Soluzioni Esercizi

Soluzioni esercizi capitolo 1

Esercizio 1.1.

1. Valgono i seguenti fatti:

   - $\cdot$ **è commutativa.** $\forall x, y \in \mathbb{R} : x \cdot y = x + y + k = y + x + k = y \cdot x$, dove nella seconda uguaglianza abbiamo sfruttato che $+^{\mathbb{R}}$ è commutativa;
   - $\cdot$ **è associativa.** $\forall x, y, z \in \mathbb{R} : (x \cdot y) \cdot z = (x + y + k) \cdot z = (x + y + k) + z + k = x + (y + k + z) + k = x + y \cdot z + k = x \cdot (y \cdot z)$, dove nella terza uguaglianza abbiamo sfruttato che $+^{\mathbb{R}}$ è associativa;
   - $-k \in \mathbb{R}$ **è elemento neutro per** $\cdot$**.** $\forall x \in \mathbb{R} : x \cdot (-k) = x + (-k) + k = x$, dove abbiamo sfruttato che $-k$ è l'opposto di k rispetto a $+^{\mathbb{R}}$;
   - **Ogni elemento di** $\mathbb{R}$ **è invertibile rispetto a** $\cdot$**.** $\forall x \in \mathbb{R} : x \cdot (-(x + 2k)) = x + (-(x + 2k)) + k = -k$.

   Abbiamo così dimostrato che $(\mathbb{R}, \cdot, -k)$ è un **gruppo abeliano**;

2. Valgono i seguenti fatti:

   - $\cdot$ **è commutativa.** Immediato dalla commutatività di $+^{\mathbb{R}}$;
   - $\cdot$ **è associativa.** $\forall x, y, z \in \mathbb{R} : (x \cdot y) \cdot z = \sqrt{(x \cdot y)^2 + z^2} = \sqrt{(\sqrt{x^2 + y^2})^2 + z^2} = \sqrt{(x^2 + y^2) + z^2} = \sqrt{x^2 + (y^2 + z^2)} = \sqrt{x^2 + (y \cdot z)^2} = x \cdot (y \cdot z)$;
   - $\cdot$ **non ha elemento neutro.** Supponiamo per assurdo $y \in \mathbb{R}$ sia elemento neutro per $\cdot$, allora $\forall x \in \mathbb{R} : x \cdot y = x$, ossia $\forall x \in \mathbb{R} : \sqrt{x^2 + y^2} = x$, dalla quale deduciamo $\forall x \in \mathbb{R} : x^2 + y^2 = x^2$, e quindi $y = 0$. Ma, ad esempio, $(-3) \cdot 0 = \sqrt{(-3)^2 + 0^2} = \sqrt{3^2} = 3 \neq -3$, assurdo.

   Dunque $(\mathbb{R}, \cdot)$ è un **semigruppo abeliano** che **non** è un **monoide** nè un **gruppo**. Conseguentemente non ha senso domandarsi se in $\mathbb{R}$ esistano elementi invertibili rispetto a $\cdot$;

3. Valgono i seguenti fatti:

- $\cdot$ **è commutativa.** Immediato dalla commutatività di $+^{\mathbb{R}}$;
- $\cdot$ **non è associativa.** Consideriamo $x = 1,\ y = 0,\ z = -4$, allora

$$(x \cdot y) \cdot z = ||x + y| + z| = ||1 + 0| + (-4)| = 3;$$
$$x \cdot (y \cdot z) = |x + |y + z|| = |1 + |0 + (-4)|| = 5;$$

- $\cdot$ **non ammette elemento neutro.** Supponiamo per assurdo $y \in \mathbb{R}$ sia elemento neutro per $\cdot$, allora $\forall x \in \mathbb{R} : x = x \cdot y = |x + y| \geq 0$, assurdo.

Dunque $(\mathbb{R}, \cdot)$ **non** è nemmeno un **semigruppo**;

4. Valgono i seguenti fatti:

   - $\cdot$ **non è commutativa.** Consideriamo $x = 2,\ y = 3$, allora:

$$x \cdot y = 2 \cdot 3 = 2 - 3 = -1;$$
$$y \cdot x = 3 \cdot 2 = 3 - 2 = 1;$$

   - $\cdot$ **non è associativa.** Consideriamo $x = 1,\ y = 4,\ z = 3$, allora:

$$(x \cdot y) \cdot z = (x - y) - z = x - y - z = 1 - 2 - 3 = -4;$$
$$x \cdot (y \cdot z) = x - (y - z) = x - y + z = 1 - 2 + 3 = 2;$$

   - $\cdot$ **non ammette elemento neutro sinistro.** Supponiamo per assurdo $x \in \mathbb{R}$ sia elemento neutro sinistro per $\cdot$, allora $\forall y \in \mathbb{R} : y = x \cdot y = x - y$, ossia $\forall y \in \mathbb{R} : x = 2y$, assurdo;
   - 0 **è elemento neutro destro per** $\cdot$**.** Immediato dalla definizione di $\cdot$.

   Dunque $(\mathbb{R}, \cdot)$ **non** è un **semigruppo**, né un **monoide**, né un **gruppo**.

5. Valgono i seguenti fatti:

   - $\cdot$ **è commutativa.** Immediato dalla definizione di massimo;
   - $\cdot$ **è associativa.** Siano $x, y, z \in \mathbb{R}$ e definiamo

$$w_1 = max\{max\{x, y\}, z\}$$
$$w_2 = max\{x, max\{y, z\}\}$$

   Allora per definizione di massimo si ha

$$x \leq max\{x, y\} \leq max\{max\{x, y\}, z\} = w_1 \tag{86}$$

$$y \leq max\{x, y\} \leq max\{max\{x, y\}, z\} = w_1 \tag{87}$$

$$z \leq max\{max\{x,y\},z\} = w_1 \tag{88}$$

Dalle (87) ed (88), per definizione di massimo, deduciamo $max\{y,z\} \leq w_1$, quindi da quest'ultima e dalla (86) abbiamo

$$w_2 = max\{x, max\{y,z\}\} \leq w_1.$$

Simmetricamente deduciamo $w_1 \leq w_2$. Conseguentemente per antisimmetria di $\leq$ si ha $w_1 = w_2$, ossia, per arbitrarietà di $x,y,z \in \mathbb{R}$, $\cdot$ è associativa;

- **L'operazione non ammette elemento neutro.** Infatti, se $z \in \mathbb{R}$ fosse elemento neutro per $\cdot$ si avrebbe $\forall x \in \mathbb{R} : x = z \cdot x = max\{z,x\}$, ossia $\forall x \in \mathbb{R} : z \leq x$, assurdo in quanto $(\mathbb{R}, \leq)$ non ammette minimo.

Dunque $(\mathbb{R}, \cdot)$ è un **semigruppo abeliano** che **non è un monoide**, e, di conseguenza, non ha senso domandarsi se siano presenti in $\mathbb{R}$ elementi invertibili rispetto a $\cdot$;

6. Evidentemente $\cdot$ è associativa, commutativa, ammette 2 come elemento neutro e $\forall x \in \mathbb{R}^* : \frac{2}{x}$ è inverso di x. Dunque $(\mathbb{R}, \cdot, 2)$ è un **gruppo abeliano**;

7. Valgono i seguenti fatti:

   - $\cdot$ **è commutativa.** Immediato dalla commutatività di $+^{\mathbb{R}}$ e $\cdot^{\mathbb{R}}$;
   - $\cdot$ **è associativa.** $\forall x,y,z \in \mathbb{R} \setminus \{-1\}$:

$$(x \cdot y) \cdot z = (x + y + xy) \cdot z = x + y + xy + z + xz + yz + xyz =$$

$$= x + y + z + xy + xz + yz + xyz$$

   Osserviamo che quest'ultima espressione è invariante per permutazioni di $\{x,y,z\}$, quindi $x \cdot (y \cdot z) = (y \cdot z) \cdot x = (x \cdot y) \cdot z$;
   - 0 **è elemento neutro per** $\cdot$**.** Immediato dalla definizione di $\cdot$;
   - **Ogni elemento di** $\mathbb{R} \setminus \{1\}$ **è invertibile rispetto a** $\cdot$**.** $\forall x \in \mathbb{R} \setminus \{-1\}$: $x \cdot (\frac{-x}{x+1}) = x + \frac{(-x)}{x+1} + \frac{-x^2}{x+1} = \frac{x^2}{x+1} + \frac{-x^2}{x+1} = 0$

   Dunque $(\mathbb{R} \setminus \{-1\}, \cdot, 0)$ è un **gruppo abeliano**;

8. Valgono i seguenti fatti:

   - $\cdot$ **è commutativa.** Immediato dalla definizione di $\cdot$;

- $\cdot$ **non è associativa.** Consideriamo $x = y = \frac{1}{2}$ e $z = \frac{1}{4}$, allora:

$$x \cdot (y \cdot z) = x \cdot \left(\frac{y+z}{y+z+1}\right) \overset{y=\frac{1}{2},\, z=\frac{1}{4}}{=} x \cdot \left(\frac{\frac{1}{2}+\frac{1}{4}}{\frac{1}{2}+\frac{1}{4}+1}\right) \overset{x=\frac{1}{2}}{=} \frac{1}{2} \cdot \frac{3}{7} = \frac{\frac{1}{2}+\frac{3}{7}}{\frac{1}{2}+\frac{3}{7}+1} = \frac{13}{27};$$

$$(x \cdot y) \cdot z = \left(\frac{x+y}{x+y+1}\right) \overset{x=y=\frac{1}{2}}{=} \left(\frac{\frac{1}{2}+\frac{1}{2}}{\frac{1}{2}+\frac{1}{2}+1}\right) \cdot z \overset{z=\frac{1}{4}}{=} \frac{1}{2} \cdot \frac{1}{4} = \frac{\frac{1}{2}+\frac{1}{4}}{\frac{1}{2}+\frac{1}{4}+1} = \frac{\frac{3}{4}}{\frac{7}{4}} = \frac{3}{7};$$

- $\cdot$ **non ammette elemento neutro.** Infatti $\forall x, y \in (0,1)$:

$$\frac{x+y}{x+y+1} = x \cdot y = x \iff x+y = x^2+xy+x \iff y = \frac{x^2}{1-x}$$

Dunque, ad esempio, per $x = \frac{2}{3}$ si avrebbe $y = \frac{4}{3} \notin (0,1)$, il che implica che $\cdot$ non ammette alcun elemento neutro.

Dunque $((0,1), \cdot)$ **non** è un **semigruppo**, quindi a maggior ragione **non è nemmeno un monoide o un gruppo**.

Esercizio 1.2. Valgono i seguenti fatti:

- $\cdot$ **è associativa.** $\forall (q,m),\ (q',m'),\ (q'',m'') \in \mathbb{Q} \times \mathbb{Z}^*$:

(I) $[(q,m) \cdot (q',m')](q'',m'') = (q+mq', mm')(q'',m'') = ((q+mq')+(mm')q'', (mm')m'')$;

(II) $(q,m)[(q',m')(q'',m'')] = (q,m)(q'+m'q'', m'm) = (q+m(q'+m'q''), m(m'm''))$.

Dunque (I) e (II) sono coincidenti in quanto le operazioni su $\mathbb{Q}$ e $\mathbb{Z}^*$ sono associative e commutative;

- $(0,1)$ **è elemento neutro per** $\cdot$**.** $\forall (q,m),\ (q',m'),\ (q'',m'') \in \mathbb{Q} \times \mathbb{Z}^*$:

$$(q,m) \cdot (0,1) = (q+m0, m1) = (q,m);$$
$$(0,1)(q,m) = (0+1q, 1m) = (q,m).$$

Quindi $(\mathbb{Q} \times \mathbb{Z}^*, \cdot, (0,1))$ è un **monoide**.

Calcoliamo gli elementi invertibili di $\mathbb{Q} \times \mathbb{Z}^*$ rispetto a $\cdot$.
$\forall (q,m),\ (q',m') \in \mathbb{Q} \times \mathbb{Z}^* : (q+mq', mm') = (q,m)(q',m') = (0,1) \iff$

$$\iff \begin{cases} q + mq' = 0 \\ mm' = 1 \end{cases}$$

Dalla seconda uguaglianza, essendo $m, m' \in \mathbb{Z}^*$, ricaviamo $m = m' = 1$ oppure $m = m' = -1$; nel primo caso, dalla prima uguaglianza del sistema ricaviamo $q' = -q$, mentre nel secondo caso troviamo $q' = q$. Abbiamo quindi ottenuto che gli elementi di $\mathbb{Q} \times \mathbb{Z}^*$ aventi un inverso destro rispetto a $\cdot$ sono tutti e soli quelli della forma $(q, 1)$ [il cui inverso destro è $(-q, 1)$] e $(q, -1)$ [(il cui inverso destro è $(q, -1)$]. D'altra parte

$$(-q, 1)(q, 1) = (-q + 1 \cdot q, 1 \cdot 1) = (0, 1)$$

quindi

$$\mathcal{U}(\mathbf{G}) = \{(q, m) \in \mathbb{Q} \times \mathbb{Z}^* \mid m \in \{-1, 1\}\},$$

dalla quale deduciamo anche che $\mathbf{G}$ non è un gruppo (in quanto $\mathcal{U}(\mathbf{G}) \neq G$).

