Istituzioni di Algebra e Geometria — Algebra, a.a. 2023-2024

Soluzioni foglio 4

1. Siano $G = <g>$ e $H = <h>$ due gruppi ciclici (utilizziamo la notazione moltiplicativa in entrambi), e sia H^G l'insieme delle applicazioni $G \to H$. Sappiamo che su H^G possiamo definire una struttura di gruppo, definendo come prodotto delle applicazioni φ e ψ l'applicazione $\varphi\psi\colon G \to H$, $x \mapsto \varphi(x)\psi(x)$. Ricordo anche che l'elemento neutro è l'applicazione $1 : G \to H$, $x \mapsto 1_H$.

   (a) Per stabilire se $\mathrm{Hom}(G, H)$ è un sottogruppo di H^G usiamo il criterio: se $\varphi, \psi \in \mathrm{Hom}(G, H)$ e $x_1, x_2 \in G$ allora:

   $$\varphi\psi^{-1}(x_1x_2) = \varphi(x_1x_2)\psi(x_1x_2)^{-1} = \varphi(x_1)\varphi(x_2)\psi(x_1)^{-1}\psi(x_2)^{-1},$$

   $$\varphi\psi^{-1}(x_1)\varphi\psi^{-1}(x_2) = \varphi(x_1)\psi(x_1)^{-1}\varphi(x_2)\psi(x_2)^{-1}.$$

   In generale gli ultimi membri di queste catene di uguaglianze non coincidono, quindi non è vero, in generale, che

   $$\varphi\psi^{-1}(x_1x_2) = \varphi\psi^{-1}(x_1)\varphi\psi^{-1}(x_2).$$

   Però se H è ciclico l'uguaglianza è soddisfatta (perché?), come abbiamo supposto. Concludiamo che se H è ciclico, allora $\mathrm{Hom}(G, H)$ è un sottogruppo di H^G. Esiste una condizione su H più debole dell'essere ciclico che garantisca che $\mathrm{Hom}(G, H)$ sia un sottogruppo di H^G?

   (b) Ricordiamo che $G = <g>$. Se $\varphi \in \mathrm{Hom}(G, H)$ deduciamo allora che

   $$\mathrm{Im}(\varphi) = \{\varphi(g^n) = \varphi(g)^n \mid n \in \mathbb{Z}\} \subseteq H.$$

   Inoltre

   $$\mathrm{Ker}(\varphi) = \{g^n \mid \varphi(g)^n = 1\} :$$

   quindi se $m = \mathrm{ord}(\varphi(g))$, segue che $\mathrm{Ker}(\varphi) = (<g^m>) < G$.

   (c) Se $\varphi\colon G \to H$ è un isomorfismo, allora $|G| = |H|$. In particolare G è infinito se e solo se anche H lo è. Si noti che ogni isomorfismo è suriettivo, quindi se φ è un isomorfismo $\varphi(g)$ deve generare H. D'altra parte φ deve anche essere iniettivo, quindi $g^m = 1$, cioè $\mathrm{ord}(\varphi(g)) = \mathrm{ord}(g)$. Provate a verificare che queste condizioni necessarie sono anche sufficienti a garantire che φ sia un isomorfismo.

2. Utilizziamo la notazione moltiplicativa sia in G che in H.

   (a) È una conseguenza del fatto che ogni sottogruppo di un gruppo ciclico è ciclico: infatti l'omomorfismo iniettivo φ induce un isomorfismo $G \simeq \mathrm{Im}(\varphi) < H$.

   (b) Sia $G = <g>$ e sia $h \in H$. Allora esiste $\gamma \in G$ tale che $\varphi(\gamma) = h$, poiché φ è suriettivo. Se $\gamma = g^m$, allora $h = \varphi(g)^m$. Pertanto $H = <\varphi(g)>$, cioè H è ciclico.

3. (a) Chiaramente $D \neq \emptyset$. Usando il criterio per sottogruppi, siano

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

allora

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

Lascio a voi verificare che l'isomorfismo cercato è $\varphi\colon D \to \mathbb{R}^* \times \mathbb{R}^*$, definito da

$$\varphi \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} = (a_1, a_2).$$

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

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

allora

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

e quindi

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

Quindi le matrici cercate sono tutte e sole quelle per cui o $p_{11}p_{12}$, o $p_{21}p_{22}$ sono non nulli.

