversi da $0_{\mathbb{Z}/n\mathbb{Z}} = \overline{0}$, mentre $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{n} = \overline{0}$. Dunque $\overline{a}$ e $\overline{b}$ sono divisori dello zero, e quindi $\mathbb{Z}/n\mathbb{Z}$ non è un dominio d'integrità. ∎

dei nuovi campi

Un aspetto della massima importanza del risultato precedente, e che merita di essere ribadito, è che se $p$ è un numero primo positivo, allora $\mathbb{Z}/p\mathbb{Z}$ è un campo.

**Corollario 2.2.2.** *Per ogni numero primo $p$ esiste un campo di ordine $p$.*

---

**Esercizio 2.7.** Determinare le soluzioni dell'equazione $\overline{3}x^2 - \overline{2} = \overline{0}$, nel campo $\mathbb{Z}/7\mathbb{Z}$.

*Soluzione.* Poichè tutti gli elementi non nulli di $F = \mathbb{Z}/7\mathbb{Z}$ sono invertibili, possiamo moltiplicare per l'inverso di $\overline{3}$, che è $\overline{5}$ (infatti $\overline{3} \cdot \overline{5} = \overline{15} = \overline{1}$), ottenendo l'equazione equivalente

$$\overline{0} = x^2 - \overline{2} \cdot \overline{5} = x^2 - \overline{3}.$$

A questo punto, possiamo testare più facilmente gli elementi di $F$, trovando che

$$\overline{1}^2 = \overline{6}^2 = \overline{1}, \quad \overline{2}^2 = \overline{5}^2 = \overline{4}, \quad \overline{3}^2 = \overline{4}^2 = \overline{2},$$

e concludendo così che l'equazione data non ha soluzioni in $F$.

---

### 2.2.2 Anelli di matrici.

Matrici

Esempi principali di anelli non commutativi sono gli anelli di matrici. Richiamiamo qui, per comidità del lettore e senza dimostrazioni, solo alcuni fatti significativi dal nostro punto di vista, limitandoci, almeno per quanto riguarda le descrizioni dettagliate, al caso di matrici a coefficienti reali.

Sia $1 \leq n \in \mathbb{N}$. Una **matrice quadrata di ordine n** a coefficienti reali è una tabella

$$(a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}.$$

dove i coefficienti $a_{ij}$ sono numeri reali. L'insieme di tutte le matrici quadrate di ordine n a coefficienti reali si denota con $M_n(\mathbb{R})$.

somma di matrici

La **somma** $A + B$ di due matrici (reali, di ordine $n$) $A = (a_{ij})$ e $B = (b_{ij})$, è la matrice (di ordine $n$) i cui coefficienti si ottengono sommando tra loro i coefficienti corrispondenti di $A$ e $B$. Ovvero, posto $(s_{ij}) = S = A + B$, si pone $s_{ij} = a_{ij} + b_{ij}$ (per ogni $i, j = 1, \ldots, n$). Un esempio è forse superfluo, ma eccone uno con $n = 2$:

$$\begin{pmatrix} 1 & -2 \\ 6 & 3 \end{pmatrix} + \begin{pmatrix} -3 & 0 \\ 1 & -4 \end{pmatrix} = \begin{pmatrix} -2 & -2 \\ 7 & -1 \end{pmatrix}.$$

Si verifica facilemente che tale somma soddisfa gli assiomi (S1) – (S4) di anello. È cioè un'operazione transitiva, commutativa, con un elemento neutro che è la matrice nulla $0_M$ (ovvero quella con tuti i coefficienti uguali a 0), e tale che ogni matrice ha una matrice 'opposta' (definita prendendo gli opposti dei coefficienti). Ad esempio, per $n = 2$,

$$0_{M_2(\mathbb{R})} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad - \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}.$$

Se $A = (a_{ij}) \in M_n(\mathbb{R})$, allora, per ogni $i = 1, 2, \ldots, n$, la n-upla di numeri reali

$$(a_{i1}\ a_{i2}\ \cdots\ a_{in})$$

è detta **i-esima riga** della matrice A. Mentre la **i-esima colonna** di A è

$$(a_{1i}\ a_{2i}\ \cdots\ a_{ni}).$$

prodotto di matrici

Il **prodotto** di due matrici quadrate di ordine n, $A = (a_{ij})$, $B = (b_{ij})$ è definito nella maniera seguente: $(a_{ij})(b_{ij}) = (c_{ij})$ dove, per ogni $i, j = 1, 2, \ldots, n$

$$c_{ij} = \sum_{r=1}^{n} a_{ir} b_{rj}. \tag{2.1}$$

Cioè il coefficiente di posto ij nella matrice prodotto è

$$a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j} + \ldots + a_{in}b_{nj}$$

ovvero il prodotto (scalare) della i-esima riga di A per la j-esima colonna di B.

*Esempi*:

$$\begin{pmatrix} 1 & -\frac{1}{2} \\ -2 & 3 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ \frac{1}{2} & -2 \end{pmatrix} = \begin{pmatrix} 1 \cdot 0 + (-\frac{1}{2} \cdot \frac{1}{2}) & 1 \cdot (-1) + (-\frac{1}{2}) \cdot (-2) \\ -2 \cdot 0 + 3 \cdot \frac{1}{2} & -2 \cdot (-1) + 3 \cdot (-2) \end{pmatrix} = \begin{pmatrix} -\frac{1}{4} & 0 \\ \frac{3}{2} & -4 \end{pmatrix}.$$

$$\begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & \frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & \frac{1}{2} & 1 \\ 3 & 0 & 1 \\ -2 & \frac{1}{2} & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 1 \\ 5 & \frac{1}{4} & 2 \\ 3 & -\frac{1}{4} & \frac{1}{2} \end{pmatrix}.$$

Si verifica che, per ogni $n \geq 1$ il prodotto di matrici quadrate di ordine n è una operazione associativa. Inoltre la **matrice identica** matrice identica

$$I_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

è l'elemento identico. Sono quindi soddisfatti anche gli assiomi (P1) (P2) (ovvero $(M_n(\mathbb{R}), \cdot)$ è un monoide). Si verifica poi che sussistono anche le proprietà distributive. Dunque, per ogni $n \geq 1$, $M_n(\mathbb{R})$ **è un anello**.

Se $n \geq 2$ il prodotto di matrici *non è commutativo*, ad esempio:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

(per $n = 1$, $M_1(\mathbb{R})$ coincide con $\mathbb{R}$).

