Corso di Laurea in Informatica
Algebra. a.a. 2023-24. Proff. P. Piazza e G. Viaggi
Compito a casa del 03/11/2023

Esercizio 1. Sia $\phi : G \to G'$ un omomorfismo di gruppi.
1.1. Abbiamo visto che $\mathrm{Im}\phi \equiv \phi(G)$ è un sottogruppo.
Verificare che se G è commutativo allora anche $\mathrm{Im}\phi$ 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 $\mathrm{Ker}\phi$ (da *kernel*, che vuol dire *nocciolo* in Inglese).

Sia G un gruppo. Diremo che $g \in G$ ha ordine n se n è il **minimo** numero intero positivo tale che $g^n = 1_G$. Denotiamo tale numero con $o(g)$. Dimostreremo, ma potete già utilizzarlo in questo compito, che se $o(g) = n$ allora il sottogruppo generato da g,

$$\langle g \rangle := \{g^t, t \in \mathbb{Z}\}$$

ha cardinalità n. Di fatto vederemo, ed è facile da dimostrare, che se g ha ordine n allora

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

e che questi elementi sono distinti. In particolare quindi: *l'ordine del sottogruppo generato da un elemento g di ordine n è precisamente n.* Se non esiste n tale che $g^n = 1_G$ allora diremo che g ha ordine infinito e scriveremo $o(g) = \infty$.

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 e

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

Determinare l'ordine di $[d]$.
Determinare l'ordine di $[3] \in \mathbb{Z}_{15}$.
(Ovviamente siamo in notazione additiva.)

Esercizio 3. Sia $\phi : G \to G'$ un omomorfismo di gruppi. ϕ è detto un **isomorfismo** se è iniettivo e suriettivo.
Verificare che se ϕ è un isomorfismo, allora $o(g) = o(\phi(g))\ \forall g \in G$.

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 [1]

[1] trovate questa tabella sia in [C] che in [PC] ma non sarebbe molto istruttivo leggerla prima di aver risolto l'esercizio

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

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

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.

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 $\mathrm{mcm}(a, b)$.

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).
Dedurne che se G è finito e $|G| = n$ allora $\forall g \in G$ si ha $g^n = 1_G$.

Esercizio 8. Sappiamo che $(\mathcal{U}(\mathbb{Z}_8), \cdot)$ 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: $(\mathcal{U}(\mathbb{Z}_8), \cdot)$ è isomorfo a $\mathbb{Z}_4$.
Suggerimento: l'esercizio 3 può risultare utile.

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 $\mathbb{Z}_6$

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

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

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.