Università degli Studi Roma Tre
Corso di Laurea in Matematica, a.a. 2011/2012
AL210 - Algebra 2
Esercitazione 3 (7 Ottobre 2011)

Esercizio 1. Sia n un intero positivo. Determinare il centro dei seguenti gruppi:

$$\mathbb{Z}_n, \ S_n, \ A_n.$$

Soluzione: Il gruppo $\mathbb{Z}_n$ è abeliano e dunque $Z(\mathbb{Z}_n) = \mathbb{Z}_n$ per ogni n. Lo stesso vale per S_n con $n = 2$, e per A_n con $n \leq 3$.

Facciamo vedere che per $n \geq 3$, si ha $Z(S_n) = \{\mathrm{id}\}$. Poiché $n \geq 3$, $S_n = S(X)$ dove X ha almeno 3 elementi. È sufficiente far vedere che preso comunque un elemento σ di S_n diverso dall'identità, esiste almeno un elemento $\tau \in S_n$ con cui σ non commuta. Sia dunque $\sigma \neq \mathrm{id}$, allora esistono almeno 2 elementi di X mossi da σ, ovvero $a, b \in X$ tali che $\sigma(a) = b$ e $\sigma(b) \neq b$. Supponiamo $\sigma(b) = a$ e sia $c \in X$, $c \neq a, b$, allora si verifica facilmente che σ non commuta con la permutazione $\tau = (abc)$, infatti:

$$(\sigma \circ \tau)(a) = \sigma(b) = a \neq c = \tau(b) = (\tau \circ \sigma)(a).$$

Analogamente, se $\sigma(b) = c \neq a$, allora σ non commuta con $\tau = (ab)$, infatti:

$$(\sigma \circ \tau)(a) = \sigma(b) = c \neq a = \tau(b) = (\tau \circ \sigma)(a).$$

Dunque, in ogni caso, esiste almeno una permutazione τ che non commuta con σ e $Z(S_n) = \{\mathrm{id}\}$.

Per $n \geq 4$, utilizzando un ragionamento analogo, si dimostra che anche il centro di A_n è banale.

Esercizio 2. Siano $(G, *)$ un gruppo e $(G', *')$ un gruppo abeliano. Si denoti con $\mathrm{Hom}(G, G')$ l'insieme degli omomorfismi da G in G'.

(a) Dimostrare che $\mathrm{Hom}(G, G')$ è un gruppo (abeliano) rispetto alla somma puntuale:

$$(\Phi + \Psi)(x) := \Phi(x) *' \Psi(x), \qquad \Phi, \Psi \in \mathrm{Hom}(G, G').$$

(b) Dimostrare che $\mathrm{Hom}(\mathbb{Z}_{12}, \mathbb{Z}_5)$ è costituito dal solo omomorfismo banale.

(c) Scrivere esplicitamente gli elementi di $\mathrm{Hom}(\mathbb{Z}_{15}, \mathbb{Z}_3)$.

(d) Determinare il numero di elementi di $\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$ in funzione di m ed n. Stabilire poi quanti di essi sono iniettivi e quanti suriettivi.

Soluzione:

(a) Siano Φ e $\Psi \in \mathrm{Hom}(G, G')$, facciamo vedere che $\Phi + \Psi \in \mathrm{Hom}(G, G')$.

$$\begin{aligned}(\Phi + \Psi)(x * y) &= \Phi(x * y) *' \Psi(x * y) = \\ &= \Phi(x) *' \Phi(y) *' \Psi(x) *' \Psi(y) = \\ &= \Phi(x) *' \Psi(x) *' \Phi(y) *' \Psi(y) = (\Phi + \Psi)(x) *' (\Phi + \Psi)(y).\end{aligned}$$

Dunque $\Phi + \Psi \in \mathrm{Hom}(G, G')$. Non è difficile poi dimostrare che:

(-) l'elemento neutro di Hom è: $\Phi_e : G \to G'$, $x \mapsto e$, dove e è l'elemento neutro di G'.