Ad ogni matrice quadrata reale A è associato un numero reale $|A| = Det(A)$ detto **determinante** di A. La definizione generale di determinante di una matrice e le sue proprietà sono parte della cosiddetta Algebra Lineare. Qui ricordo solo il caso di matrici di ordine $n = 2, 3$. (Una matrice di ordine 1 è un numero reale e coincide con il suo determinante) determinante

$$Det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc$$

$$Det \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} = a_{11} Det \begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} + (-1) a_{12} Det \begin{pmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{pmatrix} + a_{13} Det \begin{pmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}$$

Ad esempio

$$Det \begin{pmatrix} 1 & 0 & -1 \\ 0 & 2 & \frac{1}{2} \\ -\frac{1}{2} & 1 & 0 \end{pmatrix} = 1 \cdot Det \begin{pmatrix} 2 & \frac{1}{2} \\ 1 & 0 \end{pmatrix} + (-1) 0 \cdot Det \begin{pmatrix} 0 & \frac{1}{2} \\ -\frac{1}{2} & 0 \end{pmatrix} + (-1) \cdot Det \begin{pmatrix} 0 & 2 \\ -\frac{1}{2} & 1 \end{pmatrix} =$$

$$= 1(2 \cdot 0 - 1\frac{1}{2}) - 0 - 1(0 \cdot 1 - 2(-\frac{1}{2})) = -\frac{1}{2} - 0 - 1 = -\frac{3}{2}.$$

Una proprietà molto importante del determinante è che per ogni $A, B \in M_n(\mathbb{R})$: determinante di prodotti

$$Det(A \cdot B) = Det(A)Det(B). \tag{2.2}$$

Inoltre, per ogni $n \geq 1, Det(I_n) = 1$.

Un altro fatto fondamentale è che

$$A \in M_n(\mathbb{R}) \text{ è invertibile se e solo se } Det(A) \neq 0. \tag{2.3}$$

Non descriveremo qui le regole generali per determinare l'inversa di una matrice invertibile: ma ricordiamo solo il caso $n = 2$.

Sia $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$ con $\Delta = Det(A) \neq 0$. Allora matrici inverse

$$A^{-1} = \begin{pmatrix} d/\Delta & -b/\Delta \\ -c/\Delta & a/\Delta \end{pmatrix}. \tag{2.4}$$

---

Le definizioni di matrice e le operazioni che abbiamo dato nel caso di coefficienti in $\mathbb{R}$, si estendono senza differenze a matrici con coefficienti in un qualunque anello $A$, ottenendo anche in tal caso degli anelli. In generale, quindi, per $n \geq 1$, con $M_n(A)$ si denota l'anello delle matrici quadrate di ordine $n$ a coefficienti in $A$ (negli esempi ed esercizi, i casi che potranno occorrere con maggiore frequenza saranno $A = \mathbb{Z}$ e $A = \mathbb{Z}/d\mathbb{Z}$) con le operazioni di somma per componenti e di moltiplicazione righe×colonne. Funziona tutto in modo parallelo a quello del caso dei coefficienti in $\mathbb{R}$, fino alla definizione di determinante. Per quest'ultima, e la susseguente caratterizzazione degli elementi invertibili, è necessario richiedere che l'anello $A$ sia commutativo. In questi casi, il determinante è una applicazione $M_n(A) \to A$, che formalmente si definisce come nel caso a coefficienti reali. La formula per il prodotto (2.2) vale invariata, mentre la caratterizzazione degli elementi invertibili (2.3) diventa in generale la seguente: sia $A$ un anello commutativo, e sia $U \in M_n(A)$, allora $U$ è invertibile in $M_n(A)$ se e solo se $Det(U)$ è un elemento invertibile di $A$.
Ad, esempio gli elementi invertibili di $M_n(\mathbb{Z})$ sono tutte e sole le matrici intere (di ordine $n$) il cui determinante è 1 o $-1$.

---

### 2.2.3 Costruzione del campo dei razionali.

In questa paragrafo, illustriamo la costruzione rigorosa del campo $\mathbb{Q}$ dei numeri razionali. Come si vedrà, un fatto indispensabile per costruire $\mathbb{Q}$, come un campo che contenga l'anello $\mathbb{Z}$ dei numeri interi, è che $\mathbb{Z}$ è un *dominio d'integrità*: cioè, è commutativo ed il prodoto di elementi diversi da zero è diverso da zero.

Sia $\mathbb{Z}^* = \{z \in \mathbb{Z} \mid z \neq 0\}$. Iniziamo considerando l'insieme

$$\mathbb{Z} \times \mathbb{Z}^* = \{(a,b) \mid a,b \in \mathbb{Z},\ b \neq 0\}$$

di tutte le coppie ordinate di numeri interi la cui seconda componente non è zero. Su tale insieme definiamo una relazione $\sim$ ponendo, per ogni $(a,b),(c,d) \in \mathbb{Z}\times\mathbb{Z}^*$,

$$(a,b) \sim (c,d) \quad \text{se} \quad ad = bc\ .$$

Si verifica facilmente che $\sim$ è una relazione di equivalenza. Infatti:

1) $(a,b) \sim (a,b)$ per ogni $(a,b) \in \mathbb{Z}\times\mathbb{Z}^*$ perchè $ab = ba$ essendo $\mathbb{Z}$ commutativo.

2) Se $(a,b) \sim (c,d)$ allora $ad = bc$, quindi $cb = da$, cioè $(c,d) \sim (a,b)$.

3) Siano $(a,b),(c,d),(r,s) \in \mathbb{Z}\times\mathbb{Z}^*$ tali che $(a,b) \sim (c,d)$, $(c,d) \sim (r,s)$, allora $ad = bc$ e $cs = dr$; quindi $(as)d = (ad)s = (bc)s = b(cs) = b(dr) = (br)d$; poichè $d \neq 0$ e $\mathbb{Z}$ è un dominio d'integrità, per la legge di cancellazione, si ha $as = br$ e dunque $(a,b) \sim (r,s)$.

A questo punto, per ogni $(a,b) \in \mathbb{Z}\times\mathbb{Z}^*$ indichiamo con $\frac{a}{b}$ la classe di equivalenza di $(a,b)$ modulo $\sim$, e chiamiamo $\mathbb{Q}$ l'insieme quoziente modulo $\sim$, cioè

$$\mathbb{Q} = \frac{\mathbb{Z}\times\mathbb{Z}^*}{\sim} = \left\{ \frac{a}{b} \ \mid\ (a,b) \in \mathbb{Z}\times\mathbb{Z}^* \right\}\ .$$

Definiamo quindi su $\mathbb{Q}$ le operazioni di somma e prodotto nel modo seguente. Per ogni $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$,

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

Occorre verificare che si tratta di buone definizioni. Siano dunque $\frac{a}{b}, \frac{c}{d}, \frac{a'}{b'}, \frac{c'}{d'} \in \mathbb{Q}$ con $\frac{a}{b} = \frac{a'}{b'}$, $\frac{c}{d} = \frac{c'}{d'}$ ; allora $(a,b) \sim (a',b')$ e $(c,d) \sim (c',d')$, cioè $ab' = ba'$ e $cd' = dc'$. Dunque:

$$\begin{aligned} (ad+bc)b'd' &= adb'd' + bcb'd' = ab'dd' + cd'bb' = \\ &= ba'dd' + dc'bb' = a'd'bd + b'c'bd = (a'd' + b'c')bd \end{aligned}$$

e quindi

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'} = \frac{a'}{b'} + \frac{c'}{d'}\ .$$

Similmente

$$(ac)(b'd') = ab'cd' = ba'dc' = (a'c')(bd)$$

e quindi

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} = \frac{a'c'}{b'd'} = \frac{a'}{b'} \cdot \frac{c'}{d'}\ .$$

È facile provare che, con tali operazioni, $\mathbb{Q}$ è un anello commutativo con $0_{\mathbb{Q}} = \frac{0}{1}$, $1_{\mathbb{Q}} = \frac{1}{1}$. Vediamo ad esempio la distributività; osserviamo preliminarmente che per ogni $\frac{a}{b} \in \mathbb{Q}$ e $0 \neq c \in \mathbb{Z}$ si ha $\frac{a}{b} = \frac{ac}{bc}$; siano quindi $\frac{a}{b}, \frac{c}{d}, \frac{r}{s} \in \mathbb{Q}$, allora

$$\begin{aligned} \frac{a}{b}(\frac{c}{d} + \frac{r}{s}) &= \frac{a}{b}\frac{cs+dr}{ds} = \frac{a(cs+dr)}{b(ds)} = \frac{acs+adr}{bds} = \\ &= \frac{acsb+adrb}{bdsb} = \frac{ac}{bd} + \frac{ar}{sb} = \\ &= \frac{a}{b}\frac{c}{d} + \frac{a}{b}\frac{r}{s}. \end{aligned}$$

Lasciamo le altre verifiche per esercizio.

