

ESERCIZI SU
**GRUPPI, MORFISMI,
 SOTTOGRUPPI NORMALI E QUOZIENTI**

N.B.: il simbolo $\hat{\diamond}$ contrassegna gli esercizi (relativamente) più complessi.

— * —

1 — Verificare quali delle applicazioni da (a) a (e) siano dei morfismi (cioè rispettino le operazioni), e se lo sono se ne determini il nucleo e l'immagine.

- (a) $\varphi : (\mathbb{Z} \times \mathbb{Z}; +) \longrightarrow (\mathbb{C}; +)$, $(x, y) \mapsto x + iy$,
- (b) $\varphi : (\mathbb{R} \times \mathbb{R}; +) \longrightarrow (\mathbb{R} \times \mathbb{R}; +)$, $(x, y) \mapsto (x - y, x + y)$,
- (c) $\varphi : (\mathbb{C}; +) \longrightarrow (\mathbb{C}; +)$, $x + iy \mapsto x - iy$,
- (d) $\varphi : (\mathbb{R}^3; +) \longrightarrow (\mathbb{R}^3; +)$, $(x, y, z) \mapsto (x, x + y, x + y + z)$,
- (e) $\varphi : (\mathbb{R}^2 \times \mathbb{Z} \times \mathbb{C}^3; +) \longrightarrow (\mathbb{R} \times \mathbb{Z} \times \mathbb{C}^2; +)$,
 $((r_1, r_2), z, (c_1, c_2, c_3)) \mapsto (2r_1 - r_2, -3z, c_3 - 2c_1, c_2 + 4c_1 - 2c_3)$.

2 — Siano G_1 e G_2 due gruppi finiti. In ciascuna delle seguenti ipotesi

- (a) $|G_1| = 41$, $|G_2| = 12$
- (b) $|G_1| = 20$, $|G_2| = 50$
- (c) $|G_1| = 36$, $|G_2| = 54$

può esistere un morfismo $\phi : G_1 \longrightarrow G_2$ non banale (cioè non tale che $\phi(g) = 1 \ \forall g \in G_1$)? E può un tale morfismo essere iniettivo? Oppure suriettivo? In generale, quali sono le condizioni su $|G_1|$ e $|G_2|$ perché un tale morfismo possa esistere?

3 — Si consideri l'insieme $V_4 := \{1, i, j, k\}$ dotato dell'operazione (indicata moltiplicativamente) definita da

$$\begin{aligned} 1 \cdot 1 = 1 = 1 \cdot 1 \ , \quad 1 \cdot i = i = i \cdot 1 \ , \quad 1 \cdot j = j = j \cdot 1 \ , \quad 1 \cdot k = k = k \cdot 1 \\ i \cdot j = k = j \cdot i \ , \quad j \cdot k = i = k \cdot j \ , \quad k \cdot i = j = i \cdot k \ , \quad 1 \cdot k = k = k \cdot 1 \\ i^2 = 1 \ , \quad j^2 = 1 \ , \quad k^2 = 1 \end{aligned}$$

Dimostrare che:

- (a) V_4 con tale operazione è un gruppo abeliano — detto *gruppo di Klein*;
- (b) il gruppo V_4 è isomorfo al gruppo $(\mathbb{Z}_2^2 := \mathbb{Z}_2 \times \mathbb{Z}_2; +)$ — prodotto diretto di $(\mathbb{Z}_2; +)$ con sé stesso.

Suggerimento: Si possono dimostrare entrambi gli enunciati direttamente. In alternativa, la parte (a) segue subito dalla parte (b), nel senso che basta dimostrare che il gruppoide V_4 sia isomorfo a $(\mathbb{Z}_2^2; +)$, perché quest'ultimo è un gruppo e qualunque gruppoide isomorfo a un gruppo è a sua volta un gruppo.

4 — Determinare tutti i possibili morfismi dal gruppo di Klein V_4 al gruppo $(\mathcal{S}_3; \circ)$.

5 — Determinare tutti i possibili morfismi dal gruppo $(\mathcal{S}_3; \circ)$ al gruppo di Klein V_4 .

6 — Determinare tutti i possibili morfismi dal gruppo di Klein V_4 al gruppo $(\mathbb{Z}_4; +)$.

7 — Determinare tutti i gruppi G omomorfi a $\mathbb{Z}_4$, cioè tali che esista un epimorfismo $\varphi: \mathbb{Z}_4 \longrightarrow G$.

8 — Si consideri l'insieme $Q := \{1, -1, i, -i, j, -j, k, -k\}$ dotato dell'operazione (indicata moltiplicativamente) definita sinteticamente da

$$1 \cdot x = x = x \cdot 1, \quad (-x) \cdot y = -(x \cdot y) = x \cdot (-y), \quad z^2 = -1, \quad \forall x, y \in Q, z \in Q \setminus \{\pm 1\}$$

$$i \cdot j = k, \quad j \cdot k = i, \quad k \cdot i = j$$

Dimostrare che Q con tale operazione è un gruppo — detto *gruppo dei quaternioni*.

9 — Determinare tutti i morfismi dal gruppo di Klein V_4 al gruppo dei quaternioni Q .

10 — Determinare tutti i morfismi dal gruppo dei quaternioni Q al gruppo di Klein V_4 .

