

Esercizio 1. Sia $\phi: G \rightarrow G'$ un omomorfismo di gruppi.

1.1. Abbiamo visto che $\text{Im}\phi \equiv \phi(G)$ è un sottogruppo.

Verificare che se G è commutativo allora anche $\text{Im}\phi$ è commutativo.

1.2. Verificare che se $H \leq G$ allora $\phi(H) \leq G'$. Vi ricordo che $H \leq G$ è il simbolo che utilizziamo per enunciare che H è un sottogruppo di G .

1.3. Verificare che

$$\phi^{-1}(1_{G'}) = \{g \in G \mid \phi(g) = 1_{G'}\}$$

è un sottogruppo. Esso è chiamato il **nucleo** di ϕ ed è denotato con il simbolo $\text{Ker}\phi$ (da *kernel*, che vuol dire *nocciolo* in Inglese).

1.1) Siano $a, b \in G$, si ha che $a \cdot b = b \cdot a : \phi(a) \cdot \phi(b) = \phi(a \cdot b) = \phi(b \cdot a) = \phi(b) \cdot \phi(a)$

1.2) Siano $a, b \in H \Rightarrow a \cdot b^{-1} \in H$. Quindi $\phi(a) \in \phi(H)$ e $\phi(b) \in \phi(H)$.

$$\Rightarrow \phi(a) \cdot \phi(b)^{-1} = \phi(a) \cdot \phi(b^{-1}) = \phi(a \cdot b^{-1}) \text{ MA } a \cdot b^{-1} \in H \Rightarrow \phi(a \cdot b^{-1}) \in H \Rightarrow \phi(H) \leq G'$$

1.3) Siano $a, b \in \text{Ker}\phi$, quindi $\phi(a) = 1_G \wedge \phi(b) = 1_G$, come si comporta $\phi(a \cdot b^{-1})$?
 $\phi(a \cdot b^{-1}) = \phi(a) \cdot \phi(b^{-1}) = \phi(a) \cdot \phi(b)^{-1} = 1_G \cdot 1_G^{-1} = 1_G \cdot 1_G = 1_G$

Esercizio 2. Determinare l'ordine di un qualsiasi $h \in (\mathbb{Z}, +)$.

Determinare l'ordine di $[1] \in \mathbb{Z}_n$

Abbiamo visto che se $H \leq \mathbb{Z}_n$ allora $H = H_d$ con $n = kd$ per qualche k

$$H_d = \{[d], [2d], \dots, [(k-1)d], [0]\}$$

Determinare l'ordine di $[d]$.

Determinare l'ordine di $[3] \in \mathbb{Z}_{15}$.

(Ovviamente siamo in notazione additiva.)

L'ordine di ogni $h \in (\mathbb{Z}, +)$ è infinito dato che \mathbb{Z} non è un gruppo finito.

L'ordine di $1 \in \mathbb{Z}_n$ è $\sigma(1) = n$. Dato che $\mathbb{Z}_n = \{1^1, 1^2, 1^3, \dots, 1^{n-1}, 1^n = [0]\}$

L'ordine di d è k .

In \mathbb{Z}_{15} ho che:

$$3^1 = [3] \quad 3^2 = [6] \quad 3^3 = [9] \quad 3^4 = [12] \quad 3^5 = [15] = 0 \Rightarrow \sigma(3) = 5$$

Esercizio 3. Sia $\phi: G \rightarrow G'$ un omomorfismo di gruppi. ϕ è detto un **isomorfismo**

se è iniettivo e suriettivo.

Verificare che se ϕ è un isomorfismo, allora $o(g) = o(\phi(g)) \forall g \in G$.

ho che $\sigma(g) = d \Rightarrow g^d = g + g + \dots + g = 1_G$, e che $\sigma(\phi(g)) = k \Rightarrow \phi(g)^k = 1_{G'}$

$$\text{So che: } \begin{cases} 1_{G'} = \phi(g)^k = \phi(g^k) \\ 1_{G'} = \phi(1_G) = \phi(g^d) \end{cases} \Rightarrow k = d \Rightarrow \sigma(g) = \sigma(\phi(g)).$$

Esercizio 4. Consideriamo il gruppo simmetrico S_3 di tutte le bigezioni dell'insieme $\{1, 2, 3\}$ in sé stesso. Utilizziamo la notazione

$$\begin{pmatrix} 1 & 2 & 3 \\ \tau(1) & \tau(2) & \tau(3) \end{pmatrix}$$

per l'elemento $\tau \in S_3$. Il prodotto in S_3 è dato dalla composizione di bigezioni.

