Istituzioni di Algebra e Geometria — Algebra, a.a. 2024-2025

Soluzioni foglio 3

1.

(a),(b) Per la caratterizzazione di sottogruppo generato da (tre) elementi, ogni elemento di Q_8 è un prodotto finito di i, j, k; quindi per dimostrare che $Q_8 = \{-1, -i, -j, -k, 1, i, j, k\}$ è sufficiente controllare tutte le uguaglianze della parte (b), che sono di verifica immediata.

$$\begin{cases} (\pm 1)^2 = 1, \\ (\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1, \\ ij = k = -ij, \qquad jk = i = -kj, \qquad ij = -k = -ji, \\ ijk = -1, \end{cases}$$

(c) Le uguaglianze elencate sopra mostrano che 1 ha ordine 1, -1 ha ordine 2 e tutti gli altri elementi hanno ordine 4.

(d) Ovviamente abbiamo i sottogruppi impropri $\{1\}$ (che è l'unico sottogruppo che contiene un unico elemento) e Q_8 stesso.

Per il Teorema di Lagrange, i sottogruppi propri di Q_8 possono contenere o 2 o 4 elementi. Guardiamo i possibili sottogruppi che contengono 2 elementi: tra questi c'è sicuramente $G_1 = \{1, -1\}$. In realtà non ce ne sono altri! Infatti qualsiasi sottogruppo di Q_8 che contiene 2 elementi deve contenere l'1 e un altro elemento. Ora, se quest'altro elemento è ad esempio i, si vede subito che l'insieme $\{1, i\}$ non è chiuso rispetto al prodotto, perché non contiene $i^2 = -1$, quindi non può essere un sottogruppo. Ripetendo lo stesso ragionamento arriviamo alla conclusione che l'unico sottogruppo di Q_8 con 2 elementi è G_1.

Per finire, guardiamo i sottogruppi di 4 elementi. Ci sono $G_2 = \{\pm 1, \pm i\}$, $G_3 = \{\pm 1, \pm j\}$, e $G_4 = \{\pm 1, \pm j\}$. Con un ragionamento simile a quello precedente, concludiamo che non ce ne possono essere altri.

2. Usiamo la notazione moltiplicativa per G, e usiamo il criterio per sottogruppi. Se gli H_i sono sottogruppi di G allora intanto $H = \bigcap_{i \in I} H_i$ è non vuoto, perché contiene l'elemento neutro di G. Inoltre, se $a, b \in H = \bigcap_{i \in I} H_i$, allora $a, b \in H_i$ per ogni $i \in I$, dunque $ab^{-1} \in H_i$ per ogni $i \in I$, e quindi $ab^{-1} \in \bigcap_{i \in I} H_i = H$.

3. (a) Un elemento $x \in \varphi^{-1}(H' \cap K')$ se e solo se esiste $y \in H' \cap K'$ tale che $\varphi(x) = y$. Poiché $y \in H' \cap K'$, in particolare $y \in H'$, e quindi $x \in \varphi^{-1}(H')$, e $y \in K'$, e quindi $x \in \varphi^{-1}(K')$. Concludiamo che $x \in \varphi^{-1}(H') \cap \varphi^{-1}(K')$. Viceversa, se $x \in \varphi^{-1}(H') \cap \varphi^{-1}(K')$ allora abbiamo che $x \in \varphi^{-1}(H')$, e quindi esiste $y \in H'$ tale che $\varphi(x) = y$, e $x \in \varphi^{-1}(K')$, e quindi esiste $z \in K'$ tale che $\varphi(x) = z$, ma allora necessariamente $y = z \in H' \cap K'$, e quindi $x \in \varphi^{-1}(H' \cap K')$.

Poiché $H', K' \subseteq H' \vee K'$, segue che:

$$\varphi^{-1}(H' \vee K') \supseteq \varphi^{-1}(H'), \varphi^{-1}(K').$$

A lezione abbiamo dimostrato che la retroimmagine di un sottogruppo è ancora un sottogruppo, in particolare quindi $\varphi^{-1}(H' \vee K')$ è un sottogruppo di G, e come tale deve contenere il più piccolo sottogruppo contenente $\varphi^{-1}(H')$ e $\varphi^{-1}(K')$, cioè

$$\varphi^{-1}(H' \vee K') \supseteq \varphi^{-1}(H') \vee \varphi^{-1}(K').$$

(b) Un elemento $y \in \varphi(H \cap K)$ se e solo se esiste $x \in H \cap K$ tale che $\varphi(x) = y$. Poiché $x \in H \cap K$, in particolare $x \in H$, e quindi $y \in \varphi(H)$, e $x \in K$, e quindi $y \in \varphi(K)$. Concludiamo che $y \in \varphi(H) \cap \varphi(K)$.

