

## Capitolo 3

# Insiemi con un'operazione

### 3.1 Gruppoidi, semigrupperi, monoidi

**Definizione 309** Un'operazione binaria su un insieme  $G$  è una funzione:

$$f : G \times G \longrightarrow G$$

Quindi, un'operazione binaria  $f$  su un insieme  $G$  è una legge che associa ad ogni coppia  $(a, b) \in G \times G$  un elemento  $f[(a, b)] \in G$ . L'elemento  $f[(a, b)]$  viene spesso indicato con il simbolo  $a * b$ .

**Esempio 310** Diamo due esempi di operazioni binarie:

- 1) Un'operazione binaria in  $R$  è l'usuale moltiplicazione. Ad ogni coppia di numeri reali  $a$  e  $b$  viene associato il numero reale  $a \cdot b$ .
- 2) Un'operazione binaria in  $R$  è l'usuale addizione. Ad ogni coppia di numeri reali  $a$  e  $b$  viene associato il numero reale  $a + b$ .

**Nota 311** L'operazione binaria può essere indicata con qualunque simbolo. Spesso si usa però il simbolo di moltiplicazione  $\cdot$  (in questo caso diciamo che abbiamo utilizzato la **notazione moltiplicativa**) o il simbolo di addizione  $+$  (in questo caso diciamo che abbiamo utilizzato la **notazione additiva**).

**Definizione 312** Un **gruppoide** è una coppia  $(G, *)$  dove  $G$  è un insieme e  $*$  è un'operazione binaria in  $G$ .

**Esempio 313** Diamo alcuni esempi di gruppoidi:

- 1)  $(R, \cdot)$  è un gruppoide. Vedere l'esempio 310.
- 2)  $(R, +)$  è un gruppoide. Vedere l'esempio 310.
- 3)  $(N, +)$  è un gruppoide.
- 4)  $(N, \cdot)$  è un gruppoide.
- 5)  $(Z, +)$  è un gruppoide.
- 6)  $(Z, \cdot)$  è un gruppoide.
- 7)  $(Q, +)$  è un gruppoide.

- 8)  $(Q, \cdot)$  è un gruppoide.  
 9)  $(C, +)$  è un gruppoide. Dove  $C$  è l'insieme dei numeri complessi.  
 10)  $(C, \cdot)$  è un gruppoide.  
 11)  $(M(R, p, q), +)$  è un gruppoide.  
 12)  $(M(R, n, n), \cdot)$  è un gruppoide.  
 13)  $(R^*, :)$  (dove  $:$  è l'operazione di divisione) è un gruppoide.  
 14) Indichiamo con  $S$  l'insieme delle **parole**, cioè l'insieme delle stringhe finite di simboli dell'alfabeto italiano. Notiamo che le parole possono anche non avere alcun significato. Per esempio, anche  $AQRZQA$  è una parola. In  $S$  inseriamo anche la **stringa vuota** che non è dotata di alcun simbolo. In  $S$  introduciamo la funzione  $*$  di giustapposizione. Essa associa ad una coppia di parole la parola ottenuta ponendo una di seguito all'altra le due parole. Per esempio, date le parole  $STUD$  e  $ENTE$  abbiamo  $STUD * ENTE = STUDENTE$ . Ovviamente  $(S, *)$  è un gruppoide.  
 15) Dato un insieme  $A$ , si ha che  $(A^A, \circ)$  è un gruppoide. Ricordiamo che  $A^A$  è l'insieme delle funzioni  $f : A \longrightarrow A$  (vedi capitolo precedente) e  $\circ$  è l'operazione di composizione di funzioni.

**Definizione 314** Dato un gruppoide finito  $(G, *)$ , possiamo considerare la **tabella dell'operazione** di  $G$ . Per far ciò indichiamo con  $a_1, a_2, \dots, a_n$  gli elementi di  $G$ . La tabella dell'operazione di  $G$  è la matrice quadrata di ordine  $n$  tale che al posto  $i, j$  vi è l'elemento  $a_i * a_j$ . Per rendere più esplicito il tutto si scrivono a lato gli elementi. Si ha quindi una tabella così fatta:

	$a_1$	$a_2$	$\dots$	$a_j$	$\dots$	$a_n$
$a_1$	$a_1 * a_1$	$a_1 * a_2$	$\dots$	$a_1 * a_j$	$\dots$	$a_1 * a_n$
$a_2$	$a_2 * a_1$	$a_2 * a_2$	$\dots$	$a_2 * a_j$	$\dots$	$a_2 * a_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$a_i$	$a_i * a_1$	$a_i * a_2$	$\dots$	$a_i * a_j$	$\dots$	$a_i * a_n$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
$a_n$	$a_n * a_1$	$a_n * a_2$	$\dots$	$a_n * a_j$	$\dots$	$a_n * a_n$

**Esercizio 315** Sia  $G$  un insieme con  $n$  elementi. Quanti gruppoidi  $(G, \cdot)$  esistono?

**Esempio 316** Consideriamo l'insieme  $G = \{P, D\}$ . Introduciamo in esso un'operazione binaria, che indichiamo con il simbolo  $\cdot$ , ponendo:

$$P \cdot P = P, \quad P \cdot D = P, \quad D \cdot P = P, \quad D \cdot D = D$$

Abbiamo un gruppoide la cui tabella dell'operazione è:

	$P$	$D$
$P$	$P$	$P$
$D$	$P$	$D$

Facciamo osservare che l'operazione non è stata introdotta a caso. Con  $P$  si intendono infatti i numeri pari e con  $D$  si intendono i numeri dispari. La formula  $P \cdot P = P$  significa che il prodotto di un numero pari per un numero pari è un numero pari. Analogamente per gli altri prodotti.

**Esercizio 317** Scrivere la tabella dell'operazione del gruppoide  $(G = \{P, D\}, +)$  dove l'operazione di addizione  $+$  è definita da:  
 $P + P = D + D = P$ ,  $D + P = P + D = D$ .

**Definizione 318** Un gruppoide  $(G, *)$  si dice **semigrupp** se l'operazione  $*$  verifica la seguente:

**proprietà associativa:**  $a * (b * c) = (a * b) * c \quad \forall a \in G, \forall b \in G, \forall c \in G$ .

**Nota 319** In un semigrupp possiamo quindi evitare di utilizzare le parentesi quando consideriamo il prodotto di tre o più elementi. Scriviamo, per esempio,  $a * b * c$ . La proprietà associativa ci assicura infatti che, comunque noi associamo i termini, otteniamo sempre lo stesso risultato.

**Esercizio 320** Verificare che tutti i gruppoidi dati nell'esempio 313, escluso l'esempio 13, sono semigruppi.

**Definizione 321** Dato un gruppoide  $(G, *)$ , un suo elemento  $e$  si dice **elemento neutro** se esso verifica le seguenti condizioni:

$$\forall g \in G \quad e * g = g * e = g$$

**Teorema 322** In un gruppoide esiste al massimo un elemento neutro.

**DIMOSTRAZIONE.** Siano  $e$  e  $e'$  elementi neutri. Si ha quindi:

$$1) \forall g \in G \quad e * g = g * e = g$$

$$2) \forall g \in G \quad e' * g = g * e' = g.$$

Consideriamo il prodotto  $e * e'$ . Applicando 1) si ha  $e * e' = e'$ . Applicando 2) si ha  $e * e' = e$ . Da tutto ciò segue  $e = e'$ .  $\square$

**Esercizio 323** Determinare, tra tutti i gruppoidi dati in 313, quali sono dotati di elemento neutro.

**Esempio 324** Notiamo, in particolare, che:

Il gruppoide  $(R, +)$  ha come elemento neutro il numero 0.

L'esempio precedente giustifica la seguente definizione.

**Definizione 325** Quando utilizziamo la notazione additiva, se un gruppoide  $(G, +)$  è dotato di elemento neutro, indichiamo tale elemento con il simbolo 0. Quindi l'elemento neutro 0 ha la seguente proprietà:

$$\forall g \in G \quad g + 0 = 0 + g = g$$

**Esempio 326** Il gruppoide  $(R, \cdot)$  ha come elemento neutro il numero 1.

L'esempio precedente giustifica la seguente definizione.

**Definizione 327** Quando utilizziamo la notazione moltiplicativa, se un gruppoide  $(G, \cdot)$  è dotato di elemento neutro, indichiamo tale elemento con il simbolo 1. Quindi l'elemento neutro 1 ha la seguente proprietà:

$$\forall g \in G \quad g \cdot 1 = 1 \cdot g = g$$

**Definizione 328** Un **monoide** è un semigruppato dotato di elemento neutro. Un monoide è quindi un insieme dotato di un'operazione binaria che verifica la proprietà associativa e che è dotato di elemento neutro.

**Esempio 329** Vediamo quali degli esempi dati in 313 è un monoide.

- 1)  $(R, \cdot)$  è un monoide. Il numero 1 è l'elemento neutro.
- 2)  $(R, +)$  è un monoide. Il numero 0 è l'elemento neutro.
- 3)  $(N, +)$  **non** è un monoide. Non esiste l'elemento neutro.
- 4)  $(N, \cdot)$  è un monoide. Il numero 1 è l'elemento neutro.
- 5)  $(Z, +)$  è un monoide. Il numero 0 è l'elemento neutro.
- 6)  $(Z, \cdot)$  è un monoide. Il numero 1 è l'elemento neutro.
- 7)  $(Q, +)$  è un monoide. Il numero 0 è l'elemento neutro.
- 8)  $(Q, \cdot)$  è un monoide. Il numero 1 è l'elemento neutro.
- 9)  $(C, +)$  è un monoide. Il numero 0 è l'elemento neutro.
- 10)  $(C, \cdot)$  è un monoide. Il numero 1 è l'elemento neutro.
- 11)  $(M(R, p, q), +)$  è un monoide. La matrice nulla 0 è l'elemento neutro.
- 12)  $(M(R, n, n), \cdot)$  è un monoide. La matrice unità  $I$  è l'elemento neutro.
- 13)  $(R^*, :)$  **non** è un monoide. Non è verificata la proprietà associativa.
- 14)  $(S, *)$ , dove  $S$  è l'insieme delle stringhe, è un monoide. La stringa vuota è l'elemento neutro.
- 15) Dato un insieme  $A$ , si ha che  $(A^A, \circ)$  è un monoide. La funzione identica di  $A$  è l'elemento neutro.

**Definizione 330** Sia dato un gruppoide  $(G, *)$  dotato di elemento neutro  $e$ . Sia  $g$  un elemento di  $G$ . Un elemento  $g' \in G$  si dice **simmetrico** di  $g$  se esso verifica le seguenti condizioni:

$$g * g' = g' * g = e$$

**Teorema 331** Ogni elemento  $g$  di un monoide  $(G, *)$  è dotato di non più di un elemento simmetrico.

**DIMOSTRAZIONE.** Sia  $e$  l'elemento neutro di  $G$ . Sia  $g \in G$  e siano  $g'$  e  $g''$  simmetrici di  $g$ . Si ha allora:

- 1)  $g * g' = g' * g = e$
- 2)  $g * g'' = g'' * g = e$

Consideriamo il prodotto  $g' * g * g''$  (non abbiamo utilizzato le parentesi perchè si ha la proprietà associativa). Si ha:

$$g' * g * g'' = (g' * g) * g'' = (\text{per 1)}) e * g'' = g''.$$

$$\text{Si ha anche: } g' * g * g'' = g' * (g * g'') = (\text{per 2)}) g' * e = g'.$$

Da tutto ciò segue  $g' = g''$ .  $\square$

**Esempio 332** Consideriamo il monoide  $(R, +)$ . Sia  $g \in R$ . Il simmetrico di  $g$  è  $-g$ .

L'esempio precedente giustifica la seguente definizione.

**Definizione 333** Quando usiamo la notazione additiva, indichiamo il simmetrico di un elemento  $g$  con il simbolo  $-g$  e lo chiamiamo **opposto** di  $g$ . Quindi l'opposto di un elemento  $g$  di un monoide  $(G, +)$  verifica le condizioni:

$$g + (-g) = -g + g = 0$$

**Esempio 334** Consideriamo il monoide  $(R, \cdot)$ . Sia  $g \in R^*$ . Il simmetrico di  $g$  è  $g^{-1}$ .

L'esempio precedente giustifica la seguente definizione.

**Definizione 335** Quando utilizziamo la notazione moltiplicativa, indichiamo il simmetrico di un elemento  $g$  con il simbolo  $g^{-1}$  e lo chiamiamo **inverso** di  $g$ . Quindi l'inverso di un elemento  $g$  di un monoide  $(G, \cdot)$  verifica le condizioni:

$$g \cdot g^{-1} = g^{-1} \cdot g = 1$$

**Esercizio 336** Per ognuno dei monoidi dati nell'esempio 313 determinare tutti gli elementi dotati di simmetrico.

**Esercizio 337** Per ognuno dei gruppidi dati negli esempi 316 e 317 determinare tutti gli elementi dotati di simmetrico.

**Teorema 338** Sia  $(G, \cdot)$  un monoide e sia  $g \in G$  un elemento dotato di inverso. Sia esso  $g^{-1}$ . Allora anche  $g^{-1}$  è dotato di inverso. Esso è  $g$ . Tradotto in formule abbiamo:

$$(g^{-1})^{-1} = g$$

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

**Nota 339** Nel dare l'enunciato del teorema precedente abbiamo utilizzato la notazione moltiplicativa.

Utilizzando la notazione additiva, abbiamo:

$$-(-a) = a$$

**Teorema 340** Sia  $(G, \cdot)$  un monoide e siano  $g \in G$  e  $g' \in G$  elementi dotati di inversi che indichiamo con  $g^{-1}$  e  $g'^{-1}$  rispettivamente. Allora anche  $g \cdot g'$  è dotato di inverso. Esso è  $g'^{-1} \cdot g^{-1}$ . Tradotto in formule abbiamo:

$$(g \cdot g')^{-1} = g'^{-1} \cdot g^{-1}$$

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

**Esercizio 341** Enunciare il teorema precedente nel caso in cui si utilizzi la notazione additiva.

**Esercizio 342** Sia  $(G, \cdot)$  un monoide. Dimostrare che in esso non esiste alcun elemento che sia inverso di due elementi distinti.

## 3.2 Gruppi

**Definizione 343** Un **gruppo** è una coppia  $(G, *)$  dove  $G$  è un insieme e  $*$  è un'operazione binaria su  $G$  che verifica le seguenti proprietà:

1) è valida la proprietà associativa:

$$a * (b * c) = (a * b) * c \quad \forall a \in G, \forall b \in G, \forall c \in G$$

2) vi è l'elemento neutro. Esiste cioè un elemento  $e \in G$  tale che:

$$g * e = e * g = g \quad \forall g \in G$$

3) Ogni elemento  $g \in G$  è dotato di simmetrico. Per ogni elemento  $g \in G$  esiste cioè un elemento  $g' \in G$  tale che:

$$g * g' = g' * g = e$$

Un gruppo si dice **commutativo** (o **abeliano**<sup>1</sup>) se è verificata l'ulteriore condizione:

$$g * g' = g' * g \quad \forall g \in G, \forall g' \in G$$

**Nota 344** Dai teoremi 322 e 331 segue che in un gruppo si ha l'unicità dell'elemento neutro e del simmetrico di un elemento.

**Esempio 345** Diamo due esempi di gruppi abeliani:

1)  $(R, +)$  è un gruppo abeliano.

2)  $(R^*, \cdot)$  è un gruppo abeliano.

Si lascia come esercizio la verifica di ciò.

**Esercizio 346** Determinare quali dei gruppoidi assegnati in 313, in 316 e in 317 sono gruppi e quali sono gruppi abeliani.

**Esempio 347** Per ogni insieme  $A$ , sia:

$$T(A) = \{f : A \longrightarrow A \mid f \text{ biunivoca}\}$$

Le funzioni biunivoche di  $A$  in se stesso si dicono **trasformazioni** di  $A$ . Si ha che  $(T(A), \circ)$  è un gruppo. Infatti la composizione tra funzioni biunivoche è una funzione biunivoca. Quindi in  $T(A)$  è definita l'operazione di composizione. La composizione di funzioni verifica la proprietà associativa. La funzione identica  $id : A \longrightarrow A$  è l'elemento neutro. Ogni elemento di  $T(A)$  è dotato di elemento simmetrico. Un elemento di  $T(A)$  è infatti una funzione biunivoca  $f : A \longrightarrow A$ . L'elemento simmetrico di  $f$  è la funzione inversa  $f^{-1} : A \longrightarrow A$ . Sappiamo che  $f^{-1}$  è anch'essa biunivoca. Appartiene quindi a  $T(A)$ . Chiamiamo  $(T(A), \circ)$  **gruppo delle trasformazioni** di  $A$ .

<sup>1</sup>da Niels Henrik Abel (1802-1829), matematico norvegese.

**Esempio 348** Consideriamo un caso particolare del precedente esempio. Consideriamo il caso in cui  $A$  sia un insieme finito di cardinalità uguale a  $n$ . Il gruppo delle trasformazioni  $(T(A), \circ)$  viene detto **gruppo simmetrico** su  $n$  elementi. Esso viene indicato di solito con il simbolo  $\sigma_n$  o con il simbolo  $\Sigma_n$ .

**Esempio 349** Determiniamo il gruppo  $(\sigma_1, \circ)$ . Abbiamo  $\sigma_1 = T(A)$  dove  $A$  è un insieme formato da un solo elemento. Indichiamo questo elemento con il simbolo 1. Quindi  $A = \{1\}$ . Si ha ovviamente:  $\sigma_1 = \{id\}$ . Quindi  $\sigma_1$  ha un solo elemento.

