

## Capitolo 5

# Generalit  sulle Strutture Algebriche

*Pi  la matematica resta viva, pi  astratta - e quindi,  
possibilmente anche pi  pratica - diventa.*

*Eric T. Bell*

*(“The Mathematical Intelligencer”, vol.13.,n.1,1991)*

### 5.1 Operazioni su un insieme

Alcuni esempi di *operazioni* note al Lettore sono i seguenti:

- Addizione e moltiplicazione in  $N_o, Z, Q, R, C$ .
- Addizione e moltiplicazione in  $Z_n$ .
- Moltiplicazione in  $U(n)$ .
- Addizione in uno spazio vettoriale.
- Divisione in  $Q^*, R^*, C^*$ .
- Addizione in  $M_{m,n}(A)$ ,  $A = N_o, Z, R, C$ .
- Moltiplicazione righe per colonne in  $M_n(A)$ ,  $A = N_o, Z, R, C$ .
- Addizione e moltiplicazione nell’insieme dei polinomi a coefficienti in  $N_o, Z, Q, R, C$ .
- Massimo comune divisore e minimo comune multiplo in  $N$ .
- Unione e intersezione in  $P(S)$ .
- Differenza simmetrica<sup>1</sup> in  $P(S)$ .
- Composizione in  $Perm(S)$ .
- Moltiplicazione di uno scalare per un vettore in uno spazio vettoriale.

**OSSERVAZIONE 5.1.1** Tutte le operazioni elencate si presentano come delle leggi che permettono di individuare un elemento di un insieme a partire da una coppia elementi assegnati. E’

---

<sup>1</sup>Si chiama *differenza simmetrica* di due insiemi  $A$  e  $B$  l’insieme  $A \star B = (A \cup B) \setminus (A \cap B)$ .

pertanto ragionevole pensare che la nozione di *operazione* possa generalizzarsi ed esprimersi in termini precisi nel linguaggio della teoria degli insiemi. E' appunto ciò che ci proponiamo di fare in questo paragrafo.  $\diamond$

Nel seguito del capitolo  $S$  denoterá sempre un insieme non vuoto.

**DEFINIZIONE 5.1.2** Un'applicazione di  $S \times S$  in  $S$  prende il nome di *operazione interna ad  $S$* . Assegnata un'operazione  $\star : S \times S \rightarrow S$ , si pone

$$\star(a, b) = a \star b;$$

per ogni  $a, b \in S$ . L'elemento  $a \star b$  di  $S$  si chiama *composto* di  $a$  e  $b$  mediante  $\star$ .  $\diamond$

Le notazioni piú usate per le operazioni sono

- la notazione *additiva*: si usa il segno "+" e il composto di due elementi  $a, b$  si denota con  $a + b$ ;
- la notazione *moltiplicativa*: si usa il segno "." o "×" e il composto di due elementi  $a, b$  si denota con  $a \cdot b$  o  $a \times b$ , o anche con  $ab$ ;
- la notazione *esponenziale*: il composto di due elementi  $a, b$  si denota con  $a^b$ .

**DEFINIZIONE 5.1.3** Sia  $A$  un insieme non vuoto,  $A \neq S$ . Un'applicazione di  $A \times S$  in  $S$  prende il nome di *operazione esterna ad  $S$  con dominio di operatori  $A$* .  $\diamond$

Per le operazioni esterne si usano la simbologia e la terminologia introdotte per quelle interne. Un esempio di operazione esterna familiare al Lettore é, per esempio, la *moltiplicazione di uno scalare per un vettore* in uno spazio vettoriale.

**DEFINIZIONE 5.1.4** Si chiama *struttura algebrica ad  $n$  operazioni su  $S$*  ogni  $(n + 1) - pla$  del tipo

$$(S, \star_1, \star_2, \dots, \star_n),$$

ove ogni  $\star_i$  é una operazione su  $S$  (interna o esterna). L'insieme  $S$  si chiama *sostegno* della struttura. Una struttura algebrica si dice *finita* (risp. *infinita*) se il suo sostegno é un insieme finito (risp. infinito<sup>2</sup>). Se una struttura algebrica é finita, il numero di elementi del suo sostegno si chiama *ordine* della struttura; nel caso contrario si dice che la struttura ha *ordine infinito*.  $\diamond$

**ESEMPI 5.1.5** Di seguito riportiamo alcuni esempi di strutture algebriche. Questi, tra l'altro, mostrano che uno stesso insieme  $S$  puó essere sostegno di strutture algebriche diverse.

- $(N_o, +), (Z, +), (Q, +), (R, +), (C, +)$ .
- $(N_o, \cdot), (Z, \cdot), (Q, \cdot), (R, \cdot), (C, \cdot)$ .
- $(N_o, +, \cdot), (Z, +, \cdot), (Q, +, \cdot), (R, +, \cdot), (C, +, \cdot)$ .

<sup>2</sup>Un insieme é infinito se puó essere messo in corrispondenza biunivoca con un suo sottoinsieme proprio.

- $(\mathbb{Z}[x], +, \cdot), (\mathbb{Q}[x], +, \cdot), (\mathbb{R}[x], +, \cdot), (\mathbb{C}[x], +, \cdot).$
- $(\mathbb{Z}_n, +), (\mathbb{Z}_n, \cdot), (\mathbb{Z}_n, +, \cdot), (U(n), \cdot).$
- $(P(S), \cap), (P(S), \cup), (P(S), \cup, \cap).$
- $(S, \wedge), (S, \vee), (S, \wedge, \vee),$  ove  $(S, \leq)$  é un reticolo. ◇

Indicate con  $\circ$  e  $\star$  operazioni interne ad  $S$ , si definiscono le seguenti proprietà:

- Proprietá *commutativa*:

$$a \circ b = b \circ a, \quad \text{per ogni } a, b \in S.$$

- Proprietá *associativa*:

$$a \circ (b \circ c) = (a \circ b) \circ c, \quad \text{per ogni } a, b, c \in S.$$

- Proprietá *distributiva (a destra)* di  $\circ$  rispetto a  $\star$  :

$$(a \star b) \circ c = (a \circ c) \star (b \circ c), \quad \text{per ogni } a, b, c \in S.$$

**ESERCIZIO 5.1.6** Verificare che su un insieme con un solo elemento si può definire un'unica operazione e che questa risulta commutativa e associativa.

**DEFINIZIONE 5.1.7** Sia  $(S, \circ)$  una struttura algebrica con operazione interna. Un elemento  $u \in S$  si dice *neutro* se

$$u \circ a = a \circ u = a, \quad \text{per ogni } a \in S.$$

Se la struttura  $(S, \circ)$  possiede un elemento neutro si dice *unitaria*. ◇

**ESERCIZIO 5.1.8** Provare che, se  $(S, \circ)$  possiede un elemento neutro, questo é unico.

**DEFINIZIONE 5.1.9** In notazione moltiplicativa l'elemento neutro si chiama *unitá* e si denota con 1. In notazione additiva l'elemento neutro si chiama *zero* e si denota con 0. ◇

#### ESEMPI 5.1.10

- $(A, +), A = \mathbb{N}_o, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n,$  ha 0 come elemento neutro.
- $(A^*, \cdot), A = \mathbb{N}_o, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n,$  ha 1 come elemento neutro.
- Sia / l'operazione di divisione in  $\mathbb{Q}^*$ .  $(\mathbb{Q}^*, /)$  (struttura non associativa e non commutativa) non possiede elemento neutro.