Per dimostrare che $\mathbb{Q}$ è un campo, resta da provare che ogni elemento non nullo di $\mathbb{Q}$ è invertibile. Sia $\frac{a}{b} \neq 0_{\mathbb{Q}} = \frac{0}{1}$, allora $(a, b) \not\sim (0, 1)$, cioè $a = a1 \neq b0 = 0$ e quindi $\frac{b}{a} \in \mathbb{Q}$ e si ha

$$\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ba} = \frac{1}{1} = 1$$

dunque $\frac{b}{a} = (\frac{a}{b})^{-1}$. Quindi $\mathbb{Q}$ è un campo.

Il campo $\mathbb{Q}$ che abbiamo costruito si chiama (e ci mancherebbe altro) *campo dei numeri razionali*. Assicuriamoci ora che $\mathbb{Q}$ contiene l'anello $\mathbb{Z}$ dei numeri interi. In realtà, quello che mostreremo è che in $\mathbb{Q}$ c'è un sottoanallo i cui elementi possono essere identificati (uno ad uno) con i numeri interi.

Per fare questo in maniera rigorosa, consideriamo l'applicazione

$$\begin{array}{rccc} \phi: & \mathbb{Z} & \to & \mathbb{Q} \\ & a & \mapsto & \frac{a}{1} \end{array}$$

$\phi$ è un'applicazione iniettiva, infatti, supponiamo che $a, b \in \mathbb{Z}$ siano tali che $\phi(a) = \phi(b)$. Allora

$$\frac{a}{1} = \phi(a) = \phi(b) = \frac{b}{1},$$

il che significa che $(a, 1)$ e $(b, 1)$ individuano la stessa classe di equivalenza modulo $\sim$, dunque che $(a, 1) \sim (b, 1)$. Ciò a sua volta vuol diire che $a = a \cdot 1 = 1 \cdot b = b$. Dunque $\phi$ è iniettiva. Possiamo allora identificare in modo univoco ogni numero intero $a$ con la frazione $\frac{a}{1}$; il che mostra che (in un senso che non approfondiremo oltre) $\mathbb{Q}$ contiene 'una copia' di $\mathbb{Z}$. Si potrebbe anche provare - dopo aver definito in modo rigoroso la cosa - che $\mathbb{Q}$ è il *più piccolo campo* che contiene $\mathbb{Z}$.

### 2.2.4 Esercizi

**Esercizio 2.8.** Si determinino tutti gli elementi invertibili ed i divisori dello zero negli anelli $\mathbb{Z}/24\mathbb{Z}$ e $\mathbb{Z}/16\mathbb{Z}$.

**Esercizio 2.9.** Trovare le soluzioni di $x^2 = \overline{1}$, e di $x^3 = \overline{1}$, negli anelli $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ e $\mathbb{Z}/11\mathbb{Z}$.

**Esercizio 2.10.** Si provi che ogni elemento non nullo di $M_2(\mathbb{R})$ è invertibile, oppure un divisore dello zero.

**Esercizio 2.11.** Nell'anello $M_2(\mathbb{R})$ delle matrci quadrate di ordine 2 sui reali si trovino due elementi $a$ e $b$ tali che $(ab)^2 \neq a^2b^2$.

**Esercizio 2.12.** Nell'anello di matrici $M_3(\mathbb{R})$ si determinino le potenze $A^n$, con $n \geq 0$ della matrice

$$A = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

isomorfismi

Il concetto di **isomorfismo** tra anelli si definisce in modo analogo a quanto fatto per i gruppi: se $A$ e $B$ sono anelli, un isomorfismo da $A$ in $B$ è un'applicazione *biettiva* $\phi : A \to B$ tale che, per ogni $a, a' \in A$:

$$\phi(a + a') = \phi(a) + \phi(a') \qquad \phi(aa') = \phi(a)\phi(a') \qquad \phi(1_A) = 1_B.$$

Nei prossimi esercizi si approfondisce qualche aspetto di questo importante concetto, e si danno alcuni esempi.

**Esercizio 2.13.** (a) Si provi che se $\phi : A \to B$ e $\psi : B \to C$ sono isomorfismi di anelli, allora la composizione $\psi \circ \phi : A \to C$ è un isomorfismo.
(b) Si provi che se $\phi : A \to B$ è un isomorfismo di anelli, allora anche l'applicazione inversa $\phi^{-1} : B \to A$ è un isomorfismo.

**Esercizio 2.14.** Sia $D = \{\frac{a}{1} \in \mathbb{Q} \mid a \in \mathbb{Z}\}$. Si provi che $D$ è un sottoanello di $\mathbb{Q}$, e che l'applicazione $\phi : \mathbb{Z} \to D$ definita da $\phi(a) = \frac{a}{1}$ per ogni $a \in \mathbb{Z}$, è un isomorfismo

## 2.3 Polinomi

### 2.3.1 Definizioni e prime proprietà.

polinomi

Sia $R$ un anello commutativo. Un **polinomio** a coefficienti in $R$ nell'*indeterminata* $x$ è una espressione del tipo

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

dove $n$ è un numero naturale, $a_0, a_1, a_2, \ldots, a_n$ sono elementi di $R$, ed $x$ è un simbolo (detto *indeterminata*) indipendente dagli elementi di $R$.
L'insieme di tutti i polinomi a coefficienti in $R$ nell'indeterminata $x$ si denota con $R[x]$.(Questa definizione non è del tutto formale; di fatto, sarebbe possibile descrivere una costruzione rigorosa di $R[x]$ nella quale anche la misteriosa indeterminata $x$ avrà un significato formalmente preciso: tuttavia, preferisco non appesantire troppo la trattazione: chi fosse interessato può venire a chiedermi lumi).