Di nuovo, $H, K \subseteq H \vee K$, e quindi

$$\varphi(H \vee K) \supseteq \varphi(H) \vee \varphi(K).$$

Per l'inclusione opposta, sia $g' \in \varphi(H \vee K)$: allora esiste $g = \prod_{i=1}^{n} h_i k_i \in H \vee K$ tale che $\varphi(g) = g'$. Poiché φ è un omomorfismo segue allora che

$$g' = \varphi(g) = \varphi\left(\prod_{i=1}^{n} h_i k_i\right) = \prod_{i=1}^{n} \varphi(h_i)\varphi(k_i) \in \varphi(H) \vee \varphi(K),$$

per cui $\varphi(H \vee K) \subseteq \varphi(H) \vee \varphi(K)$, e quindi vale l'uguaglianza.

(c) Prendiamo l'applicazione $\psi\colon (\mathbb{R}^2, +) \to (\mathbb{R}^2, +)$ definita da $(x, y) \mapsto x + y$. È facile verificare che ψ è un omomorfismo suriettivo di gruppi. Definiamo

$$H = \{(x, 0) \mid x \in \mathbb{R}\}, \qquad K = \{(0, y) \mid y \in \mathbb{R}\},$$

che sono entrambi sottogruppi di $(\mathbb{R}^2, +)$ (verificatelo!). Abbiamo che $H \cap K = \{(0, 0)\}$, quindi necessariamente $\psi(H \cap K) = \{0\}$. Inoltre $\psi(H) = \psi(K) = \mathbb{R}$, quindi in questo caso $\psi(H) \cap \psi(K) = \mathbb{R} \not\subseteq \{0\} = \psi(H \cap K)$.

Prendiamo l'applicazione $\varphi\colon (\mathbb{R}, +) \to (\mathbb{R}^2, +)$ definita da $a \mapsto (a, 0)$. Anche in questo caso, è facile verificare che φ è un omomorfismo iniettivo di gruppi. Definiamo

$$H' = \{(b, b) \mid b \in \mathbb{R}\}, \qquad K' = \{(c, -c) \mid c \in \mathbb{R}\},$$

che sono entrambi sottogruppi di $(\mathbb{R}^2, +)$ (verificatelo!). Abbiamo che

$$H' \cap \mathrm{Im}(\varphi) = K' \cap \mathrm{Im}(\varphi) = \{(0, 0)\},$$

quindi le retroimmagini $\varphi^{-1}(H')$ e $\varphi^{-1}(K')$ sono entrambe uguali a $\{0\}$, e lo stesso vale per il loro sottogruppo unione: $\varphi^{-1}(H') \vee \varphi^{-1}(K') = \{0\}$. D'altra parte, $H' \vee K' = \mathbb{R}^2$, quindi $\varphi^{-1}(H' \vee K') = \mathbb{R} \not\subseteq \{0\} = \varphi^{-1}(H') \vee \varphi^{-1}(K')$.

4. (a) Se $H \subseteq K$ (rispettivamente $K \subseteq H$), allora $H \cup K = K$ (risp. $H \cup K = H$) è banalmente un sottogruppo. Viceversa, supponiamo che $H \not\subseteq K$ e $K \not\subseteq H$: allora esistono elementi $h \in H \setminus K$ e $k \in K \setminus H$. Se $H \cup K$ fosse un sottogruppo dovrebbe essere chiuso rispetto all'operazione in G (che indicheremo col prodotto): in particolare si dovrebbe avere $hk \in H \cup K$. Poiché sia H che K sono sottogruppi deduciamo allora che se $hk \in H$, allora $k = h^{-1}(hk) \in H$, mentre se $hk \in K$, allora $(hk)k^{-1} \in K$: in entrambi i casi si ha una contraddizione. Concludiamo che se $H \not\subseteq K$ e $K \not\subseteq H$, allora $H \cup K$ non è un sottogruppo perché non è moltiplicativamente chiuso in G.