- $(P(S), \cap)$  ha  $S$  come l'elemento neutro.

- $(P(S), \cup)$  ha  $\emptyset$  come l'elemento neutro. ◇

**ESERCIZIO 5.1.11** Sia  $(S, \leq)$  un reticolo. Dire sotto quali condizioni  $(S, \wedge)$  e  $(S, \vee)$  posseggono l'elemento neutro.

**DEFINIZIONE 5.1.12** Sia  $(S, \circ)$  una struttura algebrica dotata di elemento neutro  $u$ . Un elemento  $a \in S$  si dice *simmetrizzabile* se esiste  $a' \in S$  tale che

$$a' \circ a = a \circ a' = u .$$

L'elemento  $a'$  si chiama *simmetrico* di  $a$ . ◇

**OSSERVAZIONE 5.1.13** In una una struttura algebrica  $(S, \circ)$  dotata di elemento neutro  $u$  si ha:

- $a'$  simmetrico di  $a \Leftrightarrow a$  simmetrico di  $a'$ .
- L'elemento neutro  $u$  é simmetrizzabile e si ha  $u' = u$ .

**DEFINIZIONE 5.1.14** Nella notazione moltiplicativa il simmetrico di un elemento  $a$  si chiama *inverso* di  $a$  e si denota con  $a^{-1}$ . Nella notazione additiva il simmetrico di  $a$  si chiama *opposto* di  $a$  e si denota con  $-a$ . ◇

**ESEMPI 5.1.15**

- In  $(Z, +)$ ,  $(Z_n, +)$ ,  $(Q, +)$ ,  $(R, +)$ ,  $(C, +)$  tutti gli elementi sono simmetrizzabili.
- In  $(Z, \cdot)$ , 1 e  $-1$  sono gli unici elementi simmetrizzabili.
- In  $(Q^*, \cdot)$ ,  $(R^*, \cdot)$ ,  $(C^*, \cdot)$  tutti gli elementi sono simmetrizzabili.
- In  $(Z[x], +)$ ,  $(Q[x], +)$ ,  $(R[x], +)$ ,  $(C[x], +)$  tutti gli elementi sono simmetrizzabili.
- Una matrice  $A$  appartenente a  $(M_n(Q), \cdot)$ , o  $(M_n(R), \cdot)$  o  $(M_n(C), \cdot)$  é simmetrizzabile se, e solo se,  $\det(A) \neq 0$ . ◇

**ESERCIZIO 5.1.16** Provare che una matrice  $A$  in  $(M_2(Z), \cdot)$  é simmetrizzabile se, e solo se,  $\det(A) = \pm 1$ .

**DEFINIZIONE 5.1.17** Sia  $(S, \circ)$  una struttura algebrica con operazione interna. Un sottoinsieme non vuoto  $X$  di  $S$  si dice *parte stabile* se:

$$a \circ b \in X , \text{ per ogni } a, b \in X .$$

◇

Quando  $X$  é una parte stabile, la restrizione dell'operazione "o" a  $X \times X$  é una operazione interna ad  $X$ ; abbiamo cosí una nuova struttura algebrica  $(X, \circ)$ , che si dice *indotta* su  $X$  da  $(S, \circ)$ . In questo passaggio si conservano, per esempio, la proprietá associativa e quella commutativa.

**DEFINIZIONE 5.1.18** Sia  $(S, \circ)$  una struttura algebrica con operazione esterna e dominio di operatori  $A$ . Un sottoinsieme non vuoto  $X$  di  $S$  si dice *parte stabile* se:

$$a \circ x \in X , \text{ per ogni } x \in X \text{ e } a \in A .$$

◇

Anche in questo caso abbiamo una struttura indotta  $(X, \circ)$ .

La definizione di parte stabile si generalizza in modo ovvio al caso di strutture algebriche con piú operazioni.

**ESEMPI 5.1.19**

- L'insieme degli interi pari é stabile in  $(Z, +, \cdot)$ .
- L'insieme degli interi dispari non é stabile in  $(Z, +)$  e in  $(Z, +, \cdot)$ .
- L'insieme  $nZ$  costituito dai multipli di un fissato intero  $n \neq 0$  é una parte stabile in  $(Z, +, \cdot)$ .
- Gli insiemi  $\{0, 1\}$  e  $\{0, 1, -1\}$  sono stabili in  $(Z, \cdot)$  ma non sono stabili in  $(Z, +)$ .
- $Z$  é stabile in  $(Q, +, \cdot)$ .  $Q$  é stabile in  $(R, +, \cdot)$ .  $R$  é stabile in  $(C, +, \cdot)$ .
- I numeri complessi di modulo 1 sono una parte stabile di  $(C, \cdot)$  ma non sono una parte stabile di  $(C, +)$ .
- Le matrici diagonali d'ordine  $n$  sono una parte stabile dell'anello  $M_n(F)$ ,  $F = Q, R, C$ .
- Le matrici scalari d'ordine  $n$  sono una parte stabile dell'anello  $M_n(F)$ ,  $F = Q, R, C$ .  $\diamond$

**ESERCIZIO 5.1.20** *L'intersezione di una famiglia di parti stabili, se non é vuota, é ancora una parte stabile.*

**OSSERVAZIONE 5.1.21** L'unione di parti stabili non é in generale una parte stabile.  $\diamond$

**DEFINIZIONE 5.1.22** Sia  $X$  un insieme di elementi di una struttura algebrica. L'intersezione di tutte le parti stabili contenenti  $X$  prende il nome di *parte stabile generata da  $X$*  e si denota con  $st(X)$ .  $\diamond$

**ESERCIZIO 5.1.23** *Sia  $X$  un insieme di elementi di una struttura algebrica di sostegno  $S$ . Provare che un sottoinsieme  $Y$  di  $S$  é la parte stabile generata da  $X$  se, e solo se, valgono le seguenti due proprietá:*

- $Y$  é una parte stabile contenente  $X$ ;
- $Y$  é contenuto in ogni parte stabile che contenga  $X$ .

*Ne segue che  $st(X)$  é la minima parte stabile, rispetto all'inclusione, di  $S$  contenente  $X$ .*

**DEFINIZIONE 5.1.24** Sia  $X$  un insieme non vuoto di elementi di una struttura algebrica  $S$ . Se la parte stabile generata da  $X$  coincide con  $S$ , si dice che  $X$  é un *generatore* di  $S$ , o anche che  $X$  *genera*  $S$ .  $\diamond$

**ESEMPIO 5.1.25** Siano  $a, b$  due interi distinti e non nulli. In  $(Z, +)$  risulta:

- $st(a) = \{na : n \in Z^+\}$
- $st(a, b) = \{na + mb : n, m \in Z\}$ .  $\diamond$

**ESEMPIO 5.1.26** Siano  $X, Y$  sottoinsiemi non vuoti e distinti di  $S$ . In  $(P(S), \cap)$  risulta:

- $st(X, Y) = \{X, Y, X \cap Y\}$ .  $\diamond$

## 5.2 Semigrupperi

**DEFINIZIONE 5.2.1** Una struttura algebrica  $(S, \circ)$ , con operazione interna, si chiama *semigruppero* se l'operazione  $\circ$  é associativa. Se  $\circ$  é anche commutativa, il semigruppero si dice *commutativo* o *abeliano*.  $\diamond$

