

## Capitolo 6

# Prime Proprietá dei Gruppi

### 6.1 Sottogruppi di un gruppo

Sia  $G$  un gruppo.

**DEFINIZIONE 6.1.1** Un sottoinsieme  $H$  di  $G$  si chiama *sottogruppo* se é una parte stabile e se é un gruppo rispetto all'operazione indotta in esso da  $G$ . Per un sottogruppo  $H$  di  $G$  si usa la notazione  $H \leq G$ .  $\diamond$

**OSSERVAZIONE 6.1.2** Notiamo esplicitamente che una parte stabile di un gruppo non é necessariamente un sottogruppo. Per esempio, nel gruppo additivo degli interi, il sottoinsieme  $N_0$  degli interi non negativi é una parte stabile ma, evidentemente, non é un sottogruppo.  $\diamond$

Ogni gruppo  $G$  possiede due sottogruppi *banali*:  $\{1\}$  (*sottogruppo identico*) e  $G$ . Un sottogruppo  $H$  diverso da  $G$  si dice *proprio* e per esso si usa la notazione  $H < G$ . Valgono, inoltre, le seguenti proprietá di facile verifica:

- l'unitá di  $H$  coincide con l'unitá di  $G$ ;
- l'inverso in  $H$  di un suo elemento  $a$  coincide con l'inverso di  $a$  in  $G$ ;
- $HH = \{ab : a, b \in H\} = H$ .

Le due proposizioni che seguono forniscono degli utili test per verificare se un sottoinsieme  $H$  di  $G$  é un sottogruppo.

**PROPOSIZIONE 6.1.3** In un gruppo  $G$  valgono le seguenti equivalenze:

- $H \leq G \Leftrightarrow \left\{ \begin{array}{l} H \text{ stabile,} \\ a \in H \Rightarrow a^{-1} \in H \end{array} \right\}$  ;
- $H \leq G \Leftrightarrow a^{-1}b \in H$ , per ogni  $a, b \in H$ ;

**DIMOSTRAZIONE.** E' lasciata per esercizio al Lettore.  $\diamond$

**PROPOSIZIONE 6.1.4** In un gruppo  $G$  vale la seguente equivalenza:

- $H \leq G$ ,  $H$  finito  $\Leftrightarrow H$  sottoinsieme finito e stabile di  $G$ .

**DIMOSTRAZIONE.** La prima implicazione é ovvia. Supponiamo, dunque, che  $H$  sia un sottoinsieme finito e stabile di  $G$ . Se  $b$  é un elemento di  $H$ , risulta

$$bH = \{ba : a \in H\} \subseteq HH = H.$$

D'altra parte, grazie alla legge di cancellazione, l'applicazione

$$a \in H \rightarrow ba \in H$$

é iniettiva, onde  $|bH| = |H|$  e quindi  $bH = H$ . Ne segue che esiste un elemento  $e \in H$  tale che  $be = b$ , da cui ricaviamo che é  $e = 1$  e  $1 \in H$ .

Ora, poiché  $1 \in H = bH$ , esiste un elemento  $c \in H$  tale che  $bc = 1$ , così  $c = b^{-1}$  e abbiamo che  $b^{-1} \in H$ , per ogni  $b \in H$ . Ne segue che  $H$  é un sottogruppo di  $G$ .  $\diamond$

**ESEMPI 6.1.5** I seguenti sottoinsiemi sono sottogruppi di  $G$  :

- $\langle a \rangle = \{a^n : n \in \mathbb{Z}\}$ , con  $a \in G$ .
- Il centro  $Z(G)$  di  $G$ .

$\diamond$

**ESERCIZIO 6.1.6** *Provare che gli insiemi*

$$H = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in \mathbb{Q} \right\}, \quad K = \left\{ \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix} : a \in \mathbb{Q} \right\}$$

*sono sottogruppi di  $GL(2, \mathbb{Q})$ .*

**ESERCIZIO 6.1.7** *Siano  $G$  un gruppo e  $H$  un suo sottogruppo. Provare che ogni sottogruppo di  $H$  é anche un sottogruppo di  $G$ .*

Elenchiamo alcune proprietà e definizioni relative ai sottogruppi di un gruppo.

- L'unione di due sottogruppi non é in generale un sottogruppo.
- L'intersezione di una famiglia di sottogruppi é un sottogruppo.
- La proprietà precedente permette di definire il *sottogruppo generato* da un sottoinsieme  $X$  di  $G$  come l'intersezione di tutti i sottogruppi di  $G$  che contengono  $X$ . Tale sottogruppo si denota con  $\langle X \rangle$  ed é il piú piccolo (rispetto all'inclusione) sottogruppo di  $G$  che contiene  $X$ .
- Un sottogruppo  $H$  di  $G$  é il sottogruppo generato da un sottoinsieme  $X$  di  $G$  se, e solo se, sono verificate le due seguenti proprietà:
  - (1)  $H$  é un sottogruppo di  $G$  contenente  $X$ ,
  - (2) ogni sottogruppo  $K$  di  $G$  contenente  $X$  contiene  $H$ .
- $\langle \emptyset \rangle = \{1\}$ .
- $H \leq G$  e  $X \subseteq H \Rightarrow \langle X \rangle \subseteq H$ .
- $X \subseteq Y \Rightarrow \langle X \rangle \subseteq \langle Y \rangle$ .
- $\langle X \rangle = X \Leftrightarrow X$  é un sottogruppo.

- Se  $X$  é non vuoto,

$$\langle X \rangle = \{a_1 a_2 \cdots a_n : a_j \in X \cup X^{-1}, n \in \mathbb{N}\}, \quad (6.1)$$

ove  $X^{-1}$  denota l'insieme i cui elementi sono gli inversi degli elementi di  $X$ .

- Sia  $X = H \cup K$ , ove  $H$  e  $K$  sono sottogruppi di  $G$ . Allora  $\langle X \rangle$  si chiama *sottogruppo generato da  $H$  e  $K$*  e si denota con  $\langle H, K \rangle$ . Risulta:

$$\langle H, K \rangle = \{h_1 k_1 h_2 k_2 \cdots h_n k_n : h_j \in H, k_j \in K, n \in \mathbb{N}\}. \quad (6.2)$$

- Sia  $X = \bigcup_{H \in \mathfrak{S}} H$ , ove  $\mathfrak{S}$  é una famiglia di sottogruppi di  $G$ . Allora  $\langle X \rangle$  si chiama *sottogruppo generato dalla famiglia  $\mathfrak{S}$*  e si denota con  $\langle H : H \in \mathfrak{S} \rangle$ . Risulta:

$$\langle H : H \in \mathfrak{S} \rangle = \{a_1 a_2 \cdots a_n : a_j \in X, n \in \mathbb{N}\}. \quad (6.3)$$

- Se risulta  $\langle X \rangle = G$  si dice che  $X$  é un *generatore di  $G$* , o anche che  $G$  é *generato da  $X$* .

**ESERCIZIO 6.1.8** *Provare che l'unione di una catena (rispetto all'inclusione) di sottogruppi di un gruppo é un sottogruppo.*

**ESERCIZIO 6.1.9** *Provare che*

$$H = \{2^n : n \in \mathbb{Z}\} \quad e \quad K = \left\{ \frac{1+2n}{1+2m} : n, m \in \mathbb{Z} \right\}$$

*sono sottogruppi del gruppo moltiplicativo  $Q^*$  dei razionali.*

**ESERCIZIO 6.1.10** *Provare che  $H = \{0, 4, 8, 12\}$  é un sottogruppo del gruppo additivo di  $Z_{16}$ .*

**ESERCIZIO 6.1.11** *Siano  $G_1$  e  $G_2$  due gruppi e  $f: G_1 \rightarrow G_2$  un monomorfismo. Provare che  $f(G_1)$  é un sottogruppo di  $G_2$  isomorfo a  $G_1$ .*

**DEFINIZIONE 6.1.12** Un gruppo  $G$  (risp. un sottogruppo  $H$  di  $G$ ) si dice *ciclico* se puó essere generato da un solo elemento, cioè se esiste  $a \in G$  (risp.  $a \in H$ ) tale che  $G = \langle a \rangle$  (risp.  $H = \langle a \rangle$ ).  $\diamond$

**OSSERVAZIONE 6.1.13** Se  $G$  é un gruppo ciclico ed  $a$  un suo generatore, risulta

$$G = \{a^n : n \in \mathbb{Z}\}.$$

$\diamond$

**ESERCIZIO 6.1.14** *Sia  $G = \langle a \rangle$  il gruppo ciclico generato dall'elemento  $a$ . Provare che  $G$  é infinito se, e soltanto se,  $a$  ha ordine infinito in  $G$  e, in questo caso, risulta  $a^h \neq a^k$ , per ogni due interi non negativi e distinti  $h$  e  $k$ . Provare inoltre che  $G$  é finito d'ordine  $n$  se, e soltanto se,  $a$  ha periodo finito  $n$  in  $G$  e, in questo caso, risulta  $G = \{1 = a^0, a, a^2, \dots, a^{n-1}\}$ .*

**ESEMPI 6.1.15**

- $(Z, +)$  é un gruppo ciclico, avendosi  $Z = \langle 1 \rangle = \langle -1 \rangle$ .
- $(Z_m, +)$  é un gruppo ciclico, avendosi  $Z_m = \langle 1 \rangle$ .

◇

**ESERCIZIO 6.1.16** *Provare che ogni gruppo ciclico é abeliano.*

**ESERCIZIO 6.1.17** *Provare che il gruppo delle radici  $n$ -esime dell'unitá del campo complesso é ciclico e determinare ciascuno dei suoi generatori.*

**ESERCIZIO 6.1.18** *Provare che il gruppo additivo dei razionali  $(Q, +)$  non é ciclico.*

**SOLUZIONE.** Per assurdo, sia  $\frac{n}{m} \in Q$  un generatore di  $(Q, +)$ , con  $n, m$  coprimi e osserviamo che deve essere  $m \neq \pm 1$ , perché un intero non può generare  $(Q, +)$ . Allora dovrebbe esistere un intero  $k$  tale che

$$\frac{n}{m^2} = k \frac{n}{m}$$

e, dovendo essere  $k = \frac{1}{m}$ , abbiamo un assurdo.