4. Lascio a voi la (a) e la (b) che sono delle verifiche dirette.

(c) Per verificare che $<\sigma, \tau> \simeq \Delta_n$, si verifichi prima che ogni elemento di $<\sigma, \tau>$ si scrive in maniera unica nella forma $\sigma^a \tau^b$, con $0 \leq a \leq n-1$ e $0 \leq b \leq 1$. A questo punto consideriamo la corrispondenza

$$\begin{aligned} \varphi\colon \Delta_n &\to S_n \\ R^a D_i^b &\mapsto \sigma^a \tau^b. \end{aligned}$$

Verificate che tale applicazione è un omomorfismo ben definito, iniettivo, avente il sottogruppo $<\sigma, \tau>$ come immagine.

5. Consideriamo il poligono regolare di n lati contandone i vertici in senso antiorario a partire da P_0, e osserviamo che $P_i = P_j$ se e solo se $i \equiv j \pmod{n}$.

Ogni elemento di Δ_n si può scrivere nella forma $R^a D_0^b$ con $a \in \mathbb{Z}$ e $b \in \{0, 1\}$: tale scrittura è essenzialmente unica, nel senso che $R^a D_0^b = R^{a'} D_0^{b'}$ se e solo se $a \equiv a' \pmod{n}$ e $b = b'$.

Inoltre, vale la formula $R^h D_0 = D_0 R^{(n-1)h}$, per ogni h (provate a dimostrarla!).

L'ordine di ogni elemento di Δ_7 deve dividere $|\Delta_7| = 14$, quindi può essere 1, 2, 7, o 14. L'ordine di un elemento è 1 se e solo se l'elemento è l'unità del gruppo. Se esistesse un elemento di ordine 14, allora il gruppo Δ_7 dovrebbe essere ciclico, quindi commutativo. Poiché Δ_7 non è commutativo, i possibili ordini dei suoi elementi sono 2 e 7.

Per definizione, la rotazione R ha ordine 7: segue che $R^h \in <R>$ ha ordine 7 per ogni $h \neq 0$. Si consideri un elemento della forma $R^h D_0$: si ha

$$(R^h D_0)(R^h D_0) = R^h (D_0 R^h) D_0 = R^h R^{(7-1)h} D_0 D_0 = R^{7h} D_0^2 = 1,$$

quindi tutti gli elementi di $\Delta_7 \setminus <R>$ hanno ordine 2.

Ragionando come nel caso precedente, i possibili ordini degli elementi di $\Delta_8 \setminus \{1\}$ sono 2, 4, e 8. La rotazione R ha ordine 8: similmente si verifica che R^3, R^5 e R^7 hanno ordine 8.

Invece risulta $(R^2)^4 = R^8 = 1$ e $(R^6)^4 = R^{24} = 1$, quindi l'ordine di R^2 e R^6 è o 2 o 4: poiché si ha $(R^2)^2(P_0) = R^4(P_0) = P_4 \neq P_0$ il loro ordine è 4. Infine $(R^4)^2 = 1$ e $R^4(P_0) = P_4 \neq P_0$, quindi l'ordine di R^4 è 2.

Ragionando come nel caso precedente, si verifica infine che tutti gli elementi di $\Delta_8 \setminus <R>$ hanno ordine 2.

Il caso di Δ_9 lo lascio a voi.

6. Utilizziamo la notazione moltiplicativa sia in G che in H.

   (a) Siano $n = \mathrm{ord}(g)$ e $m = \mathrm{ord}(\varphi(g))$. Allora

   $$1_H = \varphi(1_G) = \varphi(g^n) = \varphi(g)^n,$$

   quindi necessariamente $m|n$.

   (b) Osserviamo che

   $$\varphi(g^m) = \varphi(g)^m = 1_H = \varphi(1_G),$$

   quindi se φ è iniettivo necessariamente $g^m = 1_G$, e quindi $n|m$. Quindi abbiamo due numeri naturali $n, m \in \mathbb{N}$, tali che $n|m$ e, dalla parte (a), $m|n$: segue che $n = m$.

7. In tutti i casi l'unità 1 ha ordine 1.

   Poiché $|\Delta_6| = 12$, gli elementi in $\Delta_6 \setminus \{1\}$ possono avere ordine 2, 3, 4, 6, 12. Con le notazioni usuali osserviamo che D_i ha ordine 2, R^2 ha ordine 3, R ha ordine 6: verificate voi che non ci sono elementi di ordine 4 e 12.