**Esempio 350** Determiniamo il gruppo  $(\sigma_2, \circ)$ . Abbiamo  $\sigma_2 = T(A)$  con  $A = \{1, 2\}$ . Vi sono due funzioni biunivoche di  $A$  in  $A$ :

$$\begin{array}{ccc} id: & A & \longrightarrow A \\ & 1 & \longmapsto 1 \\ & 2 & \longmapsto 2 \end{array} \quad \begin{array}{ccc} a: & A & \longrightarrow A \\ & 1 & \longmapsto 2 \\ & 2 & \longmapsto 1 \end{array}$$

Indichiamo gli elementi di  $\sigma_2$  nel modo seguente:

$$id = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad a = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$$

Si ha  $a \circ a = id$ .

Da tutto ciò segue che la tavola dell'operazione del gruppo  $(\sigma_2, \circ)$  è la seguente:

$$\begin{array}{c|cc} & id & a \\ \hline id & id & a \\ a & a & id \end{array}$$

**Esempio 351** Determiniamo il gruppo  $(\sigma_3, \circ)$ .

Abbiamo  $\sigma_3 = T(A)$  con  $A = \{1, 2, 3\}$ .

Gli elementi di  $\sigma_3$  sono:

$$\begin{aligned} id &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} & a &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} & b &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\ c &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} & d &= \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} & e &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \end{aligned}$$

Si ha:

$$a \circ a = b \circ b = c \circ c = id$$

Si ha inoltre:

$$a \circ b = d \quad b \circ a = e$$

Da tutto ciò segue che  $(\sigma_3, \circ)$  non è un gruppo abeliano.

**Esercizio 352** Scrivere la tabella dell'operazione del gruppo  $(\sigma_3, \circ)$ .

**Nota 353** Abbiamo visto che il gruppo  $(\sigma_3, \circ)$  ha cardinalità uguale a 6 e non è abeliano. Si può dimostrare (noi non lo facciamo) che ogni gruppo con meno di 6 elementi è abeliano.

**Definizione 354** La cardinalità di un gruppo finito viene chiamata **ordine** del gruppo.

**Esercizio 355** Dimostrare che il gruppo simmetrico  $\sigma_n$  ha ordine uguale a  $n!$ . Ricordiamo che, per definizione, si ha:  $n! = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 3 \cdot 2 \cdot 1$ .

**Esempio 356** Sia  $GL(R, n)$  l'insieme delle matrici  $A \in M(R, n, n)$  che sono invertibili. Sappiamo che il prodotto di due matrici invertibili è una matrice invertibile. Quindi  $GL(R, n)$  è chiuso rispetto all'operazione di moltiplicazione. Si verifica (esercizio) che  $(GL(R, n), \cdot)$  è un gruppo non abeliano. Esso viene detto **gruppo lineare**.

**Esempio 357** Sia  $\pi$  un piano e siano  $r$  e  $s$  due rette di  $\pi$  ortogonali tra loro. Sia  $P = r \cap s$ . Consideriamo il seguente sottoinsieme di  $T(\pi)$ :

$$K = \{id, s_r, s_s, s_P\}$$

dove:

$s_r$  è la simmetria rispetto alla retta  $r$ ,

$s_s$  è la simmetria rispetto alla retta  $s$ ,

$s_P$  è la simmetria rispetto al punto  $P$ .

Si verifica facilmente (esercizio) che  $(K, \circ)$  è un gruppo abeliano. Esso viene detto **gruppo quadrimomia** o **gruppo di Klein**<sup>2</sup>.

**Esercizio 358** Determinare la tabella dell'operazione del gruppo di Klein.

**Esercizio 359** Dato un piano  $\pi$  si introduca in esso un'unità di misura. Dati comunque due punti  $P$  e  $Q$  di  $\pi$ , possiamo considerare la distanza tra  $P$  e  $Q$  relativa alla unità di misura data. Indichiamo questa distanza con il simbolo  $d(P, Q)$ . Sia  $f \in T(\pi)$ . Quindi  $f$  è una funzione biunivoca da  $\pi$  in  $\pi$ . La funzione  $f$  si dice **isometria** di  $\pi$  se essa conserva le distanze; cioè:

$$\forall P \in \pi \quad \forall Q \in \pi \quad d(f(P), f(Q)) = d(P, Q)$$

Dimostrare che l'insieme delle isometrie del piano  $\pi$  con l'operazione di composizione tra funzioni è un gruppo. Esso è chiamato **gruppo delle isometrie** del piano.

**Esempio 360** Sia dato un piano  $\pi$ , un suo punto  $P$  e  $\alpha$ , con  $0 \leq \alpha < 2\pi$ . Indichiamo con  $r_{P, \alpha}$  la trasformazione del piano data dalla rotazione intorno a  $P$  in senso antiorario di un angolo di ampiezza in radianti uguale ad  $\alpha$ . Chiaramente  $r_{P, \alpha}$  è una isometria.

Si verifica facilmente (esercizio) che l'insieme:

$$\{r_{P, k\pi/2} \mid k \in \{1, 2, 3, 4\}\}$$

con l'operazione di composizione è un gruppo abeliano.

<sup>2</sup>**Felix Christian Klein** (pronuncia: Klain) (1849, 1925), matematico tedesco.



**Esercizio 361** Scrivere la tavola dell'operazione del gruppo dato nell'esempio precedente.

**Esercizio 362** Verificare la verità o falsità della seguente affermazione.

Dato un elemento  $g$  di un gruppo  $(G, \cdot)$  si ha:

$$g = g^{-1} \iff g = 1.$$

**Teorema 363** Sia  $(G, \cdot)$  un gruppo. Dati  $a \in G, b \in G, c \in G$ , si hanno le seguenti **leggi di semplificazione**:

$$a \cdot b = a \cdot c \implies b = c$$

$$b \cdot a = c \cdot a \implies b = c$$

DIMOSTRAZIONE. Facile esercizio.  $\square$

**Teorema 364** Sia  $(G, \cdot)$  un gruppo. Siano dati  $a \in G$  e  $b \in G$ . Si ha:

1) esiste ed è unico un elemento  $x \in G$  tale che  $a \cdot x = b$

2) esiste ed è unico un elemento  $y \in G$  tale che  $y \cdot a = b$

DIMOSTRAZIONE. 1) Si verifica facilmente (esercizio) che l'unico elemento  $x$  verificante la condizione data è  $a^{-1} \cdot b$ .

2) Si verifica facilmente (esercizio) che l'unico elemento  $y$  verificante la condizione data è  $b \cdot a^{-1}$ .  $\square$

**Esercizio 365** Si considerino gli elementi  $a$  e  $b$  di  $\sigma_3$  dati nell'esempio 351. Determinare  $x \in \sigma_3$  e  $y \in \sigma_3$  tali che:

$$a \circ x = b \quad \text{e} \quad y \circ a = b$$

**Esercizio 366** Dati gli elementi  $s_r$  e  $s_s$  del gruppo di Klein  $(K, \circ)$  (vedere 357), determinare  $x \in K$  e  $y \in K$  tali che:

$$s_r \circ x = s_s \quad \text{e} \quad y \circ s_r = s_s$$

**Esercizio 367** In un gruppo  $(G, \cdot)$  è valida la seguente legge di cancellazione?

$$a \cdot b \cdot c = d \cdot b \cdot e \implies a \cdot c = d \cdot e$$

### 3.3 Sottogruppi

**Definizione 368** Sia  $(G, \cdot)$  un gruppo e sia  $H \subset G$ . Il sottoinsieme  $H$  si dice **chiuso** rispetto all'operazione del gruppo se si ha:

$$\forall h \in H \quad \forall h' \in H \quad h \cdot h' \in H$$

Se  $H$  è chiuso, allora  $(H, \cdot)$  è un gruppoide. Si dice che il gruppoide  $(H, \cdot)$  è un **sottogruppo** di  $(G, \cdot)$  se  $(H, \cdot)$  è un gruppo.

Quando  $H$  è un sottogruppo di  $G$  si usa di solito il simbolo  $H < G$ .

**Nota 369** La nozione di sottoinsieme chiuso rispetto ad un'operazione si estende ovviamente al caso di sottoinsiemi di un gruppoide  $(G, \cdot)$ . In questo caso si parla di **sottogruppoide**.

**Nota 370** Ogni gruppo  $(G, \cdot)$  è dotato di almeno due sottogruppi: il gruppo  $(G, \cdot)$  stesso e il gruppo  $(\{1\}, \cdot)$  formato dal solo elemento neutro. Questi due sottogruppi si dicono **sottogruppi banali**. Un sottogruppo si dice **proprio** se non coincide con uno dei due sottogruppi banali.

**Esempio 371** Diamo due esempi di sottogruppi:

- 1) Il gruppo delle isometrie del piano è un sottogruppo del gruppo delle trasformazioni del piano.
- 2) Il gruppo di Klein è un sottogruppo del gruppo delle isometrie.

**Teorema 372** Sia  $(G, \cdot)$  un gruppo e sia  $H \subset G$ . Si ha che  $H$  è un sottogruppo di  $G$  se e solo se sono verificate le seguenti tre condizioni:

- 1)  $H \neq \emptyset$
- 2)  $h \in H, h' \in H \implies h \cdot h' \in H$
- 3)  $h \in H \implies h^{-1} \in H$

**DIMOSTRAZIONE.** Ovviamente, se  $H$  è un sottogruppo, sono verificate le condizioni 2) e 3). Inoltre  $H$  deve essere dotato almeno dell'elemento neutro e quindi  $H \neq \emptyset$ .

Dimostriamo che, se sono verificate le condizioni 1), 2) e 3), allora  $H$  è un sottogruppo.

La condizione 2) assicura che  $(H, \cdot)$  è un gruppoide. L'operazione  $\cdot$  verifica la proprietà associativa poiché essa è operazione di  $G$  che a sua volta è un gruppo. Dimostriamo ora che l'elemento neutro 1 di  $G$  appartiene ad  $H$ . Dalla proprietà 1) segue che esiste un elemento  $h$  in  $H$ . Dalla proprietà 3) segue che  $h^{-1}$  appartiene ad  $H$ . Ma allora, poiché sia  $h$  che  $h^{-1}$  appartengono ad  $H$ , dalla proprietà 2) segue che  $h \cdot h^{-1} = 1$  appartiene ad  $H$ . Dalla proprietà 3) segue infine che ogni elemento di  $H$  è dotato di inverso in  $H$ .  $\square$

**Esempio 373** Indichiamo con  $G$  l'insieme delle matrici di ordine  $n$  a coefficienti reali aventi determinante uguale a 1. Si verifica facilmente (esercizio) che  $G$  è un sottogruppo del gruppo  $(GL(R, n), \cdot)$ .

**Esempio 374** Consideriamo il seguente sottoinsieme di  $GL(R, n)$ :

$$O(n) = \{A \in GL(R, n) \mid {}^tA = A^{-1}\}$$

Si dimostra facilmente che  $O(n)$  è un sottogruppo non banale di  $(GL(R, n), \cdot)$ . Le matrici di  $O(n)$  si dicono **ortogonali**. Il gruppo  $(O(n), \cdot)$  si dice **gruppo ortogonale**.

**Esempio 375** Consideriamo il seguente sottoinsieme di  $GL(R, n)$ :

$$SO(n) = \{A \in GL(R, n) \mid {}^tA = A^{-1} \text{ e } \det(A) = 1\}$$

Si dimostra facilmente che  $SO(n)$  è un sottogruppo di  $(GL(R, n), \cdot)$ . Il gruppo  $(SO(n), \cdot)$  si dice **gruppo ortogonale speciale**.

**Nota 376** Notiamo che si ha:

$$SO(n) = G \cap O(n)$$

dove  $G$  è il sottogruppo di  $GL(R, n)$  formato dalle matrici aventi determinante uguale a 1. Sappiamo che sia  $O(n)$  che  $G$  sono sottogruppi di  $(GL(R, n), \cdot)$ . Abbiamo quindi due sottogruppi di un gruppo la cui intersezione è anch'essa un sottogruppo. Ciò non è un caso particolare, come mostra il prossimo teorema.

**Teorema 377** Sia  $(G, \cdot)$  un gruppo. Si ha:

$$(H < G) \wedge (K < G) \implies H \cap K < G$$

In altre parole, l'intersezione di sottogruppi di un gruppo è un sottogruppo del gruppo.

**DIMOSTRAZIONE.** Lasciata per esercizio.  $\square$

**Esercizio 378** Verificare l'esattezza o falsità della seguente affermazione.

Dato un gruppo  $(G, \cdot)$  si ha:

$$(H < G) \wedge (K < G) \implies H \cup K < G$$

**Esercizio 379** Si consideri il gruppo  $(Z, +)$ . Dato  $n \in Z$  indichiamo con  $nZ$  l'insieme dei numeri interi multipli di  $n$ .

Dimostrare che  $nZ$  è un sottogruppo di  $(Z, +)$ .

Determinare il sottogruppo  $3Z \cap 5Z$ .

Determinare l'insieme  $3Z \cup 5Z$  e verificare se esso è un sottogruppo di  $(Z, +)$ .

**Definizione 380** Dato un elemento  $g$  di un gruppo  $(G, \cdot)$  definiamo:

$g^0 = 1$  (ricordiamo che 1 è l'elemento neutro del gruppo);

$g^1 = g$ .

Dato  $n \in N$ , con  $n > 1$ , definiamo:

$g^n = g \cdot g \cdot \dots \cdot g$  ( $n$  volte)

$g^{-n} = g^{-1} \cdot g^{-1} \cdot \dots \cdot g^{-1}$  ( $n$  volte).

Abbiamo quindi dato la definizione delle **potenze**  $g^n$  di  $g$  per ogni  $n \in Z$ .

**Nota 381** Nel caso in cui si utilizzi la notazione additiva si parla invece di **multipli** in un elemento  $g$ .

Dato un elemento  $g$  di un gruppo  $(G, +)$  si utilizza la seguente notazione:

$0 \cdot g = 0$  (ricordiamo che 0 è l'elemento neutro del gruppo).

Dato  $n \in N$ , poniamo:

$n \cdot g = g + g + \dots + g$  ( $n$  volte)

$(-n) \cdot g = (-g) + (-g) + \dots + (-g)$  ( $n$  volte).

Da ciò segue, in particolare:

$1 \cdot g = g$ .

**Esempio 382** Consideriamo l'elemento

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

del gruppo  $(\sigma_3, \circ)$  (vedere l'esempio 351). Abbiamo (esercizio):

$$\begin{aligned}d^0 &= id \\d^1 &= d \\d^2 &= e \\d^3 &= id \\d^{-1} &= d^2 = e \\d^{-2} &= d\end{aligned}$$

**Nota 383** La definizione di potenza positiva di un elemento si estende al caso di elementi di un gruppoide associativo.

Nel caso di un monoide possiamo definire anche la potenza nulla di un elemento. Inoltre, sempre nel caso di un monoide, possiamo definire anche le potenze negative di elementi dotati di inverso.

**Teorema 384** Dato un elemento  $g$  di un gruppo  $(G, \cdot)$  si ha:

$$\begin{aligned}g^{n+m} &= g^n \cdot g^m \quad \forall n \in Z, \forall m \in Z \\g^{n \cdot m} &= (g^n)^m \quad \forall n \in Z, \forall m \in Z \\g^{-n} &= (g^n)^{-1} \quad \forall n \in Z\end{aligned}$$

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

**Esercizio 385** In un gruppo  $(G, \cdot)$  è valida la seguente proprietà sulle potenze?

$$\forall n \in Z \quad (a \cdot b)^n = a^n \cdot b^n$$

**Esercizio 386** Siano  $a$  e  $b$  elementi di un gruppo  $(G, \cdot)$  tali che  $a \cdot b = b \cdot a$ . Si ha allora la seguente proprietà?

$$\forall n \in Z \quad (a \cdot b)^n = a^n \cdot b^n$$

**Esercizio 387** Siano  $a$  e  $b$  elementi di un gruppo  $(G, \cdot)$  tali che  $a \cdot b = b \cdot a$ . Si ha allora la seguente proprietà?

$$b^{-1} \cdot a = a \cdot b^{-1}$$

**Esercizio 388** Enunciare il teorema precedente nel caso in cui si utilizzi la notazione additiva.

**Teorema 389** Dato un elemento  $g$  di un gruppo  $(G, \cdot)$ , indichiamo con il simbolo  $\langle g \rangle$  l'insieme delle potenze positive, negative, nulle dell'elemento  $g$ . Sia ha che:

- 1)  $\langle g \rangle$  è un sottogruppo di  $(G, \cdot)$ . Esso viene detto **sottogruppo generato** da  $g$ .
- 2) Se  $H$  è un sottogruppo di  $G$  e  $g \in H$ , allora  $\langle g \rangle \subset H$ .

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

**Esempio 390** Si consideri il gruppo  $(Z, +)$ . Si ha:

a)  $\langle 0 \rangle = 0$

b)  $\langle 1 \rangle = Z$

c) Dato  $n \in Z$ , allora  $\langle n \rangle = nZ$ .

Si lascia la dimostrazione di tutto ciò per esercizio.

**Esercizio 391** Determinare i sottogruppi del gruppo di Klein generati dai singoli suoi elementi.

**Esercizio 392** Determinare i sottogruppi di  $(S_3, \circ)$  generati dai singoli suoi elementi.

**Definizione 393** Sia  $F$  un qualsiasi sottoinsieme del piano. Consideriamo l'insieme delle isometrie del piano che trasformano  $F$  in  $F$  stesso. Si dimostra facilmente (esercizio) che esso è un sottogruppo del gruppo delle isometrie. Esso è pertanto un gruppo con l'operazione di composizione. Chiamiamo questo gruppo *gruppo delle trasformazioni isometriche di  $F$* .

**Esercizio 394** Si consideri un triangolo equilatero  $T$ . Determinare il gruppo delle trasformazioni isometriche di  $T$ .

