

# **Appunti sulla teoria elementare dei gruppi**

Andrea Loi



# Indice

<b>1</b>	<b>Semigrussi, monoidi e gruppi</b>	<b>1</b>
1.1	Semigrussi . . . . .	1
1.2	Monoidi . . . . .	6
1.3	Gruppi . . . . .	9
1.3.1	Alcuni esempi di gruppi . . . . .	11
1.3.2	La legge di cancellazione in un gruppo . . . . .	16
1.3.3	Potenze, il commutatore e l'ordine di un elemento . . . . .	17
1.4	Esercizi . . . . .	23
<b>2</b>	<b>Due gruppi importanti: <math>D_n</math> e <math>S_n</math></b>	<b>27</b>
2.1	Il gruppo diedrale . . . . .	27
2.2	Il gruppo delle permutazioni . . . . .	35
2.3	I cicli e il teorema fondamentale delle permutazioni . . . . .	37
2.4	Il segno di una permutazione . . . . .	43
2.5	Esercizi . . . . .	48
<b>3</b>	<b>Sottogruppi e classi laterali</b>	<b>51</b>
3.1	Sottogruppi . . . . .	51
3.2	Intersezione di sottogruppi . . . . .	54
3.3	Unione di sottogruppi . . . . .	58
3.4	Prodotto di sottogruppi . . . . .	60
3.5	Classi laterali e il teorema di Lagrange . . . . .	64
3.5.1	Ordine del prodotto di due elementi . . . . .	70
3.6	Esercizi . . . . .	72
<b>4</b>	<b>Sottogruppi normali e quozienti</b>	<b>75</b>
4.1	Sottogruppi normali . . . . .	75
4.2	Centro di un gruppo e gruppi semplici . . . . .	77
4.3	Operazioni con i sottogruppi normali . . . . .	78

4.4	Sottogruppi del gruppo lineare . . . . .	79
4.5	Quozienti . . . . .	84
4.6	Esercizi . . . . .	85
<b>5</b>	<b>Omomorfismi e isomorfismi</b>	<b>87</b>
5.1	Omomorfismi ed isomorfismi . . . . .	87
5.2	Gruppo degli automorfismi di un gruppo . . . . .	97
5.3	Il teorema di Cayley . . . . .	100
5.4	Esercizi . . . . .	101
<b>6</b>	<b>Prodotto diretto di gruppi</b>	<b>105</b>
6.1	Prodotto diretto di Gruppi . . . . .	105
6.2	Classificazione di alcuni gruppi finiti . . . . .	110
6.3	Sottogruppi del prodotto diretto di due gruppi . . . . .	113
6.4	Automorfismi del prodotto diretto di due gruppi . . . . .	114
6.5	Esercizi . . . . .	117
<b>7</b>	<b>Gruppi abeliani finiti</b>	<b>121</b>
7.1	Classificazione dei gruppi ciclici e dei loro sottogruppi . . . . .	121
7.2	Prodotti diretti di gruppi ciclici . . . . .	124
7.3	Il gruppo degli automorfismi di un gruppo ciclico . . . . .	125
7.4	Il Lemma e il Teorema di Gauss . . . . .	127
7.5	Il teorema di Frobenius-Stickelberger . . . . .	131
7.6	Esercizi . . . . .	136
	<b>Bibliografia</b>	<b>139</b>

# Capitolo 1

## Semigrupperi, monoidi e gruppi

### 1.1 Semigrupperi

Sia  $X$  un insieme diverso dal vuoto. Un'operazione binaria  $\cdot$  su  $X$  è un'applicazione

$$\cdot : X \times X \rightarrow X, (x, y) \mapsto x \cdot y.$$

Diremo che un'operazione binaria  $\cdot$  su un insieme  $X$  è associativa se

$$(x \cdot y) \cdot z = x \cdot (y \cdot z), \forall x, y, z \in X.$$

**Osservazione 1.1.1** Indicheremo con  $xy$  il prodotto  $x \cdot y$  tra due elementi  $x, y$  quando l'operazione binaria  $\cdot$  sarà chiara dal contesto. Inoltre se vale la proprietà associativa, dati tre elementi  $x, y, z$  potremo scrivere senza ambiguità  $xyz$  per indicare  $(xy)z = x(yz)$

**Definizione 1.1.2** Un semigruppero è una coppia  $(S, \cdot)$ , dove  $S \neq \emptyset$  e  $\cdot$  è un'operazione binaria su  $S$  associativa.

Dato un semigruppero  $(S, \cdot)$  diremo che  $S$  è il *supporto* del semigruppero  $(S, \cdot)$  e indicheremo la sua cardinalità con  $|S|$ . A volte chiameremo  $|S|$  l'*ordine* del semigruppero  $(S, \cdot)$ . Diremo anche che un semigruppero è *finito* (risp. *infinito*) se il suo ordine è finito (risp. infinito).

Un'operazione binaria su un insieme  $X \neq \emptyset$  è detta *commutativa* se

$$x \cdot y = y \cdot x, \forall x, y \in X.$$

Un semigruppero  $(S, \cdot)$  nel quale l'operazione binaria  $\cdot$  è commutativa verrà chiamato *semigruppero abeliano* o *commutativo*.

**Esempio 1.1.3** Le coppie  $(S, +)$  dove  $S = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ , dove  $+$  è la somma usuale sono semigrupp abeliani infiniti.

**Esempio 1.1.4** Le coppie  $(S^+, +)$  dove  $S^+ = \mathbb{N}^+, \mathbb{Z}^+, \mathbb{Q}^+, \mathbb{R}^+$  sono semigrupp abeliani infiniti. In quest'esempio  $S^+ = \{x \in S \mid x > 0\}$ .

**Esempio 1.1.5** Le coppie  $(S, \cdot)$  dove  $S = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ , dove  $\cdot$  è la moltiplicazione usuale sono semigrupp abeliani infiniti.

**Esempio 1.1.6** Le coppie  $(S, \cdot)$  dove  $S = \mathbb{N}^*, \mathbb{Z}^*, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$  sono semigrupp abeliani infiniti. In queste note indicheremo con  $S^* = S \setminus \{0\}$  se  $S$  è un insieme numerico contenente 0 (si noti che  $\mathbb{N}^+ = \mathbb{N}^*$ ).

**Esempio 1.1.7** Sia  $P$  l'insieme dei numeri interi pari allora  $(P, +)$ ,  $(P^+, +)$ ,  $(P, \cdot)$ , e  $(P^*, \cdot)$  sono semigrupp abeliani infiniti, dove la somma e la moltiplicazione sono quelle usuali.

**Esempio 1.1.8** Sia  $m \geq 2$  un numero naturale allora  $(\mathbb{Z}_m, +)$  e  $(\mathbb{Z}_m, \cdot)$  con le operazioni definite sulle classi modulo  $m$  come

$$[x]_m + [y]_m = [x + y]_m \quad (1.1)$$

e

$$[x]_m \cdot [y]_m = [xy]_m \quad (1.2)$$

sono semigrupp abeliani di ordine  $m$ .

**Esempio 1.1.9** Sia  $P(X)$  l'insieme delle parti di un insieme  $X \neq \emptyset$ . Sia  $\cup$  (risp.  $\cap$ ) l'operazione binaria su  $P(X)$  che a due elementi  $A, B \in P(X)$  ( $A, B \subset X$ ) associa la loro unione (risp. intersezione)  $A \cup B$  (risp.  $A \cap B$ ). Allora  $(P(X), \cup)$  (risp.  $(P(X), \cap)$ ) è un semigrupp abeliano. L'ordine di  $P(X)$  è finito se e solo se  $X$  ha cardinalità finita.

**Esempio 1.1.10** Sia  $X$  un insieme,  $X \neq \emptyset$ . Definiamo un'operazione binaria  $\cdot$  su  $X$  come

$$x \cdot y = x, \forall x, y \in X. \quad (1.3)$$

Si verifica immediatamente che  $(X, \cdot)$  è un semigrupp. non abeliano se  $X$  ha almeno due elementi. Analogamente possiamo definire su  $X$  l'operazione binaria

$$x \cdot y = y, \forall x, y \in X. \quad (1.4)$$

**Esempio 1.1.11** Sia  $X$  un insieme,  $X \neq \emptyset$ . Consideriamo l'insieme  $S = X^X$  costituito da tutte le applicazioni da  $X$  in se stesso con operazione binaria

$$f \circ g, \forall f, g \in S,$$

dove  $\circ$  denota la composizione di applicazioni. Si verifica immediatamente che  $(S, \circ)$  è un semigruppato. Inoltre questo semigruppato non è abeliano se  $X$  ha almeno due elementi. Infatti se  $a, b \in X, a \neq b$  allora le applicazioni (costanti)  $f, g \in S$  definite da  $f(x) = a$  e  $g(x) = b$ , per ogni  $x \in X$ , sono tali che  $f(g(a)) = a$  e  $g(f(a)) = b$  e quindi  $f \circ g \neq g \circ f$ .

Sia  $\cdot$  un'operazione binaria su un insieme  $X \neq \emptyset$ . Diremo che  $x \in X$  è *cancellabile a sinistra* (risp. *a destra*) se

$$x \cdot y = x \cdot z \Rightarrow y = z, \forall y, z \in X \quad (1.5)$$

$$(\text{risp. } y \cdot x = z \cdot x \Rightarrow y = z, \forall y, z \in X). \quad (1.6)$$

Un'operazione binaria  $\cdot$  su un insieme  $X$  soddisfa la *legge di cancellazione a sinistra* (risp. *a destra*) se ogni elemento di  $X$  è cancellabile a sinistra (risp. a destra), cioè

$$x \cdot y = x \cdot z \Rightarrow y = z, \forall x, y, z \in X \quad (1.7)$$

$$(\text{risp. } y \cdot x = z \cdot x \Rightarrow y = z, \forall x, y, z \in X). \quad (1.8)$$

Diremo che un'operazione binaria su  $X \neq \emptyset$  soddisfa la *legge di cancellazione* se soddisfa la legge di cancellazione sia a sinistra che a destra.

**Osservazione 1.1.12** Se l'operazione binaria è commutativa allora ogni  $x \in X$  è cancellabile a sinistra se e solo se è cancellabile a destra e quindi vale la legge di cancellazione a sinistra se e solo se vale la legge di cancellazione a destra se e solo se vale la legge di cancellazione.

**Esempi 1.1.13** Il lettore è invitato a convincerci fornendo se necessario una dimostrazione della validità delle affermazioni seguenti.

1. nei semigruppato abeliani  $(S, +)$  e  $(S^+, +)$  degli Esempi 1.1.3 e 1.1.4 vale la legge di cancellazione.
2. Nei semigruppato  $(S, \cdot)$  dell'Esempio 1.1.5 non vale la legge di cancellazione: infatti  $0 \cdot 2 = 0 \cdot 3$  ma  $2 \neq 3$ . Un elemento è cancellabile se e solo se è diverso da 0.

3. nei semigruppi  $(S, \cdot)$  dell'Esempio 1.1.6 vale la legge di cancellazione.
4. nei semigruppi abeliani  $(P, +)$ ,  $(P^+, +)$  e  $(P^*, \cdot)$  dell'Esempio 1.1.7 vale la legge di cancellazione. Mentre nel semigruppo abeliano  $(P, \cdot)$  dello stesso esempio non vale la legge di cancellazione (un elemento è cancellabile se e solo se è diverso da 0).
5. l'operazione binaria (1.1) soddisfa la legge di cancellazione. Mentre l'operazione binaria (1.2) non la soddisfa. Infatti  $[0]_m[0]_m = [0]_m[1]_m = [0]_m$  ma  $[0]_m \neq [1]_m$ . Lo studio degli elementi cancellabili nel semigruppo  $(\mathbb{Z}_m, \cdot)$  è legato ai divisori dello zero nell'anello  $(\mathbb{Z}_m, \cdot)$ , argomento non trattato in queste note.
6. il semigruppo abeliano  $(P(X), \cup)$  (resp.  $(P(X), \cap)$ ) non soddisfa la legge di cancellazione. Per esempio se  $A \subset B$  e  $A \subset C$  e  $B \neq C$  allora  $A = A \cap B = A \cap C$  non implica  $B = C$ .
7. sia  $X$  un insieme con almeno due elementi. Allora l'operazione binaria (1.3) (resp. (1.4)) soddisfa la legge di cancellazione a destra (resp. sinistra) ma non a sinistra (resp. destra).
8. nel semigruppo  $(S, \circ)$  dell'Esempio 1.1.11 un elemento  $f \in S$  è cancellabile a sinistra (resp. a destra) se e solo se  $f$  è iniettiva (resp. suriettiva).

Sia  $\cdot$  un'operazione binaria su un insieme  $X \neq \emptyset$ . Diremo che  $b \in X$  è *idempotente* se

$$b^2 := b \cdot b = b.$$

**Esempi 1.1.14** Il lettore è invitato a convincersi fornendo se necessario una dimostrazione della validità delle affermazioni seguenti.

1. nei semigruppi  $(S, +)$  dell'Esempio 1.1.3 l'unico elemento idempotente è 0.
2. nei semigruppi  $(S^+, +)$  dell'Esempio 1.1.4 non ci sono elementi idempotenti.
3. nei semigruppi  $(S, \cdot)$  dell'Esempio 1.1.5 ci sono due elementi idempotenti, 0 e 1.
4. nei semigruppi  $(S, \cdot)$  dell'Esempio 1.1.6 l'unico elemento idempotente è 0.



5. nei semigruppato  $(P, +)$  e  $(P, \cdot)$  l'unico elemento idempotente è 0. Nei semigruppato  $(P^+, +)$  e  $(P^*, \cdot)$  non ci sono elementi idempotenti.
6. nel semigruppato  $(\mathbb{Z}_m, +)$ ,  $[0]_m$  è l'unico elemento idempotente se  $m$  è dispari. Cosa succede se  $m$  è pari?
7. nei semigruppato degli Esempi 1.1.9 e 1.1.10 tutti gli elementi sono idempotenti.

**Osservazione 1.1.15** Nel semigruppato  $(S, \circ)$  dell'Esempio 1.1.11 ci possono essere tanti elementi idempotenti e la loro classificazione varia al variare dell'insieme  $X$ . Il lettore è inviato a riflettere sul caso  $X = \mathbb{R}$ .

Concludiamo questa sezione dimostrando l'esistenza di un elemento idempotente in un semigruppato finito.

**Proposizione 1.1.16** Sia  $(S, \cdot)$  un semigruppato finito. Allora esiste almeno un elemento idempotente di  $S$ .

**Dimostrazione:** Sia  $x \in S$  un elemento arbitrario. Per la proprietà associativa dell'operazione binaria  $\cdot$  possiamo definire

$$x^n := \underbrace{x \cdot x \cdots x}_{n \text{ volte}}, \forall n \in \mathbb{N}^+.$$

Segue che

$$x^{n+1} = x^n x = x x^n, \forall n \in \mathbb{N}^+ \quad (1.9)$$

e, per induzione su  $n$  (fissato  $m$ ) si ha:

$$x^{m+n} = x^n x^m = x^m x^n, \forall m, n \in \mathbb{N}^+. \quad (1.10)$$

La (1.10) segue facilmente fissando  $m \in \mathbb{N}_+$ , usando l'induzione su  $n$  e la (1.9). Sia

$$C(x) = \{x^n \mid n \in \mathbb{N}^+\}.$$

Poichè  $C(x) \subset S$  e  $|S| < \infty$  anche  $|C(x)| < \infty$ . Consideriamo ora l'applicazione

$$f : \mathbb{N}^+ \rightarrow C(x), n \mapsto x^n.$$

Poichè la cardinalità di  $\mathbb{N}^+$  è infinita, l'applicazione  $f$  non è iniettiva. Esisteranno quindi  $i, j \in \mathbb{N}^+$ , con  $i > j$  tali che:

$$x^i = x^j. \quad (1.11)$$

Dalla (1.10) segue allora che

$$x^i = x^{i-j}x^j = x^j. \quad (1.12)$$

Inoltre, abbiamo che

$$x^i = x^{n(i-j)}x^j, \forall n \in \mathbb{N}^+. \quad (1.13)$$

La (1.13) si dimostra per induzione come segue. Per  $n = 1$  è vera per la (1.12). Supponiamola vera per  $n$ , cioè supponiamo la validità di (1.13). Allora da (1.10), (1.11) e (1.12) si ottiene

$$\begin{aligned} x^{(n+1)(i-j)}x^j &= x^{n(i-j)+(i-j)}x^j = x^{n(i-j)}x^{i-j}x^j = \\ &= x^{n(i-j)}x^jx^{i-j} = x^i x^{i-j} = x^j x^{i-j} = x^i, \end{aligned}$$

che mostra la validità di (1.13) per  $n + 1$ .

Scegliamo ora  $k \in \mathbb{N}^+$  tale che  $k(i-j) > j$  e definiamo  $b \in S$  come

$$b := x^{k(i-j)}.$$

Mostriamo che  $b$  è un elemento idempotente. Infatti

$$\begin{aligned} b^2 &= b \cdot b = x^{k(i-j)}x^{k(i-j)} = x^{k(i-j)}x^{k(i-j)-j}x^j = x^{k(i-j)}x^jx^{k(i-j)-j} = \\ &= x^i x^{k(i-j)-j} = x^j x^{k(i-j)-j} = x^{k(i-j)} = b. \end{aligned}$$

□

**Osservazione 1.1.17** I semigruppi  $(S^+, +)$  dell' Esempio 1.1.4 mostrano che l'ipotesi che  $S$  sia finito è necessaria per la validità della proposizione precedente.

## 1.2 Monoidi

Sia  $\cdot$  un'operazione binaria su un insieme  $X \neq \emptyset$ . Un elemento  $1 \in M$  si dice *elemento neutro a destra* (risp. *sinistra*) per l'operazione binaria  $\cdot$ , se

$$x \cdot 1 = x \text{ (risp. } 1 \cdot x = x), \forall x \in X.$$

Diremo che  $1$  è un elemento neutro per l'operazione binaria  $\cdot$  se  $1$  è un elemento neutro sia a destra che a sinistra.

Se l'operazione binaria è chiara dal contesto, parleremo di elemento neutro (a destra oppure sinistra) senza specificare l'operazione binaria.

**Osservazione 1.2.1** Se l'operazione binaria su un insieme  $X$  è commutativa allora 1 è un elemento neutro a destra se e solo se 1 è un elemento neutro a sinistra se e solo se 1 è un elemento neutro.

Osserviamo che se esiste un elemento neutro 1 per un'operazione binaria su un insieme  $X$ , allora 1 è l'unico elemento neutro, e parleremo quindi di 1 come l'elemento neutro. Infatti, se  $\tilde{1} \in X$  è un altro elemento neutro allora

$$\tilde{1} = \tilde{1} \cdot 1 = 1,$$

dove nella prima uguaglianza stiamo usando il fatto che 1 è un elemento neutro a destra, mentre nella seconda che  $\tilde{1}$  è un elemento neutro a sinistra.

**Definizione 1.2.2** Un semigruppò  $(M, \cdot)$  è un monoide se esiste l'elemento neutro  $1 \in M$ .

Equivalentemente, un monoide è un tripletta  $(M, \cdot, 1)$ , dove  $(M, \cdot)$  è un semigruppò ed 1 è l'elemento neutro. Un monoide  $(M, \cdot, 1)$  è detto *abeliano* o *commutativo* se il semigruppò  $(M, \cdot)$  è abeliano.

**Notazione 1.2.3** Nel caso di un monoide abeliano scriveremo l'operazione binaria con  $+$  e l'elemento neutro con 0. Quindi un monoide abeliano sarà indicato con  $(M, +, 0)$ . Un monoide arbitrario sarà indicato con  $(M, \cdot, 1)$ .

**Esempio 1.2.4** Le coppie  $(S, +)$  dell'Esempio 1.1.3 sono monoidi abeliani infiniti dove l'elemento neutro è lo 0.

**Esempio 1.2.5** Nessuna delle coppie  $(S^+, +)$  dell'Esempio 1.1.4 è un monoide.

**Esempio 1.2.6** Le coppie  $(S, \cdot)$  dell'Esempio 1.1.5 sono monoidi abeliani infiniti con elemento neutro 1.

**Esempio 1.2.7** Le coppie  $(S, \cdot)$  dell'Esempio 1.1.6 sono monoidi sabeliani infiniti con elemento neutro 1.

**Esempio 1.2.8** Sia  $P$  l'insieme dei numeri interi pari come nell'Esempio 1.1.7. Allora  $(P, +, 0)$  è un monoide abeliano infinito. Mentre nessuna delle coppie  $(P^+, +)$ ,  $(P, \cdot)$  e  $(P^*, \cdot)$  è un monoide.

**Esempio 1.2.9** In riferimento all'Esempio 1.1.8,  $(\mathbb{Z}_m, +, [0]_m)$  e  $(\mathbb{Z}_m, \cdot, [1]_m)$  sono entrambi monoidi abeliani di ordine  $m$ .

**Esempio 1.2.10** In riferimento all'Esempio 1.1.9  $(P(X), \cup, \emptyset)$  (resp.  $(P(X), \cap, X)$ ) sono monoidi abeliani.

**Esempio 1.2.11** In riferimento all'Esempio 1.2.11,  $(X, \cdot)$  non é mai un monoide per  $|X| \geq 2$ .

**Esempio 1.2.12** In riferimento all'Esempio 1.1.11,  $(S = X^X, \circ)$  é un monoide con elemento neutro  $\text{id}_X$  ( $\text{id}_X(x) = x$  per ogni  $x \in X$ ).

Dato un monoide  $(M, \cdot, 1)$  allora l'elemento neutro è chiaramente un elemento idempotente ( $1 \cdot 1 = 1$ ).

**Proposizione 1.2.13** Sia  $(M, \cdot, 1)$  un monoide dove vale la legge di cancellazione a destra oppure a sinistra. Allora 1 é l'unico elemento idempotente.

**Dimostrazione:** Supponiamo che  $b \in M$  sia un idempotente e che valga la legge di cancellazione a destra. Allora dalla relazione

$$b \cdot b = b^2 = b = 1 \cdot b$$

si ottiene ( $b$  é cancellabile a destra)  $b = 1$ . Analogamente, se vale la legge di cancellazione a sinistra da

$$b \cdot b = b^2 = b = b \cdot 1$$

si ottiene ( $b$  é cancellabile a sinistra)  $b = 1$ . □

Senza l'ipotesi della legge di cancellazione la proposizione precedente non é valida come mostra il monoide dell'Esempio 1.2.10, dove tutti gli elementi sono idempotenti. La Proposizione 1.2.13 non si estende a semigruppi. Si pensi, per esempio, ad un insieme  $X$  con operazione binaria  $x \cdot y = x$  (cf. Esempio 1.1.10). Come abbiamo osservato in quest'esempio vale la legge di cancellazione a destra ma non a sinistra e tutti gli elementi sono idempotenti.

D'altra parte la Proposizione 1.2.13 si estende a semigruppi se si richiede che valga la legge di cancellazione (sia a destra che a sinistra).

**Proposizione 1.2.14** Sia  $(S, \cdot)$  un semigruppo dove vale la legge di cancellazione e sia  $b \in S$  un elemento idempotente. Allora  $b$  é l'elemento neutro e quindi  $(S, \cdot, b)$  é un monoide.

**Dimostrazione:** Supponiamo che  $b \in M$  sia un idempotente. Allora

$$b \cdot b \cdot x = b^2 x = bx, \forall x \in S.$$

Usando la legge di cancellazione a sinistra si ottiene quindi che  $b \cdot x = x$  per ogni  $x \in S$  e quindi  $b$  è un elemento neutro a sinistra. In modo analogo, dalla relazione

$$x \cdot b \cdot b = x \cdot b^2 = x \cdot b, \forall x \in S$$

e usando la legge di cancellazione a destra si ottiene  $b \cdot x = x$  per ogni  $x \in S$ . Quindi  $b$  è l'elemento neutro e  $(S, \cdot, b)$  è un monoide.  $\square$

Combinando la Proposizione 1.1.16 con la Proposizione 1.2.14 si ottiene:

**Corollario 1.2.15** *Un semigrupp finito dove vale la legge di cancellazione è un monoide.*

## 1.3 Gruppi

Sia  $(M, \cdot, 1)$  un monoide e sia  $x \in M$ . Diremo che  $a \in M$  è un inverso destro di  $x$  se

$$x \cdot a = 1. \quad (1.14)$$

Diremo che  $a \in M$  è un inverso sinistro di  $x$  se

$$a \cdot x = 1. \quad (1.15)$$

Diremo che  $a$  è un'inverso di  $x$  se,  $a$  è sia inverso destro che inverso sinistro. Se  $x$  ha un'inverso allora diremo che  $x$  è *invertibile*.

**Proposizione 1.3.1** *Sia  $x$  un elemento di un monoide  $(M, \cdot, 1)$ . Se  $x$  è invertibile allora il suo inverso è unico.*

**Dimostrazione:** Siano  $a$  e  $b$  due inversi di  $x$ . Per la proprietà associativa possiamo scrivere

$$a = a \cdot 1 = a \cdot (x \cdot b) = (a \cdot x) \cdot b = 1 \cdot b = b,$$

dove nella seconda uguaglianza abbiamo usato il fatto che  $b$  è l'inverso destro di  $x$  e nella terza che  $a$  è l'inverso sinistro di  $x$ .  $\square$

In virtù della proposizione precedente dato un elemento invertibile  $x \in M$  parleremo *del* suo inverso che indicheremo (momentaneamente) con  $i(x)$ .