   Poiché $|A_4| = 12$, gli elementi in $A_4 \setminus \{1\}$ possono avere ordine 2, 3, 4, 6, 12. Con le notazioni usuali osserviamo che $(1\,2)(3\,4)$ ha ordine 2 e $(1\,2\,3)$ ha ordine 3: dimostrate che non ci sono elementi di ordine 4, 6 e 12.

   Poiché $|\Delta_{12}| = 24$, gli elementi in $\Delta_{12} \setminus \{1\}$ possono avere ordine 2, 3, 4, 6, 8, 12, 24. Con le notazioni usuali osserviamo che D_i ha ordine 2, R^6 ha ordine 2, R^4 ha ordine 3, R^3 ha ordine 4, R^2 ha ordine 6, R ha ordine 12: dimostrate che non ci sono elementi di ordine 8 e 24.

   Si ha $|S_4| = 24$, e già sappiamo che gli elementi in $S_4 \setminus \{1\}$ possono avere ordine 2, 3, 4. (Ricordiamo infatti che se $\sigma = \alpha_1 \alpha_2 \dots \alpha_k$ è una decomposizione della permutazione σ in cicli disgiunti, allora $\mathrm{ord}(\sigma) = \mathrm{mcm}(\mathrm{ord}(\alpha_1), \dots, \mathrm{ord}(\alpha_k))$, quindi...)

Per finire, se G, H sono due gruppi e $\varphi\colon G \to H$ è un isomorfismo, sappiamo dall'esercizio precedente che $\mathrm{ord}(g) = \mathrm{ord}(\varphi(g))$ per ogni $g \in G$. In particolare, $\Delta_6 \ncong A_{12}$, perché Δ_6 contiene elementi di ordine 6 e A_4 no, e $\Delta_{12} \ncong S_4$, perché Δ_{12} contiene elementi di ordine 12 e S_4 no.

8. Ricordiamo gli elementi del gruppo diedrale

$$\Delta_6 = \{\ 1, R, R^2, R^3, R^4, R^5, D_0, RD_0, R^2D_0, R^3D_0, R^4D_0, R^5D_0\ \},$$

dove R è la rotazione di $\pi/3$ radianti in senso antiorario e D_0 la riflessione rispetto all'asse di simmetria passante per il vertice P_0 dell'esagono, con le relazioni

$$D_0^2 = R^6 = 1 \quad \text{e} \quad D_0R = R^5D_0.$$

Inoltre si ha che

$$<D_0>= \{1, D_0\}, \qquad <R^2>= \{1, R^2, R^4\}.$$

(a) Tenendo conto che $[\,\Delta_6 :< D_0 >] = |\Delta_6|/|< D_0 >| = 6$ e della relazione $D_0R = R^5D_0$, le classi laterali destre di Δ_6 rispetto a $<D_0>$ sono:

$$< D_0 > 1 = \{1, D_0\}, \qquad <D_0> R = \{R, R^5D_0\}, \qquad <D_0> R^2 = \{R^2, R^4D_0\},$$

$$<D_0> R^3 = \{R^3, R^3D_0\}, \qquad <D_0> R^4 = \{R^4, R^2D_0\}, \qquad <D_0> R^5 = \{R^5, RD_0\}.$$

Similmente, tenendo conto dell'indice $[\,\Delta_6 :< R^2 >] = |\Delta_6|/|< R^2 >| = 4$ e della relazione $D_0R = R^5D_0$, le classi laterali destre di Δ_6 rispetto a $<R^2>$ sono:

$$<R^2> 1 = \{1, R^2, R^4\}, \qquad <R^2> D_0 = \{D_0, R^2D_0, R^4D_0\},$$

$$<R^2> R^3 = \{R, R^3, R^5\}, \qquad <R^2> R^3D_0 = \{RD_0, R^3D_0, R^5D_0\}.$$

(b) Le classi laterali sinistre di Δ_6 rispetto a $<D_0>$ sono:

$$1 <D_0>= \{1, D_0\}, \qquad R <D_0>= \{R, RD_0\}, \qquad R^2 <D_0>= \{R^2, R^2D_0\},$$

$$R^3 <D_0>= \{R^3, R^3D_0\}, \quad R^4 <D_0> R^4 = \{R^4, R^4D_0\}, \quad R^5 <D_0>= \{R^5, R^5D_0\}.$$

Le classi laterali destre di Δ_6 rispetto a $<R^2>$ sono:

$$1 <R^2>= \{1, R^2, R^4\}, \qquad D_0 <R^2>= \{D_0, R^2D_0, R^4D_0\},$$

$$R^3 <R^2>= \{R, R^3, R^5\ \}, \qquad R^3D_0 <R^2>= \{RD_0, R^3D_0, R^5D_0\}.$$

(c) Da quanto visto sopra $R^2 <D_0> \neq <D_0> R^2$.