11 — Dimostrare che $(\mathbb{Q}; +)$ non è isomorfo a $(\mathbb{Q} \setminus \{0\}; \cdot)$.

Suggerimento: Basta dimostrare che in uno dei due gruppi vale una qualche proprietà — ad esempio, una certa identità tra formule, magari per certi elementi particolari — che certamente non vale invece nell'altro gruppo...

12 — Sia $n \in (2\mathbb{N}_+ + 1)$ un numero naturale dispari. Poniamo $x * y := \sqrt[n]{x^n + y^n}$ per ogni $x, y \in \mathbb{R}$. Verificare che $(\mathbb{R}; *)$ è un gruppo isomorfo a $(\mathbb{R}; +)$.

Suggerimento: Non si richiede una dimostrazione diretta; basta invece verificare che certe proprietà dei numeri reali e delle loro potenze con esponente dispari (che assumiamo come note), quando riformulate nel linguaggio dei gruppi, ci dicono che una certa applicazione da $\mathbb{R}$ a $\mathbb{R}$ è in effetti un isomorfismo dal gruppoide $(\mathbb{R}; *)$ al gruppoide $(\mathbb{R}; +)$. Come conseguenza, siccome il secondo gruppoide è un gruppo, allora lo è anche il primo.

13 — Sia $(G; \cdot)$ un gruppo finito, e siano $g_1, \dots, g_k \in G$ con $k \geq |G|$. Dimostrare che esistono indici $p, \dots, q \in \{0, 1, \dots, k\}$ con $p < q$ tali che $g_{p+1} g_{p+2} \cdots g_{q-1} g_q = 1_G$.

14 — Calcolare i gruppi di automorfismi $\text{Aut}(\mathbb{Z}_6; +)$, $\text{Aut}(\mathbb{Z}_8; +)$, $\text{Aut}(\mathbb{Z}_{11}; +)$ e $\text{Aut}(\mathbb{Z}; +)$.

Suggerimento: Si osservi che i gruppi $(\mathbb{Z}_n; +)$ — con $n \in \{6, 8, 11\}$ — e $(\mathbb{Z}; +)$ sono tutti ciclici, quindi un automorfismo è univocamente determinato dall'immagine di un generatore (e per generatore possiamo prendere sempre $[1]_n$ o 1).

15 — Dimostrare che $\text{Aut}(V_4; \circ) \cong \mathcal{S}_3$.

Suggerimento: Si osservi che ogni automorfismo ϕ di V_4 fissa (cioè manda in sé stesso) l'elemento neutro 1 ; pertanto ϕ stesso è univocamente determinato dalla sua restrizione al sottoinsieme $\{i, j, k\}$ di V_4 . Si dimostri poi che questo definisce in effetti una applicazione da $\text{Aut}(V_4; \circ)$ a $(\mathcal{S}_3; \circ)$, e che questa è un isomorfismo di gruppi.

16 — Dimostrare che $\text{Aut}(\mathcal{S}_3; \circ) \cong \mathcal{S}_3$.

Suggerimento: Si può ottenere da un calcolo diretto, oppure passando per il morfismo di gruppi $\Gamma: \mathcal{S}_3 \longrightarrow \text{Aut}(\mathcal{S}_3; \circ)$ che associa ad ogni $\sigma \in \mathcal{S}_3$ l'automorfismo interno $\gamma_\sigma (x \mapsto \sigma x \sigma^{-1})$, osservando poi che Γ è in effetti un isomorfismo.

17 — Sia $\{G_i\}_{i \in I}$ una famiglia di gruppi, indicizzata da un insieme I . Il corrispondente prodotto cartesiano $\prod_{i \in I} G_i$ è allora un gruppo — detto “prodotto diretto dei G_i ” — per l'operazione $(g'_i)_{i \in I} + (g''_i)_{i \in I} := (g'_i g''_i)_{i \in I}$.

Per ogni $i \in I$ sia dato un sottoinsieme $S_i \subseteq G_i$; si definisca allora

$$\prod_{i \in I} G_i^{(S)} := \left\{ (g_i)_{i \in I} \in \prod_{i \in I} G_i \mid g_i \in S_i, \forall i \in I \right\}$$

Dimostrare che:

(a) se ogni S_i è sottogruppo di G_i ($i \in I$), allora $\prod_{i \in I} G_i^{(S)}$ è sottogruppo di $\prod_{i \in I} G_i$, ed è isomorfo al prodotto diretto $\prod_{i \in I} S_i$ dei gruppi S_i ($i \in I$) — tra di loro;

(b) se ogni S_i è sottogruppo normale di G_i ($i \in I$), allora $\prod_{i \in I} G_i^{(S)}$ è sottogruppo normale di $\prod_{i \in I} G_i$, e il corrispondente gruppo quoziente $\prod_{i \in I} G_i / \prod_{i \in I} G_i^{(S)}$ è isomorfo al prodotto diretto $\prod_{i \in I} (G_i / S_i)$ dei vari gruppi quoziente G_i / S_i ($i \in I$);

(c) per ogni $j \in I$, la funzione $\pi_j: \prod_{i \in I} G_i \longrightarrow G_j ((g_i)_{i \in I} \mapsto g_j)$, è un epimorfismo;

(d) per ogni $j \in I$, la funzione $\eta_j : G_j \longrightarrow \bigtimes_{i \in I} G_i$ ($g \mapsto (g_i)_{i \in I}$) data da $g_j := g$ e $g_i := e_{G_i}$ per ogni $i \in I \setminus \{j\}$, è un monomorfismo, la cui immagine è un sottogruppo normale di $\bigtimes_{i \in I} G_i$.