**ESEMPI 5.2.2** Le strutture sottoelencate sono esempi di semigrupperi.

- $(N_o, +), (Z, +), (Q, +), (R, +), (C, +), (Z_n, +).$
- $(N_o, \cdot), (Z, \cdot), (Q, \cdot), (R, \cdot), (C, \cdot), (Z_n, \cdot), (U(n), \cdot).$
- $(Z[x], +), (Q[x], +), (R[x], +), (C[x], +).$
- $(Z[x], \cdot), (Q[x], \cdot), (R[x], \cdot), (C[x], \cdot).$
- $(P(S), \cap), (P(S), \cup).$

 $\diamond$ 

**PROPOSIZIONE 5.2.3** Sia  $(S, \circ)$  un semigruppero e  $X$  un insieme non vuoto di elementi di  $S$ . Allora risulta

$$st(X) = \{x_1 \circ x_2 \circ \cdots \circ x_n : x_1, x_2, \dots, x_n \in X \text{ e } n \in N\}.$$

**DIMOSTRAZIONE.** L'asserto segue dal fatto che l'insieme

$$\{x_1 \circ x_2 \circ \cdots \circ x_n : x_1, x_2, \dots, x_n \in X \text{ e } n \in N\}$$

verifica le due proprietá dell'esercizio 5.1.23.  $\diamond$

**PROPOSIZIONE 5.2.4** In un semigruppero  $(S, \circ)$  con elemento neutro valgono le seguenti proprietá:

- $a$  simmetrizzabile  $\Rightarrow a$  ha un unico simmetrico;
- $a$  simmetrizzabile e tale che  $a \circ b = b \circ a \Rightarrow a' \circ b = b \circ a'$ .

**DIMOSTRAZIONE.** É lasciata per esercizio al Lettore.  $\diamond$

**ESERCIZIO 5.2.5** Siano  $a, b$  elementi simmetrizzabili di un semigruppero unitario  $(S, \circ)$ . Provare che  $a \circ b$  é simmetrizzabile e

$$(a \circ b)' = b' \circ a'. \quad (5.1)$$

Provare inoltre che  $(a \circ b)' = a' \circ b'$  se, e solo se, risulta  $a \circ b = b \circ a$ .

**ESERCIZIO 5.2.6** Sull'insieme  $S = R^3$  si consideri l'operazione "  $\circ$  " definita da

$$(a, b, c) \circ (a', b', c') = (aa', (a + b + c)b' + ba', (a + b + c)c' + ca').$$

Provare che  $(S, \circ)$  é un semigruppero unitario e che un elemento  $(a, b, c)$  é invertibile se, e solo se,  $a$  e  $a + b + c$  sono entrambi diversi da zero.

**DEFINIZIONE 5.2.7** Sia  $(S, \circ)$  una struttura algebrica con operazione interna. Un elemento  $a$  si dice *cancellabile a sinistra* (*a destra*) se:

$$a \circ b = a \circ c \Rightarrow b = c \quad (b \circ a = c \circ a \Rightarrow b = c).$$

L'elemento  $a$  si dice *cancellabile* o *regolare* se é cancellabile a sinistra e a destra. Se tutti gli elementi di  $S$  sono regolari, si dice che  $(S, \circ)$  é *regolare* o anche che in  $(S, \circ)$  vale la *legge di cancellazione*.  $\diamond$

**PROPOSIZIONE 5.2.8** Sia  $(S, \circ)$  un semigruppó unitario. Allora ogni suo elemento simmetrizzabile é regolare.

**DIMOSTRAZIONE.** Siano  $u$  l'unitá del semigruppó,  $a$  un elemento simmetrizzabile e  $a'$  il suo simmetrico. Se, per due elementi  $b, c \in S$ , risulta

$$a \circ b = a \circ c,$$

abbiamo

$$a' \circ (a \circ b) = a' \circ (a \circ c) \Rightarrow (a' \circ a) \circ b = (a' \circ a) \circ c \Rightarrow u \circ b = u \circ c \Rightarrow b = c.$$

Abbiamo cosí che  $a$  é cancellabile a sinistra. Allo stesso modo si vede che  $a$  é cancellabile a destra e l'asserto é provato.  $\diamond$

**ESERCIZIO 5.2.9** Provare che un elemento  $a \in Z_n^*$  che non sia invertibile non é cancellabile.

**DEFINIZIONE 5.2.10** Sia  $(S, \circ)$  una struttura algebrica con operazione interna. Due elementi  $a, b$  di  $S$  si dicono *permutabili* se

$$a \circ b = b \circ a.$$

Un elemento permutabile con tutti gli elementi di  $S$  si dice *centrale*. L'insieme di tutti gli elementi centrali si chiama *centro* di  $(S, \circ)$  e si denota con  $Z(S)$ .  $\diamond$

**OSSERVAZIONI 5.2.11** Valgono le seguenti proprietá:

- Ogni elemento é permutabile con se stesso.
- $S = Z(S)$  se, e solo se, l'operazione  $\circ$  é commutativa.
- Se  $(S, \circ)$  é un semigruppó si ha:
  - (1)  $a, b$  permutabili con  $c \Rightarrow a \circ b$  permutabile con  $c$ ;
  - (2) Se  $Z(S)$  é non vuoto, allora:  $a, b \in Z(S) \Rightarrow a \circ b \in Z(S)$ .  $\diamond$

### 5.3 Una tabella riassuntiva

Nella tabella che segue riassumiamo alcune proprietá delle operazioni piú usate.

Proprietá	$Q, R, C$	$Z$	$N_o$	$Z_n$ $n$ non primo	$Z_p$ $p$ primo	$M_n(K)$ $K = Q, R, C$
$a + b = b + a$	si	si	si	si	si	si
$ab = ba$	si	si	si	si	si	no
$(a + b) + c = a + (b + c)$	si	si	si	si	si	si
$(ab)c = a(bc)$	si	si	si	si	si	si
$a(b + c) = ab + ac$	si	si	si	si	si	si
esiste 0	si	si	si	si	si	si
esiste 1	si	si	si	si	si	si
$b - a$ esiste ed é unico	si	si	no	si	si	si
$a^{-1}, a \neq 0,$ esiste ed é unico	si	no	no	no	si	no
$ab = 0 \Leftrightarrow a = 0$ o $b = 0$	si	si	si	no	si	no

## 5.4 Isomorfismi

**ESEMPIO 5.4.1** Consideriamo le operazioni  $\cdot, +, *$  rispettivamente su

$$S_1 = \{1, r_1, r_2, r_3\}, \quad S_2 = \{0, 1, 2, 3\}, \quad S_3 = \{e, a, b, c\},$$

definite dalle seguenti tabelle di Cayley:

$\cdot$	1	$r_1$	$r_2$	$r_3$	$+$	0	1	2	3	$*$	$e$	$a$	$b$	$c$
1	1	$r_1$	$r_2$	$r_3$	0	0	1	2	3	$e$	$e$	$a$	$b$	$c$
$r_1$	$r_1$	$r_2$	$r_3$	1	1	1	2	3	0	$a$	$a$	$b$	$c$	$e$
$r_2$	$r_2$	$r_3$	1	$r_1$	2	2	3	0	1	$b$	$b$	$c$	$e$	$a$
$r_3$	$r_3$	1	$r_1$	$r_2$	3	3	0	1	2	$c$	$c$	$e$	$a$	$b$

