

Istituzioni di Algebra e Geometria — Algebra, a.a. 2023-2024  
**Soluzioni foglio 2**

1. (a)  $G = \mathbb{N}$  è chiuso rispetto all'operazione  $a * b = a^b$ .

Per quanto riguarda l'elemento neutro è chiaro che  $a * b = a$  per ogni  $a \in G$  implica  $b = 1$ , quindi se un elemento neutro esiste, deve essere per forza 1: d'altra parte  $1 * b = 1$  per ogni  $b$ , quindi non esistono elementi neutri in  $G$  rispetto a  $*$ , e non ha nemmeno senso parlare di inverso. Si noti poi che l'operazione non è associativa:

$$(2 * 2) * 3 = 4^3 = 64 \neq 256 = 2^8 = 2 * (2 * 3).$$

Infine  $*$  non è nemmeno commutativa:  $2 * 3 = 8 \neq 9 = 3 * 2$ .

- (c) Per  $G = (1, +\infty)$  con l'operazione  $a * b = a^{\log b}$ , sia  $\alpha$  la base del logaritmo. Assumiamo per ora che  $\alpha = 10$ , provate a vedere come cambiano le risposte al variare di  $\alpha \in (0, +\infty)$ . È facile vedere che  $G$  è chiuso rispetto a  $*$ .

Per l'elemento neutro, abbiamo che se  $a * b = a$  per ogni  $a \in G$ , allora  $b = \alpha$ . Inoltre

$$\alpha * a = \alpha^{\log a} = a$$

per ogni  $a \in G$ . Concludiamo che  $\alpha$  è elemento neutro per  $*$ .

Passiamo agli inversi: sia  $a * b = \alpha$  per ogni  $a \in G$ , cioè  $a^{\log b} = \alpha$ : dalla definizione di logaritmo segue allora che  $\log b = \log_a \alpha$ : dunque  $b = \alpha^{\log_a \alpha}$  che, quindi risulta essere l'unico candidato per l'eventuale inverso di  $a$ . Risulta

$$(\alpha^{\log_a \alpha}) * a = (\alpha^{\log_a \alpha})^{\log a} = \alpha^{(\log_a \alpha)(\log a)}$$

Poiché  $(\log_a \alpha)(\log a) = \log_a a = 1$ , segue che  $a^{-1} = \alpha^{\log_a \alpha}$ .

Per quanto riguarda l'associatività, osserviamo che

$$(a * b) * c = (a^{\log b}) * c = (a^{\log b})^{\log c} = a^{(\log b)(\log c)},$$

$$a * (b * c) = a * (b^{\log c}) = a^{\log(b^{\log c})} = a^{(\log b)(\log c)}.$$

Infine cosa si deduce dall'uguaglianza  $\log(a * b) = \log(a^{\log b}) = (\log b)(\log a)$ ?

I casi (b) e (d) li lascio a voi.

2. Indichiamo col prodotto l'operazione in  $G$ , e usiamo il criterio per sottogruppi. Se gli  $H_i$  sono sottogruppi di  $G$  allora  $H = \bigcap_{i \in I} H_i$  è non vuoto perché contiene l'unità 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  $i \in I$ , quindi  $ab^{-1} \in \bigcap_{i \in I} H_i = H$ .

3. (a) L'implicazione  $H \subseteq K$  o  $K \subseteq H \Rightarrow H \cup K$  è un sottogruppo è banale. Viceversa supponiamo che  $H \not\subseteq K$  e  $K \not\subseteq H$ . Siano  $h \in H \setminus K$ ,  $k \in K \setminus H$ . Se  $H \cup K$  fosse un sottogruppo dovrebbe essere chiuso rispetto all'operazione in  $G$  (che indichiamo col prodotto): in particolare si dovrebbe avere  $hk \in H \cup K$ . Poiché sia  $H$  che  $K$  sono sottogruppi, segue 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) Avendo dato come definizione di  $H \vee K$  il minimo sottogruppo che contiene entrambi  $H$  e  $K$ , e avendo definito  $\langle H \cup K \rangle$  come l'intersezione di tutti i sottogruppi di  $G$  contenenti sia  $H$  che  $K$ , l'uguaglianza è praticamente una tautologia.