◇

### 6.1.1 Sottogruppi permutabili

Se  $A, B$  sono sottoinsiemi non vuoti di un gruppo  $G$ , poniamo

$$AB := \{ab : a \in A, b \in B\}.$$

**DEFINIZIONE 6.1.19** Due sottogruppi  $H, K$  di  $G$  si dicono *permutabili* se é  $HK = KH$ , cioè se, per ogni  $h \in H$  e  $k \in K$ , esistono  $h_1, h_2 \in H$  e  $k_1, k_2 \in K$  tali che  $hk = k_1h_1$  e  $kh = h_2k_2$ .<sup>1</sup> ◇

**TEOREMA 6.1.20** *Siano  $H, K$  sottogruppi di  $G$ . Allora risulta  $\langle H, K \rangle = HK$  se, e solo se,  $H$  e  $K$  sono permutabili.*

**DIMOSTRAZIONE.** Nell'ipotesi  $\langle H, K \rangle = HK$ , abbiamo:

- $\langle H, K \rangle = HK \Rightarrow \boxed{KH \subseteq HK}$ .
- $hk \in HK, h \in H, k \in K \Rightarrow (hk)^{-1} = k^{-1}h^{-1} \in HK$   
 $\Rightarrow k^{-1}h^{-1} = h_1k_1$  con  $h_1 \in H$  e  $k_1 \in K \Rightarrow hk =$   
 $(k^{-1}h^{-1})^{-1} = (h_1k_1)^{-1} = k_1^{-1}h_1^{-1} \in KH \Rightarrow \boxed{HK \subseteq KH}$ .

Ne segue che é  $HK = KH$ .

Nell'ipotesi  $HK = KH$ , dobbiamo provare che  $\langle H, K \rangle \subseteq HK$ , essendo evidente l'inclusione inversa.

- Sia  $h_1k_1h_2k_2 \cdots h_nk_n \in \langle H, K \rangle$ ,  $n > 0$ ,  $h_j \in H$ ,  $k_j \in K$ . Se é  $n = 1$  l'asserto é vero e quindi possiamo procedere per induzione su  $n$ :

$$\underbrace{h_1k_1h_2k_2 \cdots h_{n-1}k_{n-1}} h_nk_n = hkh_nk_n \text{ con } h \in H, k \in K \Rightarrow$$

<sup>1</sup>Notiamo esplicitamente che l'essere  $H$  e  $K$  permutabili non significa che  $hk = kh$ , per ogni  $h \in H$  e  $k \in K$ .

$$kh_n = h'k' \text{ con } h' \in H, k' \in K \text{ (perché } HK = KH) \Rightarrow$$

$$h_1k_1 \cdots h_nk_n = hh'k'k_n = h^*k^* \text{ con } h^* \in H \text{ e } k^* \in K. \quad \diamond$$

I due corollari che seguono sono di immediata dimostrazione.

**COROLLARIO 6.1.21** *Se  $G$  é un gruppo abeliano e  $H, K$  due suoi sottogruppi, allora risulta*

$$\langle H, K \rangle = HK = KH.$$

**COROLLARIO 6.1.22** *Siano  $G$  un gruppo e  $H_1, H_2, \dots, H_n$  sottogruppi di  $G$  a due a due permutabili. Allora*

$$H = H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n : h_j \in H_j\}$$

*é un sottogruppo di  $G$  e risulta  $H = \langle H_1, H_2, \dots, H_n \rangle$ .*

**DEFINIZIONE 6.1.23** Siano  $G$  un gruppo e  $H_1, H_2, \dots, H_n$  sottogruppi di  $G$  a due a due permutabili. Il sottogruppo di  $G$

$$H = H_1H_2 \cdots H_n = \{h_1h_2 \cdots h_n : h_j \in H_j\},$$

definito dal corollario precedente, si chiama *prodotto* di  $H_1, H_2, \dots, H_n$ . \(\diamond\)

**ESEMPIO 6.1.24** Vogliamo dare un esempio di due sottogruppi  $H, K$  di un gruppo per cui risulta  $\langle H, K \rangle \neq HK$ . Naturalmente, in forza del teorema 6.1.20,  $H$  e  $K$  non dovranno essere permutabili. A Tale scopo, nel gruppo  $G = GL(2, Q)$  consideriamo i sottogruppi (cfr.6.1.6 )

$$H = \left\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} : b \in Q \right\}, \quad K = \left\{ \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix} : a \in Q \right\}$$

e osserviamo che é

$$HK = \left\{ \begin{bmatrix} 1+ab & b \\ a & 1 \end{bmatrix} : a, b \in Q \right\}.$$

Osserviamo ancora che le matrici

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \text{ e } B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

appartengono ad  $HK$ , mentre il loro prodotto

$$AB = \begin{bmatrix} 2 & 3 \\ 1 & 2 \end{bmatrix}$$

non vi appartiene. Questo significa che  $HK$  non é un sottogruppo di  $GL(2, Q)$  e, quindi,  $\langle H, K \rangle \neq HK$ . \(\diamond\)

**TEOREMA 6.1.25 (identitá di Dedekind)** *Siano  $H, K, L$  sottogruppi di  $G$  tali che*

$$HK = KH \quad \text{e} \quad H \leq L.$$

*Allora risulta*

$$(i) \quad HK \cap L = H(K \cap L) \quad \text{e} \quad (ii) \quad H(K \cap L) = (K \cap L)H.$$

**DIMOSTRAZIONE.** Abbiamo:

•  $H \leq L, H \leq HK \Rightarrow H \leq HK \cap L$  e sappiamo che  $K \cap L \subseteq HK \cap L \Rightarrow H(K \cap L) \subseteq HK \cap L$ .

•  $a \in HK \cap L \Rightarrow a \in HK$  e  $a = hk$  con  $h \in H, k \in K \Rightarrow k = h^{-1}a, h^{-1} \in H \leq L, a \in HK \cap L \leq L \Rightarrow K \ni k = h^{-1}a \in L \Rightarrow k \in K \cap L \Rightarrow a \in H(K \cap L) \Rightarrow HK \cap L \subseteq H(K \cap L)$ .

Abbiamo così la (i).

• Poiché  $HK \cap L$  è un sottogruppo di  $G$ , per la (i), anche  $H(K \cap L)$  è un sottogruppo di  $G$ . Allora  $H$  e  $K \cap L$  devono essere permutabili, cioè la (ii).  $\diamond$

### 6.1.2 Sottogruppi di $(Z, +)$ e di $(Z_n, +)$ .

Abbiamo già osservato che i gruppi  $(Z, +)$  e  $(Z_n, +)$ , per ogni intero  $n > 1$  sono ciclici. Ci proponiamo, ora, di studiare i sottogruppi di tali gruppi.

**OSSERVAZIONE 6.1.26** Sia  $m$  un intero. L'insieme  $mZ = \{ma : a \in Z\}$  dei multipli di  $m$  è un sottogruppo ciclico di  $(Z, +)$ , avendosi  $mZ = \langle m \rangle$ . Inoltre risulta  $mZ = Z$  se, e solo se,  $m = \pm 1$ .  $\diamond$

**PROPOSIZIONE 6.1.27** Ogni sottogruppo  $H$  di  $(Z, +)$  è del tipo

$$mZ = \{ma : a \in Z\},$$

ove  $m$  è il minimo fra gli interi non negativi contenuti in  $H$ . In particolare si ha che tutti i sottogruppi di  $(Z, +)$  sono ciclici.

**DIMOSTRAZIONE.** Abbiamo già osservato che  $mZ$  è un sottogruppo ciclico di  $(Z, +)$ . Supponiamo dunque che  $H$  sia un sottogruppo non banale e non nullo, altrimenti l'asserto è vero. In tale ipotesi  $H$  contiene almeno un intero positivo; quindi possiamo considerare il minimo  $m$  degli interi positivi contenuti in  $H$  e risulta  $mZ \leq H$ . Detto  $a$  un elemento di  $H$ , se  $q, r$  sono rispettivamente il quoziente ed il resto della divisione di  $a$  per  $m$ , abbiamo

$$a = mq + r \Rightarrow r = a - mq \in H \Rightarrow r = 0,$$

cioè  $a$  è un multiplo di  $m$  e quindi  $H \leq mZ$ . Ne segue che  $H = mZ$ .  $\diamond$

Dalla prop.6.1.27 e dall'osservazione 6.1.26 si ha subito il seguente corollario.

**COROLLARIO 6.1.28** Gli interi 1 e  $-1$  sono gli unici generatori del gruppo  $(Z, +)$ .

**ESERCIZIO 6.1.29** Provare che  $nZ$  è contenuto in  $mZ$  se, e solo se,  $m$  divide  $n$ .

**ESERCIZIO 6.1.30** Provare che in  $(Z, +)$  il sottogruppo  $\langle a, b \rangle$  generato da due interi distinti  $a, b$  coincide col sottogruppo ciclico generato da un massimo comune divisore di  $a$  e  $b$ . Provare, inoltre, che un minimo comune multiplo di  $a$  e  $b$  è un generatore del sottogruppo intersezione di  $\langle a \rangle$  e  $\langle b \rangle$ .

**PROPOSIZIONE 6.1.31** Sia  $h$  un elemento non nullo del gruppo additivo  $(Z_n, +)$  degli interi modulo  $n$ . Allora il sottogruppo ciclico  $\langle h \rangle$  generato da  $h$  ha ordine  $\frac{n}{MCD(n,h)}$ . In particolare,  $h$  é un generatore di  $(Z_n, +)$  se, e solo se, é coprimo con  $n$ .

**DIMOSTRAZIONE.** Segue immediatamente dall'esercizio 5.6.15.  $\diamond$

**PROPOSIZIONE 6.1.32** Ogni sottogruppo del gruppo additivo  $(Z_n, +)$  é ciclico ed ha ordine divisibile per  $n$ .

**DIMOSTRAZIONE.** Assumiamo  $Z_n = \{0, 1, 2, \dots, n-1\}$ , sia  $H$  un sottogruppo non nullo di  $(Z_n, +)$  e sia  $h$  il piú piccolo intero positivo contenuto in  $H$ . Ovviamente risulta  $\langle h \rangle \leq H$ . Sia ora  $m$  un elemento di  $H$  e siano  $q, r$  il quoziente e il resto della divisione fra  $m$  ed  $h$ . Poiché risulta  $m - qh = r$  e  $m, qh \in H$ , l'intero  $r$ , che é minore di  $h$ , appartiene ad  $H$ . Ne segue che  $r = 0$ , cioè  $H \leq \langle h \rangle$ , e in definitiva abbiamo  $H = \langle h \rangle$ . Ora, dalla proposizione precedente abbiamo che l'ordine di  $H$  divide  $n$  e l'asserto é provato.  $\diamond$

Le ultime due proposizioni hanno il seguente corollario.

