A.A. 2015-2016. CORSO DI ALGEBRA 1.
PROFF. P. PIAZZA, E. SPINELLI.
SOLUZIONE ESERCIZI FOGLIO 7.

Esercizio 7. 1. Determinare l'insieme degli omomorfismi da $\mathbb{Z}_{149}$ a $\mathbb{Z}_{27}$.

Soluzione. La soluzione di questo esercizio si riduce sostanzialmente all'applicazione del Teorema di Lagrange e del Teorema Fondamentale di Omomorfismo. Vi proponiamo due metodi per risolverlo.

Metodo 1. Supponiamo che $\varphi : \mathbb{Z}_{149} \to \mathbb{Z}_{27}$ sia un omomorfismo e supponiamo per assurdo che esista un elemento $\overline{k} \in \mathbb{Z}_{149}$ diverso da $\overline{0}$, che viene inviato da φ in una classe resto $\varphi(\overline{k}) \neq \overline{0}$. Ricordiamo che in un gruppo finito G, l'ordine di un elemento $g \in G$, $o(g)$, divide $|\,G\,|$. In particolare $o(\varphi(\overline{k})) = 3$, 9, 27 (escludiamo infatti 1, poiché abbiamo assunto $\varphi(\overline{k}) \neq \overline{0}$). D'altra parte sappiamo che se $\varphi : G \to G'$ è un omomorfismo allora $o(\varphi(g))\,|\,o(g)$ (basta infatti applicare il Teorema Fondamentale di Omomorfismo a $\varphi|_{\langle g\rangle} : \langle g\rangle \to \langle\varphi(g)\rangle$). Osserviamo che 149 non è divisibile per 3 (e dunque non è divisibile per 9, né per 27), ma allora abbiamo un assurdo perché $o(\varphi(g))\,|\,o(g)$ e $o(g)\,|\,|\,G\,|$ e dunque $o(\varphi(g))\,|\,|\,G\,|$. Questo è un assurdo e dunque l'unico omomorfismo $\varphi_{\overline{0}} : \mathbb{Z}_{149} \to \mathbb{Z}_{27}$ è quello che invia ciascun elemento $\overline{k} \in \mathbb{Z}_{149}$ in $\overline{0} \in \mathbb{Z}_{27}$.

Metodo 2. Sia $\varphi : \mathbb{Z}_{149} \to \mathbb{Z}_{27}$ un omomorfismo. Sappiamo dalla teoria che $\ker(\varphi)$ è un sottogruppo normale di $\mathbb{Z}_{149}$. In particolare $|\ker(\varphi)\,|\,|\,149 = |\mathbb{Z}_{149}|$ per il Teorema di Lagrange. Si osservi che 149 è un numero primo e dunque deve risultare $|\ker(\varphi)\,| = 1$ oppure $|\ker(\varphi)\,| = 149$. Se fosse $|\ker(\varphi)| = 1$ l'omomorfismo φ sarebbe iniettivo e quindi, poiché $Im(\varphi) < \mathbb{Z}_{27}$ $149 = |\,Im(\varphi)\,| \leq |\mathbb{Z}_{27}| = 27$; assurdo. Deve quindi risultare $|\ker(\varphi)| = 149$ e dunque $\varphi = \varphi_{\overline{0}}$ ovvero l'omomorfismo banale che invia ciascun elemento di $\mathbb{Z}_{149}$ in $\overline{0}$. $\square$

Esercizio 7. 2. Sia $Pr_6 \subset \mathbb{E}^3$ un prisma retto di altezza 1 e con base esagonale regolare inscritta in una circonferenza di raggio 1 centrata nel punto $(0, 0, -\frac{1}{2})$; supponiamo che le due basi del prisma siano parallele al piano xy e che il segmento che collega il baricentro delle due basi esagonali sia $\{(0, 0, z)\,|\,|z| \leq \frac{1}{2}\}$.
Sia Σ_{Pr_6} il gruppo delle isometrie di $\mathbb{E}^3$ che fissano Pr_6.
(A) Determinare Σ_{Pr_6}.
(B) Esplicitare un omomorfismo $\varphi : \Sigma_{Pr_6} \to D_6$, dove D_6 è il gruppo diedrale per $n = 6$.
(C) Determinare il centro del gruppo Σ_{Pr_6}.