   (b) Ricordiamo la descrizione del sottogruppo unione

$$H \vee K = \{ \prod_{i=1}^{n} h_i k_i \mid h_i \in H,\ k_i \in K \ \},$$

   e che per definizione $<H \cup K>$ è l'intersezione di tutti i sottogruppi di G contenenti sia H che K. Ovviamente ogni elemento in $H \vee K$ è contenuto in ogni sottogruppo di G contenente sia H che K: in particolare ogni elemento di $H \vee K$ appartiene a $<H \cup K>$, cioè $H \vee K \subseteq <H \cup K>$. Viceversa, l'elemento neutro $1_G \in H \cap K$, dunque $h \cdot 1_G \in H \vee K$ e $1_G \cdot k \in H \vee K$ per ogni $h \in H$ e $k \in K$, quindi $H \vee K$ è un sottogruppo di G contenente sia H che K: deduciamo allora che $H \vee K \supseteq <H \cup K>$.

   (c) L'osservazione deriva direttamente dal fatto che G è un gruppo, in particolare un sottogruppo di se stesso: nella parte (a) abbiamo visto che l'unione può essere un sottogruppo se e solo se uno dei due insiemi è contenuto nell'altro, cioè o $G = H \subseteq K$, oppure $H \subseteq K = G$. D'altra parte, se $H < G$ è un sottogruppo proprio, $G \not\subseteq H$, quindi l'unica possibilità è che $H \subseteq K = G$.

5. Ricordiamo che, per un qualsiasi $x \in G$, se k è tale che $x^k = 1_G$, allora k è un multiplo di $\mathrm{ord}(x)$.

   Chiamiamo per semplicità $n = \mathrm{ord}(a)$; per definizione allora $a^n = 1_G$.

   Verifichiamo che $\mathrm{ord}(a^{-1}) = n$. Da $(a^n)^{-1} = (a^{-1})^n$ deduciamo $(a^{-1})^n = 1_G$, quindi n è divisibile per l'ordine di a^{-1}. Poiché $(a^{-1})^{-1} = a$ segue che l'ordine di a^{-1} è divisibile per n, perciò $\mathrm{ord}(a^{-1}) = n$.

   Verifichiamo che $\mathrm{ord}(b^{-1}ab) = n$. Poiché

$$(b^{-1}ab)^n = (b^{-1}ab)(b^{-1}ab)\dots(b^{-1}ab) = b^{-1}a(bb^{-1})a(b\dots b^{-1})ab = b^{-1}a^n b = 1_G$$

   deduciamo che n è divisibile per l'ordine di $b^{-1}ab$. Posto $c = b^{-1}$ abbiamo che $a = c^{-1}(b^{-1}ab)c$: chiaramente $\mathrm{ord}(c^{-1}(b^{-1}ab)c) = \mathrm{ord}(a) = n$. Scambiando a e b con $b^{-1}ab$ e c nel ragionamento precedente, ricaviamo che l'ordine di $b^{-1}ab$ è divisibile per n, perciò $\mathrm{ord}(b^{-1}ab) = n$.

   Verifichiamo che $\mathrm{ord}(ab) = \mathrm{ord}(ba)$. Poiché $ab = b^{-1}(ba)b$, la tesi segue da quanto visto sopra.

6. Ricordiamo che, per un qualsiasi $x \in G$, se k è tale che $x^k = 1_G$, allora k è un multiplo di $\mathrm{ord}(x)$.

   Siano

$$u = \mathrm{ord}(g), \qquad v = \mathrm{ord}(g), \qquad w = \mathrm{ord}(g,h), \qquad m = \mathrm{mcm}(u,v).$$

Poiché $m = \lambda u = \mu v$, allora

$$(g,h)^m = (g^{\lambda u}, h^{\mu v}) = (1_G, 1_H).$$

Deduciamo che m è divisibile per w, quindi $w \leq m$. D'altra parte

$$(1_G, 1_H) = (g,h)^w = (g^w, h^w),$$

quindi $g^w = 1_G$ in G e $h^w = 1_H$ in H. Ciò significa che w è divisibile sia per u che per v, dunque è divisibile per m, quindi $m \leq w$. Possiamo quindi concludere che $m = w$.