Infine, il monoide $\mathbf{G}$ non è commutativo. Ad esempio:

$$(2, 1) \cdot (1, 2) = (2 + 1 \cdot 1, 1 \cdot 2) = (3, 2);$$
$$(1, 2) \cdot (2, 1) = (1 + 2 \cdot 2, 2 \cdot 1) = (5, 2).$$

Esercizio 1.3. Valgono i seguenti fatti:

- $\cdot$ **è associativa.** $\forall (a, b), (a', b'), (a'', b'') \in \mathbb{Q}^* \times \mathbb{Q}$:

  (I) $[(a, b) \cdot (a', b')] \cdot (a'', b'') = \left(aa', ab' + \dfrac{b}{a'}\right) \cdot (a'', b'') = \left((aa')a'', (aa')b'' + \dfrac{ab' + \frac{b}{a'}}{a''}\right)$;

  (II) $(a, b)[(a', b')(a'', b'')] = (a, b)\left(a'a'', a'b'' + \dfrac{b'}{a''}\right) = \left(a(a'a''), a(a'b'' + \dfrac{b'}{a''}\right) + \dfrac{b}{a'a''} =$

  $$= \left(a(a'a''), a(a'b'') + \frac{ab' + \frac{b}{a'}}{a''}\right).$$

  Dunque (I) e (II) sono coincidenti in quanto le operazioni su $\mathbb{Q}^*$ e $\mathbb{Q}$ sono associative e commutative;

- $(1, 0)$ **è elemento neutro per** $\cdot$**.** $\forall a, b \in \mathbb{Q} * \times \mathbb{Q}$:

  $$(a, b)(1, 0) = \left(a1, a0 + \frac{b}{1}\right) = (a, b);$$
  $$(1, 0)(a, b) = \left(1a, 1b + \frac{0}{a}\right) = (a, b);$$

- **Ogni elemento di $\mathbb{Q}^* \times \mathbb{Q}$ è invertibile.** Mostriamo che $(\frac{1}{a}, -b)$ è l'inverso di $(a, b) \in \mathbb{Q}^* \times \mathbb{Q}$:

$$(a,b)\left(\frac{1}{a}, -b\right) = \left(a\frac{1}{a}, a(-b) + \frac{b}{\frac{1}{a}}\right) = (1,0)$$
$$\left(\frac{1}{a}, -b\right)(a,b) = \left(\frac{1}{a}a, \frac{1}{a}b + \frac{(-b)}{a}\right) = (1,0)$$

Abbiamo così dimostrato che $(\mathbb{Q}^* \times \mathbb{Q}, \cdot, (1,0))$ è un **gruppo**. Tale gruppo **non** è abeliano, ad esempio:

$$(2,1)(1,2) = \left(2 \cdot 1, 2 \cdot 2 + \frac{1}{1}\right) = (2,5);$$
$$(1,2)(2,1) = \left(1 \cdot 2, 1 \cdot 1 + \frac{2}{2}\right) = (2,2).$$

Esercizio 1.4. È immediato osservare che le applicazioni in 1, 2, 3 e 5 definiscono delle operazioni binarie sui rispettivi insiemi.

1. Valgono i seguenti fatti:

   - $\cdot$ **è commutativa.** Immediato dalla definizione di $\cdot$;
   - $\cdot$ **è associativa.** $\forall (x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R} \times \mathbb{R}^*$:

$$\text{(I) } ((x_1,y_1)\cdot(x_2,y_2))\cdot(x_3,y_3) = (x_1y_2 + y_1x_2, y_1y_2)\cdot(x_3,y_3) =$$
$$= ((x_1y_2 + y_1x_2)y_3 + (y_1y_2)x_3, (y_1y_2)y_3);$$
$$\text{(II) } (x_1,y_1)\cdot((x_2,y_2)\cdot(x_3,y_3)) = (x_1,y_1)(x_2y_3 + y_2x_3, y_2y_3) =$$
$$= (x_1(y_2y_3) + y_1(x_2y_3 + y_2x_3), y_1(y_2y_3)),$$

     e (I) e (II) sono coincidenti in quanto $\cdot^{\mathbb{R}}$ distribuisce su $+^{\mathbb{R}}$ e tali operazioni su $\mathbb{R}$ sono associative e commutative;
   - $(0,1)$ **è elemento neutro per** $\cdot$. $\forall (x,y) \in \mathbb{R} \times \mathbb{R}^* : (x,y)\cdot(0,1) = (x1 + y0, y1) = (x,y)$;
   - **Ogni elemento di $\mathbb{R} \times \mathbb{R}^*$ è invertibile rispetto a** $\cdot$. $\forall (x,y) \in \mathbb{R} \times \mathbb{R}^* : (x,y)\cdot\left(\frac{-x}{y^2}, \frac{1}{y^2}\right) = \left(\frac{x}{y} + y\left(\frac{-x}{y^2}\right), y\frac{1}{y}\right) = (0,1)$.

   Quindi $(\mathbb{R} \times \mathbb{R}^*, \cdot, (0,1))$ è un **gruppo abeliano**;

2. Valgono i seguenti fatti:

- $\cdot$ **è associativa.** $\forall (x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{R}^* \times \mathbb{R}$:

  (I) $((x_1, y_1) \cdot (x_2, y_2)) \cdot (x_3, y_3) = (x_1 x_2, y_1 x_2 + y_2)(x_3, y_3) = ((x_1 x_2)x_3, (y_1 x_2 + y_2)x_3 + y_3)$;

  (II) $(x_1, y_1) \cdot ((x_2, y_2) \cdot (x_3, y_3)) = (x_1, y_1) \cdot (x_2 x_3, y_2 x_3 + y_3) = (x_1(x_2 x_3), y_1(x_2 x_3) + y_2 x_3 + y_3)$,

  e (I) e (II) sono coincidenti in quanto $\cdot^{\mathbb{R}}$ e tali operazioni sono associative su $\mathbb{R}$;

- $(1, 0)$ **è elemento neutro per** $\cdot$**.** $\forall (x, y) \in \mathbb{R} \times \mathbb{R}^*$:

$$(x, y) \cdot (1, 0) = (x1, y1 + 0) = (x, y);$$

$$(1, 0) \cdot (x, y) = (1x, 0x + y) = (x, y);$$

- **Ogni elemento di** $\mathbb{R}^* \times \mathbb{R}$ **è invertibile rispetto a** $\cdot$**.** $\forall (x, y) \in \mathbb{R}^* \times \mathbb{R}$:

$$(x, y) \cdot \left(\frac{1}{x}, \frac{-y}{x}\right) = \left(x\frac{1}{x}, \frac{y}{x} - \frac{y}{x}\right) = (1, 0);$$

$$\left(\frac{1}{x}, \frac{-y}{x}\right) \cdot (x, y) = \left(\frac{1}{x}x, \frac{-y}{x}x + y\right) = (1, 0);$$

- $\cdot$ **non è commutativa.**

$$(1, 2) \cdot (3, 1) = (1 \cdot 3, 2 \cdot 3 + 1) = (3, 7);$$

$$(3, 1) \cdot (1, 2) = (3 \cdot 1, 1 \cdot 1 + 2) = (3, 5).$$

Quindi $(\mathbb{R}^* \times \mathbb{R}, \cdot, (1, 0))$ è un **gruppo non abeliano**;

3. L'elemento $(0, 1) \in \mathbb{R} \times \mathbb{R}$ non ammette inverso rispetto a $\cdot$. Infatti, supponiamo per assurdo $(x, y) \in \mathbb{R} \times \mathbb{R}$ sia inverso di $(0, 1)$ rispetto a $\cdot$, allora $(1, 0) = (x, y) \cdot (0, 1) = (x0, y0 + 1) = (0, 1)$, assurdo.

   Dunque $(\mathbb{R} \times \mathbb{R}, \cdot, (1, 0))$ **non è un gruppo**;

4. L'applicazione $\cdot$ non è un'operazione. Ad esempio:

$$(1, 1) \cdot (1, 1) = (0, 2) \notin \mathbb{R}^* \times \mathbb{R}^*$$

5. La struttura considerata è la ridotta moltiplicativa del campo $\mathbb{C}$, che **non è un gruppo** in quanto $(0, 0) \in \mathbb{R} \times \mathbb{R}$ non ammette inverso rispetto alla $\cdot$.

Esercizio 1.5. Chiaramente la parte complicata dell'esercizio è determinare le strutture di semigruppo su $\{a, b\}$, dunque ci limitiamo a svolgere questa, determinando poi tra queste quelle che sono anche strutture di gruppo.

Dare una struttura di semigruppo su $A = \{a, b\}$ equivale a dare un'operazione binaria $\cdot : A \times A \to A$ associativa, che a sua volta equivale a dare un'opportuna tavola di moltiplicazione su $\{a, b\}$.

Ricordiamo che ogni semigruppo finito ha almeno un elemento idempotente (cfr. Proposizione 1), dunque sulla diagonale della tavola moltiplicativa si deve presentare necessariamente una delle seguenti tre situazioni:

(1)

$\cdot$	a	b
a	a	
b		b

(2)

$\cdot$	a	b
a	a	
b		a

(3)

$\cdot$	a	b
a	b	
b		b

Cominciamo analizzando i casi (2) e (3). Sappiamo che $\cdot$ deve essere associativa, quindi in particolare devono valere le seguenti uguaglianze:

$$(a \cdot b) \cdot a = a \cdot (b \cdot a) \tag{89}$$

$$(b \cdot a) \cdot b = b \cdot (a \cdot b) \tag{90}$$

In (2) osserviamo che se $a \cdot b = b$, allora sostituendo in (90) si avrebbe $a = (b \cdot a) \cdot b$, che forza $b \cdot a = b$ (altrimenti $a = (b \cdot a) \cdot b = a \cdot b = b$, in contrasto con $a \neq b$). D'altra parte, se fosse $a \cdot b = a$, allora sostituendo in (90) si avrebbe $b \cdot a = (b \cdot a) \cdot b$, che forza $b \cdot a = a$ (altrimenti $b = b \cdot a = (b \cdot a) \cdot b = b \cdot b = a$, in contrasto con $a \neq b$). Dunque per il caso (2) abbiamo le due seguenti possibili strutture di semigruppo

$\cdot$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	a
b	a	a

Il (3) è simmetrico rispetto al caso (2), quindi le possibili strutture di semigruppo in tale caso sono

$\cdot$	a	b
a	b	a
b	a	b

$\cdot$	a	b
a	b	b
b	b	b

Nel caso (1) si nota facilmente che qualsiasi scelta si faccia per $a \cdot b$ e $b \cdot a$ in $\{a, b\}$ si ha che (89) e (90) sono soddisfatte, essendo a e b idempotenti, quindi le possibili strutture di semigruppo per tale caso sono

$\cdot$	a	b
a	a	a
b	a	b

$\cdot$	a	b
a	a	a
b	b	b

$\cdot$	a	b
a	a	b
b	a	b

$\cdot$	a	b
a	a	b
b	b	b

Complessivamente siamo quindi giunti alle seguenti otto potenziali strutture di semigruppo su $\{a, b\}$

(I)

$\cdot$	a	b
a	a	b
b	b	a

(II)

$\cdot$	a	b
a	a	a
b	a	a

(III)

$\cdot$	a	b
a	b	a
b	a	b

(IV)

$\cdot$	a	b
a	b	b
b	b	b

(V)

$\cdot$	a	b
a	a	a
b	a	b

(VI)

$\cdot$	a	b
a	a	a
b	b	b

(VII)

$\cdot$	a	b
a	a	b
b	a	b

(VIII)

$\cdot$	a	b
a	a	b
b	b	b

Verifichiamo che queste otto tavole moltiplicative effettivamente definiscono delle strutture di semigruppo su $\{a, b\}$, ossia verifichiamo che in tutti gli otto casi $\cdot$ è associativa.

Banalmente le operazioni in (II) e (IV) sono associative, mentre le operazioni in (VI) e (VII) sono, rispettivamente, $(x, y) \longmapsto x$ e $(x, y) \longmapsto y$ che sappiamo essere associative dall'Esempio 8. Inoltre notiamo che la tavola moltiplicativa di $(\mathbb{Z}_2, +, 0)$ è

$+$	0	1
0	0	1
1	1	0

quindi (I), (III) $\cong \mathbb{Z}_2$, per cui definiscono strutture di semigruppo. D'altra parte è facile rendersi conto che in (V) e (VIII), rispettivamente, moltiplicare a sinistra o a destra per a e moltiplicare a sinistra o a destra per b restituisce sempre, rispettivamente, a e b, quindi l'operazione è banalmente associativa, in quanto, rispettivamente, qualsiasi stringa in cui compare a restituisce a e qualsiasi stringa in cui compare b restituisce b, indipendentemente dall'ordine

in cui si svolgano le operazioni, mentre ovviamente in una stringa di simboli omogenea (ossia in cui compaiono solo a o solo b) l'ordine è irrilevante per idempotenza di a e b.

Infine, come già notato sopra, (I) e (III) sono gruppi; del resto ogni gruppo è un monoide cancellativo, quindi ammette uno e un solo idempotente (il suo elemento neutro), per cui (V), (VI), (VII) e (VIII) **non** sono gruppi, mentre (II) e (IV) non sono gruppi perché privi di elemento neutro.