Soluzione. Disegnamo il prisma Pr_6 ed alcune delle sue isometrie:

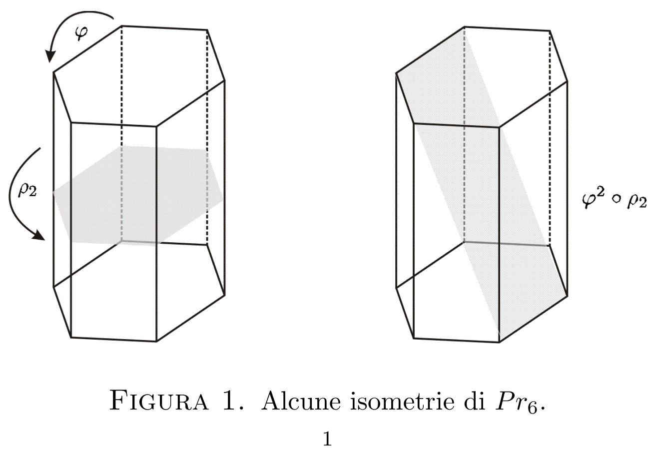

FIGURA 1. Alcune isometrie di Pr_6.

dove con φ si intende la rotazione attorno all'asse z di $\pi/3$, mentre la riflessione ρ_2 è la riflessione rispetto al piano xy (in altre parole, la mappa $(x,y,z) \mapsto (x,y,-z)$).

Ricordiamo che $D_6 = \langle \varphi, \rho \mid \rho^2 = \varphi^6 = 1,\ \rho \circ \varphi^k = \varphi^{6-k} \circ \rho \rangle$ è il gruppo delle isometrie dell'esagono regolare. Osserviamo che ogni isometria dell'esagono regolare $\mathcal{E} = Pr_6 \cap \{(x,y,z) \in \mathbb{E}^3 \mid z = 0\}$ si può estendere ad una isometria di Pr_6 nel modo seguente: sia $\vartheta : \mathcal{E} \to \mathcal{E}$ un'isometria; allora essa può essere estesa a $\Theta(x,y,z) = (\vartheta(x,y), z)$, che è una isometria di Pr_6 (sapete dire perché?). Con piccolo abuso di notazione chiameremo sempre con φ l'estensione ad $\mathbb{E}^3$ della rotazione di $\pi/3$ sul piano xy, mentre denoteremo con ρ_1 la riflessione rispetto al piano xz ovvero l'elemento corrispondente alla riflessione ρ di D_6 (con questo stiamo contestualmente assumendo che la proiezione del prisma sul piano xy sia un esagono regolare che ha una diagonale -e dunque due vertici- sull'asse x).
La mappa Φ_{xy} che associa a $Iso(\mathcal{E}) \ni \vartheta \to \Theta \in Iso(Pr_6)$ è un omomorfismo iniettivo da D_6 in Σ_{Pr_6}. Osserviamo ora che $[\Sigma_{Pr_6} : \Phi_{xy}(D_6)] = 2$: consideriamo infatti un'isometria $\sigma \in \Sigma_{Pr_6}$ in particolare si può considerare $p_{xy} \circ \sigma|_{\mathcal{E}} : \mathcal{E} \to \mathcal{E}$, dove $p_{xy} : \mathbb{E}^3 \to \{(x,y,z) \in \mathbb{E}^3 \mid z = 0\}$ è la proiezione canonica sul piano xy. Questa nuova appicazione associata a σ è un'isometria di $\mathcal{E}$; la ragione è che non vi sono elementi di $Iso(Pr_6)$ che mandano l'asse z in un'altra retta, questo perché altrimenti non sarebbe preservato Pr_6 (verificare); in particolare le restrizioni di σ all'asse z e al piano xy sono anch'esse isometrie. Sia $\pi_{xy} : \Sigma_{Pr_6} \to D_6$ l'applicazione appena definita chiaramente risulta $\pi_{xy} \circ \Phi_{xy} = \mathrm{Id}_{Aut(D_6)}$. Si tratta ora di dimostrare che essa è un omomorfismo suriettivo il cui nucleo è il sottogruppo ciclico di ordine 2 generato dalla trasformazione ρ_2, ovvero la riflessione rispetto al piano xy. La prima osservazione è che se $\pi_{xy}(\sigma) = \mathrm{id}_{\mathcal{E}}$ allora deve risultare che per ogni $(x,y,z) \in Pr_6$ deve risultare $\sigma(x,y,z) = (x,y,z)$ oppure per ogni $(x,y,z) \in Pr_6$ si deve avere $\sigma(x,y,z) = (x,y,-z)$. Questo è una conseguenza diretta del fatto che l'isometria σ preserva l'asse z e dunque si proietta ad una isometria di tale asse che fissa l'origine (verificare) e dunque essa si riduce alla moltiplicazione della terza coordinata per ± 1. Ne segue che la preimmagine tramite π_{xy} di $\mathrm{id}_{\mathcal{E}}$ è effettivamente il sottogruppo $\langle \rho_2 \rangle < \Sigma_{Pr_6}$. La verifica del fatto che π_{xy} sia effettivamente un omomorfismo è lasciata al lettore. Questo risponde alle domande (B) e (C) dell'Esercizio.