**COROLLARIO 6.1.33** Sia  $(Z_n, +)$  il gruppo additivo degli interi modulo  $n$  ed  $h$  un divisore positivo di  $n$ . Allora  $(Z_n, +)$  contiene un unico sottogruppo d'ordine  $h$ .

**DIMOSTRAZIONE.** Posto  $Z_n = \{0, 1, 2, \dots, n-1\}$  e  $n = hk$ , il sottogruppo  $\langle k \rangle$  generato da  $k$  ha ordine  $h$ . Sia ora  $H$  un sottogruppo di  $Z_n$  d'ordine  $h$ . Sappiamo che  $H$  é ciclico e che il periodo di un suo generatore  $m$  é  $h$ , per cui  $hm \equiv 0 \pmod{n}$ . Ne segue che esiste un intero  $q$  tale che  $hm = qn$ , da cui  $m = qk \in \langle k \rangle$ . Allora risulta  $H \subseteq \langle k \rangle$  e, essendo sia  $H$  che  $\langle k \rangle$  d'ordine  $h$ , risulta  $H = \langle k \rangle$ . L'asserto é dunque completamente provato.  $\diamond$

**OSSERVAZIONE 6.1.34** Notiamo esplicitamente che, se assumiamo  $Z_n = \{0, 1, 2, \dots, n-1\}$ , e  $h$  é un intero positivo che divide  $n$ , posto  $n = hk$ , il sottogruppo ciclico generato da  $h$  in  $(Z_n, +)$  ha ordine  $k$  ed é dato da

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

L'applicazione

$$m \in Z_k = \{0, 1, \dots, k-1\} \rightarrow mh \in \langle h \rangle$$

é evidentemente un isomorfismo fra i gruppi  $(Z_k, +)$  e  $\langle h \rangle$  e, per questo motivo nel seguito  $\langle h \rangle$  sará impropriamente denotato con  $Z_k$ .  $\diamond$

## 6.2 Esempi notevoli di gruppi

### 6.2.1 Il gruppo simmetrico $S_n$

Sia  $X$  un insieme finito e non vuoto con  $n$  elementi. Ricordiamo che si definisce *permutazione su  $X$*  una qualsiasi applicazione biunivoca di  $X$  su se stesso e che tutte le permutazioni su  $X$  formano un gruppo rispetto al prodotto di funzioni. Tale gruppo, che abbiamo denotato con  $Symm(X)$ , si chiama *gruppo simmetrico su  $n$  oggetti*, o *di grado  $n$* .

**OSSERVAZIONE 6.2.1** Se  $Y$  é un insieme non vuoto con  $n$  elementi e  $f$  é una funzione biunivoca di  $X$  su  $Y$ , é facile verificare che l'applicazione

$$\sigma \in S(X) \rightarrow f^{-1}\sigma f \in S(Y)$$

é un isomorfismo di gruppi. Pertanto, il gruppo  $S(X)$ , a meno di isomorfismi, dipende solo dalla cardinalità  $X$ .  $\diamond$

Per non appesantire le notazioni supporremo sempre  $X = N_n = \{1, 2, \dots, n\}$  e denoteremo con  $S_n$  il gruppo  $Symm(X)$ .

A volte può essere comodo rappresentare una permutazione  $\sigma \in S_n$  mediante la matrice

$$\begin{bmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{bmatrix},$$

che ha nella prima riga gli interi da 1 ad  $n$  disposti in ordine crescente e sotto ognuno di essi l'intero corrispondente in  $\sigma$ . Ovviamente, con questa notazione, la matrice

$$\begin{bmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{bmatrix}$$

rappresenta la permutazione identica.

**ESEMPIO 6.2.2** Le permutazioni  $\sigma$  e  $\tau$  di  $N_4 = \{1, 2, 3, 4\}$  definite da

$$\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 4, \sigma(4) = 1; \tau(1) = 3, \tau(2) = 4, \tau(3) = 1, \tau(4) = 2$$

si scrivono

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix}, \quad \tau = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix}.$$

In questo modo se, per esempio, vogliamo calcolare l'immagine di 2 nel prodotto  $\sigma\tau$ , basta leggere l'intero sotto 2 nella tabella di  $\sigma$ , nel nostro caso 3, e poi l'intero sotto 3 nella tabella di  $\tau$ ; abbiamo così  $\sigma\tau(2) = \tau(\sigma(2)) = 1$ .  $\diamond$

**ESEMPIO 6.2.3** Si riportano di seguito tutti gli elementi del gruppo simmetrico  $S_3$  :

$$1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \quad r_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \quad r_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix},$$

$$s_1 = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \quad s_2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \quad s_3 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}.$$

$\diamond$

Se  $m, n$  sono interi positivi con  $m < n$ , ad ogni  $\sigma \in S_m$  possiamo associare la permutazione  $\sigma' \in S_n$  che opera come  $\sigma$  sugli interi  $1, 2, \dots, m$  e trasforma in se stesso ogni altro elemento di  $N_n$ . L'applicazione

$$f : \sigma \in S_m \rightarrow \sigma' \in S_n$$

é un monomorfismo di gruppi e, quindi, l'immagine  $f(S_m)$  é isomorfa ad  $S_m$ .

Nel seguito identificheremo  $S_m$  con  $f(S_m)$  e, con abuso di notazione, denoteremo ancora con  $\sigma$  la permutazione  $\sigma' = f(\sigma)$ . Per esempio, con questa convenzione, la permutazione

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix},$$

considerata come elemento di  $S_6$ , é la permutazione

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 1 & 5 & 6 \end{bmatrix}.$$

Osserviamo ancora che, se  $\sigma$  e  $\tau$  sono le due permutazioni su  $N_3$  definite da

$$\sigma = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \quad \tau = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix},$$

risulta  $\sigma\tau \neq \tau\sigma$  e si ha cosí la seguente proposizione.

**PROPOSIZIONE 6.2.4** *Il gruppo simmetrico  $S_n$  non é abeliano per ogni intero  $n$  maggiore di 2.*

**ESERCIZIO 6.2.5** *Provare che  $S_3$  (che é non abeliano) possiede solo sottogruppi propri abeliani.*

Calcolare l'ordine di  $S_n$  é un facile esercizio (cfr.1.6.1). Abbiamo infatti che, se si vuole costruire una permutazione  $\sigma$  su  $N_n$ , vi sono  $n$  possibili scelte per  $\sigma(1)$ ,  $n - 1$  per  $\sigma(2)$ ,  $n - 3$  per  $\sigma(3)$  e cosí via. Ne segue per induzione che

$$|S_n| = n!. \tag{6.4}$$

**DEFINIZIONE 6.2.6** Diciamo che un elemento  $j$  di  $N_n$  é *unito* o *fisso* in una permutazione  $\sigma$  se risulta  $\sigma(j) = j$  e denotiamo con  $F(\sigma)$  l'insieme degli elementi uniti di  $\sigma$ , cioè

$$F(\sigma) = \{x \in N_n : \sigma(x) = x\}.$$

Due permutazioni  $\sigma$  e  $\tau$  si dicono *disgiunte* se i rispettivi insiemi di elementi non uniti,  $N_n \setminus F(\sigma)$  e  $N_n \setminus F(\tau)$ , sono ad intersezione vuota.  $\diamond$

**ESERCIZIO 6.2.7** *Provare che due permutazioni disgiunte sono elementi permutabili di  $S_n$ .*

**DEFINIZIONE 6.2.8** Una permutazione  $\sigma$  si dice *k-ciclo* o *ciclo di lunghezza k* se, detto  $j$  un elemento di  $N_n$  non unito in  $\sigma$ , risulta

$$N_n \setminus F(\sigma) = \{j, \sigma(j), \sigma^2(j), \dots, \sigma^{k-1}(j)\}$$

e, in questo caso, si usa per  $\sigma$  la seguente notazione

$$\sigma = (j, \sigma(j), \sigma^2(j), \dots, \sigma^{k-1}(j)).$$

Un  $n$ -ciclo  $\sigma \in S_n$  prende il nome di *permutazione ciclica* di  $N_n$ . La permutazione identica, che si chiama *ciclo banale*, é l'unico ciclo di lunghezza 1.  $\diamond$

Osserviamo esplicitamente che nella  $k$ -pla  $(j, \sigma(j), \sigma^2(j), \dots, \sigma^{k-1}(j))$  che denota il  $k$ -ciclo  $\sigma$  compaiono soltanto gli elementi di  $N_n$  spostati da  $\sigma$  e questi sono ordinati in modo che, tranne che per l'ultimo, l'immagine in  $\sigma$  di ciascuno di essi é data dal successivo, mentre l'ultimo elemento ha per immagine il primo. Inoltre, se  $t$  é un qualsiasi elemento di  $N_n$  diverso da  $j$  e spostato da  $\sigma$ , risulta anche  $\sigma = (t, \sigma(t), \sigma^2(t), \dots, \sigma^{k-1}(t))$ . Per esempio, il 5-ciclo  $\sigma = (2, 1, 3, 4, 7)$  di  $S_7$  é la permutazione su  $N_7$  definita da

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 7 & 5 & 6 & 2 \end{bmatrix};$$

in questo caso é  $F(\sigma) = \{5, 6\}$  e si ha anche

$$\sigma = (1, 3, 4, 7, 2) = (3, 4, 7, 2, 1) = (4, 7, 2, 1, 3) = (7, 2, 1, 3, 4).$$

**ESERCIZIO 6.2.9** *Provare che*

$$(i_1, i_2, \dots, i_k)^{-1} = (i_k, i_{k-1}, \dots, i_1),$$

per ogni  $k$ -ciclo  $(i_1, i_2, \dots, i_k)$  di  $S_n$ .

Dalla definizione di ciclo segue subito la seguente proposizione.

**PROPOSIZIONE 6.2.10** *Sia  $\sigma$  un  $k$ -ciclo di  $S_n$ . Allora risulta*

$$\sigma^k = 1 \text{ e } \sigma^h \neq 1, \text{ con } 1 \leq h < k,$$

*cioé ogni  $k$ -ciclo é un elemento d'ordine  $k$  in  $S_n$ .*

Nello studio del gruppo simmetrico  $S_n$  i cicli sono di fondamentale importanza. Essi infatti generano  $S_n$  e giocano in qualche modo un ruolo simile a quello dei numeri primi nella fattorizzazione degli interi, nel senso precisato dal seguente teorema.