Esercizio 1.6. No. È un fatto noto in teoria dei semigruppi che dato un semigruppo S ogni idempotente di S è contenuto in uno e un solo sottogruppo massimale di S, e tali sottogruppi massimali sono a due a due disgiunti. Quindi ogni monoide $\mathbf{M} = (M, \cdot, 1)$ che ammetta un idempotente diverso dall'elemento neutro $1_{\mathbf{M}}$ fornisce una risposta negativa alla domanda posta nell'esercizio. Ad esempio, possiamo considerare la tavola moltiplicativa (VIII) dell'Esercizio 1.6: $(\{a, b\}, \cdot, a)$ è un monoide, ma $(\{b\}, \cdot, b)$ è un monoide con $a \notin \{b\}$.

Esercizio 1.7.

1. Sia $x \in G$, allora osserviamo che $x \in S \iff x^{-1} \in S$, dal momento che $(x^{-1})^{-1} = x$. Possiamo quindi affermare l'esistenza di $X \subset S$ tale che $S = X \cup X^{-1}$, dove $X \cap X^{-1} = \emptyset$ per definizione di S e $|X| = |X^{-1}|$ per quanto appena visto (la corrispondenza biunivoca è data dalla $X \to X^{-1}$, $x \mapsto x^{-1}$). Di conseguenza $S = |X \cup X^{-1}| = |X| + |X^{-1}| = 2|X| \equiv_2 0$;

2. Essendo $\mathbf{G}$ un gruppo finito si ha $|G \setminus S| = |G| - |S| \equiv_2 |G|$, dove l'ultima relazione segue dal punto 1;

3. Supponiamo per assurdo $|G \setminus S| = 1$ (ossia l'unico elemento di $\mathbf{G}$ inverso di se stesso è $1_{\mathbf{G}}$), allora dal punto 2 abbiamo $|G| \equiv_2 |G \setminus S| \equiv_2 1$, ossia $|G|$ dispari, in contrasto con l'ipotesi che $\mathbf{G}$ abbia un numero pari di elementi.

Esercizio 1.8.

1. Siano $x, y, z \in \mathbb{Z}$ tali che $(x, y, z) \neq (0, 0, 0)$, allora

$$\begin{pmatrix} [1]_3 & [x]_3 & [y]_3 \\ [0]_3 & [1]_3 & [z]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} \cdot \begin{pmatrix} [1]_3 & [x]_3 & [y]_3 \\ [0]_3 & [1]_3 & [z]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} \cdot \begin{pmatrix} [1]_3 & [x]_3 & [y]_3 \\ [0]_3 & [1]_3 & [z]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} =$$
$$= \begin{pmatrix} [1]_3 & [2x]_3 & [2y + xz]_3 \\ [0]_3 & [1]_3 & [2z]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} \cdot \begin{pmatrix} [1]_3 & [x]_3 & [y]_3 \\ [0]_3 & [1]_3 & [z]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} =$$

$$= \begin{pmatrix} [1]_3 & [-x]_3 & [-y+xz]_3 \\ [0]_3 & [1]_3 & [-z]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} \neq \begin{pmatrix} [1]_3 & [0]_3 & [0]_3 \\ [0]_3 & [1]_3 & [0]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix};$$

Inoltre

$$\begin{pmatrix} [1]_3 & [-x]_3 & [-y+xz]_3 \\ [0]_3 & [1]_3 & [-z]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} \cdot \begin{pmatrix} [1]_3 & [x]_3 & [y]_3 \\ [0]_3 & [1]_3 & [z]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} =$$

$$= \begin{pmatrix} [1]_3 & [x-x]_3 & [y-xz+(-y+xz)]_3 \\ [0]_3 & [1]_3 & [z-z]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} = \begin{pmatrix} [1]_3 & [0]_3 & [0]_3 \\ [0]_3 & [1]_3 & [0]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix}.$$

Abbiamo così dimostrato che ogni elemento di **G** diverso dalla matrice identità ha ordine 3. Dimostriamo ora, esibendo un controesempio, che **G** non è abeliano.

$$\begin{pmatrix} [1]_3 & [1]_3 & [1]_3 \\ [0]_3 & [1]_3 & [0]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} \cdot \begin{pmatrix} [1]_3 & [0]_3 & [1]_3 \\ [0]_3 & [1]_3 & [1]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} = \begin{pmatrix} [1]_3 & [1]_3 & [0]_3 \\ [0]_3 & [1]_3 & [1]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix};$$

$$\begin{pmatrix} [1]_3 & [0]_3 & [1]_3 \\ [0]_3 & [1]_3 & [1]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} \cdot \begin{pmatrix} [1]_3 & [1]_3 & [1]_3 \\ [0]_3 & [1]_3 & [0]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix} = \begin{pmatrix} [1]_3 & [1]_3 & [2]_3 \\ [0]_3 & [1]_3 & [1]_3 \\ [0]_3 & [0]_3 & [1]_3 \end{pmatrix}.$$

2. Supponiamo **G** sia un gruppo nel quale nessun elemento abbia ordine 3 e valga

$$\forall x, y \in G : (xy)^3 = x^3y^3 \tag{91}$$

Vogliamo dimostrare che **G** è abeliano. Dividiamo la dimostrazione in passi.

(i) $\forall x, y \in G : [x, y]^3 = (xyx^{-1}y^{-1})^3 = ((xyx^{-1})y^{-1})^3 \overset{(91)}{=} (xyx^{-1})^3(y^{-1})^3 = (xyx^{-1})(xyx^{-1})(xyx^{-1})y^{-3} = xy^3x^{-1}y^{-3} = [x, y^3]$;

(ii) $\forall x, y \in G : xy^3x^{-1} = (xyx^{-1})^3 \overset{(91)}{=} x^3y^3x^{-3}$, per cui $\forall x, y \in G : x^2y^3 = y^3x^2$, ossia in **G** i cubi commutano con i quadrati, e dunque $\forall x, y \in G : [x^2, y]^3 \overset{\text{(i)}}{=} [x^2, y^3] = 1_{\mathbf{G}}$, dalla quale deduciamo $\forall x, y \in G : [x^2, y] = 1_{\mathbf{G}}$, in quanto per ipotesi in **G** non esistono elementi

aventi ordine 3 (si tenga conto del fatto che $[x^2, y]^3 = 1_{\mathbf{G}}$ se e solo se $o([x^2, y]) \mid 3$, quindi $[x^2, y]$ ha necessariamente ordine 1, ossia è l'elemento neutro). Abbiamo quindi mostrato che in $\mathbf{G}$ i quadrati commutano con ogni elemento;

(iii) $\forall x, y \in G : (yx)^2 = (yx)^3(yx)^{-1} \overset{(91)}{=} y^3x^3x^{-1}y^{-1} = y^3x^2y^{-1}$, ossia $\forall x, y \in G : yxyx = y^3x^2y^{-1}$, dalla quale deduciamo $\forall x, y \in G : (xy)^2 = y^2x^2$;

(iv) $\forall x, y \in G : (xy)^2 \overset{\text{(iii)}}{=} y^2x^2 \overset{\text{(ii)}}{=} x^2y^2$.

Conseguentemente per l'Osservazione 16 si ha che $\mathbf{G}$ è abeliano.

Esercizio 1.9. Vedere suggerimento.

Esercizio 1.10. Svolgiamo direttamente l'esercizio nella sua forma più generale, ossia il caso di $n \in \mathbb{N}_{\geq 2}$ uomini condannati a morte e cappelli di $k \in \mathbb{N}_{\geq 2}$ colori diversi. Dimostriamo che i condannati possono sempre escogitare una strategia che permetta ad almeno $n - 1$ di loro di salvarsi.

Siano $\mathbf{G} = (G, \cdot, 1_{\mathbf{G}})$ un qualsiasi gruppo di ordine k (ad esempio, $(\mathbb{Z}_k, +, [0]_k)$, $\mathcal{U} = \{u_1, \ldots, u_n\}$ l'insieme dei condannati, $\mathcal{C} = \{c_1, \ldots, c_k\}$ l'insieme dei colori dei cappelli ed $f : \mathcal{C} \to G$ una bigezione (ossia stiamo assegnando bigettivamente ad ogni colore un elemento del gruppo $\mathbf{G}$). Chiaramente il problema è simmetrico rispetto alla possibile disposizione in fila indiana degli uomini, quindi da ora in avanti, senza perdita di generalità, assumiamo che essi siano disposti (dal basso verso l'alto) secondo la sequenza $(u_1, \ldots, u_n)$. Sia $g : \mathcal{U} \to \mathcal{C}$ un'applicazione qualsiasi (ossia una possibile assegnazione di cappelli ai condannati). Chiaramente ogni siffatta g determina un elemento di $\mathbf{G}$, ossia l'elemento $x = f(g(u_2)) \cdot \ldots \cdot f(g(u_n))$, e tale elemento corrisponde al colore $f^{-1}(x)$. Osserviamo che se l'ultimo condannato della fila indiana, ossia il condannato u_1, trasmette tale numero, allora il condannato u_2 è certamente in grado di determinare il colore del proprio capello: infatti esso dapprima ritorna all'elemento $x = u_2 \cdot u_3 \cdot \ldots \cdot u_n$ tramite la f (si ricordi che questa è una bigezione), poi vedendo davanti a sé la sequenza $(g(u_3), \ldots, g(u_n))$ è in grado di calcolare l'inverso y del prodotto $f(g(u_3)) \cdot \ldots \cdot f(g(u_n))$, dunque determinare $f(g(u_2))$ "per differenza", ossia $f(g(u_2)) = x \cdot y$, e infine applicare la f^{-1} per determinare $g(u_2)$. Similmente il condannato u_3 sarà ora in grado di determinare il colore del proprio cappello, infatti esso determinerà l'elemento $f(x)$, poi vedendo davanti a sé la sequenza $(g(u_4), \ldots, g(u_n))$ e potendo calcolare $f(g(u_2))$ determinerà per differenza $f(g(u_3))$, e infine il colore del proprio cappello $g(u_3)$ applicando la f^{-1}. E così via.

Soluzioni esercizi capitolo 2

Esercizio 2.2. Ricordiamo che

$$D_n = \{1, r, r^2, \dots, r^{n-1}, s, r \circ s, r^2 \circ s, \dots, r^{n-1} \circ s\}$$

dove r è la rotazione in senso antiorario di angolo $\frac{2\pi}{n}$, mentre s è una qualsiasi riflessione in D_n. Chiaramente ogni riflessione ha ordine 2 indipendentemente da $n \geq 3$. Cerchiamo di capire quali rotazioni abbiano ordine 2. Osserviamo che la rotazione r ha ordine n, quindi $\forall k \in \{1, 2, \dots, n-1\} : r^{2k} = (r^k)^2 = 1 \iff n \mid 2k$, ma $2k < 2n$, dunque l'unica possibilità è $n = 2k$, che implica n pari e $k = \dfrac{n}{2}$.

Esercizio 2.5. Dimostriamo che se $\sigma = (a_1 \ \dots \ a_d)$ è un ciclo di S_n, allora $\forall f \in S_n : f \circ \sigma \circ f^{-1} = (f(a_1) \ \dots \ f(a_d))$.

Poniamo $\forall i \in \{1, \dots, n\} : f(a_i) = b_i$, allora $\forall i \in \{1, \dots, n\} : a_i = f^{-1}(b_i)$. Dal momento che le permutazioni sono bigezioni ed $\{1, \dots, n\} = \{a_1, \dots, a_n\}$, si ha pure $\{b_1, \dots, b_n\} = \{1, \dots, n\}$. Dimostriamo che $\forall i \in \{1, \dots, n\} : (f \circ \sigma \circ f^{-1})(b_i) = (f(a_1) \ \dots \ f(a_d))(b_i) = (b_1 \ \dots \ b_d)(b_i)$. Distinguiamo tre casi:

(i) $i \in \{1, \dots, d-1\}$, allora $(b_1 \ \dots \ b_d)(b_i) = b_{i+1}$ e $(f \circ \sigma \circ f^{-1})(b_i) = (f \circ \sigma)(f^{-1}(b_i)) = f(\sigma(a_i)) = f(a_{i+1}) = b_{i+1}$;

(ii) $i = d$, allora $(b_1 \ \dots \ b_d)(b_i) = b_1$ e $(f \circ \sigma \circ f^{-1})(b_i) = (f \circ \sigma)(f^{-1}(b_i)) = f(\sigma(a_i)) = f(a_1) = b_1$;

(iii) $i \in \{d+1, \dots, n\}$, allora $b_i \notin f(\{a_1, \dots, a_d\})$, quindi $f^{-1}(b_i) \notin \{a_1, \dots, a_d\}$, per cui $\sigma(f^{-1}(b_i)) = f^{-1}(b_i)$, e conseguentemente $(f \circ \sigma \circ f^{-1})(b_i) = f(f^{-1}(b_i)) = b_i = (b_1 \ \dots \ b_d)(b_i)$.