Suggerimento: Per evitare confusioni fuorvianti, si cominci considerando il caso in cui l'insieme I sia di soli due o tre indici, dunque studiamo il prodotto diretto di due o tre anelli... Tutto quel che c'è da capire, si manifesta già in questo caso semplice.

18  Teorema Cinese del Resto (per Gruppi) — Sia G un gruppo e sia $\{H_i\}_{i \in I}$ una famiglia di sottogruppi di G . Dimostrare che:

(a) esistono immersioni “canoniche”

$$j_s : G / \bigcap_{i \in I} H_i \hookrightarrow \bigtimes_{i \in I} G / H_i \quad , \quad g \left(\bigcap_{i \in I} H_i \right) \mapsto (g H_i)_{i \in I}$$

$$j_d : \bigcap_{i \in I} H_i \backslash G \hookrightarrow \bigtimes_{i \in I} H_i \backslash G \quad , \quad \left(\bigcap_{i \in I} H_i \right) g \mapsto (H_i g)_{i \in I}$$

(cioè, le su descritte funzioni sono effettivamente ben definite...);

(b) se $H_i \trianglelefteq G$ per ogni $i \in I$, allora j_s e j_d coincidono e sono morfismi di gruppi.

19 — Dimostrare che la “relazione” di “essere sottogruppo di” (tra gruppi) è “transitiva”, cioè, dati tre gruppi H, G, K , si ha $H \leq G, G \leq K \implies H \leq K$.

20 — Dimostrare che la “relazione” di “essere sottogruppo normale di” (tra gruppi) non è “transitiva”, cioè, dati tre gruppi H, G, K , in generale si ha

$$H \trianglelefteq G, G \trianglelefteq K \not\Rightarrow H \trianglelefteq K$$

Suggerimento: Basta di trovare tre gruppi H, G e K t.c. $H \trianglelefteq G$ e $G \trianglelefteq K$ ma $H \not\trianglelefteq K$.

21 — Sia G un gruppo, $H \leq G$ e $K \trianglelefteq G$. Dimostrare che $(H \cap K) \trianglelefteq H$.

22 — Siano H e K due sottogruppi normali di un gruppo G tali che $H \cap K = \{1\}$. Dimostrare che:

(a) $hk = kh$ per ogni $h \in H, k \in K$;

(b) $HK := \{hk \mid h \in H, k \in K\} = KH$ è sottogruppo normale di G .

Suggerimento: Si riscriva hk nella forma $hk = hkh^{-1}h$ e si ricordi che $H \trianglelefteq G$; analogamente si faccia per kh . Quindi...

23 — Siano H e K due sottogruppi di un gruppo G tali che $HK = KH$. Dimostrare che $HK = KH$ è il sottogruppo di G generato da $H \cup K$.

24 — Sia G un gruppo, $H \leq G$ e $N \trianglelefteq G$. Dimostrare che $HN = NH$.

25 — Sia G un gruppo, sia $\{N_i\}_{i \in I}$ una famiglia di sottogruppi normali di G , e sia $\langle \bigcup_{i \in I} N_i \rangle$ il sottogruppo di G generato da $\bigcup_{i \in I} N_i$. Dimostrare che $\langle \bigcup_{i \in I} N_i \rangle \trianglelefteq G$.

26 — Per un qualsiasi gruppo G , definiamo i sottoinsiemi

$$Z(G) := \{z \in G \mid zg = gz, \forall g \in G\} \quad (=: \text{“centro di } G\text{”})$$

$$C_G(g) := \{x \in G \mid xg = gx\} \quad (=: \text{“centralizzante di } g\text{”}) \quad \forall g \in G$$

Dimostrare che:

$$(a) \quad Z(G) = \bigcap_{g \in G} C_G(g) ;$$

$$(b) \quad C_G(g) \leq G \quad \text{per ogni } g \in G ;$$

$$(c) \quad Z(G) \trianglelefteq G .$$

Suggerimento: Tutto segue direttamente dalle definizioni. Inoltre, la parte (c) si può ottenere anche come conseguenza immediata delle parti (a) e (b) insieme.

27 — Sia G un gruppo, e $H \leq Z(G)$, dove $Z(G)$ indica il centro di G . Dimostrare che $H \trianglelefteq G$, e inoltre che, se il gruppo quoziente G/H è ciclico, allora G è abeliano.