Sappiamo che $[\Sigma_{Pr_6} : \Phi_{xy}(D_6)] = 2$. Vogliamo far vedere che $\Sigma_{Pr_6} \simeq D_6 \times \mathbb{Z}_2$. A tal scopo si osservi che che $\Phi_{xy}(D_6)$ commuta con $\langle \rho_2 \rangle$, ma questo è completamente evidente dalla definizione dell'omomorfismo iniettivo Φ_{xy}. L'isomorfismo è dunque dato da $\Phi : D_6 \times \mathbb{Z}_2 \to \Sigma_{Pr_6}$, data da $\Phi(\vartheta, \sigma) = \Phi_{xy}(\vartheta) \circ \Phi_z(\sigma)$ dove $\Phi_z(\overline{0}) = 1_{\Sigma_{Pr_6}}$, $\Phi_z(\overline{1}) = \rho_2$. In particolare ne segue che $\mathcal{Z}(\Sigma_{Pr_6}) = \langle \rho_2 \rangle$.
□

Esercizio 7. 3. Sia K il gruppo di Klein. Individuare quali gruppi di ordine 8 contengono K e quali contengono un sottogruppo isomorfo a $\mathbb{Z}_4$.

Soluzione. Ricordiamo che il gruppo di Klein è il gruppo delle isometrie del rettangolo. Esso può anche essere descritto nel modo seguente: $K = \langle a, b \mid a^2 = b^2 = 1, ab = ba \rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Ricordiamo anche che vi sono solamente 2 gruppi di ordine 4 e 5 gruppi di ordine 8; nello specifico, gli unici due gruppi (a meno di isomorfismi) di ordine 4 sono K e $\mathbb{Z}_4$. I cinque gruppi di ordine 8 sono invece: Q (il gruppo delle unità dei quaternioni), D_4 (ovvero il gruppo delle isometrie del quadrato), $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$ e $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Cominciamo da Q, il gruppo delle unità dei quaternioni. Dallo studio fatto nel Foglio 6 risulta che Q ha 3 sottogruppi di ordine 4, tutti e tre ciclici: $\langle \underline{i} \rangle$, $\langle \underline{j} \rangle$, $\langle \underline{k} \rangle$ (riprendendo la notazione del Foglio 6). In particolare Q non ha sottogruppi isomorfi al gruppo di Klein.

Consideriamo ora $\mathbb{Z}_8$. Si tratta di un gruppo ciclico. Sappiamo dalla teoria che i sottogruppi di un gruppo ciclico sono tutti necessariamente ciclici. In particolare $\mathbb{Z}_8$ ammette un sottogruppo isomorfo a $\mathbb{Z}_4$, ovvero il sottogruppo generato dalla classe resto $\overline{2}$.

Sia ora D_4 il gruppo delle isometrie del quadrato. Ricordiamo che esso può essere presentato nel modo seguente:

$$\langle \varphi, \rho \mid \rho^2 = \varphi^4 = 1,\ \rho \circ \varphi = \varphi^3 \circ \rho \rangle$$

dove ρ rappresenta la riflessione rispetto all'asse x e dove φ è la rotazione di $\frac{\pi}{2}$. Ricordiamo che dal punto di vista insiemistico $D_4 = \{1, \varphi, \varphi^2, \varphi^3, \rho, \rho \circ \varphi, \rho \circ \varphi^2, \rho \circ \varphi^3\}$ dove le prime quattro sono rotazioni e le seconde quattro sono riflessioni. Osserviamo che D_4 ammette sia un gruppo ciclico di ordine 4, ovvero il gruppo generato dalle rotazioni $\langle \varphi \rangle$ che un sottogruppo di Klein $\langle \rho, \varphi^2 \rangle$, ambedue normali in D_4 (verificare che il sottogruppo generato dalla riflessione ρ e dalla rotazione di π, ovvero φ^2, è isomorfo al gruppo di Klein -costruendo esplicitamente un isomorfismo tra tale sottogruppo e K-).