(-) Dato $\Phi \in \mathrm{Hom}(G, G')$, l'inverso di Φ, ovvero Φ^{-1} è l'elemento di Hom tale che $x \mapsto (\Phi(x)^{-1})$. (Far vedere che $\Phi^{-1} \in$ Hom).

Poiché $\mathbb{Z}_n$ è ciclico, un omomorfismo Φ di $\mathbb{Z}_n$ in G è completamente determinato quando si conosce $\Phi(\overline{1})$.

(b) Tutti e soli gli elementi di $\mathrm{Hom}(\mathbb{Z}_{15}, \mathbb{Z}_3)$ sono: $\Phi_0(\overline{1}) = \overline{0}$, $\Phi_1(\overline{1}) = \overline{1}$ e $\Phi_2(\overline{1}) = \overline{2}$.

(c) Supponiamo esista un elemento non nullo $\Phi \in \mathrm{Hom}(\mathbb{Z}_{12}, \mathbb{Z}_5)$, allora $\Phi(\overline{1})$ genera un sottogruppo (ciclico) di $\mathbb{Z}_5$ che necessariamente è tutto $\mathbb{Z}_5$. Per il primo teorema di omomorfismo si ha che $\mathbb{Z}_{12}/\ker(\Phi)$ è isomorfo al gruppo ciclico generato da $\Phi(\overline{1})$. Per il Teorema di Lagrange però tale sottogruppo di $\mathbb{Z}_5$ ha per ordine un divisore di 12, dunque $5 \mid 12$ che è assurdo.

(d) Facciamo vedere che $\mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$ ha d elementi dove d è il $\gcd(n, m)$.

Per il primo teorema di omomorfismo, se $\Phi \in \mathrm{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$, si deve avere $\mathbb{Z}_n/\ker\Phi \cong \mathrm{Im}(\Phi)$, dunque il numero di elementi dell'immagine di Φ è un divisore comune di m ed n. Poiché $\mathbb{Z}_n$ e $\mathbb{Z}_m$ sono ciclici, essi ammettono uno ed un solo sottogruppo per ogni divisore dell'ordine, quindi il numero di scelte per l'immagine di Φ è pari al numero di divisori comuni di m ed n, che sono tanti quanti i divisori di $d := \gcd(m, n)$.

Sia $k := |\mathrm{Im}(\Phi)|$, ovvero $\mathrm{Im}(\Phi) \cong \mathbb{Z}_k$, allora tale sottogruppo ha esattamente $\varphi(k)$ generatori (dove φ è l'indicatore di Eulero) e dunque per ogni scelta di k, divisore di d, si hanno esattamente $\varphi(k)$ omomorfismi aventi per immagine $\mathbb{Z}_k$.

La conclusione è immediata ricordando che $d = \sum_{k|d} \varphi(k)$.

Utilizzando le stesse argomentazioni di sopra, esistono omomorfismi suriettivi se e solo se m divide n e, in tal caso, ce ne sono $\varphi(m)$. Si hanno invece omomorfismi iniettivi se e solo se n divide m e sono in numero di $\varphi(n)$.

Esercizio 3. Sia $(G, +)$ un gruppo abeliano. Mostrare che:

$$\begin{array}{rcc}\Phi : G \times G & \longrightarrow & G \\ (x, y) & \longmapsto & x - y\end{array}$$

è un omomorfismo. Calcolare nucleo ed immagine di Φ.

Soluzione: Dati comunque $(x, y), (u, v) \in G \times G$, si ha:

$$\Phi((x+u, y+v)) = x + u - y - v \overset{(*)}{=}$$
$$= x - y + u - v = \Phi((x, y)) + \Phi((u, v)),$$

dove in $(*)$ si è usato il fatto che G è abeliano.

L'omomorfismo Φ è suriettivo, infatti per ogni $g \in G$ si ha $g = \Phi((g, 0))$. Il nucleo di Φ è dato dalle coppie del tipo (g, g) ed è isomorfo a G.