**Definizione 1.3.2** *Una tripletta  $(G, \cdot, 1)$  è un gruppo se è un monoide e tutti gli elementi di  $G$  sono invertibili.*

Quindi un gruppo é una tripletta  $(G, \cdot, 1)$  dove  $(G, \cdot)$  é un semigrupp (cioé l'operazione binaria  $\cdot : G \times G \rightarrow G$  é associativa) tale che:

$$x \cdot 1 = x, \forall x \in G \text{ (1 è elemento neutro a destra);} \quad (1.16)$$

$$1 \cdot x = x, \forall x \in G \text{ (1 è elemento neutro a sinistra);} \quad (1.17)$$

e per ogni  $x \in G$  esiste  $i(x)$  tale che:

$$x \cdot i(x) = 1 \text{ (} i(x) \text{ è inverso destro di } x\text{);} \quad (1.18)$$

$$i(x) \cdot x = 1 \text{ (} i(x) \text{ è inverso sinistro di } x\text{).} \quad (1.19)$$

**Osservazione 1.3.3** Come conseguenza dell'esistenza di un inverso per ogni elemento otteniamo che ogni equazione di primo grado in un gruppo  $G$  ha sempre un'unica soluzione: dati  $a, b \in G$ . esiste un unico  $x \in G$  che soddisfa l'equazione.

$$ax = b. \quad (1.20)$$

Infatti moltiplicando a sinistra (risp. destra) per  $a^{-1}$  l'equazione precedente si ottiene  $a^{-1} \cdot (a \cdot x) = (a^{-1} \cdot a) \cdot x = x$  (risp.  $a^{-1}b$ ). E quindi l'unica soluzione dell'equazione (1.20) è  $x = a^{-1}b$ .

Notiamo che alcune delle proprietà nella definizione di gruppo sono ridondanti. Infatti, come mostra la seguente proposizione, basta richiedere la validità dell'esistenza di un elemento neutro a destra (risp. sinistra) e di un inverso destro (risp. sinistro) per ogni elemento di un semigrupp per essere sicuri che il semigrupp sia in effetti un gruppo.

**Proposizione 1.3.4** Sia  $(S, \cdot)$  un semigrupp. Supponiamo che le (1.16) e (1.18) (risp. (1.17) e (1.19)) siano soddisfatte. Allora  $(S, \cdot, 1)$  é un gruppo.

**Dimostrazione:** Sia  $x \in S$ . Per la (1.18) esiste  $i(x) \in S$  tale che  $x \cdot i(x) = 1$ . Vogliamo mostrare che  $i(x)$  é anche inverso sinistro di  $x$ . Osserviamo che

$$b := i(x) \cdot x$$

é idempotente. Infatti

$$b^2 = b \cdot b = (i(x) \cdot x) \cdot (i(x) \cdot x) = i(x) \cdot (x \cdot i(x)) \cdot x = (i(x) \cdot 1) \cdot x = i(x) \cdot x = b,$$

dove nella penultima uguaglianza abbiamo usato la (1.16). Sia ora  $i(b)$  l'inverso destro di  $b$  che esiste sempre per la (1.18). Allora

$$1 = b \cdot i(b) = b^2 \cdot i(b) = b \cdot (b \cdot i(b)) = b \cdot 1 = b$$

e quindi  $i(x) \cdot x = 1$  e  $i(x)$  è inverso sinistro di  $x$ . Inoltre 1 è un elemento neutro a sinistra. Infatti

$$1 \cdot x = (x \cdot i(x)) \cdot x = x \cdot (i(x) \cdot x) = x \cdot 1 = x.$$

In modo analogo si dimostra che un semigrupp dove valgono le (1.17) e (1.19) è un gruppo.  $\square$

**Osservazione 1.3.5** Le conclusioni della Proposizione 1.3.4 non sono valide se si richiede che valgano le (1.16) e (1.19) (risp. (1.17) e (1.18)). Per esempio sia  $(X, \cdot)$  il semigrupp dato da un insieme  $X \neq \emptyset$  con operazione binaria  $x \cdot y = x$  per ogni  $x, y \in X$  (si veda l'Esempio 1.1.10). Allora ogni elemento di  $X$  è un elemento neutro a destra e ogni elemento di  $X$  ha un inverso sinistro e come abbiamo già osservato  $(X, \cdot)$  non è un monoide (si veda Esempio 1.2.11). Un altro esempio è fornito dal semigrupp  $(\mathbb{R}^*, \cdot)$  con operazione binaria

$$x \cdot y = |x| y,$$

dove  $|x|$  denota il valore assoluto di  $x \in \mathbb{R}^*$ . In questo caso 1 è un elemento neutro sinistro (ma non destro  $|x| = x \cdot 1 \neq x$ , se  $x < 0$ ) e ogni elemento  $x$  ha inverso destro dato da  $|x|^{-1}$ . D'altra parte, un qualunque  $y \in \mathbb{R}^*$ , con  $y < 0$  non ha inverso sinistro. Notiamo che in questo esempio esistono due elementi neutri a sinistra  $\pm 1$  e se si fosse scelto  $-1$  come elemento neutro sinistro allora ogni  $y \in \mathbb{R}^*$  con  $y > 0$  non avrebbe avuto inverso sinistro.

**Notazione 1.3.6** Nel resto di queste note indicheremo con  $G$  invece che con  $(G, \cdot, 1)$  un gruppo, quando l'operazione binaria e l'elemento neutro saranno chiari dal contesto. Inoltre indicheremo con  $x^{-1}$  l'inverso di un elemento  $x \in G$  ( $x \cdot x^{-1} = x^{-1} \cdot x = 1$ ). Se il gruppo  $G$  è abeliano useremo anche la notazione  $+$  per l'operazione binaria,  $0$  per l'elemento neutro e  $-x$  per l'inverso di  $x \in G$  (e scriveremo  $x + (-x) = x - x = 0$ ).

### 1.3.1 Alcuni esempi di gruppi

Il lettore è invitato a convincersi che gli esempi che seguono sono effettivamente gruppi e di capire perchè alcuni dei monoidi degli Esempi 1.2.4-1.2.12 non appartengono a questa lista.

**Esempio 1.3.7** Le coppie  $(S, +, 0)$ , dove  $S = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  e  $+$  è la somma usuale sono gruppi abeliani infiniti.

**Esempio 1.3.8** Le coppie  $(S, \cdot, 1)$ , dove  $S = \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$  e  $\cdot$  è la moltiplicazione usuale sono gruppi abeliani infiniti.

**Esempio 1.3.9** (il cerchio unitario) L'insieme

$$S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$$

è un gruppo abeliano infinito con la moltiplicazione  $\cdot$  usuale tra numeri complessi. Ricordiamo che se  $z = x + iy$  allora il suo modulo è definito come  $|z| = \sqrt{x^2 + y^2}$ . Infatti, il prodotto di due numeri complessi di modulo unitario è un numero complesso di modulo unitario, in quanto

$$|zw| = |z||w| = 1, \forall z, w \in S^1,$$

e quindi la moltiplicazione è un'operazione binaria su  $S^1$ .  $(S^1, \cdot)$  è un semigruppato perchè la legge associativa vale in  $\mathbb{C}^*$  e a fortiori in  $S^1$ . Inoltre  $1 \in S^1$  è l'elemento neutro in  $\mathbb{C}^*$  e quindi in  $S^1$ . Segue che  $(S^1, \cdot, 1)$  è un monoide abeliano. Infine se  $z \in S^1$  allora  $z^{-1} \in S^1$ . Infatti

$$z^{-1} = \frac{\bar{z}}{|z|^2} = \bar{z} \in S^1,$$

dove  $\bar{z}$  è il coniugato di  $z$  (se  $z = x + iy$  allora  $\bar{z} = x - iy$ ).

Per descrivere altri esempi di gruppi definiamo il concetto di campo. Una coppia  $\mathbb{K} = (\mathbb{K}, +, \cdot, 0, 1)$ ,  $0, 1 \in \mathbb{K}$ ,  $0 \neq 1$ , è un campo se  $(\mathbb{K}, +, 0)$  e  $(\mathbb{K}^*, \cdot, 1)$  ( $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ ) sono gruppi abeliani e vale la seguente proprietà distributiva del prodotto  $\cdot$  rispetto alla somma  $+$ :

$$x \cdot (y + z) = x \cdot y + x \cdot z, \forall x, y, z \in \mathbb{K}.$$

Segue dagli Esempi 1.3.7 e 1.3.8 che  $\mathbb{Q}$ ,  $\mathbb{R}$  e  $\mathbb{C}$  con le operazioni usuali di somma e prodotto sono campi infiniti. Esistono anche campi finiti. Quello a cui siamo interessati in questo corso è il campo  $\mathbb{Z}_p = (\mathbb{Z}_p, +, \cdot, [0]_p, [1]_p)$  degli interi modulo  $p$ , con  $p$  numero primo, con somma e moltiplicazione definite da (1.1) e (1.2). Il fatto che  $\mathbb{Z}_p$  sia un campo (con  $p$  elementi) segue dal fatto che  $(\mathbb{Z}_p, +, [0]_p)$  è un gruppo abeliano (cf. l'Esempio 1.1.8), che  $(\mathbb{Z}_p, +, [1]_p)$  è un monoide (cf. l'Esempio 1.2.9) e ogni  $[a]_p \neq [0]_p$  è invertibile. Quest'ultimo fatto si dimostra come segue: per il teorema di Bezout essendo  $a$  coprimo con  $p$  esistono  $u, v \in \mathbb{Z}$  tali che  $ua + vp = 1$ . Segue che

$$[ua]_p = [a]_p \cdot [u]_p = [u]_p \cdot [a]_p = [1]_p$$

e quindi  $[u]_p$  è l'inverso di  $[a]_p$ .

Si noti che un campo ha almeno 2 elementi ( $0 \neq 1$ ) e che  $\mathbb{Z}_2$  è un campo con 2 elementi.



**Esempio 1.3.10** (il gruppo lineare) Sia  $n \in \mathbb{N}^+$  un intero positivo e sia  $\mathbb{K}$  un campo. Definiamo  $M_n(\mathbb{K})$  come l'insieme delle matrici quadrate di ordine  $n$ , ovvero  $n \times n$ , a coefficienti in  $\mathbb{K}$ . Un elemento  $A \in M_n(\mathbb{K})$  può essere scritto come

$$A = (a_{ij}), \quad i, j = 1, \dots, n,$$

dove  $a_{ij} \in \mathbb{K}$  rappresenta l'elemento della  $i$ -esima riga e  $j$ -esima colonna.

Possiamo definire una somma tra due matrici: se  $A = (a_{ij})$  e  $B = (b_{ij})$  sono due matrici in  $M_n(\mathbb{K})$ , la matrice somma  $C := A + B \in M_n(\mathbb{K})$  è definita come

$$C = (c_{ij}), \quad c_{ij} = a_{ij} + b_{ij}, \quad i, j = 1, \dots, n.$$

Questa operazione è una somma componente per componente.

Inoltre,  $(M_n(\mathbb{K}), +, O_n)$  è un *monoide*, dove  $O_n$  denota la *matrice nulla*, cioè la matrice  $n \times n$  le cui entrate sono tutte uguali a 0, ossia:

$$O_n = (0_{ij}), \quad 0_{ij} = 0, \quad \forall i, j = 1, \dots, n.$$

Possiamo anche definire il prodotto tra due matrici: se  $A = (a_{ik})$  e  $B = (b_{kj})$  sono due matrici in  $M_n(\mathbb{K})$ , la matrice prodotto  $C := A \cdot B \in M_n(\mathbb{K})$  è definita mediante il prodotto righe per colonne, ossia:

$$C = (c_{ij}), \quad c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}, \quad i, j = 1, \dots, n.$$

Anche questa è un'operazione binaria. Inoltre,  $(M_n(\mathbb{K}), \cdot, I_n)$  è un *monoide* rispetto al prodotto, dove  $I_n$  denota la *matrice identità*, definita come:

$$I_n = (\delta_{ij}), \quad \delta_{ij} = \begin{cases} 1, & \text{se } i = j, \\ 0, & \text{se } i \neq j. \end{cases}$$

La matrice identità ha 1 su tutta la diagonale principale e 0 altrove.

La dimostrazione che  $(M_n(\mathbb{K}), \cdot, I_n)$  è un monoide segue gli stessi passaggi visti nei corsi di algebra lineare, con l'ipotesi che il campo  $\mathbb{K}$  sia  $\mathbb{R}$  o  $\mathbb{C}$ .

Per  $n \in \mathbb{N}^+$ , il *gruppo lineare generale* su un campo  $\mathbb{K}$  è definito come

$$GL_n(\mathbb{K}) = \{A \in M_n(\mathbb{K}) \mid A \text{ è invertibile}\},$$

dove una matrice  $A \in M_n(\mathbb{K})$  è detta *invertibile* se esiste una matrice  $B \in M_n(\mathbb{K})$  tale che

$$AB = BA = I_n.$$

Una tale matrice  $B$  è chiamata *inversa* di  $A$  ed è anch'essa un elemento di  $GL_n(\mathbb{K})$ , ossia invertibile. La condizione che  $A$  sia invertibile è equivalente al fatto che il suo *determinante*,  $\det(A)$ , sia diverso da 0, dove  $0 \in \mathbb{K}$  è l'elemento nullo del campo. Il determinante di una matrice quadrata  $A$  su un campo  $\mathbb{K}$  si definisce nello stesso modo che per  $\mathbb{K} = \mathbb{R}$  o  $\mathbb{K} = \mathbb{C}$ .

Si invitano i lettori a verificare che tutte le proprietà del determinante viste nei corsi di algebra lineare si estendono al caso generale di un campo arbitrario. Ad esempio, la formula di Binet, che afferma che

$$\det(AB) = \det(A) \det(B), \quad \forall A, B \in M_n(\mathbb{K}),$$

vale in qualsiasi campo  $\mathbb{K}$ .

Usando la formula di Binet, si può concludere che  $(GL_n(\mathbb{K}), \cdot, I_n)$  è un *gruppo*, che in generale non è abeliano per  $n \geq 2$ . Tuttavia, è un gruppo abeliano per  $n = 1$ , poiché  $GL_1(\mathbb{K}) = \mathbb{K}^*$ .

Concludiamo questa sezione mostrando come, a partire da un monoide, si possa costruire un gruppo considerando i suoi elementi invertibili.

**Proposizione 1.3.11** *Sia  $M = (M, \cdot, 1)$  un monoide. Definiamo l'insieme degli elementi invertibili di  $M$  come:*

$$U(M) = \{x \in M \mid x \text{ è invertibile}\}.$$

*Allora  $(U(M), \cdot, 1)$  è un gruppo.*

**Dimostrazione:** Siano  $x, y \in U(M)$ , cioè  $x$  e  $y$  sono invertibili. Dimostriamo che anche il loro prodotto è invertibile. In particolare, mostriamo che l'inverso di  $x \cdot y$  è dato da:

$$(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}. \quad (1.21)$$

Infatti:

$$(x \cdot y) \cdot (y^{-1} \cdot x^{-1}) = x \cdot (y \cdot y^{-1}) \cdot x^{-1} = x \cdot 1 \cdot x^{-1} = x \cdot x^{-1} = 1,$$

e, analogamente:

$$(y^{-1} \cdot x^{-1}) \cdot (x \cdot y) = y^{-1} \cdot (x^{-1} \cdot x) \cdot y = y^{-1} \cdot 1 \cdot y = y^{-1} \cdot y = 1.$$

Pertanto,  $x \cdot y$  è invertibile e l'inverso è  $y^{-1} \cdot x^{-1}$ . Da ciò si deduce che la moltiplicazione definita su  $M$  induce un'operazione binaria su  $U(M)$ . Ora, osserviamo che  $(U(M), \cdot)$  è un semigruppato, poiché la proprietà associativa vale in

$M$  e, quindi, anche nel sottoinsieme  $U(M)$ . Inoltre,  $(U(M), \cdot, 1)$  è un monoide, in quanto 1 è invertibile (essendo il suo stesso inverso). Infine, per costruzione, tutti gli elementi di  $U(M)$  sono invertibili, il che dimostra che  $(U(M), \cdot, 1)$  è un gruppo.  $\square$

**Osservazione 1.3.12** Segue immediatamente dalla definizione di gruppo che, se  $G$  è un gruppo, allora  $U(G) = G$ , poiché per definizione tutti gli elementi di un gruppo sono invertibili.

**Osservazione 1.3.13** La formula (1.21) si estende facilmente a più elementi: se  $x_1, \dots, x_k, k \geq 2$  sono elementi di  $G$ , allora

$$(x_1 \cdots x_k)^{-1} = x_k^{-1} \cdots x_1^{-1}.$$

Non è detto che il gruppo  $U(M)$  sia sempre interessante. Ad esempio, nel caso del monoide  $(\mathbb{Z}, +, 0)$  (rispettivamente  $(\mathbb{Z}, \cdot, 1)$ ), l'insieme degli elementi invertibili è costituito solo da 0 (rispettivamente 1). Un altro esempio è dato dal monoide  $(\mathbb{Q}, \cdot, 1)$  (rispettivamente  $(\mathbb{R}, \cdot, 1)$  e  $(\mathbb{C}, \cdot, 1)$ ), in cui l'insieme degli elementi invertibili è  $\mathbb{Q}^*$  (rispettivamente  $\mathbb{R}^*$  e  $\mathbb{C}^*$ ).

Un esempio rilevante è dato da  $U(M_n(\mathbb{K}), \cdot, I_n) = GL_n(\mathbb{K})$ , l'insieme delle matrici invertibili di ordine  $n$  su un campo  $\mathbb{K}$ .

**Esempio 1.3.14** Consideriamo il monoide  $(\mathbb{Z}_m, \cdot, [1]_m)$ , dove  $\mathbb{Z}_m$  sono gli interi modulo  $m$  e  $[1]_m$  è l'elemento neutro rispetto alla moltiplicazione modulo  $m$ . L'insieme degli elementi invertibili di  $(\mathbb{Z}_m, \cdot)$  è dato da:

$$U(\mathbb{Z}_m, \cdot) = \{[a]_m \in \mathbb{Z}_m \mid (a, m) = 1\}, \quad (1.22)$$

dove  $(a, m)$  indica il massimo comun divisore tra  $a$  e  $m$ . Infatti, se  $a$  è coprimo con  $m$ , esistono  $u, v \in \mathbb{Z}$  tali che  $ua + vm = 1$ . Questo implica che:

$$[ua]_m = [a]_m \cdot [u]_m = [u]_m \cdot [a]_m = [1]_m, \quad (1.23)$$

e quindi  $[u]_m$  è l'inverso di  $[a]_m$ . Viceversa, se  $[a]_m \in U(\mathbb{Z}_m, \cdot)$ , esiste  $[u]_m \in \mathbb{Z}_m$  tale che valga la relazione (1.23), il che implica che  $au + km = 1$  per un intero  $k$ , e quindi  $(a, m) = 1$ . Osserviamo che questo ragionamento mostra che  $\mathbb{Z}_m$  è un campo se e solo se  $m$  è un numero primo.

### 1.3.2 La legge di cancellazione in un gruppo

Un risultato fondamentale nei gruppi è espresso dalla seguente proposizione.

**Proposizione 1.3.15** *In un gruppo  $G$  vale la legge di cancellazione.*

**Dimostrazione:** Siano  $x, y, z \in G$  tali che  $xy = xz$ . Moltiplicando a sinistra per  $x^{-1}$  (l'inverso di  $x$ ) il primo e secondo membro di quest'equazione si ottiene  $x^{-1}(xy) = x^{-1}(xz)$ . Per la proprietà associativa il primo (risp. secondo) membro si scrive come  $x^{-1}(xy) = (x^{-1}x)y = 1y = y$  (risp.  $x^{-1}(xz) = (x^{-1}x)z = 1z = z$ ). Segue dunque che  $y = z$ , il che mostra la validità della legge di cancellazione a sinistra. Analogamente da  $yx = zx$  si ottiene  $y = z$  moltiplicando a destra per  $x^{-1}$ .  $\square$

A questo punto sorge spontanea una domanda: in un semigruppato o in un monoide in cui vale la legge di cancellazione, l'insieme è necessariamente un gruppo? Le due proposizioni seguenti esplorano questa questione.

**Proposizione 1.3.16** *Sia  $M$  un monoide finito. Se vale la legge di cancellazione a destra o a sinistra, allora  $M$  è un gruppo.*

**Dimostrazione:** Sia  $x \in M$ . Dimostriamo che  $x$  è invertibile. Se vale la legge di cancellazione a sinistra consideriamo la *traslazione a sinistra* definita da:

$$L_x : M \rightarrow M, y \mapsto xy.$$

Questa funzione è iniettiva: se  $L_x(y) = L_x(z)$  allora  $xy = xz$  e, cancellando  $x$  a sinistra si ottiene  $y = z$ . Poichè  $M$  è finito,  $L_x$  è anche suriettiva. Quindi esiste un elemento  $i(x) \in M$  tale che  $x \cdot i(x) = L_x(i(x)) = 1$ , dimostrando che  $i(x)$  è un inverso destro di  $x$ . Dal momento che  $1$  è l'elemento neutro a destra, segue dalla Proposizione 1.3.4 che  $i(x)$  è anche inverso sinistro di  $x$  e quindi  $x$  è invertibile. Se invece vale la legge di cancellazione a destra, consideriamo la *traslazione a destra*:

$$R_x : M \rightarrow M, y \mapsto yx$$

che si dimostra essere iniettiva, e quindi suriettiva, da cui si deduce che  $x$  è invertibile.  $\square$

**Osservazione 1.3.17** Il fatto che  $M$  sia finito è essenziale per la validità della proposizione precedente. Consideriamo, infatti, l'insieme infinito  $X$  e il monoide  $(\text{Inj}(X), \circ, id_X)$  delle applicazioni iniettive da  $X$  in se stesso, con l'operazione di composizione. In questo monoide vale la legge di cancellazione a

sinistra, ma non è un gruppo poiché esistono applicazioni iniettive non invertibili. Analoghe considerazioni valgono per il monoide  $(\text{Surj}(X), \circ, id_X)$  delle applicazioni suriettive, dove vale la legge di cancellazione a destra ma non si tratta di un gruppo.

**Corollario 1.3.18** *Sia  $S$  un semigrupp finito. Se vale la legge di cancellazione, allora  $S$  è un gruppo.*

**Dimostrazione:** Dal Corollario 1.2.15  $(S, \cdot, b)$  è un monoide, e quindi la conclusione segue dalla Proposizione 1.3.16.  $\square$

**Osservazione 1.3.19** Anche nel caso del Corollario 1.3.18, la finitezza di  $S$  è fondamentale. Ad esempio,  $(\mathbb{N}^+, +)$  è un semigrupp con infiniti elementi in cui vale la legge di cancellazione, ma non è un monoide e tantomeno un gruppo.

**Osservazione 1.3.20** Nel Corollario 1.3.18, l'ipotesi della legge di cancellazione non può essere indebolita richiedendo solo la validità della legge di cancellazione a destra (o a sinistra), anche se il semigrupp è finito. Infatti, se  $X$  è un insieme finito con almeno due elementi, l'operazione binaria (1.3) (rispettivamente, (1.4)) soddisfa la legge di cancellazione a destra (rispettivamente, a sinistra), ma  $(X, \cdot)$  non è un monoide e tantomeno un gruppo.

### 1.3.3 Potenze, il commutatore e l'ordine di un elemento

Sia  $(G, \cdot, 1)$  un gruppo,  $x \in G$  e  $m \in \mathbb{Z}$ . Definiamo

- (a)  $x^0 := 1$ ;
- (b)  $x^n := \underbrace{x \cdot x \cdots x}_{n \text{ volte}}, \text{ se } n > 0 \text{ (definizione per induzione)}$ ;
- (c)  $x^n := (x^{-1})^{-n}, \text{ se } n < 0$ .

**Osservazione 1.3.21** La relazione (c) con  $n = -1$ , mostra che  $x$  alla potenza  $-1$  è proprio  $x^{-1}$ , l'inverso di  $x$ . Inoltre la (c) vale anche se  $n > 0$ . Infatti, applicando la (3) si ottiene

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

dove si è usato il fatto che

$$(x^{-1})^{-1} = x.$$

La seguente proposizione descrive le proprietà delle potenze con esponente intero in un gruppo.

**Proposizione 1.3.22** *Sia  $G$  un gruppo. Allora per ogni  $x \in G$  e per ogni  $m, n \in \mathbb{Z}$  si ha:*

$$(1) \quad x^n = x^{n-1}x = xx^{n-1};$$

$$(2) \quad x^{m+n} = x^n x^m = x^m x^n;$$

$$(3) \quad (x^n)^{-1} = x^{-n};$$

$$(4) \quad x^{mn} = (x^m)^n = (x^n)^m.$$

**Dimostrazione:** Se  $n$  è un numero naturale la formula

$$x^n = x^{n-1}x = xx^{n-1} \quad (1.24)$$

ossia la (1) per  $n \geq 0$ , segue dalla proprietà associativa. Se  $n < 0$ :

$$x^n = (x^{-1})^{-n} = (x^{-1})^{-n} \cdot 1 = (x^{-1})^{-n} x^{-1}x = (x^{-1})^{-n+1}x = x^{n-1}x$$

dove nella penultima uguaglianza si è usato la (1.24) in quanto  $-n > 0$  e nella prima e ultima uguaglianza la (c). Analogamente

$$x^n = (x^{-1})^{-n} = 1 \cdot (x^{-1})^{-n} = xx^{-1}(x^{-1})^{-n} = x(x^{-1})^{-n+1} = xx^{n-1}.$$

Per dimostrare la (2) è sufficiente dimostrare la prima uguaglianza  $x^m x^n = x^{m+n}$ , poiché  $m+n = n+m$ . Fissiamo  $m$  e supponiamo innanzitutto che  $n$  sia un numero naturale. Procediamo per induzione su  $n$ . Se  $n = 0$ , l'uguaglianza è vera. Supponiamo che sia vera per  $n-1$ , allora usando la (1), si ha:

$$x^m x^n = x^m x^{n-1}x = x^{m+n-1}x = x^{m+n-1+1} = x^{m+n} \quad (1.25)$$

ossia la (2) quando  $n > 0$ . Se invece  $n < 0$ , allora dalla (c) e dalla (1.25) ( $-n > 0$ ) si ha:

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

Dalla (2) e dalla (a) si ottiene:

$$x^n x^{-n} = x^{n-n} = x^0 = 1$$

dalla quale segue la (3) per l'unicità dell'inverso. Infine, per dimostrare la (4), è sufficiente dimostrare la prima uguaglianza  $(x^m)^n = x^{mn}$ , poiché  $mn = nm$ .