ugauaglianza di polinomi

Due polinomi $a_0 + a_1x + a_2x^2 + \ \ldots\ + a_nx^n$ e $c_0 + c_1x + c_2x^2 + \ \ldots\ + c_mx^m$ a coefficienti in $R$ sono **uguali** se $a_i = b_i$ per ogni $i \geq 0$; con la convenzione che i coefficienti non scritti sono uguali a zero (cioè $a_i = 0$ per ogni $i > n$ e $c_i = 0$ per ogni $c_i > m$; in particolare confrontando due polinomi possiamo sempre supporre $n = m$).
Un'altra convenzione familiare è che scrivendo semplicemente $x^n$ si intende $1_Rx^n$.
Ogni elemento di $R$ è un polinomio, quindi $R \subseteq R[x]$. Abitualmente, indicheremo i polinomi con lettere $f, g, h, \ldots$

somme e prodotti

Sull'insieme dei polinomi $R[x]$ si definiscono somma e prodotto nel modo seguente (che è la generalizzazione di quello familiare nel caso di polinomi a coefficienti reali). Quindi, se

$$f = a_0 + a_1x + a_2x^2 + \ \ldots\ + a_nx^n \ \text{ e } \ g = c_0 + c_1x + c_2x^2 + \ \ldots\ + c_mx^m$$

sono polinomi a coefficienti in $R$, con $n \geq m$, si pone

$$f + g = (a_0 + c_0) + (a_1 + c_1)x + (a_2 + c_2)x^2 + \ \ldots\ + (a_n + c_n)x^n$$

(dove abbiamo eventualmente aggiunto coefficienti $c_i = 0$ per $i > m$), e

$$fg = d_0 + d_1x + d_2x^2 + \ \ldots\ + d_{n+m}x^{n+m}$$

dove, per ogni $0 \leq i \leq n + m$

$$d_i = \sum_{r=0}^{i} a_r c_{i-r} \ .$$

Potete constatare da soli che queste sono le operazioni sui polinomi che vi sono già familiari dalle scuole superiori. Inoltre si verifica che con tali operazioni l'insieme $R[x]$ è un anello in cui zero e identità sono, rispettivamente, $0_R$ e $1_R$. $R[x]$ si chiama **l'anello dei polinomi** nell'indeterminata $x$ a coefficienti in $R$, e chiaramente contiene $R$ come sottoanello.

Se $f$ è un polinomio e $f \neq 0$, conveniamo di scrivere

$$f = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$$

grado di un polinomio

con $a_n \neq 0$. Il numero naturale $n$ è detto allora **grado** del polinomio $f$ e si denota con $\deg f$, e $a_n$ è detto **coefficiente direttivo** di $f$. Un polinomio $f$ si dice **monico** se il suo coefficiente direttivo è $1_R$. Osserviamo quindi che $\deg f = 0$ se e solo se $f \in R \setminus \{0\}$. Le seguenti proprietà sono di immediata verifica.

**Proposizione 2.3.1.** *Siano $f, g \in R[x] \setminus \{0_R\}$. Allora*

**(1)** $\deg(f+g) \leq \max\{\deg f, \deg g\}$

**(2)** $\deg(fg) \leq \deg f + \deg g$, *con uguaglianza se $R$ è un dominio d'integrità.*

Osserviamo che l'uguaglianza al punto (2) può non sussistere se $R$ non è un dominio d'integrità; ad esempio, in $(\mathbb{Z}/6\mathbb{Z})[x]$ : $(\overline{2}x + \overline{1})(\overline{3}x + \overline{1}) = \overline{6}x^2 + \overline{5}x + \overline{1} = \overline{5}x + \overline{1}$.

**Proposizione 2.3.2.** *Sia $R$ un dominio d'integrità. Allora $R[x]$ è un dominio d'integrità.*

*Dimostrazione.* (1) Sia $R$ un dominio d'integrità, e siano $f, g \in R[x]$ polinomi non nulli. Allora $\deg f \geq 0$ e $\deg g \geq 0$; quindi per il punto (2) della Proposizione precedente, $\deg(fg) = \deg f + \deg g \geq 0$, e dunque $fg \neq 0$. Quindi $R[x]$ è un dominio d'integrità. ∎

I casi che ci interessano maggiormente (e che possono essere tenuti come quelli di riferimento) sono quelli di polinomi a coefficienti in $\mathbb{Z}$, $\mathbb{Q}$ o $\mathbb{R}$. In queste situazioni familiari, una procedure molto comune è quella che consiste nel "sostituire" l'indeterminata con un "valore" noto. Ad esempio se $f = 1 + 3x^2 - 2x^4$, e $u = \sqrt{3}$, allora si scrive

$$f(u) = f(\sqrt{3}) = 1 + 3(\sqrt{3})^2 - 2(\sqrt{3})^4 = 1 + 3 \cdot 3 - 2 \cdot 9 = -8.$$

Si osservi che, in questo esempio, $f$ è a coefficienti in $\mathbb{Z}$, mentre l'elemento che sostituiamo appartiene a $\mathbb{R}$ (ma non a $\mathbb{Z}$); questo si può fare perché $\mathbb{Z}$ è un *sottoanello* di $\mathbb{R}$. La procedura di sostituzione si può fare in assoluta generalità, senza molte complicazioni: vediamo come.

Sia $R$ un sottoanello dell'anello $S$ (si pensi, ad esempio, a $R = \mathbb{Z}$ e $S = \mathbb{Q}$,e sia $b \in S$. Sia $f = a_0 + a_1x + a_2x^2 + \ \ldots \ + a_nx^n$ un polinomio in $R[x]$. Poichè i coefficienti $a_i$ sono in particolare elementi di $S$, ha senso considerare la *sostituzione di $x$ con $b$ in $f$*: sostituzione

$$f(b) = a_0 + a_1b + a_2b^2 + \ \ldots \ + a_nb^n$$

che è un elemento di $S$.

Fissato l'elemento $b$ da sostituire, la sostituzione dá luogo ad una applicazione

$$\begin{array}{rcl} R[x] & \to & S \\ f & \mapsto & f(b). \end{array}$$

che si comporta bene rispetto alle operazioni (somma e prodotto di polinomi di $R[x]$, e somma e prodotto in $S$); precisamente, si ha per ogni $f, g \in R[x]$,

$$(f+g)(b) = f(b) + g(b) \qquad\qquad (fg)(b) = f(b)g(b).$$

### 2.3.2 Divisione tra polinomi.

Siano $f, g$ polinomi a coefficienti in $R$. Diciamo che $f$ **divide** $g$ (e scriviamo $f|g$) se esiste $h \in R[x]$ tale che $g = fh$ (e, in tal caso, si dice anche che $g$ è un multiplo di $f$). divisibilità

Ad esempio, per ogni anello commutativo $R$ ed ogni numero naturale $n$, il polinomio $x - 1 \in \mathbb{R}[x]$ è un divisore di $x^n - 1$. Infatti, come si verifica facendo i calcoli,

$$x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \ldots + x^2 + x + 1).$$

Essendo l'anello dei polinomi ben lontano dall'essere un campo, fissati casualmente due polinomi in $R[x]$ è assai improbabile che uno dei due divida l'altro. Tuttavia, se $R$ è un campo è possibile definire una divisione con resto. Questo fatto è una proprietà estremamente importante degli anelli di polinomi a coefficienti su un campo, che li rende per diversi aspetti, simili all'anello $\mathbb{Z}$ dei numeri interi.