**PROPOSIZIONE 6.2.11** *Ogni permutazione  $\sigma \in S_n$  può decomporre in un prodotto di cicli non banali e disgiunti. Tale decomposizione é unica a meno dell'ordine dei cicli nella fattorizzazione.*

**DIMOSTRAZIONE.** Essendo l'asserto ovvio nei casi  $n = 1, 2$ , possiamo supporre  $n > 2$  e procedere per induzione su  $n$ . Siano, dunque,  $j$  un elemento di  $N_n$  non unito in  $\sigma$  ed  $m$  il piú piccolo intero positivo tale che  $\sigma^m(j) = j$ . Osserviamo che, nel caso  $m = n$ ,  $\sigma$  é un ciclo di lunghezza  $n$  e non abbiamo nulla da provare. Se é  $m < n$ , detta  $\tau$  la permutazione che fissa  $j, \sigma(j), \sigma^2(j), \dots, \sigma^{m-1}(j)$  e opera come  $\sigma$  sui rimanenti  $n - m$  elementi di  $N_n$ , risulta

$$\sigma = (j, \sigma(j), \sigma^2(j), \dots, \sigma^{m-1}(j)) \tau = \tau (j, \sigma(j), \sigma^2(j), \dots, \sigma^{m-1}(j)).$$

Si noti che, per costruzione, il ciclo  $(j, \sigma(j), \sigma^2(j), \dots, \sigma^{m-1}(j))$  e la permutazione  $\tau$  sono disgiunti e, quindi, permutabili. Inoltre, in forza della legge di cancellazione,  $\tau$  é l'unica permutazione in  $S_n$  che verifica l'uguaglianza precedente. Allora, potendosi  $\tau$  riguardare come una permutazione su  $n - m$  oggetti, dall'ipotesi di induzione su  $n$  segue facilmente l'asserto.  $\diamond$

Nel seguito, quando parleremo di *fattorizzazione di una permutazione in cicli disgiunti*, sottintenderemo sempre che tali cicli sono non banali. La scrittura di una permutazione  $\sigma$  come prodotto di cicli disgiunti prende il nome di *notazione ciclica* di  $\sigma$  ed é chiaro che, se un elemento  $j \in N_n$  non compare in nessuno dei cicli che fattorizzano  $\sigma$ , allora  $j$  é unito in  $\sigma$ .

**PROPOSIZIONE 6.2.12** *L'ordine di un elemento  $\sigma$  di  $S_n$  é uguale al minimo comune multiplo delle lunghezze dei cicli che fattorizzano  $\sigma$ .*

**DIMOSTRAZIONE.** Sia  $\sigma_1\sigma_2\cdots\sigma_k$  la fattorizzazione di  $\sigma$  in cicli disgiunti, sia  $s_j$  l'ordine di  $\sigma_j$  e poniamo

$$m = mcm(s_1, s_2, \dots, s_k), \quad m = s_j m_j,$$

per ogni  $j = 1, 2, \dots, k$ . I cicli  $\sigma_1, \sigma_2, \dots, \sigma_k$  sono a due a due disgiunti e quindi a due a due permutabili; ne segue che

$$\sigma^t = \sigma_1^t \sigma_2^t \cdots \sigma_k^t,$$

per ogni intero  $t$ . Allora risulta

$$\sigma^m = \sigma_1^m \sigma_2^m \cdots \sigma_k^m = (\sigma_1^{s_1})^{m_1} (\sigma_2^{s_2})^{m_2} \cdots (\sigma_k^{s_k})^{m_k} = 1.$$

Inoltre, se  $t$  é un intero positivo minore di  $m$ , esiste un indice  $j$  tale che  $t$  non é multiplo di  $s_j$ . Ne segue che

$$\sigma_j^t \neq 1$$

e

$$\sigma^t = \sigma_1^t \sigma_2^t \cdots \sigma_k^t \neq 1.$$

L'asserto é cosí provato. ◇

### 6.2.2 Il gruppo alterno $A_n$

Sia  $S_n$  il gruppo simmetrico su  $n$  oggetti, cioè il gruppo di tutte le permutazioni sull'insieme  $N_n = \{1, 2, \dots, n\}$ . I cicli di lunghezza 2 prendono il nome di *trasposizioni* ed é chiaro che, per ogni trasposizione  $\sigma$ , risulta  $\sigma = \sigma^{-1}$ . Ogni trasposizione ha dunque periodo due in  $S_n$ .

Osserviamo che ogni ciclo, e quindi ogni permutazione, può scriversi come prodotto di trasposizioni; infatti si ha

$$(j_1, j_2, \dots, j_k) = (j_1, j_2)(j_1, j_3) \cdots (j_1, j_{k-1})(j_1, j_k).$$

Una permutazione  $\sigma$  può in generale fattorizzarsi in modi diversi mediante trasposizioni, nel senso che le trasposizioni di una sua fattorizzazione e il loro numero non sono degli invarianti di  $\sigma$ ; in altre parole possiamo dire che per le trasposizioni non vale un teorema analogo a quello dimostrato per la decomposizione di una permutazione in cicli.

**DEFINIZIONE 6.2.13** Allo scopo di trovare un invariante delle possibili fattorizzazioni di una permutazione in trasposizioni diamo le seguenti definizioni per una permutazione  $\sigma$  :

- Considerata una coppia  $(i, j)$ , ove  $i, j$  sono elementi di  $N_n$  con  $i < j$ , si dice che  $\sigma$  presenta un'*inversione* su  $(i, j)$  se risulta  $\sigma(i) > \sigma(j)$ .

- Si dice che  $\sigma$  é una permutazione *pari* se presenta un numero pari di inversioni, *dispari* nel caso contrario.

- si definisce *segno* di  $\sigma$ , e si denota con  $sgn(\sigma)$ , l'intero 1 o  $-1$  a seconda che  $\sigma$  sia rispettivamente pari o dispari. ◇

**ESEMPIO 6.2.14** Ogni trasposizione é una permutazione dispari e il suo segno é  $-1$ . La permutazione identica é ovviamente pari.  $\diamond$

Per ogni permutazione  $\sigma$  risulta

$$\prod_{\{i,j\} \subseteq N_n} \frac{i-j}{\sigma(i)-\sigma(j)} = \prod_{i < j} \frac{i-j}{\sigma(i)-\sigma(j)} = \text{sgn}(\sigma)$$

e, per ogni due permutazioni  $\sigma$  e  $\tau$ , risulta

$$\begin{aligned} \text{sgn}(\sigma\tau) &= \prod_{i < j} \frac{i-j}{(\sigma\tau)(i)-(\sigma\tau)(j)} = \\ &= \left( \prod_{i < j} \frac{i-j}{\sigma(i)-\sigma(j)} \right) \left( \prod_{i < j} \frac{\sigma(i)-\sigma(j)}{\tau(\sigma(i))-\tau(\sigma(j))} \right) = \\ &= \left( \prod_{i < j} \frac{i-j}{\sigma(i)-\sigma(j)} \right) \left( \prod_{\sigma(i) < \sigma(j)} \frac{\sigma(i)-\sigma(j)}{\tau(\sigma(i))-\tau(\sigma(j))} \right) = \\ &= \left( \prod_{i < j} \frac{i-j}{\sigma(i)-\sigma(j)} \right) \left( \prod_{i < j} \frac{i-j}{\tau(i)-\tau(j)} \right) = \text{sgn}(\sigma)\text{sgn}(\tau). \end{aligned}$$

Resta dunque provata la seguente proposizione.

**PROPOSIZIONE 6.2.15** *Il prodotto di due permutazioni dello stesso segno é pari e quello di segno diverso é dispari.*

**DEFINIZIONE 6.2.16** L'insieme di tutte le permutazioni pari di  $S_n$  costituisce un sottogruppo di  $S_n$ , che si denota con  $A_n$  e si chiama *gruppo alterno* su  $n$  oggetti o di grado  $n$ .

**ESERCIZIO 6.2.17** *Provare che risulta*

$$|A_n| = \frac{1}{2}n!. \quad (6.5)$$

**ESERCIZIO 6.2.18** *Provare che un ciclo é una permutazione pari o dispari a seconda che la sua lunghezza sia rispettivamente dispari o pari.*

**ESERCIZIO 6.2.19** *Provare che, se  $\sigma_1\sigma_2\cdots\sigma_s$  e  $\tau_1\tau_2\cdots\tau_t$  sono due fattorizzazioni in trasposizioni di una stessa permutazione, allora gli interi  $s$  e  $t$  hanno la stessa parit , cio  sono entrambi pari o entrambi dispari.*

### 6.2.3 Gruppi di Permutazioni e Teorema di Cayley

Siano  $X$  un insieme non vuoto (finito o infinito) e  $Symm(X)$  il gruppo di tutte le permutazioni su  $X$ .

**DEFINIZIONE 6.2.20** Un gruppo  $G$  prende il nome *gruppo di permutazioni* su  $X$  se é sottogruppo di  $Symm(X)$ .  $\diamond$

La teoria dei gruppi di permutazioni é equivalente all'intera teoria dei gruppi nel senso precisato dal seguente teorema.

**PROPOSIZIONE 6.2.21 (teorema di Cayley)** *Ogni gruppo  $G$  é isomorfo ad un gruppo di permutazioni sull'insieme degli elementi di  $G$ .*

**DIMOSTRAZIONE.** Per ogni elemento  $g \in G$ , la traslazione destra di ampiezza  $g$

$$\tau_g : x \in G \rightarrow xg \in G$$

é una funzione biunivoca e quindi una permutazione sugli elementi di  $G$ . Si verifica facilmente che l'applicazione

$$\tau : g \in G \rightarrow \tau_g \in S(G)$$

é un monomorfismo di  $G$  in  $S(G)$ . Ne segue che  $G$  é isomorfo a  $\tau(G)$ , cioè l'asserto.  $\diamond$

Figura 6.1: A.Cayley (1821-1895)

### 6.2.4 Il gruppo diedrale di grado $n$

Sia  $\Sigma$  l'insieme dei punti della retta euclidea  $R$  o del piano euclideo  $R^2$ . Una permutazione  $f$  sugli elementi di  $\Sigma$  prende il nome di *isometria* se conserva la distanza euclidea, cioè se verifica la seguente proprietà:

$$d(A, B) = d(f(A), f(B)), \text{ per ogni due punti } A, B \in \Sigma,$$

ove si é denotata con  $d$  la funzione distanza euclidea. Le isometrie di  $\Sigma$  formano un gruppo, che si chiama *gruppo delle isometrie di  $\Sigma$*  e si denota con  $Isom(\Sigma)$ .