(d) A voi la risposta.

9. La mappa φ è un omomorfismo se e solo se, per ogni $g, h \in G$:

$$\varphi(gh) = \varphi(g)\varphi(h) \quad \Leftrightarrow \quad (gh)^2 = g^2h^2 \quad \Leftrightarrow \quad ghgh = gghh \quad \Leftrightarrow \quad hg = gh,$$

cioè se e solo se G è abeliano.

In generale, non è biettivo; ad esempio, l'endomorfismo del gruppo moltiplicativo $\mathbb{R}^*$ che manda $x \mapsto x^2$ non è suriettivo.

10. Sia G un gruppo abeliano di ordine finito n, e sia m tale che $\mathrm{MCD}(n, m) = 1$. Seguendo un ragionamento molto simile a quello dell'esercizio precedente, il fatto che G sia abeliano implica che la mappa $\varphi : g \mapsto g^m$ è un omomorfismo, perché per ogni $g, h \in G$:

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

Studiamo il nucleo $\mathrm{Ker}(\varphi)$: un elemento $g \in G$ appartiene al nucleo se $\varphi(g) = g^m = 1_G$, quindi l'ordine dell'elemento g divide m. D'altra parte, per il teorema di Lagrange, l'ordine di un qualsiasi elemento di G divide $|G| = n$, quindi l'unica possibilità è che $\mathrm{ord}(g) = 1$, cioè $g = 1_G$, e quindi φ è iniettivo. Grazie al teorema fondamentale di omomorfismo per gruppi, un endomorfismo iniettivo di un gruppo finito è un automorfismo, perché $G/\{1_G\} \simeq G \simeq \mathrm{Im}(\varphi)$, e quindi $\mathrm{Im}(\varphi) = G$, cioè φ iniettivo è anche suriettivo.

11. Usiamo la notazione moltiplicativa, e poniamo $|G| = m$, $|H| = n$, con $\mathrm{MCD}(m, n) = 1$. Sia $\varphi \in \mathrm{Hom}(G, H)$ un omomorfismo $G \to H$, e consideriamo la sua immagine $\mathrm{Im}(\varphi)$. Poiché $\mathrm{Im}(\varphi) < H$, la sua cardinalità $|\mathrm{Im}(\varphi)|$ divide la cardinalità di $|H| = n$. Per il teorema fondamentale di omomorfismo per gruppi, $\mathrm{Im}(\varphi) \simeq G/\mathrm{Ker}(\varphi)$, e quindi

$$|\mathrm{Im}(\varphi)| = |G/\mathrm{Ker}(\varphi)| = \frac{m}{|\mathrm{Ker}(\varphi)|},$$

da cui decidiamo che $|\mathrm{Im}(\varphi)|$ divide anche m. Siccome m ed n sono coprimi, l'unica possibilità è che $|\mathrm{Im}(\varphi)| = 1$, da cui $|\mathrm{Ker}(\varphi)| = m$, cioè $\mathrm{Im}(\varphi) = \{1_H\}$ e $\mathrm{Ker}(\varphi) = G$: questo significa che φ è la mappa banale $G \to H$ che manda $g \mapsto 1_H$ per ogni $g \in G$, e non c'è altra possibilità.

12. Per il sottogruppo L delle matrici triangolari inferiori consideriamo

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \in L, \qquad \text{e} \qquad B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}).$$

Verificate che allora:

$$BAB^{-1} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \notin L,$$

cioè L non è normale in $\mathrm{GL}_2(\mathbb{R})$.

Provate a modificare l'argomento per dimostrare che U non è normale in $\mathrm{GL}_2(\mathbb{R})$.