Fissiamo  $m$  e supponiamo inizialmente che  $n$  sia un numero naturale. Procediamo per induzione su  $n$ . Se  $n = 0$ , l'uguaglianza è vera. Supponiamo che sia vera per  $n - 1$ , ossia  $(x^m)^{n-1} = x^{m(n-1)}$ , allora, usando la (1) otteniamo:

$$(x^m)^n = (x^m)^{n-1}x^m = x^{m(n-1)}x^m = x^{mn-m+m} = x^{mn}, \quad (1.26)$$

ossia la (4) quando  $n > 0$ .

Se invece  $n < 0$ , allora:

$$(x^m)^n = ((x^m)^{-1})^{-n} = (x^{-m})^{-n} = x^{(-m)(-n)} = x^{mn},$$

dove nella prima uguaglianza si è usata la (c), nella seconda la (3) e nella terza la (1.26).  $\square$

**Notazione 1.3.23** Supponiamo  $G$  abeliano e usiamo la notazione additiva  $G = (G, +, 0)$ . Allora le (a), (b), (c), (1), (2), (3), (4) si scrivono come segue.

- $0 \cdot x = 0$ ;
- $nx = \underbrace{x + \cdots + x}_{n \text{ volte}}, \text{ se } n > 0$ ;
- $nx = (-n)(-x) \text{ se } n < 0$ ;
- $nx = (n - 1)x + x = x + (n - 1)x$ ;
- $(m + n)x = nx + mx = mx + nx$ ;
- $-(nx) = (-n)x$ ;
- $(mn)x = n(mx) = m(nx)$ .

**Definizione 1.3.24** Sia  $G$  un gruppo. Diremo che  $x, y \in G$  commutano o sono permutabili se

$$xy = yx.$$

Dati due elementi qualunque  $x, y \in G$ , chiameremo il commutatore tra  $x$  e  $y$  il seguente elemento di  $G$ :

$$[x, y] = xyx^{-1}y^{-1}.$$

Segue immediatamente che  $x, y \in G$  sono permutabili se e solo se  $[x, y] = 1$ . Chiaramente l'elemento neutro commuta con ogni altro elemento del gruppo.

**Proposizione 1.3.25** Siano  $x, y \in G$  due elementi permutabili, cioè  $[x, y] = 1$ . Allora, per ogni  $m, n \in \mathbb{Z}$ , valgono i seguenti fatti:

$$(i) [x^n, y^m] = 1;$$

$$(ii) (xy)^n = x^n y^n.$$

**Dimostrazione:** La (i) per  $n = -1$  e  $m = 1$  e per  $n = m = -1$  e cioè

$$[x^{-1}, y] = 1 \quad (1.27)$$

e

$$[x^{-1}, y^{-1}] = 1 \quad (1.28)$$

seguono facilmente da  $[x, y] = 1$  e sono lasciate come semplice verifica.

Per dimostrare la (i) supponiamo prima  $n \in \mathbb{N}$  e lavoriamo per induzione su  $n$ . La base dell'induzione è chiara: se  $n = 0$  allora  $[x^0, y^m] = [1, y^m] = 1$ . Supponiamo che la (i) sia vera per tutti i naturali strettamente minori di  $n \geq 1$ . In particolare

$$[x^{n-1}, y^m] = 1 \quad (1.29)$$

e

$$[x, y^m] = 1 \quad (1.30)$$

Allora

$$x^n y^m = x x^{n-1} y^m = x y^m x^{n-1} = y^m x x^{n-1} = y^m x^n,$$

dove nella seconda uguaglianza si è usata la (1.29), nella terza la (1.30) e nella prima e ultima la (1) della Proposizione 1.3.22. La (i) è quindi dimostrata quando  $n \in \mathbb{N}$ .

Se  $n < 0$  allora essendo  $-n > 0$  possiamo scrivere

$$x^n y^m = (x^{-1})^{-n} y^m = y^m (x^{-1})^{-n} = y^m x^n,$$

dove nella seconda uguaglianza abbiamo usato la (1.27).

Per dimostrare la (ii), supponiamo  $n \in \mathbb{N}$  e lavoriamo per induzione su  $n$ . Se  $n = 0$ :  $(xy)^0 = 1 = 1 \cdot 1 = x^0 y^0$ . Supponiamo la (ii) valga per  $n - 1$  e cioè  $(xy)^{n-1} = x^{n-1} y^{n-1}$ . Allora

$$(xy)^n = (xy)^{n-1} xy = x^{n-1} y^{n-1} xy = x^{n-1} x y^{n-1} y = x^n y^n,$$

dove nella prima e nell'ultima uguaglianza abbiamo usato la (1) della Proposizione 1.3.22 e nella terza uguaglianza abbiamo usato  $[x, y^{n-1}] = 1$  la cui validità segue dalla (i). Se  $n < 0$  allora

$$(xy)^n = ((xy)^{-1})^{-n} = (x^{-1} y^{-1})^{-n} = (x^{-1})^{-n} (y^{-1})^{-n} = x^n y^n,$$

dove nella seconda uguaglianza abbiamo usato la (1.28) e nella terza la (ii) per  $-n > 0$ .  $\square$



**Osservazione 1.3.26** In un gruppo abeliano  $G$  le (i) e (ii) valgono per ogni coppia di elementi e in effetti si dimostra che se  $x_1, \dots, x_k, x_j \in G$  e  $[x_l, x_m] = 1$  per ogni  $l, m = 1, \dots, k$ , allora

$$(x_1 \cdots x_k)^n = x_1^n \cdots x_k^n. \quad (1.31)$$

**Osservazione 1.3.27** Se in gruppo  $G$  vale che

$$(xy)^2 = x^2y^2$$

per ogni coppia di elementi  $x, y \in G$ . Allora il gruppo è abeliano. Infatti

$$xyxy = (xy)^2 = x^2y^2 = xxyy$$

e cancelando  $x$  a sinistra e  $y$  a destra si ottiene  $xy = yx$ . Essendo  $x$  e  $y$  arbitrari segue che il gruppo è abeliano. Viene spontaneo chiedersi: se in gruppo  $G$  vale

$$(xy)^3 = x^3y^3, \quad (1.32)$$

per ogni coppia di elementi  $x, y \in G$ . Possiamo affermare che il gruppo  $G$  è abeliano? La risposta è negativa in generale (si veda l'Esercizio 1.8).

Concludiamo questo paragrafo (e questo capitolo) definendo l'ordine di un elemento in un gruppo e le sue principali proprietà.

Sia dunque  $G$  un gruppo e sia  $x \in G$ .

Consideriamo l'insieme

$$A_x = \{n \in \mathbb{N}^+ \mid x^n = 1\}.$$

Se  $A_x \neq \emptyset$  allora, per il principio del buon ordinamento, esiste  $o(x) \in \mathbb{N}^+$  tale che  $o(x)$  è il più piccolo naturale tale che

$$x^{o(x)} = 1.$$

**Definizione 1.3.28** Sia  $A_x \neq \emptyset$ . Chiameremo  $o(x)$  l'ordine dell'elemento  $x$ . Se invece  $A_x = \emptyset$  diremo che l'ordine di  $x$  è infinito e scriveremo  $o(x) = \infty$ .

**Esempio 1.3.29** Se  $G = (\mathbb{Z}, +, 0)$  e  $x \in \mathbb{Z}$ . Allora  $o(x) = \infty$  per ogni  $x \neq 0$ . Mentre  $o(x) = 1$  se  $x = 0$ .

**Esempio 1.3.30** Se  $G = (\mathbb{Z}_m, +, [0]_m)$ . Allora  $o([1]_m) = m$ .

**Osservazione 1.3.31** In un gruppo arbitrario  $o(x) = 1$  se e solo se  $x = 1$ .

**Osservazione 1.3.32** Se  $G$  ha ordine finito, allora  $o(x) < \infty$  per ogni  $x \in G$ . Infatti l'applicazione

$$f : \mathbb{N}^+ \rightarrow G, d \mapsto x^d$$

non può essere iniettiva ed esistono quindi  $u, v \in \mathbb{N}^+, u > v$  tali che  $x^u = x^v$ . Se  $u = v + n, n \in \mathbb{N}^+$ , possiamo scrivere  $x^u = x^{v+n} = x^v$  da cui  $x^n = 1$  e quindi l'insieme  $A_x \neq \emptyset$ .

Ricordiamo che il massimo comun divisore tra due interi  $a$  e  $b$  si denota con  $(a, b)$ .

**Proposizione 1.3.33** Sia  $G$  un gruppo,  $x \in G$  tale che  $o(x) = m \in \mathbb{N}^+$ . Allora

- (i)  $x^k = 1$  se e solo se  $m \mid k$ ;
- (ii)  $x^k = x^n$  se e solo se  $n - k \equiv 0 \pmod{m}$ ;
- (iii)  $o(x^k) = \frac{m}{(m, k)}$ ;
- (iv)  $o(x^{-1}) = m$ .

**Dimostrazione:** dimostrazione della (i): se  $m \mid k$  allora  $k = mq, q \in \mathbb{Z}$ . Quindi

$$x^k = x^{mq} = (x^m)^q = 1^q = 1$$

Viceversa, se supponiamo  $x^k = 1$ . Per la divisione euclidea possiamo scrivere

$$k = mq + r, 0 \leq r < m.$$

Segue che

$$x^k = x^{mq+r} = x^{mq}x^r = (x^m)^q x^r 1 \cdot x^r = x^r.$$

Essendo  $m = o(x)$  il più piccolo naturale positivo tale che  $x^m = 1$  si ottiene  $r = 0$  e quindi  $k = mq$ , ossia  $m \mid k$ .

Dimostrazione della (ii):  $x^k = x^n$  se e solo se  $x^{k-n} = 1$ . Quindi, per la (i),  $m \mid k - n$  e quindi la tesi.

Dimostrazione della (iii): siano  $s := o(x^k)$  e  $d = (m, k)$ . Quindi  $d \mid m$  e  $d \mid k$ , ossia  $m = dm_1$  e  $k = dk_1$ . Inoltre  $(m_1, k_1) = 1$ . La dimostrazione sarà conclusa se mostriamo che  $m_1 = s$ . Sfruttando prima la condizione che  $(x^k)^s = 1$  si ottiene

$$1 = (x^k)^s = x^{ks} = x^{dk_1s}$$

Per la (i) segue che  $m = dm_1 \mid dk_1s$ , cioè  $m_1 \mid k_1s$ . Essendo  $(m_1, k_1) = 1$  si ottiene

$$m_1 \mid s. \tag{1.33}$$

D'altra parte

$$(x^k)^{m_1} = x^{km_1} = x^{dk_1m_1} = x^{dm_1k_1} = x^{mk_1} = (x^m)^{k_1} = 1^{k_1} = 1.$$

Sempre dalla (i) si deduce che

$$s \mid m_1. \quad (1.34)$$

Mettendo insieme le (1.33) e la (1.34) si ottiene  $s = m_1$ . La (iv) segue dalla (iii) per  $k = -1$ .  $\square$

**Esempio 1.3.34** Calcoliamo l'ordine di  $[15]_{24}$  in  $\mathbb{Z}_{24}$ . Osserviamo che  $o([1]_{24}) = 24$  e  $[15]_{24} = 15[1]_{24}$ . Dalla (iii) della Proposizione 1.3.25 si deduce dunque che:

$$o([15]_{24}) = \frac{24}{(15, 24)} = \frac{24}{3} = 8.$$

**Esempio 1.3.35** Calcoliamo l'ordine di  $[4]_9$  in  $U(\mathbb{Z}_9, \cdot)$ . Osserviamo

$$U(\mathbb{Z}_9) = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$$

$([2]_9)^2 = [4]_9$ ,  $([2]_9)^3 = [8]_9$ ,  $([2]_9)^4 = [7]_9$ ,  $([2]_9)^5 = [5]_9$ ,  $([2]_9)^6 = [1]_9$  quindi  $o([2]_9) = 6$ . Analogamente si verifica facilmente o con un calcolo diretto che  $o([4]_9) = 3$ , oppure suando la (iii) della Proposizione 1.3.25

$$o([4]_9) = o([2]_9^2) = \frac{6}{(6, 2)} = \frac{6}{2} = 3.$$

## 1.4 Esercizi

**Esercizio 1.1** Si dica quali delle seguenti operazioni binarie sull'insieme indicato é associativa e commutativa. Si dica inoltre per quali di queste operazioni esiste un elemento neutro e quali  $x \in \mathbb{R}$  sono invertibili. In particolare si identifichino i semigrupp, i monoidi e i gruppi.

1.  $x \cdot y = x + y + k$ ,  $x, y \in \mathbb{R}$  e  $k \in \mathbb{R}$  una costante fissata;
2.  $x \cdot y = \sqrt{x^2 + y^2}$ ,  $x, y \in \mathbb{R}$ ;
3.  $x \cdot y = |x + y|$ ,  $x, y \in \mathbb{R}$ ;
4.  $x \cdot y = x - y$ ,  $x, y \in \mathbb{R}$ ;
5.  $x \cdot y = \max\{x, y\}$ ,  $x, y \in \mathbb{R}$ ;
6.  $x \cdot y = \frac{xy}{2}$ ,  $x, y \in \mathbb{R}^*$ ;

$$7. x \cdot y = x + y + xy, x \in \mathbb{R} \setminus \{-1\};$$

$$8. x \cdot y = \frac{x+y}{x+y+1}, x \in (0, 1) = \{x \in \mathbb{R} \mid 0 < x < 1\}.$$

**Esercizio 1.2** Sia  $G$  il prodotto cartesiano  $\mathbb{Q} \times \mathbb{Z}^*$ . Definiamo un'operazione su  $G$  nel modo seguente:

$$(q, m) \cdot (q', m') = (q + mq', mm').$$

Si provi che  $(G, \cdot)$  é un monoide e si calcolino gli elementi invertibili. Si dica se  $G$  é un gruppo e se  $G$  é abeliano.

**Esercizio 1.3** Sia  $G$  il prodotto cartesiano  $\mathbb{Q}^* \times \mathbb{Q}$ . Definiamo un'operazione su  $G$  nel modo seguente:

$$(a, b) \cdot (a', b') = (aa', ab' + \frac{b}{a'}).$$

Si provi che  $G$  é un gruppo e si dica se  $G$  é abeliano.

**Esercizio 1.4** Si dica quali delle seguenti applicazioni definisce un'operazione binaria e quale di queste definisce un'operazione di gruppo sull'insieme indicato.

1.  $(a, b) \cdot (c, d) = (ad + bc, bd)$  su  $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid y \neq 0\}$ ;
2.  $(a, b) \cdot (c, d) = (ac, bc + d)$  su  $\{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x \neq 0\}$ ;
3.  $(a, b) \cdot (c, d) = (ac, bc + d)$  su  $\mathbb{R} \times \mathbb{R}$ ;
4.  $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$  su  $\mathbb{R}^* \times \mathbb{R}^*$ ;
5.  $(a, b) \cdot (c, d) = (ac - bd, ad + bc)$  su  $\mathbb{R} \times \mathbb{R}$ .

**Esercizio 1.5** Sia  $A = \{a, b\}$  un insieme con due elementi. Descrivere tutte le operazioni binarie su  $A$ . In particolare si dica quali di queste operazioni é commutativa e associativa. Si dica inoltre per quali di queste operazioni esiste un elemento neutro e quali elementi di  $A$  sono invertibili. Mostrare infine che ci sono 8 strutture di semigrupp di cui 6 non abeliane e 2 abeliane e che di queste solo 2 risultano un gruppo.

**Esercizio 1.6** Sia  $(M, \cdot, 1)$  un monoide e sia  $S$  un sottoinsieme di  $M$  tale che  $(S, \cdot)$  risulta un semigrupp e  $1 \notin S$ . Si puó affermare che  $(S, \cdot)$  non é un monoide?

**Esercizio 1.7** Sia  $G$  un gruppo finito e sia  $S$  l'insieme degli elementi di  $G$  diversi dal proprio inverso  $S = \{x \in G \mid x \neq x^{-1}\}$ . Dimostrare che:

1.  $S$  ha un numero pari di elementi;
2.  $|G| \equiv |G \setminus S| \pmod{2}$ ;
3. se  $G$  ha un numero pari di elementi allora esiste  $x \in G \setminus S, x \neq 1$  (quindi un gruppo di ordine pari ha almeno un elemento di ordine 2).

**Esercizio 1.8**

1. Sia  $G$  il gruppo costituito dalle matrici a entrate in  $\mathbb{Z}_3$  della forma

$$\begin{bmatrix} [1]_3 & [a]_3 & [b]_3 \\ 0 & [1]_3 & [c]_3 \\ 0 & 0 & [1]_3 \end{bmatrix}$$

Si dimostri che  $G$  è un gruppo non abeliano dove tutti gli elementi diversi dall'elemento neutro hanno ordine 3.

2. Sia  $G$  un gruppo che non ha elementi di ordine 3. Supponiamo che

$$(xy)^3 = x^3y^3, \forall x, y \in G. \quad (1.35)$$

Dimostrare che  $G$  è abeliano.

(Suggerimento per la seconda parte: si osservi che

$$[x, y]^3 = ((xyx^{-1})y^{-1})^3 \stackrel{(1.35)}{=} xy^3x^{-1}y^{-3} = [x, y^3], \forall x, y \in G \quad (1.36)$$

e che

$$xy^3x^{-1} = (xyx^{-1})^3 = ((xy)x^{-1})^3 \stackrel{(1.35)}{=} (xy)^3x^{-3} \stackrel{(1.35)}{=} x^3y^3x^{-3}, \forall x, y \in G$$

dalla quale segue

$$[x^2, y^3], \forall x, y \in G, \quad (1.37)$$

la quale ci dice che i quadrati sono permutabili con tutti i cubi. Dalla (1.8) e dalla (1.36) si ottiene dunque

$$[x^2, y], \forall x, y \in G, \quad (1.38)$$

la quale ci dice che i quadrati sono permutabili con ogni elemento del gruppo. Dalla (1.36) e dalla (1.37) si ottiene

$$[x, y]^3 = [x, y^3] = xy^3x^{-1}y^{-3} = xyx^{-1}y^{-1} = [x, y], \forall x, y \in G$$

e quindi

$$\begin{aligned} 1 &= [x, y]^2 = xyx^{-1}y^{-1}xyx^{-1}y^{-1} \stackrel{(1.37)}{=} xyxyxyx^{-3}y^{-3} = (xy)^3x^{-3}y^{-3} \stackrel{(1.35)}{=} \\ &= x^3y^3x^{-3}y^{-3} \stackrel{(1.38)}{=} xyx^{-1}y^{-1} = [x, y]. \end{aligned}$$

**Esercizio 1.9** Sia  $n \in \mathbb{N}_+$  e  $p$  un primo. Si dimostri che

$$|GL_n(\mathbb{Z}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}).$$

(Suggerimento: le righe di una matrice di  $GL_n(\mathbb{Z}_p)$  sono linearmente indipendenti. Quindi la prima riga  $r_1$  di una tale matrice può essere qualsiasi cosa tranne il vettore nullo, quindi ci sono  $p^n - 1$  possibilità per la prima riga. Per ognuna di queste possibilità, la seconda riga  $r_2$  può essere qualsiasi cosa tranne un multiplo della prima riga, il che dà  $p^n - p$  possibilità. Per qualsiasi scelta di  $r_1$  e  $r_2$  delle prime due righe, la terza riga può essere qualsiasi cosa tranne una combinazione lineare di  $r_1$  e  $r_2$ . Il numero di combinazioni lineari  $\lambda_1 r_1 + \lambda_2 r_2$  è  $p^2$  cioè il numero di scelte per la coppia  $\lambda_1$  e  $\lambda_2$ . Ne consegue che per ogni  $r_1$  e  $r_2$  ci sono  $p^n - p^2$  possibilità per la terza riga. Procedendo allo stesso modo sulle rimanenti righe si ottiene il risultato).

**Esercizio 1.10** Dieci uomini vengono condannati a morte e rinchiusi nella stessa cella la notte precedente all'esecuzione. Gli viene data però una possibilità per salvarsi la vita. La mattina dell'esecuzione i dieci condannati verranno messi in fila indiana e verrà messo sulla testa di ognuno di essi un cappello di colore o bianco o nero. Nessuno dei condannati potrà vedere il colore del proprio cappello (quello che ha nella propria testa) ma solo, eventualmente, quello dei condannati che si trovano di fronte a lui. Per salvarsi, ognuno di loro, a turno potrà dire la parola "nero" oppure la parola "bianco". Se la parola detta da un condannato corrisponde al colore del proprio cappello allora il condannato sarà graziato e quindi liberato. In caso contrario sarà ucciso. Quale è la strategia che i dieci condannati dovranno escogitare la notte prima dell'esecuzione per essere sicuri che almeno 9 di loro siano graziati? Generalizzare a  $n$  condannati e  $k$  colori.

## Capitolo 2

### Due gruppi importanti: $D_n$ e $S_n$

Questo capitolo è dedicato a due gruppi di ordine finito che rivestono un ruolo importante nella teoria dei gruppi: il gruppo diedrale e il gruppo simmetrico.

#### 2.1 Il gruppo diedrale

Sia  $n \geq 3$  e sia  $P_n$  un poligono regolare di  $n$  lati in un piano euclideo  $\mathcal{E}$ . Consideriamo l'insieme  $D_n$  costituito dalle isometrie  $f$  di  $\mathcal{E}$  che lasciano invariato  $P_n$ , cioè  $f(P_n) = P_n$ .

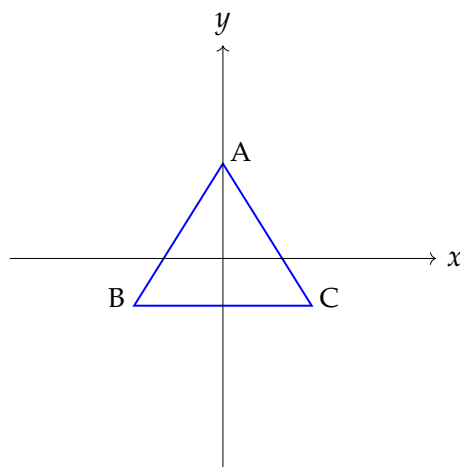
Possiamo allora definire un'operazione binaria associativa su  $D_n$  data dalla composizione ( $f \circ g$ , per ogni  $f, g \in D_n$ ) che rende  $D_n = (D_n, \circ, 1)$  un monoide, dove 1 denota l'applicazione identità da  $\mathcal{E}$  in se stesso.

Essendo le isometrie di  $\mathcal{E}$  applicazioni invertibili deduciamo anche che  $D_n$  è un gruppo, chiamato il *gruppo diedrale*. Infatti l'inverso  $f^{-1}$  di un isometria  $f$  di  $\mathcal{E}$  soddisfa  $f^{-1}(P_n) = P_n$ .

Per capire meglio la natura del gruppo diedrale  $D_n$ , analizziamo in dettaglio i casi  $n = 3$  e  $n = 4$ .

#### Il gruppo $D_3$

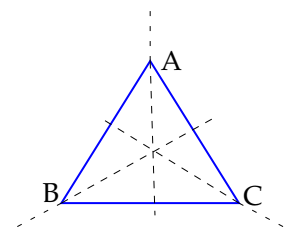
In questo caso il poligono regolare  $P_3$  è un triangolo equilatero di vertici  $A$ ,  $B$  e  $C$  che possiamo pensare centrato nell'origine degli assi di un sistema di riferimento cartesiano e tale che il vertice  $A$  appartenga all'asse positiva delle ordinate.



Le isometrie distinte del piano che fissano il triangolo sono 6:

- l'applicazione identica, denotata con 1;
- la rotazione  $r_{\frac{2\pi}{3}}$  in senso antiorario intorno all'origine di angolo  $\frac{2\pi}{3} = 120^\circ$ ;
- la rotazione  $r_{\frac{4\pi}{3}}$  in senso antiorario intorno all'origine di angolo  $\frac{4\pi}{3} = 240^\circ$ ;
- la riflessione  $s_A$  rispetto alla bisettrice dell'angolo  $A$ ;
- la riflessione  $s_B$  rispetto alla bisettrice dell'angolo  $B$ ;
- la riflessione  $s_C$  rispetto alla bisettrice dell'angolo  $C$ .

Le bisettrici sono rappresentati in figura.