E' evidente che, a meno dei nomi dati alle tre operazioni e agli elementi dei tre insiemi, le strutture considerate sono la stessa struttura; esse sono cioè *algebricamente equivalenti* o, come usualmente si dice, *isomorfe*. Per esempio possiamo identificare la seconda e la terza ponendo:

$$+ = *, \quad 0 = e, \quad 1 = a, \quad 2 = b, \quad 3 = c.$$

Nasce, cosí, l'esigenza di definire rigorosamente le situazioni che permettono di ritenere algebricamente equivalenti due strutture algebriche. Ciò si può fare introducendo il concetto di *isomorfismo*.  $\diamond$

**DEFINIZIONE 5.4.2** Siano  $(S, \circ_1)$  e  $(S', \circ_2)$  strutture algebriche con operazioni interne. Una applicazione biunivoca  $f: S \rightarrow S'$  si dice *isomorfismo* se

$$f(a \circ_1 b) = f(a) \circ_2 f(b), \quad \text{per ogni } a, b \in S.$$

$\diamond$

**DEFINIZIONE 5.4.3** Siano  $(S, \circ_1)$  e  $(S', \circ_2)$  strutture algebriche con operazioni esterne aventi lo stesso dominio di operatori  $A$ . Un'applicazione biunivoca  $f: S \rightarrow S'$  si dice *isomorfismo* se

$$f(\alpha \circ_1 a) = \alpha \circ_2 f(a), \quad \text{per ogni } \alpha \in A \text{ e } a \in S.$$

$\diamond$

**DEFINIZIONE 5.4.4** Un *isomorfismo* fra due strutture algebriche ad  $n$  operazioni

$$(S, \star_1, \star_2, \dots, \star_n) \quad \text{e} \quad (S', \circ_1, \circ_2, \dots, \circ_n)$$

é un'applicazione biunivoca  $f: S \rightarrow S'$  per cui esiste una permutazione  $\sigma$  degli indici  $1, 2, \dots, n$ , tale che  $f$  é un isomorfismo fra  $(S, \star_j)$  e  $(S', \circ_{\sigma(j)})$ , per ogni  $j = 1, 2, \dots, n$ .  $\diamond$

Riportiamo di seguito alcune proprietá degli isomorfismi di facile dimostrazione:

- L'identitá é un isomorfismo di ogni struttura algebrica in se stessa.
- $f$  isomorfismo  $\Rightarrow f^{-1}$  isomorfismo (*l'inverso di  $f$* ).
- $S_1 \xrightarrow{f} S_2 \xrightarrow{g} S_3$ ,  $f, g$  isomorfismi  $\Rightarrow S_1 \xrightarrow{fg} S_3$  isomorfismo.
- La relazione di isomorfismo fra strutture algebriche é di equivalenza.

**OSSERVAZIONE 5.4.5** Dal punto di vista algebrico due strutture isomorfe possono considerarsi equivalenti. Questo fatto si esprime dicendo che *lo studio delle strutture algebriche si fa a meno di isomorfismi*.  $\diamond$

**ESEMPIO 5.4.6** Si considerino le strutture algebriche  $(R^+, \cdot)$ , ove  $R^+$  denota l'insieme dei numeri reali positivi, e  $(R, +)$ . E' noto che la funzione logaritmo

$$\log : a \in R^+ \rightarrow \log a \in R$$

é biunivoca. Essa é un isomorfismo di  $(R^+, \cdot)$  in  $(R, +)$  perché risulta

$$\log(ab) = \log(a) + \log(b), \quad \text{per ogni } a, b \in R^+.$$

L'isomorfismo inverso della funzione logaritmo é la funzione esponenziale.  $\diamond$

**ESEMPIO 5.4.7** Sia  $S = \{1, 2, 3, \dots, n\}$  e, per ogni sottoinsieme  $A$  di  $S$ , si definisca la *funzione caratteristica  $f_A$  di  $A$*  nel seguente modo:

$$f_A(j) = \begin{cases} 1 & \text{se } j \in A \\ 0 & \text{se } j \notin A \end{cases},$$

per ogni  $j \in S$ . Denotato con  $V_n$  l'insieme delle  $n$ -ple ordinate degli elementi di  $Z_2 = \{0, 1\}$ , si può definire in  $V_n$  un'operazione di addizione nel seguente modo:

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n),$$

ove  $a_i + b_i$  é l'addizione modulo 2. Allora le strutture algebriche  $(P(S), \star)$ , ove  $\star$  é l'operazione di differenza simmetrica, e  $(V_n, +)$  sono isomorfe; un isomorfismo essendo dato dalla funzione  $f : P(S) \rightarrow V_n$  definita da

$$f(A) = (f_A(1), f_A(2), \dots, f_A(n)),$$

per ogni sottoinsieme  $A$  di  $S$ .  $\diamond$

## 5.5 Morfismi

Le definizioni che seguono introducono una importante generalizzazione del concetto di isomorfismo.

**DEFINIZIONE 5.5.1** Siano  $(S_1, \circ)$  e  $(S_2, *)$  due strutture algebriche con operazioni interne. Un'applicazione  $f: S_1 \rightarrow S_2$  si chiama *morfismo* o *omomorfismo* se:

$$f(a \circ b) = f(a) * f(b) \text{ per ogni } a, b \in S_1.$$

◇

**DEFINIZIONE 5.5.2** Siano  $(S_1, \circ)$  e  $(S_2, *)$  strutture algebriche con operazioni esterne aventi lo stesso dominio di operatori  $A$ . Una applicazione  $f: S_1 \rightarrow S_2$  si chiama *morfismo* se:

$$f(\alpha \circ a) = \alpha * f(a), \text{ per ogni } \alpha \in A \text{ e } a \in S_1.$$

◇

**DEFINIZIONE 5.5.3** Un *morfismo* fra due strutture

$$(S_1, \circ_1, \circ_2, \dots, \circ_n) \text{ , } (S_2, *_1, *_2, \dots, *_n)$$

ad  $n$  operazioni é una applicazione  $f: S_1 \rightarrow S_2$  se é un morfismo fra  $(S_1, \circ_j)$  e  $(S_2, *_j)$ , per ogni  $j = 1, 2, \dots, n$ .

◇

**OSSERVAZIONE 5.5.4** Un morfismo biiettivo é un isomorfismo. La nozione di morfismo é dunque una generalizzazione di quella di isomorfismo. Essa é molto utile perché due strutture non isomorfe possono essere legate tra loro da un morfismo e, come vedremo, vi sono proprietà delle strutture algebriche che sono conservate dai morfismi.

◇

**DEFINIZIONE 5.5.5** Un morfismo  $f$  si dice *monomorfismo* se é iniettivo, *epimorfismo* se é suriettivo.

◇

**ESERCIZIO 5.5.6** Siano  $S_1 = (S_1, \circ)$  e  $S_2 = (S_2, *)$  due strutture algebriche con operazioni interne e  $f: S_1 \rightarrow S_2$  un monomorfismo. Provare che  $f(S_1)$  é una parte stabile di  $(S_2, *)$ . Provare inoltre che la restrizione  $f: S_1 \rightarrow f(S_1)$  é un isomorfismo fra  $(S_1, \circ)$  e la struttura algebrica indotta da  $(S_2, *)$  su  $f(S_1)$ .