Suggerimento: notare che le isometrie cercate trasformano vertici in vertici.

**Esercizio 395** Determinare il gruppo delle trasformazioni isometriche di un quadrato.

**Esercizio 396** Determinare il gruppo delle trasformazioni isometriche di un pentagono regolare.

**Esercizio 397** Determinare il gruppo delle trasformazioni isometriche di un esagono regolare.

**Definizione 398** Chiamiamo *gruppo diedrale di grado  $n$*  il gruppo delle trasformazioni isometriche di un poligono regolare di  $n$  lati.

**Esercizio 399** Determinare, per ogni  $n \geq 3$  il gruppo diedrale di grado  $n$ .

Suggerimento: Analizzare gli esempi precedenti del triangolo, del quadrato, del pentagono e dell'esagono. Distinguere tra  $n$  pari e  $n$  dispari.

**Esercizio 400** Determinare il gruppo delle trasformazioni isometriche di un triangolo isoscele non equilatero.

**Esercizio 401** Determinare il gruppo delle trasformazioni isometriche di un triangolo scaleno.

**Esercizio 402** Determinare il gruppo delle trasformazioni isometriche di un rettangolo che non sia un quadrato.

**Esercizio 403** Determinare il gruppo delle trasformazioni isometriche di una circonferenza.

### 3.4 Periodo di un elemento

**Definizione 404** Dato un elemento  $g$  di un gruppo  $(G, \cdot)$ , si definisce **periodo** di  $g$  il più piccolo numero intero positivo  $n$ , tale che  $g^n$  sia uguale all'elemento neutro. Se non esiste alcun numero intero positivo tale che  $g^n$  sia uguale all'elemento neutro, si dice che  $g$  ha **periodo infinito**.

**Esempio 405** Dall'esempio 382 segue che il periodo dell'elemento  $d$  del gruppo  $(\sigma_3, \circ)$  è uguale a 3.

**Esercizio 406** Calcolare il periodo di ogni elemento del gruppo  $(\sigma_3, \circ)$  (vedere esempio 351 per la definizione di  $\sigma_3$ ).

**Esercizio 407** Calcolare il periodo di ogni elemento del gruppo di Klein (vedere esempio 357 per la definizione).

**Esercizio 408** Calcolare il periodo di ogni elemento del gruppo dato nell'esempio 360.

**Nota 409** Sia dato un gruppo  $(G, \cdot)$  e un suo elemento  $g$ .

Dalla definizione di periodo di un elemento, segue che  $g$  ha periodo uguale a 1 se e solo se  $g = 1$ .

Si verifica poi facilmente (esercizio) che  $g \neq 1$  ha periodo 2 se e solo se  $g = g^{-1}$ .

**Teorema 410** Sia  $g$  un elemento di un gruppo  $(G, \cdot)$ . Si ha che il periodo di  $g$  è uguale al periodo di  $g^{-1}$ .

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

Ricordiamo ora alcune proprietà aritmetiche.

Sia fissato un numero  $n \in N$ . Quindi  $n$  è un numero intero positivo. Sappiamo che, dato comunque un numero  $a \in N$ , possiamo dividere  $a$  per  $n$  e ottenere un numero intero  $q$  (quoziente) con resto un numero intero positivo o nullo  $r$  minore di  $n$ . Sappiamo ciò fin dalle scuole elementari. Dato quindi  $a \in Z$  con  $\geq 0$ , sappiamo determinare due numeri interi  $q$  e  $r$  tali che si abbia:

$$a = qn + r$$

Notiamo che si ha  $0 \leq r < n$ .

Vogliamo generalizzare tutto ciò al caso di un numero  $a \in Z$  negativo.

Abbiamo il seguente teorema.

**Teorema 411** Sia fissato  $n \in N$ . Dato  $a \in Z$ , esistono e sono unici i numeri  $q \in Z$  e  $r \in Z$  tali che:

$$a = qn + r \quad \text{con} \quad 0 \leq r < n$$

DIMOSTRAZIONE. Nel caso in cui  $a \geq 0$  sappiamo come fare.

Studiamo ora il caso in cui si abbia  $a < 0$ . Consideriamo  $-a$ . Si ha  $-a > 0$ . Appliciamo a  $-a$  l'algoritmo appena detto. Otteniamo  $-a = q'n + r'$  con

$q' \in Z$  e  $r' \in Z$  tale che  $0 \leq r' < n$ . Abbiamo allora  $a = -q'n + (-r')$  con  $-n < -r' \leq 0$ . Distinguiamo due casi. Se  $r' = 0$  abbiamo  $a = qn + r$  con  $q = -q'$  e  $r = 0$ . Se  $r' > 0$  abbiamo  $a = -q'n - n + (n - r') = (-q' - 1)n + (n - r')$  con  $0 < n - r' < n$ . Abbiamo perciò  $a = qn + r$  con  $q = -q' - 1$  e  $r = n - r'$ .

Bene, per ogni  $a \in Z$  abbiamo ora un algoritmo per determinare i numeri  $q$  e  $r$  verificanti le condizioni richieste.

Dobbiamo ora dimostrare che  $r$  e  $q$  sono unici. Si abbia:

$a = qn + r$  con  $q \in Z$  e  $0 \leq r < n$  e si abbia anche:

$a = q'n + r'$  con  $q' \in Z$  e  $0 \leq r' < n$ .

Sia  $r' \geq r$ . Allora  $0 \leq r' - r = (q - q')n \leq r' < n$ . Da cui  $0 \leq (q - q')n < n$ . Da ciò segue  $0 \leq q - q' < 1$ . Ma allora, essendo  $q - q'$  un intero positivo o nullo, si ha  $q - q' = 0$ ; da cui  $q = q'$  e  $r = r'$ . Cioè la tesi.  $\square$

**Esempio 412** Per rendere più chiaro l'algoritmo facciamo un esempio. Prendiamo  $a = -1223$  e  $b = 14$ .

Consideriamo il numero 1223 e dividiamolo per 14. Utilizzando una qualsiasi calcolatrice tascabile otteniamo  $1223/14 = 87,35\dots$  Abbiamo perciò  $q' = 87$ . Si ha poi  $r' = 1223 - 87 \cdot 14 = 1223 - 1218 = 5$ .

Abbiamo pertanto:

$$1223 = 87 \cdot 14 + 5$$

Ne segue:

$$-1223 = -87 \cdot 14 - 5 = -87 \cdot 14 - 14 + 14 - 5 = -88 \cdot 14 + 9$$

I nostri  $q$  e  $r$  cercati sono quindi rispettivamente -88 e 9.

**Teorema 413** Sia  $(G, \cdot)$  un gruppo e sia  $g$  un suo elemento. Allora:

1) se  $g$  ha periodo infinito:  $g^h = g^k \iff h = k$

2) se  $g$  ha periodo  $n$ :  $g^h = g^k \iff h - k = qn$

**DIMOSTRAZIONE.** Sia  $g^h = g^k$ . Supponiamo  $h \geq k$ . Da  $g^h = g^k$  segue  $1 = g^h \cdot (g^k)^{-1} = g^{h-k}$ .

Distinguiamo ora i due casi:

1)  $g$  ha periodo infinito. Quindi da  $g^{h-k} = 1$  segue  $h = k$ .

Il viceversa è ovvio.

2)  $g$  ha periodo  $n$ . Si consideri  $h - k = qn + r$  con  $0 \leq r < n$ . Allora:

$$1 = g^{h-k} = g^{qn+r} = (g^n)^q \cdot g^r = 1^q \cdot g^r = 1 \cdot g^r = g^r.$$

Da ciò segue, poiché  $0 \leq r < n$  e  $n$  è il periodo di  $g$ , che si ha  $r = 0$ . Quindi  $h - k = qn$ .

Il viceversa è ovvio.  $\square$

**Teorema 414** Sia  $g$  un elemento di un gruppo  $(G, \cdot)$ . Si ha:

1) se il periodo di  $g$  è infinito allora il sottogruppo  $\langle g \rangle$  ha cardinalità  $\aleph_0$

2) se il periodo di  $g$  è  $n$ , con  $n$  finito, allora la cardinalità del sottogruppo  $\langle g \rangle$  è uguale a  $n$ .

**DIMOSTRAZIONE.** Ricordiamo che  $\langle g \rangle$  è dato da tutte le potenze di  $g$ .

Distinguiamo i due casi.

1) Se il periodo di  $g$  è infinito, dal caso 1) del teorema precedente segue che  $\langle g \rangle$  è in corrispondenza biunivoca con  $\mathbb{N}_0$ . Abbiamo quindi la tesi.

2) Sia  $n$ , con  $n$  finito, il periodo di  $g$ . Sia  $g' \in \langle g \rangle$ . Quindi  $g' = g^p$  con  $p \in \mathbb{Z}$ . Applicando il teorema 411 abbiamo:

$p = qn + r$  con  $0 \leq r < n$ . Quindi, applicando il teorema 413, abbiamo  $g^p = g^r$ . Da tutto ciò segue che si ha:

$$\langle g \rangle = \{g^1 = g, g^2, g^3, \dots, g^{n-1}, g^n = 1\}$$

Inoltre, applicando sempre il teorema 413, si ha (esercizio) che questi  $n$  elementi di  $\langle g \rangle$  sono tutti distinti. Da cui la tesi.  $\square$

**Nota 415** Sia  $g$  un elemento di un gruppo  $(G, \cdot)$ . Sia  $n$  il periodo (finito) di  $g$ . Supponiamo di dover calcolare  $g^p$  per  $|p|$  molto più grande di  $n$ .

La dimostrazione del teorema precedente ci suggerisce un metodo per calcolare  $g^p$ . Si divide  $p$  per  $n$  e se ne considera il resto  $r$ . Dal teorema precedente segue  $g^r = g^p$ . Con questo metodo dobbiamo fare meno calcoli. Il numero  $r$  ha infatti verifica la relazione  $0 \leq r < n$ . Il che in questo caso ci è molto utile.

**Esercizio 416** Consideriamo la matrice

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

Calcolare  $A^{100}$  e  $A^{1000}$ .

### 3.5 Gruppi ciclici

**Definizione 417** Un gruppo  $(G, \cdot)$  si dice **ciclico** se esiste un suo elemento  $g$  tale che  $\langle g \rangle = G$ . L'elemento  $g$  si dice **generatore** del gruppo  $G$ .

In altre parole, un gruppo  $G$  si dice ciclico con generatore  $g$ , se ogni elemento di  $G$  è potenza di  $g$ .

**Esempio 418** Il gruppo  $(\mathbb{Z}, +)$  è ciclico con generatore 1. (Vedere l'esempio b) di 390).

**Esercizio 419** Verificare che anche l'elemento  $-1$  è generatore del gruppo  $(\mathbb{Z}, +)$ .

**Teorema 420** Se  $g$  è generatore di un gruppo  $(G, \cdot)$ , allora anche  $g^{-1}$  è generatore del gruppo.

DIMOSTRAZIONE. Esercizio.  $\square$

**Teorema 421** Se un gruppo  $(G, \cdot)$  ha un generatore di periodo  $n$ , allora ogni altro generatore di  $G$  ha periodo  $n$ .

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$



**Teorema 422** Se un gruppo  $(G, \cdot)$  ha un generatore di periodo infinito, allora ogni altro generatore di  $G$  ha periodo infinito.

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

**Teorema 423** Ogni gruppo ciclico è abeliano.

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

**Esercizio 424** Ogni gruppo abeliano è ciclico?

**Esercizio 425** Il gruppo di Klein è ciclico? Determinare tutti i sottogruppi ciclici del gruppo di Klein.

**Esercizio 426** Si consideri il gruppo simmetrico  $(\sigma_3, \circ)$ . Determinare tutti i suoi sottogruppi ciclici.

**Teorema 427** Tutti i sottogruppi di un gruppo ciclico sono ciclici.

DIMOSTRAZIONE. Sia  $(G, \cdot)$  un gruppo ciclico e sia  $g$  un suo generatore. Sia  $H$  un suo sottogruppo. Se  $H$  è un sottogruppo banale, chiaramente  $H$  è ciclico. Supponiamo quindi che  $H$  sia un sottogruppo proprio. Esistono quindi in  $H$  elementi distinti dall'elemento neutro 1. poiché il gruppo  $G$  è generato da  $g$ , tutti gli elementi di  $H$  sono potenze di  $g$ . Tra queste potenze ne esiste almeno una positiva. Sia infatti  $h \neq 1$ . Sia  $h = g^s$ . Se  $s > 0$  siamo a posto. Se  $s < 0$  consideriamo l'elemento  $h^{-1} = g^{-s}$ , esso è potenza positiva di  $g$  ed appartiene ad  $H$ , poiché  $H$  è un sottogruppo.

Sia  $n$  il più piccolo intero positivo tale che  $g^n \in H$ . Vogliamo dimostrare che  $g^n$  è generatore di  $H$ . Sia  $a \in H$ . Poiché  $g$  è generatore di  $G$  si ha  $a = g^p$  con  $p \in \mathbb{Z}$ . Applicando il teorema 411 abbiamo:

$p = qn + r$  con  $q \in \mathbb{Z}, r \in \mathbb{Z}$  e  $0 \leq r < n$ . Quindi:

$$g^p = g^{qn} \cdot g^r = (g^n)^q g^r \implies g^r = [(g^n)^q]^{-1} g^p$$

Poiché  $H$  è un sottogruppo di  $G$ , da  $g^n \in H$  segue  $(g^n)^q \in H$  e quindi  $[(g^n)^q]^{-1} \in H$ . Da cui, poiché si ha anche  $g^p \in H$ , segue  $g^r \in H$ . Dalla definizione di  $n$  segue  $r = 0$ . Da cui la tesi.  $\square$

## 3.6 Teorema di Lagrange e applicazioni

**Definizione 428** Sia  $(G, \cdot)$  un gruppo e sia  $H$  un suo sottogruppo. Fissato  $a \in G$  consideriamo il seguente sottoinsieme di  $G$ :

$$\{h \cdot a \mid h \in H\}$$

Indichiamo tale classe con  $H \cdot a$  e la chiamiamo **classe laterale destra** relativa a  $H$ , determinata da  $a$ .

In altre parole, per determinare la classe laterale destra  $H \cdot a$ , prendiamo tutti gli elementi di  $H$  e li moltiplichiamo a destra per  $a$ .

**Esempio 429** Consideriamo il gruppo di Klein  $(K, \circ)$ . (Vedere esempio 357). Consideriamo  $s_r \in K$ . Sia  $H$  il sottogruppo generato da  $s_r$ . Abbiamo:

$$H = (s_r) = \{s_r, s_r^2 = id\} = H$$

Consideriamo tutte le classi laterali destre di  $H$ . Abbiamo

$$H \circ id = \{s_r \circ id = s_r, id \circ id = id\}$$

Consideriamo ora  $H \circ s_r$ . Abbiamo:

$$H \circ s_r = \{s_r \circ s_r = id, id \circ s_r = s_r\}$$

Pertanto  $H \circ id = H \circ s_r$ .

Svolgendo in modo analogo i calcoli troviamo:

$$H \circ s_s = H \circ s_P = \{s_r \circ s_s = s_P, id \circ s_s = s_s\}$$

Notiamo che ogni elemento di  $K$  appartiene ad una ed una sola classe laterale destra relativa ad  $H$ .

Notiamo che vi sono due classi laterali destre e che ogni classe laterale destra ha due elementi; tanti quanti gli elementi di  $H$ .

**Esempio 430** Si consideri il gruppo simmetrico  $\sigma_3$  (vedere l'esempio 351). Sia  $H$  il sottogruppo generato da:

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

Si possono determinare tutte le classi laterali destre relative ad  $H$  (esercizio). Si nota che anche in questo caso ogni elemento di  $S_3$  appartiene ad una ed una sola classe laterale destra.

Si nota inoltre che vi sono tre classi laterali destre e che ogni classe laterale destra ha due elementi; tanti quanti gli elementi di  $H$ .

In ognuno dei due casi precedenti abbiamo che ogni elemento del gruppo considerato appartiene ad una ed una sola classe laterale destra relativa ad  $H$  e che le classi laterali destre relative ad  $H$  hanno tutte un numero di elementi pari al numero di elementi di  $H$ . Tutto ciò è generalizzato dal seguente teorema.

**Teorema 431** Sia  $(G, \cdot)$  un gruppo e sia  $H$  un suo sottogruppo. Si ha che:

1) ogni elemento di  $G$  appartiene ad una ed una sola classe laterale destra relativa ad  $H$ .

2) Ogni classe laterale destra relativa ad  $H$  ha la stessa cardinalità di  $H$ .

**DIMOSTRAZIONE.** Lasciate per esercizio. Per dimostrare la 2) si consiglia di considerare l'applicazione  $f : H \longrightarrow H \cdot a$  definita da  $f(h) = h \cdot a$  e di dimostrare che essa è una corrispondenza biunivoca.  $\square$

**Teorema 432** [Teorema di LAGRANGE<sup>3</sup>] In un gruppo finito  $G$  l'ordine di un suo sottogruppo  $H$  è un sottomultiplo dell'ordine del gruppo.

DIMOSTRAZIONE. Sia  $|G| = n$  e  $|H| = p$ .

Gli elementi di  $G$  sono suddivisi in classi laterali destre relative ad  $H$ . Supponiamo che vi siano  $q$  classi laterali destre distinte. Abbiamo pertanto suddiviso gli  $n$  elementi di  $G$  in  $q$  sottoinsiemi disgiunti. Ognuno di tali sottoinsiemi ha, per il teorema 431,  $p$  elementi. Da tutto ciò segue  $n = p \cdot q$ .  $\square$

Il teorema di Lagrange ci dice che l'ordine di un sottogruppo di un gruppo finito è un sottomultiplo dell'ordine del gruppo. Ci chiediamo se, dato un gruppo  $(G, \cdot)$  di ordine  $n$ , per ogni sottomultiplo  $h$  di  $n$  esista un sottogruppo di  $G$  di ordine  $h$ . La risposta è, in generale, negativa. Se però il gruppo  $(G, \cdot)$  è ciclico, la risposta è positiva. Si ha infatti il seguente teorema.