13. Usiamo il criterio di normalità: siano $A \in \mathrm{SL}_n(\mathbb{R})$ e $B \in \mathrm{GL}_n(\mathbb{R})$. Il teorema di Binet ci dice che

$$\det(BAB^{-1}) = \det(B)\det(A)\det(B)^{-1} = \det(A) = 1,$$

cioè $BAB^{-1} \in \mathrm{SL}_n(\mathbb{R})$.

Una dimostrazione alternativa consiste nell'osservare che $\mathrm{SL}_n(\mathbb{R}) = \mathrm{Ker}(\det)$ è il nucleo dell'omomorfismo det da $\mathrm{GL}_n(\mathbb{R})$ al gruppo moltiplicativo $\mathbb{R}$.

14. Usiamo il criterio di normalità: dati $h \in H$ e $\gamma \in G$, vogliamo dimostrare che allora $\gamma^{-1}h\gamma \in H$. Osserviamo che se $h_1, h_2 \in H$ risulta

$$\gamma^{-1}(h_1h_2)\gamma = (\gamma^{-1}h_1\gamma)(\gamma^{-1}h_2\gamma).$$

Poiché ogni elemento di H è della forma

$$h = \prod_{i=1}^{n} g_i^2,$$

deduciamo che basta dimostrare la tesi per gli elementi della forma $g^2 \in H$, e per questi elementi:

$$\gamma^{-1}g^2\gamma = \gamma^{-1}g\gamma\gamma^{-1}g\gamma = (\gamma^{-1}g\gamma)^2 \in H.$$

15. Ricordiamo che $Z(G)$ è il sottogruppo degli elementi di G che commutano con tutti gli altri, detto centro di G.

(a) Usando il criterio di normalità , dati $g \in G$ e $h \in H \subseteq Z(G)$, allora $ghg^{-1} = h \in H$: in particolare H è normale.

(b) Poiché $|H| = 2$ segue che $H = \{1_G, h\}$; inoltre poiché $H \lhd G$, per ogni $g \in G$ si ha $ghg^{-1} \in H = \{1_G, h\}$. Quindi abbiamo due possibilità: o $ghg^{-1} = 1_G$, oppure $ghg^{-1} = h$. Se $ghg^{-1} = 1_G$ allora $gh = g$ per ogni $g \in G$, quindi necessariamente $h = 1_G$. Se invece $ghg^{-1} = h$, allora $gh = hg$ per ogni $g \in G$, cioè $H \subseteq Z(G)$.

16. (a) Se $h \in H$, allora $\psi(gh) = (gh)^{-1} = h^{-1}g^{-1} \in Hg^{-1}$ perché H è un sottogruppo di G: quindi $\psi(gH) \subseteq Hg^{-1}$. Viceversa, se $h \in H$ allora $hg^{-1} = \psi(gh^{-1})$: poiché H è sottogruppo di G segue che $gh^{-1} \in gH$, dunque $\psi(gH) \supseteq Hg^{-1}$. Dalla doppia inclusione segue l'uguaglianza.

(b) Se $h \in H$, allora $\varphi_g(hg) = ghgg^{-1} = gh \in gH$: concludiamo che $\varphi_g(Hg) \subseteq gH$. Viceversa, se $h \in H$ allora $gh = ghgg^{-1} = \varphi_g(hg)$, dunque $\varphi_g(Hg) \supseteq gH$. Dalla doppia inclusione segue l'uguaglianza.

17. (a) Per mostrare che $gHg^{-1} < G$ usiamo il criterio per sottogruppi: fissato $g \in G$ è chiaro che $gHg^{-1} \neq \emptyset$. Consideriamo due elementi di gHg^{-1}, diciamo gag^{-1} e gbg^{-1}, con $a, b \in H$: allora

$$(gag^{-1})(gbg^{-1})^{-1} = gag^{-1}gb^{-1}g^{-1} = g(ab^{-1})g^{-1}.$$

Poiché H è un sottogruppo e $a, b \in H$, deduciamo che $ab^{-1} \in H$, dunque

$$(gag^{-1})(gbg^{-1})^{-1} = g(ab^{-1})g^{-1} \in gHg^{-1}.$$

(b) Se $H \lhd G$, per definizione le classi laterali destre e sinistre coincidono: $\forall\ g \in G$, $gH = Hg$. A voi dedurre che questo è equivalente all'enunciato richiesto.