Quindi  $D_3$  è un gruppo di ordine 6. Se indichiamo con  $r = r_{\frac{2\pi}{3}}$  allora  $r_{\frac{4\pi}{3}} = r^2 = r \circ r$ ,  $r^3 = r \circ r \circ r = 1$  (osserviamo che le rotazioni in senso antiorario di angolo  $\frac{\pi}{3}$  e  $\frac{4\pi}{3}$  sono date rispettivamente da  $r^2$  e  $r$ ). Possiamo quindi scrivere

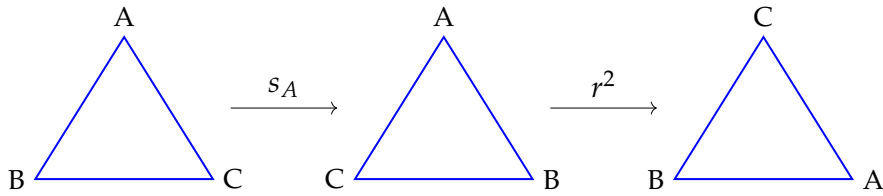
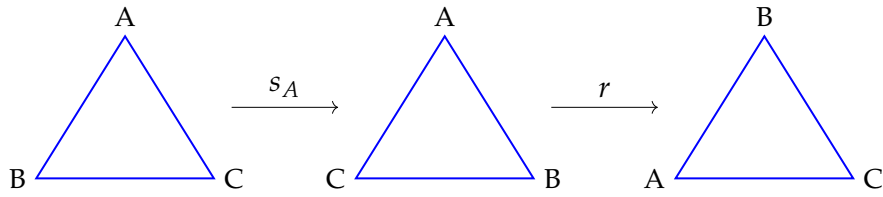
$$D_3 = \{1, r, r^2, s_A, s_B, s_C\}$$



Vediamo più a fondo la struttura di gruppo. Chiaramente

$$r^3 = s_A^2 = s_B^2 = s_C^2 = 1.$$

Quindi  $r$  ha ordine 3 e le riflessioni hanno ordine 2. Si può facilmente verificare che  $r \circ s_A = s_C$ ,  $r^2 \circ s_A = s_B$ , come mostrato dai seguenti disegni:



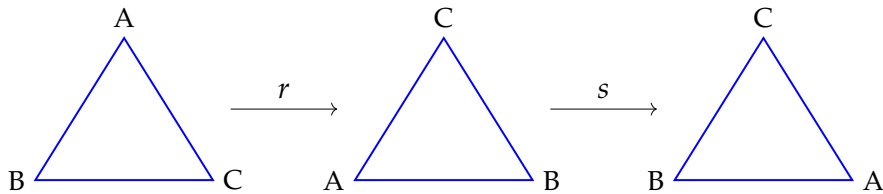
Possiamo quindi esprimere gli elementi di  $D_3$  in funzione di  $r$  e di  $s := s_A$  come

$$D_3 = \{1, r, r^2, s, r \circ s, r^2 \circ s\}$$

Osserviamo anche che la rotazione  $r$  e la riflessione  $s$  non commutano. Più precisamente

$$s \circ r = r^2 \circ s = s_B, \quad (2.1)$$

come si evince dal seguente disegno e da quello precedente:



Quindi  $D_3$  è un gruppo non abeliano. Usando la relazione (2.1) possiamo quindi calcolare i prodotti in  $D_3$

Per esempio

$$s \circ r^2 = s \circ r \circ r = r^2 \circ s \circ r = r^4 \circ s = r \circ s$$

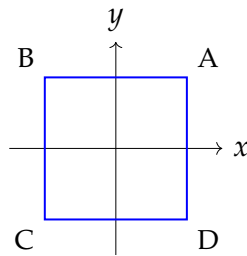
e analogamente per gli altri elementi.

Si ottiene quindi facilmente la seguente tavola moltiplicativa per il gruppo  $D_3$ .

$\cdot$	1	$r$	$r^2$	$s$	$rs$	$r^2s$
1	1	$r$	$r^2$	$s$	$rs$	$r^2s$
$r$	$r$	$r^2$	1	$rs$	$r^2s$	$s$
$r^2$	$r^2$	1	$r$	$r^2s$	$s$	$rs$
$s$	$s$	$r^2s$	$rs$	1	$r^2$	$r$
$rs$	$rs$	$s$	$r^2s$	$r$	1	$r^2$
$r^2s$	$r^2s$	$rs$	$s$	$r^2$	$r$	1

### Il gruppo $D_4$

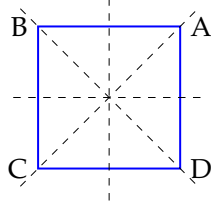
In questo caso il poligono regolare  $P_4$  è un quadrato di vertici  $A, B, C$  e  $D$  come in figura, che possiamo pensare centrato nell'origine degli assi di un sistema di riferimento cartesiano  $xy$  e simmetrico rispetto all'asse delle ordinate.



Le isometrie distinte del piano che fissano il quadrato sono 8:

- l'applicazione identica, denotata con 1;
- la rotazione  $r_{\frac{\pi}{2}}$  in senso antiorario intorno all'origine di angolo  $\frac{\pi}{2}$ ;
- la rotazione  $r_{\pi}$  in senso antiorario intorno all'origine di angolo  $\pi$ ;
- la rotazione  $r_{\frac{3\pi}{2}}$  in senso antiorario intorno all'origine di angolo  $\frac{3\pi}{2}$ ;
- la riflessione  $s_{AC}$  rispetto alla diagonale  $AC$ ;
- la riflessione  $s_{BD}$  rispetto alla diagonale  $BD$ ;
- la riflessione  $s_x$  rispetto all'asse delle ascisse;
- la riflessione  $s_y$  rispetto all'asse delle ordinate.

Gli assi di simmetria sono rappresentati come segue.



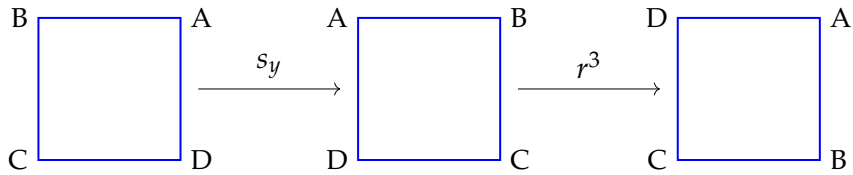
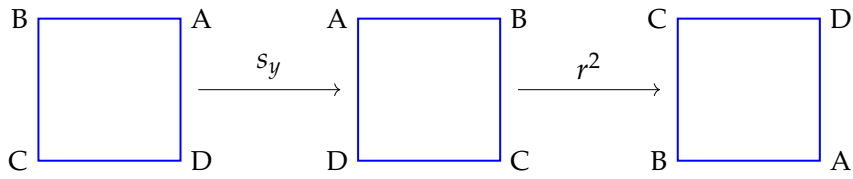
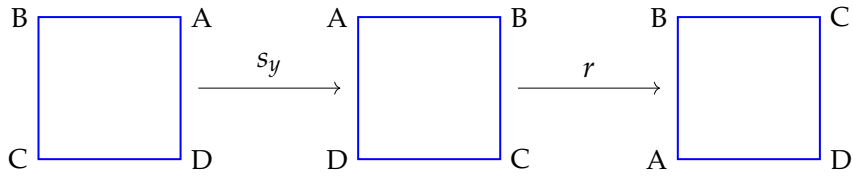
Quindi  $D_4$  è un gruppo di ordine 8. Se indichiamo con  $r = r_{\frac{\pi}{2}}$  allora  $r_{\pi} = r^2$ ,  $r^3 = r_{\frac{3\pi}{2}}$  e  $r^4 = 1$ . Possiamo quindi scrivere

$$D_4 = \{1, r, r^2, r^3, s_{AC}, s_{BD}, s_x, s_y\}$$

Osserviamo che

$$r^4 = s_{AC}^2 = s_{BD}^2 = s_x^2 = s_y^2 = 1$$

e che  $r \circ s_y = s_{BD}$ ,  $r^2 \circ s_y = s_x$ ,  $r^3 \circ s_y = s_{AC}$  come mostrano i seguenti disegni:



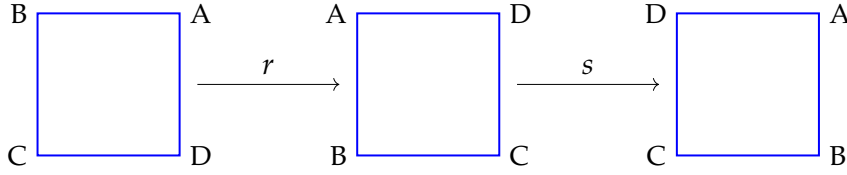
Possiamo quindi esprimere gli elementi di  $D_4$  in funzione di  $r$  e di  $s := s_y$  come

$$D_4 = \{1, r, r^2, r^3, s, r \circ s, r^2 \circ s, r^3 \circ s\}$$

Osserviamo anche che la rotazione  $r$  e la riflessione  $s$  non commutano. Più precisamente

$$s \circ r = r^3 \circ s = s_{AC}, \quad (2.2)$$

come si evince dal seguente disegno e dal disegno precedente:



Quindi  $D_4$  è un gruppo non abeliano. Usando la relazione (2.2) possiamo quindi calcolare i prodotti in  $D_4$  e ottenere la seguente tavola moltiplicativa per questo gruppo.

$\cdot$	1	$r$	$r^2$	$r^3$	$s$	$rs$	$r^2s$	$r^3s$
1	1	$r$	$r^2$	$r^3$	$s$	$rs$	$r^2s$	$r^3s$
$r$	$r$	$r^2$	$r^3$	1	$rs$	$r^2s$	$r^3s$	$s$
$r^2$	$r^2$	$r^3$	1	$r$	$r^2s$	$r^3s$	$s$	$rs$
$r^3$	$r^3$	1	$r$	$r^2$	$r^3s$	$s$	$rs$	$r^2s$
$s$	$s$	$r^3s$	$r^2s$	$rs$	1	$r^3$	$r^2$	$r$
$rs$	$rs$	$s$	$r^3s$	$r^2s$	$r$	1	$r^3$	$r^2$
$r^2s$	$r^2s$	$rs$	$s$	$r^3s$	$r^2$	$r$	1	$r^3$
$r^3s$	$r^3s$	$r^2s$	$rs$	$s$	$r^3$	$r^2$	$r$	1

## Il caso generale

Assumiamo che il poligono regolare  $P_n$  sia centrato nell'origine di un sistema di riferimento cartesiano. Come osservato nei casi  $n = 3$  e  $n = 4$  gli assi di simmetria del poligono  $P_n$  sono disposti in maniera diversa, a seconda che il numero dei suoi lati sia pari (metà degli assi passano per i vertici opposti e metà passano per il centro dei lati opposti) oppure dispari (ogni asse passa per un vertice e il centro del lato opposto). Ovviamente tutti gli assi di simmetria passano per l'origine.

Quindi

$$D_n = \{1, r, \dots, r^{n-1}, s_1, \dots, s_n\},$$

dove  $r$  è la rotazione intorno all'origine in senso antiorario di angolo  $\frac{2\pi}{n}$ ,  $r^n = 1$  e  $s_h$ ,  $h = 1, \dots, n$  è la riflessione rispetto al  $h$ -esimo asse di simmetria del

poligono,  $s_h^2 = 1$ . Dunque  $D_n$  è un gruppo di ordine  $2n$ . Il seguente lemma segue dai corsi di geometria (si veda anche l'Osservazione 2.1.5).

**Lemma 2.1.1** *Sia  $O$  un punto fissato del piano. Sia  $\mathcal{R}$  l'insieme delle rotazioni piane intorno a  $O$  e sia  $\mathcal{S}$  l'insieme delle riflessioni piane rispetto a rette passanti per  $O$ . Allora*

1.  $r_1 \circ r_2 \in \mathcal{R}, \forall r_1, r_2 \in \mathcal{R};$
2.  $s \circ t \in \mathcal{R}, \forall s, t \in \mathcal{S};$
3.  $r \circ s \in \mathcal{S}, s \circ r \in \mathcal{S}, \forall r \in \mathcal{R}, \forall s \in \mathcal{S}.$

*A parole: la composizione di due rotazioni o di due riflessioni è una rotazione, mentre la composizione di una riflessione e di una rotazione o di una rotazione e di una riflessione è una riflessione.*

**Teorema 2.1.2**  $D_n, n \geq 3$  è un gruppo non abeliano di ordine  $2n$ . Sia  $s$  una qualunque riflessione in  $D_n$ , allora

$$D_n = \{1, r, \dots, r^{n-1}, s, r \circ s, \dots, r^{n-1} \circ s\}. \quad (2.3)$$

Inoltre,

$$s \circ r = r^{n-1} \circ r. \quad (2.4)$$

**Dimostrazione:** Abbiamo già osservato che  $D_n$  è un gruppo con  $2n$  elementi. Per il lemma precedente,  $\{r, \dots, r^{n-1}\}$  sono tutte rotazioni distinte e conseguentemente  $r^k \circ s$  sono  $n$  riflessioni distinte per  $k = 1, \dots, n-1$ . Segue che  $\{s, r \circ s, \dots, r^{n-1} \circ s\} = \{s_1, \dots, s_n\}$  e quindi vale la (2.3). Osserviamo ora che  $s \circ r$  è una riflessione per il Lemma 2.1.1. Quindi

$$s \circ r \circ s \circ r = (s \circ r)^2 = 1$$

che implica  $s \circ r = r^{-1} \circ s^{-1} = r^{n-1} \circ s$  ossia la (2.4) la quale mostra anche che  $D_n$  non è abeliano.  $\square$

Per induzione su  $n$  dalla (2.4) si ottiene facilmente il seguente corollario

**Corollario 2.1.3** *Siano  $r$  e  $s$  come nel Teorema 2.1.2. Allora*

$$s \circ r^{n-k} = r^k \circ s, \forall k = 1, \dots, n-1. \quad (2.5)$$

**Notazione 2.1.4** Per esprimere in maniera concisa il gruppo diedrale si usa la notazione

$$D_n = \langle r, s \mid r^n = s^2 = 1, sr = r^{n-1}s \rangle$$

che viene chiamata una *presentazione* del gruppo diedrale con *generatori*  $r$  e  $s$  (non tratteremo le presentazioni di gruppi in queste note). Questa scrittura significa semplicemente che gli elementi del gruppo  $D_n$  si ottengono moltiplicando gli elementi di  $r$  e di  $s$  e tenendo conto del fatto che  $r$  ha ordine  $n$ ,  $s$  ha ordine 2 e che vale la relazione  $sr = r^{n-1}s = r^{-1}s$ .

**Osservazione 2.1.5** Sia  $P_n$  un poligono regolare inscritto nella circonferenza unitaria e simmetrico rispetto all'asse delle ascisse. Sia  $r$  la rotazione di angolo  $\frac{2\pi}{n}$  in senso antiorario rispetto all'origine; allora

$$r^k = \begin{bmatrix} \cos \frac{2\pi k}{n} & -\sin \frac{2\pi k}{n} \\ \sin \frac{2\pi k}{n} & \cos \frac{2\pi k}{n} \end{bmatrix}, \quad k = 1, \dots, n-1.$$

Le  $n$  riflessioni del gruppo diedrale si descrivono in modo uniforme come riflessioni rispetto alle rette che formano un angolo  $\alpha = \frac{h\pi}{n}$  con l'asse positivo delle ascisse, per  $h = 0, 1, \dots, n-1$ . Ponendo  $s_h := s_{\frac{h\pi}{n}}$ , si ha

$$s_h = \begin{bmatrix} \cos \frac{2\pi h}{n} & \sin \frac{2\pi h}{n} \\ \sin \frac{2\pi h}{n} & -\cos \frac{2\pi h}{n} \end{bmatrix}, \quad h = 0, 1, \dots, n-1.$$

Scegliamo in particolare

$$s := s_0 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

cioè la riflessione rispetto all'asse delle ascisse. Con questa scelta, le relazioni fondamentali del gruppo diedrale (come, ad esempio,  $r^n = I$ ,  $s^2 = I$  e  $srs = r^{-1}$ ) si verificano direttamente per moltiplicazione di matrici.

Più in generale, per  $\alpha \in \mathbb{R}$  la rotazione  $r_\alpha$  in senso antiorario intorno all'origine di angolo  $\alpha$  è data da

$$r_\alpha = \begin{bmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{bmatrix},$$

mentre la riflessione  $s_\alpha$  rispetto alla retta passante per l'origine che forma un angolo  $\alpha$  con l'asse positivo delle ascisse è

$$s_\alpha = \begin{bmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{bmatrix}.$$

Usando le usuali identità trigonometriche si ottengono facilmente le seguenti composizioni:

1.  $r_\alpha \circ r_\beta = r_{\alpha+\beta}$  (in particolare  $r_\alpha r_\beta = r_\beta r_\alpha$ );
2.  $s_\alpha \circ s_\beta = r_{2(\alpha-\beta)}$  (quindi  $s_\beta \circ s_\alpha = r_{2(\beta-\alpha)}$ );
3.  $r_\alpha \circ s_\beta = s_{\beta+\frac{\alpha}{2}}$  e simmetricamente  $s_\beta \circ r_\alpha = s_{\beta-\frac{\alpha}{2}}$ .

## 2.2 Il gruppo delle permutazioni

Sia  $X$  un insieme non vuoto. Definiamo

$$S_X = \{f : X \rightarrow X \mid f \text{ è invertibile}\}$$

e consideriamo l'operazione binaria  $\circ$  su  $S_X$ , data dalla composizione di funzioni. Si tratta effettivamente di un'operazione binaria, in quanto la composizione di due funzioni invertibili è ancora invertibile. Inoltre, è immediato verificare che  $(S_X, \circ, \text{id}_X)$  risulta essere un gruppo, chiamato *gruppo delle permutazioni* dell'insieme  $X$ . Usando la notazione del capitolo precedente possiamo scrivere che  $U((X^X, \circ)) = S_X$ . Nel caso in cui  $X$  sia finito con  $|X| = n \in \mathbb{N}^+$ , indicheremo  $S_X$  con  $S_n$ , chiamato anche *gruppo simmetrico su  $n$  elementi*. Il suo ordine è  $|S_n| = n!$ . Osserviamo che se  $|X| \geq 3$ , allora  $S_X$  è un gruppo non abeliano. Infatti, se  $x, y, z \in X$  sono tre elementi distinti, le due permutazioni  $f, g \in S_X$ , definite come segue:

$$f(x) = y, \quad f(y) = x, \quad f(t) = t \text{ per ogni } t \neq x, y$$

e

$$g(x) = z, \quad g(z) = x, \quad g(t) = t \text{ per ogni } t \neq x, z$$

non commutano tra loro. Infatti, abbiamo:

$$(f \circ g)(x) = f(g(x)) = f(z) = z, \quad \text{mentre} \quad (g \circ f)(x) = g(f(x)) = g(y) = y$$

e poiché  $y \neq z$ , concludiamo che  $f \circ g \neq g \circ f$ .

Dato  $f \in S_X$ , definiamo il *supporto* di  $f$  come

$$\text{supp}(f) = \{x \in X \mid f(x) \neq x\},$$

ovvero il sottoinsieme di  $X$  costituito dagli elementi che vengono "mossi" dalla permutazione  $f$ . Chiaramente  $\text{supp}(f) = \emptyset$  se e solo se  $f = \text{id}_X$ . Vediamo alcune proprietà del supporto.

**Proposizione 2.2.1** *Sia  $f \in S_X$ . Allora:*

1.  $\text{supp}(f^{-1}) = \text{supp}(f)$ ;
2.  $f(x) \in \text{supp}(f)$ , per ogni  $x \in \text{supp}(f)$ .

**Dimostrazione.** La (1) si dimostra sfruttando il fatto che  $f^{-1}$  è iniettiva:

$$x \in \text{supp}(f) \iff f(x) \neq x \iff x = f^{-1}(f(x)) \neq f^{-1}(x) \iff x \in \text{supp}(f^{-1}).$$

Per dimostrare la (2), supponiamo per assurdo che esista  $x \in \text{supp}(f)$  tale che  $f(x) \notin \text{supp}(f)$ . Allora  $f(f(x)) = f(x)$  e applicando l'inversa a entrambi i membri si ottiene  $f(x) = x$ , in contraddizione con il fatto che  $x \in \text{supp}(f)$ .  $\square$

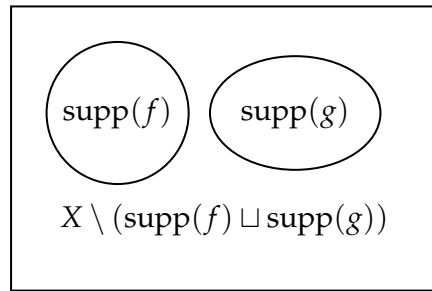
Due permutazioni  $f, g \in S_X$  si dicono *disgiunte* se

$$\text{supp}(f) \cap \text{supp}(g) = \emptyset.$$

**Proposizione 2.2.2** Se  $f, g \in S_X$  sono disgiunte, allora  $f$  e  $g$  commutano tra loro.

**Dimostrazione.** Scriviamo  $X$  come unione di tre insiemi disgiunti:

$$X = \text{supp}(f) \sqcup \text{supp}(g) \sqcup (X \setminus (\text{supp}(f) \sqcup \text{supp}(g))).$$



Consideriamo i seguenti casi:

- Se  $x \in \text{supp}(f)$ , allora:

$$(g \circ f)(x) = g(f(x)) = f(x) = f(g(x)) = (f \circ g)(x),$$

dove nella seconda e terza uguaglianza abbiamo usato il fatto che  $x, f(x) \in \text{supp}(f)$  e l'ipotesi che  $f$  e  $g$  siano disgiunte, quindi  $f(x) \notin \text{supp}(g)$  (per la (2) della Proposizione 2.2.1);

- Se  $x \in \text{supp}(g)$ , ragionando in modo analogo, otteniamo:

$$(g \circ f)(x) = (f \circ g)(x).$$

- Se  $x \in X \setminus (\text{supp}(f) \sqcup \text{supp}(g))$ , allora  $f(x) = g(x) = x$ , e quindi:

$$(g \circ f)(x) = (f \circ g)(x) = x.$$



### 2.3. I CICLI E IL TEOREMA FONDAMENTALE DELLE PERMUTAZIONI 37

Segue che  $(g \circ f)(x) = (f \circ g)(x)$  per ogni  $x \in X$ , e quindi  $f \circ g = g \circ f$ .  $\square$

Per rappresentare una permutazione  $f \in S_n$  possiamo usare una matrice  $2 \times 1$  della forma

$$f = \begin{pmatrix} 1 & 2 & \cdots & n \\ f(1) & f(2) & \cdots & f(n) \end{pmatrix},$$

dove nella prima riga compaiono i numeri da 1 a  $n$  e nella seconda riga le loro immagini tramite  $f$  (la seconda riga consiste di tutti e solo i numeri da 1 a  $n$  essendo  $f$  una bigezione).

**Esempio 2.2.3** I 6 elementi di  $S_3$  possono quindi essere descritti come segue.

$$\begin{aligned} id &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\ \tau_3 &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \end{aligned}$$

Con questa notazione possiamo anche calcolare il prodotto (composizione) di due permutazioni in modo agevole.

**Esempio 2.2.4** Siano

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}, f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} \in S_5.$$

Allora, siccome  $f(1) = 3$  e  $g(3) = 4$ , possiamo scrivere 4 come primo elemento della seconda riga; siccome  $f(2) = 2$  e  $g(2) = 3$  possiamo scrivere 3 come secondo elemento della seconda riga e così via ottenendo la permutazione

$$g \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}.$$

## 2.3 I cicli e il teorema fondamentale delle permutazioni

Sia  $f \in S_X$  e  $a \in \text{supp}(f)$ . Definiamo l'*orbita di  $a$  tramite  $f$*  come

$$\text{orb}_f(a) = \{f^j(a) \mid j \in \mathbb{Z}\}. \quad (2.6)$$

Per comprendere meglio come sia fatto questo insieme, definiamo una relazione d'equivalenza su  $X$ :

$$a \sim_f b \iff \exists j \in \mathbb{Z} \text{ tale che } b = f^j(a).$$

Si verifica immediatamente che  $\sim_f$  è effettivamente una relazione d'equivalenza:

- **Riflessività:**  $a \sim_f a$  in quanto  $a = f^0(a) = \text{id}_X(a) = a$ ;
- **Simmetria:** se  $a \sim_f b$ , allora esiste  $j \in \mathbb{Z}$  tale che  $b = f^j(a)$ , quindi  $a = f^{-j}(b)$ , cioè  $b \sim_f a$ ;
- **Transitività:** siano  $a \sim_f b$ , cioè  $b = f^j(a)$  per qualche  $j \in \mathbb{Z}$ , e  $b \sim_f c$ , cioè  $c = f^k(b)$  per qualche  $k \in \mathbb{Z}$ . Allora  $c = f^k(b) = f^k(f^j(a)) = f^{j+k}(a)$ , per cui  $a \sim_f c$ .

Si deduce allora che se  $a \in \text{supp}(f)$  si ha

$$\text{orb}_f(a) = [a]_{\sim_f},$$

dove  $[a]_{\sim_f}$  denota la classe d'equivalenza dell'elemento  $a$  rispetto alla relazione d'equivalenza  $\sim_f$ . Se il supporto di  $f$  è finito, l'orbita di un suo elemento può essere descritta come segue.