Esempi di isometrie del piano euclideo sono: le *rotazioni* intorno ad un punto e le *simmetrie ortogonali*, o *riflessioni*, rispetto alle rette.

Se  $X$  un sottoinsieme non vuoto di  $\Sigma$ , un'isometria  $T$  di  $\Sigma$  che trasformi  $X$  in se stesso, cioè  $T(X) = X$ , si chiama *simmetria* di  $X$ . Le simmetrie di  $X$  costituiscono un sottogruppo del gruppo delle isometrie di  $\Sigma$ , che prende il nome di *gruppo delle simmetrie* di  $X$  e si denota con  $Isom(X)$ .

Sia  $P(n)$  un poligono regolare con  $n \geq 3$  lati. Il gruppo delle simmetrie di  $P(n)$  prende il nome di *gruppo diedrale di grado  $n$*  e si denota con  $D_n$ . Il gruppo  $D_n$  verifica le seguenti proprietà.

- $D_n$  contiene esattamente  $2n$  elementi:

(i) le  $n$  rotazioni  $r_0 = 1, r_1, \dots, r_{n-1}$  intorno al centro di  $P(n)$ , ove  $r_j$  denota la rotazione di ampiezza  $\frac{2\pi}{n}j$ .

(ii) le riflessioni  $s_1, s_2, \dots, s_n$  rispetto agli  $n$  assi di simmetria di  $P(n)$ .

- Se denotiamo con *Rot* una rotazione e con *Rif* una riflessione, risulta

$$Rot Rot = Rot, Rot Rif = Rif, Rif Rot = Rif, Rif Rif = Rot.$$

- Le  $n$  rotazioni formano un sottogruppo di  $D_n$  (*sottogruppo delle rotazioni*).

- $s_j s_j = 1 \Rightarrow s_j = s_j^{-1} \Rightarrow \{1, s_j\}$  é un sottogruppo di  $D_n$ .

- $r_i^n = 1, (s_i s_j)^n = 1, r_i s_j = s_j r_i^{-1}$ .

Nella figura 6.2 sono rappresentate le rotazioni non banali e le riflessioni di un triangolo equilatero.

Figura 6.2: Il gruppo  $D_3$

**ESERCIZIO 6.2.22** *Provare che  $S_3$  e  $D_3$  sono gruppi isomorfi.*

**ESERCIZIO 6.2.23** *Provare che il sottogruppo delle rotazioni di  $D_n$  è ciclico, un suo generatore essendo la rotazione  $r_1$ .*

**ESERCIZIO 6.2.24** *Sia  $P(n)$  un poligono regolare con  $n$  lati e si fissino due assi di simmetria di  $P(n)$  formanti un angolo di  $\frac{\pi}{n}$ . Denotate con  $s$  e  $s'$  le corrispondenti riflessioni del gruppo diedrale  $D_n$ , provare che risulta*

$$D_n = \langle s, s' \rangle .$$

*(Si può provare che ogni gruppo  $G$  generato da due elementi  $a, b$  tali che*

$$a^2 = b^2 = 1 \text{ e } |ab| = n$$

*è isomorfo a  $D_n$ . )*

Se numeriamo ciclicamente in senso orario i vertici del poligono  $P(n)$  con gli interi da 0 ad  $n - 1$ , ogni elemento  $g \in D_n$ , trasformando vertici di  $P(n)$  in vertici di  $P(n)$ , individua una permutazione  $\bar{g}$  dell'insieme  $X = \{0, 1, \dots, n - 1\}$ , cioè un elemento del gruppo  $Symm(X)$ . L'applicazione

$$f : g \in D_n \rightarrow \bar{g} \in Symm(X)$$

è un monomorfismo di gruppi e quindi  $D_n$  è isomorfo al sottogruppo  $f(D_n)$  di  $Symm(X)$ . Abbiamo così che il gruppo diedrale  $D_n$  può essere identificato con un gruppo di permutazioni sui vertici del poligono  $P(n)$ <sup>2</sup>.

**ESERCIZIO 6.2.25** *Provare che il sottogruppo delle rotazioni di  $D_n$  è isomorfo al gruppo additivo degli interi modulo  $n$ .*

**ESERCIZIO 6.2.26** *Provare che il gruppo diedrale  $D_n$  è isomorfo ad un gruppo di permutazioni sui lati del poligono  $P_n$ .*

## 6.2.5 Il gruppo diedrale infinito

Consideriamo il gruppo  $Isom(R)$  delle isometrie della retta reale, che identifichiamo col campo reale  $R$ . Ricordiamo che sono isometrie di  $R$ : le *traslazioni*, e le *riflessioni* intorno ad un punto.

Se poniamo

$$D_\infty = \{f \in Isom(R) : f(Z) = Z\},$$

$D_\infty$  è un sottogruppo di  $Isom(R)$  che si chiama *gruppo diedrale infinito*.

Se, per ogni  $a \in R$ , poniamo

$$t_a = \text{traslazione di ampiezza } a,$$

$$s_a = \text{riflessione rispetto ad } a,$$

risulta

$$D_\infty = \{t_n : n \in Z\} \cup \{s_n : n \in Z\} \cup \{s_{n+\frac{1}{2}} : n \in Z\}.$$

---

<sup>2</sup>Si noti che abbiamo ottenuto una rappresentazione di  $D_n$  come gruppo di permutazioni su un insieme con  $n$  elementi mentre la rappresentazione che si ottiene col teorema di Cayley identifica  $D_n$  con un gruppo di permutazioni su  $2n$  elementi.

**ESERCIZIO 6.2.27** Nel gruppo diedrale infinito  $D_\infty$  consideriamo le riflessioni  $s_0$  e  $s_{\frac{1}{2}}$  di centro 0 e  $\frac{1}{2}$ , rispettivamente. Provare che risulta

$$D_\infty = \langle s_0, s_{\frac{1}{2}} \rangle .$$

(Si può provare che ogni gruppo  $G$  generato da due elementi  $a, b$  tali che

$$a^2 = b^2 = 1 \text{ e } |ab| = \infty$$

è isomorfo a  $D_\infty$ .)

### 6.2.6 Prodotto diretto esterno di gruppi

Siano  $G_1, G_2, \dots, G_n$  gruppi. Nel prodotto cartesiano

$$G = G_1 \times G_2 \times \cdots \times G_n$$

definiamo la seguente operazione

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1b_1, a_2b_2, \dots, a_nb_n),$$

rispetto alla quale  $G$  risulta un gruppo e si ha

$$1 = (1, 1, \dots, 1), \quad (a_1, a_2, \dots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \dots, a_n^{-1}).$$

**DEFINIZIONE 6.2.28** Il gruppo  $G$  si chiama *prodotto diretto esterno* dei gruppi  $G_1, G_2, \dots, G_n$  e si denota con

$$G = G_1 \times G_2 \times \cdots \times G_n.$$

Se i gruppi  $G_1, G_2, \dots, G_n$  sono additivi, anche per  $G$  si usa la notazione additiva e si dice che  $G$  è *somma diretta esterna* di  $G_1, G_2, \dots, G_n$ ; in questo caso si usa la notazione

$$G = G_1 \oplus G_2 \oplus \cdots \oplus G_n.$$

◇

**ESERCIZIO 6.2.29**  $G = G_1 \oplus G_2 \oplus \cdots \oplus G_n$  è abeliano se, e soltanto se,  $G_1, G_2, \dots, G_n$  sono tutti abeliani.

**ESERCIZIO 6.2.30** Scrivere la tabella di Cayley di  $Z_2 \oplus Z_3$ .

**ESERCIZIO 6.2.31** Provare che  $Z_2 \oplus Z_2$  non è isomorfo a  $Z_4$ .

**ESERCIZIO 6.2.32** Sia  $S$  un insieme con due elementi e  $\star$  l'operazione di differenza simmetrica in  $P(S)$ . Provare che il gruppo  $(P(S), \star)$  è isomorfo a  $Z_2 \oplus Z_2$ .

### 6.2.7 Il 4–gruppo di Klein

Sia  $K = \{1, a, b, c\}$  ove é

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, a = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, b = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}, c = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Allora  $K$ , rispetto alla moltiplicazione righe per colonne, é un sottogruppo abeliano di  $GL(2, Q)$  che si chiama *4–gruppo di Klein* o *gruppo quadrimio*.

In  $K$  valgono le seguenti proprietà :

$$a^2 = b^2 = c^2 = 1, \quad ab = c, \quad ac = b, \quad bc = a.$$

Il 4–gruppo di Klein ha la seguente tabella di Cayley.

**TABELLA DI CAYLEY  
DEL 4–GRUPPO DI KLEIN**

$\cdot$	1	$a$	$b$	$c$
1	1	$a$	$b$	$c$
$a$	$a$	1	$c$	$b$
$b$	$b$	$c$	1	$a$
$c$	$c$	$b$	$a$	1

**ESERCIZIO 6.2.33** *Provare che  $K$  é isomorfo al gruppo delle simmetrie di un rettangolo che non sia un quadrato.*

**ESERCIZIO 6.2.34** *Verificare che  $\{1, a\}$ ,  $\{1, b\}$ ,  $\{1, c\}$ , sono gli unici sottogruppi propri e non banali di  $K$  e disegnare il diagramma di Hasse del reticolo dei sottogruppi di  $K$ .*

**ESERCIZIO 6.2.35** *Provare che  $K$  e  $(Z_4, +)$  non sono gruppi isomorfi. Provare, inoltre, che un gruppo finito d'ordine 4 é isomorfo a  $K$  o a  $(Z_4, +)$ .*

### 6.2.8 Il gruppo dei quaternioni

Sia  $Q_2 = \{1, -1, i, -i, j, -j, k, -k\}$  ove é

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

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

Allora  $Q_2$ , rispetto alla moltiplicazione righe per colonne, é un sottogruppo di  $GL(4, Q)$  che si chiama *gruppo dei quaternioni* .

In  $Q_2$  valgono le seguenti proprietà :

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

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

Il gruppo dei quaternioni ha la seguente tabella di Cayley.