**Teorema 2.3.3.** *Sia $F$ un campo, e siano $g, f \in F[x]$ con $f \neq 0$. Allora esistono due polinomi $h, r \in F[x]$ tali che* divisione euclidea di polinomi

$$\begin{array}{ll} (i) & g = hf + r \\ (ii) & r = 0 \quad \textit{oppure} \quad \deg(r) \leq \deg(f) - 1 \end{array}$$

*inoltre, $h, r$ sono univocamente determinati da tali condizioni.*

*Dimostrazione.* 1) (esistenza) Sia $f = a_0 + a_1x + \ldots + a_nx^n$ con $a_n \neq 0$ e $g = b_0 + b_1x + \ldots + b_mx^m$. Se $g = 0$ allora $g = 0f + 0$. Sia quindi $g \neq 0$ e procediamo per induzione su $m = \deg(g)$.

Sia $m = 0$, allora $g \in F$. Se $n = \deg f \geq 1$ allora possiamo scrivere $g = 0f + g$ e siamo a posto perchè $\deg g = 0 < \deg f$; se invece $\deg f = 0$, allora $f = a_0 \in F\backslash\{0\}$ è invertibile in $F$ e $g = a_0(a_0^{-1}g) = fh + 0$ con $h = a_0^{-1}g$. Sia ora $m \geq 1$ e supponiamo l'enunciato vero per ogni polinomio dividendo di grado $\leq m-1$.
Se $m \leq n-1$ allora $g = 0f + g$ soddisfa le condizioni. Sia $m \geq n$, e poniamo

$$g_1 = a_ng - b_mx^{m-n}f = a_n(b_0+b_1x+\ldots+b_mx^m) - b_mx^{m-n}(a_0+a_1x+\ldots+a_nx^n) =$$

$$= a_nb_0 + \ldots + a_nb_mx^m - a_0b_mx^{m-n} - \ldots - a_{n-1}b_mx^{m-1} - a_nb_mx^m \ .$$

Allora $\deg g_1 \leq m-1$; quindi, per ipotesi induttiva esistono $h_1, r_1 \in F[x]$ tali che $g_1 = h_1f + r_1$ e $r_1 = 0$ o $\deg r_1 \leq n-1$. Segue che

$$g = a_n^{-1}(g_1 + b_mx^{m-n}f) = a_n^{-1}(h_1f + r_1 + b_mx^{m-n}f) = a_n^{-1}(h_1 + b_mx^{m-n})f + a_n^{-1}r_1$$

e l'enunciato è soddisfatto con $h = a_n^{-1}(h_1 + b_mx^{m-n})$ ed $r = a_n^{-1}r_1$.

2) (unicità) Supponiamo di poter scivere $g = hf + r = h'f + r'$ con la condizione (ii) soddisfatta. Allora $(h-h')f = r' - r$, se fosse $h \neq h'$ avremmo l'assurdo $\deg(f) \leq \deg((h-h')f) = \deg(r-r') \leq \deg(f) - 1$. Quindi $h = h'$ da cui discende immediatamente anche $r = r'$. ∎

La dimostrazione del Teorema fornisce anche il metodo per eseguire una divisione tra polinomi; si tratta di ripetere il passo in cui si dividono i monomi di grado massimo, ottenendo un monomio che va moltiplicato per il divisore e quindi sottratto dal polinomio su cui si sta operando, ottenendo così un polinomio di grado inferiore, ed andando avanti. È il solito metodo che si impara nelle scuole.

---

**Esercizio 2.15.** Nell'anello $\mathbb{Q}[x]$ dividere $g = 2x^4 - x^2 + 5x$ per $f = x^2 - x + 1$. esempio pratico

*Soluzione.* La familiare tabella:

| | | | | | |
|---|---|---|---|---|---|
| $2x^4$ | | $-x^2$ | $+5x$ | | $x^2 - x + 1$ |
| $2x^4$ | $-2x^3$ | $+2x^2$ | | | $2x^2 + 2x - 1$ |
| | $2x^3$ | $-3x^2$ | $+5x$ | | |
| | $2x^3$ | $-2x^2$ | $+2x$ | | |
| | | $x^2$ | $+3x$ | | |
| | | $x^2$ | $+x$ | $-1$ | |
| | | | $2x$ | $-1$ | |

Quindi, $g = (2x^2 + 2x - 1)f + (2x - 1)$.

---

Oltre al Teorema 2.3.3, vi sono molti altri vantaggi nel lavorare con polinomi a coefficienti su un campo. Per il momento ci limitiamo ad alcune osservazioni elementari (ma importanti).
Sia $F$ un campo, e $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ un polinomio non nullo a coefficenti in $F$, con $a_n \neq 0_F$. Allora $a_n$ è invertibile in $F$, e si può scrivere

$$f = a_n(x^n + a_n^{-1}a_{n-1}x^{n-1} + \ldots + a_n^{-1}a_1 x + a_n^{-1}a_0.)$$

Ovvero $f = a_n f_0$ è il prodotto del suo coefficiente direttivo $a_n$ per un polinomio monico $f_0$ (che, è chiaro, sono univocamante individuati da $f$). Più in generale, se $0_F \neq a \in F$, allora si può scrivere $f = a(a^{-1}f)$, e dunque $a$ divide $f$ (similmente si vede che il polinomio $af$ divide $f$). Quindi, ogni elemento non nullo di $F$, ed ogni prodotto di $f$ per un elemento non nullo di $F$ sono divisori di $f$ (si rifletta a come e perché tali affermazioni non valgano se l'anello dei coefficienti non è un campo - ad esempio nel caso di $\mathbb{Z}[x]$). Un polinomio $g \in F[x]$ si dirà un *divisore proprio* di $f$ se $g$ divide $f$, e non è del tipo sopra descritto. divisori propri
A questo punto, dovrebbe essere facile per il lettore provare il Lemma seguente.

**Lemma 2.3.4.** *Sia $F$ un campo, e siano $0 \neq f, g \in F[x]$.*

*(i) Se $g$ è un divisore proprio di $f$, allora $0 < \deg g < \deg f$.*

*(ii) Se $g|f$ e $f|g$, allora esiste un $0 \neq c \in F$ tale che $g = cf$.*

**Definizione.** Sia $F$ una campo, e sia $f \in F[x]$ un polinomio tale che $\deg f \geq 1$. Allora $f$ si dice un polinomio **irriducibile** in $F[x]$ se non ha divisori propri in $F[x]$. Altrimenti, si dice riducibile. polinomi irriducibili

**Esempio.** Il polinomio $x^3 + 2x^2 + 2x + 1 \in \mathbb{Q}[x]$ è riducibile in $\mathbb{Q}[x]$; infatti si trova facilmente che $x^3 + 2x^2 + 2x + 1 = (x + 1)(x^2 + x + 1)$. Mentre $x^2 + x + 1$ è un polinomio irriducibile di $\mathbb{Q}[x]$ (lo si dimostri).

I polinomi irriducibili svolgono nell'anello $F[x]$ ($F$ campo) un ruolo analogo a quello che i numeri primi svolgono nell'anello $\mathbb{Z}$. Osserviamo ora che, grazie al Lemma 2.3.4, possiamo formulare equivalentemente la definizione di sopra, dicendo che un polinomio $f$ a coefficienti su un campo $F$ è irriducibile se e solo se $f$ non ha divisori di grado strettamente minore del proprio. In altri termini se non è possibile scrivere $f = gh$ con $g$ e $h$ polinomi tali che $\deg g < \deg f$ e $\deg h < \deg f$.