**Proposizione 2.3.1** *Sia  $f \in S_X$  tale che  $|\text{supp}(f)| < \infty$  e sia  $a \in \text{supp}(f)$ . Allora esiste un naturale  $d \geq 2$  tale che*

$$f^d(a) = a$$

e

$$\text{orb}_f(a) = \{a, f(a), f^2(a), \dots, f^{d-1}(a)\}. \quad (2.7)$$

**Dimostrazione:** Consideriamo l'applicazione

$$F : \mathbb{N}^+ \rightarrow \text{orb}_f(a) = [a]_{\sim_f}, \quad i \mapsto f^i(a).$$

Quest'applicazione non può essere iniettiva, in quanto

$$|\text{orb}_f(a)| \leq |\text{supp}(f)| < \infty = |\mathbb{N}^+|.$$

Esistono quindi  $i, j \in \mathbb{N}^+$ , con  $i > j$ , tali che  $f^i(a) = f^j(a)$ , e quindi

$$f^{i-j}(a) = a, \quad i - j > 0.$$

Segue che l'insieme

$$A := \{n \in \mathbb{N}^+ \mid f^n(a) = a\} \neq \emptyset$$

### 2.3. I CICLI E IL TEOREMA FONDAMENTALE DELLE PERMUTAZIONI 39

e, per il principio del buon ordinamento, esiste  $d \in \mathbb{N}^+$  tale che  $f^d(a) = a$  e per ogni  $h \in A$  con  $h \neq d$  si ha  $d < h$ . Segue allora che gli elementi  $a, f(a), f^2(a), \dots, f^{d-1}(a)$  sono tutti distinti e che

$$\{a, f(a), f^2(a), \dots, f^{d-1}(a)\} \subseteq \{f^j(a) \mid j \in \mathbb{Z}\} = \text{orb}_f(a)$$

(infatti, se  $f^p(a) = f^q(a)$  con  $p > q$ ,  $0 \leq p, q \leq d-1$ , allora  $f^{p-q}(a) = a$ , con  $0 < p-q \leq d-1$ , in contrasto con la minimalità di  $d$ ). Osserviamo anche che  $d \geq 2$ ; altrimenti, se  $d = 1$ , allora  $f(a) = a$ , in contrasto con la scelta di  $a \in \text{supp}(f)$ . Resta quindi da dimostrare che

$$\text{orb}_f(a) \subseteq \{a, f(a), f^2(a), \dots, f^{d-1}(a)\}.$$

Sia dunque  $f^j(a) \in \text{orb}_f(a)$ ,  $j \in \mathbb{Z}$ . Dividendo  $j$  per  $d$  possiamo scrivere

$$j = dq + r, \quad 0 \leq r \leq d-1$$

e ottenere

$$f^j(a) = f^{dq+r}(a) = f^r(f^{dq}(a)) = f^r(a) \in \{a, f(a), f^2(a), \dots, f^{d-1}(a)\},$$

il che mostra l'inclusione desiderata e conclude la dimostrazione. (Nell'ultima uguaglianza abbiamo usato il fatto che  $f^{dq}(a) = a$  per ogni  $q \in \mathbb{Z}$ . Questa si può dimostrare prima per induzione su  $q$ , supponendo  $q \in \mathbb{N}$  e usando  $f^d(a) = a$ ; se invece  $q < 0$  allora  $f^{dq}(a) = f^{(-d)(-q)}(a) = a$  che si ottiene dal caso precedente e da  $f^{-d}(a) = a$ ).  $\square$

Siano  $a \in X$  e  $f \in S_X$  come nella proposizione precedente. Usando la notazione precedente, deduciamo che se restringiamo  $f$  all'orbita  $\text{orb}_f(a) = \{a, f(a), f^2(a), \dots, f^{d-1}(a)\}$  di  $a$  possiamo scrivere

$$f|_{\text{orb}_f(a)} = \begin{pmatrix} a & f(a) & f^2(a) & \dots & f^{d-1}(a) \\ f(a) & f^2(a) & f^3(a) & \dots & a \end{pmatrix}.$$

Chiameremo una tale permutazione un *ciclo di lunghezza  $d$*  o  *$d$ -ciclo*. Useremo anche la notazione

$$(a \ f(a) \ f^2(a) \ \dots \ f^{d-1}(a))$$

per indicare un tale ciclo. Più in generale un  $l$ -ciclo,  $l \in \mathbb{N}^+$ ,  $l \geq 2$ , è una permutazione di  $l$  elementi  $\{a_1, \dots, a_l\}$  della forma

$$(a_1 \ a_2 \ \dots \ a_l) := \begin{pmatrix} a_1 & a_2 & \dots & a_l \\ a_2 & a_3 & \dots & a_1 \end{pmatrix}. \quad (2.8)$$

Un ciclo di lunghezza 2 è chiamato *trasposizione*. Si osservi che usando questa notazione possiamo cambiare l'ordine degli elementi *ciclicamente* per descrivere lo stesso elemento. Quindi

$$(a_1 a_2 \cdots a_l) = (a_i a_{i+1} \cdots a_1), \forall i = 1, \dots, l. \quad (2.9)$$

**Esempio 2.3.2** Le trasposizioni e i 3-cicli di  $S_3$  (cfr. Esempio 2.2.3) sono:

$$\tau_1 = (1\ 2), \tau_2 = (1\ 3), \tau_3 = (2\ 3), \sigma_1 = (1\ 2\ 3), \sigma_2 = (1\ 3\ 2).$$

La notazione (2.9) è molto utile per calcolare il prodotto di due cicli come mostrano i seguenti esempi.

**Esempio 2.3.3** Si considerino in  $S_4$  i due cicli  $g = (1234)$  e  $f = (123)$ . Allora il loro prodotto (composizione)  $g \circ f$  si calcola come segue. Osserviamo che  $(g \circ f)(1) = 3$ ,  $(g \circ f)(3) = 2$ ,  $(g \circ f)(2) = 4$  e  $(g \circ f)(4) = 1$ . Siamo giunti al punto iniziale 1 e quindi

$$g \circ f = (1324)$$

che è ancora un ciclo.

**Esempio 2.3.4** Non sempre la composizione di cicli è un ciclo. Per esempio siano  $g = (12345)$  e  $f = (13)$  in  $S_5$ . Allora  $(g \circ f)(1) = 4$ ,  $(g \circ f)(4) = 5$ ,  $(g \circ f)(5) = 1$  siamo tornati all'elemento 1 e quindi  $g \circ f$  ristretta all'insieme  $\{1, 4, 5\}$  è il ciclo  $(145)$ . Osserviamo che  $(g \circ f)(2) = 3$ ,  $(g \circ f)(3) = 2$  siamo tornati all'elemento 2 e quindi  $g \circ f$  ristretta all'insieme  $\{2, 3\}$  è la trasposizione  $(23)$ . Quindi

$$g \circ f = (145)(23) = (23)(145),$$

in accordo con l'Esempio 2.2.4.

Descriviamo ora alcune proprietà dei cicli.

**Proposizione 2.3.5** (alcune proprietà dei cicli) Sia  $\sigma = (a_1 a_2 \cdots a_l)$  un ciclo di lunghezza  $l$ , allora:

- (i)  $\text{supp}(\sigma) = \{a_1, \dots, a_l\}$ ;
- (ii)  $o(\sigma) = l$ ;
- (iii)  $\sigma^{-1} = (a_l \dots a_2 a_1)$ ;
- (iv) se esiste  $j \in \mathbb{Z}$  tale che  $\sigma^j \neq \text{id}$ , allora  $\text{supp}(\sigma^j) = \text{supp}(\sigma)$ .

### 2.3. I CICLI E IL TEOREMA FONDAMENTALE DELLE PERMUTAZIONI 41

**Dimostrazione:** La (i) segue direttamente dalla definizione di ciclo. Osserviamo che se  $0 < h \leq l-1$ ,  $\sigma^h(a_1) = a_{1+h} \neq a_1$ , mentre  $\sigma^l(a_j) = a_j$  per ogni  $j$ . Quindi la (ii) segue dalla definizione di ordine di un elemento. Sia  $\tilde{\sigma} = (a_l \dots a_2 a_1)$  allora:  $\tilde{\sigma}(a_1) = a_l$  e  $\tilde{\sigma}(a_j) = a_{j-1}$  per ogni  $1 < j \leq l$ . Segue che  $\tilde{\sigma} \circ \sigma = \sigma \circ \tilde{\sigma} = \text{id}$  e la (iii) è dimostrata. Infine, per dimostrare la (iv) osserviamo che  $\text{supp}(\sigma^j) \subseteq \text{supp}(\sigma)$ : infatti se  $x \notin \text{supp}(\sigma)$  allora  $\sigma(x) = x$  e quindi  $\sigma^j(x) = x$  che implica  $x \notin \text{supp}(\sigma^j)$ . Per dimostrare  $\text{supp}(\sigma) \subseteq \text{supp}(\sigma^j)$  possiamo supporre  $0 < j < l$ . Infatti dividendo  $j$  per  $l$  si ottiene:

$$j = lq + r, \quad q \in \mathbb{Z}, \quad 0 < r < l,$$

dove  $r \neq 0$  altrimenti  $\sigma^j = \text{id}$  e

$$\sigma^j = \sigma^{lq+r} = \sigma^{lq} \sigma^r = \text{id} \circ \sigma^r = \sigma^r.$$

Sia dunque  $x \in \text{supp}(\sigma)$  allora  $\sigma(x) \neq x$ . Per la (i)  $x = a_i$  per un certo  $i = 1, \dots, l$ . D'altra parte

$$\sigma^j(a_i) = \begin{cases} a_{i+j} & \text{se } i+j \leq l, \\ a_{i+j-l} & \text{se } i+j > l. \end{cases}$$

In entrambi i casi, sfruttando il fatto che  $0 < j < l$ , si deduce che  $\sigma^j(a_i) \neq a_i$ . Allora  $x = a_i \in \text{supp}(\sigma^j)$  e quindi  $\text{supp}(\sigma) \subseteq \text{supp}(\sigma^j)$ .  $\square$

**Osservazione 2.3.6** La potenza di un ciclo non è un ciclo in generale. Per esempio se  $\sigma = (1234) \in S_4$  allora  $\sigma^2 = (13)(24)$ , che è il prodotto di due trasposizioni (si veda l'Esercizio 2.9).

Concludiamo questo paragrafo con il seguente teorema che evidenzia l'importanza dei cicli come elementi fondamentali per esprimere qualsiasi permutazione con supporto finito come una composizione di cicli.

**Teorema 2.3.7** (il teorema fondamentale delle permutazioni) Sia  $X$  un insieme non vuoto, e sia  $f \in S_X$  tale che  $f \neq \text{id}_X$  e  $|\text{supp}(f)| < \infty$ . Allora, esistono cicli disgiunti  $\sigma_1, \dots, \sigma_t$ , con  $t \geq 1$ , tali che

$$f = \sigma_1 \circ \dots \circ \sigma_t. \quad (2.10)$$

Inoltre la scomposizione (2.10) è unica a meno dell'ordine dei cicli  $\sigma_j$ . Infine, l'ordine di  $f$  è dato da:

$$o(f) = (l_1, \dots, l_t), \quad (2.11)$$

dove  $l_j = o(\sigma_j)$  per  $j = 1, \dots, t$ , e  $(l_1, \dots, l_t)$  rappresenta il minimo comune multiplo degli  $l_j$ .

**Dimostrazione:** Dalla Proposizione 2.3.1, esistono  $t \geq 1$ , elementi distinti  $a_1, a_2, \dots, a_t \in \text{supp}(f)$ , e interi  $d_1, d_2, \dots, d_t$ , con  $d_j \geq 2$ , tali che

$$\text{supp}(f) = [a_1]_{\sim_f} \sqcup [a_2]_{\sim_f} \sqcup \dots \sqcup [a_t]_{\sim_f},$$

dove

$$[a_j]_{\sim_f} = \text{orb}_f(a_j) = \{a_j, f(a_j), \dots, f^{d_j-1}(a_j)\}, \quad j = 1, \dots, t.$$

Definiamo la permutazione  $g \in S_X$  come la composizione dei seguenti cicli disgiunti:

$$g = \left( a_1 f(a_1) \dots f^{d_1-1}(a_1) \right) \circ \left( a_2 f(a_2) \dots f^{d_2-1}(a_2) \right) \circ \dots \circ \left( a_t f(a_t) \dots f^{d_t-1}(a_t) \right).$$

Poiché  $\text{supp}(f) = \text{supp}(g)$  e  $f(x) = g(x)$  per ogni  $x \in \text{supp}(f)$ , si deduce che  $f = g$ . Pertanto, possiamo scrivere:

$$f = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_t,$$

dove  $\sigma_j = \left( a_j, f(a_j), \dots, f^{d_j-1}(a_j) \right)$  per  $j = 1, \dots, t$ . Poiché i cicli  $\sigma_j$  commutano tra loro, ne consegue che tale scomposizione è unica a meno dell'ordine. Per dimostrare la (2.11) sia  $d = o(f)$ . Allora

$$\text{id}_X = f^d = (\sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_t)^d = \sigma_1^d \circ \sigma_2^d \circ \dots \circ \sigma_t^d, \quad (2.12)$$

dove abbiamo utilizzato il fatto che i cicli  $\sigma_j$  commutano, cioè  $[\sigma_j, \sigma_k] = 1$  per ogni  $j \neq k$ , e l'Osservazione 1.3.26. Dimostriamo ora che questa uguaglianza implica che:

$$\sigma_j^d = \text{id}_X \quad \forall j = 1, \dots, t. \quad (2.13)$$

Supponiamo per assurdo che esista un  $k = 1, \dots, t$  tale che  $\sigma_k^d \neq \text{id}_X$ . In particolare, dalla Proposizione 2.3.5, sappiamo che:

$$\text{supp}(\sigma_k^d) = \text{supp}(\sigma_k), \quad (2.14)$$

e che esiste  $x \in X$  tale che:

$$\sigma_k^d(x) \neq x. \quad (2.15)$$

Mostriamo ora che:

$$\sigma_j^d(x) = x \quad \forall j \neq k. \quad (2.16)$$

Se  $\sigma_j^d = \text{id}_X$ , la (2.16) è immediata. Altrimenti, se  $\sigma_j^d \neq \text{id}_X$ , dalla Proposizione 2.3.5 segue che  $\text{supp}(\sigma_j^d) = \text{supp}(\sigma_j)$ . Dato che  $\sigma_j$  e  $\sigma_k$  sono disgiunti, lo stesso vale per  $\sigma_j^d$  e  $\sigma_k^d$ , e quindi  $\sigma_j^d(x) = x$ . Abbiamo così dimostrato la (2.16).

A questo punto, combinando la (2.12), la (2.15) e la (2.16), otteniamo:

$$x = \text{id}_X(x) = f^d(x) = (\sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_t)^d(x) = \sigma_k^d(x) \neq x,$$

che fornisce la contraddizione desiderata.

Poiché  $o(\sigma_j) = l_j$ , segue dalla Proposizione 1.3.33 che  $l_j \mid d$  per ogni  $j$ ; quindi  $d$  è un multiplo comune di  $l_1, \dots, l_t$ . Sia ora  $h$  un altro multiplo comune. Allora  $l_j \mid h$  per ogni  $j$ , perciò  $\sigma_j^h = \text{id}_X$  e

$$f^h = \sigma_1^h \circ \cdots \circ \sigma_t^h = \text{id}_X.$$

Ancora per la Proposizione 1.3.33 si ha  $d \mid h$ . Ne segue che  $d$  è il minimo comune multiplo di  $l_1, \dots, l_t$ , e la (2.11) è dimostrata.  $\square$

**Corollario 2.3.8** *Sia  $f \in S_X$  con  $|\text{supp}(f)| < \infty$  sia  $p$  un numero primo. Allora  $o(f) = p$  se e solo se  $f$  si può scrivere come prodotto di cicli disgiunti ognuno dei quali ha ordine  $p$ .*

## 2.4 Il segno di una permutazione

Sia  $X$  un insieme non vuoto, sia  $f \in S_X$  tale che  $f \neq \text{id}_X$ ,  $|\text{supp}(f)| < \infty$ , e sia

$$f = \sigma_1 \circ \cdots \circ \sigma_t,$$

la scomposizione (2.10) in cicli disgiunti  $\sigma_1, \dots, \sigma_t$ , con  $t \geq 1$ , la cui esistenza è garantita dal teorema fondamentale delle permutazioni.

Definiamo il numero naturale positivo

$$N(f) = (l_1 - 1) + (l_2 - 1) + \cdots + (l_t - 1) = \sum_{j=1}^t l_j - t,$$

dove  $l_j = o(\sigma_j)$  è la lunghezza del ciclo  $\sigma_j$ , con  $j = 1, \dots, t$ . Definiamo il *segno* di  $f$  come

$$\text{sign}(f) := (-1)^{N(f)} \in \{-1, +1\}. \quad (2.17)$$

Si deduce immediatamente dal fatto che i cicli  $\sigma_j$  nella scomposizione di  $f$  commutano che questa definizione è ben posta.

**Definizione 2.4.1** *Diremo che  $f$  è di classe pari se  $\text{sign}(f) = +1$  (ossia  $N(f)$  è pari), mentre diremo che  $f$  è di classe dispari se  $\text{sign}(f) = -1$  (ossia  $N(f)$  è dispari).*

**Lemma 2.4.2** Ogni  $f \in S_X$  con  $f \neq id_X$  e  $|supp(f)| < \infty$  si scrive come prodotto di  $N(f)$  trasposizioni.

**Dimostrazione:** Osserviamo preliminarmente che un ciclo di lunghezza  $l$ , si può scrivere come prodotto di  $l - 1$  trasposizioni. Infatti

$$(a_1 a_2 \cdots a_l) = (a_1 a_2)(a_2 a_3) \cdots (a_{l-1} a_l). \quad (2.18)$$

Quindi, per ogni  $j = 1, \dots, t$ , ogni  $\sigma_j$  nella scomposizione  $f = \sigma_1 \circ \cdots \circ \sigma_t$  in cicli disgiunti si può scrivere come prodotto di  $l_j - 1$  trasposizioni. Ne segue che  $f$  si può scrivere come prodotto di  $N(f) = (l_1 - 1) + \cdots + (l_t - 1)$  trasposizioni.  $\square$

**Osservazione 2.4.3** Il lemma non afferma né che la scomposizione è unica, né che le trasposizioni sono disgiunte. Per esempio, un  $l$ -ciclo può essere anche scritto come prodotto di  $l - 1$  trasposizioni

$$(a_1 a_2 \cdots a_l) = (a_1 a_l)(a_1 a_{l-1}) \cdots (a_1 a_3)(a_1 a_2),$$

che differisce dalla scomposizione (2.18).

**Teorema 2.4.4** (moltiplicatività della funzione segno) Siano  $f, g \in S_X$  tali che  $f, g \neq id_X$  e  $|supp(f)| < \infty, |supp(g)| < \infty$ . Allora

$$sign(f \circ g) = sign(f) sign(g). \quad (2.19)$$

**Dimostrazione:** La dimostrazione procede analizzando vari casi.

CASO 1:  $supp(f) \cap supp(g) = \emptyset$

Siano  $f = \sigma_1 \circ \cdots \circ \sigma_t$  e  $g = \rho_1 \circ \cdots \circ \rho_u$  la scomposizione di  $f$  e  $g$  in cicli disgiunti. Notiamo che l'ipotesi  $supp(f) \cap supp(g) = \emptyset$  è equivalente a

$$supp(\sigma_j) \cap supp(\rho_k), \forall j = 1, \dots, t, \forall k = 1, \dots, u.$$

Segue che

$$f \circ g = \sigma_1 \circ \cdots \circ \sigma_t \circ \rho_1 \circ \cdots \circ \rho_u$$

è la scomposizione di  $f \circ g$  in cicli disgiunti. Se quindi  $o(\sigma_j) = l_j, j = 1, \dots, t$  e  $o(\rho_k) = m_k, k = 1, \dots, u$ , allora

$$N(f \circ g) = \sum_{j=1}^t l_j - t + \sum_{k=1}^u m_k - u = N(f) + N(g).$$



Dalla quale

$$\text{sign}(f \circ g) = (-1)^{N(f \circ g)} = (-1)^{N(f) + N(g)} = (-1)^{N(f)} (-1)^{N(g)} = \text{sign}(f) \text{sign}(g).$$

CASO 2:  $|\text{supp}(f) \cap \text{supp}(g)| = 1$ ,  $f$  e  $g$  cicli.

Senza ledere alla generalità possiamo supporre

$$f = (a_1 \cdots a_m), g = (a_m b_1 \cdots b_l), a_j \neq b_k, \forall j = 1, \dots, m, \forall k = 1, \dots, l.$$

Quindi  $N(f) = m - 1$  e  $N(g) = l$ . D'altra parte

$$f \circ g = (a_1 \cdots a_m) \circ (a_m b_1 \cdots b_l) = (a_1 \cdots a_m b_1 \cdots b_l)$$

e quindi

$$N(f \circ g) = l + m - 1 = N(f) + N(g)$$

$$\text{e } \text{sign}(f \circ g) = \text{sign}(f) \text{sign}(g).$$

CASO 3:  $|\text{supp}(f) \cap \text{supp}(g)| = 2$ ,  $f$  ciclo e  $g$  trasposizione. Analizziamo i due sottocasi seguenti.

CASO 3A: I due elementi comuni di  $f$  e  $g$  sono consecutivi.

Possiamo supporre senza ledere alla generalità che

$$f = (a_1 a_2 \cdots a_{m-1} a_m), g = (a_{m-1} a_m).$$

Segue che

$$\begin{aligned} f \circ g &= (a_1 a_2 \cdots a_{m-1} a_m)(a_{m-1} a_m) \\ &= (a_1 a_2 \cdots a_{m-1})(a_{m-1} a_m)(a_{m-1} a_m) \\ &= (a_1 a_2 \cdots a_{m-1}). \end{aligned}$$

Osserviamo che

$$N(f) = m - 1, N(g) = 1, N(f \circ g) = m - 2 = N(f) + N(g) \pmod{2}.$$

Quindi

$$\text{sign}(f \circ g) = (-1)^{N(f \circ g)} = (-1)^{N(f) + N(g)} = (-1)^{N(f)} (-1)^{N(g)} = \text{sign}(f) \text{sign}(g).$$

CASO 3B: I due elementi comuni di  $f$  e  $g$  non sono consecutivi.

Possiamo supporre che

$$f = (a_1 a_2 \cdots a_{m-1} a_m), g = (a_i a_m), 1 < i < m - 1.$$

Segue che

$$\begin{aligned}
 f \circ g &= (a_1 a_2 \cdots a_{m-1} a_m)(a_i a_m) \\
 &= (a_1 a_2 \cdots a_i)(a_i a_{i+1} \cdots a_m)(a_i a_m) \\
 &= (a_1 a_2 \cdots a_i)(a_{i+1} \cdots a_m a_i)(a_i a_m) \\
 &= (a_1 a_2 \cdots a_i)(a_{i+1} \cdots a_m)(a_m a_i)(a_i a_m) \\
 &= (a_1 a_2 \cdots a_i)(a_{i+1} \cdots a_m).
 \end{aligned}$$

Osserviamo che

$$N(f \circ g) = (i - 1) + (m - i - 1) = m - 2 = N(f) + N(g) \pmod{2}.$$

Quindi si deduce, come prima, che

$$\text{sign}(f \circ g) = \text{sign}(f) \text{sign}(g).$$

CASO 4:  $f$  permutazione qualunque e  $g$  trasposizione. Distinguiamo i due sottocasi seguenti.

CASO 4A:  $|\text{supp}(f) \cap \text{supp}(g)| = 1$ . Per il teorema fondamentale delle permutazioni, possiamo scrivere  $f = \sigma_1 \circ \cdots \circ \sigma_t$  con  $\sigma_j$  cicli disgiunti. Senza ledere alla generalità possiamo assumere che  $|\text{supp}(\sigma_t) \cap \text{supp}(g)| = 1$  e quindi  $\text{supp}(\sigma_k) \cap \text{supp}(g) = \emptyset$  per ogni  $k \neq t, k = 1, \dots, t-1$ . Consideriamo il ciclo  $\sigma = \sigma_t \circ g$ , allora

$$f \circ g = \sigma_1 \circ \cdots \circ \sigma_t \circ g = \sigma_1 \circ \cdots \circ \sigma_{t-1} \circ \sigma.$$

Per il CASO 1 essendo  $\text{supp}(\sigma_1 \circ \cdots \circ \sigma_{t-1}) \cap \text{supp}(\sigma) = \emptyset$  possiamo scrivere

$$\text{sign}(f \circ g) = \text{sign}(\sigma_1 \circ \cdots \circ \sigma_{t-1}) \text{sign}(\sigma) = \text{sign}(\sigma_1 \circ \cdots \circ \sigma_{t-1}) \text{sign}(\sigma_t \circ g).$$

D'altra parte  $\text{sign}(\sigma_t \circ g) = \text{sign}(\sigma_t) \text{sign}(g)$ , per il CASO 2. Segue che

$$\begin{aligned}
 \text{sign}(f \circ g) &= \text{sign}(\sigma_1 \circ \cdots \circ \sigma_{t-1}) \text{sign}(\sigma_t) \text{sign}(g) \\
 &= \text{sign}(\sigma_1 \circ \cdots \circ \sigma_t) \text{sign}(g) = \text{sign}(f) \text{sign}(g),
 \end{aligned}$$

dove nella seconda uguaglianza stiamo abbiamo usato ancora il CASO 1.

CASO 4B:  $|\text{supp}(f) \cap \text{supp}(g)| = 2$ .

Se  $f = \sigma_1 \circ \cdots \circ \sigma_t$  con  $\sigma_j$  cicli disgiunti, allora, senza perdere di generalità, possiamo considerare i due sottocasi seguenti.

CASO 4B<sub>1</sub>:  $|\text{supp}(\sigma_{t-1}) \cap \text{supp}(g)| = 1$  e  $|\text{supp}(\sigma_t) \cap \text{supp}(g)| = 1$ . Consideriamo il ciclo  $\sigma = \sigma_t \circ g$ . Allora  $|\text{supp}(\sigma_{t-1}) \cap \text{supp}(\sigma)| = 1$  allora per il CASO 2

$$\text{sign}(\sigma_{t-1} \circ \sigma) = \text{sign}(\sigma_{t-1}) \text{sign}(\sigma) = \text{sign}(\sigma_{t-1}) \text{sign}(\sigma_t) \text{sign}(g).$$

Usando il CASO 1 e la precedente si ottiene:

$$\begin{aligned} \text{sign}(f \circ g) &= \text{sign}(\sigma_1 \circ \cdots \circ \sigma_{t-1} \circ \sigma) \\ &= \text{sign}(\sigma_1 \circ \cdots \circ \sigma_{t-2}) \text{sign}(\sigma_{t-1} \circ \sigma) \\ &= \text{sign}(\sigma_1 \circ \cdots \circ \sigma_{t-2}) \text{sign}(\sigma_{t-1}) \text{sign}(\sigma_t) \text{sign}(g) \\ &= \text{sign}(\sigma_1 \circ \cdots \circ \sigma_t) \text{sign}(g) = \text{sign}(f) \text{sign}(g). \end{aligned}$$

CASO 4B<sub>2</sub>:  $|\text{supp}(\sigma_t) \cap \text{supp}(g)| = 2$ .

Se  $f = \sigma_1 \circ \cdots \circ \sigma_t$  con  $\sigma_j$  cicli disgiunti, allora, senza perdere di generalità, possiamo supporre  $|\text{supp}(\sigma_t) \cap \text{supp}(g)| = 2$ . Allora, usando il CASO 1 e il CASO 3 si ottiene

$$\begin{aligned} \text{sign}(f \circ g) &= \text{sign}(\sigma_1 \circ \cdots \circ \sigma_{t-1}) \text{sign}(\sigma_t \circ g) \\ &= \text{sign}(\sigma_1 \circ \cdots \circ \sigma_{t-1}) \text{sign}(\sigma_t) \text{sign}(g) \\ &= \text{sign}(\sigma_1 \circ \cdots \circ \sigma_t) \text{sign}(g) = \text{sign}(f) \text{sign}(g). \end{aligned}$$

CASO 5 (caso generale):  $f, g$  permutazioni arbitrarie.