28 — Siano G un gruppo e H un sottogruppo di G . Definiamo poi

$$C_G(H) := \{x \in G \mid xh = hx \forall h \in H\} , \quad N_G(H) := \{x \in G \mid xH = Hx\} .$$

Dimostrare che:

$$(a) \quad C_G(H) \leq H , \quad N_G(H) \leq G , \quad H \trianglelefteq N_G(H) ;$$

$$(b) \quad \text{se } H \trianglelefteq K \leq G, \text{ allora } K \subseteq N_G(H) ;$$

$$(c) \quad H \trianglelefteq G \iff N_G(H) = G ;$$

$$(d) \quad \text{per ogni } \phi \in \text{Aut}(G) \text{ si ha } H \trianglelefteq G \iff \phi(H) \trianglelefteq G ;$$

$$(e) \quad \text{dato } \alpha \in \text{Aut}(G) \text{ tale che } \alpha(H) = H, \text{ si ha}$$

$$\alpha(C_G(H)) = C_G(H) \quad \text{e} \quad \alpha(N_G(H)) = N_G(H) .$$

29 — Sia G un gruppo qualsiasi. Per ogni $g \in G$, sia $\gamma_g : G \longrightarrow G$ l'applicazione definita da $\gamma_g(x) := gxg^{-1}$, per ogni $x \in G$. Dimostrare che:

(a) $\gamma_g \in \text{Aut}(G)$, cioè γ_g è un automorfismo di G , per ogni $g \in G$ (detto “automorfismo interno” associato a g);

(b) $\text{Int}(G) := \{\gamma_g \mid g \in G\} \trianglelefteq \text{Aut}(G)$, cioè $\text{Int}(G)$ è sottogruppo normale di $\text{Aut}(G)$;

(c) l'applicazione $\Gamma : G \longrightarrow \text{Aut}(G)$ è un morfismo di gruppi;

(d) il nucleo del morfismo $\Gamma : G \longrightarrow \text{Aut}(G)$ è $\text{Ker}(\Gamma) = Z(G)$.

30 — Sia G un gruppo, e $H \trianglelefteq G$ con $|H| = 2$. Dimostrare che $H \subseteq Z(G)$.

Suggerimento: Si analizzi l'effetto degli operatori $\gamma_g : G \longrightarrow G \ (x \mapsto g x g^{-1})$ — per ogni $g \in G$ — sul sottogruppo H ...

31 — Sia G un gruppo, e $H \leq G$ con $(G : H) = 2$. Dimostrare che $H \trianglelefteq G$.

Suggerimento: L'ipotesi $(G : H) = 2$ significa che il sottogruppo H ha due classi laterali sinistre e due classi laterali destre; in entrambi i casi, una di queste due classi è la classe laterale (sinistra o destra, rispettivamente) dell'elemento neutro del gruppo $e_G \in G$: in formule, abbiamo $G/H = \{\kappa_1, \kappa_2\}$ e $H \backslash G = \{c_1, c_2\}$ con $\kappa_1 = e_G H$, $\kappa_2 = \gamma H$, e $c_1 = H e_G$, $c_2 = H \ell$. Inoltre, le classi laterali di H (sinistre o destre, rispettivamente) formano una partizione di G , quindi è $G = \kappa_1 \dot{\cup} \kappa_2$ e $G = c_1 \dot{\cup} c_2$, da cui segue che $\kappa_2 = G \setminus \kappa_1$ e $c_2 = G \setminus c_1$. Infine, le classi laterali sinistra e destra di H coincidono entrambe con H stesso, e da questo (e da quanto già visto) possiamo concludere che $\kappa_1 = H = c_1$ e $\kappa_2 = G \setminus H = c_2$. Dunque $gH = Hg$ per ogni $g \in G$, cioè $H \trianglelefteq G$.

32 — Per un qualsiasi gruppo G , consideriamo gli elementi $(g, h) := g h g^{-1} h^{-1}$ — per ogni $g, h \in G$ — e il sottogruppo da essi generato in G , cioè

$$G' := \left\langle \{ (g, h) := g h g^{-1} h^{-1} \mid g, h \in G \} \right\rangle \quad (=: \text{“sottogruppo derivato” di } G)$$

Dimostrare che:

- (a) $G' \trianglelefteq G$;
- (b) G è abeliano $\iff G' = \{1_G\}$.

33 — Sia $N := \{ \text{id}, (12)(34), (13)(24), (14)(23) \}$ ($\subseteq \mathcal{S}_4$). Dimostrare che:

- (a) $N \trianglelefteq \mathcal{S}_4$;
- (b) $\hat{\cong} \mathcal{S}_4 / N \cong \mathcal{S}_3$.

Suggerimento: La parte (a) si può ottenere con un calcolo diretto. Per la parte (b), cerchiamo un isomorfismo da $\mathcal{S}_4 / N$ a $\mathcal{S}_3$; siccome il primo è un gruppo quoziente, un tale isomorfismo ci sarebbe dato dal Teorema Fondamentale di Omomorfismo se troviamo un morfismo $\varphi : \mathcal{S}_4 \longrightarrow \mathcal{S}_3$ che abbia immagine $\mathcal{S}_3$ (cioè sia suriettivo) e nucleo N — da cui quindi seguirà anche la parte (a). Per trovare un tale φ , si può procedere seguendo questo schema:

— [1] siccome ogni morfismo manda un elemento di ordine n in un elemento di ordine un divisore di n , e poiché ogni permutazione ciclica di lunghezza n ha ordine n , dobbiamo avere che $\varphi((ab))$, risp. $\varphi((abc))$, risp. $\varphi((abcd))$, dev'essere una permutazione di

ordine 1 oppure 2, risp. 1 oppure 3, risp. 1 oppure 2 oppure 4: ma quest'ultimo caso va scartato, perché non esistono elementi di ordine 4 in $\mathcal{S}_3$...