**Teorema 433** Sia  $(G, \cdot)$  un gruppo ciclico di ordine  $n$  e sia  $h$  un sottomultiplo di  $n$ . Si ha che esiste uno ed un solo sottogruppo di  $G$  avente ordine  $h$ .

DIMOSTRAZIONE. Dimostriamo l'esistenza di un sottogruppo di  $G$  avente ordine  $h$ . Sia  $n = h \cdot q$ . Sia  $g$  un generatore di  $G$ . Quindi  $g$  ha periodo  $n$ . Consideriamo l'elemento  $g^q$ . Dimostriamo che  $g^q$  ha periodo  $h$ . Abbiamo innanzitutto

$$(g^q)^h = g^{q \cdot h} = g^n = 1$$

Supponiamo ora per assurdo che esista  $0 < h' < h$  tale che  $(g^q)^{h'} = 1$ . Ma allora si ha  $g^{q \cdot h'} = 1$  con  $q \cdot h' < q \cdot h = n$ . Ma ciò è assurdo poiché  $g$  ha periodo  $n$ .

poiché  $g^q$  ha periodo  $h$ , abbiamo che il sottogruppo generato da  $g^q$  ha ordine  $h$ . Abbiamo dimostrato l'esistenza di un sottogruppo di ordine  $h$ .

Omettiamo la dimostrazione che non esistono altri sottogruppi di ordine  $h$ .  $\square$

**Teorema 434** Sia  $(G, \cdot)$  un gruppo finito di ordine  $n$  e sia  $g \in G$ . Si ha allora:

1) Il periodo di  $g$  è un divisore di  $n$ ;

2)  $g^n = 1$

3)  $g^{-1} = g^{n-1}$

DIMOSTRAZIONE. Sappiamo che il sottogruppo  $\langle g \rangle$  ha ordine uguale al periodo di  $g$  (teorema 414). La tesi segue quindi dal teorema di Lagrange.

2) Sia  $p$  il periodo di  $g$ . Dalla parte 1) segue  $n = p \cdot q$ . Ma allora si ha:

$$g^n = g^{p \cdot q} = (g^p)^q = 1^q = 1$$

3) Applicando la parte 2) si ottiene:

$$1 = g^n = g \cdot g^{n-1}$$

Da ciò segue la tesi.  $\square$

---

<sup>3</sup>**Giuseppe Luigi Lagrange**(1736-1813), matematico italiano di origine francese. Ha insegnato a Torino, Berlino e Parigi.

### 3.7 Gruppoidi quozienti

Dato un insieme  $G$  e una relazione  $\sim$  di equivalenza in esso, abbiamo considerato (vedere 111) l'insieme quoziente  $G/\sim$  dato dalle sue classi di equivalenza.

Se in  $G$  è data anche una operazione  $\cdot : G \times G \longrightarrow G$ , vogliamo definire una operazione in  $G/\sim$ .

Prima di far ciò abbiamo bisogno della seguente definizione.

**Definizione 435** Sia  $(G, \cdot)$  un gruppoide. Sia  $\sim$  una relazione di equivalenza di  $G$ . La relazione di equivalenza  $\sim$  e l'operazione  $\cdot$  di  $G$  si dicono **compatibili** se si ha:

$$a \sim a' \wedge b \sim b' \implies a \cdot b \sim a' \cdot b'.$$

**Esempio 436** La relazione di equivalenza in  $M(R, n, n)$  data da:

$$A \sim A' \iff \det(A) = \det(A')$$

non è compatibile con l'operazione di addizione tra matrici se  $n > 1$ . Diamo un controesempio per  $n = 2$ . Siano date le matrici:

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, A' = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, B' = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

Si ha  $A \sim A'$ ,  $B \sim B'$ . Ma  $A + B \not\sim A' + B'$ .

Dare un controesempio per  $n > 2$ .

**Esempio 437** La relazione di equivalenza in  $M(R, n, n)$  data nel precedente esempio è compatibile con l'operazione di moltiplicazione tra matrici.

Infatti, da  $A \sim A'$ ,  $B \sim B'$ , segue  $\det(A) = \det(A')$  e  $\det(B) = \det(B')$ . Da cui, per il teorema di Binet<sup>4</sup>  $\det(A \cdot B) = \det(A' \cdot B')$ . Cioè  $A \cdot B \sim A' \cdot B'$ .

**Definizione 438** Dato un gruppoide  $(G, \cdot)$  e una relazione di equivalenza  $\sim$  compatibile con l'operazione  $\cdot$  di  $G$ , chiamiamo **operazione su  $G/\sim$  indotta** dall'operazione su  $G$  la seguente operazione:

$$[a] \cdot [b] = [a \cdot b]$$

**Nota 439** Nella formula precedente abbiamo indicato con  $[a]$  la classe di equivalenza cui appartiene  $a$ . Ricordiamo che abbiamo:

$$a \sim a' \iff [a] = [a']$$

Osserviamo bene come abbiamo definito l'operazione tra gli elementi  $[a]$  e  $[b]$  di  $G/\sim$ .

*Scegliamo* un elemento  $a \in [a]$ ; *scegliamo* un elemento  $b \in [b]$ ; consideriamo il prodotto  $a \cdot b$  in  $G$ ; consideriamo la classe di equivalenza cui appartiene questo elemento; consideriamo cioè la classe  $[a \cdot b]$ . Quest'ultima classe è, per definizione,

<sup>4</sup>Jacques-Philippe-Marie Binet, (1786-1856), matematico e astronomo francese.

il prodotto della classe  $[a]$  per la classe  $[b]$ .

Notiamo che, nel dare tale definizione, abbiamo dovuto *scegliere* gli elementi  $a$  e  $b$  delle due classi. Ci chiediamo allora: cosa sarebbe successo se avessimo scelto altri due elementi nelle due classi? Avremmo ottenuto lo stesso risultato? Ci chiediamo cioè se la definizione di moltiplicazione in  $G/\sim$  dipenda o no dalla scelta dei rappresentanti delle due classi. Se essa non dipende dalla scelta diremo che abbiamo una **definizione ben posta** di moltiplicazione in  $G/\sim$ .

Dimostriamo che la definizione è ben posta.

Sia  $a' \sim a$  e sia  $b' \sim b$ . Dobbiamo dimostrare che si ha  $[a \cdot b] = [a' \cdot b']$ ; cioè che si ha  $a \cdot b \sim a' \cdot b'$ . Ma ciò è vero per la definizione di compatibilità dell'operazione con la relazione di equivalenza.

**Teorema 440** Sia  $(G, \cdot)$  un gruppoide e sia  $\sim$  una relazione di equivalenza compatibile con l'operazione  $\cdot$  di  $G$ . Abbiamo quindi un gruppoide  $(G/\sim, \cdot)$  dove  $\cdot$  è l'operazione su  $G/\sim$  indotta dall'operazione  $\cdot$  su  $G$ . Si ha:

1) Se l'operazione  $\cdot$  in  $G$  è associativa, allora anche l'operazione  $\cdot$  in  $G/\sim$  è associativa.

Ricordiamo che un gruppoide con l'operazione associativa si dice semigrupp. Possiamo quindi affermare:

$(G, \cdot)$  semigrupp  $\implies (G/\sim, \cdot)$  semigrupp.

2) Se  $(G, \cdot)$  è dotato di elemento neutro 1, allora  $[1]$  è elemento neutro di  $(G/\sim, \cdot)$ .

3) Ricordiamo che un monoide è un gruppoide associativo con elemento neutro. Si ha quindi:

$(G, \cdot)$  monoide  $\implies (G/\sim, \cdot)$  monoide.

4) Sia  $(G, \cdot)$  un gruppoide dotato di elemento neutro. Sia  $g \in G$  dotato di inverso  $g^{-1}$ , allora  $[g^{-1}]$  è l'inverso di  $[g]$  in  $(G/\sim, \cdot)$ . Cioè:

$$[g^{-1}] = [g]^{-1}$$

Quindi si ha:

5)  $(G, \cdot)$  gruppo  $\implies (G/\sim, \cdot)$  gruppo.

6) Se l'operazione in  $G$  è commutativa, allora l'operazione indotta in  $G/\sim$  è commutativa.

Quindi, in particolare, si ha:

7)  $(G, \cdot)$  gruppo abeliano  $\implies (G/\sim, \cdot)$  gruppo abeliano.

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

## 3.8 Gruppi quozienti

Abbiamo appena visto (vedere parte 7) del teorema 440) che, se abbiamo un gruppo  $(G, \cdot)$  e una relazione di equivalenza  $\sim$  compatibile con l'operazione del gruppo, abbiamo che  $G/\sim$  con l'operazione indotta dall'operazione su  $G$  è un gruppo.

Consideriamo un esempio importante di ciò.

**Teorema 441** Sia  $(G, \cdot)$  un gruppo e sia  $H$  un suo sottogruppo. Poniamo la seguente relazione in  $G$ :

$$a \sim b \iff a \cdot b^{-1} \in H$$

Si ha che:

- 1) la relazione  $\sim$  definita sopra è una relazione di equivalenza.
- 2) Possiamo quindi considerare l'insieme quoziente  $G/\sim$ . La classe di equivalenza  $[a]_{\sim}$  determinata da  $a \in G$  è data da:

$$[a]_{\sim} = H \cdot a$$

Da tutto ciò segue che l'insieme quoziente  $G/\sim$  è dato dall'insieme delle classi laterali destre relative ad  $H$ .

DIMOSTRAZIONE. Lasciata per esercizio.

Ci chiediamo se la relazione di equivalenza appena definita e l'operazione  $\cdot$  di  $G$  siano compatibili.

**Esempio 442** Consideriamo il gruppo  $(\sigma_3, \circ)$  e il suo sottogruppo  $K$  generato da

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

Si può verificare (esercizio) che la relazione di equivalenza definita in 441 e l'operazione  $\circ$  di  $\sigma_3$  non sono compatibili.

Dall'esempio precedente segue che affinché la relazione di equivalenza e l'operazione del gruppo siano compatibili è necessario porre alcune restrizioni. Prima di far ciò poniamo in  $G$  una seconda relazione di equivalenza.

**Teorema 443** Sia  $(G, \cdot)$  un gruppo e sia  $H$  un suo sottogruppo. Poniamo la seguente relazione in  $G$ :

$$a \approx b \iff a^{-1} \cdot b \in H$$

Si ha che:

- 1) la relazione  $\approx$  definita sopra è una relazione di equivalenza.
- 2) Possiamo quindi considerare l'insieme quoziente  $G/\approx$ . La classe di equivalenza  $[a]_{\approx}$  determinata da  $a \in G$  è data da:

$$[a]_{\approx} = \{a \cdot h \mid h \in H\}$$

Indichiamo quindi tale classe con  $a \cdot H$  e la chiamiamo **classe laterale sinistra** relativa a  $H$ , determinata da  $a$ .

- 3) per ogni  $a \in G$  si ha  $|H| = |a \cdot H|$ .

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

**Esempio 444** Consideriamo le classi laterali sinistre del gruppo di Klein  $K$  relative al sottogruppo  $H$  dato nell'esempio 429. Sappiamo (vedere l'esempio 357) che il gruppo di Klein è commutativo, quindi si ha ovviamente  $H \cdot a = a \cdot H$  per ogni  $a \in K$ . Abbiamo già determinato nell'esempio 429 le classi laterali destre.

Il fatto che nell'esempio precedente le classi laterali sinistre coincidano con le classi laterali destre dipende dal fatto che il gruppo è abeliano. Si ha infatti, in generale, il seguente teorema.

**Teorema 445** Se  $(G, \cdot)$  è un gruppo abeliano, allora, per ogni sottogruppo  $H$ , le classi laterali sinistre coincidono con le classi laterali destre.

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

I seguenti esercizi ci mostrano che, se nel teorema precedente si toglie l'ipotesi che il gruppo sia abeliano, allora le classi laterali sinistre possono coincidere o non coincidere con le classi laterali destre.

**Esempio 446** Si consideri il gruppo simmetrico  $\sigma_3$ . Sia  $H$  il sottogruppo generato da:

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

Nell'esempio 430 si sono determinate le classi laterali destre relative a  $H$ . Determinare le classi laterali sinistre relative ad  $H$ . Notare che esse non coincidono con le classi laterali sinistre relative ad  $H$ .

In alcuni casi, anche se il gruppo non è abeliano, le classi laterali sinistre coincidono con le destre:

**Esempio 447** Si consideri il gruppo simmetrico  $\sigma_3$  su 3 elementi. Sia  $K$  il sottogruppo generato da

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

Si ha (esercizio) che le classi laterali sinistre relative a  $K$  coincidono con le classi laterali destre.

**Definizione 448** Sia  $(G, \cdot)$  un gruppo e  $H$  un suo sottogruppo. Il sottogruppo  $H$  si dice **normale** se per ogni  $a \in G$  si ha:

$$a \cdot H = H \cdot a$$

Quindi le classi laterali sinistre coincidono con le classi laterali destre; le chiamiamo quindi semplicemente **classi laterali**.

Se  $H$  è un sottogruppo normale di  $G$  indichiamo ciò con il simbolo  $H \triangleleft G$ .

**Esempio 449** Consideriamo il gruppo simmetrico  $(\sigma_3, \circ)$ . I due esempi precedenti ci mostrano che il sottogruppo  $K$  è normale, mentre il sottogruppo  $H$  non è normale.

**Nota 450** La condizione  $a \cdot H = H \cdot a$  non significa  $a \cdot h = h \cdot a \quad \forall h \in H$  ma:  $\forall h \in H$ , esiste  $h' \in H$  tale che  $a \cdot h = h' \cdot a$  e viceversa:  $\forall h' \in H$  esiste  $h \in H$  tale che  $a \cdot h = h' \cdot a$ .

**Nota 451** Ovviamente, se  $(G, \cdot)$  è abeliano, ogni suo sottogruppo è normale.

**Teorema 452** Sia  $(G, \cdot)$  un gruppo e  $H$  un suo sottogruppo. Dimostrare che si ha:

$$H \text{ normale} \iff g \cdot h \cdot g^{-1} \in H \quad \forall g \in G, \forall h \in H$$

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

**Teorema 453** Sia  $(G, \cdot)$  un gruppo e sia  $H$  un suo sottogruppo normale. La relazione d'equivalenza in  $G$  definita da:

$$a \sim a' \iff a \cdot a'^{-1} \in H$$

è compatibile con l'operazione di  $G$ .

DIMOSTRAZIONE. Sia  $a \sim a'$  e  $b \sim b'$ . Quindi si ha:

$$a = h \cdot a' \text{ e } b = h' \cdot b' \text{ con } h \in H \text{ e } h' \in H.$$

Ne segue:

$$a \cdot b = h \cdot a' \cdot h' \cdot b'.$$

Poiché  $H$  è un sottogruppo normale, esiste  $h'' \in H$  tale che  $a' \cdot h' = h'' \cdot a'$ .

Sostituendo ciò nell'ultimo membro della formula precedente otteniamo:

$$a \cdot b = h \cdot a' \cdot h' \cdot b' = h \cdot h'' \cdot a' \cdot b'.$$

Ma  $h \in H$  e  $h'' \in H$ . Poiché  $H$  è un sottogruppo, si ha  $h \cdot h'' = h''' \in H$ .

Da tutto ciò segue  $a \cdot b = h''' \cdot a' \cdot b'$ .

Quindi  $a \cdot b \sim a' \cdot b'$ .  $\square$

**Definizione 454** Sia  $(G, \cdot)$  un gruppo e sia  $H$  un suo sottogruppo normale. Il teorema precedente ci assicura che la relazione

$$a \sim a' \iff a \cdot a'^{-1} \in H$$

è compatibile con l'operazione di  $G$ . Quindi, per la parte 5) del teorema 440 sappiamo che  $(G/\sim, \cdot)$  è un gruppo. Indichiamo  $G/\sim$  con il simbolo  $G/H$ . Il gruppo  $(G/H, \cdot)$  viene chiamato **gruppo quoziente** relativo ad  $H$ .

Gli elementi di  $G/H$  sono quindi le classi laterali sinistre (o destre). Notiamo che l'operazione indotta è data da (esercizio):

$$(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$$

Notiamo, in particolare, che l'elemento neutro del gruppo  $(G/H, \cdot)$  è la classe laterale  $1 \cdot H = H$ .

L'inversa della classe laterale  $a \cdot H$  è la classe laterale  $a^{-1} \cdot H$ .



**Esercizio 455** Si consideri il gruppo di Klein  $(K, \circ)$  e il suo sottogruppo  $H$  generato da  $s_r$  (per il simbolismo vedere l'esempio 429). Determinare il gruppo  $(K/H, \circ)$  e scrivere la sua tabella di moltiplicazione.

**Esercizio 456** Si consideri il gruppo simmetrico  $(\sigma_3, \circ)$  e il suo sottogruppo  $K$  generato da

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

Abbiamo visto nell'esempio 447 che  $K$  è un sottogruppo normale. Determinare il gruppo  $(\sigma_3/K, \circ)$  e scrivere la sua tabella di moltiplicazione.

**Esercizio 457** Sia  $(G, \cdot)$  un gruppo con  $2n$  elementi e sia  $H$  un suo sottogruppo con  $n$  elementi. Dimostrare che  $H$  è un sottogruppo normale di  $G$ .

