Istituzioni di Algebra e Geometria — Algebra, a.a. 2023-2024
Soluzioni foglio 3

1. (a) Lascio a voi la verifica che $G \times H$ è un gruppo con l'operazione data.

   (b) 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
$$(g,h)^m = (g^{\lambda u}, h^{\mu v}) = (1,1).$$
   Deduciamo che m è divisibile per w, quindi $w \leq m$. D'altra parte
$$(1,1) = (g,h)^w = (g^w, h^w),$$
   quindi $g^w = 1$ in G e $h^w = 1$ in H. Ciò significa che w è divisibile sia per u che per v, dunque è divisibile per m, quindi $m \leq w$. Si conclude allora che $m = w$.

2. Cominciamo a mostrare che l'applicazione φ è un omomorfismo, infatti:
$$\varphi((h,k)(h',k')) = \varphi(hh', kk') = hh'kk';$$
   grazie all'ipotesi (b) si ha $h'k = kh'$, e quindi
$$\varphi((h,k)(h',k')) = hkh'k' = \varphi(h,k)\varphi(h',k').$$
   Per dimostrare che φ è iniettivo, mostriamo che $\mathrm{Ker}(\varphi) = \{(1_H, 1_K)\}$. L'inclusione $\supseteq$ è ovvia; viceversa, se $(h,k) \in \mathrm{Ker}(\varphi)$ allora
$$1_G = \varphi(h,k) = hk,$$
   da cui segue che $k^{-1} = h \in H$. Poiché K è un sottogruppo risulta anche $k^{-1} \in K$, dunque $h = k^{-1} \in H \cap K = \{1_G\}$ per l'ipotesi (a). Concludiamo che $\mathrm{Ker}(\varphi) = \{(1_H, 1_K)\}$.

   L'ultimo step è dimostrare la suriettività di φ, e la lascio a voi.

3. Scrivo la soluzione per il caso del sottogruppo unione, lascio a voi il caso dell'intersezione.

   (a) Si ha $H', K' \subseteq H' \vee K'$, quindi
$$\varphi^{-1}(H' \vee K') \supseteq \varphi^{-1}(H'), \varphi^{-1}(K').$$
   Poiché sappiamo che $\varphi^{-1}(H' \vee K')$ è un sottogruppo di G (perché?), esso deve contenere il più piccolo sottogruppo che contiene $\varphi^{-1}(H')$ e $\varphi^{-1}(K')$, cioè
$$\varphi^{-1}(H' \vee K') \supseteq \varphi^{-1}(H') \vee \varphi^{-1}(K').$$

(b) 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 $\varphi\colon (\mathbb{R}, +) \to (\mathbb{R}^2, +)$ definita da $a \mapsto (a, 0)$. Verificate 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 $(\mathbb{R}^2, +)$ (verificate anche questo).
È facile vedere che

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

quindi le retroimmagini $\varphi^{-1}(H')$ e $\varphi^{-1}(K')$ sono entrambe uguali a $\{0\}$, e lo stesso vale per il loro sottogruppo unione: $\varphi^{-1}(H') \vee \varphi^{-1}(K') = \{0\}$.
È altrettanto facile calcolare che $H' \vee K' = \mathbb{R}^2$, quindi $\varphi^{-1}(H' \vee K') = \mathbb{R}$.

4. Ricordiamo che $Z(G)$, il centro di G, è il sottoinsieme (sottogruppo) degli elementi che commutano con tutti gli altri. Osserviamo che φ_g è un omomorfismo: per ogni scelta di $a, b \in G$ si ha

$$\varphi_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \varphi_g(a)\varphi_g(b).$$

Inoltre la composizione $\varphi_g \circ \varphi_{g^{-1}}$ applicata ad un elemento $a \in G$ dà:

$$(\varphi_g \circ \varphi_{g^{-1}})(a) = \varphi_g(g^{-1}a(g^{-1})^{-1}) = g(g^{-1}ag)g^{-1} = a,$$

cioè il coniugio φ_g è invertibile e $\varphi_g^{-1} = \varphi_{g^{-1}}$. In totale quindi il coniugio è un isomorfismo.