7. (a) Osserviamo che $a^m = b^m = 1_G$, per la definizione di m. Poiché G è abeliano risulta allora

$$(ab)^m = abab\ldots ab = a^m b^m = 1_G.$$

   (b) Il fatto che $\mathrm{ord}(ab) | m$ segue immediatamente dalla parte (a). Per costruire un esempio in cui non vale l'uguaglianza, prendiamo in $\mathbb{Z}_{12}$ gli elementi 2 e 4. È facile vedere che $\mathrm{ord}(2) = 6$ e $\mathrm{ord}(4) = 3$, perché

$$6 \cdot 2 \equiv 0 \pmod{12}, \qquad 3 \cdot 4 \equiv 0 \pmod{12}$$

   (attenzione, qui stiamo usando la notazione additiva!) e non esistono interi minori con la stessa proprietà. D'altra parte $6 = \mathrm{mcm}(3,6)$ non è l'ordine di $2+4=6$ in $\mathbb{Z}_{12}$: $\mathrm{ord}(6) = 2$.

   (c) Siano $u = \mathrm{ord}(a)$, $v = \mathrm{ord}(b)$, e quindi $m = uv$. Sia $w = \mathrm{ord}(ab)$: si ha

$$1_G = (ab)^{uw} = a^{uw} b^{uw} = b^{uw},$$

   quindi v divide uw: poiché u e v sono coprimi, allora v divide w. In maniera simile si dimostra che anche u divide w. Dal fatto che u e v sono coprimi si deduce facilmente che $uv \leq w$. Poiché la disuguaglianza inversa è ovvia, concludiamo che $uv = w$.

   (d) Usiamo il criterio per sottogruppi: siano $a, b \in T(G)$, e sia $m = \mathrm{mcm}(\mathrm{ord}(a), \mathrm{ord}(b))$. Allora (di nuovo poiché G è abeliano) risulta:

$$(ab^{-1})^m = a^m (b^{-1})^m = 1_g (b^m)^{-1} = 1_G,$$

   cioè ab^{-1} ha ordine finito, e quindi $ab^{-1} \in T(G)$.

8. (a) Osserviamo che $M_a^2 = I_2$ ma $M_a \neq I_2$, quindi $\mathrm{ord}(M_a) = 2$: in particolare $M_a \in T(\mathrm{GL}_2(\mathbb{R}))$. Però

$$M_a M_b = \begin{pmatrix} ab^{-1} & 0 \\ 0 & a^{-1}b \end{pmatrix},$$

   da cui otteniamo che

$$(M_a M_b)^N = \begin{pmatrix} a^N b^{-N} & 0 \\ 0 & a^{-N} b^N \end{pmatrix}$$

   Non è difficile vedere che, per una scelta sufficientemente generale di a e b (quale?), l'elemento $M_a M_b$ non ha ordine finito, cioè $T(\mathrm{GL}_2(\mathbb{R}))$ non è moltiplicativamente chiuso: in particolare, non è un sottogruppo di $\mathrm{GL}_2(\mathbb{R})$.

(b) Chiaramente $M_a \neq I_2$. Dalla parte (a), se $n = 1$ risulta $\mathrm{ord}(M_a) = 2$. La stessa cosa accade se $n \geq 2$ e $a = 1$. Supponiamo che $n \geq 2$ e $a \neq 1$: in tal caso

$$M_a^2 = \begin{pmatrix} a^{n-1} & 0 \\ 0 & a^{n-1} \end{pmatrix}$$

quindi nessuna potenza pari di M_a può essere la matrice identica. Similmente si verifica (lascio a voi) che nessuna potenza dispari di M_a può essere la matrice identica. Anche il caso $n = 0$ si verifica nello stesso modo.

(c) Abbiamo appena dimostrato che le matrici

$$M_a = \begin{pmatrix} 0 & a \\ a^{-1} & 0 \end{pmatrix}$$

hanno tutte ordine 2, ma il prodotto di due di esse non ha ordine 2. Quindi l'insieme degli elementi di ordine al più 2 di $\mathrm{GL}_2(\mathbb{R})$ non è un sottogruppo.

9. (a) Il sottoinsieme $D \neq \emptyset$ è un sottogruppo; usando il criterio infatti, dati due elementi

$$A = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix}, \qquad B = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix},$$

abbiamo che

$$AB^{-1} = \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \begin{pmatrix} b_1^{-1} & 0 \\ 0 & b_2^{-1} \end{pmatrix} = \begin{pmatrix} a_1 b_1^{-1} & 0 \\ 0 & a_2 b_2^{-1} \end{pmatrix} \in D.$$

Consideriamo adesso l'applicazione $\varphi\colon D \to \mathbb{R}^* \times \mathbb{R}^*$ che manda un elemento $A \in D$ come sopra nella coppia $(a_1, a_2) \in \mathbb{R}^* \times \mathbb{R}^*$. Abbiamo che

$$\varphi(AB) = \varphi \begin{pmatrix} a_1 b_1 & 0 \\ 0 & a_2 b_2 \end{pmatrix} = (a_1 b_1, a_2 b_2) = \varphi \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \varphi \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix} = \varphi(A)\varphi(B),$$

cioè φ è un omomorfismo, ed è facile vedere che è biettivo, e quindi un isomorfismo.