### 3.9 Le classi resto

**Definizione 458** Sia  $n \in \mathbb{N}$ . Poniamo in  $\mathbb{Z}$  la seguente relazione:

$$a \sim a' \iff a - a' = q \cdot n \text{ con } q \in \mathbb{Z}.$$

Quindi  $a \sim a'$  se e solo se  $a - a'$  è un multiplo di  $n$ . Usiamo il seguente simbolismo:

se  $a \sim b$  scriviamo  $a \equiv b \pmod{n}$  e diciamo  $a$  **congruo**  $b$  **modulo**  $n$ . La relazione si dice **relazione di congruenza modulo**  $n$ .

**Teorema 459** La relazione di congruenza modulo  $n$  è una relazione di equivalenza.

**DIMOSTRAZIONE.** Daremo nella nota 470 una veloce dimostrazione che sfrutta i teoremi visti in precedenza.

Vogliamo però dare anche una dimostrazione diretta.

Dobbiamo dimostrare che sono valide le proprietà riflessiva, simmetrica e transitiva.

(a) proprietà riflessiva:

$$a \equiv a \pmod{n} \quad \forall a \in \mathbb{Z}.$$

Infatti  $a - a = 0 = 0n$ .

(b) proprietà simmetrica:

$$a \equiv b \pmod{n} \implies b \equiv a \pmod{n}.$$

Infatti:

$$\begin{aligned} a \equiv b \pmod{n} &\implies a - b = qn, \quad q \in \mathbb{Z} \implies \\ &\implies b - a = -qn, \quad -q \in \mathbb{Z} \implies b \equiv a \pmod{n}. \end{aligned}$$

(c) proprietà transitiva:

$$a \equiv b \pmod{n}, \quad b \equiv c \pmod{n} \implies a \equiv c \pmod{n}.$$

Infatti da:

$$a \equiv b \pmod{n}, \quad b \equiv c \pmod{n}$$

segue:

$$a - b = hn, \quad b - c = kn \quad \text{con } h \in \mathbb{Z}, \quad k \in \mathbb{Z}.$$

E quindi:

$$a - c = a - b + b - c = hn + kn = (h + k)n, \quad h + k \in Z \implies a \equiv c \pmod{n}.$$

Cioè la tesi.  $\square$

**Definizione 460** Data in  $Z$  la relazione di equivalenza della congruenza modulo  $n$  indichiamo con  $Z_n$  l'insieme quoziente di  $Z$  relativo a tale relazione di equivalenza. Gli elementi di  $Z_n$  sono classi di equivalenza. Dato  $a \in Z$  indichiamo con  $[a]_n$  la classe di equivalenza determinata da  $a$ ; essa viene chiamata **classe di congruenza modulo  $n$  determinata da  $a$** . Si ha quindi (esercizio):

$$[a]_n = \{a + hn, h \in Z\}$$

**Esempio 461** Si consideri  $n = 2$ . Si ha:

$[0]_2 = \{0 + 2h, h \in Z\}$ . Essa è quindi l'insieme dei numeri pari.

$[1]_2 = \{1 + 2h, h \in Z\}$ . Essa è quindi l'insieme dei numeri dispari.

Si ha perciò  $Z_2 = \{[0]_2, [1]_2\}$ .

**Esempio 462** Si consideri  $n = 3$ . Si ha:

$[0]_3 = \{0 + 3h, h \in Z\}$ . Essa è quindi l'insieme dei numeri multipli di 3.

$[1]_3 = \{1 + 3h, h \in Z\}$ . Essa è quindi l'insieme dei numeri che, divisi per 3, hanno resto 1.

$[2]_3 = \{2 + 3h, h \in Z\}$ . Essa è quindi l'insieme dei numeri che, divisi per 3, hanno resto 2.

Si ha perciò  $Z_3 = \{[0]_3, [1]_3, [2]_3\}$ .

**Esercizio 463** Determinare  $Z_4$ .

**Esercizio 464** Determinare  $Z_5$ .

**Esercizio 465** Determinare  $Z_1$ .

Dato  $n \in N$ , vogliamo ora determinare  $Z_n$ . Gli esempi 461 e 462 e gli esercizi 463 e 464 dovrebbero averci dato l'idea. Si ha il seguente teorema.

**Teorema 466** Sia  $n \in N$ . Allora:

$$Z_n = \{[0]_n, [1]_n, [2]_n, \dots, [n-2]_n, [n-1]_n\}.$$

**DIMOSTRAZIONE.** Per dimostrare ciò dobbiamo far vedere che ogni numero intero  $a$  appartiene ad una delle  $n$  classi scritte sopra e che tali classi sono tutte distinte. Dato un numero intero  $a$ , lo possiamo dividere per  $n$  in  $Z$  (vedere il teorema 411). Abbiamo cioè:

$$a = qn + r, \quad q \in Z, \quad r \in Z, \quad 0 \leq r < n.$$

Da ciò deriva  $[a]_n = [r]_n$ . Abbiamo quindi visto che, se  $a \geq 0$ , esso appartiene ad una delle  $n$  classi scritte sopra.

Dobbiamo ora far vedere che le  $n$  classi di cui sopra sono tutte distinte. Basta far vedere che, dati  $r \neq r'$  tali che  $0 \leq r < n$  e  $0 \leq r' < n$ , allora  $r \not\equiv r' \pmod{n}$ . Supponiamo  $r' > r$  (se  $r' < r$  si invertono tra loro  $r$  e  $r'$ ). Si ha

quindi  $0 < r' - r < n$ . Supponiamo, per assurdo, che si abbia  $r' \equiv r \pmod{n}$ . Quindi  $r' - r = qn$  con  $q \in \mathbb{N}$ . Abbiamo perciò  $0 < r' - r = qn < n$ ; quindi  $0 < qn < n$ . Dividendo per  $n$ , si ottiene  $0 < q < 1$ . Il che è assurdo, essendo  $q$  un numero intero.  $\square$

**Nota 467** Per determinare la classe di congruenza modulo  $n$  cui appartiene un numero  $a$  positivo, dobbiamo quindi dividere  $a$  per  $n$  e considerare il resto  $r$ . Per questo motivo le classi di congruenza modulo  $n$  vengono anche chiamate **classi resto** modulo  $n$ .

**Teorema 468** L'operazione di addizione in  $Z$  è compatibile con la relazione di congruenza modulo  $n$  per ogni  $n > 0$ .

DIMOSTRAZIONE. Daremo nella nota 470 una veloce dimostrazione.

Vogliamo però dare anche una dimostrazione diretta.

Sia  $a \equiv a' \pmod{n}$ ,  $b \equiv b' \pmod{n}$ . Quindi:

$a - a' = qn$ ,  $b - b' = q'n$  con  $q \in \mathbb{Z}$ ,  $q' \in \mathbb{Z}$ . Dobbiamo dimostrare che si ha  $a + b \equiv a' + b' \pmod{n}$ , cioè  $(a + b) - (a' + b') = sn$  con  $s \in \mathbb{Z}$ . Sommando membro a membro si ha  $(a + b) - (a' + b') = a - a' + b - b' = (q + q')n$ . Ponendo  $s = q + q'$ , abbiamo  $(a + b) - (a' + b') = sn$ .  $\square$

**Teorema 469** Sia  $n \in \mathbb{N}$ . L'insieme  $Z_n$  con l'operazione definita da:

$$[a]_n + [b]_n = [a + b]_n$$

è un gruppo commutativo.

L'elemento neutro è  $[0]_n$ .

Dato  $0 \leq a < n$ , l'elemento opposto di  $[a]_n$  è l'elemento  $[n - a]_n$ . Cioè:

$$-[a]_n = [n - a]_n$$

DIMOSTRAZIONE. Sappiamo che  $(Z, +)$  è un gruppo commutativo. Il teorema segue quindi dal teorema precedente e dalla parte 7) del teorema 440.

Poiché  $0$  è l'elemento neutro del gruppo  $(Z, +)$ , si ha che  $[0]_n$  è l'elemento neutro di  $(Z_n, +)$ .

Dato  $0 \leq a < n$ , si ha che  $-a$  è l'opposto di  $a$  in  $(Z, +)$ . Quindi l'opposto di  $[a]_n$  è  $[-a]_n$ . Ma  $-a \equiv n - a \pmod{n}$ , quindi si ha:

$$-[a]_n = [-a]_n = [n - a]_n \quad \square$$

**Nota 470** Sia dato il gruppo  $(Z, +)$  e sia  $n \in \mathbb{N}$ . Si consideri il sottogruppo  $\langle n \rangle$  generato da  $n$ . Si ha  $\langle n \rangle = n\mathbb{Z}$  (vedere parte c) dell'esempio 390). Si verifica subito che la relazione di congruenza modulo  $n$  è uguale alla relazione relativa al sottogruppo  $\langle n \rangle$  definita nel teorema 431. Ma allora, per la parte 1) del teorema 441, si ha che la relazione di congruenza è una relazione di equivalenza. D'altronde il gruppo  $(Z, +)$  è abeliano, quindi il suo sottogruppo  $\langle n \rangle$  è normale (vedere nota 451). Ma allora la relazione di congruenza è compatibile con l'operazione di addizione in  $Z$  (vedere il teorema 453). Si ha inoltre che il gruppo  $(Z_n, +)$  è uguale al gruppo  $(Z/nZ, +)$  (vedere la definizione

454). Notiamo inoltre che  $Z/nZ$  ha come elementi le classi laterali (vedere la definizione 454). Abbiamo cioè:

$$[a]_n = a + nZ$$

**Esempio 471** Ecco la tabella dell'operazione del gruppo  $(Z_2, +)$ :

	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[0]_2$

Notare che  $[1]_2$  ha come opposto se stesso.

**Esempio 472** Ecco la tabella dell'operazione del gruppo  $(Z_3, +)$ :

	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[1]_3$	$[1]_3$	$[2]_3$	$[0]_3$
$[2]_3$	$[2]_3$	$[0]_3$	$[1]_3$

Notare che  $[1]_3$  e  $[2]_3$  sono opposti tra loro.

**Esercizio 473** Scrivere la tabella dell'operazione del gruppo  $(Z_4, +)$  e determinare l'opposto di ogni elemento.

**Esercizio 474** Scrivere la tabella dell'operazione del gruppo  $(Z_5, +)$  e determinare l'opposto di ogni elemento.

**Teorema 475** Il gruppo  $(Z_n, +)$  è un gruppo ciclico con generatore  $[1]_n$ .  
 DIMOSTRAZIONE. Sia  $[q]_n \in Z_n$ . Per il teorema 466 possiamo supporre  $0 \leq q < n$ . Si ha allora  $[q]_n = [1]_n + \cdots + [1]_n$  ( $q$  volte). Ogni elemento di  $Z_n$  è quindi ottenibile come “potenza” di  $[1]_n$ . Da ciò la tesi.  $\square$

**Esercizio 476** Si consideri il gruppo  $(Z_{20}, +)$ . Determinare un suo sottogruppo di ordine 4 e un suo sottogruppo di ordine 10.

Suggerimento: sfruttare il teorema precedente e il teorema 433.

**Esercizio 477** Determinare tutti i generatori dei gruppi  $(Z_n, +)$  con  $n = 2, 3, 4, 5, 6, 7$ .

**Teorema 478** Consideriamo il gruppo  $(Z_n, +)$ . Si ha:

$[a]_n$  è generatore di  $Z_n \iff a$  è primo con  $n$ .

Ricordiamo che due numeri interi non nulli  $a$  e  $b$  si dicono primi tra loro se il loro massimo comun divisore è 1.

DIMOSTRAZIONE. Omessa.  $\square$

Fino a questo momento abbiamo considerato l'operazione di addizione in  $Z$  ed abbiamo considerato l'operazione indotta in  $Z_n$ . D'ora in poi tentiamo di farlo stesso con l'operazione di moltiplicazione in  $Z$ .

**Teorema 479** La relazione di congruenza modulo  $n$  è compatibile con l'operazione di moltiplicazione in  $Z$ .

DIMOSTRAZIONE. Sia  $a \equiv a' \pmod{n}$ ,  $b \equiv b' \pmod{n}$ . Quindi:

$a - a' = qn$ ,  $b - b' = q'n$  con  $q \in Z$ ,  $q' \in Z$ . Dobbiamo dimostrare che si ha  $ab - a'b' = s'n$  con  $s' \in Z$ . Si ha:

$ab - a'b' = ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') = qnb + a'q'n = (qb + a'q')n$ .

Da cui  $s' = qb + a'q'$ . Da cui la tesi.  $\square$

**Teorema 480** Poiché l'operazione di moltiplicazione in  $Z$  è compatibile con la relazione di congruenza modulo  $n$ , è possibile definire su  $Z_n$  l'operazione di moltiplicazione nel seguente modo:

$$[a]_n \cdot [b]_n = [a \cdot b]_n.$$

Si ha che  $(Z_n, \cdot)$  è un monoide (è cioè un gruppoide associativo avente  $[1]_n$  come elemento neutro) commutativo.

DIMOSTRAZIONE. Sappiamo che il gruppoide  $(Z, \cdot)$  è un monoide commutativo (vedere l'esempio 329), quindi il gruppoide quoziente  $(Z_n, \cdot)$  è anch'esso un monoide commutativo. Poiché 1 è l'elemento neutro di  $(Z, \cdot)$ , l'elemento neutro di  $(Z_n, \cdot)$  è  $[1]_n$ .  $\square$

**Nota 481** Ci chiediamo se  $(Z_n, \cdot)$  sia un gruppo. Non può venirci in aiuto il teorema 440 poiché  $Z$  con l'operazione di moltiplicazione non è un gruppo. Notiamo che si ha:

$$[0]_n \cdot [a]_n = [0]_n \quad \forall [a]_n \in Z_n$$

L'elemento  $[0]_n$  non è dotato quindi di inverso. Ne segue che  $(Z_n, \cdot)$  non è un gruppo.

Visto che  $[0]_n$  non è dotato di inverso, eliminiamo da  $Z_n$  l'elemento  $[0]_n$ . Consideriamo cioè  $Z_n^* = Z_n - \{[0]_n\}$ . Ci chiediamo se abbiamo così ottenuto un gruppo.

**Esempio 482** Consideriamo  $Z_4^*$ . Si ha  $[2]_4 \cdot [2]_4 = [0]_4 \notin Z_4^*$ . L'operazione di moltiplicazione non è quindi definita in  $Z_4^*$ .

Si ha, più in generale, il seguente teorema:

**Teorema 483** Dato  $n \in N$ , se  $n = p \cdot q$  con  $p \in N, p \neq 1$  e  $q \in N, q \neq 1$ , l'insieme  $Z_n^*$  non è chiuso rispetto all'operazione di moltiplicazione.

DIMOSTRAZIONE. Sia  $n = p \cdot q$ . Dalle ipotesi su  $p$  e  $q$  segue  $[p]_n \in Z_n^*$  e  $[q]_n \in Z_n^*$ . Si ha poi  $[p]_n \cdot [q]_n = [0]_n \notin Z_n^*$ . Da cui la tesi.  $\square$

**Esempio 484** D'altra parte si ha che  $(Z_5^*, \cdot)$  è un gruppo abeliano. Ecco infatti la tabella della moltiplicazione di  $Z_5$ :

	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

Dall'esame della tabella si nota che  $(Z_5^*, \cdot)$  è un gruppo abeliano.

**Definizione 485** Sia  $n \neq 0$ . Dato il gruppoide  $(Z_n, \cdot)$ , indichiamo con  $\text{Inv}(Z_n)$  l'insieme degli elementi di  $Z_n$  dotati di inverso rispetto all'operazione di moltiplicazione.

**Teorema 486** L'insieme  $\text{Inv}(Z_n)$  con l'operazione di moltiplicazione di  $Z_n$  è un gruppo abeliano.

**DIMOSTRAZIONE.** Dobbiamo innanzitutto dimostrare che  $\text{Inv}(Z_n)$  è chiuso rispetto all'operazione di moltiplicazione.

Siano  $a \in \text{Inv}(Z_n)$  e  $b \in \text{Inv}(Z_n)$ . Siano  $a^{-1}$  e  $b^{-1}$  gli inversi di  $a$  e  $b$  rispettivamente. Dal teorema 340 segue che  $b^{-1} \cdot a^{-1}$  è l'inverso di  $a \cdot b$ . Abbiamo dimostrato che  $\text{Inv}(Z_n)$  è chiuso rispetto alla moltiplicazione. La proprietà associativa è ovviamente dimostrata. Poiché  $[1]_n^{-1} = [1]_n$  abbiamo anche che  $\text{Inv}(Z_n)$  è dotato di elemento neutro. Sia ora  $[a]_n \in \text{Inv}(Z_n)$ . Dobbiamo dimostrare che esso è dotato di inverso. Per definizione di  $\text{Inv}(Z_n)$  abbiamo che esiste  $[a]_n^{-1} \in Z_n$ . Dobbiamo dimostrare che  $[a]_n^{-1} \in \text{Inv}(Z_n)$ . Ma  $[a]_n^{-1}$  ha come inverso  $[a]_n$  e quindi è invertibile. L'operazione di moltiplicazione è ovviamente commutativa.  $\square$

Il teorema precedente può essere generalizzato. Si ha infatti il seguente teorema.

**Teorema 487** Sia  $(G, \cdot)$  un monoide. Sia, per definizione,  $\text{Inv}(G)$  l'insieme degli elementi di  $G$  dotati di inverso. Si ha che l'insieme  $\text{Inv}(G)$  con l'operazione di moltiplicazione di  $G$  è un gruppo.

**DIMOSTRAZIONE.** Lasciata per esercizio: è una facile generalizzazione della dimostrazione del teorema precedente.  $\square$

**Esempio 488** Cerchiamo  $\text{Inv}(Z_4)$ . L'elemento  $[2]_4$  non è invertibile. Infatti, se esistesse un elemento  $[a]_4$  che è inverso di  $[2]_4$ , dovrebbe esistere  $q \in Z$  tale che  $2a - 1 = 4q$ ; da cui  $2a - 4q = 1$ . Quest'ultima uguaglianza è assurda perchè il primo membro di essa è divisibile per 2, mentre il secondo membro non lo è. L'elemento  $[3]_4$  ha come inverso se stesso. Quindi  $\text{Inv}(Z_4) = \{[1]_4, [3]_4\}$ .