Consideriamo ora il prodotto diretto $\mathbb{Z}_4 \times \mathbb{Z}_2$, ovvero il gruppo delle coppie $(\overline{k}, \overline{h})$ dove la prima coordinata è una classe resto modulo 4 e la seconda una classe resto modulo 2, e dove l'operazione gruppale è costruita coordinata per coordinata partendo dalle operazioni su $\mathbb{Z}_4 \times \mathbb{Z}_2$. Verificate che $\langle(\overline{1}, \overline{0})\rangle$ è un sottogruppo ciclico di ordine 4 e che $\langle(\overline{2}, \overline{0}), (\overline{0}, \overline{1})\rangle$ è invece un sottogruppo isomorfo al gruppo di Klein.

Infine sia $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ il prodotto diretto di 3 copie di $\mathbb{Z}_2$. Cominciamo osservando che tutti gli elementi non banali di tale gruppo hanno ordine 2 (verificate!). In particolare non esistono elementi di ordine 4, e dunque esso non può contenere un sottogruppo isomorfo a $\mathbb{Z}_4$. Invece il gruppo generato da $\langle(\overline{1}, \overline{0}, \overline{0}), (\overline{0}, \overline{1}, \overline{0})\rangle$ è isomorfo al gruppo di Klein (ve ne sono altri? quali?). □

Esercizio 7.4. Sia S_n il gruppo simmetrico su n elementi.
(A) Sia $H < S_n$. Mostrare che H è normale se e soltanto se per ogni trasposizione $(i\,j) \in S_n$ risulta

$$(i\,j)\,H\,(i\,j) = H$$

(B) Sia K il gruppo di Klein. Determinare un omomorfismo iniettivo $\varphi : K \to S_4$. [*Suggerimento. Ragionare sull'ordine degli elementi di* K]
(C) Dimostrare che $\varphi(K)$ è un sottogruppo normale. [*Suggerimento. Utilizzare il punto* (A)]

Soluzione. Partiamo dal punto (A). Si chiedeva di verificare che:

$$H \text{ è normale in } S_n \quad \Leftrightarrow \quad (i\,j)\,H\,(i\,j) = H, \ \ \forall (i\,j) \ \text{ trasposizione in } \ S_n$$

Un verso di questa affermazione è di facile verifica: sia infatti H normale in S_n. Ne segue che per ogni elemento $\gamma \in S_n$ deve risultare $\gamma\,H\,\gamma^{-1} = H$. Osserviamo che le trasposizioni $(i\,j)$ sono elementi di S_n di ordine 2, ovvero sono inverse di sé stesse. Dunque la condizione di normalità per H, in restrizione alle trasposizioni ci da la condizione: $(i\,j)\,H\,(i\,j)$.

Dimostriamo ora $(\Leftarrow)$. Ricordiamo che ciascuna permutazione $\gamma \in S_n$ può essere scritta come prodotto di cicli disgiunti: sia $\gamma = \sigma_1^\gamma \cdots \sigma_{m_\gamma}^\gamma$ una scirttura di γ come prodotto di cicli disgiunti. Sappiamo inoltre (Appunti di Algebra 1, T. Campanella, Capitolo 4, §3, Osservazione 2. (ii)) che ciascun ciclo può essere espresso come prodotto di trasposizioni, scriviamo quindi $\sigma_j^\gamma = \tau_1^{j,\gamma} \cdots \tau_{\ell_{j,\gamma}}^{j,\gamma}$. Ciascun elemento $\gamma \in S_n$ ammette quindi una scrittura del tipo seguente:

$$\gamma = (\tau_1^{\gamma,1} \cdots \tau_{\ell_{\gamma,1}}^{\gamma,1}) \cdot (\tau_1^{\gamma,2} \cdots \tau_{\ell_{\gamma,2}}^{\gamma,2}) \cdots (\tau_1^{\gamma,m_\gamma} \cdots \tau_{\ell_{\gamma,m_\gamma}}^{\gamma,m_\gamma})$$

possiamo cioè scrivere ciascun elemento $\gamma \in S_n$ come prodotto di trasposizioni. Si osservi ora che data la precedente espressione per γ è molto semplice ottenere un'espressione di γ^{-1} come prodotto di trasposizioni:

$$\gamma^{-1} = (\tau_{\ell_{\gamma,m_\gamma}}^{\gamma,m_\gamma} \cdots \tau_1^{\gamma,m_\gamma}) \cdots (\tau_{\ell_{\gamma,1}}^{\gamma,1} \cdots \tau_1^{\gamma,1})$$

Siamo quindi nelle condizioni di mostrare l'implicazione $(\Leftarrow)$: sia γ un elemento di S_n, scriviamo γ e γ^{-1} come prodotto di trasposizioni come mostrato in precedenza; allora:

$$\gamma H \gamma^{-1} = (\tau_1^{\gamma,1} \cdots \tau_{\ell_{\gamma,1}}^{\gamma,1}) \cdots (\tau_1^{\gamma,m_\gamma} \cdots \tau_{\ell_{\gamma,m_\gamma}}^{\gamma,m_\gamma}) H (\tau_{\ell_{\gamma,m_\gamma}}^{\gamma,m_\gamma} \cdots \tau_1^{\gamma,m_\gamma}) \cdots (\tau_{\ell_{\gamma,1}}^{\gamma,1} \cdots \tau_1^{\gamma,1})$$

Utilizzando quindi la prorietà $(i\,j)\,H\,(i\,j) = H$, per ogni trasposizione $(i\,j)$ possiamo concludere.

Nel punto (B) si chiede invece di individuare un sottogruppo di S_4 isomorfo al gruppo di Klein (già protagonista dell'esercizio 7.3). Ricordiamo che il gruppo di Klein è $\mathbb{Z}_2 \times \mathbb{Z}_2$ ed i suoi elementi hanno tutti ordine 2. Sappiamo (*Appunti di Algebra 1*, T. Campanella, Capitolo 4, §3, Proposizione 2. (ii)) che l'ordine di una permutazione $\gamma \in S_n$ è il minimo comune multiplo degli ordini dei cicli che compaiono nella sua scomposizione in cicli disgiunti. In particolare un elemento $\gamma \in S_n$ può avere ordine 2 se e solo se è una trasposizione oppure è un prodotto di trasposizioni disgiunte. Nel caso particolare di S_4 dunque gli elementi di ordine 2 sono solamente i seguenti:

- *Cicli di ordine* 2 *(trasposizioni):* $(1\,2)$, $(1\,3)$, $(1\,4)$, $(2\,3)$, $(2\,4)$, $(3\,4)$.
- *Prodotti di cicli di ordine* 2 *disgiunti:* $(1\,2)\,(3\,4)$, $(1\,3)\,(2\,4)$, $(1\,4)\,(2\,3)$.

Osserviamo inoltre che valgono le relazioni seguenti:

$$(1\,2)\,(3\,4)\cdot(1\,3)\,(2\,4) = (1\,4)\,(2\,3) = (1\,3)\,(2\,4)\cdot(1\,2)\,(3\,4)$$

Ne deduciamo che il sottogruppo generato dai prodotti di cicli di ordine 2 disgiunti è isomorfo al gruppo di Klein: $K \simeq \langle(1\,2)\,(3\,4),(1\,3)\,(2\,4)\rangle$. Sottolineamo che da un punto di vista insiemistico abbiamo:

$$\langle(1\,2)\,(3\,4),(1\,3)\,(2\,4)\rangle = \{(1),\,(1\,2)\,(3\,4),(1\,3)\,(2\,4),(1\,4)\,(2\,3)\}$$