(b) Stiamo cercando le matrici P tali che esiste $A \in D$ per cui $PAP^{-1} \notin D$. Se

$$P = \begin{pmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{pmatrix},$$

allora

$$P \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} P^{-1} = \frac{1}{\det(P)} \begin{pmatrix} a_1 p_{11} p_{22} - a_2 p_{12} p_{21} & (a_2 - a_1) p_{11} p_{12} \\ (a_1 - a_2) p_{21} p_{22} & a_2 p_{11} p_{22} - a_1 p_{12} p_{21} \end{pmatrix},$$

e quindi le matrici P cercate sono tutte e sole quelle per cui o $p_{11}p_{12} \neq 0$, o $p_{21}p_{22} \neq 0$.

10. Per definizione, φ è un omomorfismo se e solo se per ogni scelta di $g, h \in G$ si ha

$$ghgh = (gh)^2 = \varphi(gh) = \varphi(g)\varphi(h) = g^2h^2 = gghh.$$

Moltiplicando primo e ultimo membro a sinistra per g^{-1} e a destra per h^{-1} deduciamo che φ è un omomorfismo se e solo se per ogni scelta di $g, h \in G$ si ha $hg = gh$, cioè se e solo se G è abeliano.

Supponiamo ora che G sia abeliano: allora φ un endomorfismo di G, ma in generale non è biettivo: ad esempio, se $G = \mathbb{R}^*$ gruppo moltiplicativo, l'endomorfismo non è né iniettivo né suriettivo. Invece se consideriamo $G = \mathbb{Z}$ come gruppo additivo (e quindi l'endomorfismo $\varphi : z \mapsto 2z$), allora la mappa è un automorfismo.

11. Cominciamo a verificare che φ è un endomorfismo: dati $g, h \in G$, allora, usando la commutatività dell'operazione di G, abbiamo che

$$\varphi(gh) = (gh)^m = g^m h^m = \varphi(g)\varphi(h).$$

Per dimostrare che φ è un automorfismo dobbiamo dimostrare che è biettivo. Cominciamo a calcolarne il nucleo:

$$\operatorname{Ker}(\varphi) = \{g \in G \mid \varphi(g) = g^m = 1_G\}$$

Allora l'ordine del gruppo $\langle g \rangle$ è un fattore u di m: d'altra parte $\langle g \rangle$ è un sottogruppo di G, quindi il suo ordine u è anche un fattore di n per il Teorema di Lagrange. Poiché $\mathrm{MCD}(n, m) = 1$ per ipotesi, segue che $u = 1$, cioè $g = 1$. Quindi φ è iniettivo, e siccome è una funzione iniettiva da un insieme finito in se stesso, è anche suriettivo, e quindi è un automorfismo.

12. Utilizziamo la notazione moltiplicativa sia in G che in H. Siano $m = \#G$, $n = \#H$. Se $\varphi \in \operatorname{Hom}(G, H)$, per il primo teorema di omomorfismo di gruppi si ha $\operatorname{Im}(\varphi) \cong G/\operatorname{Ker}(\varphi)$. Il Teorema di Lagrange implica che n è divisibile per $\#\operatorname{Im}(\varphi)$ e

$$\#\operatorname{Im}(\varphi) = m/\#\operatorname{Ker}(\varphi).$$

Poiché $\mathrm{MCD}(n, m) = 1$ segue allora che $\#\operatorname{Im}(\varphi) = 1$, ovvero $\#\operatorname{Ker}(\varphi) = m$, quindi $G = \operatorname{Ker}(\varphi)$ e $\operatorname{Im}(\varphi) = \{1_H\}$. In totale, φ può essere solo l'omomorfismo definito da $g \mapsto 1_H$.

N.B. Ricordate che in generale il metodo per risolvere un esercizio non è unico. Se qualche cosa non vi è chiara, e/o se pensate di aver trovato un errore di stampa, fatemi sapere!