Un'ovvia avvertenza è che un polinomio va sempre considerato come un elemento dell'anello dei polinomi di un esplicito campo, ed è in tale anello dei polinomi che ha

senso chiedersi se sia o meno irriducibile. Ad esempio, il polinomio $x^4+1 \in \mathbb{Q}[x]$ è irriducibile (lo si provi per esercizio), mentre il polinomio $x^4+1 \in \mathbb{R}[x]$ è riducibile, dato che, in $\mathbb{R}[x]$, $x^4+1 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$.

fattorizzazioni in irriducibili

**Fattorizzazioni di polinomi.** Se $F$ è un campo, i polinomi irriducibili svolgono, nell'anello dei polinomi $F[x]$, lo stesso ruolo che i numeri primi svolgono in $\mathbb{Z}$. In particolare, *ogni polinomio non costante in $F[x]$ si scrive come il* **prodotto di polinomi irriducibili** *di $F[x]$, e tale prodotto è unico a ameno di eventuali scambi tra i fattori, ed a meno di moltiplicare qualcuno di tali fattori per un elemento non-nullo di $F$.*
Questo fatto, importantissimo, si esprime dicendo che, se $F$ è un campo, l'anello $F[x]$ è *Fattoriale*. Ad esempio, sia $F = \mathbb{Q}$; consideriamo il polinomio $f = x^4 - 4 = (x^2+2)(x^2-2)$, e si verifica facilmente che $x^2-2$ e $x^2+2$ sono irriducibili in $\mathbb{Q}[x]$ (come sarà chiaro nella prossima sezione); quindi quella di sopra è *la* fattorizzazione in irriducibili di $f$ in $\mathbb{Q}[x]$. Ora, $x^2+2$ è irriducibile anche come polinomio in $\mathbb{R}[x]$, mentre non lo è $x^2-2$, infatti - in $\mathbb{R}[x]$ - $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$; quindi la fattorizzazione in irriducibili di $f$ in $\mathbb{R}[x]$ è: $f = (x^2+2)(x-\sqrt{2})(x+\sqrt{2}$.

MCD

**Massimo comun divisore tra polinomi.**
Come per i numeri interi, se $F$ è un campo è possibile parlare di massimo comun divisore tra due polinomi non nulli di $F[x]$.
La definizione è la stessa. Siano $f$ e $g$ polinomi non nulli a coefficienti su un campo $F$. Un polinomio $d \in F[x]$ si dice un *massimo comun divisore* di $f$ e $g$ se

- $d|f$ e $d|g$;
- se $h \in F[x]$ è tale che $h|f$ e $h|g$, allora $h|d$.

Come nel caso degli interi, si prova che polinomi non nulli $f$ e $g$ in $F[x]$ ammettono sempre un massimo comun divisore $d$, che può essere scritto nella forma

$$d = \alpha \cdot f + \beta \cdot g$$

con $\alpha, \beta \in F[x]$; anzi, $d$ è, tra i polinomi che si scrivono in questa forma, uno di grado minimo (diverso da zero). Inoltre, dal Lemma 2.3.4, segue che, se $d$ e $d_1$ sono due massimi comun divisori di $f$ e $g$, esiste un $0 \neq a \in F$ tale che $d_1 = ad$. Ne segue, sempre per il Lemma 2.3.4, che $f$ e $g$ hanno un *unico* massimo comun divisore *monico*, che si denota quindi con $(f, g)$.

Infine, anche con l'anello $F[x]$, per calcolare il massimo comun divisore di due polinomi non nulli, è possibile applicare l'algoritmo di Euclide. La procedura è la stessa del caso dei numeri interi (ed è fondata sulla divisione euclidea, Teorema

2.3.3), per cui, invece che descriverla nuovamente in generale, ci limitiamo a fornire un esempio della sua applicazione.

**Esempio.** Calcolare un MCD in $\mathbb{Q}[x]$ dei polinomi: algoritmo di Euclide

$$f = 12x^7 + 5x^5 + 10x^4 - 7x^3 + 10x^2 \ , \qquad g = 2x^5 - x^4 + 2x^3 + 1 \ .$$

L'algoritmo di Euclide opera mediante le divisioni successive. In questo caso si ha:

$$\begin{array}{ll} f = (6x^2 + 3x - 2)g + r_1 & r_1 = 2x^4 - 3x^3 + 4x^2 - 3x + 2 \\ g = (x+1)r_1 + r_2 & r_2 = x^3 - x^2 + x - 1 \\ r_1 = (2x-1)r_2 + r_3 & r_3 = x^2 + 1 \\ r_2 = (x-1)r_3 + 0 & \end{array}$$

quindi $r_3 = x^2 + 1$ è un MCD di $f$ e $g$.

### 2.3.3 Radici di un polinomio.

**Definizione.** Sia $R$ un anello e $0 \neq f \in R[x]$. Un elemento $a \in R$ si dice **radice** (o, anche, "zero") di $f$ se $f(a) = 0$. Ad esempio, $\sqrt[3]{2}$ è una radice del polinomio $x^3 - 2 \in \mathbb{R}[x]$; mentre (lo si verifichi per esercizio) $\sqrt{3} - \sqrt{2}$ è radice di $x^4 - 10u^2 + 1 \in \mathbb{R}[x]$. radici

Un primo criterio di riducibilità di un polinomio è il noto Teorema di Ruffini. Si tratta, in fin dei conti, di una conseguenza del Teorema 2.3.3, e dunque, ancora una volta, è una proprietà dei polinomi per la quale è richiesto che l'anello dei coefficienti sia un campo. Teorema di Ruffini

**Teorema 2.3.5. (di Ruffini)** *Sia $F$ un campo, $0 \neq f \in F[x]$ ed $a \in F$. Allora $a$ è una radice di $f$ se e solo se $(x - a)$ divide $f$.*

*Dimostrazione.* Supponiamo che $f(a) = 0$, e dividiamo $f$ per $(x - a)$, abbiamo

$$f = (x - a)h + r$$

con $r = 0$ o $\deg r = 0$. Quindi, in ogni caso, $r \in F$ e dunque $r(a) = r$. Ora

$$0 = f(a) = (a - a)h(a) + r(a) = 0h(a) + r = r$$

quindi $f = (x - a)h$ cioè $(x - a)$ divide $f$.
Viceversa, supponiamo che $(x - a)$ divida $f$. Allora $f = (x - a)h$ per qualche $h \in F[x]$ e pertanto

$$f(a) = (a - a)h(a) = 0h(a) = 0$$

quindi $a$ è una radice di $f$. ∎

Osserviamo che una conseguenza banale del Teorema di Ruffini è che un polinomio $0 \neq f$ a coefficienti in un campo $F$ ha divisori di primo grado se e soltanto se ha radici in $F$. Infatti se $g = ax + b$ (con $a, b \in F$) è un divisore di $f$, allora $g = a(x - (-ba^{-1}))$, e quindi anche $x - (-ba^{-1})$ è un divisore di $f$; pertanto $-ba^{-1}$ è una radice di $f$.