(c) Osserviamo che

$$Core_G(H) = \bigcap_{g \in G} gHg^{-1}$$

è contenuto in H semplicemente perché $H = 1_G H 1_G^{-1}$. Inoltre essendo intersezione di sottogruppi, $Core_G(H)$ è sicuramente un sottogruppo di G. Per dimostrare che è normale usiamo il criterio di normalità : siano $\gamma \in G$ e $k \in Core_G(H)$: allora per ogni $g \in G$ esiste $h_{\gamma^{-1}g} \in H$ tale che

$$k = (\gamma^{-1}g)h_{\gamma^{-1}g}(\gamma^{-1}g)^{-1}.$$

Quindi per ogni $g \in G$ risulta $\gamma k \gamma^{-1} = g h_{\gamma^{-1}g} g^{-1} \in gHg^{-1}$, dunque $\gamma k \gamma^{-1} \in Core_G(H)$ per ogni scelta di $\gamma \in G$.

(d) Se $N \subseteq H$ è normale in G allora per ogni $n \in N$ e $\gamma \in G$ si ha che $\gamma n \gamma^{-1} \in N$, cioè $n \in gNg^{-1} \subseteq gHg^{-1}$, con $g = \gamma^{-1}$. Concludiamo che $n \in Core_G(H)$.

18. (a) Poniamo $H = \varphi^{-1}(H')$ e siano $h \in H$ e $g \in G$: usando il criterio, dobbiamo dimostrare che $ghg^{-1} \in H$ o, in altre parole, che

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} \in H'.$$

Ma questo è vero perché H' è normale in G' e $\varphi(h) \in H'$.

(b) Poniamo $H' = \varphi(H)$ e siano $h' \in H'$ e $g' \in G'$: usando di nuovo il criterio, dobbiamo dimostrare che $g'h'g'^{-1} \in H' = \varphi(H)$. Si noti che esistono $h \in H$ e $g \in G$ tali che $h' = \varphi(h)$ e $g' = \varphi(g)$, poiché φ è suriettivo. Quindi

$$g'h'g'^{-1} = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(ghg^{-1}).$$

Poiché H è normale in G sappiamo che $ghg^{-1} \in H$, dunque $\varphi(ghg^{-1}) \in H'$, ovvero che H' è normale in G'.

19. Osserviamo che $[G, G]$ è il sottogruppo di G generato dagli elementi $[a, b] = aba^{-1}b^{-1}$, cioè il sottoinsieme i cui elementi sono tutti e soli i prodotti della forma $\prod_{i=1}^{n}[a_i, b_i]$. Non è detto (e, infatti, non è in generale vero) che ogni elemento di $[G, G]$ sia della forma $[a, b]$.

(a) Usiamo il criterio di normalità: se $g \in G$, allora

$$\begin{aligned} g[a,b]g^{-1} &= g(aba^{-1}b^{-1})g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) \\ &= (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1} = [gag^{-1}, gbg^{-1}] \in [G,G]. \end{aligned}$$

Se $\prod_{i=1}^{n}[a_i, b_i] \in [G, G]$ e $g \in G$ allora si può verificare che

$$g\left(\prod_{i=1}^{n}[a_i, b_i]\right)g^{-1} = \prod_{i=1}^{n}\left(g[a_i, b_i]g^{-1}\right).$$

Per quanto visto sopra, il membro di destra è un prodotto di elementi di $[G, G]$, quindi è un elemento di $[G, G]$ esso stesso: in particolare $[G, G]$ è normale in G.

(b) Siano $a, b \in G$: poiché $aba^{-1}b^{-1} = [a, b] \in [G, G]$ segue che $\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}$ nel quoziente $G/[G, G]$, che quindi è commutativo.

(c) Se G/H è abeliano, per ogni coppia $a, b \in G$ segue che $abH = baH$, cioè $aba^{-1}b^{-1} \in H$. Perciò per ogni coppia $a, b \in G$ si ha $[a, b] = aba^{-1}b^{-1} \in H$. Ma allora anche il sottogruppo $[G, G]$ generato dagli elementi della forma $[a, b]$ è contenuto in H. Viceversa, se $[G, G] \subseteq H$ allora per ogni coppia $a, b \in G$ abbiamo

$$(abH)(a^{-1}b^{-1}H) = H = 1_{G/H},$$

quindi $(aH)(bH) = abH = (a^{-1}b^{-1}H)^{-1} = baH = (bH)(aH)$.

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!