Esercizio 4. Dato il gruppo $(\mathbb{R}, +)$ dimostrare che il quoziente $\mathbb{R}/\mathbb{Z}$ è isomorfo al seguente sottogruppo di $(\mathbb{C}^*, \cdot)$:

$$H := \{z \in \mathbb{C}^* : |z| = 1\}.$$

Soluzione: Costruiamo un omomorfismo $\mathbb{R} \to \mathbb{C}^*$ di nucleo $\mathbb{Z}$ e immagine H ed applicando il primo teorema di omomorfismo si otterrà l'isomorfismo cercato. Sia:

$$\begin{aligned} \psi : \mathbb{R} &\longrightarrow \mathbb{C}^* \\ x &\longmapsto \cos(2\pi x) + i \sin(2\pi x) \end{aligned}$$

Non è difficile verificare che ψ è un omomorfismo di gruppi, infatti, ricordando che il prodotto di due numeri complessi ha per modulo il prodotto dei moduli e per argomento la somma degli argomenti, si ha:

$$\psi(x+y) = \cos(2\pi(x+y)) + i \sin(2\pi(x+y)) =$$
$$= (\cos(2\pi x) + i \sin(2\pi x))(\cos(2\pi y) + i \sin(2\pi y)) = \psi(x)\psi(y).$$

Il nucleo $\ker \psi = \{x \in \mathbb{R} : \cos(2\pi x) + i \sin(2\pi x) = 1\} = \mathbb{Z}$, l'immagine di ψ è invece data dai numeri complessi $z = \rho(\cos(\vartheta) + i \sin(\vartheta))$ tali che $\rho = 1$, ovvero i numeri complessi di modulo 1.

Esercizio 5. Sia dato il gruppo $(\mathbb{Q}, +)$.

(a) Descrivere il gruppo quoziente $\mathbb{Q}/\mathbb{Z}$.

(b) Calcolare l'ordine di $\frac{2}{7} + \mathbb{Z}$.

(c) Stabilire se $\mathbb{Q}/\mathbb{Z}$ è ciclico.

Soluzione: Sia $q \in \mathbb{Q}$, allora q si può scrivere in modo unico come $q = r + z$ con $z \in \mathbb{Z}$ e $r = 0$ oppure $0 < r = \frac{a}{b} < 1$ e $\gcd(a, b) = 1$. Siano dunque $q_1 = r_1 + z_1$ e $q_2 = r_2 + z_2 \in \mathbb{Q}$, si ha:

$$q_1 + \mathbb{Z} = q_2 + \mathbb{Z} \Leftrightarrow q_1 - q_2 \in \mathbb{Z} \Leftrightarrow (r_1 - r_2) + (z_1 - z_2) \in \mathbb{Z} \Leftrightarrow r_1 = r_2.$$

Dunque $\mathbb{Q}/\mathbb{Z} = \left\{r + \mathbb{Z} : \; r = 0 \; \text{ oppure } \; 0 < r = \frac{a}{b} < 1, \gcd(a, b) = 1\right\}$.

Ogni elemento $\frac{a}{b} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ ha ordine finito, infatti

$$(\frac{a}{b} + \mathbb{Z}) + \overset{b-\text{volte}}{\cdots} + (\frac{a}{b} + \mathbb{Z}) = b\frac{a}{b} + \mathbb{Z} \in \mathbb{Z}.$$

Poiché $\mathbb{Q}/\mathbb{Z}$ ha infiniti elementi ed ognuno di essi ha ordine finito, il gruppo non può essere ciclico.

Esercizio 6. Esibire un esempio di automorfismo non interno.

Soluzione: Sia $G = A_4$ e si consideri il sottogruppo V_4 normale in A_4. Sia $\sigma := (123) \in A_4$ e si denoti con γ_σ l'automorfismo interno di A_4 dato dal coniugio tramite σ. La restrizione $\overline{\gamma} := \gamma_\sigma |_{V_4}$ è certamente un automorfismo di V_4, essendo V_4 normale in A_4. Facciamo vedere che $\overline{\gamma}$ non è l'identità.

Si ha: $\overline{\gamma}((12)(34)) = (123)(12)(34)(132) = (14)(23)$, dunque $\overline{\gamma}$ è un automorfismo di V_4 che non è interno (V_4 è abeliano e ha l'identità come unico automorfismo interno).