Provate invece a dimostrare l'uguaglianza prendendo come definizione di  $H \vee K$  questa:

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

che abbiamo dimostrato essere equivalente.

- (c) Provate a utilizzare la prima affermazione della parte (a).

4. Come prima cosa osserviamo che la definizione è ben posta, cioè dà effettivamente un elemento di  $G^X$ . L'elemento neutro è l'applicazione

$$\begin{aligned} u: X &\rightarrow G \\ a &\mapsto 1_G. \end{aligned}$$

Sia ora  $\varphi \in G^X$ : poiché  $G$  è un gruppo,  $\varphi(a)$  ha un inverso in  $G$  per ogni  $a \in X$ . Ne deduciamo che  $\varphi\varphi^{-1} = \varphi^{-1}\varphi = u$ , dove

$$\begin{aligned} \varphi^{-1}: X &\rightarrow G \\ a &\mapsto \varphi(a)^{-1}. \end{aligned}$$

La verifica dell'associatività la lascio a voi.

Infine se  $G$  è abeliano, allora  $G^X$  è abeliano perché  $\varphi(a)\psi(a) = \psi(a)\varphi(a)$  per ogni  $a \in X$ . Viceversa sia  $G^X$  abeliano e siano  $h, g \in G$ : le applicazioni  $\varphi_g: a \mapsto g$  e  $\varphi_h: a \mapsto h$  sono in  $G^X$ , dunque commutano, cioè  $G$  è abeliano:

$$gh = \varphi_g(a)\varphi_h(a) = \varphi_h(a)\varphi_g(a) = hg.$$

5. (a)  $\text{SL}_n(\mathbb{R}) < \text{GL}_n(\mathbb{R})$  è un sottogruppo: usando il criterio, se  $A, B \in \text{SL}_n(\mathbb{R})$  allora  $\det(AB^{-1}) = \det(A)\det(B^{-1}) = \det(A)\det(B)^{-1} = 1$ , quindi  $AB^{-1} \in \text{SL}_n(\mathbb{R})$ . ✓  
(Alternativamente, possiamo anche osservare che  $\text{SL}_n(\mathbb{R}) = \text{Ker}(\det)$ , dove con  $\det$  indichiamo l'omomorfismo determinante  $(\text{GL}_n(\mathbb{R}), \cdot) \rightarrow (\mathbb{R}^*, \cdot)$ .)

- (d)  $GL_n^-(\mathbb{R})$  non è un sottogruppo di  $GL_n(\mathbb{R})$ : si vede immediatamente che non è stabile, infatti se  $A, B \in GL_n^-(\mathbb{R})$  allora  $\det(AB) = \det(A)\det(B) > 0$ , cioè  $AB \notin GL_n^-(\mathbb{R})$ . Inoltre non contiene l'identità  $I_n$ , che ha determinante positivo.
- (e)  $GL_n^+(\mathbb{R}) < GL_n(\mathbb{R})$  è un sottogruppo: anche per lui possiamo usare il criterio per dimostrarlo. Date  $A, B \in GL_n^+(\mathbb{R})$  allora  $\det(AB^{-1}) = \det(A)\det(B)^{-1} > 0$ , quindi  $AB^{-1}$  è ancora un elemento di  $GL_n^+(\mathbb{R})$ . ✓
- (f)  $SL_n^+(\mathbb{R})$  non è un sottogruppo di  $GL_n(\mathbb{R})$ : ad esempio, non contiene gli inversi dei suoi elementi, perché data una matrice  $A \in SL_n^+(\mathbb{R})$  con  $\det(A) > 1$ , si ha che  $A^{-1} \notin SL_n^+(\mathbb{R})$ , perché ovviamente  $\det(A^{-1}) = (\det(A))^{-1} < 1$ .