Infine abbiamo che $\varphi_g = \mathrm{id}$ se e solo se $\varphi_g(a) = \mathrm{id}(a)$ per ogni $a \in G$, se e solo se $gag^{-1} = a$ per ogni $a \in G$, se e solo se $ga = ag$ per ogni $a \in G$, cioè se e solo se $g \in Z(G)$.

5. Sia $n = \operatorname{ord}(a)$: per definizione allora $a^n = 1 : G$.

Verifichiamo che $\operatorname{ord}(a^{-1}) = n$. Da $(a^n)^{-1} = (a^{-1})^n$ deduciamo $(a^{-1})^n = 1$, 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 $\operatorname{ord}(a^{-1}) = n$.

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

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

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

Per verificare che $\mathrm{ord}(ab) = \mathrm{ord}(ba)$ è sufficiente osservare che $ab = b^{-1}(ba)b$, quindi la tesi segue da quanto visto sopra.

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

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

(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 $2 + 4$ in $\mathbb{Z}_{12}$ (qual è invece?).

(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 $ab^{-1} \in T(G)$.

7. (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 $\operatorname{ord}(M_a) = 2$. 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.

8. $\alpha\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 6 & 4 & 2 & 3 & 5 & 7 \end{pmatrix} = (26534)$.

9. Le decomposizioni sono:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 5 & 3 & 2 & 4 & 1 & 6 \end{pmatrix} = (1\,7\,6)(2\,5\,4), \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (1\,6\,2\,7)(3\,5).$$

10. Calcoliamo

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 4 & 5 & 6 & 3 & 1 & 2 \end{pmatrix} = (1\,7\,2\,4\,6)(3\,5).$$

Gli ordini di $(1\,7\,2\,4\,6)$ e $(3\,5)$ sono 5 e 2 rispettivamente. Infine

$$\operatorname{sgn}(1\,7\,2\,4\,6) = \operatorname{sgn}((1\,6)(1\,5)(1\,2)(1\,6)) = (-1)^4 = 1, \qquad \operatorname{sgn}(3\,5) = -1.$$

11. Indichiamo come sempre con 1 la permutazione identità.

Il gruppo simmetrico S_2 è formato solo dall'identità e dalla trasposizione $(1\,2)$:

$$S_2 = \{1, (1\,2)\},$$

e si ha che $\operatorname{sgn}(1) = 1$, $\operatorname{sgn}(1\,2) = -1$, $\operatorname{ord}(1) = 1$, $\operatorname{ord}(1\,2) = 2$.

Lo studio di S_3 lo abbiamo già visto a lezione: S_3 ha 6 elementi, che sono, oltre all'identità 1 (di ordine e segno 1), le 3 trasposizioni

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\,2), \qquad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (1\,3), \qquad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (2\,3),$$

che hanno tutte ordine 2 e segno -1. Infine ci sono i 2 cicli

$$\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix} = (1\,2\,3), \qquad \begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix} = (1\,3\,2),$$

che hanno ordine 3 e segno 1: $\mathrm{sgn}(1\,2\,3) = \mathrm{sgn}((1\,3)(1\,2)) = 1$ e $\mathrm{sgn}(1\,3\,2) = \mathrm{sgn}((1\,2)(1\,3)) = 1$.

Consideriamo S_4. Per elencare i suoi elementi possiamo procedere elencando prima quei σ per cui $\sigma(1) = 1$, poi quelli per cui $\sigma(1) = 2$, poi quelli per cui $\sigma(1) = 3$, e infine quelli per cui $\sigma(1) = 4$. In ciascuno di questi casi si può pensare a σ come a una permutazioni su 3 elementi.