— [2] siccome dev'essere $\text{Ker}(\varphi) = N$, abbiamo $\varphi((ab)) \neq \text{id}$ — per ogni a, b tali che $a \neq b$ — perché $(ab) \notin N$; in particolare $\varphi((ab))$ non ha ordine 1, quindi (vedi sopra) ha ordine 2, dunque è della forma $\varphi((ab)) = (xy)$ per qualche $x, y \in \{1, 2, 3\}$, $x \neq y$;

— [3] sempre perché $\text{Ker}(\varphi) = N$, abbiamo il vincolo che $\varphi((ab)(cd)) = \text{id}$ — per ogni a, b, c, d tali che $\{a, b, c, d\} = \{1, 2, 3, 4\}$ — che a sua volta significa che $\varphi((ab)) = \varphi((cd))^{-1} = \varphi((cd)^{-1}) = \varphi((cd))$;

— [4] dai punti [2] e [3] abbiamo $\varphi((12)) = \varphi((34)) = (x_1 y_1)$, $\varphi((13)) = \varphi((24)) = (x_2 y_2)$, $\varphi((23)) = \varphi((14)) = (x_3 y_3)$ con $x_i \neq y_i$; inoltre, $(x_1 y_1)$, $(x_2 y_2)$ e $(x_3 y_3)$ sono tre permutazioni differenti in quanto $\varphi((12)) \neq \varphi((13))$, risp. $\varphi((13)) \neq \varphi((23))$, risp. $\varphi((23)) \neq \varphi((12))$, in quanto $(12)(13)^{-1} = (12)(13) \notin N = \text{Ker}(\varphi)$, risp. $(13)(23)^{-1} = (13)(23) \notin N = \text{Ker}(\varphi)$, risp. $(23)(12)^{-1} = (23)(12) \notin N = \text{Ker}(\varphi)$;

— [5] a questo punto facciamo una scelta per $(x_i y_i)$ — con $i \in \{1, 2, 3\}$ — ponendo $\varphi((12)) := (12)$, $\varphi((13)) := (13)$, $\varphi((23)) := (23)$; da questa premessa otteniamo un'unica possibilità per il valore di φ sulle altre permutazioni: infatti, poniamo $\varphi((34)) := (12)$, $\varphi((24)) := (13)$, $\varphi((14)) := (23)$ per il punto [3], $\varphi((ab)(cd)) := \text{id}$ per avere $\text{Ker}(\varphi) = N$, e poi per le restanti permutazioni — che sono tutte cicliche di ordine 3 oppure 4 — usiamo la condizione che φ sia un morfismo: così ad esempio definiamo

$$\varphi((134)) = \varphi((14)(13)) := \varphi((14))\varphi((13)) = (23)(13) = (123)$$

$$\varphi((1234)) = \varphi((14)(13)(12)) := \varphi((14))\varphi((13))\varphi((12)) = (23)(13)(12) = (13)$$

questo permette effettivamente di definire φ su tutto $\mathcal{S}_4$ perché tale gruppo è generato dal sottoinsieme $\{(ab) \mid a \neq b\}$ e per quest'ultimo i valori di φ sono già assegnati una volta scelte le tre permutazioni $(x_i y_i) \in \mathcal{S}_3$.

N.B.: con scelte diverse della terna ordinata $((x_i y_i))_{i=1,2,3}$ di permutazioni in $\mathcal{S}_3$ si trovano diversi morfismi φ che tutti soddisfano le nostre richieste; in totale ci sono $3! = 6$ diverse possibilità, e quindi abbiamo esattamente 6 diversi isomorfismi da $\mathcal{S}_4/N$ a $\mathcal{S}_3$.

34 — Dato un insieme E , per ogni $F \subseteq E$ consideriamo i sottoinsiemi di $\mathcal{S}(E)$ dati da

$$G_F := \{ \sigma \in \mathcal{S}(E) \mid \sigma(F) = F \} \quad , \quad G_{(F)} := \{ \nu \in \mathcal{S}(E) \mid \nu(f) = f, \quad \forall f \in F \}$$

e anche la relazione $\sim$ in G_F definita da

$$\sigma' \sim \sigma'' \iff \sigma' \Big|_F = \sigma'' \Big|_F \quad \forall \sigma', \sigma'' \in \mathcal{S}(E)$$

dove $\sigma \Big|_F$ come sempre indica la restrizione di $\sigma \in \mathcal{S}(E)$ al sottoinsieme F .

Dimostrare che:

(a) la relazione $\sim$ è un'equivalenza in G_F ;