Per il Lemma 2.4.2 possiamo scrivere  $g = \tau_1 \circ \cdots \circ \tau_{N(g)}$ , con  $\tau_j, j = 1, \dots, N(g)$ , trasposizioni. Dimostriamo la (2.19) ossia

$$\text{sign}(f \circ g) = \text{sign}(f) \text{sign}(g) = \text{sign}(f) \text{sign}(\tau_1 \circ \cdots \circ \tau_{N(g)}) \quad (2.20)$$

per induzione su  $N(g)$ . Se  $N(g) = 1$  allora la (2.20) segue dal CASO 4. Supponiamo, per ipotesi induttiva, che la (2.20) valga per  $N(g) - 1$  cioè che

$$\text{sign}(f \circ \tau_1 \circ \cdots \circ \tau_{N(g)-1}) = \text{sign}(f) \text{sign}(\tau_1 \circ \cdots \circ \tau_{N(g)-1}).$$

Allora, sempre per il CASO 4 e l'ipotesi induttiva si ha

$$\begin{aligned} \text{sign}(f \circ \tau_1 \circ \cdots \circ \tau_{N(g)}) &= \text{sign}(f \circ \tau_1 \circ \cdots \circ \tau_{N(g)-1}) \text{sign}(\tau_{N(g)}) \\ &= \text{sign}(f) \text{sign}(\tau_1 \circ \cdots \circ \tau_{N(g)-1}) \text{sign}(\tau_{N(g)}) \\ &= \text{sign}(f) \text{sign}(\tau_1 \circ \cdots \circ \tau_{N(g)}) = \text{sign}(f) \text{sign}(g). \end{aligned}$$

**Corollario 2.4.5** Sia  $f \in S_n$ . Allora  $f$  è di classe pari se e solo se si scrive come composizione di un numero pari di trasposizioni.

**Dimostrazione:** Se  $f$  è di classe pari allora, per il Lemma 2.4.2,  $f = \tau_1 \circ \cdots \circ \tau_{N(f)}$ , con  $N(f)$  pari.

Viceversa se  $f = \tau_1 \circ \cdots \circ \tau_{2s}$  allora per il Teorema

$$\text{sign}(\tau_1 \circ \cdots \circ \tau_{2s}) = \text{sign}(\tau_1) \cdots \text{sign}(\tau_{2s}) = (-1)^{2s} = 1.$$

□

Alla luce del corollario, visto che  $\text{id}_X = \tau \circ \tau$ , dove  $\tau$  è una trasposizione, definiamo il segno di  $\text{id}_X$  uguale a 1, ossia  $\text{id}_X$  è di classe pari.

**Osservazione 2.4.6** Osserviamo che non è restrittivo supporre che nel Teorema 2.4.4  $f, g$  siano elementi di  $S_n$  per un qualche  $n$ . Infatti essendo i supporti di  $f$  e  $g$  finiti possiamo prendere  $n = |\text{supp}(f)| + |\text{supp}(g)|$  e considerare  $f|_{S_n}, g|_{S_n} \in S_n$  che soddisfano  $\text{sign}(f|_{S_n}) = \text{sign}(f)$  e  $\text{sign}(g|_{S_n}) = \text{sign}(g)$ .

## 2.5 Esercizi

**Esercizio 2.1** Si descrive il gruppo dell'isometrie del piano che fissano un rettangolo (che non sia un quadrato).

**Esercizio 2.2** Sia  $G = D_n$ ,  $n \geq 3$ , il gruppo diedrale. Determinare il sottoinsieme  $S \subset G$  costituito da tutti gli elementi di ordine 2.

**Esercizio 2.3** Sia  $f$  la permutazione di  $S_{12}$  data da

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 5 & 6 & 7 & 10 & 12 & 9 & 4 & 3 & 11 & 8 & 2 & 1 \end{pmatrix}.$$

Si scriva la decomposizione in cicli disgiunti di  $f, f^2, f^3$  e  $f^5$  e si calcolino gli ordini di queste permutazioni.

**Esercizio 2.4** Siano  $f$  e  $g$  la permutazioni di  $S_{10}$  definite come segue:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 4 & 5 & 7 & 9 & 8 & 10 & 6 & 3 & 1 \end{pmatrix} \text{ e } g = (23).$$

Si trovi la decomposizione in cicli disgiunti delle permutazioni  $f, g, f \circ g$  e  $g \circ f$  e si calcolino gli ordini di queste permutazioni.

**Esercizio 2.5** Dimostrare che due cicli  $\sigma$  e  $\tau$  della stessa lunghezza sono coniugati, cioè esiste una permutazione  $f$  tale che  $f^{-1} \circ \sigma \circ f = \tau$ .

**Esercizio 2.6** Sia  $\sigma$  un ciclo di lunghezza  $l$  e  $k \in N_+$  tale che  $\sigma^k \neq id$ . Mostrare che esistono  $t$  cicli disgiunti  $\sigma_1, \dots, \sigma_t$  tutti della stessa lunghezza  $m$ , tali che  $l = mt$  e

$$\sigma^k = \sigma_1 \circ \dots \circ \sigma_t. \quad (2.21)$$

Mostrare, inoltre che  $m = \frac{l}{(k,l)}$  e  $t = (k,l)$ . (Suggerimento: usare il fatto che  $\text{supp}(\sigma^k) = \text{supp}(\sigma)$  e il teorema fondamentale delle permutazioni. Per l'ultima parte si calcolino gli ordini di  $\sigma^k$  e  $\sigma_1 \circ \dots \circ \sigma_t$ ).

**Esercizio 2.7** Mostrare che se  $\sigma_1, \dots, \sigma_t$  sono cicli disgiunti tutti della stessa lunghezza  $m$  allora esiste un ciclo  $\sigma$  di lunghezza  $l = mt$  e  $k \in N_+$  tali che  $\sigma^k = \sigma_1 \circ \dots \circ \sigma_t$ . (Suggerimento: se  $\sigma_j = (a_{j1} \dots a_{jm})$ ,  $j = 1, \dots, t$ , si definisca

$$\sigma = (a_{11}a_{21} \dots a_{t1}a_{12}a_{22} \dots a_{t2} \dots a_{1m}a_{2m} \dots a_{tm})$$

e si verifichi che  $\sigma^t = \sigma_1 \circ \dots \circ \sigma_t$ ).

**Esercizio 2.8** Dimostrare che  $S_n$  é generato da  $\{A_n, \tau\}$  dove  $\tau$  é una trasposizione arbitraria.

**Esercizio 2.9** Sia  $\sigma$  un ciclo di lunghezza  $l$ . Dimostrare che

1.  $\sigma^2$  é un ciclo se e solo se  $l$  é dispari;
2. se  $l$  é dispari allora  $\sigma$  é il quadrato di un ciclo di lunghezza  $l$ ;
3. se  $l$  é pari,  $l = 2m$ , allora  $\sigma^2$  é il prodotto di due cicli di lunghezza  $m$ ;
4. se  $l = tm$ , allora  $\sigma^t$  é il prodotto di  $t$  cicli di lunghezza  $m$ ;
5. se  $l$  é un numero primo allora ogni potenza di  $\sigma$  é un ciclo.

(Suggerimento: usare l'Esercizio 2.6).

**Esercizio 2.10** Il cubo di Rubik può essere visto come un gruppo algebrico  $\mathcal{R}$ , dove le operazioni sono rappresentate dalle mosse che si possono eseguire sulle facce del cubo (si veda anche wikipedia). Più precisamente, ogni elemento di  $\mathcal{R}$  può essere scritto come prodotto di un numero finito delle seguenti mosse di base o delle loro inverse.

- $U$ : Rotazione di 90 gradi della faccia superiore (Upper) in senso orario;
- $D$ : Rotazione di 90 gradi della faccia inferiore (Down) in senso orario;
- $L$ : Rotazione di 90 gradi della faccia sinistra (Left) in senso orario;

- $R$ : Rotazione di 90 gradi della faccia destra (Right) in senso orario;
  - $F$ : Rotazione di 90 gradi della faccia frontale (Front) in senso orario;
  - $B$ : Rotazione di 90 gradi della faccia posteriore (Back) in senso orario.
1. Calcolare l'ordine di ogni mossa di base;
  2. Calcolare l'ordine degli elementi  $R^{-1}D$  e  $R^{-1}D^{-1}$ ;
  3. Dimostrare che la permutazione dei 20 cubetti del cubo di Rubik (8 angoli e 12 spigoli) indotta da una qualunque mossa é di classe pari.

# Capitolo 3

## Sottogruppi e classi laterali

### 3.1 Sottogruppi

**Definizione 3.1.1** Sia  $G$  un gruppo e sia  $H \subseteq G$ ,  $H \neq \emptyset$ . Diremo che  $H$  è un sottogruppo di  $G$  se valgono le seguenti proprietà:

- (S1): Stabilità, ovvero per ogni  $x, y \in H$ , anche il prodotto  $x \cdot y \in H$ .
- (S2): Esistenza dell'inverso, ovvero per ogni  $x \in H$ , anche l'inverso  $x^{-1} \in H$ .

**Osservazione 3.1.2** La condizione (S1), chiamata anche di *chiusura*, è equivalente ad affermare che l'operazione binaria  $\cdot$  ristretta ad  $H \subseteq G$  definisce un'operazione binaria su  $H$ .

**Notazione 3.1.3** Useremo la notazione  $H \leq G$  per indicare che  $H$  è un sottogruppo di  $G$ .

**Proposizione 3.1.4** Se  $H$  è un sottogruppo di  $G$ , allora  $1$ , l'elemento neutro di  $G$  appartiene a  $H$ .

**Dimostrazione:** Consideriamo un qualsiasi elemento  $x \in H$  che esiste in quanto  $H \neq \emptyset$ . Dall'esistenza dell'inverso (S2) abbiamo che  $x^{-1} \in H$  e dalla stabilità (S1), abbiamo che  $x \cdot x^{-1} = 1 \in H$ . Quindi, l'elemento neutro  $1$  appartiene a  $H$ .  $\square$

**Osservazione 3.1.5** Ogni gruppo  $G$  possiede sempre almeno due sottogruppi: il sottogruppo banale  $\{e\}$ , che contiene solo l'elemento neutro, e il gruppo  $G$  stesso. Un sottogruppo  $H$  di  $G$  è *proprio* se  $H \neq G$ , ossia se  $H$  è strettamente contenuto in  $G$ .

**Osservazione 3.1.6** Se  $H$  è un sottogruppo di  $G$ , allora  $H$  è a sua volta un gruppo rispetto alla stessa operazione di  $G$ . In particolare se  $G$  è abeliano allora ogni suo sottogruppo è abeliano.

**Esempi 3.1.7** Si verifica facilmente che i seguenti sottoinsiemi già incontrati nel Capitolo 1 sono sottogruppi.

$$(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$$

$$(\mathbb{Q}^*, \cdot) < (\mathbb{R}^*, \cdot) < (\mathbb{C}^*, \cdot)$$

$$(S^1, \cdot) < (\mathbb{C}^*, \cdot).$$

**Esempio 3.1.8** Sia  $a$  un elemento di un insieme  $X$  e sia

$$H_a = \{f \in S_X \mid f(a) = a\}.$$

l'insieme delle permutazioni di un insieme  $X$  che fissano  $a$ . Allora  $H_a$  è un sottogruppo di  $S_X$ . Infatti

- $H_a \neq \emptyset$ : La permutazione identità  $\text{id}_X \in S_X$  fissa ogni elemento di  $X$ , quindi in particolare  $\text{id}_X(a) = a$ , cioè  $\text{id}_X \in \text{Stab}(a)$ .
- (S1): Se  $f, g \in H_a$ , allora  $f(a) = a$  e  $g(a) = a$ . Dunque, per la composizione  $f \circ g$ , si ha  $(f \circ g)(a) = f(g(a)) = f(a) = a$ , quindi  $f \circ g \in H_a$ .
- (S2): Sia  $f \in H_a$ , allora  $f(a) = a$ . Sia  $f^{-1} \in S_X$ . Allora  $f^{-1}(a) = a$  e quindi  $f^{-1} \in H_a$ .

Essendo soddisfatte le proprietà (S1) e (S2) allora  $H_a \subset S_X$ .

**Esempio 3.1.9** (il gruppo alterno  $A_n$ ) Sia  $X$  un insieme con  $n$  elementi e sia  $S_n$  il gruppo simmetrico delle permutazioni di  $X$ . Definiamo il *gruppo alterno*  $A_n$  come l'insieme delle permutazioni di classe pari di  $S_n$ :

$$A_n = \{f \in S_n \mid \text{sign}(f) = 1\}.$$

Allora  $A_n$  è un sottogruppo di  $S_n$  e  $|A_n| = \frac{n!}{2}$ .

- $A_n \neq \emptyset$  in quanto  $\text{sign}(\text{id}_X) = 1$ .



- (S1): Siano  $f, g \in A_n$ , allora  $\text{sign}(f) = \text{sign}(g) = 1$ . Quindi per il Teorema 2.4.4,

$$\text{sign}(f \circ g) = \text{sign}(f) \text{sign}(g) = 1 \cdot 1 = 1.$$

Quindi,  $f \circ g \in A_n$ .

- (S2): Sia  $f \in A_n$ , allora

$$1 = \text{sign}(\text{id}_x) = \text{sign}(f \circ f^{-1}) = \text{sign}(f) \text{sign}(f^{-1}) = \text{sign}(f^{-1})$$

e quindi  $f^{-1} \in A_n$ .

Dunque,  $A_n < S_n$ . Per dimostrare  $A_n$  ha  $\frac{n!}{2}$  elementi consideriamo l'applicazione

$$A_n \rightarrow S_n \setminus A_n : f \mapsto f \circ \tau,$$

dove  $\tau$  è una trasposizione fissata. Quest'applicazione è ben definita in quanto  $\text{sign}(f \circ \tau) = \text{sign}(f) \text{sign}(\tau) = 1 \cdot -1 = -1$ . Inoltre è invertibile con inversa  $S_n \setminus A_n \rightarrow A_n, g \mapsto g \circ \tau$ . Dal momento che  $S_n$  è l'unione disgiunta di  $A_n$  e  $S_n \setminus A_n$  segue che

$$|A_n| = |S_n \setminus A_n| = \frac{|S_n|}{2} = \frac{n!}{2}.$$

Le due proposizioni seguenti sono a volte utili per dimostrare che in sottoinsieme di un gruppo è un sottogruppo.

**Proposizione 3.1.10** *Sia  $G$  un gruppo e  $H \subseteq G$ , con  $H \neq \emptyset$ . Se l'ordine di  $H$ , è finito e  $H$  è stabile (cioè soddisfa la condizione (S1) nella definizione di sottogruppo), allora  $H$  è un sottogruppo di  $G$ .*

**Dimostrazione:** Resta da verificare la condizione (S2), cioè che l'inverso di ogni elemento di  $H$  appartiene ancora a  $H$ . Sia  $a \in H$ . Se  $a = 1$ , allora il suo inverso è  $a^{-1} = 1 \in H$ . Supponiamo ora che  $a \neq 1$  e definiamo l'applicazione

$$f : \mathbb{N}^+ \rightarrow H, \quad n \mapsto a^n.$$

Questa applicazione è ben definita perché vale la condizione (S1). Poiché  $|H| < \infty$ ,  $f$  non è iniettiva. Esisteranno quindi  $m, n \in \mathbb{N}^+$ , con  $m > n$ , tali che  $f(m) = a^m = a^n = f(n)$ . Poiché  $m = n + k$  per qualche  $k > 0$ , otteniamo  $a^{n+k} = a^n a^k = a^n$ , e quindi  $a^k = 1$ . Segue che:

$$a^k = a^{k-1} a = 1.$$

Ora,  $k - 1 \geq 1$ , altrimenti, se  $k = 1$ , si avrebbe  $a = 1$ , che abbiamo escluso. Pertanto,  $a^{k-1} = a^{-1}$  è l'inverso di  $a$  e, grazie alla condizione (S1),  $a^{-1} = a^{k-1} \in H$ . Essendo  $a$  arbitrario  $H$  soddisfa la (S2) e quindi  $H \leq G$ .  $\square$

**Osservazione 3.1.11** In virtù di questa proposizione, nell'Esempio 3.1.9, per dimostrare che  $A_n$  è un sottogruppo, si sarebbe potuta evitare la verifica della condizione (S2).

**Proposizione 3.1.12** Sia  $G$  un gruppo e  $H \subset G$ , con  $H \neq \emptyset$ . Allora  $H \leq G$  se e solo se

$$x^{-1}y \in H, \forall x, y \in H. \quad (3.1)$$

**Dimostrazione:** Supponiamo che  $H \leq G$  e siano  $x, y \in H$ . Allora  $x^{-1} \in H$  per la (S2) e, per la (S1),  $x^{-1}y \in H$ . Quindi, la (3.1) è verificata. Viceversa, supponiamo che valga la (3.1) e siano  $x, y \in H$ . Allora, per la (3.1), si ha che  $x^{-1}x = 1 \in H$ . Sempre per la (3.1), si deduce che  $x^{-1} \cdot 1 = x^{-1} \in H$ , ossia vale la (S2). Inoltre, applicando ancora la (3.1), si ha  $(x^{-1})^{-1}y = xy \in H$ , quindi vale anche la (S1).  $\square$

## 3.2 Intersezione di sottogruppi

La seguente proposizione mostra che l'intersezione di un numero arbitrario di sottogruppi è ancora un sottogruppo

**Proposizione 3.2.1** Sia  $I$  un insieme di cardinalità qualunque e sia  $\{H_i\}_{i \in I}$  una famiglia di sottogruppi di  $G$ ,  $H_i \leq G$ , per ogni  $i \in I$ . Allora la loro intersezione  $H = \cap_{i \in I} H_i$  è un sottogruppo di  $G$ .

**Dimostrazione:** L'insieme  $H \subseteq G$  è non vuoto. Infatti,  $1 \in H_i$  per ogni  $i \in I$ , quindi  $1 \in H = \cap_{i \in I} H_i$ . Siano  $x, y \in H$ . Allora  $x, y \in H_i$  per ogni  $i \in I$ . Poiché  $H_i \leq G$ , segue dalla parte "se" della Proposizione 3.1.12 che  $x^{-1}y \in H_i$ , per ogni  $i \in I$ , e quindi  $x^{-1}y \in H = \cap_{i \in I} H_i$ . Per la parte "solo se" della Proposizione 3.1.12, si deduce che  $H \leq G$ .  $\square$

Sia  $G$  un gruppo e sia  $X \subseteq G$  un sottoinsieme di  $G$ . Consideriamo il sottoinsieme  $\langle X \rangle \subseteq G$  ottenuto come l'intersezione di tutti i sottogruppi di  $G$  che contengono  $X$ :

$$\langle X \rangle = \bigcap_{X \subset H \leq G} H$$

Osserviamo che  $\langle X \rangle \neq \emptyset$  in quanto stiamo prendendo l'intersezione di una famiglia non vuota di sottoinsiemi di  $X$  dato che  $G$  è un sottoinsieme di  $G$  che contiene  $X$ . Inoltre,  $\langle X \rangle \leq G$  per la Proposizione 3.2.1.

**Definizione 3.2.2** Chiameremo  $\langle X \rangle$  il sottogruppo di  $G$  generato da  $X$ .

Notiamo anche che  $\langle X \rangle$  è il più piccolo sottogruppo di  $G$  che contiene  $X$ , nel senso che se  $H \leq G$  è tale che  $X \subseteq H$  allora  $\langle X \rangle \subseteq H$ .

**Osservazione 3.2.3** Se  $X = \emptyset$  allora  $\langle X \rangle = \{1\}$ , dove  $1$  è l'elemento neutro di  $G$ . Inoltre se  $X \leq G$  allora  $\langle X \rangle = X$ .

La seguente proposizione fornisce una descrizione utile di  $\langle X \rangle$  come il sottoinsieme di  $G$  costituito dagli elementi che possono essere espressi come prodotto di elementi di  $X$  e dei loro inversi.

**Proposizione 3.2.4** Sia  $G$  un gruppo e  $X \subseteq G$ ,  $X \neq \emptyset$ . Allora

$$\langle X \rangle = \{ x_1^{\epsilon_1} \cdots x_k^{\epsilon_k} \mid k \geq 1, x_j \in X, \epsilon_j \in \{1, -1\} \}.$$

**Dimostrazione:** Sia

$$A := \{ x_1^{\epsilon_1} \cdots x_k^{\epsilon_k} \mid k \geq 1, x_j \in X, \epsilon_j \in \{1, -1\} \}.$$

Vogliamo mostrare che  $A = \langle X \rangle$ . Per prima cosa, se  $H \leq G$  è un sottogruppo con  $X \subseteq H$ , allora, poiché  $H$  è chiuso per inversi e prodotti e contiene  $X$ , ogni elemento di  $A$  appartiene a  $H$ . Dunque

$$A \subseteq \bigcap_{X \subseteq H \leq G} H = \langle X \rangle.$$

Per l'inclusione opposta, verifichiamo che  $A$  è un sottogruppo di  $G$  che contiene  $X$ . Anzitutto  $A \neq \emptyset$ : fissato  $x \in X$  (possibile perché  $X \neq \emptyset$ ), si ha  $xx^{-1} = 1 \in A$  (basta prendere  $k = 2$ ,  $x_1 = x_2 = x$ ,  $\epsilon_1 = 1$ ,  $\epsilon_2 = -1$ ). Inoltre  $X \subseteq A$  perché, per  $x \in X$ , scegliendo  $k = 1$  e  $\epsilon_1 = 1$  si ha  $x \in A$ .

Siano ora  $x, y \in A$  con

$$x = x_1^{\epsilon_1} \cdots x_m^{\epsilon_m}, \quad y = y_1^{\eta_1} \cdots y_n^{\eta_n},$$

dove  $x_i, y_j \in X$  e  $\epsilon_i, \eta_j \in \{1, -1\}$ . Allora

$$x^{-1}y = x_m^{-\epsilon_m} \cdots x_1^{-\epsilon_1} y_1^{\eta_1} \cdots y_n^{\eta_n}.$$

Scriviamo il prodotto precedente come

$$x^{-1}y = z_1^{\chi_1} \cdots z_{m+n}^{\chi_{m+n}},$$

dove, per  $1 \leq i \leq m$ , poniamo  $z_i := x_{m-i+1}$  e  $\chi_i := -\epsilon_{m-i+1}$ , mentre, per  $1 \leq i \leq n$ , poniamo  $z_{m+i} := y_i$  e  $\chi_{m+i} := \eta_i$ . Allora  $z_\ell \in X$  e  $\chi_\ell \in \{1, -1\}$  per ogni  $\ell$ , dunque  $x^{-1}y \in A$ .

Segue quindi, dalla Proposizione 3.1.12, che  $A$  è un sottogruppo di  $G$  che contiene  $X$ , per cui  $\langle X \rangle \subseteq A$ . In conclusione  $A = \langle X \rangle$ .  $\square$

Un caso particolarmente interessante si verifica quando  $X = \{x\}$ ,  $x \in G$ . In questo caso, il sottogruppo generato da  $X$  si può scrivere come

$$\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}. \quad (3.2)$$

**Definizione 3.2.5** Il gruppo  $\langle x \rangle$  è chiamato gruppo ciclico generato dall'elemento  $x$ .

**Osservazione 3.2.6** Si noti che un gruppo ciclico è sempre abeliano per la proprietà delle potenze

$$x^n x^m = x^{n+m} = x^m x^n, \quad \forall m, n \in \mathbb{Z}.$$

Nel caso di un gruppo ciclico  $\langle x \rangle$ , come mostra la proposizione seguente, l'ordine dell'elemento  $x \in G$  è proprio uguale all'ordine (ossia la cardinalità) del gruppo ciclico generato da  $x$ .

**Proposizione 3.2.7** Sia  $G$  un gruppo e  $x \in G$ . Allora

$$|\langle x \rangle| = o(x). \quad (3.3)$$

**Dimostrazione:** Supponiamo che  $o(x) = m$ , con  $m \in \mathbb{N}^+$ . Mostriamo che

$$\langle x \rangle = \{1, x, \dots, x^{m-1}\},$$

da cui si ottiene che  $m = o(x) = |\langle x \rangle|$ . L'inclusione

$$\{1, x, \dots, x^{m-1}\} \subseteq \langle x \rangle$$

segue dalla (3.2). Per dimostrare l'inclusione opposta, sia  $x^n \in \langle x \rangle$  con  $n \in \mathbb{Z}$ . Allora, dividendo  $n$  per  $m$ , possiamo scrivere

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

Dunque

$$x^n = x^{mq+r} = x^{mq} x^r = (x^m)^q x^r = 1 \cdot x^r = x^r.$$

Ma  $x^r \in \{1, x, \dots, x^{m-1}\}$ , poiché  $0 \leq r < m$ , e quindi

$$\langle x \rangle \subseteq \{1, x, \dots, x^{m-1}\}.$$

Viceversa, supponiamo che  $|\langle x \rangle| = m$ , con  $m \in \mathbb{N}^+$ . Mostriamo che  $o(x) = m$ . Consideriamo l'applicazione

$$f : \mathbb{Z} \rightarrow \langle x \rangle, \quad n \mapsto x^n.$$

Poiché  $|\mathbb{Z}| = \infty$  e  $|\langle x \rangle| < \infty$ , segue che  $f$  non è iniettiva. Esisteranno quindi  $n, k \in \mathbb{Z}$  con  $n > k$  tali che  $x^n = x^k$ , ovvero  $x^{n-k} = 1$ . Di conseguenza, l'insieme  $\{n \in \mathbb{N}^+ \mid x^n = 1\}$  non è vuoto, e quindi  $o(x) = d$  per qualche  $d \in \mathbb{N}^+$ . Dalla prima parte,  $d = o(x) = |\langle x \rangle| = m$ . Abbiamo dunque dimostrato che  $o(x) = m$  se e solo se  $|\langle x \rangle| = m$ , e quindi la (3.3) è dimostrata.  $\square$

**Proposizione 3.2.8** (*classificazione dei sottogruppi di  $\mathbb{Z}$* ) Sia  $H$  un sottogruppo di  $\mathbb{Z} = (\mathbb{Z}, +, 0)$ . Allora esiste  $h \in \mathbb{N}$  tale che

$$H = h\mathbb{Z} = \{hz \mid z \in \mathbb{Z}\}.$$

*In particolare, tutti i sottogruppi di  $\mathbb{Z}$  sono ciclici.*

**Dimostrazione:** Se  $H = \{0\}$ , allora  $H = 0\mathbb{Z}$ , che è il sottogruppo banale. Supponiamo quindi che  $H \neq \{0\}$ . Allora esiste  $a \in H$ , con  $a \neq 0$ . Possiamo assumere che  $a > 0$ , poiché se  $a < 0$ , il suo opposto  $-a \in H$  e  $-a > 0$ . Per il principio del buon ordinamento, esiste  $h \in H$ ,  $h > 0$ , che è il più piccolo elemento positivo in  $H$ . Vogliamo dimostrare che  $H = h\mathbb{Z}$ . L'inclusione  $h\mathbb{Z} \subseteq H$  è immediata:  $h \in H$  implica che ogni suo multiplo  $hz \in H$ , per ogni  $z \in \mathbb{Z}$ .