**ESERCIZIO 5.5.7** Provare le seguenti implicazioni:

- $S_1 \xrightarrow{f} S_2 \xrightarrow{g} S_3$ ,  $f, g$  morfismi  $\Rightarrow S_1 \xrightarrow{fg} S_3$  morfismo.
- $S_1 \xrightarrow{f} S_2$ ,  $f$  morfismo,  $X$  parte stabile di  $S_1 \Rightarrow f(X)$  parte stabile di  $S_2$ .

**ESEMPI 5.5.8**

- Le applicazioni  $a \in N \rightarrow a \in Z$ ,  $a \in Z \rightarrow a \in Q$ ,  $a \in Q \rightarrow a \in R$ ,  $a \in R \rightarrow a \in C$  sono morfismi rispetto alle operazioni  $+$  e  $\cdot$ .
- L'applicazione  $m \in Z \rightarrow [m] \in Z_n$  é un morfismo rispetto alle operazioni  $+$  e  $\cdot$ .
- L'applicazione  $A \in M_n(K) \rightarrow \det(A) \in K$ ,  $K = Q, R, C$ , é un morfismo fra  $(M_n(K), \cdot)$  e  $(K, \cdot)$ .

◇

**ESEMPIO 5.5.9** Siano  $V$  e  $W$  spazi vettoriali su un campo  $F$ . Allora ogni applicazione lineare fra  $V$  e  $W$  é un omomorfismo fra i gruppi additivi di  $V$  e  $W$ .  $\diamond$

**DEFINIZIONE 5.5.10** Un morfismo di una struttura algebrica  $S$  in se stessa si chiama *endomorfismo* di  $S$ . Un isomorfismo di una struttura algebrica in se stessa si chiama *automorfismo* di  $S$ .  $\diamond$

## 5.6 Gruppi e primi esempi

**DEFINIZIONE 5.6.1** Una struttura algebrica  $(S, \circ)$  si chiama *gruppo* se é un semigruppato con elemento neutro e con tutti gli elementi simmetrizzabili. In altre parole  $(S, \circ)$  é un gruppo se sono verificate le seguenti proprietà:

1. l'operazione  $\circ$  é associativa;
2. esiste l'elemento neutro  $u$ ;
3. ogni elemento di  $S$  é simmetrizzabile.

Se l'operazione  $\circ$  é commutativa il gruppo si dice *commutativo* o *abeliano*.  $\diamond$

Un gruppo si dice *moltiplicativo* (risp. *additivo*) se per la sua operazione si usa la notazione moltiplicativa (risp. additiva). Richiamiamo esplicitamente l'attenzione del Lettore sul fatto che la scelta della notazione per l'operazione di un gruppo é ininfluenza sulle proprietà algebriche del gruppo stesso.

**ESEMPI 5.6.2** Le strutture sottoelencate sono esempi di gruppi.

- $(Z, +), (Q, +), (R, +), (C, +), (Z_n, +)$  (*gruppi additivi* di  $Z, Q, R, C, Z_n$ ).
- $(nZ, +)$ , con  $n \in Z$  e  $nZ = \{nz : z \in Z\}$ .
- $(Q^*, \cdot), (R^*, \cdot), (C^*, \cdot), (U(n), \cdot), (Z_p^*, \cdot)$  *pprimo* (*gruppi moltiplicativi* di  $Q, R, C, Z_p$ ).
- $(Z[x], +), (Q[x], +), (R[x], +), (C[x], +), (Z_n[x], +)$  (*gruppi additivi* di  $Z[x], Q[x], R[x], C[x], Z_n[x]$ ).
- $(M_{m,n}(A), +)$ , con  $A = Z, Q, R, C$  (*gruppo additivo* di  $M_{m,n}(A)$ ).
- $(GL(n, F), \cdot)$ , con  $F = Q, R, C$  e  $GL(n, F) :=$  insieme delle matrici quadrate ad elementi in  $F$  con determinante non nullo (*gruppo lineare (generale)*).
- $(SL(n, F), \cdot)$ , con  $F = Q, R, C$  e  $GL(n, F) :=$  insieme delle matrici quadrate ad elementi in  $F$  con determinante 1 (*gruppo lineare speciale*).
- $(P(S), \star)$ , ove  $\star$  é l'operazione di differenza simmetrica nell'insieme delle parti di un insieme non vuoto  $S$ .
- $(G_n, \cdot)$ , con  $G_n = \{z \in C : z^n = 1\}$  (*il gruppo delle radici n-esime dell'unitá di C*).  $\diamond$

**ESERCIZIO 5.6.3** *Provare che un numero complesso  $\alpha$  é una radice n-esima dell'unitá di C se, e solo se, é del tipo  $\alpha = \cos(2\frac{m}{n}\pi) + i \sin(2\frac{m}{n}\pi)$ , con  $m \in Z$ .*

**ESEMPIO 5.6.4** Sia  $V$  uno spazio vettoriale su un campo  $F$ , per esempio  $F = Q, R, C$ . Allora  $V$ , rispetto all'addizione fra vettori, é un gruppo abeliano, detto *gruppo additivo di  $V$* .  $\diamond$

**ESERCIZIO 5.6.5** *Provare che l'insieme  $\text{Aut}(S)$  degli automorfismi di una struttura algebrica  $S$  é un gruppo rispetto al prodotto tra funzioni (il gruppo degli automorfismi di  $S$ ).*

Nel seguito, tranne esplicito avviso,  $G = (G, \cdot)$  denoterá sempre un gruppo moltiplicativo. Sará un utile esercizio per il Lettore trovare l'analogo nella notazione additiva di tutti i concetti che si daranno in notazione moltiplicativa.

**ESERCIZIO 5.6.6** *Siano  $a, b$  elementi di un gruppo  $G$ . Provare che ciascuna delle equazioni  $ax = b$  e  $xa = b$  ammette un'unica soluzione in  $G$ .*

Figura 5.1: N.H.Abel (1802-1829)

**DEFINIZIONE 5.6.7** Si chiama potenza  $n$ -esima di un elemento  $a \in G$ , e si denota con  $a^n$ , l'elemento di  $G$  definito per ricorrenza da

- per  $n \geq 0$  :

$$a^0 = 1, \quad a^n = a^{n-1}a,$$

- per  $n < 0$  :

$$a^n = (a^{-1})^{-n}.$$

$\diamond$

**OSSERVAZIONE 5.6.8** Sono verificate le seguenti proprietá, per ogni  $a, b \in G$ .

- $a^m a^n = a^{m+n} = a^n a^m$ .

- $ab = ba \Rightarrow (ab)^n = a^n b^n$ .