**TABELLA DI CAYLEY  
DEL GRUPPO  $Q_2$  DEI QUATERNIONI**

	1	$i$	$-1$	$-i$	$j$	$-k$	$-j$	$k$
1	1	$i$	$-1$	$-i$	$j$	$-k$	$-j$	$k$
$i$	$i$	$-1$	$-i$	1	$k$	$j$	$-k$	$-j$
$-1$	$-1$	$-i$	1	$i$	$-j$	$k$	$j$	$-k$
$-i$	$-i$	1	$i$	$-1$	$-k$	$-j$	$k$	$j$
$j$	$j$	$-k$	$-j$	$k$	$-1$	$-i$	1	$i$
$-k$	$-k$	$-j$	$k$	$j$	$i$	$-1$	$-i$	1
$-j$	$-j$	$k$	$j$	$-k$	1	$i$	$-1$	$-i$
$k$	$k$	$j$	$-k$	$-j$	$-i$	1	$i$	$-1$

**ESERCIZIO 6.2.36** Determinare il periodo di ciascuno degli elementi di  $Q_2$ .

### 6.2.9 L'automorfo di un gruppo

Denotiamo con  $Aut(G)$  l'insieme di tutti gli automorfismi di un gruppo  $G$ . Sappiamo che il prodotto definito da

$$(f, g) \in Aut(G) \times Aut(G) \rightarrow f \circ g \in Aut(G)$$

induce una struttura di gruppo su  $Aut(G)$ . Questo gruppo si chiama *gruppo degli automorfismi di  $G$*  o *automorfo di  $G$* .

**OSSERVAZIONE 6.2.37** La funzione  $a \rightarrow a^n$ , se  $G$  é abeliano, é un automorfismo di  $G$ , per ogni intero  $n \neq 0$ . ◇

**PROPOSIZIONE 6.2.38** La funzione  $a \rightarrow a^{-1}$  é un automorfismo di  $G$  se, e soltanto se,  $G$  é abeliano.

**DIMOSTRAZIONE.** Se la nostra funzione é un automorfismo, per ogni  $a, b \in G$ , abbiamo

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

◇

**ESERCIZIO 6.2.39** Provare che un gruppo  $G$  é abeliano se, e solo se, l' applicazione

$$a \in G \rightarrow a^2 \in G$$

é un endomorfismo di  $G$ .

6.2.10 Tabella riassuntiva di gruppi

PROPRIETA' DI ALCUNI GRUPPI

Gruppo	Operazione	Forma degli elementi	Elemento neutro	Inverso	Abeliano
$Z$	addizione	$n$	0	$-n$	si
$Q^+$	moltiplicazione	$m/n$ $m, n > 0$	1	$n/m$	si
$Z_m$	addizione modulo $m$	$n$	0	$m - n$	si
$R^*$	moltiplicazione	$a$	1	$1/a$	si
$S_n$	composizione	$\begin{pmatrix} 1 & \dots & n \\ i_1 & \dots & i_n \end{pmatrix}$	$\begin{pmatrix} 1 & \dots & n \\ 1 & \dots & n \end{pmatrix}$	$\begin{pmatrix} i_1 & \dots & i_n \\ 1 & \dots & n \end{pmatrix}$	no per $n > 2$
$GL(2, R)$	moltiplicazione	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $ad - bc \neq 0$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$	no
$SL(2, R)$	moltiplicazione	$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $ad - bc = 1$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$	no
$U(m)$	moltiplicazione modulo $m$	$n$ $MCD(n, m) = 1$	1	soluzione di $nx \equiv 1(mod m)$	si
$R^n$	addizione vettoriale	$(a_1, \dots, a_n)$	$(0, \dots, 0)$	$(-a_1, \dots, -a_n)$	si
$D_n$	composizione	$r_j, s$	$r_0$	$r_{n-j}, s$	no

6.3 Lateralì di un sottogruppo e teorema di Lagrange

Siano  $G$  un gruppo e  $H$  un suo sottogruppo.

DEFINIZIONE 6.3.1 Le due relazioni  $\mathcal{R}'_H$  e  $\mathcal{R}''_H$  sugli elementi di  $G$  definite da

$$a, b \in G, a\mathcal{R}'_H b \Leftrightarrow a^{-1}b \in H, \tag{6.6}$$

$$a, b \in G, a\mathcal{R}''_H b \Leftrightarrow ab^{-1} \in H, \tag{6.7}$$

si chiamano *congruenze*, rispettivamente *sinistra* e *destra*, *modulo H* ed é un esercizio provare che risultano d'equivalenza.  $\diamond$

**OSSERVAZIONE 6.3.2** Nel caso  $G$  sia un gruppo additivo, le relazioni  $\mathfrak{R}'_H$  e  $\mathfrak{R}''_H$  sono definite rispettivamente da

$$a, b \in G, a\mathfrak{R}'_H b \Leftrightarrow -a + b \in H$$

e

$$a, b \in G, a\mathfrak{R}''_H b \Leftrightarrow a - b \in H.$$

◇

**OSSERVAZIONE 6.3.3** Se  $G$  é abeliano, le relazioni  $\mathfrak{R}'_H$  e  $\mathfrak{R}''_H$  coincidono. ◇

**DEFINIZIONE 6.3.4** La classe di  $\mathfrak{R}'_H$ -equivalenza di un elemento  $a$ , che si vede facilmente essere data da

$$[a]_{\mathfrak{R}'_H} = aH = \{ah : h \in H\}, \quad (6.8)$$

si chiama *laterale sinistro di  $H$  in  $G$  relativo ad  $a$* .

La classe di  $\mathfrak{R}''_H$ -equivalenza di un elemento  $a$ , data da

$$[a]_{\mathfrak{R}''_H} = Ha = \{ha : h \in H\}, \quad (6.9)$$

si chiama *laterale destro di  $H$  in  $G$  relativo ad  $a$* . ◇

**OSSERVAZIONE 6.3.5** Osserviamo che  $H$  stesso é un suo laterale sinistro, essendo  $[1]_{\mathfrak{R}'_H} = 1H = H$ . Analogamente  $H$  é un suo laterale destro, essendo  $[1]_{\mathfrak{R}''_H} = H1 = H$ . ◇

**OSSERVAZIONE 6.3.6** I laterali sinistri (risp. destri) di  $H$  in  $G$  formano una partizione degli elementi di  $G$ . ◇

**OSSERVAZIONE 6.3.7** Nel caso  $G$  sia un gruppo additivo, le (6.8) e (6.9) si scrivono rispettivamente

$$[a]_{\mathfrak{R}'_H} = a + H = \{a + h : h \in H\}$$

e

$$[a]_{\mathfrak{R}''_H} = H + a = \{h + a : h \in H\}.$$

◇

**ESEMPIO 6.3.8** Con riferimento alla notazione usata nell'esempio 6.2.3, consideriamo il sottogruppo  $H = \{1, s_1\}$  di  $S_3$ . I laterali sinistri di  $H$  in  $S_3$  sono:

$$1H = s_1H = H, \quad r_1H = s_2H = \{r_1, s_2\}, \quad r_2H = s_3H = \{r_2, s_2\}.$$

I laterali destri di  $H$  in  $S_3$  sono:

$$H1 = Hs_1 = H, \quad Hr_1 = Hs_3 = \{r_1, s_3\}, \quad Hr_2 = Hs_2 = \{r_2, s_2\}.$$

Si noti che i laterali sinistri di  $H$  definiscono una partizione sugli elementi di  $S_3$  diversa da quella individuata dai laterali destri di  $H$ . ◇

**ESEMPIO 6.3.9** Nel gruppo additivo degli interi  $(Z, +)$  si consideri il sottogruppo  $H = mZ$ , con  $m$  intero maggiore di 1. Allora le relazioni  $\mathfrak{R}'_H$  e  $\mathfrak{R}''_H$  coincidono con la congruenza modulo  $m$ .  $\diamond$

**ESERCIZIO 6.3.10** Siano  $H, K$  due sottogruppi di un gruppo  $G$ . Provare che

$$aH \cap aK = a(H \cap K) \quad e \quad Ha \cap Ka = (H \cap K)a,$$

per ogni elemento  $a \in G$ .

**PROPOSIZIONE 6.3.11** Per ogni  $a \in G$ , le funzioni (traslazioni ristrette ad  $H$ )

$$h \in H \rightarrow ah \in aH \quad e \quad h \in H \rightarrow ha \in Ha$$

sono biunivoche, ne segue che  $|H| = |aH| = |Ha|$ .

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

**PROPOSIZIONE 6.3.12** Gli insiemi quoziente  $G/\mathfrak{R}'_H$  e  $G/\mathfrak{R}''_H$ , cioé gli insiemi dei laterali di  $H$  rispettivamente sinistri e destri, sono equipotenti.

**DIMOSTRAZIONE.** Osserviamo che risulta:

$$\begin{aligned} aH = bH &\Leftrightarrow a \equiv b \pmod{\mathfrak{R}'_H} \Leftrightarrow a^{-1}b \in H \\ \Leftrightarrow a^{-1}b = (a^{-1})(b^{-1})^{-1} \in H &\Leftrightarrow a^{-1} \equiv b^{-1} \pmod{\mathfrak{R}''_H} \Leftrightarrow Ha^{-1} = Hb^{-1}. \end{aligned}$$

Ne segue che é ben definita la funzione

$$aH \in G/\mathfrak{R}'_H \rightarrow Ha^{-1} \in G/\mathfrak{R}''_H,$$

la quale é biunivoca.  $\diamond$

**DEFINIZIONE 6.3.13** Se l'insieme quoziente  $G/\mathfrak{R}'_H$  (o equivalentemente  $G/\mathfrak{R}''_H$ ) é finito ed ha ordine  $n$ , l'intero  $n$  si chiama *indice di  $H$  in  $G$*  e si denota con  $|G : H|$  o con  $[G : H]$ . Se  $G/\mathfrak{R}'_H$  (o equivalentemente  $G/\mathfrak{R}''_H$ ) é infinito, si dice che  $H$  ha *indice infinito in  $G$* .  $\diamond$

Osserviamo che risulta  $|G : G| = 1$  e che  $|G : 1|$  é uguale a  $|G|$  se  $G$  é finito ed é infinito se  $G$  é infinito.

**ESERCIZIO 6.3.14** Siano  $A$  un campo e  $f(x_1, x_2, \dots, x_n)$  un polinomio in  $n$  indeterminate a coefficienti in  $A$ . Detto  $G_f$  il gruppo delle simmetrie di  $f$ , provare che il numero dei polinomi distinti del tipo

$$f(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) \quad \text{con } \sigma \in S_n$$

é uguale all'indice di  $G_f$  in  $S_n$ <sup>3</sup>.