Dimostriamo ora l'inclusione opposta,  $H \subseteq h\mathbb{Z}$ . Sia  $z \in H$ , dividendo  $z$  per  $h$  possiamo scrivere

$$z = qh + r, \quad 0 \leq r < h.$$

Poiché  $z \in H$  e  $qh \in h\mathbb{Z} \subseteq H$ , otteniamo che  $z - qh = r \in H$ . Dato che  $h$  è il più piccolo elemento positivo in  $H$ , segue che  $r = 0$ , quindi  $z = qh \in h\mathbb{Z}$ . Essendo  $z$  arbitrario, concludiamo che  $H \subseteq h\mathbb{Z}$ . Infine, l'ultima affermazione segue dal fatto che  $h \in \mathbb{Z}$ , in notazione additiva, è il generatore del sottogruppo ciclico  $\langle h \rangle = h\mathbb{Z}$ .  $\square$

**Esempio 3.2.9** Sia  $G$  l'insieme di tutte le isometrie di  $\mathbb{R}^2$  che fissano l'origine, cioè le matrici ortogonali di ordine 2. Per ogni  $n \geq 3$ , il gruppo diedrale  $D_n$ , descritto nel Capitolo 2, è un sottogruppo di  $G$  generato da una rotazione  $r$  intorno all'origine e dalla simmetria rispetto all'asse delle ordinate.

### 3.3 Unione di sottogruppi

In generale l'unione di sottogruppi non è un sottogruppo come mostra la seguente

**Proposizione 3.3.1** *Siano  $H$  e  $K$  due sottogruppi di un gruppo  $G$ . Allora  $H \cup K$  è un sottogruppo di  $G$  se e solo se  $H \leq K$  oppure  $K \leq H$ .*

**Dimostrazione:** Se  $H \leq K$  (resp.  $K \leq H$ ), allora  $H \cup K = K \leq G$  (resp.  $H \cup K = H \leq G$ ). Supponiamo ora che  $H \cup K \leq G$  e dimostriamo che  $H \leq K$  oppure  $K \leq H$ . Se, per esempio  $H \not\leq K$  (il caso  $K \not\leq H$  si tratta in modo analogo scambiando il ruolo di  $H$  e  $K$ ), allora esiste  $h \in H$  tale che  $h \notin K$ . Sia  $k \in K$ . Allora  $hk \in H \cup K$ , poiché per ipotesi  $H \cup K$  è un sottogruppo di  $G$  e soddisfa quindi la proprietà di chiusura (S1). Tuttavia,  $hk \notin K$ , altrimenti  $hk = k'$ , per qualche  $k' \in K$ , e quindi  $h = k'k^{-1} \in K$ , in contrasto con la scelta di  $h$ . Di conseguenza,  $hk \in H$ . Ma allora,  $h^{-1}hk = k \in H$ . Essendo  $k$  arbitrario, segue che  $K \subseteq H$ .  $\square$

**Corollario 3.3.2** *Un gruppo  $G$  non può essere scritto come unione di due suoi sottogruppi propri.*

**Dimostrazione:** Supponiamo per assurdo che  $G = H \cup K$  con  $H < G$  e  $K < G$ . Allora per la Proposizione 3.3.1, essendo  $G$  un sottogruppo di se stesso si ha  $H \leq K$  oppure  $K \leq H$ . Quindi  $H \cup K = K = G$  oppure  $H \cup K = H = G$  in contrasto con il fatto che  $H$  e  $K$  sono strettamente contenuti in  $G$ .  $\square$

**Osservazione 3.3.3** Esistono gruppi che possono essere scritti come unione di tre loro sottogruppi propri. Per esempio, sia  $G = (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$  con l'operazione

$$([a]_2, [b]_2) + ([c]_2, [d]_2) = ([a + b]_2, [c + d]_2).$$

Si verifica immediatamente che  $G$  è un gruppo abeliano il cui elemento neutro è  $([0]_2, [0]_2)$  e l'opposto di un elemento  $([a]_2, [b]_2)$  è dato da  $([-a]_2, [-b]_2)$ . Consideriamo i tre sottogruppi ciclici e propri  $H$ ,  $K$  e  $L$  di  $G$  generati rispettivamente da  $([1]_2, [0]_2)$ ,  $([0]_2, [1]_2)$  e  $([1]_2, [1]_2)$ :

$$H = \langle ([1]_2, [0]_2) \rangle = \{([0]_2, [0]_2), ([1]_2, [0]_2)\}$$

$$K = \langle ([0]_2, [1]_2) \rangle = \{([0]_2, [0]_2), ([0]_2, [1]_2)\}$$

$$L = \langle ([1]_2, [1]_2) \rangle = \{([0]_2, [0]_2), ([1]_2, [1]_2)\}.$$

Allora  $G = H \cup K \cup L$ .

La Proposizione 3.3.1 può essere generalizzata come segue.

**Definizione 3.3.4** Sia  $G$  un gruppo. Una famiglia non vuota  $\{H_i\}_{i \in I}$  di sottogruppi di  $G$  si dice *catena* se per ogni  $i, j \in I$  vale  $H_i \subseteq H_j$  oppure  $H_j \subseteq H_i$ .

**Proposizione 3.3.5 (unione di una catena)** Sia  $G$  un gruppo e  $\{H_i\}_{i \in I}$  una catena non vuota di sottogruppi di  $G$ . Allora

$$H = \bigcup_{i \in I} H_i$$

è un sottogruppo di  $G$ .

**Dimostrazione:** Per ogni  $i$  si ha  $1 \in H_i$ , dunque  $1 \in H$ . Siano  $x, y \in H$ : esistono  $i, j$  tali che  $x \in H_i$  e  $y \in H_j$ . Poiché la famiglia è una catena, senza perdere generalità  $H_i \subseteq H_j$ ; quindi  $x, y \in H_j$  e, per il criterio di sottogruppo,  $x^{-1}y \in H_j \subseteq H$ . Ne segue che  $H$  è un sottogruppo di  $G$ .  $\square$

Un corollario immediato è il seguente.

**Corollario 3.3.6** Sia  $\{H_i\}_{i \in \mathbb{N}}$  una famiglia di sottogruppi di  $G$  tali che  $H_i \subseteq H_j$  se  $i \leq j$ . Allora  $H = \bigcup_{i \in \mathbb{N}} H_i \leq G$ .

**Osservazione 3.3.7** La condizione per cui, per tutti  $i, j \in I$ , si ha  $H_i \subseteq H_j$  oppure  $H_j \subseteq H_i$ , può essere indebolita. Tutto procede comunque se, per tutti  $i, j \in I$ , esiste un  $k \in I$  tale che  $H_i \subseteq H_k$  e  $H_j \subseteq H_k$ .

I risultati precedenti ci dicono quindi, che in generale l'unione di sottogruppi non è un sottogruppo. La proposizione che segue descrive il gruppo generato dall'unione.

**Proposizione 3.3.8** Sia  $G$  un gruppo. Sia  $I$  un insieme di cardinalità non nulla e sia  $\{H_i\}_{i \in I}$  una famiglia di sottogruppi di  $G$ . Allora il sottogruppo di  $G$  generato dall'unione è

$$\left\langle \bigcup_{i \in I} H_i \right\rangle = \left\{ x_1 x_2 \dots x_k \mid k \geq 0, x_j \in H_{i_j}, i_j \in I \right\}.$$

**Dimostrazione:** Poniamo

$$H := \left\langle \bigcup_{i \in I} H_i \right\rangle, \quad A := \left\{ x_1 x_2 \dots x_k \mid k \geq 0, x_j \in H_{i_j}, i_j \in I \right\}.$$

Dimostrazione prima l'inclusione  $A \subseteq H$ . Sia  $x = x_1 \dots x_k \in A$ . Per definizione di  $A$ , ogni  $x_j$  appartiene a qualche  $H_{i_j}$ , dunque  $x_j \in \bigcup_{i \in I} H_i \subseteq H$  (perché  $H$  è un sottogruppo che contiene l'unione). Essendo  $H$  un sottogruppo, è

chiuso per prodotto: quindi  $x = x_1 \cdots x_k \in H$ . Nel caso  $k = 0$  il prodotto è per convenzione  $1 \in H$ , poiché ogni sottogruppo contiene l'identità. Pertanto  $A \subseteq H$ .

Dimostriamo ora l'inclusione  $H \subseteq A$ . Mostriamo che  $A \leq G$  e che contiene  $\bigcup_{i \in I} H_i$ . Infatti  $1 \in A$  (caso  $k = 0$ ); se  $a = x_1 \cdots x_k \in A$  e  $b = y_1 \cdots y_\ell \in A$ , allora  $ab = x_1 \cdots x_k y_1 \cdots y_\ell \in A$ , quindi  $A$  è chiuso per prodotto; inoltre  $a^{-1} = x_k^{-1} \cdots x_1^{-1} \in A$  perché ogni  $H_{i_j}$  è un sottogruppo, dunque chiuso per inversi. Quindi  $A \leq G$ . Per ogni  $i \in I$  e  $h \in H_i$  si ha  $h \in A$  prendendo  $k = 1$ , perciò  $\bigcup_{i \in I} H_i \subseteq A$ . Per minimalità di  $H = \langle \bigcup_{i \in I} H_i \rangle$  tra i sottogruppi che contengono l'unione, segue  $H \subseteq A$ . Dalle due inclusioni otteniamo  $H = A$ .  $\square$

### 3.4 Prodotto di sottogruppi

Il *prodotto* di due sottogruppi  $H$  e  $K$  di un gruppo  $G$  è l'insieme dei prodotti di tutti gli elementi di  $H$  con tutti gli elementi di  $K$ . Formalmente, il prodotto di  $H$  e  $K$  è definito come:

$$H \cdot K = \{h \cdot k \mid h \in H, k \in K\}.$$

In altre parole, si prende ciascun elemento  $h$  di  $H$  e ciascun elemento  $k$  di  $K$  e si considera il prodotto  $h \cdot k$ , dove l'operazione  $\cdot$  è quella del gruppo  $G$ .

**Esempio 3.4.1** Consideriamo il gruppo simmetrico  $G = S_3$ , ovvero:

$$S_3 = \{1, (12), (13), (23), (123), (132)\}.$$

Siano  $H = \langle (12) \rangle = \{1, (12)\}$  e  $K = \langle (13) \rangle = \{1, (13)\}$  due sottogruppi di  $S_3$ . Il prodotto  $H \cdot K$  è dato da

$$H \cdot K = \{1, (13), (12), (123)\}.$$

Analogamente, possiamo calcolare il prodotto  $K \cdot H$  ottenendo

$$K \cdot H = \{1, (12), (13), (132)\}.$$

Come si può vedere,  $H \cdot K \neq K \cdot H$ , quindi il prodotto di sottogruppi non è commutativo in generale.

Da ora in poi scriveremo  $HK = H \cdot K$ . Diremo che  $H$  e  $K$  *commutano* o sono *permutabili* se  $HK = KH$ .



**Osservazione 3.4.2** Chiaramente  $G$  è abeliano, allora due suoi sottogruppi  $H$  e  $K$  commutano. Nella notazione additiva scriveremo  $H + K$  invece che  $HK$ .

Nella seguente proposizione mostriamo che se  $H$  e  $K$  commutano allora  $HK$  è un sottogruppo di  $G$ . Indichiamo con  $\langle H, K \rangle = \langle H \cup K \rangle$  il sottogruppo di  $G$  generato dall'unione di  $H$  e  $K$ .

**Proposizione 3.4.3** *Sia  $G$  un gruppo e  $H, K$  suoi sottogruppi. Le seguenti condizioni sono equivalenti:*

- (i)  $HK = \langle H, K \rangle$ ;
- (ii)  $HK = KH$ ;
- (iii)  $HK \leq G$ .

**Dimostrazione:** (i)  $\Rightarrow$  (ii): Supponiamo che  $HK = \langle H, K \rangle$ , cioè che  $HK$  sia il sottogruppo generato da  $H$  e  $K$ . Vogliamo dimostrare che  $HK = KH$ . Ricordiamo che  $\langle H, K \rangle$  è il più piccolo sottogruppo di  $G$  che contiene sia  $H$  che  $K$ . In particolare, ciò significa che tutti i prodotti di elementi di  $K$  e  $H$  appartengono a  $\langle H, K \rangle$ , e quindi

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

Per dimostrare l'inclusione  $HK \subseteq KH$  (e quindi l'uguaglianza  $HK = KH$ ), sia  $hk \in HK$ ,  $h \in H$  e  $k \in K$ . Allora, visto che  $HK = \langle H, K \rangle$  è un gruppo l'inverso di  $hk$  appartiene a  $HK$  e quindi

$$(hk)^{-1} = h'k', \quad h' \in H, \quad k' \in K.$$

Dal momento che gli inversi di elementi di  $H$  e  $K$  stanno in  $H$  e  $K$ , si ha:

$$hk = (h'k')^{-1} = k'^{-1}h'^{-1} \in KH,$$

la quale mostra  $HK \subseteq KH$ .

(ii)  $\Rightarrow$  (iii): Supponiamo ora che  $HK = KH$ . Per dimostrare che  $HK$  è un sottogruppo, osserviamo che è diverso dal vuoto. Infatti  $H$  e  $K$  sono sottogruppi di  $G$ , contengono entrambi l'elemento neutro  $1$  di  $G$  e quindi  $1 = 1 \cdot 1 \in HK$ , e  $HK$  contiene l'elemento neutro. Prendiamo due elementi arbitrari  $h_1k_1, h_2k_2 \in HK$ , dove  $h_1, h_2 \in H$  e  $k_1, k_2 \in K$ . Allora, visto che  $HK = KH$ , possiamo scrivere  $k_1k_2^{-1}h_2^{-1} = h_3k_3$ , con  $h_3 \in H$  e  $k_3 \in K$  e quindi:

$$(h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = h_1h_3k_3 \in HK.$$

Dunque  $HK \leq G$  per la Proposizione 3.1.12.

(iii)  $\Rightarrow$  (i): Infine, supponiamo che  $HK \leq G$ . Per definizione, il sottogruppo generato da  $H$  e  $K$ ,  $\langle H, K \rangle$ , è il più piccolo sottogruppo di  $G$  che contiene sia  $H$  che  $K$ . Poiché  $H \subseteq HK$  e  $K \subseteq HK$ , e  $HK$  è un sottogruppo di  $G$ , si ha che:

$$\langle H, K \rangle \subseteq HK.$$

D'altra parte, siccome  $\langle H, K \rangle$  (come abbiamo già osservato) contiene tutti i prodotti di elementi di  $H$  e  $K$ , abbiamo anche  $HK \subseteq \langle H, K \rangle$ . Quindi,  $HK = \langle H, K \rangle$ .  $\square$

**Esempio 3.4.4** Sia  $G = (\mathbb{Z}, +, 0)$  il gruppo degli interi e siano  $H$  e  $K$  due suoi sottogruppi non banali, cioè diversi dal sottogruppo nullo  $\{0\}$ . Per la Proposizione 3.2.8, esisteranno  $m, n \in \mathbb{N}^+$  tali che  $H = m\mathbb{Z}$  e  $K = n\mathbb{Z}$ . Vogliamo descrivere i sottogruppi  $H \cap K$  e  $H + K = \langle H, K \rangle$  in funzione di  $m$  e  $n$ . Notiamo che  $H + K = \langle H, K \rangle \leq \mathbb{Z}$ , per la Proposizione 3.4.3, essendo  $\mathbb{Z}$  abeliano.

Osserviamo preliminarmente che, per ogni  $u, v \in \mathbb{N}$  si ha:

$$u\mathbb{Z} \subseteq v\mathbb{Z} \Leftrightarrow v \mid u \quad (3.4)$$

Iniziamo con  $H + K = \langle H, K \rangle$ . Per la Proposizione 3.2.8 esiste  $d \in \mathbb{N}^+$  tale che

$$H + K = m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}.$$

Mostriamo che  $d$  è il massimo comun divisore tra  $m$  e  $n$ ,  $d = (m, n)$ . Infatti visto che  $m\mathbb{Z} \subseteq d\mathbb{Z}$  e  $n\mathbb{Z} \subseteq d\mathbb{Z}$  segue dalla (3.4) che  $d \mid m$  e  $d \mid n$ . Inoltre se  $a \in \mathbb{N}$  è tale che  $a \mid m$  e  $a \mid n$  allora per la (3.4), si ha  $m\mathbb{Z} \subseteq a\mathbb{Z}$  e  $n\mathbb{Z} \subseteq a\mathbb{Z}$  e quindi

$$H + K = m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z} \subseteq a\mathbb{Z}.$$

Da questa (ancora per la (3.4)) segue che  $a \mid d$ , la quale mostra che  $d$  è in effetti il massimo comun divisore tra  $m$  e  $n$ . Abbiamo quindi dimostrato che

$$m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}.$$

Consideriamo ora  $H \cap K$ . Per la Proposizione 3.2.8 esiste  $s \in \mathbb{N}^+$  tale che

$$H \cap K = m\mathbb{Z} \cap n\mathbb{Z} = s\mathbb{Z}.$$

Mostriamo che  $s$  è il minimo comune multiplo tra  $m$  e  $n$ ,  $s = [m, n]$ . Infatti visto che  $s\mathbb{Z} \subseteq m\mathbb{Z}$  e  $s\mathbb{Z} \subseteq n\mathbb{Z}$  segue dalla (3.4) che  $m \mid s$  e  $n \mid s$ . Inoltre se

$a \in \mathbb{N}$  è tale che  $m \mid a$  e  $n \mid a$  allora per la (3.4), si ha  $a\mathbb{Z} \subseteq m\mathbb{Z}$  e  $a\mathbb{Z} \subseteq n\mathbb{Z}$  e quindi

$$a\mathbb{Z} \subseteq m\mathbb{Z} \cap n\mathbb{Z} = s\mathbb{Z}.$$

Da questa (ancora per la (3.4)) segue che  $s \mid a$ , la quale mostra che  $d$  è il minimo comune multiplo tra  $m$  e  $n$ , ossia Abbiamo quindi dimostrato che

$$m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}.$$

Concludiamo questo paragrafo calcolando la cardinalità dell'insieme di  $HK$ , per due sottogruppi finiti  $H$  e  $K$  di un gruppo  $G$ .

**Proposizione 3.4.5** *Siano  $H$  e  $K$  due sottogruppi finiti di un gruppo  $G$ . Allora*

$$|HK| = \frac{|H||K|}{|H \cap K|}. \quad (3.5)$$

**Dimostrazione:** Sia  $f : H \times K \rightarrow HK$ , definita da  $f(h, k) = hk$ , e consideriamo la seguente relazione di equivalenza  $\sim_f$  su  $H \times K$ : dati  $(h_1, k_1), (h_2, k_2) \in H \times K$ ,

$$(h_1, k_1) \sim_f (h_2, k_2) \iff h_1 k_1 = f(h_1, k_1) = f(h_2, k_2) = h_2 k_2. \quad (3.6)$$

Sia  $\frac{H \times K}{\sim_f}$  lo spazio quoziente corrispondente e denotiamo con  $[(h, k)]_{\sim_f}$  la classe di equivalenza dell'elemento  $(h, k) \in H \times K$ . Poiché  $f$  è suriettiva, l'applicazione

$$\tilde{f} : \frac{H \times K}{\sim_f} \rightarrow HK, \quad [(h, k)]_{\sim_f} \mapsto \tilde{f}([(h, k)]_{\sim_f}) = f(h, k) = hk,$$

è una bigezione. Pertanto,

$$\left| \frac{H \times K}{\sim_f} \right| = |HK|. \quad (3.7)$$

Fissiamo ora  $(h_0, k_0) \in [(h, k)]_{\sim_f}$ , e definiamo l'applicazione

$$g : [(h, k)]_{\sim_f} \rightarrow H \cap K, \quad (h_1, k_1) \in [(h, k)]_{\sim_f} \mapsto h_1^{-1} h_0.$$

Quest' applicazione è ben definita in virtù di (3.6):

$$(h_0, k_0) \sim_f (h_1, k_1) \Rightarrow h_1^{-1} h_0 = k_1 k_0^{-1} \in H \cap K.$$

Inoltre  $g$  è invertibile, con inversa

$$g^{-1} : H \cap K \rightarrow [(h, k)]_{\sim_f}, \quad s \mapsto (h_0 s^{-1}, s k_0).$$

Segue allora che

$$|[ (h, k) ]_{\sim_f}| = |H \cap K|, \quad \forall (h, k) \in H \times K, \quad (3.8)$$

ossia le classi di equivalenza hanno tutte la stessa cardinalità, che è uguale a  $|H \cap K|$ . Combinando la (3.7) con la (3.8), otteniamo

$$|H||K| = |H \times K| = \left| \frac{H \times K}{\sim_f} \right| \cdot |[ (h, k) ]_{\sim_f}| = |HK| \cdot |H \cap K|,$$

da cui otteniamo la (3.5).  $\square$

### 3.5 Classi laterali e il teorema di Lagrange

Dato un gruppo  $G$  la scelta di un suo sottogruppo  $H$  e di un elemento  $x \in G$  definisce due sottoinsiemi naturali di  $G$ , la *classe laterale sinistra di  $x$  rispetto ad  $H$* :

$$xH = \{xh \mid h \in H\} \quad (3.9)$$

la *classe laterale destra di  $x$  rispetto ad  $H$* :

$$Hx = \{hx \mid h \in H\} \quad (3.10)$$

**Esempio 3.5.1** Consideriamo il gruppo simmetrico  $S_3$

$$S_3 = \{1, (12), (13), (23), (123), (132)\}$$

e il suo sottogruppo  $H = \langle (12) \rangle = \{1, (12)\}$ , di ordine 2.

Le classi laterali sinistre sono della forma  $xH$ , dove  $x \in S_3$ :

$$\begin{aligned} 1H &= \{1 \cdot 1, 1 \cdot (12)\} = \{1, (12)\}, \\ (12)H &= \{(12) \cdot 1, (12) \cdot (12)\} = \{(12), 1\}, \\ (13)H &= \{(13) \cdot 1, (13) \cdot (12)\} = \{(13), (132)\}, \\ (23)H &= \{(23) \cdot 1, (23) \cdot (12)\} = \{(23), (123)\}, \\ (123)H &= \{(123) \cdot 1, (123) \cdot (12)\} = \{(123), (13)\}, \\ (132)H &= \{(132) \cdot 1, (132) \cdot (12)\} = \{(132), (23)\}. \end{aligned}$$

Quindi le classi laterali sinistre distinte di  $H$  in  $S_3$  sono:

$$\{1, (12)\}, \quad \{(13), (132)\}, \quad \{(23), (123)\}.$$

Allo stesso modo, calcoliamo le classi laterali destre  $Hx$  per ogni elemento di  $S_3$ :

$$\begin{aligned} H1 &= \{1 \cdot 1, (12) \cdot 1\} = \{1, (12)\}, \\ H(12) &= \{1 \cdot (12), (12) \cdot (12)\} = \{(12), 1\}, \\ H(13) &= \{1 \cdot (13), (12) \cdot (13)\} = \{(13), (123)\}, \\ H(23) &= \{1 \cdot (23), (12) \cdot (23)\} = \{(23), (132)\}, \\ H(123) &= \{1 \cdot (123), (12) \cdot (123)\} = \{(123), (23)\}, \\ H(132) &= \{1 \cdot (132), (12) \cdot (132)\} = \{(132), (13)\}. \end{aligned}$$

Quindi le classi laterali destre distinte di  $H$  in  $S_3$  sono:

$$\{1, (12)\}, \quad \{(13), (123)\}, \quad \{(23), (132)\}.$$

Riassumiamo in una tabella le classi laterali sinistre e destre distinte per il sottogruppo  $H = \{1, (12)\}$  in  $S_3$ :

$x$	Classe laterale sinistra $xH$	Classe laterale destra $Hx$
1	$\{1, (12)\}$	$\{1, (12)\}$
(13)	$\{(13), (132)\}$	$\{(13), (123)\}$
(23)	$\{(23), (123)\}$	$\{(23), (132)\}$

Questo esempio mostra che le classi laterali sinistre e destre non coincidono necessariamente.

Dato un gruppo  $G$  e un suo sottogruppo  $H$ , possiamo definire due relazioni d'equivalenza  $\sim$  e  $\sim'$  su  $G$  come segue:

$$x \sim y \iff x^{-1}y \in H, \quad x, y \in G \quad (3.11)$$

$$x \sim' y \iff xy^{-1} \in H, \quad x, y \in G. \quad (3.12)$$

La verifica che si tratti effettivamente di due relazioni d'equivalenza si ottiene immediatamente. Vediamola per la  $\sim$  (per la  $\sim'$  è analoga).