$\diamond$

**ESERCIZIO 5.6.9** *Trovare quattro matrici quadrate  $A, B, C, D$  in  $GL(2, Q)$  tali che  $(AB)^2 \neq A^2 B^2$  e  $(CD)^2 = C^2 D^2$ .*

**DEFINIZIONE 5.6.10** Sia  $a$  un elemento di  $G$ . Se esiste un intero  $m \neq 0$  tale che  $a^m = 1$  si dice che  $a$  é *periodico* o che ha *ordine finito*. In questo caso, il piú piccolo intero positivo  $n$  tale che  $a^n = 1$  si chiama *ordine* o *periodo* di  $a$  e si denota con  $|a|$  o con  $o(a)$ . Se per ogni intero positivo  $m$  risulta  $a^m \neq 1$  si dice che  $a$  é *aperiodico* o che ha *ordine infinito*.  $\diamond$

**ESERCIZIO 5.6.11** *Provare che un gruppo finito  $G$  d'ordine pari contiene almeno un elemento di periodo due.*

**SOLUZIONE.** Osserviamo che un elemento  $a \in G \setminus \{1\}$  ha periodo due se, e solo se,  $a = a^{-1}$  e che gli elementi  $b$  di  $G \setminus \{1\}$  per cui é  $b \neq b^{-1}$  sono in numero pari; deve, dunque, esistere in  $G$  almeno un elemento di periodo due.  $\diamond$

**PROPOSIZIONE 5.6.12** *Siano  $a$  un elemento di un gruppo  $G$  di periodo  $n$  ed  $m$  un intero positivo. Allora risulta  $a^m = 1$  se, e solo se,  $m$  é un multiplo di  $n$ .*

**DIMOSTRAZIONE.** Se é  $m = hn$ , risulta

$$a^m = a^{hn} = (a^n)^h = 1^h = 1,$$

ció la prima parte dell'asserto. Se é  $a^m = 1$ , detti  $q$  ed  $r$  il quoziente ed il resto della divisione tra  $m$  ed  $n$ , risulta

$$1 = a^m = a^{nq+r} = (a^n)^q a^r = a^r.$$

Allora, essendo  $r$  un intero non negativo minore di  $n$ , deve essere  $r = 0$  e l'asserto é provato.  $\diamond$

**OSSERVAZIONE 5.6.13** L'unitá é l'unico elemento di un gruppo di periodo 1.  $\diamond$

**ESERCIZIO 5.6.14** *L'analogo additivo del concetto di potenza  $n$ -sima di un elemento  $a$  si chiama multiplo di  $a$  secondo l'intero  $n$  e si denota con  $na$ . Definire i multipli in un gruppo additivo e studiarne le prime proprietá. Definire l'ordine di un elemento di un gruppo additivo.*

**ESERCIZIO 5.6.15** *Siano  $n > 1$  ed  $h \not\equiv 0 \pmod{n}$  due interi. Allora il periodo di  $h$  nel gruppo additivo  $(\mathbb{Z}_n, +)$  degli interi modulo  $n$  é uguale a  $\frac{n}{MCD(n,h)}$ . In particolare,  $h$  ha ordine  $n$  se, e solo se,  $n$  ed  $h$  sono coprimi.*

**SOLUZIONE.** Poniamo  $k = \frac{n}{MCD(n,h)}$ .

Se  $n$  ed  $h$  sono coprimi, ció  $k = n$ ,  $h$  ha periodo  $n$  in  $(\mathbb{Z}_n, +)$  perché nessuno degli interi

$$h, 2h, 3h, \dots, (n-1)h$$

é divisibile per  $n$ ; altrimenti  $h$  avrebbe un fattore non banale in comune con  $n$ .

Se  $n$  ed  $h$  non sono coprimi, non é restrittivo supporre che  $h$  sia minore di  $n$  perché ogni intero é congruo modulo  $n$  al proprio resto della divisione per  $n$ . In queste ipotesi risulta  $n = kh$  e gli interi

$$h, 2h, 3h, \dots, (k-1)h,$$

essendo positivi e minori di  $n$ , non sono divisibili per  $n$ . Ne segue che  $k$  é il periodo di  $h$  e l'asserto é provato.  $\diamond$

**ESEMPI 5.6.16**

- In  $(Z, +)$ ,  $(Q, +)$ ,  $(R, +)$ ,  $(C, +)$  ogni elemento diverso da zero ha ordine infinito.
- In  $(Q^*, \cdot)$ ,  $(R^*, \cdot)$  ogni elemento diverso da 1 e  $-1$  ha ordine infinito e risulta  $o(-1) = 2$ .
- In  $(C^*, \cdot)$  un elemento diverso da 1 ha periodo finito se, e solo se, é una radice  $n$ -esima dell'unitá, per qualche intero  $n > 1$ . Ne segue che gli elementi di periodo finito sono tutti e soli quelli del tipo

$$\cos\left(2\frac{m}{n}\pi\right) + i \operatorname{sen}\left(2\frac{m}{n}\pi\right), \text{ con } m, n \text{ interi e } n > 0.$$

Ogni radice  $n$ -esima dell'unitá ha ordine minore o uguale ad  $n$ . Quelle che hanno ordine  $n$  si chiamano *primitive*.  $\diamond$

**ESERCIZIO 5.6.17** Sia  $\alpha = \cos\left(2\frac{m}{n}\pi\right) + i \operatorname{sen}\left(2\frac{m}{n}\pi\right)$  una radice  $n$ -esima dell'unitá sul campo complesso  $C$ . Provare che  $\alpha$  é una radice primitiva se, e solo se,  $m$  ed  $n$  sono coprimi.

**DEFINIZIONE 5.6.18** Un gruppo  $G$  si dice *periodico*, o *di torsione*, se ogni suo elemento é periodico.  $G$  si dice *aperiodico*, o *senza torsione*, se ogni suo elemento diverso da 1 é aperiodico.  $G$  si dice *misto* se possiede sia elementi periodici diversi da 1 che elementi aperiodici.  $\diamond$

**ESEMPI 5.6.19**

- I gruppi finiti sono periodici.
- I gruppi  $(Z, +)$ ,  $(Q, +)$ ,  $(R, +)$ ,  $(C, +)$  sono aperiodici.
- I gruppi  $(Q^*, \cdot)$ ,  $(R^*, \cdot)$ ,  $(C^*, \cdot)$  sono misti.  $\diamond$

**PROPOSIZIONE 5.6.20** In un gruppo ogni elemento é regolare, cioé in esso vale la legge di cancellazione.

**DIMOSTRAZIONE.** É una conseguenza immediata della prop.5.2.8.  $\diamond$

**PROPOSIZIONE 5.6.21** Sia  $G$  un gruppo tale che  $a^2 = 1$ , per ogni  $a \in G$ . Allora  $G$  é abeliano.

**DIMOSTRAZIONE.** Se  $a, b \in G$ , abbiamo

$$aabb = a^2b^2 = 1 \cdot 1 = 1 = (ab)^2 = abab$$

e dalla legge di cancellazione ricaviamo  $ab = ba$ .  $\diamond$

**ESERCIZIO 5.6.22** Provare che un gruppo  $G$  é abeliano se, e solo se, risulta

$$(ab)^{-1} = a^{-1}b^{-1}, \text{ per ogni } a, b \in G.$$

**ESERCIZIO 5.6.23** Provare che un gruppo  $G$  é abeliano se, e solo se, risulta

$$(ab)^2 = a^2b^2, \text{ per ogni } a, b \in G.$$

**ESERCIZIO 5.6.24** Siano  $G$  un gruppo ed  $a$  un suo elemento di periodo 2. Provare che  $bab^{-1}$  ha periodo 2, per ogni  $b \in G$ . Dedurne che, se  $a$  é l'unico elemento di  $G$  di periodo 2, allora  $a$  é un elemento centrale in  $G$ .