Dunque se $\sigma_1 = (a_1 \ \dots \ a_d)$ e $\sigma_2 = (c_1 \ \dots \ c_d)$ sono cicli della stessa lunghezza è sufficiente considerare una permutazione $g \in S_n$ tale che $\forall i \in \{1, \dots, d\} : g^{-1}(a_i) = c_i$ e dedurre che, posto $f = g^{-1}$, si ha $f^{-1} \circ \sigma_1 \circ f = g \circ \sigma_1 \circ g^{-1} = (g(a_1) \ \dots \ g(a_d)) = (c_1 \ \dots c_d) = \sigma_2$, ossia quanto cercato.

Esercizio 2.6. Cominciamo osservando che possiamo limitarci a considerare $1 \leq k \leq l$. Infatti, per il *teorema della divisione euclidea* $\exists q, r \in \mathbb{N}$ tali che $k = qk + r$, dove $0 \leq r < k$, quindi

$$\sigma^k = \sigma^{qk+r} = (\sigma^k)^q \sigma^r = \sigma^r$$

Inoltre la tesi è ovviamente valida nel caso $k \in \{1, \ l\}$, quindi ci limitiamo a considerare $1 < k < l$. Dalla teoria (cfr. Proposizione 15), essendo $\sigma^k \neq id$

sappiamo che $supp(\sigma^k) = supp(\sigma)$, ossia le due permutazioni muovono gli stessi elementi. Supponiamo $\sigma = (a_1 \ \dots \ a_l)$. Per il *teorema fondamentale delle permutazioni* σ^k ammette una e una sola decomposizione $\sigma_1 \circ \dots \circ \sigma_t$ nel prodotto di cicli disgiunti, dove ovviamente $supp(\sigma_i)$ coincide con l'orbita di un suo qualsiasi elemento rispetto alla σ^k. Sia $i \in \{1, \dots, l\}$, allora gli elementi dell'orbita di a_i rispetto a σ^k hanno la forma $a_{mk+i \ (mod\ l)}$ con $m \in \mathbb{N}$. Osserviamo che $\forall u, v \in \mathbb{N} : uk + i \equiv_l vk + i \iff (u - v)k \equiv_l 0$, per cui il più piccolo $u - v$ positivo che realizza l'uguaglianza è $\frac{l}{(l,k)}$. Segue che gli elementi di $\left\{ a_i, a_{k+i}, a_{2k+i}, \dots, a_{\left(\frac{l}{(l,k)}-1\right)k+i} \right\}$ sono distinti e costituiscono l'orbita di a_i, ossia il supporto del ciclo fattore che lo muove. Conseguentemente $\forall j \in \{1, \dots, t\}$:

$$l(\sigma_j) = o(\sigma_j) = \frac{l}{(l,k)}$$

Esercizio 2.7. Per quanto visto nell'esercizio precedente, se un ciclo σ di lunghezza l e $k \in \mathbb{N}^+$ realizzano $\sigma^k = \sigma_1 \circ \dots \circ \sigma_t$, con $\sigma_1, \dots, \sigma_t$ cicli disgiunti, allora necessariamente $t = (l, k)$. Nello specifico $k = t$ realizza tale condizione $(l = mt \Rightarrow t \mid l)$. Supponiamo

$$\begin{aligned} \sigma_1 &= (a_{11} \ a_{12} \ \dots \ a_{1m}) \\ \sigma_2 &= (a_{21} \ a_{22} \ \dots \ a_{2m}) \\ &\dots \\ \sigma_t &= (a_{t_1} \ a_{t2} \ \dots \ a_{tm}) \end{aligned}$$

e consideriamo il seguente ciclo $\sigma = (a_{11} \, a_{21} \dots a_{t1} \, a_{12} \, a_{22} \ \dots \ a_{t2} \dots \ a_{1m} \, a_{2m} \dots \ a_{tm})$. Per verifica diretta si ha che $\sigma^k = \sigma_1 \circ \dots \circ \sigma_t$.

Esercizio 2.8. Osserviamo che se τ è una trasposizione qualsiasi di S_n, allora l'applicazione $F : A_n \to \{\eta \in S_n \mid sign(\eta) = -1\}$, $f \mapsto f \circ \tau$ è bigettiva, dal momento che è una involuzione (ossia è inversa di se stessa). In particolare, quindi

$$S_n = A_n \cup \{\eta \in S_n \mid sign(\eta) = -1\} = A_n \cup (A_n \circ \tau)$$

per cui $S_n \subseteq \langle A_n, \tau \rangle \subseteq S_n$, e dunque $S_n = \langle A_n, \tau \rangle$.

Esercizio 2.9. Se σ^2 è un ciclo, allora, essendo $supp(\sigma^2) = supp(\sigma)$, si ha $\frac{o(\sigma)}{(2, o(\sigma))} = o(\sigma^2) = o(\sigma)$, quindi $(2, o(\sigma)) = 1$, ossia l è dispari. Il viceversa e i restanti punti sono immediati dall'*Esercizio 2.6*.

Soluzioni esercizi capitolo 3

Esercizio 3.1.

1. H è un sottogruppo di **G**, infatti $\forall a_1, a_2 \in \mathbb{Q}^+ : ln(a_1) - ln(a_2) = ln\left(\frac{a_1}{a_2}\right) \in H$;
2. H **non** è un sottogruppo di **G**, infatti $\forall n_1, n_2 \in \mathbb{N}^+ : ln(n_1) - ln(n_2) = ln\left(\frac{n_1}{n_2}\right)$, il quale non è necessariamente un elemento di H. Infatti, ad esempio, per ogni $\frac{n_1}{n_2} \in \mathbb{Q} \setminus \mathbb{N}$ si ha $\frac{n_1}{n_2} \notin H$, dal momento che $ln : \mathbb{R}^+ \to \mathbb{R}$ è una bigezione, quindi $\forall x \in \mathbb{R}, \exists! y \in \mathbb{R}^+ : x = ln(y)$;
3. H **non** è un sottogruppo di **G**. Infatti osserviamo che $tan(\pi/4) = 1$, dunque $\pi/4 \in H$, ma $\pi/4 + \pi/4 = \pi/2 \notin H$, dal momento che la tangente non è nemmeno definita per $\pi/2$.
4. H è un sottogruppo di **G**, infatti: $\forall m_1, n_1, m_2, n_2 \in \mathbb{Z} : (2^{m_1}3^{n_1})(2^{m_2}3^{n_2})^{-1} = 2^{m_1}3^{n_1}2^{-m_2}3^{-n_2} = 2^{m_1-m_2}3^{n_1-n_2} \in H$;
5. H è un sottogruppo di **G**, infatti $\forall (x_1, y_1), (x_2, y_2) \in G : y_1 = 2x_1,\ y_2 = 2x_2 \Rightarrow y_1 - y_2 = 2x_1 - 2x_2 = 2(x_1 - x_2)$, ossia $(x_1, y_1) - (x_2, y_2) = (x_1 - x_2, y_1 - y_2) \in H$.

Esercizio 3.3. Sia X un insieme, vogliamo dimostrare che $(\mathcal{P}(X), \triangle, \emptyset)$ è un gruppo abeliano.

- $\triangle$ **è commutativa.** Immediato dalla definizione della differenza simmetrica;
- $\triangle$ **è associativa.** Siano $\forall A, B, C \in \mathcal{P}(X)$ e denotiamo con A', B', C' i loro complementari in X, allora:

$$(A \triangle B) \triangle C = ((A \setminus B) \cup (B \setminus A)) \triangle C =$$
$$= [(((A \setminus B) \cup (B \setminus A))) \setminus C] \cup [C \setminus ((A \setminus B) \cup (B \setminus A))] =$$
$$= [((B' \cap A) \cup (A' \cap B)) \cap C'] \cup [C \cap ((B' \cap A) \cup (A' \cap B))'] =$$
$$= [((B' \cap A) \cup (A' \cap B)) \cap C'] \cup [C \cap ((B \cup A') \cap (A \cup B'))] =$$
$$= [((B' \cap A) \cup (A' \cap B)) \cap C'] \cup [C \cap ((B \cap A) \cup (A' \cap B'))] =$$
$$= ((A \cap B' \cap C') \cup (A' \cap B \cap C')) \cup (A \cap B \cap C) \cup (A' \cap B' \cap C') =$$

$$= (A \cap B \cap C) \cup (A \cap B' \cap C') \cup (A' \cap B \cap C') \cup (A' \cap B' \cap C).$$

Osserviamo ora che l'espressione ottenuta è invariante per permutazioni dell'insieme $\{A, B, C\}$, dunque $(A \triangle B) \triangle C = (B \triangle C) \triangle A = A \triangle (B \triangle C)$, dove nella seconda uguaglianza abbiamo sfruttato la commutatività di $\triangle$. Dall'arbitrarietà di $A, B, C \in \mathcal{P}(X)$ otteniamo che $\triangle$ è associativa;

- $\emptyset$ **è elemento neutro per** $\triangle$**.** Immediato dalla definizione di $\triangle$;
- **Ogni elemento di** $\mathcal{P}(X)$ **è invertibile rispetto a** $\triangle$**.** Si osserva immediatamente che $\forall A \in \mathcal{P}(X) : A \triangle A = \emptyset$.

È così dimostrato che $(\mathcal{P}(X), \triangle, \emptyset)$ è un gruppo abeliano.

Sia $Y \in \mathcal{P}(X)$, allora $\mathcal{P}(Y) \subseteq \mathcal{P}(X)$, dunque $\forall A, B \in \mathcal{P}(Y) : A \triangle B \in \mathcal{P}(X)$, e ovviamente $\emptyset \in \mathcal{P}(Y)$, quindi $(\mathcal{P}(Y), \triangle, \emptyset) \leq (\mathcal{P}(X), \triangle, \emptyset)$.

Esercizio 3.7. Abbiamo già mostrato nell'*Esercizio 2.2* che D_n ha esattamente n elementi di ordine 2 se e solo se n è dispari. Abbiamo anche visto che tali elementi di ordine 2 sono le simmetrie, dunque gli n elementi che non hanno ordine 2 sono le rotazioni, e chiaramente la composizione di rotazioni è ancora una rotazione.

Esercizio 3.8.

1. S_X è finito in quanto per ipotesi X è finito, dunque anche $H \subseteq S_X$ è necessariamente finito, quindi per verificare che si tratta di un sottogruppo di S_X è sufficiente verificarne la stabilità rispetto alla composizione. $\forall f, g \in H, \forall x \in A : (f \circ g)(x) = f(g(x)) \in A$, dal momento che essendo $f, g \in H$ si ha $x \in A \Rightarrow g(x) \in A \Rightarrow f(g(x)) \in A$;
2. Consideriamo $X = \mathbb{R}$ ed $A = \mathbb{N}$. Allora la funzione

$$\begin{aligned} s : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x + 1 \end{aligned}$$

è un elemento di H, ma la sua inversa

$$\begin{aligned} s^{-1} : \mathbb{R} &\to \mathbb{R} \\ x &\mapsto x - 1 \end{aligned}$$

non è un elemento di H, dal momento che $s^{-1}(0) = -1 \notin \mathbb{N}$.

Esercizio 3.9.

1. Sia $f \in S_n \setminus \{id\}$, allora sappiamo dalla teoria (cfr. Lemma 2) che f può essere scritta come prodotto di $N(f)$ trasposizioni. D'altra parte l'identità id può essere scritta come prodotto di una trasposizione qualsiasi con se stessa, quindi si ha quanto cercato;

2. È sufficiente dimostrare che riusciamo a generare la permutazione identità ed ogni trasposizione, poi la tesi seguirà nel caso generale dal punto precedente. Chiaramente $id = (1\ 2)(1\ 2)$. Ricordiamo che (cfr. *Esercizio 2.5*) $\forall f \in S_n$, $\forall (a_1\ \dots\ a_d) \in S_n : f \circ (a_1\ \dots\ a_d) \circ f^{-1} = (f(a_1)\ \dots\ f(a_d))$, per cui $\forall i, j \in \{1, \dots, n\} \setminus \{1\}$ (se uno tra i e j fosse 1 non ci sarebbe niente da dimostrare), $i < j$:

$$(i\ j) = (i\ 1)(1\ j)(1\ i)$$

3. Preliminarmente osserviamo che $id \in A_n$ è prodotto di tre cicli, dal momento che $id = (1\ 2\ 3)(1\ 2\ 3)(1\ 2\ 3)$. Sia ora $f \in A_n \setminus \{id\}$, allora esistono $\tau_1, \tau_2, \dots, \tau_{2k-1}, \tau_{2k}$ trasposizioni tali che $f = \tau_1\tau_2 \dots \tau_{2k-1}\tau_{2k}$, dal momento che $N(f) \equiv_2 0$. Per ottenere la tesi è sufficiente mostrare che il prodotto di due trasposizioni può essere espresso come prodotto di 3-cicli. Siano $(a\ b), (c\ d) \in S_n$ due trasposizioni. Distinguiamo tre casi:

   (i) $|\{a, b\} \cap \{c, d\}| = 2$, quindi necessariamente $\{a, b\} = \{c, d\}$, e dunque $(a\ b) = (c\ d)$, per cui $(a\ b)(c\ d) = (a\ b)(a\ b) = id$, che abbiamo già visto potersi esprimere come prodotto di 3-cicli;

   (ii) $|\{a, b\} \cap \{c, d\}| = 1$. Senza perdita di generalità supponiamo $b = c$, allora $(a\ b)(c\ d) = (a\ b)(b\ d) = (a\ b\ d)$;

   (iii) $|\{a, b\} \cap \{c, d\}| = 0$, allora $(a\ b)(c\ d) = (a\ b)(b\ c)(b\ c)(c\ d) = (a\ b\ c)(b\ c\ d)$.