esempio

Ad esempio, il polinomio $x^2 + x - 1$ è irriducibile in $\mathbb{Q}[x]$ dato che ha grado 2 e non ha radici in $\mathbb{Q}$ (e quindi non ha divisori di grado 1 in $\mathbb{Q}[x]$); d'altra parte $x^2 + x - 1$ è riducibile in $\mathbb{R}[x]$, dato che, in $\mathbb{R}[x]$,

$$x^2 + x - 1 = \left(x - \frac{-1 + \sqrt{5}}{2}\right)\left(x - \frac{-1 - \sqrt{5}}{2}\right).$$

L'esempio che abbiamo dato tratta un polinomio di secondo grado a coefficienti reali, per i quali esiste una ben nota formula esplicita per il calcolo delle radici. Per polinomi di grado superiore, applicare il teorema di Ruffini ai fini di studiare l'irriducibilità è meno agevole (il famoso teorema di Galois asserisce, in particolare, che non esistono formule risolutive generali per calcolare le radici di un polinomio razionale di grado maggiore o uguale a 5); tuttavia, almeno per polinomi monici in $\mathbb{Q}[x]$ i cui coefficienti sono tutti degli interi, c'è un facile trucco.

radici di polinomi interi

Sia $f = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ un polinomio monico in $\mathbb{Q}[x]$, tale che i coefficienti $a_0, a_1, \ldots, a_{n-1}$ sono numeri interi e $a_0 \neq 0$. Supponiamo che $q \in \mathbb{Q}$ sia una radice di $f$. Sia $q = a/b$, con $a, b \in \mathbb{Z}$, $(a, b) = 1$ e $b \geq 1$. Allora

$$0 = f(\alpha) = q^n + a_{n-1}q^{n-1} + \ldots + a_1 q + a_0 = \frac{a^n}{b^n} + a_{n-1}\frac{a^{n-1}}{b^{n-1}} + \ldots + a_1\frac{a}{b} + a_0.$$

Moltiplicando per $b^n$ si ha

$$-a^n = a_{n-1}a^{n-1}b + \ldots + a_1 a b^{n-1} + a_0 b^n.$$

Questa è una relazione tra numeri interi, e siccome $a$ e $b$ sono coprimi, da essa segue che $b = 1$. Dunque $q = a \in \mathbb{Z}$; inoltre $-a_0 = a^n + a_{n-1}a^{n-1} + \ldots + a_1 a = (a^{n-1} + a_{n-1}a^{n-2} + \ldots + a_1)a$, e dunque $a$ divide $a_0$ in $\mathbb{Z}$. Abbiamo cioè provato che le eventuali radici in $\mathbb{Q}$ di un polinomio monico i cui coefficienti sono numeri interi, sono numeri interi che dividono (come numeri interi) il termino noto $a_0$ del polinomio (questa osservazione è generalizzata nell'esercizio 1). Ad esempio, il polinomio $f = x^4 + 2x^3 - 7x + 1$ non ha radici in $\mathbb{Q}$ (e dunque non ha divisori di primo grado in $\mathbb{Q}[x]$), dato che 1 e $-1$ non sono radici di $f$.

molteplicità di radici

Torniamo ad occuparci di polinomi su un campo generico. Sia $0 \neq f$ un polinomio a coefficienti sul campo $F$ e sia $a \in F$ una radice di $f$. Allora $(x - a)$ divide $f$, e

quindi si può scrivere $f = (x-a)g$ con $g \in F[x]$. A sua volta, $a$ potrebbe essere una radice di $g$; in tal caso $(x-a)$ divide $g$, e quindi $(x-a)^2$ divide $f$. Dunque, se $a$ è una radice di $f$, esiste un massimo intero positivo $m(a)$ tale che $(x-a)^m$ divide $f$. Tale intero si chiama *molteplicità (algebrica)* della radice $a$, e chiaramente soddisfa $1 \leq m(a) \leq \deg f$. Possiamo fattorizzare $f$ come $f = (x-a)^{m(a)}h$, dove $h \in F[x]$, e $h(a) \neq 0$. Se $m(a) = 1$, la radice $a$ si dice *semplice*, altrimenti si dice multipla. Un criterio per il calcolo delle eventuali radici multiple di un polinomio $f \in F[x]$ è fornito dall'esercizio 6.

Considerazioni di simile natura sono applicate per dimostrare la seguente e importantissima conseguenza del Teorema di Ruffini. radici distinte

**Teorema 2.3.6.** *Sia $F$ un campo e $0 \neq f \in F[x]$, con $n = \deg f$. Allora il numero di radici distinte di $f$ in $F$ è al più $n$.*

*Dimostrazione.* Siano $\alpha_1, \alpha_2, \ldots, \alpha_k$ radici distinte di $f$ in $F$. Procedendo per induzione su $k$ proviamo che $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$ divide $f$. Per $k = 1$ è il teorema di Ruffini. Sia quindi $k \geq 2$ e assumiamo per ipotesi induttiva che $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{k-1})$ divida $f$. Sia $g \in F[x]$ tale che $f = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{k-1})\cdot g$. Allora

$$0 = f(\alpha_k) = (\alpha_k-\alpha_1)(\alpha_k-\alpha_2)\cdots(\alpha_k-\alpha_{k-1})g(\alpha_k)$$

in cui il termine di destra è un prodotto di elementi del campo $F$; quindi, poichè $\alpha_k \neq \alpha_i$ per $i = 1, 2, \ldots, k-1$, deve essere $g(\alpha_k) = 0$. Per il Teorema di Ruffini $(x-\alpha_k)$ divide $g$, quindi $g = (x-\alpha_k)h$ per un $h \in F[x]$ e dunque

$$f = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_{k-1})(x-\alpha_k)h$$

Quindi, per il principio di induzione, l'affermazione è provata. Ora se $\alpha_1, \alpha_2, \ldots, \alpha_t$ sono *tutte* le radici distinte di $f$, per quanto appena visto $d = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_t)$ divide $f$ e quindi $n = \deg f \geq \deg d = t$. ∎

In effetti, il Teorema precedente può essere reso ulteriormente preciso nel modo seguente (la verifica consiste nel ripercorrere con attenzione la dimostrazione del Teorem 2.3.6 tenendo conto delle osservazioni che lo precedono.

**Teorema 2.3.7.** *Sia $F$ un campo, e sia $0 \neq f \in F[x]$, un polinomio non nullo di grado $n$. Siano $a_1, a_2, \ldots, a_k$ le radici distinte di $f$ in $F$, e per ogni $i = 1, 2, \ldots, k$, sia $m_i = m(a_i)$ la molteplicità della radice $a_i$. Allora $m_1 + m_2 + \cdots + m_k \leq n$.*

### 2.3.4 Esercizi.

**Esercizio 2.16.** Si provi che se $F$ è un campo allora l'insieme degli elementi invertibili di $F[x]$ è $F \setminus \{0\}$. [sugg. : Se $f \in F[x]$ è invertibile esiste $g \in F[x]$ tale che $1 = fg$. Poiché $F$ è un campo (ed in particolare un dominio d'integrità, si ha $0 = \deg(1) = \deg f + \deg g$, . . . ]

**Esercizio 2.17.** Si dica per quali valori di $a \in \mathbb{Q}$, $x^2+1$ divide $x^4+3x^3+x-a^2$ nell'anello $\mathbb{Q}[x]$.