**ESERCIZIO 5.6.25** Sia  $K$  un campo. Provare che il centro del gruppo  $GL(n, K)$  é l'insieme delle matrici scalari non nulle di ordine  $n$ .

**DEFINIZIONE 5.6.26** Siano  $G$  un gruppo e  $a$  un suo elemento. L'applicazione

$$\tau_a^s : x \in G \rightarrow ax \in G$$

si chiama *traslazione sinistra di ampiezza  $a$* . L'applicazione

$$\tau_a^d : x \in G \rightarrow xa \in G$$

si chiama *traslazione destra di ampiezza  $a$* . Se  $G$  é abeliano le traslazioni sinistra e destra di ampiezza  $a$  coincidono e, in questo caso, si parla semplicemente di *traslazione di ampiezza  $a$*  e la si denota col simbolo  $\tau_a$ .  $\diamond$

**ESERCIZIO 5.6.27** Provare che, se  $\tau_a^s = \tau_a^d$  per ogni elemento  $a$  di un gruppo  $G$ , allora  $G$  é abeliano.

**PROPOSIZIONE 5.6.28** Ogni traslazione sinistra (destra) di un gruppo  $G$  é una permutazione dell'insieme degli elementi di  $G$ .

**DIMOSTRAZIONE.** Sia  $a \in G$  e si supponga  $\tau_a^s(x) = \tau_a^s(y)$ , con  $x, y \in G$ . Allora risulta  $ax = ay$  e, per la legge di cancellazione,  $x = y$ ; cioè  $\tau_a^s$  é iniettiva. Inoltre, per ogni  $y \in G$ , risulta  $\tau_a^s(a^{-1}y) = y$ ; cosí  $\tau_a^s$  é anche suriettiva e quindi biunivoca.  $\diamond$

## 5.7 Anelli, corpi, campi e primi esempi

**DEFINIZIONE 5.7.1** Una struttura algebrica con due operazioni interne (*addizione e moltiplicazione*)  $A = (A, +, \cdot)$  si chiama *anello* se sono verificate le seguenti proprietà:

1.  $(A, +)$  é un gruppo abeliano,
2.  $(A, \cdot)$  é un semigruppó,
3. la moltiplicazione é distributiva rispetto all'addizione.

L'anello  $A$  si dice *commutativo* se la moltiplicazione é commutativa, si dice *unitario* se la moltiplicazione ammette elemento neutro 1.  $\diamond$

### ESEMPI 5.7.2

- $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Z}_n, +, \cdot)$  sono anelli commutativi unitari.
- $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$  sono anelli commutativi unitari.
- $(\mathbb{Z}[x], +, \cdot)$ ,  $(\mathbb{Q}[x], +, \cdot)$ ,  $(\mathbb{R}[x], +, \cdot)$ ,  $(\mathbb{C}[x], +, \cdot)$  sono anelli commutativi unitari.
- $(M_n(\mathbb{Z}), +, \cdot)$ ,  $(M_n(\mathbb{Z}_m), +, \cdot)$ ,  $(M_n(\mathbb{Q}), +, \cdot)$ ,  $(M_n(\mathbb{R}), +, \cdot)$ ,  $(M_n(\mathbb{C}), +, \cdot)$  sono anelli unitari non commutativi.
- $(2\mathbb{Z}, +, \cdot)$  é un anello commutativo privo di unitá.  $\diamond$

**OSSERVAZIONE 5.7.3** In un anello  $(A, +, \cdot)$  valgono le seguenti proprietà, per ogni  $a, b, c \in A$  e  $n \in \mathbb{Z}$ .

- $a0 = 0a = 0$ ,
- $a(-b) = (-a)b = -ab$ ,
- $(-a)(-b) = ab$ ,
- $(na)b = a(nb) = n(ab)$ ,
- $a(b - c) = ab - ac$  e  $(b - a)c = bc - ac$ . ◇

**OSSERVAZIONE 5.7.4** Se in un anello unitario  $A$  risulta  $1 = 0$ , abbiamo:

$$a = a1 = a0 = 0, \text{ per ogni } a \in A \Rightarrow A = \{0\}.$$

L'anello  $A = \{0\}$  si chiama *anello nullo*. ◇

Nel seguito  $A$  denoterá un anello che, tranne esplicito avviso, supporremo sempre non nullo.

**DEFINIZIONE 5.7.5** Sia  $a \in A$  con  $a \neq 0$ . L'elemento  $a$  si dice *divisore sinistro (destro) dello zero* se esiste in  $A$  un elemento  $b \neq 0$  tale che  $ab = 0$  ( $ba = 0$ .) L'elemento  $a$  si dice *divisore dello zero* se é divisore sia sinistro che destro dello zero. ◇

**ESERCIZIO 5.7.6** *Provare che in un anello esiste un divisore sinistro dello zero se, e solo se, esiste un divisore destro dello zero.*

**DEFINIZIONE 5.7.7** Un elemento  $a \in A$  si dice *nilpotente* se esiste un intero positivo  $n$  tale che  $a^n = 0$ . ◇

**OSSERVAZIONE 5.7.8** Un elemento nilpotente  $a$  di un anello é anche un divisore sinistro dello zero. Possono però esistere elementi non nilpotenti che sono divisori sinistri dello zero. Ad esempio, per l'elemento  $3 \in \mathbb{Z}_{21}$ , abbiamo  $3 \cdot 7 = 0$  e  $3^n \neq 0$  per ogni intero positivo  $n$ . ◇

**DEFINIZIONE 5.7.9** Un anello non nullo privo di divisori sinistri dello zero si chiama *anello integro*. Un anello integro commutativo si chiama *dominio di integritá*. ◇

**DEFINIZIONE 5.7.10** Sia  $A$  unitario. Un elemento  $a \in A$  si dice *invertibile* se é tale nel semigruppato  $(A, \cdot)$ . ◇

**OSSERVAZIONE 5.7.11** L'insieme degli elementi invertibili di un anello unitario  $A$  si denota con  $U(A)$  ed é un gruppo rispetto alla moltiplicazione. In particolare é un gruppo moltiplicativo l'insieme  $U(n)$  degli elementi invertibili di  $\mathbb{Z}_n$ . ◇

**DEFINIZIONE 5.7.12** Un anello unitario  $A$  si chiama *corpo* se é non nullo e ogni suo elemento non nullo é invertibile, cioè se  $U(A) = A \setminus \{0\}$ . Un corpo commutativo si chiama *campo*. ◇

**ESEMPIO 5.7.13** Le strutture algebriche  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$  e  $(\mathbb{Z}_p, +, \cdot)$ , con  $p$  primo, sono esempi di campi. Daremo nel seguito (cfr.7.3.4) un esempio di corpo (non commutativo).

Figura 5.2: J.H.M.Wedderburn (1882-1948)

Riportiamo senza dimostrazione il seguente importante teorema.