4. Per quanto visto nel punto precedente ogni $f \in A_n$ è prodotto di 3-cicli, quindi è sufficiente mostrare che ogni 3-ciclo è generato da $\{(1\,2\,3), (1\,2\,4), \dots, (1\,2\,n)\}$. Siano $i, j, k \in \{1, \dots, n\} \setminus \{1, 2\}$, a due a due distinti, allora $(1\,2\,k)(1\,2\,i)(1\,2\,k)^{-1} = (2\,k\,i) = (i\,2\,k)$ e $(1\,2\,j)(i\,2\,k)(1\,2\,j)^{-1} = (i\,j\,k)$, per cui

   $$(i\,j\,k) = (1\,2\,j)(1\,2\,k)(1\,2\,i)(1\,2\,k)^{-1}(1\,2\,j)^{-1}$$

   D'altra parte, se uno e uno solo tra i, j, k sta in $\{1, 2\}$, che senza perdita di generalità possiamo assumere sia i, dato che alla peggio possiamo rinominarli, allora $(1\,2\,k)(1\,2\,j)(1\,2\,k)^{-1} = (2\,k\,j)$ e $(1\,2\,j)(2\,k\,j)(1\,2\,j)^{-1} = (j\,k\,1) = (1\,j\,k)$, per cui

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

Infine, supponiamo esattamente due tra i, j, k siano in $\{1, 2\}$. A meno di riordinare e rinominare gli indici si presentano esattamente due casi. Se $i = 1,\ j = 2$ non abbiamo niente da dimostrare, mentre se $i = 1,\ k = 2$, allora $(i\ j\ k) = (1\ j\ 2) = (j\ 2\ 1) = (1\ 2\ j)^{-1}$.

5. Abbiamo visto in (2) che S_n è generato da $\{(1\ 2), (1\ 3), \ldots, (1\ n)\}$, quindi è sufficiente verificare che tale insieme è generato da $\{(1\ 2), (1\ 2\ \ldots\ n)\}$. Mostriamolo procedendo per induzione su $n \in \mathbb{N}_{\geq 3}$.

   Passo base $(n = 3)$: Chiaramente

   $$(1\ 3) = (1\ 2)(1\ 2\ \ldots\ n)(1\ 2)(1\ 2\ \ldots\ n)^{-1}(1\ 2)$$

   Passo induttivo: Supponiamo la tesi vera per $n - 1 \in \mathbb{N}_{\geq 3}$. Allora

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

   dalla quale segue la tesi essendo, per ipotesi induttiva, $(1\ n-1)$ generato da $\{(1\ 2), (1\ 2\ \ldots\ n)\}$.

Esercizio 3.10. Per il *Teorema di Lagrange* si ha $|G| = [G : K]|K|$, ma applicando nuovamente il *Teorema di Lagrange* si ha anche $|K| = [K : H]|H|$, per cui $[G : H]|H| = |G| = [G : K][K : H]|H|$, e dunque $[G : H] = [G : K][K : H]$.

Soluzioni esercizi capitolo 4

Esercizio 4.3. Dalla teoria sappiamo che

$$Z(GL_n(\mathbb{Z}_p)) = \{aI_n \mid a \in \mathbb{Z}_p^*\}$$

Quindi $|Z(GL_n(\mathbb{Z}_p))| = p - 1$. Per quanto riguarda la seconda parte dell'esercizio, invece, considerato un qualsiasi campo $\mathbb{K}$ e $k \in \mathbb{K}^*$, e fissata una matrice $B \in GL_n(\mathbb{K})$ tale che $det(B) = k$ (essa esiste, infatti basta considerare la matrice diagonale $B = diag(k, 1, \ldots, 1)$), consideriamo l'applicazione $SL_n(\mathbb{K}) \to \{C \in GL_n(\mathbb{K}) \mid det(C) = k\},\ A \mapsto AB$, che chiaramente è invertibile con inversa data dalla $\{C \in GL_n(\mathbb{K})\} \to SL_n(\mathbb{K}),\ A \mapsto CB^{-1}$ (si osservi che entrambe le applicazioni sono ben definite in virtù del *Teorema di Binet*). Conseguentemente, essendo $det : GL_n(\mathbb{Z}_p) \to \{1, 2, \ldots, p-1\}$ suriettiva, concludiamo $|SL_n(\mathbb{Z}_p)| = \dfrac{|GL_n(\mathbb{Z}_p)|}{p-1}$.

Esercizio 4.4. Consideriamo $K = \langle H, x\rangle$, allora $H \leq K \leq G$, per cui per l'*Esercizio 3.10* si ha $p = [G : H] = [G : K][K : H]$. Essendo p un primo, deduciamo che uno dei due fattori è p e l'altro 1. Ma $[K : H] > 1$ (dal momento che $x \in K$, $x \notin H$, dunque $xH = H$), quindi $[G : K] = 1$, per cui $K = G$. Dunque la tesi diventa $H \trianglelefteq < H, x >$. Ricordiamo che un elemento di $\langle H, x\rangle$ ha la forma $g_1^{\alpha_1} \cdot \ldots \cdot g_n^{\alpha_n}$, dove $n \in \mathbb{N}^+$, $\{g_1, \ldots, g_n\} \subseteq H \cup \{x\}$, $\alpha_1, \ldots, \alpha_n \in \mathbb{Z}$. Mostriamo la tesi procedendo per induzione su n e sfruttando il primo criterio di normalità.

Passo base (n=1): Se $g_1 \in H$, allora ovviamente $H^{g_1^{\alpha_1}} \leq H$, mentre se $g_1 = x$ ciò segue dall'ipotesi $xH = Hx$;

Passo induttivo: Supponiamo la tesi valida per un certo $n \in \mathbb{N}^+$, allora

$$(g_1^{\alpha_1} \cdot \ldots \cdot g_n^{\alpha_n} \cdot g_{n+1}^{\alpha_{n+1}})^{-1} H (g_1^{\alpha_1} \cdot \ldots \cdot g_n^{\alpha_n} \cdot g_{n+1}^{\alpha_{n+1}}) = g_{n+1}^{-\alpha_{n+1}} (g_1^{\alpha_1} \cdot \ldots \cdot g_n^{\alpha_n})^{-1} H (g_1^{\alpha_1} \cdot \ldots \cdot g_n^{\alpha_n}) g_{n+1}^{\alpha_{n+1}} \leq$$

$$\leq g_{n+1}^{-\alpha_{n+1}} H g_{n+1}^{\alpha_{n+1}} \leq H,$$

dove il primo $\leq$ è conseguenza dell'ipotesi induttiva, mentre il secondo segue dal passo base.

Esercizio 4.5. Cominciamo dimostrando che $H \trianglelefteq \mathbf{G}$. Supponiamo per assurdo esista $s \in G$ tale che $o(s) = 2$ con $H^s \not\leq H$, ossia esiste $h \in H \setminus \{1\}$ tale che $o(shs) = 2$, quindi $sh^2s = (shs)(shs) = 1$, per cui $h^2 = 1$, in contrasto con l'ipotesi $h \in H \setminus \{1\}$.

Passiamo all'abelianità. Osserviamo che $\forall s \in G \setminus H, \forall h \in H : o(sh) = 2$, dal momento che $sh \notin H$ (in caso contrario si avrebbe $sh \notin H$, assurdo). Quindi $\forall s \in G \setminus H, \forall h \in H : shsh = 1 \Rightarrow shs = h^{-1}$. Dunque $\forall h_1, h_2 \in H : [h_1, h_2] = h_1 h_2 h_1^{-1} h_2^{-1} = h_1 h_2 (sh_1 s)(sh_2 s) = h_1 h_2 s h_1 h_2 s = (h_1 h_2)(h_1 h_2)^{-1} = 1$. È così dimostrato che H è abeliano.

Infine $h \in H \Rightarrow h^{-1} \in H$, per cui $h = 1$ oppure $h \neq h^{-1}$ (altrimenti $o(h) = 2$, in contrasto con la definizione di H), quindi $n \equiv_2 1$, ossia $|H|$ dispari.

Esercizio 4.6. L'inclusione è ovvia dalle definizioni. Per quanto all'*Esercizio 4.8* si ha $Z(S_3) = \{id\}$, mentre $Z(A_3) = A_3 \neq \{id\}$ ($|A_3| = \frac{3!}{2}$, quindi $A_3 \cong \mathbb{Z}_3$, per cui A_3 abeliano).

Esercizio 4.7. Cominciamo trattando il caso i cui $o(xy) = n \in \mathbb{N}^+$. Se $o(xy) = 1$, allora $xy = 1 \Rightarrow y = x^{-1} \Rightarrow yx = x^{-1}x = 1 \Rightarrow o(xy) = 1 = o(yx) \Rightarrow o(yx) \mid o(xy)$. Ora supponiamo che $o(xy) = n + 1 \in \mathbb{N}^+$ per qualche $n \in \mathbb{N}$. Non è difficile osservare che $x(yx)^{n+1}y = (xy)^{n+2} = (xy)^{n+1}(xy) = xy$, per

cui $(yx)^{n+1} = 1 \Rightarrow o(yx) \mid n+1 = o(xy)$.

Simmetricamente $o(xy) \mid o(yx)$, quindi $o(xy) = o(yx)$.
Chiaramente, per quanto appena mostrato, i due ordini coincidono anche se $o(xy)$ non è finito.

Per quanto riguarda la seconda parte dell'esercizio, $\forall y \in G : o(yxy^{-1}) = o(xy^{-1}y) = o(x) = k$, quindi, essendo per ipotesi x l'unico elemento di G avente ordine k, $yxy^{-1} = x \Rightarrow yx = xy$, e dunque $x \in Z(\mathbf{G})$.

Esercizio 4.8. Sia $f \in Z(S_n)$, allora, in particolare, per definizione si ha che f e $(1\,2\,\ldots\,n)$ commutano. Ma allora $id = [f, (1\,2\,\ldots\,n)] = f(1\,2\,\ldots\,n)f^{-1}(1\,2\,\ldots\,n)^{-1} = (f(1)\,f(2)\,\ldots\,f(n))(1\,2\,\ldots\,n)^{-1}$, per cui

$$(f(1)\,f(2)\,f(3)\,\ldots\,f(n)) = (1\,2\,3\,\ldots\,n) \tag{92}$$

D'altra parte anche f e $(1\ 2)$ devono commutare, per cui procedendo similmente si ottiene

$$(f(1)\,f(2)) = (1\,2) \tag{93}$$

Dalla (93) deduciamo che $f(1) = 1$ e $f(2) = 2$ oppure $f(1) = 2$ e $f(2) = 1$; ma nel secondo caso dalla (92) si otterrebbe $1 = f(2) = 3$, assurdo. Dunque $f(1) = 1$, $f(2) = 2$ e dalla (92) deduciamo $f = id$.

Esercizio 4.9. Sia $f \in Z(A_n)$, allora per ogni $i \in \{3, \ldots, n\}$ si ha che f e $(1\ 2\ i)$ commutano. Procedendo come nell'esercizio precedente deduciamo che $\forall i \in \{3, \ldots, n\}$:

$$(f(1)\,f(2)\,f(i)) = (1\,2\,i)$$

Ma chiaramente ciò è possibile se e solo se $f = id$.

Esercizio 4.10. Ricordiamo che se $r = r_{\frac{2\pi}{n}}$ e $s \in D_n$ è una qualunque riflessione, allora

$$D_n = \{id, r, r^2, \ldots, r^{n-1}, s, s \circ r, \ldots, s \circ r^{n-1}\}$$

Cominciamo osservando che nessuna riflessione s può stare nel centro $Z(D_n)$. Infatti se $s \in D_n$, allora $rs = sr \Rightarrow r^{-1} = srs = r \Rightarrow r^2 = id$, in contrasto con il fatto che $o(r) = n \geq 3$. Sia ora $k \in \{0, 1, \ldots, n-1\}$, allora se $r^k \in Z(D_n)$ si deve avere in particolare $sr^k = r^k s = s(sr^k s) = sr^{-k} \Rightarrow r^{2k} = id$, dalla quale deduciamo che $o(r) = n \mid 2k < 2n$, dunque $n = 2k$. Infine osserviamo che

se $k = \frac{n}{2}$, allora per ogni riflessione s si ha $sr^{\frac{n}{2}}s = r^{-\frac{n}{2}} = r^{\frac{n}{2}}$, ossia $r^{\frac{n}{2}}s = sr^{\frac{n}{2}}$. Quindi se n è dispari il centro è banale, mentre se n è pari il centro è $\{id, r^{\frac{n}{2}}\}$.

Soluzioni esercizi capitolo 5

Esercizio 5.1. $\forall x, y \in \mathbb{R}^* : f(x)f(y) = f(x) + f(y) + f(x)f(y) = (x-1) + (y-1) + (x-1)(y-1) = (x-1)y + y - 1 = xy - 1 = f(xy)$. D'altra parte f è chiaramente bigettiva (la sua inversa è la $G \to \mathbb{R}^*,\ x \mapsto x+1$, ben definita in quanto $-1 \notin G$). È così dimostrato che f è un isomorfismo $\mathbb{R}^* \to \mathbf{G}$.