- Se $\sigma(1) = 1$ abbiamo l'identità 1 e

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 2 & 4 & 3\end{pmatrix} = (3\,4), \qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 2 & 4\end{pmatrix} = (2\,3),$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 3 & 4 & 2\end{pmatrix} = (2\,4)(2\,3), \qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 3 & 2\end{pmatrix} = (1\,4)(2\,3), \qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 1 & 4 & 2 & 3\end{pmatrix} = (2\,3)(2\,4).$$

- Se $\sigma(1) = 2$

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 3 & 4\end{pmatrix} = (1\,2),$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix} = (1\,2)(3\,4), \qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix} = (1\,3)(1\,2), \qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 3 & 1\end{pmatrix} = (1\,4)(1\,2),$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 4 & 1\end{pmatrix} = (1\,4)(1\,3)(1\,2), \qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 4 & 1 & 3\end{pmatrix} = (1\,3)(1\,4)(1\,2).$$

- Se $\sigma(1) = 3$ abbiamo

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 1 & 4\end{pmatrix} = (1\,3),$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 2 & 4\end{pmatrix} = (1\,2)(1\,3), \qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 2 & 4 & 1\end{pmatrix} = (1\,4)(1\,3), \qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 1 & 2\end{pmatrix} = (1\,3)(2\,4),$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 1 & 4 & 2\end{pmatrix} = (1\,2)(1\,4)(1\,3), \qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 3 & 4 & 2 & 1\end{pmatrix} = (1\,4)(1\,2)(1\,3).$$

- Infine se $\sigma(1) = 4$ abbiamo

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 3 & 1\end{pmatrix} = (1\,4),$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 3 & 2\end{pmatrix} = (1\,2)(1\,4), \qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 2 & 1 & 3\end{pmatrix} = (1\,4)(1\,3), \qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 2 & 1\end{pmatrix} = (1\,4)(2\,3),$$

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 1 & 2 & 3\end{pmatrix} = (1\,2)(1\,3)(1\,4), \qquad \begin{pmatrix}1 & 2 & 3 & 4\\ 4 & 3 & 1 & 2\end{pmatrix} = (1\,3)(1\,2)(1\,4).$$

Per ogni permutazione è indicata una possibile scomposizione in trasposizioni: verificatene l'uguaglianza e calcolate il segno per ogni permutazione.

Per quanto riguarda l'ordine, l'identità ha ordine 1. Ci sono 9 permutazioni di ordine 2:

$$(1\,2),\qquad (1\,3),\qquad (1\,4),\qquad (2\,3),\qquad (2\,4),\qquad (3\,4),$$

$$(1\,2)(3\,4),\qquad (1\,3)(2\,4),\qquad (1\,4)(2\,3).$$

Ci sono 8 permutazioni di ordine 3 che sono tutte 3–cicli:

$$(1\,2)(1\,3),\qquad (1\,2)(1\,4),\qquad (1\,3)(1\,2),\qquad (1\,3)(1\,4),$$

$$(1\,4)(1\,2),\qquad (1\,4)(1\,3),\qquad (2\,3)(2\,4),\qquad (2\,4)(2\,3).$$

Infine ci sono 6 permutazioni di ordine 4 che sono tutte 4–cicli:

$$(1\,4)(1\,3)(1\,2),\qquad (1\,3)(1\,4)(1\,2),\qquad (1\,2)(1\,4)(1\,3),$$

$$(1\,4)(1\,2)(1\,3),\qquad (1\,2)(1\,3)(1\,4),\qquad (1\,3)(1\,2)(1\,4).$$

Per la domanda (b), calcoliamo

$$(1\,2\,3\,4)^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (1\,3)(2\,4),$$

segue che $(1\,2\,3\,4)^2$ non è un ciclo. A questo punto lascio a voi rispondere alla domanda (a).

12. (a) Siano $\alpha = (1\,a)$, $\beta = (1\,b)$ e $\sigma = (1\,a)(1\,b)(1\,a) = \alpha\beta\alpha = \alpha\beta\alpha^{-1}$. Chiaramente σ lascia fissi tutti gli elementi in

$$\{\ \widehat{1}, 2, \ldots, a-1, \widehat{a}, a+1, \ldots, b-1, \widehat{b}, b+1, \ldots, n\ \}$$

(dove quando scrivo $\widehat{i}$ intendo che ho tolto quell'indice).
Invece sugli elementi 1, a, e b σ agisce nel modo seguente:

$$\sigma(1) = \alpha\beta(a) = \alpha(a) = 1, \qquad \sigma(a) = \alpha\beta(1) = \alpha(b) = b, \qquad \sigma(b) = \alpha\beta(b) = \alpha(1) = a.$$

Deduciamo che $\sigma = (a\,b)$.
È vero o falso che $(1\,b)(1\,a)(1\,b) = (1\,a)(1\,b)(1\,a)$?