- (b) $(G_F; \circ)$ è sottogruppo di $(\mathcal{S}(E); \circ)$;
- (c) la relazione $\sim$ è compatibile con l'operazione " $\circ$ " in G_F ;
- (d) il gruppo quoziente $G_F / \sim$ è isomorfo al gruppo di permutazioni $(\mathcal{S}(F); \circ)$;
- (e) $G_{(F)}$ è sottogruppo normale di G_F ;
- (f) il gruppo quoziente $G_F / G_{(F)}$ è isomorfo al gruppo di permutazioni $(\mathcal{S}(F); \circ)$;
- (g) $\sim = \rho_d^{G_{(F)}}$ dove $\rho_d^{G_{(F)}}$ è la relazione destra in G_F canonicamente associata a $G_{(F)}$;
- (h) $\sim = \rho_s^{G_{(F)}}$ dove $\rho_s^{G_{(F)}}$ è la relazione sinistra in G_F canonicamente associata a $G_{(F)}$;
- (i) l'applicazione $\mathcal{R}_F : G_F \longrightarrow \mathcal{S}(F)$, $\sigma \mapsto \mathcal{R}_F(\sigma) := \sigma|_F$, è suriettiva;
- (j) la relazione $\sim$ è l'equivalenza in G_F canonicamente associata all'applicazione $\mathcal{R}_F$;
- (k) l'applicazione $\mathcal{R}_F : G_F \longrightarrow \mathcal{S}(F)$, $\sigma \mapsto \mathcal{R}_F(\sigma) := \sigma|_F$, è un epimorfismo dal gruppo $(G_F; \circ)$ al gruppo $(\mathcal{S}(F); \circ)$.

Suggerimento: L'enunciato è molto ridondante, e la sua dimostrazione si può semplificare di molto. La linea più semplice da seguire può essere questa che sintetizziamo. I punti (b) e (i) sono sostanzialmente indipendenti, e si possono dimostrare per primi. Per il resto, si cominci dimostrando (j), che implica (a); poi si dimostri parte del (k) — precisamente, il fatto che $\mathcal{R}_F$ sia un morfismo (il fatto che sia “epi-” segue dal punto (i)! — che insieme a (j) implica (c); a questo punto, dimostrando il punto (g) — oppure il punto (h) — ne consegue automaticamente anche il punto (h) — oppure il punto (g), rispettivamente — e il punto (e), e anche il fatto che i punti (d) ed (f) sono equivalenti, perché i gruppi quoziente di cui si parla coincidono (sono soltanto scritti usando notazioni diverse). Infine questi due enunciati (d) ed (f) — che sono appunto equivalenti — si ottengono dal Teorema Fondamentale di Omomorfismo applicato all'epimorfismo di gruppi $\mathcal{R}_F : G_F \longrightarrow \mathcal{S}(F)$.

35 $\hat{\mathbb{Z}}$ — Sia $\mathbb{K} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\} \cup \{\mathbb{Z}_p\}_{p \text{ primo}}$, o più in generale sia $\mathbb{K}$ un qualsiasi campo. Si consideri $\mathbb{P}_{\mathbb{K}} := \mathbb{K} \cup \{\infty\}$ e sia $\mathcal{G}_{\mathbb{P}_{\mathbb{K}}}$ il sottogruppo del gruppo $(\mathcal{S}(\mathbb{P}_{\mathbb{K}}); \circ)$ di tutte le permutazioni di $\mathbb{P}_{\mathbb{K}}$ definito da

$$\mathcal{G}_{\mathbb{P}_{\mathbb{K}}} := \left\{ f \in \mathbb{P}_{\mathbb{K}}^{\mathbb{P}_{\mathbb{K}}} \mid \exists a, b, c, d \in \mathbb{K} : ad - bc \neq 0 \in \mathbb{K}, f(x) = \frac{ax + b}{cx + d} \quad \forall x \in \mathbb{P}_{\mathbb{K}} \right\}$$

Dimostrare che $\mathcal{G}_{\mathbb{P}_{\mathbb{K}}}$ è isomorfo al gruppo quoziente $GL_2(\mathbb{K}) / \mathbb{K}^* I_2$, dove I_2 è la matrice identità 2×2 e $\mathbb{K}^* I_2 := \{\kappa I_2 \mid \kappa \in \mathbb{K}^* := \mathbb{K} \setminus \{0\}\}$ è sottogruppo centrale (e quindi normale) di $GL_2(\mathbb{K})$.

Suggerimento: Basterà trovare un isomorfismo $\phi : GL_2(\mathbb{K}) / \mathbb{K}^* I_2 \xrightarrow{\cong} \mathcal{G}_{\mathbb{P}_{\mathbb{K}}}$. A sua volta, questo sarà indotto dal Teorema Fondamentale di Omomorfismo come $\phi = \varphi_*$ dove $\varphi : GL_2(\mathbb{K}) \xrightarrow{\cong} \mathcal{G}_{\mathbb{P}_{\mathbb{K}}}$ sia un epimorfismo con nucleo $\text{Ker}(\varphi) = \mathbb{K}^* I_2$. Per trovare un

tale φ , si noti che bisogna associare a ogni $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{K})$ una permutazione di $\mathbb{P}_{\mathbb{K}}$ scelta tra quelle in $\mathcal{G}_{\mathbb{P}_{\mathbb{K}}}$...