Esercizio 5.2.

1. Consideriamo l'applicazione $f : \mathbb{R} \to S^1,\ x \mapsto e^{i2\pi x}$. Dalle proprietà delle potenze si ha che f è un omomorfismo, inoltre $ker(f) = \{x \in \mathbb{R} \mid f(x) = (1,0)\} = \{x \in \mathbb{R} \mid (cos(2\pi x), sin(2\pi x)) = (1,0)\} = \mathbb{Z}$, dove l'ultima uguaglianza segue dal fatto che $cos(2\pi x) = 1$ e $sin(2\pi x) = 0$ se e solo se $2\pi x = 2\pi k$ per qualche $k \in \mathbb{Z}$, ossia $x = k \in \mathbb{Z}$. Infine, osserviamo che f è suriettiva per definizione di S^1, quindi per il *primo teorema di isomorfismo* si ha $\mathbb{R}/\mathbb{Z} = \mathbb{R}/ker(f) \cong S^1$.

2. Consideriamo l'applicazione $g : \mathbb{Z} \to S^1,\ z \mapsto e^{i(\frac{2\pi}{n})z}$. Dalle proprietà delle potenze si ha che g è un omomorfismo il cui nucleo è $ker(g) = \{z \in \mathbb{Z} \mid e^{i(\frac{2\pi}{n})z} = 1\} = n\mathbb{Z}$ e la cui immagine è U_n (da ciò segue anche che U_n è un sottogruppo di S^1), quindi per il *primo teorema di isomorfismo* si ha $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/ker(f) \cong U_n$.

3. Dimostriamo più in generale che se $\mathbf{G}$ è un gruppo di ordine $2n$ che ammette un elemento g_1 di ordine 2 ed un elemento g_2 di ordine n tali che $g_1 g_2 g_1 = g_2^{-1}$, allora $\mathbf{G} \cong D_n$. Non è difficile vedere, sfruttando le ipotesi, che $G = \{1, g_2, g_2^2, \ldots, g_2^{n-1}, g_1, g_1 g_2 \ldots, g_1 g_2^{n-1}\}$. Consideriamo l'applicazione $f : D_n \to G$ definita tramite la $\forall k \in \{0,1,\ldots,n-1\},\ \forall j \in \{0,1\} :\ f(s^j r^k) = g_1^j g_2^k$. Evidentemente f è una bigezione per costruzione, quindi non ci resta da mostrare altro se non che f è un omomorfismo di gruppi. Osserviamo che si presentano cinque casi:

   - $f(ss) = f(1) = 1 = g_1 g_1 = f(s)f(s)$;
   - $f(r^{k_1} r^{k_2}) = f(r^{k_1+k_2}) = g_2^{k_1+k_2} = g_2^{k_1} g_2^{k_2} = f(r^{k_1})f(r^{k_2})$;
   - $f((sr^k)s) = f(r^{-k}) = f(r^{n-k}) = g_2^{n-k} = g_2^{-k} = g_1 g_2^k g_1 = f(sr^k)f(s)$;
   - $f(s(sr^k)) = f(r^k) = g_2^k = g_1(g_1 g_2^k) = f(s)f(sr^k)$;
   - $f((sr^{k_1})(sr^{k_2})) = f((sr^{k_1}s)r^{k_2}) = f(r^{-k_1} r^{k_2}) = f(r^{k_2-k_1}) = g_2^{k_2-k_1} = g_2^{-k_1} g_2^{k_2} = (g_1 g_2^{k_1})(g_1 g_2^{k_2}) = f(sr^{k_1})f(sr^{k_2})$.

È così dimostrato che f definisce un isomorfismo.

Nel caso in esame dell'esercizio notiamo che $o(r) = n$, $o(s) = 2$ e $srs = r^{-1}$. Dico che $|\langle r, s\rangle| = 2n$. Infatti un elemento di tale sottogruppo generato ha la forma $r^k s^m$ oppure $s^m r^k$ per qualche $k \in \{0, 1, \ldots, n-1\}$ e $m \in \{0, 1\}$, ma osserviamo che (se $m = 1$ e $k \neq 0$) si ha $r^k s = ssr^k s = sr^{-k} = sr^{n-k}$, quindi possiamo assumere gli elementi siano tutti della forma $s^m r^k$ con $m \in \{0, 1\}$ e $k \in \{0, 1, \ldots, m-1\}$. Osserviamo ora che le ipotesi sugli ordini implicano che gli elementi dell'insieme $\{1, r, \ldots, r^{n-1}, s, sr, \ldots, sr^{n-1}\}$ sono tutti distinti (in particolare si osservi che non esiste alcun $k \in \{0, 1, \ldots, n-1\}$ tale che $s = r^k$, dal momento che se così fosse si avrebbe $1 = s(1) = r^k(1) = u^k$, in contrasto con $o(u) = n$), da cui segue quanto asserito sulla cardinalità del sottogruppo generato.

Esercizio 5.3.

1.

2. Cominciamo dimostrando che $SU(2)$ è un sottogruppo di $GL_2(\mathbb{C})$. Siano

$$A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$$

$$B = \begin{pmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{pmatrix}$$

Elementi di $SU(2)$, allora

$$A^{-1}B = \begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{pmatrix} = \begin{pmatrix} \overline{\alpha}\gamma + \beta\overline{\delta} & \overline{\alpha}\delta - \beta\overline{\gamma} \\ \overline{\beta}\gamma - \alpha\overline{\delta} & \overline{\beta}\delta + \alpha\overline{\gamma} \end{pmatrix} = \begin{pmatrix} \overline{\alpha}\gamma + \beta\overline{\delta} & \overline{\alpha}\delta - \beta\overline{\gamma} \\ -\overline{\overline{\alpha}\delta - \beta\overline{\gamma}} & \overline{\overline{\alpha}\gamma + \beta\overline{\delta}} \end{pmatrix}$$

Infine osserviamo che per il *Teorema di Binet* si ha $det(A^{-1}B) = det(A^{-1})det(B) = 1$, dunque $A^{-1}B \in SU(2)$. Dato che chiaramente $SU(2) \neq \emptyset$ (ad esempio perché la matrice identità è un suo elemento), è così dimostrato che $SU(2)$ è un sottogruppo di $GL_2(\mathbb{C})$.

Consideriamo l'applicazione $S^3 \to SU(2),\ (\alpha, \beta) \mapsto \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix}$

Mostriamo che f un omomorfismo di gruppi. Siano $(\alpha, \beta), (\gamma, \delta) \in S^3$, allora

$$f((\alpha, \beta)(\gamma, \delta)) = f(\alpha\gamma - \beta\overline{\delta}, \alpha\delta + \beta\overline{\gamma}) = \begin{pmatrix} \alpha\gamma - \beta\overline{\delta} & \alpha\delta + \beta\overline{\gamma} \\ -\overline{\alpha} \cdot \overline{\delta} - \overline{\beta}\gamma & \overline{\alpha} \cdot \overline{\gamma} - \overline{\beta}\delta \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ -\overline{\delta} & \overline{\gamma} \end{pmatrix}$$

$$= f(\alpha, \beta) f(\gamma, \delta)$$

Inoltre $ker(f) = \left\{ (\alpha, \beta) \in S^3 \mid \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} = \{(1,0)\}$, dunque f è iniettiva, mentre la suriettività è immediata dalle definizioni. È così dimostrato che f è un isomorfismo di gruppi.

Esercizio 5.4. Supponiamo per assurdo $\mathbb{Z}$ e $\mathbb{Q}$ siano isomorfi, allora necessariamente $\mathbb{Q}$ dovrebbe essere ciclico, dal momento che $\mathbb{Z}$ lo è (cfr. Proposizione 43). Ma per ogni $\frac{m}{n} \in \mathbb{Q} : \frac{m+1}{n} \notin \left\langle \frac{m}{n} \right\rangle = \left\{ \frac{am}{n} \in \mathbb{Q} | a \in \mathbb{Z} \right\}$, dal momento che $m \nmid m+1$.

Esercizio 5.5.

- Supponiamo per assurdo $(\mathbb{Q}, +)$ e $(\mathbb{Q}^*, \cdot)$ (risp. $(\mathbb{R}, +)$ e $(\mathbb{R}^*, \cdot)$) siano isomorfi, allora per definizione esiste $f : \mathbb{Q} \to \mathbb{Q}^*$ (risp. $\mathbb{R} \to \mathbb{R}^*$) isomorfismo. Dalla suriettività di f si ha l'esistenza di $x \in \mathbb{Q}$ (risp. $x \in \mathbb{R}$) tale che $f(x) = -1$, quindi $f(2x) = f(x+x) = f(x)f(x) = (-1)^2 = 1 = f(0)$, dalla quale per iniettività di f deduciamo $2x = 0$, ossia $x = 0$, e quindi $1 = f(0) = -1$, assurdo;
- $e^x : \mathbb{R} \to \mathbb{R}^+$ è un isomorfismo tra i gruppi $(\mathbb{R}, +)$ e $(\mathbb{R}^+, \cdot)$;
- Supponiamo per assurdo $(\mathbb{Q}, +)$ e $(\mathbb{Q}^+, \cdot)$ siano isomorfi, allora per definizione esiste $f : \mathbb{Q} \to \mathbb{Q}^+$ isomorfismo. Dal momento che f è suriettiva esiste $q \in \mathbb{Q}$ tale che $f(q) = 2$, ma allora $2 = f(\frac{q}{2} + \frac{q}{2}) = f(\frac{q}{2})^2$, e dunque $f(\frac{q}{2}) = \sqrt{2}$, assurdo.

Esercizio 5.6. Dalla teoria sappiamo che sappiamo che $\mathbf{G}/Z(\mathbf{G}) \cong Inn(\mathbf{G})$

1. Da quanto ricordato in apertura segue $Inn(S_3) \cong S_3$, dal momento che S_3 ha centro banale. Inoltre sappiamo che $Inn(S_3) \subseteq Aut(S_3)$, quindi $|Aut(S_3)| \geq |Inn(S_3)| = |S_3| = 6$. D'altra parte dall'*Esercizio 5.8* segue che gli automorfismi di S_3 preservano l'ordine, quindi ogni $h \in Aut(S_3)$ induce una permutazione sull'insieme delle trasposizioni di S_3, e viceversa, essendo S_3 generato dalle sue trasposizioni, ogni siffatta permutazione induce un automorfismo di S_3. Ne segue che $|Aut(S_3)| \leq 6$, per cui $Inn(S_3) = Aut(S_3)$ e $|Aut(S_3)| = 6$;
2. Segue da quanto ricordato in apertura sfruttando l'*Esercizio 4.9*;

3. Segue da quanto ricordato in apertura sfruttando l'*Esercizio 4.10*.

Esercizio 5.7. Per definizione $G = \langle X \rangle = \{g_1^{\alpha_1} \cdot \ldots \cdot g_n^{\alpha_n} \mid n \in \mathbb{N}^+, g_1, \ldots, g_n \in X, \alpha_1, \ldots, \alpha_n \in \mathbb{Z}\}$. Quindi se $x \in G$ si ha che esistono $n \in \mathbb{N}^+, g_1, \ldots, g_n \in X, \alpha_1, \ldots, \alpha_n \in \mathbb{Z}$ tali che $x = g_1^{\alpha_1} \cdot \ldots \cdot g_n^{\alpha_n}$, per cui $f(x) = f(g_1^{\alpha_1} \cdot \ldots \cdot g_n^{\alpha_n}) = f(g_1)^{\alpha_1} \cdot \ldots \cdot f(g_n)^{\alpha_n} = g(g_1)^{\alpha_1} \cdot \ldots \cdot g(g_n)^{\alpha_n} = g(g_1^{\alpha_1} \cdot \ldots \cdot g_n^{\alpha_n}) = g(x)$. Dall'arbitrarietà di g di conclude $f = g$.

Esercizio 5.8.

1. $f(x^{o(x)}) = f(1) = 1$, ossia $f(x)^{o(x)} = 1$, per cui $o(f(x)) \mid o(x)$;
2. Dimostriamo che f ha nucleo banale. $x \in ker(f) \Rightarrow f(x) = 1$, quindi per ipotesi $o(x) = o(f(x)) = o(1)$, da cui deduciamo $x = 1$.

L'ultima affermazione è immediata da 1. considerando la proiezione canonica sul quoziente $\pi : G \to G/N$.