**Esempio 489** Determiniamo  $\text{Inv}(Z_6)$ . Con un ragionamento analogo a quello svolto nell'esempio precedente si nota che gli elementi  $[a]_6$  con  $a = 2, 3, 4$  non sono invertibili. L'elemento  $[5]_6$  ha come inverso se stesso. Quindi  $\text{Inv}(Z_6) = \{[1]_6, [5]_6\}$ .

**Esercizio 490** Determinare  $\text{Inv}(Z_n)$  per ogni  $1 \leq n \leq 8$ .

**Esercizio 491** Una studentessa del corso dell'anno accademico 1993-94, dopo aver svolto l'esercizio precedente, si è accorta che in tutti gli otto casi considerati si ha  $[n-1]_n^{-1} = [n-1]_n$ . Ha provato poi con qualche  $n > 8$  ed ha ottenuto sempre la stessa risposta. Ha perciò fatto la seguente congettura che chiamiamo **congettura della studentessa**:

$$\forall n \in N \quad [n-1]_n^{-1} = [n-1]_n$$

Dimostrare la verità o falsità della congettura della studentessa.

**Esercizio 492** Uno studente del corso dell'anno accademico 1993-94, dopo aver svolto l'esercizio 490, si è accorto che, se  $n \leq 8$  è pari, allora  $[2]_n$  non è dotato di inverso. Se invece  $n < 8$  è dispari, allora  $[2]_n$  è dotato di inverso. Anche lui ha provato con qualche  $n > 8$  ed ha sempre ottenuto la stessa risposta. Ha quindi formulato la seguente congettura che ovviamente chiamiamo **congettura dello studente**:

- 1)  $\forall n = 2p$ , con  $p \in N$ , si ha che  $[2]_n$  non è dotato di inverso;
- 2)  $\forall n = 2p - 1$ , con  $p \in N$ , si ha che  $[2]_n$  è dotato di inverso.

Dimostrare la verità o falsità della congettura dello studente.

**Esercizio 493** Determinare le tabelle di moltiplicazione dei gruppi  $(\text{Inv}(Z_n), \cdot)$  per ogni  $1 \leq n \leq 8$ .

**Esercizio 494** Uno studente del corso dell'anno accademico 1994-95, dopo aver svolto l'esercizio precedente, si è accorto che tutte le tabelle di moltiplicazione dei gruppi in questione, oltre ad essere simmetriche rispetto alla diagonale principale (il che non lo ha meravigliato perchè ben sa che i gruppi in questione sono abeliani), sono simmetriche anche rispetto alla diagonale secondaria. Ha quindi formulato la seguente congettura che ovviamente chiamiamo **congettura del secondo studente**:

le tabelle di moltiplicazione dei gruppi  $(\text{Inv}(Z_n), \cdot)$  per ogni  $n$  sono simmetriche rispetto alla diagonale secondaria.

Dimostrare la verità o falsità della congettura del secondo studente.

**Esercizio 495** Uno studente del corso dell'anno accademico 1996-97 ha fatto la seguente congettura (che chiamiamo **congettura del terzo studente**):

La classe  $[a]_n$  è dotata di inverso in  $Z_n$  se e solo se nella riga corrispondente all'elemento  $[a]_n$  della tabella moltiplicativa del gruppoide  $(Z_n, \cdot)$  compaiono tutti gli elementi di  $Z_n$ .

Dimostrare la verità o falsità della congettura.

Svolgendo l'esercizio 490 si sono determinati gli eventuali inversi dei singoli elementi di  $Z_n$  (con  $n \leq 8$ ) andando per tentativi. Certamente, se  $n$  è un numero grande, è troppo lungo procedere per tentativi. È, per esempio, estremamente

lungo e noioso determinare l'eventuale inverso di  $[200]_{65537}$ .

In effetti vi è un algoritmo che permette di fare questo calcolo in breve tempo. Per poter spiegare questo algoritmo abbiamo bisogno di studiare alcune proprietà aritmetiche. Faremo ciò nel prossimo paragrafo.

### 3.10 Proprietà aritmetiche

**Definizione 496** Dati due numeri  $p \in \mathbb{Z}$  e  $a \in \mathbb{Z}$  si dice che  $p$  è **divisore** di  $a$  (o che  $p$  **divide**  $a$ ) se esiste un numero  $q \in \mathbb{Z}$  tale che  $a = q \cdot p$ . Per indicare che  $p$  divide  $a$  si usa il simbolo  $p|a$ . Spesso, quando  $p|a$ , si dice che  $a$  è un **multiplo** di  $p$  e che  $p$  è un **sottomultiplo** di  $a$ .

**Teorema 497** Dati  $d \in \mathbb{Z}$ ,  $a \in \mathbb{Z}$ ,  $b \in \mathbb{Z}$  si ha:

$$d|a, d|b \implies d|x \cdot a + y \cdot b \quad \forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}.$$

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

**Nota 498** In particolare si ha:

$$d|a \implies d|-a$$

**Nota 499** Dato comunque un numero  $a \in \mathbb{Z}$ , si ha che i numeri  $\pm 1$  e  $\pm a$  sono divisori di  $a$ .

**Nota 500** Il numero 0 ha come divisori tutti i numeri  $a \in \mathbb{Z}$ .

**Definizione 501** Un numero  $a \in \mathbb{Z}$  si dice **primo** se  $a \neq \pm 1$  e gli unici divisori di  $a$  sono  $\pm 1$  e  $\pm a$ .

**Definizione 502** Dati  $a \in \mathbb{Z}^*$  e  $b \in \mathbb{Z}^*$  (quindi  $a$  e  $b$  sono numeri interi non nulli), un numero  $d \in \mathbb{Z}$  si dice **massimo comun divisore** di  $a$  e  $b$  se esso verifica le seguenti condizioni:

1)  $d > 0$

2)  $d|a$  e  $d|b$

3) se  $d' \in \mathbb{Z}$  è tale che  $d'|a$  e  $d'|b$ , allora  $d'|d$ .

Dimostreremo in 505 che, dati  $a$  e  $b$ , esiste ed è unico il loro massimo comun divisore. Il massimo comun divisore di  $a$  e  $b$  viene indicato con il simbolo  $M.C.D.(a, b)$  oppure con il simbolo  $(a, b)$ . Noi useremo di solito quest'ultimo.

**Teorema 503** Dati  $a \in \mathbb{Z}^*$  e  $b \in \mathbb{Z}^*$ , si ha:

$$(a, b) = (|a|, |b|)$$

DIMOSTRAZIONE. Si ha ovviamente:

$$d|a \iff d|(-a)$$

Da ciò segue facilmente (esercizio) la tesi.  $\square$



**Nota 504** Possiamo perciò d'ora in poi limitarci a considerare il massimo comun divisore di numeri interi positivi.

**Teorema 505** Dati  $a \in N$  e  $b \in N$ , esiste ed è unico il loro massimo comun divisore.

**DIMOSTRAZIONE.** Dimostriamo innanzitutto l'unicità. Siano  $d$  e  $d'$  massimi comun divisori di  $a$  e  $b$ . Si ha che  $d'$  divide sia  $a$  che  $b$ . Quindi, essendo  $d$  massimo comun divisore di  $a$  e  $b$ , si ha  $d = p \cdot d'$  con  $p \in N$  poiché sia  $d$  che  $d'$  sono positivi. Analogamente si dimostra che si ha  $d' = p' \cdot d$ . Abbiamo allora:  $d' = p' \cdot d = p' \cdot p \cdot d'$ . Ne segue  $1 = p' \cdot p$ . Essendo  $p$  e  $p'$  interi positivi abbiamo  $p = p' = 1$ . Quindi  $d = d'$ .

Dimostriamo ora l'esistenza del massimo comun divisore. Determineremo il massimo comun divisore di  $a \in N$  e  $b \in N$  utilizzando un algoritmo, detto **algoritmo di Euclide**<sup>5</sup>.

Per rendere più chiaro l'algoritmo, lo descriviamo innanzitutto scegliendo due numeri particolari  $a = 2184$  e  $b = 1980$ . Vedremo in seguito che il procedimento seguito si applica ad una qualsiasi coppia di numeri naturali.

Cominciamo con il dividere il maggiore dei due numeri per l'altro:

$$\underline{2184} = \underline{1980} \cdot 1 + \underline{204}$$

Abbiamo sottolineato il dividendo, il divisore e il resto. Dividiamo il divisore per il resto:

$$\underline{1980} = \underline{204} \cdot 9 + \underline{144}$$

Continuiamo con lo stesso procedimento:

$$\underline{204} = \underline{144} \cdot 1 + \underline{60}$$

$$\underline{144} = \underline{60} \cdot 2 + \underline{24}$$

$$\underline{60} = \underline{24} \cdot 2 + \underline{12}$$

$$\underline{24} = \underline{12} \cdot 2 + 0$$

Quindi il numero 12 è l'ultimo resto non nullo. Dimostriamo che esso è il massimo comun divisore.

Innanzitutto 12 è un numero positivo. La prima condizione è quindi verificata. Dimostriamo ora che 12 divide i due numeri.

Dall'ultima uguaglianza segue che il numero 12, oltre a dividere ovviamente se stesso, divide anche 24. Dalla penultima uguaglianza, sfruttando il teorema 497, segue che 12 divide 60. Dalla terzultima uguaglianza segue che 12 divide 144. Analogamente 12 divide 204, quindi anche 1980 e quindi anche 2184. Abbiamo verificato che 12 è divisore comune di 2184 e 1980.

Dobbiamo ora verificare che esso è il massimo comun divisore. A tal scopo scriviamo i resti delle successive divisioni come combinazioni lineari del dividendo

<sup>5</sup>**Euclide**, (terzo-quarto secolo a.C.), matematico greco che descrisse l'algoritmo nei suoi "Elementi".

e del divisore:

$$\underline{204} = \underline{2184} + \underline{1980} \cdot (-1)$$

$$\underline{144} = \underline{1980} + \underline{204} \cdot (-9)$$

$$\underline{60} = \underline{204} + \underline{144} \cdot (-1)$$

$$\underline{24} = \underline{144} + \underline{60} \cdot (-2)$$

$$\underline{12} = \underline{60} + \underline{24} \cdot (-2)$$

Supponiamo ora che  $d'$  sia divisore comune di 2184 e 1980. Dalla prima delle uguaglianze precedenti segue che  $d'$  divide 204. Dalla seconda uguaglianza segue che  $d'$  divide 144; dalla terza segue che  $d'$  divide 60; dalla quarta segue che  $d'$  divide 24; dalla quinta segue che  $d'$  divide 12. Abbiamo dimostrato che 12 è il massimo comun divisore.

Possiamo utilizzare questo algoritmo per due numeri  $a \in N$  e  $b \in N$  qualsiasi. Se  $a = b$ , allora ovviamente  $(a, b) = a = b$ . Sia  $a > b$ . Appliciamo il nostro algoritmo. Abbiamo:

$$\underline{a} = \underline{b} \cdot q_0 + \underline{r_0} \quad \text{con } 0 \leq r_0 < b$$

$$\underline{b} = \underline{r_0} \cdot q_1 + \underline{r_1} \quad \text{con } 0 \leq r_1 < r_0$$

$$\underline{r_0} = \underline{r_1} \cdot q_2 + \underline{r_2} \quad \text{con } 0 \leq r_2 < r_1$$

...

$$\underline{r_{n-2}} = \underline{r_{n-1}} \cdot q_n + \underline{r_n} \quad \text{con } 0 \leq r_n < r_{n-1}$$

$$\underline{r_{n-1}} = \underline{r_n} \cdot q_{n+1} + 0$$

Ad un certo punto dobbiamo necessariamente ottenere un resto uguale a 0 perchè la successione dei resti è una successione strettamente decrescente di numeri maggiori o uguali a 0. L'ultimo resto non nullo è il massimo comun divisore di  $a$  e  $b$ . Per dimostrare ciò basta seguire la falsariga della dimostrazione data nell'esempio numerico. Lasciamo per esercizio la dimostrazione dell'unicità.  $\square$

**Teorema 506** Dati  $a \in Z^*$  e  $b \in Z^*$ , sia  $d$  il massimo comun divisore di  $a$  e  $b$ . Allora esistono  $x \in Z$  e  $y \in Z$  che verificano la seguente **identità di Bezout**<sup>6</sup>:

$$d = a \cdot x + b \cdot y$$

**DIMOSTRAZIONE.** Consideriamo innanzitutto il caso in cui si abbia  $a \in N$  e  $b \in N$ . Si applichi l'algoritmo di Euclide per determinare  $d$ . Esso è l'ultimo resto  $r_n$  non nullo. Dalla penultima identità si scrive  $r_n$  come combinazione lineare a coefficienti interi di  $r_{n-1}$  e di  $r_{n-2}$ . Poiché  $r_{n-1}$  è a sua volta combinazione lineare a coefficienti interi di  $r_{n-2}$  e di  $r_{n-3}$ , si scrive  $r_n$  come combinazione

<sup>6</sup>Étienne Bézout, (1730-1783), matematico francese.

lineare di  $r_{n-2}$  e di  $r_{n-3}$ . Continuando in questo modo si scrive  $r_n$  come combinazione lineare di  $a$  e  $b$ .

Siano ora  $a \in Z^*$  e  $b \in Z^*$ . Consideriamo i numeri  $|a| \in N$  e  $|b| \in N$ . Dal teorema 503 segue  $d = (a, b) = (|a|, |b|)$ . Per quel che abbiamo appena dimostrato, esistono  $x' \in Z$  e  $y' \in Z$  tali che  $d = |a| \cdot x' + |b| \cdot y'$ . Supponiamo che si abbia  $a < 0$  e  $b < 0$ . Abbiamo allora  $d = a \cdot (-x') + b \cdot (-y')$ . Ponendo  $x = -x'$  e  $y = -y'$  abbiamo la tesi. Nel caso in cui  $a > 0$  e  $b < 0$  oppure  $a < 0$  e  $b > 0$  ci si comporta in modo analogo.  $\square$

**Nota 507** I numeri  $x$  e  $y$  dell'identità di Bezout non sono unici. Dimostriamo che ve ne sono infiniti.

Si ha ovviamente:

$0 = a \cdot b + b \cdot (-a)$ . Quindi  $\forall n \in Z$  si ha  $0 = a \cdot (b \cdot n) + b \cdot (-a \cdot n)$ . Data allora l'identità di Bezout:

$$d = a \cdot x + b \cdot y$$

si ha  $\forall n \in Z$ :

$$d = d + 0 = a \cdot x + b \cdot y + a \cdot (b \cdot n) + b \cdot (-a \cdot n) = a \cdot (x + b \cdot n) + b \cdot (y - a \cdot n)$$

**Esempio 508** Vogliamo determinare l'identità di Bezout che lega i numeri 2184 e 1980 con il loro massimo comun divisore 12. Applicando l'algoritmo di Euclide avevamo trovato le seguenti identità:

$$\underline{204} = \underline{2184} + \underline{1980} \cdot (-1)$$

$$\underline{144} = \underline{1980} + \underline{204} \cdot (-9)$$

$$\underline{60} = \underline{204} + \underline{144} \cdot (-1)$$

$$\underline{24} = \underline{144} + \underline{60} \cdot (-2)$$

$$\underline{12} = \underline{60} + \underline{24} \cdot (-2)$$

Sostituiamo nell'ultima identità il numero 24 con la sua combinazione lineare di 144 e 60 (penultima identità) e così di seguito. Si ha:

$$\begin{aligned} \underline{12} &= \underline{60} + \underline{24} \cdot (-2) = \underline{60} + [\underline{144} + \underline{60} \cdot (-2)] \cdot (-2) = \underline{144} \cdot (-2) + \underline{60} \cdot 5 = \\ &= \underline{144} \cdot (-2) + [\underline{204} + \underline{144} \cdot (-1)] \cdot 5 = \underline{204} \cdot 5 + \underline{144} \cdot (-7) = \\ &= \underline{204} \cdot 5 + [\underline{1980} + \underline{204} \cdot (-9)] \cdot (-7) = \underline{1980} \cdot (-7) + \underline{204} \cdot 68 = \\ &= \underline{1980} \cdot (-7) + [\underline{2184} + \underline{1980} \cdot (-1)] \cdot 68 = \underline{2184} \cdot 68 + \underline{1980} \cdot (-75) \end{aligned}$$

Abbiamo quindi determinato l'identità di Bezout:

$$12 = 2184 \cdot 68 + 1980 \cdot (-75)$$

**Esercizio 509** Calcolare il massimo comun divisore dei numeri 73810 e 9318. Determinare quindi  $x \in Z$  e  $y \in Z$  tali che

$$(73810, 9318) = 73810 \cdot x + 9318 \cdot y$$

**Esercizio 510** Calcolare il massimo comun divisore dei numeri 73810 e -9318. Determinare quindi  $x \in Z$  e  $y \in Z$  tali che

$$(73810, -9318) = 73810 \cdot x + (-9318) \cdot y$$

**Definizione 511** Due numeri  $a \in Z^*$  e  $b \in Z^*$  si dicono **primi tra loro** se hanno come divisore comune solamente i numeri  $\pm 1$ .

Si ha quindi che  $a$  e  $b$  sono primi tra loro se e solo se  $(a, b) = 1$ .