36 $\hat{\Rightarrow}$ — Sia $\phi : G \longrightarrow G'$ un morfismo di gruppi. Dimostrare che:

- (a) $\phi(1_G) = 1_{G'}$;
- (b) $\phi(g^{-1}) = \phi(g)^{-1}$ per ogni $g \in G$;
- (c) per ogni $H \leq G$ si ha $\phi(H) \leq G'$, con $\phi(H) \subseteq \text{Im}(\phi) := \phi(G)$; in particolare, si ha sempre $\text{Im}(\phi) = \phi(G) \leq G'$;
- (d) per ogni $H \trianglelefteq G$ si ha $\phi(H) \trianglelefteq \text{Im}(\phi) = \phi(G)$, ma in generale $\phi(H) \not\trianglelefteq G'$;
- (e) per ogni $H' \leq G'$ si ha $\phi^{-1}(H') \leq G$, con $\phi^{-1}(H') \supseteq \text{Ker}(\phi) := \phi^{-1}(1_{G'})$;
- (f) per ogni $H' \leq G'$ tale che $(H' \cap \text{Im}(\phi)) \trianglelefteq \text{Im}(\phi)$ si ha $\phi^{-1}(H') \trianglelefteq G$; in particolare, $\text{Ker}(\phi) := \phi^{-1}(1_{G'}) \trianglelefteq G$;
- (g) per ogni $H \leq G$ si ha $\phi^{-1}(\phi(H)) = H \text{Ker}(\phi) = \text{Ker}(\phi) H$;
- (h) per ogni $H' \leq G'$ si ha $\phi(\phi^{-1}(H')) = H' \cap \text{Im}(\phi) = \text{Im}(\phi) \cap H'$;
- (i) le applicazioni $H \mapsto \phi(H)$ e $H' \mapsto \phi^{-1}(H')$ dall'insieme dei sottogruppi di G all'insieme dei sottogruppi di G' si restringono a biiezioni $\mathcal{S}_G^{\text{Ker}(\phi)} \xrightarrow{\quad} \mathcal{S}_{G', \text{Im}(\phi)}$ e $\mathcal{S}_G^{\text{Ker}(\phi)} \xleftarrow{\quad} \mathcal{S}_{G', \text{Im}(\phi)}$ — dove poniamo $\mathcal{S}_G^{\text{Ker}(\phi)} := \{ H \leq G \mid H \supseteq \text{Ker}(\phi) \}$ e $\mathcal{S}_{G', \text{Im}(\phi)} := \{ H' \leq G' \mid H' \subseteq \text{Im}(\phi) \}$ — che sono inverse l'una dell'altra.

Suggerimento: L'enunciato è lungo ma non (realmente) difficile. Le parti (a) e (b) sono elementari, basta ricordare alcune proprietà specifiche dell'elemento neutro e dell'inverso in un gruppo. Per il resto, si possono utilizzare vari risultati considerati in precedenza. Infine, si noti che la parte (i) è sostanzialmente una riformulazione di quanto già enunciato nelle parti precedenti.

37 — Dato un gruppo G , siano

$$\lambda : G \hookrightarrow \mathcal{S}(G), \quad g \mapsto \lambda_g \left(\begin{array}{c} G \xrightarrow{\quad} G \\ x \mapsto \lambda_g(x) := g x \end{array} \right)$$

$$\rho : G \hookrightarrow \mathcal{S}(G), \quad g \mapsto \rho_g \left(\begin{array}{c} G \xrightarrow{\quad} G \\ x \mapsto \rho_g(x) := x g^{-1} \end{array} \right)$$

i monomorfismi di gruppi dati dal Teorema di Cayley (per gruppi), e si ponga

$$\lambda(G) := \text{Im}(\lambda), \quad \rho(G) := \text{Im}(\rho).$$

Si considerino poi

$$C(\lambda(G)) := \{ \sigma \in \mathcal{S}(G) \mid \sigma \circ \lambda_g = \lambda_g \circ \sigma, \quad \forall g \in G \}$$

$$C(\rho(G)) := \{ \tau \in \mathcal{S}(G) \mid \tau \circ \rho_g = \rho_g \circ \tau, \quad \forall g \in G \}.$$

Dimostrare che

$$C(\lambda(G)) = \rho(G) \quad , \quad C(\rho(G)) = \lambda(G) \quad .$$

38 — Dato un morfismo di anelli $\phi : R \longrightarrow A$, dimostrare che la funzione associata

$$G_n(\phi) : GL_n(R) \longrightarrow GL_n(A) \quad , \quad (r_{i,j}) \mapsto G_n(\phi)\left((r_{i,j})\right) := (\phi(r_{i,j}))$$

è un morfismo di gruppi. Inoltre, si dimostri che:

- (a) per $\phi = id_A$ si ha $G_n(id_A) = id_{GL_n(A)}$;
- (b) se $\psi : A \longrightarrow T$ è un analogo morfismo, si ha $G_n(\psi \circ \phi) = G_n(\psi) \circ G_n(\phi)$.

39 $\hat{\mathbb{Z}}$ — Sia $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\} \cup \{\mathbb{Z}_n\}_{n \in \mathbb{N}}$, o più in generale sia $\mathbb{A}$ un qualsiasi anello unitario. Dato $n \in \mathbb{N}_+$, sia $GL_n(\mathbb{A})$ l'usuale gruppo delle matrici $n \times n$ invertibili a coefficienti in $\mathbb{A}$. Consideriamo in esso i sottoinsiemi

$$\begin{aligned} S_n(\mathbb{A}) &:= \{ (m_{i,j})_{i=1,\dots,n}^{j=1,\dots,n} \in GL_n(\mathbb{A}) \mid m_{i,j} = \delta_{i,j} \alpha, \forall i \neq j, \alpha \in U(\mathbb{A}) \} \\ D_n(\mathbb{A}) &:= \{ (m_{i,j})_{i=1,\dots,n}^{j=1,\dots,n} \in GL_n(\mathbb{A}) \mid m_{i,j} = 0, \forall i \neq j \} \\ T_n^+(\mathbb{A}) &:= \{ (m_{i,j})_{i=1,\dots,n}^{j=1,\dots,n} \in GL_n(\mathbb{A}) \mid m_{i,j} = 0, \forall i > j \} \\ T_n^-(\mathbb{A}) &:= \{ (m_{i,j})_{i=1,\dots,n}^{j=1,\dots,n} \in GL_n(\mathbb{A}) \mid m_{i,j} = 0, \forall i < j \} \\ U_n^\pm(\mathbb{A}) &:= \{ (u_{i,j})_{i=1,\dots,n}^{j=1,\dots,n} \in T_n^\pm(\mathbb{A}) \mid u_{k,k} = 1, \forall k \} \end{aligned}$$