<sup>3</sup>Questo problema é legato allo studio delle equazioni algebriche risolubili *per radicali* ed é proprio in quest'ambito che é nato il concetto di *gruppo*.

**TEOREMA 6.3.15 (teorema di Lagrange)** *Se  $G$  é un gruppo finito e  $H$  un suo sottogruppo, allora*

$$|G : H| = \frac{|G|}{|H|} \quad (6.10)$$

*e quindi  $|H|$  é un divisore di  $|G|$ .*

**DIMOSTRAZIONE.** Nelle nostre ipotesi, i laterali sinistri di  $H$  formano una partizione di  $G$  in blocchi aventi tutti lo stesso ordine  $|H|$ . Da questa osservazione segue subito l'asserto.  $\diamond$

**OSSERVAZIONE 6.3.16** Il teorema di Lagrange dice che l'ordine di un sottogruppo di un gruppo finito  $G$  é un divisore dell'ordine di  $G$  ma, si faccia bene attenzione, non garantisce che un divisore positivo di  $|G|$  é l'ordine di un sottogruppo di  $G$ . Quest'ultima affermazione é in generale falsa, come mostra l'esercizio 9.1.9. Essa é, però, vera per il gruppo additivo  $(\mathbb{Z}_n, +)$  degli interi modulo  $n$  (cfr.6.1.33) e, come vedremo, per alcune classi speciali di gruppi.  $\diamond$

Figura 6.3: J.L.Lagrange (1736-1813)

**ESERCIZIO 6.3.17** *Provare che ogni gruppo finito d'ordine primo é ciclico.*

**ESERCIZIO 6.3.18** *Provare che un gruppo finito d'ordine dispari non possiede elementi d'ordine pari.*

**PROPOSIZIONE 6.3.19** *Se  $G$  é finito d'ordine  $m$ , allora il periodo di ogni elemento di  $G$  divide  $m$ . Inoltre risulta  $a^m = 1$ , per ogni  $a \in G$ .*

**DIMOSTRAZIONE.** Se  $a \in G$ , deve essere  $|\langle a \rangle| = n \leq m$  e, per il teorema di Lagrange,  $m$  é del tipo  $m = nq$ . La restante parte segue dalla prop.5.6.12.  $\diamond$

**ESERCIZIO 6.3.20** *Determinare tutti i sottogruppi del gruppo  $Q_2$  dei quaternioni (cfr. par. 6.2.8).*

## 6.4 Esercizi

**6.4.1** Posto  $G = \{(a, b) \in \mathbb{R}^2 : a \neq 0, a + b \neq 0\}$ , si consideri la seguente operazione "o" su  $G$ :

$$(a, b) \circ (c, d) = (ac, (a + b)(c + d) - ac).$$

Provare che  $(G, \circ)$  é un gruppo e che  $H = \{(1, a) : a > -1\}$  é un suo sottogruppo.

**6.4.2** Provare che  $U(10) = \{1, 3, 7, 9\}$  e che  $\langle 3 \rangle = U(10)$ .

**6.4.3** Provare che in  $(\mathbb{Z}_{10}, +)$  risulta  $\langle 2 \rangle = \{0, 2, 4, 6, 8\}$ .

**6.4.4** Provare che in  $(\mathbb{Z}, +)$  risulta  $\langle -1 \rangle = \mathbb{Z}$ .

**6.4.5** Determinare gli interi  $n$  per cui  $(\mathbb{Z}_n^*, \cdot)$  é un gruppo.

**6.4.6** Si considerino i seguenti gruppi:  $(\mathbb{Z}_{12}, +)$ ,  $U(10)$ ,  $U(12)$ . Per ognuno di essi se ne determini l'ordine e si calcoli l'ordine di ciascuno dei suoi elementi.

**6.4.7** Determinare i possibili ordini di un gruppo ciclico avente un unico generatore.

**6.4.8** Siano  $G$  un gruppo,  $H$  un sottogruppo di  $G$ ,  $a$  un elemento di  $G$  di periodo finito  $n$  ed  $m$  un intero positivo coprimo con  $n$ . Usando l'identitá di Bézout (*cf.* 2.3.10), nell'ipotesi che  $a^m$  appartiene ad  $H$ , provare che anche  $a$  appartiene ad  $H$ .

**6.4.9** Provare che  $U(14) = \langle 3 \rangle = \langle 5 \rangle$ .

**6.4.10** Provare che il gruppo  $U(20)$  non é ciclico.

**6.4.11** Nel gruppo  $SL(2, \mathbb{R})$  trovare l'ordine dei seguenti elementi:

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad AB.$$

**6.4.12** Trovare l'ordine di

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

in  $SL(2, \mathbb{R})$ .

**6.4.13** Provare che

$$G = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}$$

é un sottogruppo ciclico infinito di  $SL(2, \mathbb{R})$ .

**6.4.14** Trovare tutti gli elementi dei sottogruppi  $\langle 10 \rangle$  e  $\langle 20 \rangle$  del gruppo additivo  $\mathbb{Z}_{30}$ .

**6.4.15** Trovare tutti gli elementi dei sottogruppi  $\langle 3 \rangle$  e  $\langle 7 \rangle$  del gruppo  $U(20)$ .

**6.4.16** Sull'insieme  $S = R^* \times R$ , si definisca la seguente operazione "o":

$$(a, b) \circ (c, d) = (ac, bc + d).$$

Provare che  $(S, \circ)$  é un gruppo non abeliano e che i suoi elementi di periodo 2 sono tutti e soli quelli del tipo  $(-1, d)$ ,  $d \in R$ . Provare, inoltre, che il gruppo non contiene elementi di periodo 3.

**6.4.17** Dimostrare che un gruppo privo di sottogruppi non banali é necessariamente ciclico.

**6.4.18** Provare che in un gruppo abeliano  $G$  tutti gli elementi di periodo finito costituiscono un sottogruppo (il *sottogruppo di torsione* di  $G$ ). E' vera questa proprietá in un gruppo non abeliano?

**6.4.19** Siano  $G$  un gruppo e  $a$  un suo elemento. Provare che l'insieme di tutti gli elementi di  $G$  permutabili con  $a$  formano un sottogruppo di  $G$ . Tale sottogruppo si chiama *centralizzante di  $a$  in  $G$*  e si denota con  $C_G(a)$ . Provare, inoltre che

$$a \in Z(G) \Leftrightarrow C_G(a) = G, \quad Z(G) = \bigcap_{a \in G} C_G(a).$$

**6.4.20** Si consideri la seguente relazione  $C_G$  tra gli elementi di un gruppo  $G$  :

$$aC_G b \Leftrightarrow \text{esiste } x \in G \text{ tale che } a = x^{-1}bx.$$

Provare che  $C_G$  é una relazione d'equivalenza; essa prende il nome di *coniugio tra gli elementi di  $G$* . Le classi di  $C_G$ -equivalenza si chiamano *classi di coniugio* degli elementi di  $G$  e, se  $a \in G$ , la classe di coniugio di  $a$  si denota con  $[a]_{C_G}$  oppure con  $cl(a)$ . Due elementi di  $G$  equivalenti rispetto alla relazione di coniugio si dicono *coniugati* e, se  $a, x \in G$ , l'elemento  $x^{-1}ax$  si chiama *coniugato di  $a$  mediante  $x$*  e si denota con  $a^x$ . Provare che valgono le seguenti due proprietá:

$$cl(a) = \{x^{-1}ax : x \in G\}, \quad a \in Z(G) \Leftrightarrow cl(a) = \{a\}.$$

**6.4.21** Sia  $H$  un sottogruppo di un gruppo  $G$  e, per ogni  $a \in G$ , si ponga

$$H^a = a^{-1}Ha = \{a^{-1}ha : h \in H\}.$$

Provare che  $H^a$  é un sottogruppo di  $G$ . Tale sottogruppo si chiama *coniugato di  $H$  mediante  $a$* .

**6.4.22** Provare che nell'insieme  $L(G)$  di tutti i sottogruppi di un gruppo  $G$ , la relazione  $\Gamma_G$  definita da

$$H\Gamma_G K \Leftrightarrow H = x^{-1}Kx, \text{ per qualche } x \in G$$

é di equivalenza; essa prende il nome di *coniugio tra i sottogruppi di  $G$* . Le classi di  $\Gamma_G$ -equivalenza si chiamano *classi di coniugio* dei sottogruppi di  $G$  e la classe di coniugio di un sottogruppo  $H$  di  $G$  si denota con  $[H]_{\Gamma_G}$  oppure con  $cl(H)$ . Due sottogruppi di  $G$  equivalenti rispetto alla relazione di coniugio si dicono *coniugati*.

**6.4.23** Sia  $G$  un gruppo. Per ogni due elementi  $a, b$  di  $G$  si chiama *commutatore* della coppia  $(a, b)$  l'elemento  $[a, b]$  di  $G$  definito da

$$[a, b] = a^{-1}b^{-1}ab.$$

Provare che, per ogni  $a, b, c \in G$ , valgono le seguenti proprietà:

- $[a, b] = 1 \Leftrightarrow ab = ba$ ;
- $ab = ba[a, b]$ ;  $[a, b]^{-1} = [b, a]$ ;
- $[ab, c] = b^{-1}[a, c]b[b, c]$ ;  $[a, bc] = [a, c]c^{-1}[a, b]c$ ;
- $[a^{-1}, b] = (a[a, b]a^{-1})^{-1}$ ;  $[a, b^{-1}] = (b[a, b]b^{-1})^{-1}$ .

**6.4.24** Siano  $G$  un gruppo abeliano e  $H = \{a \in G : a^2 = 1\}$ . Provare che  $H$  è un sottogruppo di  $G$ .

**6.4.25** Siano  $G$  un gruppo abeliano e  $H$  l'insieme dei quadrati di  $G$ , cioè  $H = \{a^2 : a \in G\}$ . Provare che  $H$  è un sottogruppo di  $G$ .

**6.4.26** Sia  $R^*$  il gruppo moltiplicativo dei numeri reali e siano  $H$  e  $K$  i seguenti sottoinsiemi di  $R^*$  :

$$H = (R \setminus Q) \cup \{1\}, \quad K = \{a \in R^* : a \geq 1\}.$$

Provare che  $H$  e  $K$  non sono sottogruppi di  $R^*$ .