**Esercizio 512** Verificare se i numeri 37957 e 123957 sono primi tra loro.

### 3.11 Ancora le classi resto

Abbiamo visto nell'esempio 488 che gli elementi invertibili di  $(Z_4, \cdot)$  sono dati dagli elementi  $[a]_4$  tali che  $a$  e 4 siano primi tra loro. Nel caso di  $(Z_6, \cdot)$  accade una cosa analoga (vedere l'esempio 489). Ci chiediamo se è vero, in generale, che gli elementi invertibili di  $(Z_n, \cdot)$  sono tutti e soli gli elementi  $[a]_n$  tali che  $a$  e  $n$  siano primi tra loro.

Innanzitutto ci chiediamo se tutto ciò abbia senso. Infatti tutto sembra dipendere dalla scelta dell'elemento della classe  $[a]_n$ . Ci chiediamo cioè: se  $a$  e  $n$  sono primi tra loro e se  $b \in [a]_n$ , è vero che  $b$  e  $n$  sono primi tra loro? La risposta è affermativa. Si ha infatti:

**Teorema 513** Sia  $b \in [a]_n$ . Allora  $(a, n) = (b, n)$ .

**DIMOSTRAZIONE.** Sia  $d = (a, n)$ . Sia  $b = a + q \cdot n$ . Poiché  $d$  è divisore di  $a$  e di  $n$  è anche divisore di  $b$ . Dimostriamo che  $d$  è il massimo comun divisore di  $b$  e  $n$ . Sia  $d'$  divisore di  $b$  e  $n$ . Da  $a = b - q \cdot n$  segue che  $d'$  è divisore di  $a$  e  $n$ . Essendo  $d$  il massimo comun divisore di  $a$  e  $n$ , si ha che  $d'$  divide  $d$ .  $\square$

**Teorema 514** Sia  $n \in N$ . Si ha  $\text{Inv}(Z_n) = \{[a]_n \text{ tali che } (a, n) = 1\}$ .

**DIMOSTRAZIONE.** Dimostriamo innanzitutto che, se  $[a]_n$  è dotato di inverso, allora  $(a, n) = 1$ .

Sia  $[b]_n = [a]_n^{-1}$ . Allora si ha:

$a \cdot b = 1 + q \cdot n$ . Da cui  $a \cdot b - q \cdot n = 1$ . Ma  $d = (a, n)$  è divisore di  $a$  e di  $n$ ; quindi è divisore di  $a \cdot b - q \cdot n = 1$ . Quindi  $d = \pm 1$ . Quindi  $(a, n) = 1$ .

Dobbiamo ora dimostrare che, se  $(a, n) = 1$ , allora  $[a]_n$  è dotato di inverso.

Poiché  $(a, n) = 1$ , dall'identità di Bezout (vedere teorema 506) segue che esistono  $x \in Z$  e  $y \in Z$  tali che:

$$a \cdot x + n \cdot y = 1.$$

Da ciò segue  $a \cdot x = 1 + (-y) \cdot n$ . E quindi:

$$[a \cdot x]_n = [a]_n \cdot [x]_n = [1]_n$$

Pertanto:

$$[x]_n = [a]_n^{-1}$$

Abbiamo dimostrato il nostro teorema.  $\square$

**Nota 515** La dimostrazione del teorema precedente ci dà un algoritmo per determinare l'inverso di un elemento di  $(Z_n, \cdot)$  (ammesso che esso esista). Cerchiamo, per esempio, l'inverso di  $[10]_{23}$  in  $(Z_{23}, \cdot)$ . Sappiamo che il massimo comun divisore di 10 e 23 è 1. Utilizzando l'algoritmo di Euclide, possiamo determinare l'identità di Bezout che lega i numeri 1, 10 e 23 (vedere teorema 506). Svolgendo i calcoli (esercizio) si ottiene l'identità di Bezout:

$$1 = 10 \cdot 7 + 23 \cdot (-3)$$

Quindi  $[7]_{23} \cdot [10]_{23} = [1]_{23}$ .  
Pertanto abbiamo:

$$[10]_{23}^{-1} = [7]_{23}$$

**Esercizio 516** Determinare  $\text{Inv}(Z_{18})$  e, per ogni suo elemento, determinare l'inverso.

**Esercizio 517** Determinare  $\text{Inv}(Z_{24})$  e, per ogni suo elemento, determinare l'inverso.

**Teorema 518** Sia  $n \in \mathbb{N}$ . Se  $n$  non è primo allora  $Z_n^*$  non è chiuso rispetto alla moltiplicazione.

Se  $n$  è primo allora  $(Z_n^*, \cdot)$  è un gruppo.

**DIMOSTRAZIONE.** Se  $n$  non è primo dal teorema 483 segue che  $Z_n^*$  non è chiuso rispetto alla moltiplicazione.

Se  $n$  è un numero primo allora dal teorema precedente segue  $\text{Inv}(Z_n) = Z_n^*$  e quindi  $(Z_n^*, \cdot)$  è un gruppo.  $\square$

**Esercizio 519** Il numero 257 è primo. Quindi  $[200]_{257}$  è dotato di inverso. Calcolarlo.

**Esercizio 520** Il numero 65537 è primo. Quindi  $[200]_{65537}$  è dotato di inverso. Calcolarlo.

**Nota 521** Abbiamo affermato nei precedenti due esercizi che i numeri 257 e 65537 sono primi. Si ha:

$$257 = 2^{(2^3)} + 1$$

$$65537 = 2^{(2^4)} + 1$$

Quindi i due numeri precedenti sono del tipo:

$$F(h) = 2^{(2^h)} + 1$$

Abbiamo utilizzato il simbolo  $F(h)$  per indicare questi numeri perchè essi sono chiamati **numeri di Fermat**<sup>7</sup>. Fermat infatti aveva affermato che i numeri di questo tipo sono tutti primi. In effetti si ha:

$$F(1) = 5$$

---

<sup>7</sup>**Pierre de Fermat**, (1601-1665), matematico francese.

$$F(2) = 17$$

$$F(3) = 257$$

$$F(4) = 65537$$

sono tutti numeri primi. Si ha poi:

$$F(5) = 4294967297$$

Ebbene, Eulero<sup>8</sup> nel 1732 ha dimostrato che  $F(5)$  non è primo. Si ha infatti

$$F(5) = 641 \cdot 6700417$$

Anche il numero  $F(6)$  non è primo. Si ha infatti:

$$F(6) = 18446744073709551617 = 274177 \cdot 67280421310721$$

Quindi vi sono dei controesempi all'affermazione di Fermat. In effetti a tutt'oggi non è stato trovato alcun numero di Fermat  $F(h)$  con  $h > 4$  che sia primo. Quindi Fermat ha sbagliato in modo clamoroso.

Ma Fermat non ha sempre fatto congetture presto rivelatesi sbagliate. Famoso è l'**ultimo teorema di Fermat**. Fermat ha affermato che, dato  $n > 2$  non esistono numeri naturali  $a, b$  e  $c$  tali che  $a^n + b^n = c^n$ . Egli però non ne ha dato la dimostrazione. Per secoli i matematici hanno provato a dimostrare ciò o a darne un controesempio. Nel giugno del 1993 il matematico inglese Andrew Wiles ha dichiarato di aver dimostrato il teorema. In effetti un'attenta verifica della dimostrazione ha mostrato che in essa vi era un "buco". Vi era cioè un punto ancora non dimostrato.

Nel 1995 Wiles ha coperto il "buco". Il teorema ora è effettivamente dimostrato. Il bel libro di S.Singh (vedere bibliografia) descrive, in modo divulgativo, la lunga storia di questo teorema.

**Definizione 522** Si definisce **funzione di Eulero** la seguente funzione:

$$\Phi : N \longrightarrow N$$

$$\Phi(1) = 1;$$

se  $n > 1$ ,  $\Phi(n)$  è il numero di interi minori di  $n$  e primi con  $n$ .

Quindi, per esempio:  $\Phi(1) = 1$ ,  $\Phi(2) = 1$ ,  $\Phi(3) = 2$ ,  $\Phi(4) = 2$

$\Phi(5) = 4$ ,  $\Phi(6) = 2$ .

**Nota 523** Se  $p$  è un numero primo, allora  $\Phi(p) = p - 1$ .

**Teorema 524** [Teorema di Eulero] Sia  $n$  un numero intero positivo e sia  $a$  un numero intero primo con  $n$ . Allora si ha:

$$1) \quad a^{\Phi(n)} \equiv 1 \pmod{n};$$

---

<sup>8</sup>Leonhard Euler, (1707-1783), matematico svizzero.

2)  $a^{-1} \equiv a^{\Phi(n)-1} \pmod{n}$ .

**DIMOSTRAZIONE.** Consideriamo il gruppo  $(\text{Inv}(Z_n), \cdot)$ . Dalla definizione di funzione di Eulero e dal teorema 514 segue che l'ordine di  $\text{Inv}(Z_n)$  è uguale a  $\Phi(n)$ . Il fatto che  $a$  sia primo con  $n$  implica  $[a]_n \in \text{Inv}(Z_n)$ . La parte 1) segue dalla parte 2 del teorema 434. La parte 2) segue immediatamente dalla parte 3) del teorema 434.  $\square$

**Nota 525** Dato  $n$  intero positivo e  $[a]_n \in \text{Inv}(Z_n)$ , abbiamo a suo tempo determinato  $[a]_n^{-1}$  utilizzando l'identità di Bezout. La parte 2) del teorema di Eulero (vedere teorema 524 ci fornisce un altro algoritmo per la determinazione di  $[a]_n^{-1}$ .

**Teorema 526** [Teorema di Fermat] Sia  $p$  un numero primo. Per ogni numero intero  $a$  si ha:

$$a^p \equiv a \pmod{p}$$

**DIMOSTRAZIONE.** Se  $a \equiv 0 \pmod{p}$  il teorema è ovviamente vero.

Se  $a \not\equiv 0 \pmod{p}$ , dalla nota 523 e dal teorema di Eulero segue

$$a^{p-1} \equiv 1 \pmod{p}$$

Moltiplicando ambo i membri per  $a$  segue la tesi.  $\square$ .

## 3.12 Omomorfismi

**Definizione 527** Siano dati due gruppi  $(G, *)$  e  $(G', *')$ . Una funzione  $f : G \longrightarrow G'$  si dice **omomorfismo** (tra gruppi) se verifica la seguente proprietà:

$$f(a * b) = f(a) *' f(b) \quad \forall a \in G \quad \forall b \in G$$

Spesso, per mettere in evidenza le operazioni dei due gruppi, si scrive:

$$f : (G, *) \longrightarrow (G', *')$$

Se la funzione  $f$ , oltre ad essere un omomorfismo tra gruppi, è anche biunivoca, allora si dice **isomorfismo**; in questo caso i due gruppi  $(G, *)$  e  $(G', *')$  si dicono **isomorfi**.

**Esercizio 528** Indichiamo con  $R^+$  l'insieme dei numeri reali positivi.

1) Dimostrare che  $(R^+, \cdot)$  è un gruppo abeliano.

2) Dimostrare che la funzione  $\exp : (R, +) \longrightarrow (R^+, \cdot)$  definita da

$$\exp(a) = e^a$$

è un isomorfismo tra gruppi.

**Esercizio 529** Dimostrare che l'applicazione  $\log : (R^+, \cdot) \longrightarrow (R, +)$  che associa a  $b$  il suo logaritmo  $\log(b)$  è un isomorfismo tra gruppi.

Notare che si ha che la funzione  $\log$  è l'inversa della funzione  $\exp$ .

**Teorema 530** Sia  $f : (G, *) \longrightarrow (G', *')$  un isomorfismo tra gruppi. Allora la funzione  $f^{-1}$  è un isomorfismo tra gruppi.

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

**Esercizio 531** L'applicazione  $f : (M(R, n, n), +) \longrightarrow (R, +)$  definita da  $f(A) = \det(A)$  è un omomorfismo tra gruppi?

**Esercizio 532** L'applicazione  $f : (GL(R, n), \cdot) \longrightarrow (R^*, \cdot)$  definita da  $f(A) = \det(A)$  è un omomorfismo tra gruppi?

**Esercizio 533** Dimostrare che il gruppoide  $(G = \{P, D\}, +)$  assegnato nell'esercizio 317 è un gruppo. Si consideri la funzione:

$$f : G \longrightarrow Z_2$$

assegnata nell'esercizio precedente.

Verificare che la funzione  $f$  è un isomorfismo tra i gruppi  $(G, +)$  e  $(Z_2, +)$ .

**Nota 534** D'ora in poi usiamo la notazione moltiplicativa per indicare le operazioni dei gruppi.

**Teorema 535** Sia  $f : (G, \cdot) \longrightarrow (G', \cdot)$  un omomorfismo tra gruppi. Allora:

1) Se 1 è l'elemento neutro del gruppo  $(G, \cdot)$  allora  $f(1)$  è l'elemento neutro del gruppo  $(G', \cdot)$ .

2) Dato un elemento  $g$  nel gruppo  $(G, \cdot)$ , allora  $f(a) \in f(G)$  ha come inverso l'elemento  $f(a^{-1})$ .

In altre parole si ha:

$$[f(a)]^{-1} = [f(a^{-1})]$$

3) Dato un elemento  $g$  nel gruppo  $(G, \cdot)$ , allora si ha

$$f(g^n) = [f(g)]^n \quad \forall n \in Z$$

4) Si ha che  $(f(G), \cdot)$  è un sottogruppo del gruppo  $(G', \cdot)$ .

DIMOSTRAZIONE. Lasciata per esercizio.  $\square$

**Nota 536** Nell'enunciato del teorema precedente abbiamo utilizzato la notazione moltiplicativa sia per il gruppo  $(G, \cdot)$  che per il gruppo  $(G', \cdot)$ . Abbiamo quindi utilizzato lo stesso simbolo  $\cdot$  sia per l'operazione in  $G$  sia per l'operazione in  $G'$ . È bene notare che le due operazioni non sono necessariamente la stessa operazione.

**Definizione 537** Sia  $f : (G, \cdot) \longrightarrow (G', \cdot)$  un omomorfismo tra gruppi. Poniamo:

$$\ker(f) = \{a \in G \mid f(a) = 1\}$$

Chiamiamo tale sottoinsieme di  $G$  **nucleo**<sup>9</sup> di  $f$ .

<sup>9</sup>Il simbolo  $\ker$  è l'abbreviazione della parola tedesca *kern* che significa appunto nucleo, anima.



**Teorema 538** Sia  $f : (G, \cdot) \longrightarrow (G', \cdot)$  un omomorfismo tra gruppi. Allora:

1) Si ha che  $(\ker(f), \cdot)$  è un sottogruppo normale di  $(G, \cdot)$

2) Sia  $a \in G$  e sia  $b = f(a)$ . Allora si ha:

$$f^{-1}(b) = a \cdot \ker f.$$

3) Dati  $a \in G$  e  $a' \in G$  si ha:

$$f(a) = f(a') \iff a \cdot \ker f = a' \cdot \ker f.$$

4) Da 2) segue che:

$$f \text{ iniettiva} \iff \ker f = \{1\}.$$

**DIMOSTRAZIONE.** Lasciata per esercizio. Per dimostrare che  $\ker f$  è un sottogruppo normale di  $G'$  si consiglia di utilizzare il teorema 452.  $\square$

**Esercizio 539** Sia  $n \in \mathbb{Z}$ . Si consideri l'applicazione  $f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$  definita da  $f(x) = nx$ .

Dimostrare che  $f$  è un omomorfismo tra gruppi per ogni  $n$ .

Determinare nucleo e immagine di  $f$  per ogni  $n \in \mathbb{Z}$ .

Determinare i valori di  $n$  per i quali  $f$  è surgettivo, i valori per i quali  $f$  è iniettivo e i valori per i quali  $f$  è un isomorfismo.

**Esercizio 540** Sia  $R^n[x]$  l'insieme dei polinomi in una variabile  $x$  a coefficienti reali di grado minore di  $n$ . Dimostrare che  $R^n[x]$  con l'operazione  $+$  di addizione tra polinomi è un gruppo abeliano.

Dimostrare che l'applicazione  $d : (R^n[x], +) \longrightarrow (R^{n-1}[x], +)$  che associa ad un polinomio la sua derivata è un omomorfismo tra gruppi. Determinare nucleo e immagine di  $d$ . Per ogni  $p(x) \in R^{n-1}[x]$ , determinare  $d^{-1}(p(x))$ .

**Definizione 541** Siano  $(G, \cdot)$  e  $(G', \cdot)$  gruppi. Indichiamo con il simbolo  $\text{Hom}(G, G')$  l'insieme degli omomorfismi tra gruppi  $f : (G, \cdot) \longrightarrow (G', \cdot)$ .

**Teorema 542** Siano  $f : (G, \cdot) \longrightarrow (G', \cdot)$  e  $f' : (G', \cdot) \longrightarrow (G'', \cdot)$  omomorfismi tra gruppi. Allora:

1)  $f' \circ f : (G, \cdot) \longrightarrow (G'', \cdot)$  è un omomorfismo tra gruppi.

2) Se sia  $f$  che  $f'$  sono isomorfismi, allora  $f' \circ f$  è un isomorfismo.

**DIMOSTRAZIONE.** Lasciata per esercizio.  $\square$

**Definizione 543** Dato un gruppo  $(G, \cdot)$ , chiamiamo **endomorfismo** di  $G$  un omomorfismo del gruppo  $G$  in se stesso.

Indichiamo con  $\text{End}(G)$  l'insieme degli endomorfismi di  $G$ .

Chiamiamo **automorfismo** un endomorfismo che sia un isomorfismo.

Indichiamo con  $\text{Auto}(G)$  l'insieme degli isomorfismi di  $G$  in se stesso.

**Teorema 544** Sia  $(G, \cdot)$  un gruppo. L'insieme  $\text{End}(G)$  con l'operazione di composizione tra funzioni è un monoide, cioè un gruppoide associativo dotato di elemento neutro. L'elemento neutro è dato dall'automorfismo identico.