I casi rimanenti li lascio per voi.

6. In  $GL_2(\mathbb{R})$ , se consideriamo le due matrici

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad \text{e} \quad b = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix},$$

abbiamo che  $ax = b$  e  $xa = b$  hanno rispettivamente soluzione

$$x = \begin{pmatrix} 1 & 1 \\ 1/2 & 1 \end{pmatrix}, \quad \text{e} \quad x = \begin{pmatrix} 1 & 1/2 \\ 1 & 1 \end{pmatrix}.$$

7. (a) Se  $a^2 = 1$  per ogni  $a \in G$ ,  $\forall a \in G: a^{-1} = a$ . Quindi  $G$  è abeliano perché

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba.$$

Provate a dimostrare con degli esempi che non vale il viceversa.

(b) Supponiamo che  $a^{-1}b^{-1} = (ab)^{-1}$  per ogni  $a, b \in G$ . Applicando tale relazione ai due elementi  $a^{-1}$  e  $b^{-1}$  di  $G$  e tenendo conto che  $a = (a^{-1})^{-1}$  e  $b = (b^{-1})^{-1}$  segue

$$ab = (a^{-1}b^{-1})^{-1} = (b^{-1})^{-1}(a^{-1})^{-1} = ba,$$

per ogni  $a, b \in G$ , cioè  $G$  è abeliano.

(c) Se  $a^2b^2 = (ab)^2$  per ogni  $a, b \in G$ , allora  $G$  è abeliano perché:

$$ab = a^{-1}(a^2b^2)b^{-1} = a^{-1}(ab)^2b^{-1} = a^{-1}(abab)b^{-1} = ba.$$

8. Se  $ab = ba$ , allora:

$$[a, b] = aba^{-1}b^{-1} = baa^{-1}b^{-1} = 1.$$

Viceversa se  $[a, b] = 1$ , allora:

$$ab = aba^{-1}b^{-1}ba = [a, b]ba = ba.$$

9. (a) Chiaramente  $1_G \in Z(G)$ , perché  $1_g g = g = g 1_g$  per ogni  $g \in G$ . Se  $x, y \in Z(G)$  e  $g \in G$  allora:

$$g(xy) = (gx)y = (xg)y = x(gy) = x(yg) = (xy)g,$$

cioè  $xy \in Z(G)$ . Infine, se  $x \in Z(G)$  e  $g \in G$  allora:

$$g^{-1}x = xg^{-1} \Rightarrow (g^{-1}x)^{-1} = (xg^{-1})^{-1} \Rightarrow x^{-1}g = gx^{-1},$$

cioè  $x^{-1} \in Z(G)$ .

- (b) Questa è quasi una tautologia:  $G$  è abeliano se e solo se  $xy = yx$  per ogni  $x, y \in G$  se e solo se  $G = Z(G)$ .

- (c) Sia  $A = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \in Z(\text{GL}_2(\mathbb{R}))$ . La condizione  $AB = BA$  applicata alle matrici diagonali implica che

$$\begin{pmatrix} b_1 a_{1,1} & b_1 a_{1,2} \\ b_2 a_{2,1} & b_2 a_{2,2} \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix} = \begin{pmatrix} b_1 a_{1,1} & b_2 a_{1,2} \\ b_1 a_{2,1} & b_2 a_{2,2} \end{pmatrix}$$

per ogni scelta di  $b_1, b_2 \in \mathbb{R}^*$ . Quindi deve valere  $b_1 a_{1,2} = b_2 a_{1,2}$  e  $b_2 a_{2,1} = b_1 a_{2,1}$  per ogni scelta di  $b_1, b_2 \in \mathbb{R}^*$ , da cui deduciamo  $a_{1,2} = a_{2,1} = 0$ . Adesso imponiamo la commutatività con le matrici “antidiagonali”:

$$\begin{pmatrix} 0 & c_1 a_{1,1} \\ c_2 a_{2,2} & 0 \end{pmatrix} = \begin{pmatrix} a_{1,1} & 0 \\ 0 & a_{2,2} \end{pmatrix} \begin{pmatrix} 0 & c_1 \\ c_2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & c_1 \\ c_2 & 0 \end{pmatrix} \begin{pmatrix} a_{1,1} & 0 \\ 0 & a_{2,2} \end{pmatrix} = \begin{pmatrix} 0 & c_1 a_{2,2} \\ c_2 a_{1,1} & 0 \end{pmatrix}$$

per ogni scelta di  $c_1, c_2 \in \mathbb{R}^*$ . Allora deve valere  $c_1 a_{1,1} = c_1 a_{2,2}$  per ogni scelta di  $c_1, c_2 \in \mathbb{R}^*$ , e quindi  $a_{1,1} = a_{2,2}$ . In totale, se  $A \in Z(\text{GL}_2(\mathbb{R}))$ , allora  $A = \lambda I_2$  per qualche  $\lambda \in \mathbb{R}^*$ . Lascio a voi dimostrare che vale anche il viceversa, e dedurre quindi che

$$Z(\text{GL}_2(\mathbb{R})) = \{\lambda I_2 \mid \lambda \in \mathbb{R}^*\}.$$

10. (a) Si ricordi che una relazione è d’equivalenza se è riflessiva, simmetrica e transitiva.

Chiaramente  $1 \cdot a \cdot 1^{-1} = a$ , quindi il coniugio è riflessivo.

Inoltre  $gag^{-1} = b$  se e solo se  $hbb^{-1} = a$  dove  $h = g^{-1}$ , quindi il coniugio è simmetrico.

Infine se  $gag^{-1} = b$  e  $hbh^{-1} = c$ , segue che

$$(hg)a(hg)^{-1} = hgag^{-1}h^{-1} = c,$$

quindi il coniugio è anche transitivo.

- (b) L’implicazione  $G$  abeliano  $\Rightarrow$  il coniugio coincide con l’uguaglianza è ovvia.

Viceversa, supponiamo che il coniugio coincida con l’uguaglianza in  $G$ . Siano  $a, b \in G$ : allora  $x = bab^{-1}$  è coniugato ad  $a$ , quindi  $x = a$ : pertanto  $a = bab^{-1}$  o, equivalentemente,  $ab = ba$ , cioè  $a$  e  $b$  commutano.

11. (a) Sia  $\varphi : (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \cdot)$ ,  $x \mapsto e^x$ . Dal corso di Analisi I dovrete sapere che

$$\varphi(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} e^{x_2} = \varphi(x_1) \varphi(x_2).$$

Deduciamo che  $\varphi$  è un omomorfismo. L'applicazione è iniettiva: infatti l'equazione  $e^x = 1$  ha come unica soluzione  $x = 0$ , cioè  $\text{Ker}(\varphi) = \{0\}$ . L'applicazione non è suriettiva: infatti  $e^x > 0$  per ogni  $x \in \mathbb{R}$ , cioè  $\text{Im}(\varphi) = (0, +\infty)$ .

- (b) Sia  $\psi : (\mathbb{R}^*, \cdot) \rightarrow (\mathbb{R}, +)$ ,  $x \mapsto \log |x|$ , e sia  $\alpha$  sia la base del logaritmo. L'applicazione non è iniettiva, poiché  $\psi(x) = \psi(-x)$ . L'applicazione è suriettiva, poiché l'equazione  $\log |x| = y$  ha come soluzioni  $x = \pm \alpha^y$ . Di nuovo da Analisi I sappiamo che

$$\psi(x_1 x_2) = \log |x_1 x_2| = \log |x_1| + \log |x_2| = \psi(x_1) + \psi(x_2),$$

quindi  $\psi$  è un omomorfismo. In particolare  $\text{ker}(\psi) = \{ \pm 1 \}$ .

