

1. Sia (G, \cdot) un gruppo.
 - (a) Verificare che l'elemento neutro e di G è unico.
 - (b) Verificare che per ogni $x \in G$, l'inverso x^{-1} di x in G è unico.
2. (*prodotto diretto di gruppi*) Siano (G_1, e_1, \circ) e $(G_2, e_2, *)$ due gruppi.
 - (a) Verificare che il prodotto cartesiano $G_1 \times G_2$, col prodotto definito da $(x_1, x_2) \cdot (y_1, y_2) := (x_1 \circ x_2, y_1 * y_2)$, è un gruppo.
 - (b) Determinare l'elemento neutro di $G_1 \times G_2$ rispetto al prodotto così definito.
 - (c) Determinare l'inverso di $(x_1, x_2) \in G_1 \times G_2$ rispetto al prodotto così definito.
 - (d) Verificare che se G_1 e G_2 sono abeliani, anche $G_1 \times G_2$ è abeliano.
 - (e) Siano $(G_1, e_1, \circ) = (\mathbf{Z}_2, \bar{0}, +)$ e $(G_2, e_2, *) = (\mathbf{Z}_3, \bar{0}, +)$. Scrivere la tabella dell'operazione indotta su $\mathbf{Z}_2 \times \mathbf{Z}_3$.
3. Siano (G_1, \cdot) e (G_2, \cdot) due gruppi e sia $\varphi: G_1 \rightarrow G_2$ un isomorfismo di gruppi.
 - (a) Verificare che $\varphi(e_1) = e_2$, dove e_1 ed e_2 sono rispettivamente l'elemento neutro di G_1 e l'elemento neutro di G_2 .
 - (b) Verificare che per ogni $x \in G_1$, l'inverso di $\varphi(x)$ in G_2 è dato da $\varphi(x)^{-1} = \varphi(x^{-1})$.
 - (c) Verificare che l'ordine di x in G_1 è uguale all'ordine di $\varphi(x)$ in G_2 .
4. Considerare i seguenti gruppi di ordine 4:
 - (a) $A = \{1, -1, i, -i\}$ con l'operazione data dalla moltiplicazione fra numeri complessi.
 - (b) \mathbf{Z}_4 con la somma fra classi resto.
 - (c) $\mathbf{Z}_2 \times \mathbf{Z}_2$ con la somma definita da $(\bar{x}, \bar{y}) + (\bar{u}, \bar{v}) = (\overline{x+u}, \overline{y+v})$.
 - (d) \mathbf{Z}_5^* col prodotto fra classi resto.
 - (e) \mathbf{Z}_{12}^* col prodotto fra classi resto.
 - (f) \mathbf{Z}_8^* col prodotto fra classi resto.

(4.a) Scrivere le rispettive tabelle moltiplicative e determinare quali di essi sono isomorfi tra loro.

(4.b) Quali di essi sono ciclici?
5. Sia $n \in \mathbf{N}$. L'ordine $\text{ord}_n(x)$ di $x \in \mathbf{Z}_n^*$ è il più piccolo $r > 0$ tale che $x^r \equiv 1 \pmod{n}$.
 - (a) Sia $n = 7$. Calcolare $\text{ord}_n(x)$ per ogni $x \in \mathbf{Z}_n^*$.
 - (b) Sia n primo. Dimostrare che $\text{ord}_n(x)$ divide $n - 1$ per ogni $x \in \mathbf{Z}_n^*$.
 - (c) Sia $n \in \mathbf{N}$. Calcolare l'ordine di $-1 \pmod{n}$.
6. Siano n, m interi positivi con $\text{gcd}(n, m) = 1$.
 - (a) Verificare che l'applicazione biiettiva

$$\varphi: \mathbf{Z}_{nm} \rightarrow \mathbf{Z}_n \times \mathbf{Z}_m, \quad \bar{x} \mapsto (\bar{x} \pmod{n}, \bar{x} \pmod{m})$$

è un isomorfismo di gruppi. Ne segue che, se $\text{gcd}(n, m) = 1$, il prodotto diretto $\mathbf{Z}_n \times \mathbf{Z}_m$ è un gruppo ciclico.

- (b) Determinare gli elementi di ordine 6 in $\mathbf{Z}_2 \times \mathbf{Z}_3 \cong \mathbf{Z}_6$.
7. Siano n, m interi positivi con $\text{gcd}(n, m) > 1$.
- (a) Verificare che in $\mathbf{Z}_n \times \mathbf{Z}_m$ non ci sono elementi di ordine nm (suggerimento: sfruttare il fatto che in questo caso $\text{mcm}(n, m) < nm$ e calcolare

$$(\bar{x}, \bar{y}) + \dots + (\bar{x}, \bar{y}) = (??, ??), \quad \text{mcm}(n, m)\text{-volte.}$$

- Ne segue che, se $\gcd(n, m) > 1$, il prodotto diretto $\mathbf{Z}_n \times \mathbf{Z}_m$ non è un gruppo ciclico.
- (b) Verificare che non ci sono elementi di ordine 9 in $\mathbf{Z}_3 \times \mathbf{Z}_3$.
 - (c) Verificare che non ci sono elementi di ordine 12 in $\mathbf{Z}_2 \times \mathbf{Z}_6$.

Il prototipo del gruppo ciclico di ordine n è il gruppo additivo $(\mathbf{Z}_n, +)$. Vedremo che in un gruppo ciclico di ordine n vale il seguente fatto:

Per ogni divisore d di n , ci sono $\varphi(d)$ elementi di ordine d . (*)

- 8. Verificare (*) nel caso del gruppo $(\mathbf{Z}_{12}, +)$ e del gruppo \mathbf{Z}_{15} (magari fare i conti con Pari/Gp).
- 9. Sia $p \in \mathbf{N}$ un numero primo. Verificare che in \mathbf{Z}_p vale l'uguaglianza $(\bar{x} + \bar{y})^p = \bar{x}^p + \bar{y}^p$, per ogni $\bar{x}, \bar{y} \in \mathbf{Z}_p$ (suggerimento: usare la formula di Newton).
Verificare che per $n = 4$, tale uguaglianza non vale.
- 10. Dimostrare che $\sum_{\bar{x} \in \mathbf{Z}_n} \bar{x} = \bar{0}$ in \mathbf{Z}_n , per ogni n dispari.
- 11. Calcolare $(p-1)!$ in \mathbf{Z}_p , per p primo.
- 12. Sia G un gruppo tale che $g^2 = e$, per ogni $g \in G$. Dimostrare che G è abeliano.