4.1 Scrivere tutti gli elementi di S_3 .

4.2 Scrivere la tabella moltiplicativa di S_3

4.3 Quali sono i possibili ordini degli elementi di S_3 ?

4.4 Determinare l'ordine di ogni elemento di S_3 .

4.5 Quali sono i possibili ordini dei sottogruppi di S_3 ?

4.6 Verificare che S_3 ha quattro sottogruppi ciclici: 3 di ordine 2 ed uno di ordine

3.

4.7 Verificare che

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

è uno di tali sottogruppi e che $aH \neq Ha$ per a uguale a

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

$$4.1) S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}$$

4.3) I possibili ordini sono 1 (per l'id.), 2 per le traspos. e 3 per i 3-cicli.

$$4.4) \begin{cases} \{x \in S_3 \mid \sigma(x) = 1\} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \right\} \\ \{x \in S_3 \mid \sigma(x) = 2\} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \\ \{x \in S_3 \mid \sigma(x) = 3\} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\} \end{cases}$$

4.2)

$\downarrow \circ \rightarrow$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$
	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$
	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$
	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

4.5) considero i divisori non banali di $|S_3|=6$, che sono 2, 3, so per il teo. di struttura dei gruppi ciclici che esistono tanti sottogruppi quanti sono i divisori di n , e hanno ordine $\frac{6}{2}=3$ e $\frac{6}{3}=2$.

4.6) I sottogruppi ciclici sono:

$$H' = \left\{ 1, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\} \quad \text{ORDINE 2} \quad H'' = \left\{ 1, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\} \quad \text{ORDINE 2} \quad H''' = \left\{ 1, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \quad \text{ORDINE 2}$$

$$K = \left\{ 1, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} \quad \text{ORDINE 3}$$

4.7) $H = \left\{ 1, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\}$ e' un sottogruppo: $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot 1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot 1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \in H$
 $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ S_3 non e' commutativo.

Esercizio 5. Verificare che l'intersezione di 2 sottogruppi di un gruppo G è un sottogruppo. Estendere il risultato a l'intersezione di una famiglia arbitraria di sottogruppi in G .

Sia G un gruppo, ed H, H' due sottogruppi di G . Considero $H \cap H'$
 Siano $a, b \in H \cap H' \Rightarrow a \in H \wedge a \in H' \wedge b \in H \wedge b \in H' \Rightarrow a \cdot b^{-1} \in H \wedge a \cdot b^{-1} \in H' \Rightarrow a \cdot b^{-1} \in H \cap H'$.
 Sia $K := H_1 \cap H_2 \cap \dots \cap H_n$ l'intersezione di n sottogruppi di G . Se $a \in K \Rightarrow \forall i \in \{1, \dots, n\} a \in H_i$
 e se $b \in K \Rightarrow \forall i \in \{1, \dots, n\} b \in H_i \Rightarrow \forall i \in \{1, 2, \dots, n\} a, b \in H_i$, ma H_i e' un sottogruppo,
 quindi $\forall i \in \{1, \dots, n\} a \cdot b^{-1} \in H_i \Rightarrow a \cdot b^{-1} \in H_1 \cap H_2 \cap \dots \cap H_n = K \Rightarrow K$ e' un sottogruppo.

Esercizio 6. Consideriamo il gruppo commutativo $(\mathbb{Z}, +)$ e siano H e K due suoi sottogruppi.

Sappiamo che $H = a\mathbb{Z}$ e $K = b\mathbb{Z}$ per opportuni $a, b \in \mathbb{N}$. Caratterizzare $H \cap K$ in termini del mcm(a, b).

H e' definito come $\{x \cdot a \mid x \in \mathbb{Z}\}$, quindi $\forall x \in H, a \mid x$. $K = \{x \cdot b \mid x \in \mathbb{Z}\} \Rightarrow \forall x \in K, b \mid x$.

H contiene tutti i multipli di a e K tutti i multipli di b .

quindi se H contiene gli x per cui $x \mid a$ e K contiene gli x per cui $x \mid b$, allora $H \cap K$ contiene gli elementi divisi da a e b . $H \cap K$ contiene tutti i

multipli comuni di a e b . Sappiamo che il più piccolo elemento di HNK è $\text{mcm}(a,b)$. Tutti i numeri multipli di a e b , sono i multipli di $\text{mcm}(a,b)$, quindi $\text{HNK} = \{x \cdot \text{mcm}(a,b) \mid x \in \mathbb{Z}\} = \text{mcm}(a,b)\mathbb{Z}$.