Inoltre, *soltanto per il caso in cui l'anello $\mathbb{A}$ sia commutativo* — come nel caso di $\mathbb{A} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\} \cup \{\mathbb{Z}_n\}_{n \in \mathbb{N}}$ — consideriamo anche il sottoinsieme

$$SL_n(\mathbb{A}) := \{ (m_{i,j})_{i=1,\dots,n}^{j=1,\dots,n} \in GL_n(\mathbb{A}) \mid \det((m_{i,j})_{i=1,\dots,n}^{j=1,\dots,n}) = 1 \}$$

Dimostrare che:

- (a) $\hat{\mathbb{Z}}$ tutti questi sottoinsiemi sono sottogruppi di $GL_n(\mathbb{A})$;
- (b) $\hat{\mathbb{Z}}$ $S_n(\mathbb{A}) = Z(GL_n(\mathbb{A}))$;
- (c) $D_n(\mathbb{A}) \leq T_n^\pm(\mathbb{A})$ ma $D_n(\mathbb{A}) \not\leq T_n^\pm(\mathbb{A})$;
- (d) $T_n^\pm(\mathbb{A}) \leq GL_n(\mathbb{A})$ ma $T_n^\pm(\mathbb{A}) \not\leq GL_n(\mathbb{A})$;
- (e) $U_n^+(\mathbb{A}) \leq T_n^+(\mathbb{A})$ e $U_n^-(\mathbb{A}) \leq T_n^-(\mathbb{A})$;
- (f) il gruppo quoziente $T_n^\pm(\mathbb{A}) / U_n^\pm(\mathbb{A})$ è isomorfo al gruppo $D_n(\mathbb{A})$;
- (g) $SL_n(\mathbb{A}) \leq GL_n$ (nel caso in cui l'anello $\mathbb{A}$ sia commutativo);
- (h) il gruppo quoziente $GL_n(\mathbb{A}) / SL_n$ è isomorfo al gruppo $U(\mathbb{A})$ (nel caso in cui l'anello $\mathbb{A}$ sia commutativo).

Suggerimento: Si consideri prima il caso $n = 2$, nel quale già si verificano tutti i fenomeni significativi. Da questo si può anche dedurre il caso generale, osservando che GL_2 si immerge come sottogruppo in GL_n tramite un monomorfismo che manda una matrice (invertibile) 2×2 in una matrice (invertibile) $n \times n$ ottenuta inserendo nell'angolo in alto a sinistra la matrice 2×2 assegnata, inserendo tanti "1" nelle posizioni diagonali rimaste libere e tanti "0" in tutte le altre posizioni non ancora riempite. In breve, si lavori con matrici a blocchi di forma $\left(\begin{array}{c|c} 2 \times 2 & 2 \times (n-2) \\ \hline (n-2) \times 2 & (n-2) \times (n-2) \end{array} \right)$.

Per la parte (a), la cosa delicata è dimostrare che per una matrice triangolare (superiore o inferiore) con coefficienti sulla diagonale invertibili esiste la matrice inversa e quest'ultima è a sua volta triangolare (dello stesso tipo). Si analizzi prima il caso $n = 2$, e poi si osservi che si può procedere per induzione, dove nel passaggio da n a $n+1$ una matrice (quadrata) di ordine $n+1$ si scompone come matrice a blocchi i cui blocchi siano di taglia $n \times n$ (in alto a sinistra), $1 \times n$ (in alto a destra), $n \times 1$ (in basso a sinistra) e 1×1 (in basso a destra).

Le parti (e) e (f) si possono ottenere osservando che l'applicazione $T_n^\pm(\mathbb{A}) \longrightarrow D_n(\mathbb{A})$ data da $(m_{i,j})_{i=1,\dots,n}^{j=1,\dots,n} \mapsto (\delta_{i,j} m_{i,j})_{i=1,\dots,n}^{j=1,\dots,n}$ è un epimorfismo (in breve, "estrae la diagonale" da una matrice triangolare), con $U_n^\pm(\mathbb{A})$ come nucleo; questo ci dà (e), e inoltre anche (f) applicando il Teorema Fondamentale di Omomorfismo.

Le parti (g) ed (h) seguono dall'osservazione che la ben nota applicazione "determinante" $\det : GL_n^\pm(\mathbb{A}) \longrightarrow U(\mathbb{A})$ è un epimorfismo (per il Teorema di Binet), il cui nucleo è esattamente $SL_n^\pm(\mathbb{A})$; questo ci dà (g), e a seguire anche (h) applicando il Teorema Fondamentale di Omomorfismo.