Esercizio 5.9. Si ricordi che il quoziente $\mathbb{R}^* / \langle \pi \rangle$ è per definizione costituito dalle classi laterali sinistre (o equivalentemenete destre) del sottogruppo (normale) $\langle \pi \rangle$. Cominciamo deducendo condizioni necessarie affinché un elemento di tale quoziente abbia ordine n. Supponiamo $o(x \langle \pi \rangle) = n$. Osserviamo che per ogni $x \in \mathbb{R}^*$ si ha $(x \langle \pi \rangle)^n = x^n \langle \pi \rangle = \langle \pi \rangle$ se e solo se $x^n \in \langle \pi \rangle = \{\pi^m \mid m \in \mathbb{Z}\}$, ossia esiste $m \in \mathbb{Z}$ tale che $x^n = \pi^m$. Si noti che per n dispari si deve avere necessariamente $x > 0$, mentre per n pari esiste $m \in \mathbb{Z}$ tale che $x^n = \pi^m$ se e solo se esiste $m \in \mathbb{Z}$ tale che $(-x)^n = \pi^m$, e $x \not\sim -x$. Conseguentemente possiamo cominciare analizzando il caso $x > 0$. Se $x^n = \pi^m$ con $m \geq n$, possiamo applicare la divisione con resto e ottenere $m = qn + r$, dove $0 \leq r < n$, allora $x^n = \pi^m = \pi^{qn+r}$ se e solo se $(\pi^{-q}x)^n = \pi^r$, e $\pi^{-q}x \sim x$, in quanto $(\pi^q x^{-1})x = \pi^q \in \langle \pi \rangle$, ossia $x \langle \pi \rangle = (\pi^{-1}x) \langle \pi \rangle$, quindi senza perdita di generalità possiamo assumere $0 \leq m < n$. Osserviamo ora che m ed n devono essere coprimi. Infatti, supponiamo per assurdo $(m, n) = k \geq 2$, allora esistono $m', n' \in \mathbb{N}^+$ tali che $m = km'$ e $n = kn'$, e in particolare si osservi che necessariamente $1 < n'$. Allora $(x^{n'})^k = x^n = \pi^m = (\pi^{m'})^k$, dalla quale (essendo sia x che π positivi) deduciamo $x^{n'} = \pi^{m'}$, in contrasto con l'ipotesi che $x \langle \pi \rangle$ abbia ordine n. Abbiamo quindi dedotto che necessariamente $0 \leq m < n$ ed $(m, n) = 1$, dunque nel caso dispari esistono al più $\varphi(n)$ (dove con φ denotiamo la *funzione di Eulero*, ossia la funzione che associa ad 1 il naturale 1 e ad ogni $n \in \mathbb{N}_{\geq 2}$ il numero di naturali positivi strettamente più piccoli di n e coprimi con esso) elementi di ordine n, mentre nel caso pari ne esistono al più $2\varphi(n)$. Per concludere la dimostrazione è sufficiente quindi esibire nel caso dispari $\varphi(n)$ elementi distinti di $\mathbb{R}^* \langle \pi \rangle$ aventi ordine n, mentre in quello

pari $2\varphi(n)$. È di verifica immediata che per n dispari possiamo considerare la famiglia $\{\pi^{\frac{n}{k}}\langle\pi\rangle \mid 0 < k < n,\ (n,k) = 1\}$, mentre in quello pari possiamo considerare $\{\pm\pi^{\frac{n}{k}}\langle\pi\rangle \mid 0 < k < n,\ (n,k) = 1\}$.

Esercizio 5.10. Si ha $o((1\ 3)) = 2$, $o((1\ 2\ 3\ 4)) = 4$ e $(1\ 3)(1\ 2\ 3\ 4)(1\ 3) = (3\ 2\ 1\ 4) = (4\ 3\ 2\ 1) = (1\ 2\ 3\ 4)^{-1}$, inoltre con argomenti simili a quelli utilizzati nel terzo punto dell'*Esercizio 5.2* si dimostra che il sottogruppo generato da tali permutazioni in S_4 ha ordine 8. Quindi per il risultato generale ottenuto nel terzo punto dell'*Esercizio 5.2* si ha $\langle(1\ 3), (1\ 2\ 3\ 4)\rangle \cong D_4$.

Soluzioni esercizi capitolo 6

Esercizio 6.1. Consideriamo l'applicazione $f : \mathbb{R} \times \{-1, 1\} \to \mathbb{R}^*,\ (x, s) \mapsto se^x$. Dal momento che $e^x : \mathbb{R} \to \mathbb{R}^+$ è bigettiva, la f risulta essere una bigezione. Per concludere è sufficiente mostrare che f è un omomorfismo.

Esercizio 6.2.

1. Utilizziamo il criterio di sottogruppo. $\forall x, y \in G : (x, x)^{-1}(y, y) = (x^{-1}, x^{-1})(y, y) = (x^{-1}y, x^{-1}y) \in D$;
2. Supponiamo $D \trianglelefteq G$, allora $\forall x, y \in G : (x, y^{-1}xy) = (x^{-1}xx, y^{-1}xy) = (x^{-1}, y^{-1})(x, x)(x, y) = (x, y)^{-1}(x, x)(x, y) \in D$, per cui $x = y^{-1}xy$, ossia $yx = xy$. Viceversa, se G è abeliano allora $G \times G$ è abeliano, quindi ogni suo sottogruppo è normale.

Esercizio 6.3. Consideriamo $\mathbf{G} = \mathbb{Z}_2 \times \mathbb{Z}_2$ e siano $N_1 = \langle(1, 0)\rangle$, $N_2 = \langle(0, 1)\rangle$ ed $N_3 = \langle(1, 1)\rangle$, allora le condizioni 1. e 2. sono soddisfatte, ma chiaramente $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong N_1 \times N_2 \times N_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Esercizio 6.4. Useremo il *Teorema prodotto* per dimostrare la tesi. A tale proposito, osserviamo i seguenti fatti:

(i) Sia $f(g) \in f(G) \cap ker(f)$, allora $f(g) = f(f(g)) = 1$, dove la prima uguaglianza vale per l'ipotesi $f \circ f = f$ e la seconda in quanto $f(g) \in ker(f)$, ossia $f(G) \cap ker(f) = \{1\}$;

(ii) $\forall g \in G : f(f(g)^{-1}g) = f(f(g))^{-1}f(g) = f(g)^{-1}f(g) = 1$, quindi $f(g)^{-1}g \in ker(f)$, e dunque $g = f(g)(f(g)^{-1}1)g \in f(G)ker(f)$, ossia $G = f(G)ker(f)$;

(iii) Essendo G abeliano, $f(G) \trianglelefteq G$.

La tesi è quindi conseguenza del *Teorema prodotto*.

Esercizio 6.5.

1. Immediato dalle definizioni;

2. $\widetilde{F} : K \to G \times H$ è un omomorfismo, allora $\forall i \in \{1,2\} : f_i = p_i \circ \widetilde{F}$ omomorfismo in quanto composizione di omomorfismi, inoltre $\forall x \in K$: $F(x) = (f_1(x), f_2(x)) = ((p_1 \circ \widetilde{F})(x), (p_2 \circ \widetilde{F})(x)) = \widetilde{F}(x)$, per cui $F = \widetilde{F}$.

Esercizio 6.6. Supponiamo tutti gli elementi di $G \setminus \{1\}$ abbiano ordine 2, allora, in particolare, ogni elemento di G è inverso di se stesso. Siano $x, y \in G$, allora $xyxy = 1$, ossia $xy = yx$, quindi G è abeliano. Sia $a \in G \setminus \{1\}$ un elemento di ordine 2, allora $|\langle a \rangle| = 2$, per cui $G \setminus \langle a \rangle \neq \emptyset$. Sia $b \in G \setminus \langle a \rangle$, allora $o(b) = 2$. a, b sono distinti per scelta e hanno entrambi ordine 2, quindi $ab \neq 1$ (se $ab = 1$, allora $a = b^{-1} = b$, in contrasto con l'ipotesi che siano distinti). D'altra parte $a, b \notin \{1\}$, quindi $ab \notin \{a, b\}$. Conseguentemente $\langle a, b \rangle = \{1, a, b, ab\}$ sono tutti distinti. Sia $c \in G \setminus \langle a, b \rangle$, allora $o(c) = 2$. Osserviamo che per come è stato scelto c si ha che ac, bc e abc sono tre elementi distinti di G che non coincidono con nessuno degli elementi di $\{1, a, b, ac\}$. Di conseguenza

$$G = \{1, a, b, c, ab, ac, bc, abc\}$$

Quindi $G = \langle a, b \rangle \langle c \rangle$, inoltre $\langle a, b \rangle \langle c \rangle \trianglelefteq G$ (dal momento che G è abeliano) e $\langle a, b \rangle \cap \langle c \rangle = \{1\}$, dunque dal *teorema prodotto* si ha

$$G \cong \langle a, b \rangle \langle c \rangle \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

.

Esercizio 6.7.

(i) Dato che $b \notin H = \langle a \rangle$, le classi laterali destre $\langle a \rangle$ e $\langle a \rangle b$ sono distinte. Quindi

$$G = \langle a \rangle \cup \langle a \rangle b = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

in quanto gli elementi dell'insieme al membro più a destra della catena di uguagliaglianze è costituito da otto elementi distinti di G;

(ii) Chiaramente $ba \notin \{1, a, a^2, a^3, b\}$ (in caso contrario si avrebbe $b \in \langle a \rangle$, in contrasto con la scelta di b).

Esercizio 6.8.

(i) Supponiamo per assurdo si abbia $ba = a^2b$, allora si avrebbe $a = 1a = b^2a = b(ba) = ba^2b = (ba)(ab) = (a^2b)(ab) = a^2(ba)b = a^2(a^2b)b = a^4b^2 = 1$, ossia $a = 1$, in contrasto con l'ipotesi $o(a) = 4$;

(ii) Dall'esercizio 6.7 sappiamo che $G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$, quindi se $ab = ba$ ovviamente G risulta essere abeliano. $G = \langle a \rangle \langle b \rangle$, inoltre $\langle a \rangle \cap \langle b \rangle = \{1\}$ e per abelianità di G tali sottogruppi sono normali, dunque dal *teorema prodotto* concludiamo $G \cong \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$;

(iii) Si ha $|G| = 8 = 2 \cdot 4$, inoltre $o(a) = 4$ e $o(b) = 2$ e, dall'ipotesi $ba = a^3b$, $bab = a^3b^2 = a^3 = a^{-1}$, quindi, per quanto visto nel terzo punto della soluzione dell'*Esercizio 5.2*, si ha $G \cong D_4$.

Esercizio 6.9.

(i) Dall'Esercizio 6.7 sappiamo che $G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$. Per ipotesi tutti gli elementi di $G \setminus H$ hanno ordine 4, quindi a^2 è l'unico elemento di ordine 2 di $\mathbf{G}$, e conseguentemente $o(b^2) = \frac{o(b)}{(o(b),2)} = \frac{4}{2} = 2 \Rightarrow a^2 = b^2$;

(ii)
- Supponiamo per assurdo $ba = a^2b$, allora $ba = b^3$ (dato che $a^2 = b^2$ per il punto precedente), e quindi $a = b^2 = a^2$, quindi $a = 1$, in contrasto con l'ipotesi $o(a) = 4$;
- Supponiamo per assurdo $ba = ab$, allora $(a^3b)^2 = (a^3)^2b^2 = a^6b^2 = a^8 = 1$, quindi $a^3b = a^2$, e dunque $ab = 1$, assurdo.

(iii) Dai precedenti punti si ha $G = \{1, a, a^2, a^3, b, ab, a^2b, ba\}$. Esibiamo un isomorfismo esplicito con Q_8

$$
\begin{aligned}
G &\longrightarrow Q_8 \\
1 &\longmapsto id \\
a &\longmapsto i \\
a^2 &\longmapsto -1 \\
a^3 &\longmapsto -i \\
b &\longmapsto j \\
ab &\longmapsto k \\
a^2b &\longmapsto -j \\
a^3b &\longmapsto -k
\end{aligned}
$$

(iv) Si vedano gli esercizi precedenti e i punti precedenti del presente esercizio.

Esercizio 6.10. Svolgiamo direttamente l'esercizio nella sua forma più generale, ossia mostriamo che un gruppo G di ordine $2p$, con p primo dispari, è isomorfo a $\mathbb{Z}_{2p}$ (se abeliano) oppure a D_p (se non abeliano).

Supponiamo G sia un gruppo abeliano di ordine $2p$, p primo dispari. Dico che in G esiste almeno un elemento di ordine $2p$. Supponiamo per assurdo G non abbia alcun elemento di ordine $2p$. Per l'*Esercizio 1.7* esiste $x \in G$ avente ordine 2. Osserviamo ora che non esiste alcun $y \in G$ tale che $o(y) = p$, altrimenti per la Proposizione 30 si avrebbe $o(xy) = mcm(o(x), o(y)) = 2p$ (dal momento che $(2, p) = 1$ ed x, y commutano, essendo G abeliano), in contrasto con l'assunto che nessun elemento di G abbia ordine $2p$. Conseguentemente, per il *teorema di Lagrange*, ogni elemento di $G \setminus \{1\}$ ha ordine 2. Dato che $2p \geq 2 \cdot 3 = 6$, in G esistono almeno due elementi distinti x, y aventi ordine 2, ma allora, essendo G abeliano, si ha $\langle x, y\rangle = \{1, x, y, xy\} \leq G$, in contrasto con il *teorema di Lagrange* (dato che ovviamente $4 \nmid 2p$). Conseguentemente in G esiste almeno un elemento di ordine $2p$ e $G \cong \mathbb{Z}_{2p}$.