Per dimostrare che il sottogruppo in questione è normale in S_4 si può procedere in due modi: il primo è utilizzando il punto (A) e verificare che coniugando ciascuno degli elementi non banali del sottogruppo per una qualsiasi trasposizione rimaniamo nel sottogruppo (verificando cioè a mano che $(i\,j)\,\langle(1\,2)\,(3\,4),(1\,3)\,(2\,4)\rangle\,(i\,j) = \langle(1\,2)\,(3\,4),(1\,3)\,(2\,4)\rangle$, qualsiasi sia la trasposizione $(i\,j)$). Il secondo metodo invece è il seguente. Sappiamo che dato un gruppo generico l'ordine di un elemento è invariante per coniugio, ovvero se G è un gruppo finito e $g \in G$ allora $o(g) = o(hgh^{-1})$, qualsiasi sia $h \in G$. D'altra parte per i gruppi simmetrici abbiamo un'altra caratteristica che rimane invariata per coniugio, la parità del numero di trasposizioni che occorrono per scrivere un elemento: sia $\gamma \in G$ e sia $\gamma = \tau_1 \cdots \tau_m$ una scrittura di γ come prodotto di trasposizioni allora la parità del numero m è ben definita e non dipende dalla particolare scrittura; questo implica in particolare che la parità di tale numero è preservata per coniugio, sia infatti $\gamma_0 = \tau_1^0 \cdots \tau_n^0$ una scrittura come prodotto di trasposizioni di un altro elemento di S_n allora $\gamma_0\,\gamma, \gamma_0^{-1} = \tau_1^0 \cdots \tau_n^0 \cdot \tau_1 \cdots \tau_m \cdot \tau_n^0 \cdots \tau_1^0$ pertanto la parità di $\gamma_0\,\gamma\,\gamma_0^{-1}$ è quella di $2n+m$ che ha la stessa parità di m.
Da tale discussione risulta chiaro che $\langle(1\,2)\,(3\,4),(1\,3)\,(2\,4)\rangle$ è normale in S_4. Ciascun elemento $\gamma \in S_4$ deve infatti mandare ciascun elemento non banale di tale sottogruppo in un elemento di ordine 2 che possa essere scritto con un numero pari di trasposizioni, ovvero deve inviare ciascun elemento non banale del sottogruppo in uno dei seguenti tre elementi: $(1\,2)\,(3\,4)$, $(1\,3)\,(2\,4)$, $(1\,4)\,(2\,3)$. Ne segue che il sottogruppo in questione è normale. $\square$

Esercizio 7.5. Sia $(G,\cdot)$ un gruppo finito.
(A) Sia g un elemento di G. Verificare che la formula $\iota_g(h) = g\,h\,g^{-1}$ definisce un automorfismo del gruppo G. [*Nota.* Gli automorfismi di questo tipo sono detti "automorfismi interni"]
(B) Verificare che l'applicazione $\mathcal{I}_G : G \to Aut(G)$, $\mathcal{I}_G :\, g \mapsto \iota_g$, dove $\iota_g(h) = g\,h\,g^{-1}$, è un omomorfismo di gruppi il cui nucleo è il centro del gruppo G.
(C) Sia $\varphi \in Aut(G)$. Trovare un' espressione per $\varphi \circ \iota_g \circ \varphi^{-1}$ come automorfismo interno; dedurre che $Out(G) = Aut(G)/\mathcal{I}_G(G)$ è un gruppo. [*Nota.* Tale gruppo è noto come gruppo degli "automorfismi esterni" del gruppo G]
(D) Esibire una coppia (φ, G) dove G è un gruppo finito e φ è un automorfismo di G tale che $\pi(\varphi) \neq \mathrm{Id}_{Out(G)}$ dove $\pi : Aut(G) \to Aut(G)/\mathcal{I}_G(G)$ è l'omomorfismo dato dal passaggio al quoziente.
(E) Determinare il gruppo degli automorfismi interni del gruppo delle unità dei quaternioni, Q, e del gruppo simmetrico su 3 elementi S_3.

Soluzione. Cominciamo dal punto (A). Viene chiesto di verificare che l'applicazione $\iota_g : G \to G$ definita da $\iota_g(h) = g\,h\,g^{-1}$ definisce un automorfismo di G. Per verificare questo fatto bisogna far vedere che ι_g è un omomorfismo biiettivo la cui inversa sia ancora un omomorfismo. Iniziamo verificando che ι_g è un omomorfismo

$$\iota_g(h_1\,h_2) = g\,h_1\,h_2\,g^{-1} = g\,h_1\,(g^{-1}\,g)\,h_2\,g^{-1} = (g\,h_1\,g^{-1})\,(g\,h_2\,g^{-1}) = \iota_g(h_1)\,\iota_g(h_2)$$

Per quanto riguarda l'inversa osserviamo che l'omomorfismo $\iota_{g^{-1}}$ è l'applicazione inversa di ι_g (verificate) e questo conclude (A).