Esercizio 7. Sia (G, \cdot) un gruppo e sia $g \in G$ un elemento di ordine finito. Sia $n = o(g)$. Verificare che $g^m = 1_G$ se e solo se n divide m .
Suggerimento: in una direzione è immediato. Nell'altra usare la divisione e la definizione di ordine di un elemento.
Verificare che se G è finito e $|G| = n$ allora ogni suo elemento g ha ordine finito e $o(g)$ divide n (utilizzare Lagrange).
Dedurre che se G è finito e $|G| = n$ allora $\forall g \in G$ si ha $g^n = 1_G$.

PUNTO 1) Se n divide $m \Rightarrow m = n \cdot k$ per qualche $k \in \mathbb{Z}$, quindi $g^m = g^{n \cdot k} =$

$$g^n \cdot g^n \cdot \dots \cdot g^n = 1_G \cdot 1_G \cdot \dots \cdot 1_G = 1_G. \text{ Dall'altro verso, se } g^m = 1_G \Rightarrow$$

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

$$g^n \cdot g^n \cdot \dots \cdot g^n = 1_G \Leftrightarrow g^{m-nk} = 1_G \Leftrightarrow m-nk = n \Leftrightarrow m = nk + n$$

$$\Leftrightarrow m = n \cdot (k+1) \Leftrightarrow m \text{ divide } n. \blacksquare$$

1 PUNTI 2 e 3 LI FARO' POI

Esercizio 8. Sappiamo che $(U(\mathbb{Z}_8), \cdot)$ ha una struttura di gruppo di ordine 4 (perché utilizzando la funzione di Eulero si ha $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 4$). Scrivere la tabella moltiplicativa di questo gruppo. Vero o Falso: $(U(\mathbb{Z}_8), \cdot)$ è isomorfo a \mathbb{Z}_4 .
Suggerimento: l'esercizio 3 può risultare utile.

Definisco esplicitamente $U(\mathbb{Z}_8) = \{[1], [3], [5], [7]\}$

\cdot	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Non è isomorfo a \mathbb{Z}_4 , in quanto (\mathbb{Z}_4, \cdot) non è un gruppo, e non ha un inverso per ogni elemento. In $U(\mathbb{Z}_8)$ ogni elemento ha ordine 1, in \mathbb{Z}_4 , $[3]$ ha ordine 3,

per l'es. 3 non possono essere isomorfi.

Esercizio 9. Dimostrare che

- $(\mathbb{Z}, +)$ non è isomorfo a $(\mathbb{Q} \setminus \{0\}, \cdot)$.

Suggerimento: l'esercizio 3 può nuovamente essere utile

- S_3 non è isomorfo a \mathbb{Z}_6

basta trovare uno stesso elemento che ha ordini diversi nei due gruppi.

• in $(\mathbb{Z}, +)$, $\sigma(-1) = \infty$ in $(\mathbb{Q} \setminus \{0\}, \cdot)$, $\sigma(-1) = 2$.

• \mathbb{Z}_6 ha un elemento, ossia 1 che è di ordine 6, in S_3 tutti gli elementi hanno ordine 1, 2 o 3, mai 6.

Esercizio 10. Sia (G, \cdot) un gruppo e ρ una relazione di equivalenza. Diremo che ρ è compatibile con \cdot se

$$g\rho g', \gamma\rho\gamma' \Rightarrow (g \cdot \gamma) \rho (g' \cdot \gamma').$$

Dimostrare che se ρ è compatibile con \cdot allora l'insieme delle classi di equivalenza G/ρ ha una naturale struttura di gruppo data da:

$$[g] \star [h] := [g \cdot h].$$

Dovete verificare che questa operazione è ben definita e che $(G/\rho, \star)$ è un gruppo.

dimostro che \star non dipende dalla scelta dei rappresentanti:

ho che $a\rho b$ $c\rho d$

$$[a] \star [c] = [b] \star [d] \Rightarrow [a \cdot c] = [b \cdot d] \Rightarrow (a \cdot c) \rho (b \cdot d) \Leftrightarrow a\rho b \wedge c\rho d$$

VERO PER
IPOTESI