Supponiamo G sia un gruppo non abeliano di ordine $2p$, p primo dispari. Per l'*Esercizio 1.7* esiste $x \in G$ avente ordine 2. D'altra parte non tutti gli elementi di G possono avere ordine 2 (altrimenti G sarebbe abeliano), quindi esiste almeno un elemento y che non ha ordine 2, da cui segue $o(y) = p$ per il *teorema di Lagrange* (se fosse $o(y) = 2p$ si avrebbe $G \cong \mathbb{Z}_{2p}$, e quindi G ciclico in contrasto con l'ipotesi che sia non abeliano). Mostriamo ora che tutti gli elementi in $G \setminus \langle y\rangle$ hanno ordine 2. Supponiamo per assurdo esista $z \in G \setminus \langle y\rangle$ tale che $o(z) \neq 2$, allora, essendo per ipotesi G non abeliano, per *teorema di Lagrange* si ha $o(z) = p$. Dalla teoria (cfr. Capitolo 3) sappiamo che

$$| \langle x\rangle \langle y\rangle | = \frac{| \langle y\rangle || \langle z\rangle |}{| \langle y\rangle \cap \langle z\rangle |},$$

quindi

$$| \langle y\rangle \cap \langle z\rangle | = \frac{| \langle y\rangle || \langle z\rangle |}{| \langle y\rangle \langle z\rangle |} = \frac{p^2}{| \langle y\rangle \langle z\rangle |},$$

per cui $| \langle y\rangle \langle z\rangle | \in \{1, p, p^2\}$. Tuttavia $\{1, y, y^2, ..., y^{p-1}, x\} \subseteq \langle y\rangle \langle z\rangle$, quindi $| \langle y\rangle \langle z\rangle | \geq p + 1$. D'altra parte $\langle y\rangle \langle z\rangle \subseteq G$, quindi $| \langle y\rangle \langle z\rangle | \leq |G| = 2p < p^2$. Siamo così giunti ad un assurdo, e quindi $\forall z \in G \setminus \langle p\rangle : o(z) = 2$. Conseguentemente l'elemento xy ha ordine 2, infatti in caso contrario si avrebbe $x \in \langle y\rangle$, in contrasto con l'ipotesi che $o(x) = 2$, per cui $xyx = y^{-1}$. Da quanto visto nel terzo punto della soluzione dell'*Esercizio 5.2* concludiamo $G \cong D_p$.

Soluzioni esercizi capitolo 7

Esercizio 7.1.

1. Si ha (in notazione additiva) (cfr. Proposizione 27)

$$|H+K| = \frac{|H||K|}{|H \cap K|}$$

Quindi $|H||K| = |H+K||H \cap K|$, dalla quale per definizione deduciamo $|H+K| \mid |H||K|$;

2. Segue dal *Teorema numerico* tenendo conto del fatto che H e K sono anche sottogruppi di $H+K$ (anch'esso abeliano in quanto sottogruppo di un gruppo abeliano).

Esercizio 7.2.

- $n = 28$: $\mathbb{Z}_2 \times \mathbb{Z}_{14}$ è un gruppo di ordine 28 non ciclico (si ricordi che $G_1 \times G_2$ è ciclico se e solo se G_1 e G_2 sono gruppi finiti aventi cardinalità coprime);
- $n = 30$: si ha $30 = 2 \cdot 3 \cdot 5$, quindi per il *lemma di decomposizione primaria* si ha $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{30}$, quindi G ciclico;
- $n = 130$: si ha $130 = 2 \cdot 5 \cdot 13$, quindi come nel caso precedente otteniamo $G \cong \mathbb{Z}_{130}$, quindi G ciclico;
- $n = 131$: si ha che 131 è primo, quindi $G \cong \mathbb{Z}_{131}$, e dunque G ciclico.

Esercizio 7.3. Sappiamo che $Inn(G) \cong G/Z(G)$ e $Inn(G) \leq Aut(G)$. Dunque se $Aut(G)$ è ciclico concludiamo che anche $Inn(G)$ è ciclico (in quanto sottogruppo di un gruppo ciclico), e quindi anche $G/Z(G)$ lo è (in quanto isomorfo ad un gruppo ciclico). Conseguentemente esiste $g \in G$ tale che $G/Z(G) = \langle gZ(G) \rangle$. Siano $g_1, g_2 \in G$, allora per quanto detto poc'anzi esistono $n_1, n_2 \in \mathbb{N}$ tali che $g_1Z(G) = g^nZ(G)$ e $g_2Z(G) = g^mZ(G)$, ossia esistono $z_1, z_2 \in Z(G)$ soddisfacenti $g^{-n}g_1 = z_1$ e $g^{-m}g_2 = z_2$, e quindi $g_1 = g^nz_1$ e $g_2 = g^mz_2$. Di conseguenza $g_1g_2 = (g^nz_2)(g^mz_2) = g^n(z_1g^m)z_2 = g^n(g^mz_1)z_2 = (g^ng^m)(z_1z_2) = (g^mg^n)(z_2z_1) = g^m(g^nz_2)z_1 = (g^mz_2)(g^nz_1) = g_2g_1$. Dall'arbitrarietà di $g_1, g_2 \in G$ deduciamo che G è abeliano.

Esercizio 7.4 Si presentano due casi: $p \neq q$ (e quindi $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$ per il *lemma di decomposizione prima*) oppure $p = q$; nel secondo caso, a sua volta, dalla classificazione dei gruppi di ordine p^2, si ha $G \cong \mathbb{Z}_{p^2}$ oppure $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. Distinguiamo i tre casi.

- $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$: Dal *teorema di Lagrange* si ha che un sottogruppo H di G può avere solo ordini $\{1, p, q, pq\}$. Mostriamo che esiste uno e un solo sottogruppo di G di ordine p. L'esistenza è assicurata dal *lemma di Cauchy*. Dimostriamo l'unicità. Siano H e K sottogruppi di G di ordine p, allora

$$|HK| = \frac{|H||K|}{|H \cap K|} = \frac{p^2}{|H \cap K|}$$

per abelianità di G si ha che HK è un sottogruppo di G, inoltre osserviamo che $H \cap K \leq H$, quindi applicando nuovamente il *teorema di Lagrange* si ha $|H \cap K| \in \{1, p\}$. Ma osserviamo che tale cardinalità non può essere 1, dato che in tal caso si avrebbe $|HK| = p^2$, in contrasto con il *teorema di Lagrange* (dato che $p^2 \nmid pq$, essendo p e q primi distinti). Conseguentemente $|H \cap K| = p$, dalla quale deduciamo $H = K$ (dato che $H \cap K$ è sottoinsieme sia di H che di K ed entrambi hanno cardinalità p per ipotesi). Analogamente si dimostra che in G esiste esattamente uno e un solo sottogruppo di ordine q. Dunque G ha esattamente quattro sottogruppi (a meno di isomorfismi questi sono quello banale, $\mathbb{Z}_p$, $\mathbb{Z}_q$ e $\mathbb{Z}_p \times \mathbb{Z}_q$);

- $G \cong \mathbb{Z}_{p^2}$: dal *teorema di Lagrange* si ha che un sottogruppo H di G può avere solo ordini $\{1, p, p^2\}$. Mostriamo che esiste uno e un solo sottogruppo di G di ordine p. L'esistenza segue ancora una volta dal *lemma di Cauchy*. Dimostriamo l'unicità. Siano H e K sottogruppi di G aventi ordine p, allora

$$|HK| = \frac{|H||K|}{|H \cap K|}$$

Dato che $H \cap K \leq H$, per il *teorema di Lagrange* si ha $|H \cap K| \in \{1, p\}$. Ma osserviamo che se $|H \cap K| = 1$, allora si avrebbe che $H, K \trianglelefteq G$ (essendo G abeliano), $H \cap K = \{1\}$ e $HK = G$ (dal momento che $|HK| = p^2 = |G|$), e dunque per il *teorema prodotto* $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$, in contrasto con l'ipotesi $G \cong \mathbb{Z}_{p^2}$ (si osservi che $\mathbb{Z}_p^2 \ncong \mathbb{Z}_p \times \mathbb{Z}_p$). Dunque $|H \cap K| = p$, per cui $H = K$. Dunque G ha esattamente tre sottogruppi (a meno di isomorfismi questi sono quello banale, $\mathbb{Z}_p$ e $\mathbb{Z}_{p^2}$;

- $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$: dal *teorema di Lagrange* si ha che un sottogruppo H di G può avere solo ordini $\{1, p, p^2\}$. Siano H e K due sottogruppi di ordine p, allora per il *teorema di Lagrange* (essendo $H \cap K \leq H$) si ha $|H \cap K| \in \{1, p\}$. Se $|H \cap K| = p$ deduciamo $H = K$, in caso contrario abbiamo che H e K si intersecano nel solo elemento neutro 1. Conseguentemente in G si hanno al più $\frac{p^2-1}{p-1} = p + 1$ sottogruppi di ordine p. Dimostriamo ora che si hanno esattamente $p + 1$ sottogruppi di ordine p. Supponiamo per assurdo si abbiano esattamente $H_1, \ldots, h_k$, con $1 \leq k < p + 1$, sottogruppi

di G di ordine p, allora per quanto visto poc'anzi si ha $|H_1 \cup \ldots \cup H_K| = (p-1)k+1 < (p-1)(p+1)+1 = p^2-1+1 = p^2$, dunque (essendo $|G| = p^2$) si ha che esiste $x \in G \setminus (H_1 \cup \ldots \cup H_k)$. Dal momento che $x \neq 1$ si ha necessariamente $o(x) = p$ (si osservi che $o(x) \neq p^2$, dato che se così non fosse si avrebbe $G \cong \mathbb{Z}_{p^2}$), quindi $\langle x \rangle$ è un sottogruppo di G di ordine p differente da H_i per ogni $i \in \{1, \ldots, k\}$. Assurdo. Dunque G ha esattamente $p+1$ sottogruppi di ordine p, e quindi ha esattamente $p+3$ sottogruppi (quello banale, i $p+1$ di ordine p e G stesso).

Esercizio 7.6. Cominciamo osservando che se $\varphi : \mathbb{Z}_m \times \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_n$ è un omomorfismo di gruppi, allora si ha $\varphi([x]_m, [y]_n) = \varphi(([x]_m, [0]_n) + ([0]_m, [y]_n)) = \varphi([x]_m, [0]_n) + \varphi([0]_m, [y]_n)$ per ogni $x, y \in \mathbb{Z}$. Siano $h_1 : \mathbb{Z}_m \to \mathbb{Z}_m \times \mathbb{Z}_n,\ [x]_m \mapsto ([x]_m, [0]_n)$ e $h_2 : \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_n,\ [y]_m \mapsto ([0]_m, [y]_n)$ (si osservi che tali applicazioni sono omomorfismi di gruppo). Osserviamo ora che $h_1 : \mathbb{Z}_m \to \mathbb{Z}_m \times \mathbb{Z}_n$ coincide con la coppia di omomorfismi $(p_1 \circ h_1, p_2 \circ h_1)$ e che l'omomorfismo $p_2 \circ h_1 : \mathbb{Z}_m \to \mathbb{Z}_n$ è banale (ossia $ker(p_2 \circ h_1) = \mathbb{Z}_m$) in quanto $\mathbb{Z}_m$ e $\mathbb{Z}_n$ sono due gruppi finiti con cardinalità coprime. Similmente si osserva che l'omomorfismo $h_2 : \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_n$ coincide con la coppia $(p_1 \circ h_2, p_2 \circ h_2)$ e che l'omomorfismo $p_1 \circ h_2 : \mathbb{Z}_n \to \mathbb{Z}_m$ è banale. Consideriamo gli omomorfismi $\varphi_1 = p_1 \circ h_1 : \mathbb{Z}_m \to \mathbb{Z}_m$ e $\varphi_2 = p_2 \circ h_2 : \mathbb{Z}_n \to \mathbb{Z}_n$. In definitiva, quindi, per ogni $x, y \in \mathbb{Z}$ si ha $\varphi([x]_m, [y]_n) = \varphi([x]_m, [0]_n) + \varphi([0]_m, [y]_n) = h_1([x]_m) + h_2([y]_n) = ((p_1 \circ h_1)([x]_m), [0]_n) + ([0]_m, (p_2 \circ h_2)([y]_n)) = (\varphi_1([x]_m), [0]_n) + ([0]_m, \varphi_2([y]_n)) = (\varphi_1([x]_m), \varphi_2([y]_n))$. Conseguentemente $\varphi = \varphi_1 \times \varphi_2$, come cercato.

Esercizio 7.7. Si ha $\langle x \rangle = \{\alpha x \mid \alpha \in \mathbb{Z}\}$ e $\langle y \rangle = \{\beta y \mid \beta \in \mathbb{Z}\}$, per cui $\langle x \rangle + \langle y \rangle = \{\alpha x + \beta y \mid \alpha, \beta \in \mathbb{Z}\} = \langle \alpha, \beta \rangle = G$, dove la penultima uguaglianza segue dall'abelianità di G. D'altra parte

$$|G| = |\langle x \rangle + \langle y \rangle| = \frac{|\langle x \rangle||\langle y \rangle|}{|\langle x \rangle \cap \langle y \rangle|},$$

per cui $o(x)o(y) = |\langle x \rangle||\langle y \rangle| = |G||\langle x \rangle \cap \langle y \rangle|$, e quindi $|G| \mid o(x)o(y)$, dalla quale deduciamo quanto cercato ($p \mid |G| \Rightarrow p \mid o(x)o(y) \Rightarrow p \mid o(y)$, dove l'ultima implicazione è conseguenza del fatto che p è primo e $p \nmid o(x)$ per ipotesi).