Nel punto (B) si vuole dimostrare che $\mathcal{I}_G : G \to Aut(G)$ definita da $\mathcal{I}_G(g) = \iota_g$ è un omomorfismo. A tal scopo ci basta dimostrare che $\mathcal{I}_G(g_1\, g_2) = \mathcal{I}_G(g_1) \circ \mathcal{I}_G(g_2)$:

$$\iota_{g_1\, g_2}(g) = (g_1\, g_2)\, g\, (g_1\, g_2)^{-1} = g_1\, (g_2\, g\, g_2^{-1})\, g_1^{-1} = \iota_{g_1}(\iota_{g_2}(g)) = (\iota_{g_1} \circ \iota_{g_2})(g)$$

Questo dimostra che $\mathcal{I}_G$ è un omomorfismo. Andiamo ora a studiare il nucleo dell'omomorfismo $\mathcal{I}_G$. $\mathcal{I}_G(g) = \iota_g = \mathrm{Id}_G$ se e soltanto se $g\, h\, g^{-1} = \iota_g(h) = h$, $\forall h \in G$ se e soltanto se $g\, h = h\, g$ $\forall h \in G$ se e soltanto se $g \in \mathcal{Z}(G)$.

Nel punto (C) si chiede, dato un automorfismo $\varphi \in Aut(G)$ di esplicitare l'automorfismo interno cui corrisponde la composizione $\varphi \circ \iota_g \circ \varphi^{-1}$:

$$(\varphi \circ \iota_g \circ \varphi^{-1})(h) = \varphi(\iota_g(\varphi^{-1}(h))) = \varphi(g\, \varphi^{-1}(h)\, g^{-1}) = \varphi(g)\, h\, \varphi(g^{-1}) = \iota_{\varphi(g)}(h)$$

Questo rapido conto in particolare dimostra che il sottogruppo $\mathcal{I}_G(G) = Inn(G) < Aut(G)$ è in realtà un sottogruppo normale del gruppo degli automorfismi. Il gruppo quoziente $Out(G) = Aut(G)/Inn(G)$ è detto gruppo degli automorfismi esterni.

Per rispondere al punto (D) bisogna esibire un esempio di un gruppo G e di un automorfismo φ che non è un automorfismo interno. L'esempio più semplice è il seguente: si prenda come gruppo il gruppo di Klein $K \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ e si consideri l'automorfismo dato da $\varphi(\overline{1}, \overline{0}) = (\overline{0}, \overline{1})$ e $\varphi(\overline{0}, \overline{1}) = (\overline{1}, \overline{0})$, $\varphi(\overline{1}, \overline{1}) = (\overline{1}, \overline{1})$. Essendo il gruppo di Klein commutativo ne segue che non esistono automorfismi interni. In particolare $Aut(K) = Out(K)$ e dunque l'automorfismo sopra definito è un automorfismo di K che non è un automorfismo interno.

Nell'ultimo punto, il punto (E), veniva chiesto di determinare il gruppo degli automorfismi interni del gruppo delle unità dei quaternioni, Q, e di S_3. Per quanto riguarda il primo, segue dallo studio fatto nel Foglio 6, che $\mathcal{Z}(Q) \simeq \mathbb{Z}_2$ e che $Q/\mathcal{Z}(Q) \simeq K \simeq \langle \iota_{\underline{i}}, \iota_{\underline{j}} \rangle$ (dove abbiamo utilizzato le notazioni del Foglio 6 per gli elementi di Q). Per quanto riguarda il gruppo simmetrico S_3 osserviamo che $\mathcal{Z}(S_3) = \mathrm{id}_{S_3}$ e dunque l'omomorfismo $\mathcal{I}_{S_3} : S_3 \to Inn(S_3) < Aut(S_3)$ è un isomorfismo sull'immagine e dunque $Inn(S_3) = \langle \iota_{(1\,2)}, \iota_{(2\,3)}, \iota_{(1\,3)} \rangle$. In particolare S_3 è un sottogruppo di $Aut(S_3)$. $\square$