**TEOREMA 5.7.14 (teorema di Wedderburn)** *Ogni corpo finito é un campo.*

**DEFINIZIONE 5.7.15** Sia  $A$  un anello per cui non esiste alcun intero positivo  $n$  tale che  $na = 0$ , per ogni elemento  $a$  di  $A$ . Allora si dice che  $A$  ha *caratteristica zero*. Nel caso contrario, il minimo intero positivo  $c$  per cui  $ca = 0$ , per ogni elemento  $a$  di  $A$ , prende il nome di *caratteristica di  $A$* .  $\diamond$

**OSSERVAZIONE 5.7.16** L'anello nullo é l'unico anello di caratteristica 1.  $\diamond$

**ESERCIZIO 5.7.17** *Provare che:*

- $Z, Q, R, C$ , hanno *caratteristica zero*;
- $Z_m$  ha *caratteristica  $m$* ;
- $M_n(A)$ ,  $A = Z, Q, R, C, Z_m$ , ha *la stessa caratteristica di  $A$* ;
- $A[x]$ ,  $A = Z, Q, R, C, Z_m$ , ha *la stessa caratteristica di  $A$* .

**ESERCIZIO 5.7.18** *Sia  $K$  un campo. Provare che l'insieme  $M_n(K)$  delle matrici quadrate d'ordine  $n$  su  $K$  é un anello unitario rispetto alle operazioni di addizione e di moltiplicazione righe per colonne. Provare, inoltre, che  $M_n(K)$  ha la stessa caratteristica di  $K$ .*

## 5.8 Esercizi

**5.8.1** Portare in forma additiva le seguenti espressioni moltiplicative:

$$a^2b^3, a^{-2}(b^{-1}c)^2, (ab^2)^{-3}c^2 = 1.$$

**5.8.2** Sia  $B$  una matrice sui reali di tipo  $m \times n$ , con  $m \neq n$ , tal che  $B^t B$  sia invertibile ( $B^t$  denota la trasposta di  $B$ ). Posto  $A = B(B^t B)^{-1} B^t$ , provare che risulta  $A^2 = A$ .

**5.8.3** Verificare che in  $Z$  l'operazione di sottrazione non é associativa.

**5.8.4** In  $N_o$  si consideri la seguente operazione

$$n \circ m = |n - m|$$

e si provi che essa é commutativa e non associativa, che ammette elemento neutro e che esistono elementi non regolari.

**5.8.5** Completare la seguente tavola di Cayley in modo che essa definisca una operazione associativa sull'insieme  $\{a, b, c, d\}$ .

$\circ$	$a$	$b$	$c$	$d$
$a$	$a$	$b$	$c$	$d$
$b$	$b$	$a$	$c$	$d$
$c$	$c$	$d$	$c$	$d$
$d$				

**5.8.6** Provare che le operazioni definite sull'insieme  $\{a, b\}$  dalle seguenti tabelle di Cayley individuano due strutture algebriche isomorfe.

$\circ$	$a$	$b$	$\star$	$a$	$b$
$a$	$a$	$a$	$a$	$a$	$b$
$b$	$a$	$b$	$b$	$b$	$b$

**5.8.7** Sia

$$S = \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} : a, b, c \in Z_4 \right\}.$$

Provare che  $(S, \cdot)$ , ove  $\cdot$  indica la moltiplicazione righe per colonne, é un semigrupp unitario e determinare i suoi elementi invertibili.

**5.8.8** Nell'insieme  $R \setminus \{1\}$  si consideri la seguente operazione

$$a \circ b = \frac{(a-1)(b-1)}{2} + 1$$

e si provi che essa definisce un gruppo abeliano.

**5.8.9** Nell'insieme  $R$  si consideri la seguente operazione

$$a \circ b = \sqrt[5]{a^5 + b^5}$$

e si provi che essa definisce un gruppo abeliano.

**5.8.10** Nell'insieme  $R$  si consideri la seguente operazione

$$a \circ b = ab + a + b$$

e si provi che essa definisce un gruppo abeliano.

**5.8.11** Nell'insieme  $Q^+$  dei numeri razionali positivi si consideri la seguente operazione

$$a \circ b = \frac{ab}{2}$$

e si provi che essa definisce un gruppo abeliano.

**5.8.12** Provare che l'insieme dei numeri razionali del tipo  $3^m 6^n$ , ove  $m$  ed  $n$  sono interi, é un gruppo rispetto alla moltiplicazione.

**5.8.13** Su  $R^* = R \setminus \{0\}$  si consideri l'operazione "o" definita da

$$a \circ b = \begin{cases} ab & \text{se } a > 0 \\ \frac{a}{b} & \text{se } a < 0 \end{cases}$$

Provare che  $(R^*, \circ)$  é un gruppo.

Figura 5.3: K.Heisemberg (1901-1976)

**5.8.14** Provare che le matrici a coefficienti reali del tipo

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

formano un gruppo non abeliano rispetto alla moltiplicazione righe per colonne. Questo gruppo é noto come *gruppo di Heisemberg*.

**5.8.15** Provare che le matrici a coefficienti in  $Z_3$  del tipo

$$A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}, \text{ con } \det(A) = 1,$$

formano un gruppo rispetto alla moltiplicazione righe per colonne. Verificare se questo gruppo é abeliano.

**5.8.16** Sia  $S$  l'insieme delle matrici reali del tipo

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

Provare che  $S$  é un gruppo rispetto all'addizione e che  $S \setminus \{0\}$  é un gruppo rispetto alla moltiplicazione righe per colonne.

**5.8.17** Sia  $G$  l'insieme delle seguenti funzioni di  $R \setminus \{0, 1\}$  in se stesso:

$$i(x) = x, \quad a(x) = 1 - x, \quad b(x) = \frac{1}{x}, \quad c(x) = \frac{1}{1-x}, \quad d(x) = \frac{x}{x-1}, \quad e(x) = \frac{x-1}{x}.$$

Provare che  $G$ , rispetto al prodotto tra funzioni, forma un gruppo e scrivere la sua tabella di Cayley. Verificare, inoltre, se tale gruppo é abeliano.

**5.8.18** Siano  $a, b$  elementi di un gruppo  $G$  ed  $n$  un intero. Provare che risulta

$$(a^{-1}ba)^n = a^{-1}b^n a.$$

**5.8.19** Una matrice quadrata  $A$  d'ordine  $n$  i cui elementi appartengono ad un insieme  $X$  con  $n$  elementi si dice *quadrato latino* se ogni elemento di  $X$  compare esattamente una volta in ogni riga e colonna di  $A$ . Per esempio la matrice

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

é un quadrato latino. Provare che la tabella dell'operazione di un gruppo finito é un quadrato latino.

**5.8.20** Calcolare l'inverso di  $abc$ , ove  $a, b, c$  sono elementi di un gruppo. Stabilire poi se, e quando, é vera la relazione  $(abc)^{-1} = a^{-1}b^{-1}c^{-1}$ .

**5.8.21** Siano  $a, b, c$  elementi di un gruppo. Risolvere le seguenti equazioni in  $x$ :

$$axb = c, \quad a^{-1}xa = c, \quad acxb = c.$$

**5.8.22** Trovare esempi di anelli contenenti elementi  $a, b$  diversi da zero tali che  $ab = 0$ .

**5.8.23** Provare che in un anello commutativo unitario vale la *formula di Newton del binomio*, cioé che, per ogni intero non negativo  $n$  e per ogni  $a, b \in A$ , risulta

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

**5.8.24** Provare che gli elementi invertibili dell'anello  $M_2(Z)$  sono tutti e soli quelli con determinante uguale a  $\pm 1$ .