**Esercizio 2.18.** In $\mathbb{Q}[x]$ si considerino i polinomi

$$f = x^5 - 2x^4 + x^3 - 9x^2 + 18x - 9 \qquad g = x^5 - x^3 - 9x^2 + 9 \ .$$

Determinare un massimo comun divisore di $f$ e $g$.

**Esercizio 2.19.** Si dica per quali $a \in \mathbb{Z}$ i seguenti polinomi sono coprimi in $\mathbb{Q}[x]$,

$$3x^4 + 4x^3 + ax^2 + ax + a \qquad\qquad x^2 + 2x + 1 \ .$$

**Esercizio 2.20.** Si provi che i polinomi a coefficienti razionali

$$x^3 + x^2 + x + 2 \qquad \text{e} \qquad x^4 + 1$$

sono irriducibili in $\mathbb{Q}[x]$.

**Esercizio 2.21.** Sia $f = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$, con $a_0, a_1, \ldots, a_n \in \mathbb{Z}$, e sia $u = a/b \in \mathbb{Q}$ (con $a, b \in \mathbb{Z}$, $b \geq 1$ e $(a,b) = 1$). Si provi che se $u$ è una radice di $f$, allora $b|a_n$ e $a|a_0$.

**Esercizio 2.22.** In $\mathbb{Q}[x]$ si considerino i polinomi

$$f = x^4 + 3x^3 + 2x^2 + x + 6 \qquad g = x^3 + x^2 + 2x + 3 \ .$$

Si determini un massimo comun divisore di $f$ e $g$.

**Esercizio 2.23.** Sia $f = 1 - 3x + x^3 \in \mathbb{Q}[x]$.

(a) Si provi che $f$ è irriducibile in $\mathbb{Q}[x]$.

(b) Sia $u$ una radice complessa di $f$ e sia $K = \mathbb{Q}[u]$. Si provi che $12 - 3u^2 = (2u^2 + u - 4)^2$ in $K$.

**Esercizio 2.24.** Sia $p$ un numero primo, con $p \not\equiv 1 \pmod 3$. Si provi che il polinomio $x^2 + x + 1$ è irriducibile in $\mathbb{Z}_p[x]$.

**Esercizio 2.25.** Si fattorizzino i polinomi $x^9 - x$ e $x^5 - 2x^3 - x^2 + 2$ in irriducibili in $\mathbb{Q}[x]$, $\mathbb{R}[x]$ e $\mathbb{C}[x]$.

**Esercizio 2.26.** Si determini per quali valori $h \in \mathbb{Z}$ il polinomio $f_h = x^4 - x^2 + hx + 1$ è irriducibile in $\mathbb{Q}[x]$.

**Esercizio 2.27.** 1) Si fattorizzi $x^4 + 3x + 2$ in $\mathbb{Q}[x]$.

2) Siano $p, q$ primi positivi. Si provi che, escluso il caso $p = 2$, $q = 3$, il polinomio $x^4 + qx + p$ è irriducibile in $\mathbb{Q}[x]$.

**Appendice: Costruzione formale dell'anello dei polinomi.** Sia $R$ un anello commutativo e consideriamo l'insieme di tutte le sequenze infinite costruzione formale di $R[x]$

$$(a_0,\ a_1,\ a_2,\ a_3,\ \ldots\ldots) \qquad\qquad (*)$$

ad elementi $a_0, a_1, a_2, \ldots$ in $R$. Osserviamo che tale insieme può essere identificato con l'insieme $R^{\mathbb{N}}$ di tutte le applicazioni da $\mathbb{N}$ in $R$, facendo corrispondere alla sequenza $(a_0, a_1, a_2, a_3,\ \ldots)$ l'applicazione che ad ogni $n \in \mathbb{N}$ associa l'elemento $a_n$ della sequenza.
Denotiamo con $B$ il sottoinsieme costituito da tutte le sequenze quasi ovunque nulle, cioè le sequenze che hanno un numero finito di termini $a_i$ diversi da zero (che corrispondono alle applicazioni $f$ da $\mathbb{N}$ in $R$ per le quali esiste un $k$ tale che $f(i) = 0$ per ogni $i \geq k$). Su $B$ definiamo una somma ponendo

$$(a_0, a_1, a_2, a_3, \ldots) + (b_0, b_1, b_2, b_3,\ \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, a_3 + b_3,\ \ldots)\ .$$

Si verifica facilmente che rispetto a tale operazione $B$ soddisfa gli assiomi (S1), (S2) e (S3) per gli anelli, con elemento neutro $0_B = (0, 0, 0, \ldots)$.
Introduciamo quindi una moltiplicazione ponendo

$$(a_0, a_1, a_2, a_3, \ldots)(b_0, b_1, b_2, b_3,\ \ldots) = (c_0, c_1, c_2, c_3,\ \ldots)$$

dove, per ogni $i \in \mathbb{N}$: $c_i = \sum_{r=0}^{i} a_r b_{i-r}$. (osserviamo che se $a_r = 0$ per $r \geq n$ e $b_s = 0$ per $s \geq m$ allora $c_i = 0$ per $i \geq n + m$ e quindi $(c_0, c_1, c_2, c_3,\ \ldots) \in B$). Con un po' di lavoro, ma senza difficoltà, anche in questo caso si dimostra che rispetto a tale prodotto $B$ soddisfa gli assiomi (P1) e (P2) di anello, con identità $1_B = (1, 0, 0, 0, \ldots)$, e che è soddisfatta la proprietà distributiva del prodotto rispetto alla somma.
Quindi, con tali operazioni, $B$ è un anello commutativo.
Consideriamo ora la applicazione $R \to B$ che ad ogni $a \in R$ associa $(a, 0, 0, \ldots)$. Essa è un omomorfismo iniettivo di anelli; possiamo quindi identificare $(a, 0, 0, \ldots)$ con l'elemento $a \in R$ e considerare $R$ come sottoanello di $B$.
Poniamo ora $x = (0, 1, 0, 0, \ldots)$. Allora, applicando la definizione di prodotto in $B$, e ragionando per induzione, si prova che per ogni $n \in \mathbb{N}$

$$x^n = (0, 0, \ldots, 0, 1, 0, \ldots)$$

con 1 al posto $n$. Da ciò segue che per ogni $a \in \mathbb{R}$

$$ax^n = (a, 0, 0, \ldots)(0, 0, \ldots, 0, 1, 0\ldots) = (0, 0, \ldots, 0, a, 0\ldots)$$

con $a$ al posto $n$. Quindi, ogni $f = (a_0, a_1, \ldots, a_n, 0, 0, \ldots) \in B$ si scrive

$$f = (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) + (0, 0, a_2, \ldots) + (0, 0, \ldots, 0, a_n, 0, \ldots) = a_0 + a_1 x + a_2 x^2 + \ldots a_n x^n\ .$$

Quindi, ragionando nell'estensione $R \subseteq B$, si ha $B = R[x]$. Questo si dice l'anello dei polinomi a coefficienti in $R$ nell'indeterminata $x$.