- (i) Sia  $\chi : (\mathbb{C}^*, \cdot) \rightarrow (\text{GL}_2(\mathbb{R}), \cdot)$ ,  $a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$ . È facile verificare che

$$\begin{aligned} \chi((a + ib)(c + id)) &= \chi(ac - bd + i(ad + bc)) = \begin{pmatrix} ac - bd & -ad - bc \\ ad + bc & ac - bd \end{pmatrix} \\ &= \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \chi(a + ib) \chi(c + id). \end{aligned}$$

Deduciamo che  $\chi$  è un omomorfismo. Chiaramente non è suriettiva poiché

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \notin \text{Im}(\chi).$$

Infine

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} = I_2$$

se e solo se  $a = 1$ ,  $b = 0$ , cioè  $\text{Ker}(\chi) = \{1\}$ : quindi  $\chi$  è iniettiva (perché?).

I casi rimanenti sono tutti per voi.

12. (c) Sia  $\varphi : (\mathbb{Z}_{10}, +) \rightarrow (\mathbb{Z}_5, +)$ ,  $n \pmod{10} \mapsto n \pmod{5}$ . Per verificare che  $\varphi$  è ben definita, bisogna verificare che

$$n_1 \equiv n_2 \pmod{10} \quad \Rightarrow \quad n_1 \equiv n_2 \pmod{5}.$$

Poiché  $n_1 - n_2 = 10x = 5(2x)$ , deduciamo che l'implicazione indicata sopra è soddisfatta, quindi  $\varphi$  è ben definita. Il lettore verifichi che  $\varphi$  è un omomorfismo suriettivo, ma non iniettivo e che  $\text{ker}(\varphi)$  è costituito dalle classi di 0 e di 5.

- (e) Sia  $\psi : (\mathbb{Z}_4, +) \rightarrow (\mathbb{Z}_5, +)$ ,  $n \pmod{4} \mapsto n \pmod{5}$ . Si noti che  $0 \equiv 4 \pmod{4}$ , ma  $0 \not\equiv 4 \pmod{5}$ , quindi  $\psi$  non è un'applicazione ben definita (cioè non è un'applicazione).

Lascio a voi gli altri punti dell'esercizio.

13. Dato un gruppo  $G$ , il suo insieme degli automorfismi è

$$\text{Aut}(G) = \{f : G \rightarrow G \mid f \text{ è un isomorfismo}\}.$$

Consideriamo la coppia  $(\text{Aut}(G), \circ)$ , dove  $\circ$  è l'usuale composizione di funzioni, che già sappiamo essere associativa. L'elemento neutro è l'applicazione identità  $\text{id}_G : G \rightarrow G$ , che manda qualsiasi elemento  $g \in G$  in se stesso. Inoltre, per ogni  $f \in \text{Aut}(G)$  sappiamo che esiste l'applicazione inversa, cioè  $f^{-1} \in \text{Aut}(G)$  tale che  $f \circ f^{-1} = f^{-1} \circ f = \text{id}_G$ . Concludiamo quindi che  $(\text{Aut}(G), \circ)$  è un gruppo.

14. Utilizziamo la notazione moltiplicativa sia in  $G$  che in  $H$ , e usiamo il criterio per sottogruppi. Siano  $g, h \in K$ : poiché  $\varphi$  e  $\psi$  sono omomorfismi di gruppi moltiplicativi

$$\varphi(gh^{-1}) = \varphi(g)\varphi(h^{-1}) = \varphi(g)\varphi(h)^{-1} = \psi(g)\psi(h)^{-1} = \psi(g)\psi(h^{-1}) = \psi(gh^{-1}),$$

cioè  $gh^{-1} \in K$ , e quindi  $K$  è un sottogruppo di  $G$

15. Vi lascio la verifica che  $\varphi$  è un omomorfismo se e solo se  $G$  è abeliano (che comunque trovate negli appunti del 18 ottobre). Per la seconda parte, si noti che

$$\varphi^2(g) = \varphi(g^{-1}) = (g^{-1})^{-1} = g = \text{id}(g),$$

dunque  $\varphi$  è biiettivo.

**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!