- **Riflessività:**

Dobbiamo dimostrare che  $x \sim x$  per ogni  $x \in G$ . Questo significa verificare che  $x^{-1}x \in H$ .

$$x \sim x \iff x^{-1}x \in H.$$

Ora, sappiamo che  $x^{-1}x = 1$ , dove 1 è l'elemento neutro di  $G$ . Poiché  $H$  è un sottogruppo di  $G$ , l'elemento neutro 1 appartiene a  $H$ .

$$x^{-1}x = 1 \in H.$$

Quindi  $x \sim x$  per ogni  $x \in G$ .

- **Simmetria:**

Supponiamo che  $x \sim y$ , cioè  $x^{-1}y \in H$ . Quindi per la (S2)

$$(x^{-1}y)^{-1} = y^{-1}x \in H.$$

Pertanto,  $y \sim x$ , e la simmetria è dimostrata.

- **Transitività:**

Supponiamo che  $x \sim y$  e  $y \sim z$ , cioè  $x^{-1}y \in H$  e  $y^{-1}z \in H$ . Dobbiamo dimostrare che  $x \sim z$ , cioè  $x^{-1}z \in H$ .

Osserviamo che:

$$x^{-1}z = x^{-1}y \cdot y^{-1}z.$$

Poiché  $x^{-1}y \in H$  e  $y^{-1}z \in H$ , e  $H$  è chiuso rispetto al prodotto (essendo un sottogruppo), abbiamo che:

$$x^{-1}z = (x^{-1}y)(y^{-1}z) \in H.$$

Pertanto,  $x \sim z$ , e la transitività è dimostrata.

Il legame tra queste relazioni d'equivalenza e le classi laterali è espresso dalla seguente:

**Proposizione 3.5.2** *Sia  $G$  un gruppo e  $H \leq G$  e siano  $\sim$  (risp.  $\sim'$ ) la relazione d'equivalenza (3.11) (risp. (3.12)). Allora la classe d'equivalenza  $[x]_{\sim}$  (risp.  $[x]_{\sim'}$ ) di un elemento  $x \in G$  coincide con la classe laterale sinistra (risp. destra) di  $x$  rispetto ad  $H$ , ossia*

$$[x]_{\sim} = xH \text{ (risp. } [x]_{\sim'} = Hx) \quad (3.13)$$

**Dimostrazione:** Dimostriamo la  $[x]_{\sim} = xH$  con la doppia inclusione.

- $[x]_{\sim} \subseteq xH$ : Per definizione,  $[x]_{\sim}$  è la classe d'equivalenza di  $x$  rispetto alla relazione  $\sim$ . La relazione  $y \sim x$  implica che  $yx^{-1} \in H$ , quindi  $y = xh$  per qualche  $h \in H$ . Se  $y \in [x]_{\sim}$ , allora  $y = xh$  per qualche  $h \in H$ , e quindi  $y \in xH$ . Dunque,  $[x]_{\sim} \subseteq xH$ .
- $xH \subseteq [x]_{\sim}$ : Consideriamo un elemento arbitrario  $y \in xH$ . Allora  $y = xh$  per qualche  $h \in H$ . Poiché  $y = xh$ , abbiamo che  $yx^{-1} = h$ , e siccome  $h \in H$ , segue che  $y \sim x$ . Pertanto,  $y \in [x]_{\sim}$ . Quindi,  $xH \subseteq [x]_{\sim}$ .

Poiché entrambe le inclusioni sono verificate, abbiamo che  $[x]_{\sim} = xH$ . La dimostrazione per  $[x]_{\sim'} = Hx$  è analoga e segue lo stesso schema, considerando le classi laterali destre.  $\square$

La proposizione seguente mostra che le classi laterali sinistre e destre hanno tutte la stessa cardinalità e lo stesso vale per cardinalità degli spazi quoziente  $G/\sim$  e  $G/\sim'$  rispetto alle relazioni d'equivalenza (3.11) e (3.12).

**Proposizione 3.5.3** *Sia  $G$  un gruppo e  $H \leq G$ . Allora*

$$|xH| = |Hy|, \forall x, y \in G \quad (3.14)$$

$$|G/\sim| = |G/\sim'|. \quad (3.15)$$

**Dimostrazione:** Sia  $x \in G$  fissato e consideriamola classe laterale sinistra  $x$  rispetto ad  $H$ , ovvero  $xH = \{xh \mid h \in H\}$ . Vogliamo dimostrare che  $xH$  è in biezione con  $H$ , il che implica che tutti i laterali sinistri di  $H$  hanno la stessa cardinalità di  $H$ . Definiamo l'applicazione  $f : H \rightarrow xH$  come:

$$f(h) = xh \quad \text{per ogni } h \in H.$$

Verifichiamo che  $f$  è una biezione:

- *Iniettività:* Supponiamo che  $f(h_1) = f(h_2)$ , cioè  $xh_1 = xh_2$ . Per la legge di cancellazione si ottiene  $h_1 = h_2$ . Quindi,  $f$  è iniettiva.
- *Suriettività:* per costruzione.

Poiché  $f$  è sia iniettiva che suriettiva, essa è una biezione. Di conseguenza,  $xH$  ha la stessa cardinalità di  $H$ . In modo analogo si dimostra che dato  $y \in G$  l'applicazione

$$g : H \rightarrow Hy, \quad g(h) = hy$$

è una bigezione e che quindi  $|Hy| = |H|$ . Abbiamo quindi dimostrato che  $|Hy| = |H| = |xH|$ , per ogni  $x, y \in G$ , ossia la (3.14). Per dimostrare la (3.15) definiamo un'applicazione

$$F : G/\sim \rightarrow G/\sim', \quad F(xH) = Hx^{-1}.$$

Verifichiamo che  $F$  è ben definita ed invertibile.

- *Ben definita:* Supponiamo che  $xH = yH$ . Ciò significa che esiste  $h \in H$  tale che  $x = yh$ . Prendiamo l'inverso di  $x$ , otteniamo:

$$x^{-1} = (yh)^{-1} = h^{-1}y^{-1}.$$

Di conseguenza, possiamo scrivere:

$$Hx^{-1} = H(h^{-1}y^{-1}) = Hy^{-1}.$$

L'uguaglianza  $H(h^{-1}y^{-1}) = Hy^{-1}$  deriva dal fatto che  $h^{-1} \in H$  e moltiplicare un elemento a sinistra per un elemento di  $H$  non cambia la classe laterale destra. Pertanto,  $Hx^{-1} = Hy^{-1}$ , il che dimostra che  $F$  è ben definita.

- *Inversa di  $F$* : è immediato verificare che l'inversa di  $F$  è data da

$$F^{-1} : G/\sim' \rightarrow G/\sim, F^{-1}(Hx) = x^{-1}H.$$

Poiché  $F$  è ben definita e invertibile, essa è una bigezione e la (3.15) è dimostrata.  $\square$

**Notazione 3.5.4** La cardinalità di  $|G/\sim| = |G/\sim'|$  prende il nome di *indice di  $H$  in  $G$*  e si indica con  $[G : H]$ .

Il seguente teorema, insieme ai suoi corollari, rappresenta senza dubbio i risultati più importanti nella teoria dei gruppi finiti.

**Teorema 3.5.5 (teorema di Lagrange)** *Sia  $G$  un gruppo finito e  $H \leq G$  un suo sottogruppo. Allora*

$$|G| = [G : H] \cdot |H|. \quad (3.16)$$

**Dimostrazione:** Dalla Proposizione 3.5.3, sappiamo che ogni classe laterale (sinistra o destra) ha la stessa cardinalità, pari a  $|H|$ . Le classi laterali forniscono una partizione dell'insieme  $G$ . Poiché  $G$  è l'unione disgiunta di  $[G : H]$  classi laterali, ciascuna delle quali ha cardinalità  $|H|$ , otteniamo

$$|G| = [G : H] \cdot |H|.$$

Questo conclude la dimostrazione.  $\square$

Una conseguenza immediata del teorema di Lagrange è il seguente:

**Corollario 3.5.6** *Sia  $G$  un gruppo finito e  $H \leq G$ . Allora l'ordine di  $H$  divide quello di  $G$*

**Osservazione 3.5.7** Il teorema di Lagrange afferma che, in un gruppo finito  $G$ , ogni sottogruppo ha un ordine che divide l'ordine di  $G$ . Tuttavia, il fatto che un intero positivo divida l'ordine di  $G$  non implica necessariamente l'esistenza di un sottogruppo di tale ordine. Ad esempio, consideriamo il gruppo alterno  $A_4$ , la cui cardinalità è 12. Nonostante 6 divida 12, non esiste alcun sottogruppo di  $A_4$  con ordine 6, come dimostreremo in seguito (cfr. Corollario 6.2.5).



**Corollario 3.5.8** *Sia  $G$  un gruppo finito e  $H \leq G$ . Allora, per ogni  $x \in G$ , si ha:*

- (i)  $o(x) \mid |G|$ , dove  $o(x)$  è l'ordine dell'elemento  $x$ ;
- (ii)  $x^{|G|} = 1$ .

**Dimostrazione:** (i): Dal teorema di Lagrange, sappiamo che l'ordine di ogni sottogruppo di  $G$  divide l'ordine di  $G$ . In particolare (cf. (3.3))

$$|\langle x \rangle| = o(x) \mid |G|.$$

(ii): Poiché, dal punto (i),  $o(x) \mid |G|$  l'uguaglianza  $x^{|G|} = 1$  segue dalla (i) della Proposizione 1.3.33.  $\square$

**Corollario 3.5.9** *Sia  $G$  un gruppo finito di ordine  $p$ , con  $p$  primo. Allora:*

- (i) *gli unici sottogruppi di  $G$  sono quelli banali;*
- (ii)  *$G$  è ciclico ed è generato da qualunque  $x \in G$ ,  $x \neq 1$ , ossia  $G = \langle x \rangle$ .*

**Dimostrazione:** (i): Sia  $H \leq G$  un sottogruppo di  $G$ . Dal Corollario 3.5.6, sappiamo che l'ordine di  $H$  deve dividere l'ordine di  $G$ . Poiché  $|G| = p$  e  $p$  è primo, i divisori di  $p$  sono solo 1 e  $p$ . Quindi, l'ordine di  $H$  può essere soltanto 1 o  $p$ . Se  $|H| = 1$ , allora  $H = \{1\}$ , il sottogruppo banale. Se  $|H| = p$ , allora  $H = G$ , poiché l'ordine di  $H$  è uguale all'ordine di  $G$ . Di conseguenza, gli unici sottogruppi di  $G$  sono  $\{1\}$  e  $G$  stesso.

(ii): Ora dimostriamo che  $G$  è ciclico. Poiché  $|G| = p$ , per (i) del Corollario 3.5.8, ogni elemento  $x \in G$  ha un ordine che divide  $p$ . Essendo  $p$  primo, l'ordine di  $x$  può essere soltanto 1 o  $p$ . Se  $o(x) = 1$ , allora  $x = 1$ . Se  $o(x) = p$ , allora  $x$  genera tutto il gruppo  $G$ , ossia  $G = \langle x \rangle$ . Quindi, qualunque elemento  $x \in G$  con  $x \neq 1$  genera  $G$ , il che dimostra che  $G$  è ciclico.  $\square$

**Osservazione 3.5.10** Dimostreremo in seguito (cfr. Corollario 7.1.5) che, se un gruppo  $G$  non possiede sottogruppi propri diversi da  $\{1\}$ , allora  $G$  ha ordine primo  $p$  (e quindi è ciclico per il Corollario 3.5.8).

Usando i Corollari 3.5.6 e 3.5.8 si riottengono alcuni risultati classici sulla teoria elementare dei numeri, riassunti nei due corollari seguenti. Ricordiamo che la funzione di Eulero  $\phi : \mathbb{N}^+ \rightarrow \mathbb{N}^+$  conta il numero di interi positivi minori di  $n$  che sono coprimi con  $n$ , ovvero il numero di interi  $a$  tali che  $(a, n) = 1$ . Formalmente, è definita come:

$$\phi(n) = |\{a \in \mathbb{N}^+ \mid 1 \leq a < n, (a, n) = 1\}|$$

**Corollario 3.5.11 (teorema di Eulero-Fermat)** Siano  $a, n \in \mathbb{N}^+$  con  $(a, n) = 1$ . Allora

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

**Dimostrazione:** Indichiamo con  $U(\mathbb{Z}_n)$  il gruppo (moltiplicativo) delle classi invertibili modulo  $n$ :

$$U(\mathbb{Z}_n) = \{[x]_n \in \mathbb{Z}_n \mid (x, n) = 1\}.$$

Per definizione di funzione di Eulero e per la (1.22) si ottiene  $|U(\mathbb{Z}_n)| = \phi(n)$ . Poiché  $(a, n) = 1$ , la classe  $[a]_n$  appartiene a  $U(\mathbb{Z}_n)$ . Per la (ii) del Corollario 3.5.8 applicato a  $G = U(\mathbb{Z}_n)$  e  $x = [a]_n$ , otteniamo

$$[a]_n^{\phi(n)} = [1]_n.$$

Questa uguaglianza tra classi equivale alla congruenza  $a^{\phi(n)} \equiv 1 \pmod{n}$ , come voluto.  $\square$

**Corollario 3.5.12** Siano  $a$  e  $n$  interi positivi. Allora

$$n \mid \phi(a^n - 1).$$

**Dimostrazione:** Consideriamo il gruppo  $U(\mathbb{Z}_m)$ ,  $m = a^n - 1$ . Per la (1.22) il suo ordine è dato da  $|U(\mathbb{Z}_m)| = \phi(a^n - 1)$  e  $[a]_m$  appartiene a questo gruppo, in quanto  $a$  è coprimo con  $a^n - 1$ . Osserviamo anche che  $o([a]_m) = n$ . Infatti  $[a]_m^n = [1]_m$  ( $m = a^n - 1 \mid a^n - 1$ ) e  $a^d - 1$  non è divisibile per  $a^n - 1$  per  $d < n$  (e dunque  $n$  è il più piccolo intero positivo tale che  $[a]_m^n = [1]_m$ ). Per la (i) del Corollario 3.5.8 si ottiene dunque

$$o([a]_m) = n \mid |U(\mathbb{Z}_m)| = \phi(a^n - 1).$$

$\square$

### 3.5.1 Ordine del prodotto di due elementi<sup>1</sup>

**Proposizione 3.5.13** Sia  $G$  un gruppo e siano  $x, y \in G$ , con  $o(x) = m$  e  $o(y) = n$ , tali che  $(m, n) = 1$ . Se  $x$  e  $y$  commutano, allora  $o(xy) = mn = [m, n]$ , dove  $[m, n]$  denota il minimo comune multiplo tra  $m$  e  $n$ .

<sup>1</sup>Questa sezione non rientra nel programma d'esame.

**Dimostrazione:** Poiché  $x$  e  $y$  commutano, possiamo scrivere:

$$(xy)^{mn} = x^{mn}y^{mn} = (x^m)^n(y^n)^m = 1.$$

Da ciò segue che l'ordine di  $xy$ , denotato con  $k := o(xy)$ , divide il minimo comune multiplo di  $m$  e  $n$ , ovvero  $k \mid [m, n] = mn$ .

Osserviamo ora che  $(m, n) = 1$  implica che i sottogruppi generati da  $x$  e  $y$ , ovvero  $\langle x \rangle$  e  $\langle y \rangle$ , hanno intersezione banale:

$$\langle x \rangle \cap \langle y \rangle = \{1\}.$$

Infatti, se  $z \in \langle x \rangle \cap \langle y \rangle$ , allora  $o(z)$  divide sia  $m$  che  $n$ . Poiché  $(m, n) = 1$ , ciò implica che  $o(z) = 1$ , quindi  $z = 1$ . A questo punto, considerando che  $(xy)^k = x^k y^k = 1$ , otteniamo che:

$$x^k = y^{-k} \in \langle x \rangle \cap \langle y \rangle = \{1\},$$

da cui segue che  $x^k = y^k = 1$ . Questo implica che  $m \mid k$  e  $n \mid k$  e quindi  $[m, n] \mid k$  e pertanto  $k = [m, n]$ .  $\square$

**Corollario 3.5.14** Sia  $G$  un gruppo e siano  $x, y \in G$  con ordini finiti  $o(x) = m$  e  $o(y) = n$ . Se  $x$  e  $y$  commutano, allora esiste  $z \in G$  tale che  $o(z) = [m, n]$ .

**Dimostrazione:** Sia  $\mathcal{P} = \{p \text{ primo} \mid p \mid m \text{ oppure } p \mid n\}$  l'unione dei primi che compaiono nelle fattorizzazioni di  $m$  o di  $n$ . Per ogni  $p \in \mathcal{P}$  indichiamo con  $\alpha_p \geq 0$  l'esponente di  $p$  in  $m$  (ponendo  $\alpha_p = 0$  se  $p \nmid m$ ) e con  $\beta_p \geq 0$  l'esponente di  $p$  in  $n$  (ponendo  $\beta_p = 0$  se  $p \nmid n$ ). Allora

$$m = \prod_{p \in \mathcal{P}} p^{\alpha_p}, \quad n = \prod_{p \in \mathcal{P}} p^{\beta_p}.$$

Definiamo

$$m' = \prod_{\substack{p \in \mathcal{P} \\ \alpha_p \geq \beta_p}} p^{\alpha_p}, \quad n' = \prod_{\substack{p \in \mathcal{P} \\ \beta_p > \alpha_p}} p^{\beta_p}.$$

È chiaro che  $m' \mid m$  e  $n' \mid n$ . Inoltre  $(m', n') = 1$ , poiché per ogni  $p \in \mathcal{P}$  le condizioni  $\alpha_p \geq \beta_p$  e  $\beta_p > \alpha_p$  sono mutuamente esclusive, quindi nessun primo compare con esponente positivo in entrambi i prodotti. Inoltre, per ogni  $p \in \mathcal{P}$  l'esponente di  $p$  in  $m'n'$  è

$$\begin{cases} \alpha_p & \text{se } \alpha_p \geq \beta_p, \\ \beta_p & \text{se } \beta_p > \alpha_p, \end{cases} \quad \text{ossia } \max\{\alpha_p, \beta_p\}.$$

Dunque

$$m'n' = \prod_{p \in \mathcal{P}} p^{\max(\alpha_p, \beta_p)} = [m, n].$$

Poniamo ora  $a = x^{m/m'}$  e  $b = y^{n/n'}$ . Poiché  $x$  e  $y$  commutano, anche  $a$  e  $b$  commutano. Per la (iii) della Proposizione 1.3.33, otteniamo

$$o(a) = \frac{m}{(m, m/m')} = \frac{m}{m/m'} = m', \quad o(b) = \frac{n}{(n, n/n')} = \frac{n}{n/n'} = n'.$$

Poiché  $(m', n') = 1$  e  $ab = ba$ , per la Proposizione 3.5.13 segue

$$o(ab) = o(a)o(b) = m'n' = [m, n].$$

Ponendo  $z = ab$  si ha dunque  $o(z) = [m, n]$ , come volevasi dimostrare.  $\square$

**Osservazione 3.5.15** I risultati precedenti non valgono se gli elementi non commutano. Per esempio in  $S_3$  gli elementi  $x = (12)$  e  $y = (123)$  hanno ordini primi ( $o(x) = 2$  e  $o(y) = 3$ ),  $xy = (23)$  e  $o(xy) = o((23)) = 2 \neq 6 = [2, 3]$ . Anche se gli elementi commutano ma gli ordini non sono primi il risultato non vale. per esempio la classe  $[2]_4 \in \mathbb{Z}_4$  ha ordine due, commuta con se stessa ma l'ordine di  $[0]_4 = [2]_4 + [2]_4$  è 1. Si dimostra (noi non lo faremo) che dati  $m, n, r$  numeri naturali diversi da 1 esiste sempre un gruppo finito  $G$  e  $x, y \in G$  tali che  $o(x) = m, o(y) = n$  e  $o(xy) = r$ .

## 3.6 Esercizi

**Esercizio 3.1** Dire quali dei seguenti insiemi  $H$  sono sottogruppi del gruppo  $G$  indicato:

1.  $G = (\mathbb{R}, +), H = \{\ln a \mid a \in \mathbb{Q}, a > 0\}$ ;
2.  $G = (\mathbb{R}, +), H = \{\ln n \mid n \in \mathbb{Z}, n > 0\}$ ;
3.  $G = (\mathbb{R}, +), H = \{x \in \mathbb{R} \mid \tan x \in \mathbb{Q}\}$ ;
4.  $G = (\mathbb{R}^*, \cdot), H = \{2^n 3^m \mid m, n \in \mathbb{Z}\}$ ;
5.  $G = (\mathbb{R} \times \mathbb{R}, +), H = \{(x, y) \mid y = 2x\}$ .

**Esercizio 3.2** Si consideri l'insieme  $G = \{(a, b) \mid a, b \in \mathbb{Q}, a \neq 0\}$  con l'operazione binaria definita da

$$(a, b) \cdot (c, d) = (ac, ad + b).$$

Dopo aver verificato che  $(G, \cdot)$  è un gruppo, si verifichi che  $H = \{(a, b) \in G \mid b = 0\} < G$ .

**Esercizio 3.3** Sia  $X$  un insieme e sia  $\Delta_X$  la differenza simmetrica, cioè l'operazione su  $\mathcal{P}(X)$  definita da:

$$A, B \in \mathcal{P}(X), A \Delta_X B = (A \setminus B) \cup (B \setminus A).$$

Si dimostri che  $(\mathcal{P}(X), \Delta_X)$  è un gruppo abeliano. Sia  $Y \subseteq X$ . Si dimostri che  $(\mathcal{P}(Y), \Delta_Y) \leq (\mathcal{P}(X), \Delta_X)$ .

**Esercizio 3.4** Si dimostri che l'insieme  $G$  delle funzioni da  $\mathbb{R}$  in  $\mathbb{R}$  con l'operazione definita da

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

è un gruppo abeliano e che i seguenti sottoinsiemi sono sottogruppi di  $G$ .

1.  $C(\mathbb{R}) = \{\text{funzioni continue } f : \mathbb{R} \rightarrow \mathbb{R}\};$
2.  $D(\mathbb{R}) = \{\text{funzioni derivabili } f : \mathbb{R} \rightarrow \mathbb{R}\};$
3.  $I(\mathbb{R}) = \{\text{funzioni integrabili } f : \mathbb{R} \rightarrow \mathbb{R}\}.$

**Esercizio 3.5** In ognuno dei casi seguenti mostrare che  $H$  è un sottogruppo di  $S_X$ .

1.  $X = \{x \in \mathbb{R} \mid x \neq 0, 1\}, H = \{id, f, g\}$ , dove  $f(x) = \frac{1}{1-x}, g(x) = \frac{x-1}{x}$ ;
2.  $X = \{x \in \mathbb{R} \mid x \neq 0\}, H = \{id, f, g, h\}$ , dove  $f(x) = \frac{1}{x}, g(x) = -x, h(x) = -\frac{1}{x}$ ;
3.  $X = \{x \in \mathbb{R} \mid x \neq 0, 1\}, H = \{id, f, g, h, j, k\}$ , dove  $f(x) = 1-x, g(x) = \frac{1}{x}, h(x) = \frac{1}{1-x}, j(x) = \frac{x-1}{x}$  e  $k(x) = \frac{x}{x-1}$ .

**Esercizio 3.6** Per ogni coppia di numeri reali  $a, b, a \neq 0$ , si definisca la funzione  $f_{a,b} : \mathbb{R} \rightarrow \mathbb{R}, x \mapsto ax + b$ . Si dimostri che:

1.  $f_{a,b} \in S_{\mathbb{R}}$ ;
2.  $f_{a,b} \circ f_{c,d} = f_{ac, ad+b}$ ;
3.  $f_{a,b}^{-1} = f_{a^{-1}, -ba^{-1}}$ ;
4.  $H = \{f_{a,b} \mid a \in \mathbb{R}, a \in \mathbb{R}^*\} < S_{\mathbb{R}}$ .

**Esercizio 3.7** Sia  $G = D_n, n \geq 3$ , il gruppo diedrale. Dimostrare che  $G$  ha esattamente  $n$  elementi di ordine 2 se e solo se  $n$  è dispari. Nel caso che  $n$  sia dispari dimostrare che gli  $n$  elementi di  $G$  che non hanno ordine 2 formano un sottogruppo abeliano di  $G$ .

**Esercizio 3.8** Sia  $X$  un insieme finito e  $A$  un sottoinsieme di  $X$ . Sia  $H$  il sottoinsieme di  $S_X$  che consiste di tutte le permutazioni  $f \in S_X$  tale che  $f(x) \in A$ , per ogni  $x \in A$ .

1. Dimostrare che  $H < S_X$ ;
2. Fornire un esempio dove la conclusione del punto precedente non vale se  $X$  é un insieme infinito.

**Esercizio 3.9**

- (1) Dimostrare che l'insieme delle trasposizioni di  $S_n$  genera  $S_n$ ;
- (2) Dimostrare che l'insieme  $\{(12), (13), \dots, (1n)\}$  genera  $S_n$ ;
- (3) Dimostrare che i cicli di lunghezza 3 generano  $A_n$ , for  $n \geq 3$ ;
- (4) Dimostrare che l'insieme  $\{(123), (124), \dots, (12n)\}$  genera  $A_n$ ;
- (5) Dimostrare che  $S_n$  é generato da  $\{(12), (12 \dots n)\}$ .

(Suggerimento: per (3) usare  $(13)(12) = (123)$  e  $(12)(34) = (321)(134)$ ; per (4) usare  $(abc) = (1ca)(1ab)$ ,  $(1ab) = (1b2)(12a)(12b)$  e  $(1b2) = (12b)^2$ ; per (5) usare  $(1 \dots n)(12)(1 \dots n)^{-1} = (23)$  e  $(12)(23)(12) = (13)$ ).

**Esercizio 3.10** Siano  $H$  e  $K$  sottogruppi di un gruppo finito  $G$  tali che  $H \leq K \leq G$ . Si dimostri che  $[G : H] = [G : K][K : H]$ .