(b) Sappiamo che ogni permutazione si può scrivere come prodotto di trasposizioni: dunque se $\sigma \in S_n$ esistono $a_i, b_i \in \{\ 1, \ldots, n\ \}$ con $a_i < b_i$ tali che

$$\sigma = \prod_{i=1}^{h} (a_i\,b_i).$$

Se $a_i = 1$ allora $(a_i\,b_i) = (1\,b_i)$. Se $a_i \neq 1$, per quanto visto sopra,

$$(a_i\,b_i) = (1\,a_i)(1\,b_i)(1\,a_i),$$

come volevamo dimostrare.

(c) Cominciamo a scomporre la permutazione in trasposizioni:

$$(3\,7\,2\,5)(1\,3\,4\,6)(2\,3) = (3\,7)(3\,2)(3\,5)(1\,3)(1\,4)(1\,6)(2\,3).$$

Ora sostituiamo ad ogni (a, b) con $a \neq 1$ la permutazione $(1\,b)(1\,a)(1\,b)$, e otteniamo:

$$(3\,7\,2\,5)(1\,3\,4\,6)(2\,3) = (1\,7)(1\,3)(1\,7)(1\,2)(1\,3)(1\,2)(1\,5)(1\,3)(1\,5)(1\,3)(1\,4)(1\,6)(1\,3)(1\,2)(1\,3).$$

13. (a) L'affermazione è banalmente vera se $k = 1$. Sia $k \geq 2$ e siano $a_1, \ldots, a_k \in \{ 1, \ldots, n \}$ tutti i soli gli elementi a due a due distinti non fissati da σ e supponiamo che

$$\sigma(a_i) = a_{i+1}, \qquad \sigma(a_k) = a_1.$$

Chiaramente se $1 \leq h \leq k$

$$\sigma^h(a_i) = a_{i+h},\ i = 1, \ldots, k-1, \qquad \sigma^h(a_k) = a_h.$$

Concludiamo che $\sigma^k = 1$ ma $\sigma^h \neq 1$ se $h < k$.

(b) Tenendo conto della parte (a), a voi la risposta.

(c) L'affermazione segue dalla scomposizione in trasposizioni del ciclo $\sigma = (a_1\, a_2\, a_3\, \ldots\, a_{k-1}\, a_k)$, insieme al fatto che ogni trasposizione contribuisce con un -1, infatti

$$\sigma = \prod_{i=2}^{k} (a_1, a_i),$$

quindi $\operatorname{sgn}(\sigma) = (-1)^{k-1}$.

14. Sia $\sigma = (a_1\, a_2\, a_3\, \ldots\, a_{k-1}\, a_k)$. Si ricordi che $\sigma^{-1} = \sigma^{k-1}$ e che se $1 \leq h \leq k$

$$\sigma^h(a_i) = a_{i+h},\ i = 1, \ldots, k-1, \qquad \sigma^h(a_k) = a_h.$$

In particolare

$$\sigma^{-1}(a_1) = a_k, \qquad \sigma^{-1}(a_i) = a_{i-1},\ i = 2, \ldots, k,$$

cioè σ^{-1} è il ciclo $(a_1\, a_k\, a_{k-1}\, \ldots\, a_3\, a_2)$. È vero o falso che ogni potenza di σ è un ciclo?

15. (a) Se $\tau = (b\,c)$, risulta

$$\sigma\tau(a) = \sigma(a) = b \neq c = \tau(b) = \tau\sigma(a),$$

dunque $\sigma\tau \neq \tau\sigma$.

(b) Se per assurdo $Z(S_n) \neq \{ 1 \}$, allora esisterebbe $\sigma \in Z(S_n) \setminus \{1\}$. Poiché $\sigma \neq 1$ esiste $a \in \{ 1, \ldots, n \}$ tale che $\sigma(a) = b \neq a$. Se $n \geq 3$ esiste $c \notin \{ a, b \}$. Per quanto visto sopra esiste $\tau \in S_n$ tale che $\sigma\tau \neq \tau\sigma$, in contraddizione con l'ipotesi $\sigma \in Z(S_n)$.

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!