L'insieme  $\text{Auto}(G)$  con l'operazione di composizione è un gruppo.

**DIMOSTRAZIONE.** Lasciata per esercizio.  $\square$

**Esercizio 545** Dati i gruppi  $(\mathbb{Z}_n, +)$ , calcolare  $\text{End}(\mathbb{Z}_n)$  e  $\text{Auto}(\mathbb{Z}_n)$  per  $n = 2, n = 3, n = 4$ .

**Nota 546** Per poter risolvere l'esercizio precedente sono stati necessari molti calcoli. I prossimi due teoremi ci permetteranno di eliminare quasi tutti i calcoli.

**Teorema 547** Sia  $\phi : (G, \cdot) \longrightarrow (G', \cdot)$  un omomorfismo tra gruppi.

Sia  $g \in G$  di periodo  $n$ . Allora  $\phi(g)$  ha periodo uguale ad un sottomultiplo di  $n$ .

**DIMOSTRAZIONE.** Si ha  $[\phi(g)]^n = \phi(g^n) = \phi(1) = 1$ . Quindi  $\phi(g)$  ha periodo finito. Sia esso  $p$ .

Sia  $n = p \cdot q + r$  con  $0 \leq r < p$ . Quindi:

$$1 = \phi(g^n) = [\phi(g)]^n = [[\phi(g)]^p]^q \cdot [\phi(g)]^r = 1^q \cdot \phi(g)^r = [\phi(g)]^r$$

da cui, poiché  $p$  è il più piccolo intero positivo tale che  $[\phi(g)]^p = 1$ , segue  $r = 0$ . Per cui  $n = p \cdot q$ .  $\square$

**Teorema 548** Sia  $(G, \cdot)$  un gruppo ciclico avente come generatore  $g$ . Sia  $(G', \cdot)$  un gruppo e sia  $g'$  un suo elemento. Cerchiamo un omomorfismo tra gruppi:

$$\phi : (G, \cdot) \longrightarrow (G', \cdot)$$

tale che

$$\phi(g) = g'$$

Si ha:

1) Se  $g$  ha periodo infinito allora esiste ed è unico un omomorfismo  $\phi$  tale che  $\phi(g) = g'$ ;

2) Se  $g$  ha periodo finito uguale a  $n$ , vi sono due possibilità:

2a) Il periodo di  $g'$  è  $p$  con  $n = pq$  e  $q \in \mathbb{Z}$ ; allora esiste ed è unico un omomorfismo  $\phi$  tale che  $\phi(g) = g'$ ;

2b) Il periodo di  $g'$  è infinito oppure non è un sottomultiplo di  $n$ ; allora non esiste alcun omomorfismo  $\phi$  tale che  $\phi(g) = g'$ .

**DIMOSTRAZIONE.** L'omomorfismo cercato dovrà necessariamente verificare la condizione  $\phi(g^h) = g'^h$ . Dato un elemento  $a \in G$ , esiste almeno un intero  $h$  tale che  $a = g^h$ , poniamo allora:

$$\phi(a) = g'^h$$

Da ciò deriva che, se l'omomorfismo esiste, esso è unico.

Dobbiamo dimostrare che la definizione è ben posta. Dobbiamo cioè dimostrare che, se  $a = g^h = g^k$ , allora  $g'^h = g'^k$ . Distinguiamo i vari casi:

1) Il periodo di  $g$  è infinito. In questo caso dal teorema 413, parte 1, segue che  $g^h = g^k$  implica  $h = k$ . L'applicazione è quindi ovviamente ben posta. Si verifica facilmente che essa è un omomorfismo tra gruppi. L'unicità segue dall'osservazione fatta all'inizio della dimostrazione.

2a) Il periodo di  $g$  è  $n$ . Dalla seconda parte del teorema 413 segue che  $g^h = g^k$  implica  $h \equiv k \pmod{n}$ . Ma allora, posto  $h = k + sn$  e ricordando che si ha  $n = pq$  con  $p$  periodo di  $g'$ , abbiamo:

$$g'^h = g'^{k+sn} = g'^k \cdot g'^{spq} = g'^k \cdot [g'^p]^{sq} = g'^k \cdot [1]^{sq} = g'^k$$

cioè la tesi.

2b) Segue dal teorema 547.  $\square$

**Esercizio 549** Si consideri il gruppo ciclico  $(Z, +)$ . Determinare  $\text{End}(Z)$  e dimostrare che il gruppoide  $(\text{End}(Z), \circ)$  è isomorfo al gruppoide  $(Z, \cdot)$ .

**Esempio 550** Vogliamo determinare tutti gli omomorfismi

$$\phi : (Z_4, +) \longrightarrow (Z_6, +)$$

Il gruppo  $(Z_4, +)$  è ciclico con generatore  $[1]_4$  di periodo 4. Per definire un omomorfismo è quindi sufficiente definire  $\phi([1]_4)$ . Cerchiamo gli elementi di  $Z_6$  che abbiano periodo uguale ad un sottomultiplo di 4.

L'elemento  $[0]_6$  ha periodo 1. Esiste quindi un unico omomorfismo  $\phi_0$  tale che  $\phi_0([1]_4) = [0]_6$ . Si verifica facilmente che si ha

$$\phi_0([a]_4) = [0]_6 \quad \forall [a]_4 \in Z_4$$

Si tratta quindi dell'omomorfismo nullo.

L'elemento  $[1]_6$  ha periodo 6. Non esiste quindi un omomorfismo  $\phi$  tale che  $\phi([1]_4) = [1]_6$ .

L'elemento  $[2]_6$  ha periodo 3. Non esiste quindi un omomorfismo  $\phi$  tale che  $\phi([1]_4) = [2]_6$ .

L'elemento  $[3]_6$  ha periodo 2. Esiste quindi un unico omomorfismo  $\phi_1$  tale che  $\phi_1([1]_4) = [3]_6$ . Si verifica facilmente che si ha:

$$\phi_1([0]_4) = \phi_1([2]_4) = [0]_6 \quad \text{e} \quad \phi_1([1]_4) = \phi_1([3]_4) = [3]_6$$

Per l'elemento  $[4]_6$  vale lo stesso discorso fatto per l'elemento  $[2]_6$ .

Per l'elemento  $[5]_6$  vale lo stesso discorso fatto per l'elemento  $[1]_6$ .

Abbiamo quindi solo due omomorfismi.

**Esercizio 551** Determinare tutti gli omomorfismi tra gruppi:

$$\phi : (Z, +) \longrightarrow (Z_2, +)$$

e per ognuno di essi determinarne nucleo e immagine.

**Esercizio 552** Determinare tutti gli omomorfismi tra gruppi:

$$\phi : (Z_2, +) \longrightarrow (Z_3, +)$$

e per ognuno di essi determinarne nucleo e immagine.

**Esercizio 553** Determinare tutti gli omomorfismi tra gruppi:

$$\phi : (Z_2, +) \longrightarrow (Z_4, +)$$

e per ognuno di essi determinarne nucleo e immagine.

**Esercizio 554** Determinare tutti gli omomorfismi tra gruppi:

$$\phi : (Z_2, +) \longrightarrow (Z, +)$$

e per ognuno di essi determinarne nucleo e immagine.

**Esercizio 555** Sia  $n \in \mathbb{N}$ . Per ogni  $n$  determinare tutti gli omomorfismi tra gruppi:

$$\phi : (Z_n, +) \longrightarrow (Z, +)$$

e per ognuno di essi determinarne nucleo e immagine.

**Esercizio 556** Determinare il gruppoide  $(\text{End}(Z_2), \circ)$  e la sua tabella dell'operazione.

**Esercizio 557** Determinare il gruppo  $(\text{Auto}(Z_2), \circ)$  e la sua tabella dell'operazione.

**Esercizio 558** Determinare il gruppoide  $(\text{End}(Z_3), \circ)$  e la sua tabella dell'operazione.

**Esercizio 559** Determinare il gruppo  $(\text{Auto}(Z_3), \circ)$  e la sua tabella dell'operazione.

**Esercizio 560** Determinare il gruppoide  $(\text{End}(Z_4), \circ)$  e la sua tabella dell'operazione.

**Esercizio 561** Determinare il gruppo  $(\text{Auto}(Z_4), \circ)$  e la sua tabella dell'operazione.

**Esercizio 562** Determinare il gruppoide  $(\text{End}(Z_5), \circ)$  e la sua tabella dell'operazione.

**Esercizio 563** Determinare il gruppo  $(\text{Auto}(Z_5), \circ)$  e la sua tabella dell'operazione.

**Esercizio 564** Si consideri il gruppo  $(G = \{1, -1, i, -i\}, \cdot)$ . Determinare tutti gli omomorfismi tra gruppi:

$$\phi : (G, \cdot) \longrightarrow (Z_4, +)$$

e per ognuno di essi determinarne nucleo e immagine.

**Esercizio 565** Sia dato il gruppo  $(Z_4, +)$ . Dimostrare che il gruppo  $(\text{Auto}(Z_4), \circ)$  è isomorfo al gruppo  $(Z_2, +)$ .

**Esercizio 566** Siano  $p$  e  $q$  due divisori di un numero naturale  $n$ . Dimostrare che esiste ed è unico un endomorfismo  $f$  di  $Z_n$  tale che  $f([1]_n) = [p]_n$ . Dimostrare che esiste ed è unico un endomorfismo  $g$  di  $Z_n$  tale che  $g([1]_n) = [q]_n$ . Dimostrare che esiste ed è unico un endomorfismo  $h$  di  $Z_n$  tale che  $h([1]_n) = [p \cdot q]_n$  e verificare che si ha  $h = f \circ g$ .

**Nota 567** Nel primo capitolo abbiamo dato un teorema di decomposizione per una funzione tra insiemi.

Data una funzione  $f : A \longrightarrow B$  abbiamo decomposto la funzione  $f$  nel modo seguente:

$$f = i \circ g \circ \pi$$

dove: la funzione  $\pi : A \longrightarrow A/\sim$  è la funzione surgettiva definita da:

$$\pi(a) = [a]_{\sim}$$

(avendo posto  $a \sim a' \iff f(a) = f(a')$ );

la funzione  $g : A/\sim \longrightarrow B' = \text{Im}(A)$  è la funzione biunivoca definita da:

$$g([a]_{\sim}) = f(a)$$

la funzione  $i : B' \longrightarrow B$  è la funzione iniettiva definita da:

$$i(b') = b'$$

**Teorema 568** [Teorema dell'omomorfismo tra gruppi]

Dato un omomorfismo tra gruppi:

$$f : (A, \cdot) \longrightarrow (B, \cdot)$$

si ha che:

1) La relazione di equivalenza in  $A$  definita da:

$$a \sim a' \iff f(a) = f(a')$$

è compatibile con l'operazione in  $A$ .

2)  $A/\sim = A/\ker f$

3)  $(A/\ker f, \cdot)$  è un gruppo, avendo posto:

$$(a \cdot \ker f) \cdot (a' \cdot \ker f) = (a \cdot a') \cdot \ker f$$

4) La funzione:

$$\pi : (A, \cdot) \longrightarrow (A/\ker f, \cdot)$$

definita da  $\pi(a) = a \cdot \ker f$  è un omomorfismo surgettivo tra gruppi.

5) La funzione:

$$g : (A/\ker f, \cdot) \longrightarrow (B' = \text{Im}(A), \cdot)$$

è un isomorfismo tra gruppi.

6) La funzione:

$$i : (B', \cdot) \longrightarrow (B, \cdot)$$

definita da  $i(b') = b'$  è un omomorfismo iniettivo tra gruppi.

7) Si ha infine:

$$f = i \circ g \circ \pi$$

**DIMOSTRAZIONE.** 1) Dimostriamo che la relazione  $\sim$  è compatibile con l'operazione di  $A$  (per la definizione di compatibilità vedere la definizione 435). Si

ha infatti:

$a \sim a', b \sim b' \implies f(a) = f(a'), f(b) = f(b')$ . Quindi, poiché  $f$  è un omomorfismo tra gruppi, si ha:

$$f(a \cdot b) = f(a) \cdot f(b) = f(a') \cdot f(b') = f(a' \cdot b')$$

da cui segue  $a \cdot b \sim a' \cdot b'$ .

2) e 3) Il teorema 538 ci dice che

$$a \sim a' \iff a \cdot \ker f = a' \cdot \ker f$$

Inoltre il teorema 538 ci dice che il nucleo è un sottogruppo normale. Possiamo considerare il gruppo quoziente  $(A/\ker f, \cdot)$  (vedere definizione 454). Da tutto ciò segue  $A/\sim = A/\ker f$ .

4), 5) e 6). Facili dimostrazioni. Lasciate per esercizio.  $\square$

**Esercizio 569** Applicare il teorema di omomorfismo all'omomorfismo tra gruppi:

$f : (Z, +) \longrightarrow (Z_8, +)$  definito da  $f(a) = [4a]_8$ .

**Esercizio 570** Dato il gruppo  $(Z_6, +)$  sia  $H$  il suo sottogruppo generato da  $[2]_6$ . Determinare il gruppo  $(Z_6/H, +)$  e dimostrare che esso è isomorfo al gruppo  $(Z_2, +)$

**Esercizio 571** Dato il gruppo  $(Z_6, +)$  sia  $K$  il suo sottogruppo generato da  $[3]_6$ . Determinare il gruppo  $(Z_6/K, +)$  e dimostrare che esso è isomorfo al gruppo  $(Z_3, +)$

**Esercizio 572** Dato il gruppo  $(\sigma_3, \circ)$ , sia  $H$  il suo sottogruppo generato da

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

Sappiamo che  $H$  è un sottogruppo normale.

Dimostrare che i gruppi  $(\sigma_3/H, \circ)$  e  $(Z_2, +)$  sono isomorfi.

**Teorema 573** Sia  $(G, \cdot)$  un gruppo ciclico. Allora:

1) se  $G$  ha infiniti elementi, allora  $(G, \cdot)$  è isomorfo al gruppo  $(Z, +)$ ;

2) Se  $G$  ha  $n$  elementi, allora  $(G, \cdot)$  è isomorfo al gruppo  $(Z_n, +)$ .

DIMOSTRAZIONE. Lasciata per esercizio.

Suggerimento. Sia  $g$  un generatore di  $G$ . Applicare il teorema di omomorfismo all'omomorfismo tra gruppi

$$f : (Z, +) \longrightarrow (G, \cdot)$$

definito da:

$$f(p) = g^p \quad \square$$

**Esercizio 574** Si consideri il gruppo  $(Z_3^*, \cdot)$ . Determinare, se esiste, un gruppo  $(Z_n, +)$  isomorfo ad esso.

**Esercizio 575** Si consideri il gruppo  $(Z_5^*, \cdot)$ . Determinare, se esiste, un gruppo  $(Z_n, +)$  isomorfo ad esso.

**Esercizio 576** Si consideri il gruppo  $(Z_7^*, \cdot)$ . Determinare, se esiste, un gruppo  $(Z_n, +)$  isomorfo ad esso.

**Esercizio 577** Si consideri il gruppo  $(Z_{11}^*, \cdot)$ . Determinare, se esiste, un gruppo  $(Z_n, +)$  isomorfo ad esso.

**Esercizio 578** Si consideri il gruppo  $(Z_{13}^*, \cdot)$ . Determinare, se esiste, un gruppo  $(Z_n, +)$  isomorfo ad esso.

**Esercizio 579** Sia  $G$  un gruppo finito e sia  $f : (G, \cdot) \longrightarrow (G', \cdot)$  un omomorfismo tra gruppi.

Dimostrare che si ha:

$$|G| = |\ker f| \cdot |f(G)|$$

### 3.13 Bibliografia

1) **I.Cattaneo Gasparini** *Strutture algebriche, operatori lineari*, Veschi.

Il secondo capitolo, esclusi gli ultimi tre paragrafi, è dedicato allo studio dei gruppi.

2) **I.Cattaneo Gasparini, G.Selmi** *Esercizi di algebra lineare con applicazioni alle funzioni di matrici e ai sistemi differenziali*, Veschi.

I paragrafi 7 e 8 del primo capitolo contengono esercizi risolti su semigrupp e gruppi.

3) **P.Maroscia** *Problemi di geometria*, Masson editoriale Veschi.

Nel capitolo 2 vengono assegnati e svolti molti esercizi sulle proprietà dei numeri interi e sulle congruenze. Nel capitolo 3 sono assegnati e svolti molti esercizi sui gruppi.

4) **B.Scimemi** *Algebretta*, decibel editrice.

I paragrafi 6,7,8,9,10 sono dedicati alle proprietà dei numeri interi. Il paragrafo 11 alle congruenze.

5) **B.Scimemi** *Gruppi*, decibel editrice

Nel quarto paragrafo e in tutti i successivi sono trattati più o meno tutti gli argomenti da noi trattati in questo capitolo.

6) **L.Childs** *Algebra, un'introduzione concreta*, ETS

Libro di circa 350 pagine suddiviso in 49 capitoli.

I capitoli 3 e 4 sono dedicati alle proprietà dei numeri interi. I capitoli 6 e 7 sono dedicati alle congruenze. Il capitolo 11 è parzialmente dedicato ai gruppi.

7) **R. Procesi Ciampi, R.Rota** *Algebra moderna. Esercizi*, Veschi.

Il quarto capitolo è dedicato ad esercizi sui gruppi.

8) **L.Lombardo Radice** *Istituzioni di algebra astratta*, Feltrinelli.

I capitoli 3 e 4 sono dedicati alla teoria dei gruppi.

9) **I.N.Herstein** *Algebra*, Editori Riuniti.

Il secondo capitolo è dedicato alla teoria dei gruppi.

10) **S.Singh** *L'ultimo teorema di Fermat*, Rizzoli.

Un bel libro divulgativo che descrive la lunga storia del teorema creando una suspense da "giallo".