**6.4.27** In  $M_2(\mathbb{Z})$  si consideri il sottoinsieme

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + b + c + d = 0 \right\}.$$

Provare che  $H$  è un sottogruppo di  $(M_2(\mathbb{Z}), +)$ .

**6.4.28** In  $M_2(\mathbb{Z})$  si consideri il sottoinsieme

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a + b + c + d = 1 \right\}.$$

Verificare se  $H$  è un sottogruppo di  $(M_2(\mathbb{Z}), +)$ .

**6.4.29** Sia  $H$  un sottogruppo additivo di  $R$  e si ponga  $K = \{2^a : a \in H\}$ . Provare che  $K$  è un sottogruppo moltiplicativo di  $R^*$ .

**6.4.30** Provare che i sottogruppi di un gruppo  $G$ , rispetto alla relazione di inclusione, formano un reticolo (il *reticolo dei sottogruppi* di  $G$ ).

**6.4.31** Si considerino le seguenti funzioni di  $R$  in  $R$

$$f_1(x) = x + 1, \quad f_2(x) = x|x|$$

e si stabilisca se sono omomorfismi di  $(R, +)$  in  $(R, \cdot)$ .

**6.4.32** Siano  $G$  il gruppo additivo dei numeri reali e  $G'$  il gruppo moltiplicativo dei numeri reali positivi. Provare che l'applicazione

$$x \in G \rightarrow 2^x \in G'$$

é un isomorfismo fra  $G$  e  $G'$ .

**6.4.33** Verificare se la funzione  $f(x) = x^3$  é un automorfismo del gruppo additivo dei numeri reali.

**6.4.34** Provare che, a meno di isomorfismi, esistono un solo gruppo di ordine 2, un solo gruppo di ordine 3 e due gruppi di ordine 4.

**6.4.35** Provare che i gruppi  $Z_4$ ,  $U(5)$  e  $U(10)$  sono isomorfi.

**6.4.36** Si ponga

$$H = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \text{ e } K = \left\{ \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} : a, b \in \mathbb{Q} \right\}.$$

Provare che  $H$  e  $K$ , rispetto all'operazione di addizione, sono due gruppi isomorfi.

**6.4.37** Provare che l'insieme

$$G = \left\{ \begin{pmatrix} 1-n & -n \\ n & 1+n \end{pmatrix} : n \in \mathbb{Z} \right\},$$

rispetto al prodotto righe per colonne, é un gruppo abeliano isomorfo a  $(\mathbb{Z}, +)$ .

**6.4.38** Provare che l'insieme

$$G = \left\{ \begin{pmatrix} 1-2n & n \\ -4n & 1+2n \end{pmatrix} : n \in \mathbb{Z} \right\},$$

rispetto al prodotto righe per colonne, é un gruppo abeliano isomorfo a  $(\mathbb{Z}, +)$ .

**6.4.39** Verificare che la funzione  $f(a + ib) = a - ib$  é un automorfismo del gruppo additivo e di quello moltiplicativo dei numeri complessi.

**6.4.40** Provare che i gruppi  $(\mathbb{Z}, +)$  e  $(2\mathbb{Z}, +)$  sono isomorfi. Stabilire inoltre se sono isomorfi gli anelli  $(\mathbb{Z}, +, \cdot)$  e  $(2\mathbb{Z}, +, \cdot)$ .

**6.4.41** Calcolare il numero dei cicli di lunghezza  $n$  in  $S_n$ .

**6.4.42** Dire se le permutazioni  $(1, 3, 5)(2, 4, 5)$  e  $(1, 4)(2, 5)(3, 6)$  sono elementi permutabili di  $S_6$ .

**6.4.43** Calcolare il periodo e le inverse di ciascuna delle seguenti permutazioni:

$$(1, 3, 5)(2, 4, 5), (2, 4, 5)(1, 3, 5), (1, 4)(2, 5)(3, 6), (1, 7, 9, 8)(2, 1, 5, 8, 7).$$

**6.4.44** Fattorizzare in cicli disgiunti e calcolare le inverse delle seguenti permutazioni:

$$\left[ \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 1 & 7 & 5 & 8 & 4 & 9 & 10 & 6 \end{array} \right], \left[ \begin{array}{cccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 4 & 9 & 1 & 8 & 7 & 6 & 3 & 5 & 2 \end{array} \right].$$

**6.4.45** Calcolare il numero delle trasposizioni di  $S_n$ .

**6.4.46** Fattorizzare in trasposizioni e trovare il segno di ciascuna delle seguenti permutazioni:

$$(1, 3, 5, 7)(6, 8, 2, 4), (6, 7, 8)(5, 3, 1), (1, 4, 7, 9)(2, 3, 6, 8).$$

**6.4.47** Consideriamo la prima tabella delle due seguenti, formata da 15 quadrati numerati e da uno spazio libero.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

Supponiamo che i quadrati numerati possano scorrere orizzontalmente e verticalmente usando lo spazio libero senza fuoriuscire dalla tabella stessa. Provare che, muovendo i quadrati nel modo anzidetto, non é possibile trasformare la prima tabella nella seconda.

**6.4.48** Sia  $G$  un sottogruppo di  $S_n$ . Provare che, se  $G$  non é un sottogruppo di  $A_n$ , allora metà dei suoi elementi sono permutazioni pari e metà dispari.

**6.4.49** Nel gruppo additivo  $Z_5$  degli interi modulo 5 si consideri la seguente funzione

$$\sigma : n \in Z_5 \rightarrow 2n \in Z_5.$$

Provare che  $\sigma$  é una permutazione sugli elementi di  $Z_5$ , determinare il gruppo ciclico  $G$  generato da  $\sigma$  e descrivere le orbite di  $G$  sugli elementi di  $Z_5$ .

**6.4.50** Provare che, per ogni intero  $n > 1$ , il gruppo  $Isom(R^2)$  contiene un sottogruppo ciclico finito d'ordine  $n$ .

**6.4.51** Provare che, per ogni intero  $n > 1$ , il gruppo  $SO(2)$  contiene un elemento di periodo  $n$ .

**6.4.52** Sia  $G$  il gruppo delle simmetrie di una circonferenza. Provare che, per ogni intero positivo  $n$ ,  $G$  contiene almeno un elemento d'ordine  $n$ . Provare inoltre che  $G$  contiene elementi d'ordine infinito.

**6.4.53** Sia  $G$  il gruppo delle simmetrie di una circonferenza. Dire se  $G$  può essere pensato come un gruppo di permutazioni sui punti della circonferenza e, in caso di risposta affermativa, verificare se  $G$  è transitivo su tali punti.

**6.4.54** Sia  $G$  un sottogruppo di un gruppo diedrale finito e, per ogni  $\sigma \in G$ , si ponga

$$\text{sgn}(\sigma) = \begin{cases} +1 & \text{se } \sigma \text{ è una rotazione,} \\ -1 & \text{se } \sigma \text{ è una riflessione.} \end{cases}$$

Provare che l'applicazione  $\text{sgn}$  è un omomorfismo di  $G$  in  $(\{+1, -1\}, \cdot)$ .

**6.4.55** Sia  $G$  un sottogruppo del gruppo diedrale infinito e, per ogni  $\sigma \in G$ , si ponga

$$\text{sgn}(\sigma) = \begin{cases} +1 & \text{se } \sigma \text{ è una traslazione,} \\ -1 & \text{se } \sigma \text{ è una riflessione.} \end{cases}$$

Provare che l'applicazione  $\text{sgn}$  è un omomorfismo di  $G$  in  $(\{+1, -1\}, \cdot)$ .

**6.4.56** Provare che i gruppi  $S_4$  e  $D_{12}$  non sono isomorfi.

**6.4.57** Provare che il gruppo  $Q_2$  dei quaternioni non è isomorfo al gruppo  $D_4$ .

**6.4.58** Sia  $n$  un intero maggiore di 2. Provare che nel gruppo ortogonale  $O(2)$  il sottogruppo generato dalle due matrici

$$\begin{pmatrix} \cos \frac{2\pi}{n} & \text{sen} \frac{2\pi}{n} \\ -\text{sen} \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

è isomorfo al gruppo diedrale  $D_n$ .

**6.4.59** Descrivere il gruppo delle simmetrie di un rettangolo.

**6.4.60** Determinare esempi di figure geometriche i cui gruppi di simmetrie sono rispettivamente isomorfi ai gruppi additivi di  $Z_2$  e  $Z_3$ , ad  $S_3$  ed al 4-gruppo di Klein.

**6.4.61** Provare che il gruppo diedrale  $D_n$  è isomorfo al sottogruppo di  $GL(2, C)$  generato dalle due matrici

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ e } \begin{bmatrix} e^{\frac{2\pi i}{n}} & 0 \\ 0 & e^{-\frac{2\pi i}{n}} \end{bmatrix}.$$

**6.4.62** Provare che l'insieme di matrici

$$\left\{ \begin{bmatrix} \epsilon & n \\ 0 & 1 \end{bmatrix} : \epsilon = \pm 1, n \in Z \right\}$$

è un sottogruppo di  $GL(2, Z)$  isomorfo al gruppo diedrale  $D_\infty$ .

**6.4.63** Provare che la seguente tabella di moltiplicazione definisce un gruppo isomorfo al gruppo  $Q_2$  dei quaternioni

	$e$	$a$	$a^2$	$a^3$	$b$	$ba$	$ba^2$	$ba^3$
$e$	$e$	$a$	$a^2$	$a^3$	$b$	$ba$	$ba^2$	$ba^3$
$a$	$a$	$a^2$	$a^3$	$e$	$ba^3$	$b$	$ba$	$ba^2$
$a^2$	$a^2$	$a^3$	$e$	$a$	$ba^2$	$ba^3$	$b$	$ba$
$a^3$	$a^3$	$e$	$a$	$a^2$	$ba$	$ba^2$	$ba^3$	$b$
$b$	$b$	$ba$	$ba^2$	$ba^3$	$a^2$	$a^3$	$e$	$a$
$ba$	$ba$	$ba^2$	$ba^3$	$b$	$a$	$a^2$	$a^3$	$e$
$ba^2$	$ba^2$	$ba^3$	$b$	$ba$	$e$	$a$	$a^2$	$a^3$
$ba^3$	$ba^3$	$b$	$ba$	$ba^2$	$a^3$	$e$	$a$	$a^2$