

Istituzioni di Algebra e Geometria — Algebra, a.a. 2025-2026
Soluzioni foglio 6

1. (a) Applicando quanto dimostrato nell'esercizio 2 del foglio 2, visto che A è un gruppo abeliano, segue che lo stesso è vero per A^X . Resta da dimostrare che l'operazione di prodotto è associativa, e che valgono le proprietà distributive. Siano quindi $\varphi, \psi, \chi \in A^X$, e sia $x \in X$; allora:

$$\varphi(\psi\chi)(x) = \varphi(x)(\psi\chi(x)) = \varphi(x)(\psi(x)\chi(x)) = (\varphi(x)\psi(x))\chi(x) = (\varphi\psi(x))\chi(x) = \varphi(\psi\chi)(x),$$

cioè il prodotto è associativo. Inoltre:

$$\varphi(\psi + \chi)(x) = \varphi(x)(\psi(x) + \chi(x)) = \varphi(x)\psi(x) + \varphi(x)\chi(x) = \varphi\psi(x) + \varphi\chi(x),$$

quindi vale la proprietà distributiva a sinistra; in maniera simile si verifica che vale anche la distributività a destra.

- (b) Se A è commutativo allora, in base alla definizione data per il prodotto, abbiamo

$$\begin{aligned} \varphi\psi: X &\rightarrow A \\ x &\mapsto (\varphi\psi)(x) = (\varphi(x))(\psi(x)), \end{aligned}$$

$$\begin{aligned} \psi\varphi: X &\rightarrow A \\ x &\mapsto (\psi\varphi)(x) = (\psi(x))(\varphi(x)), \end{aligned}$$

cioè $\varphi\psi = \psi\varphi$ come funzioni. Viceversa, supponiamo che A^X sia commutativo, e siano $a, b \in A$. Allora possiamo definire le seguenti funzioni costanti in A^X

$$\begin{aligned} \varphi: X &\rightarrow A \\ x &\mapsto a, \end{aligned}$$

$$\begin{aligned} \psi: X &\rightarrow A \\ x &\mapsto b. \end{aligned}$$

Scelto $c \in A$ abbiamo allora

$$ab = \varphi(c)\psi(c) = (\varphi\psi)(c) = (\psi\varphi)(c) = \psi(c)\varphi(c) = ba :$$

deduciamo che A è commutativo.

- (c) Se A è unitario e 1_A è la sua unità, si verifica che la funzione costante

$$\begin{aligned} \epsilon: X &\rightarrow A \\ x &\mapsto 1_A \end{aligned}$$

che associa ad ogni elemento di X 1_A è l'unità dell'anello A^X . Viceversa, se A^X è unitario e ϵ è la sua unità, significa che per ogni $\varphi \in A^X$

$$(\varphi\epsilon)(x) = \varphi(x)\epsilon(x) = \varphi(x) = \epsilon(x)\varphi(x) = (\epsilon\varphi)(x).$$

In particolare, se fissiamo un qualsiasi elemento $a \in A$ e applichiamo la proprietà alla funzione costante φ definita nella parte (b), allora

$$(\varphi\epsilon)(x) = a\epsilon(x) = a,$$

per cui necessariamente ϵ è una funzione costante, e la sua immagine è l'unità di A .

2. Abbiamo visto nell'esercizio precedente che la funzione costante ϵ è l'unità di A^X . Similmente, si può verificare che lo zero di A^X è la funzione costante

$$\begin{aligned} \omega: X &\rightarrow A \\ x &\mapsto 0_A. \end{aligned}$$

- (a) L'applicazione $\varphi \in A^X$ è invertibile se e solo se esiste $\psi \in A^X$ tale che $\varphi\psi = \epsilon$ come applicazioni, cioè se e solo se per ogni $x \in X$ si ha

$$\varphi(x)\psi(x) = (\varphi\psi)(x) = \epsilon(x) = 1_A.$$

Questo si può verificare se e solo se $\text{Im}(\varphi) \subseteq A^*$, dove vi ricordo che la notazione A^* indica gli elementi invertibili dell'anello A .

- (b) Nel caso in cui o X o A si riducono a un solo elemento, non c'è praticamente niente da dimostrare. Supponiamo che sia X che A abbiano almeno due elementi distinti: sia $x_0 \in X$ fissato e si consideri

$$\begin{aligned} \varphi: X &\rightarrow A \\ x &\mapsto \begin{cases} 0_A & \text{se } x = x_0, \\ 1_A & \text{se } x \neq x_0. \end{cases} \end{aligned}$$

Per quanto visto sopra φ non è invertibile in A^X : d'altra parte φ non è l'applicazione nulla ω . Concludiamo che A^X non è un corpo anche se A lo è.

- (c) Di nuovo, il caso in cui o X o A si riducono a un solo elemento è banale. Supponiamo che sia X che A abbiano almeno due elementi distinti e siano $x_0 \in X$ e $\varphi \in A^X$ definiti come sopra. Posto

$$\begin{aligned} \psi: X &\rightarrow A \\ x &\mapsto \begin{cases} 1_A & \text{se } x = x_0, \\ 0_A & \text{se } x \neq x_0, \end{cases} \end{aligned}$$

segue che $\psi \neq \omega$ ma

$$(\varphi\psi)(x_0) = \varphi(x_0)\psi(x_0) = 0_A \cdot 1_A = 0_A = \omega(x_0)$$

e che

$$(\varphi\psi)(x) = \varphi(x)\psi(x) = 1_A \cdot 0_A = 0_A = \omega(x)$$

per ogni $x \in X \setminus \{x_0\}$, dunque $\varphi\psi = \omega$, cioè A^X contiene sempre divisori dello zero.

3. (a) È vero che se $ab = b$ per ogni $b \in A$ allora $a = 1_A$, infatti basta applicare tale proprietà all'elemento $b = 1_A$, e otteniamo $a = a1_A = 1_A$.
- (b) Sia $a \in A$ invertibile, e siano b_1 e b_2 due inversi moltiplicativi, quindi $ab_1 = b_1a = 1_A$ e $ab_2 = b_2a = 1_A$. Allora

$$b_1 = b_11_A = b_1(ab_2) = (b_1a)b_2 = 1_Ab_2 = b_2.$$

4. (a) L'insieme L consiste in tutte e sole le matrici triangolari inferiori, cioè della forma

$$\begin{pmatrix} a_{11} & 0 \\ a_{21} & a_{22} \end{pmatrix}$$

per qualche $a_{11}, a_{21}, a_{22} \in \mathbb{R}$. È facile verificare che L è un sottoanello (unitario) di $\mathbb{R}^{2,2}$.

- (b) L'insieme A consiste in tutte e sole le matrici aventi diagonale nulla, cioè della forma

$$\begin{pmatrix} 0 & a_{12} \\ a_{21} & 0 \end{pmatrix}$$

per qualche $a_{12}, a_{21} \in \mathbb{R}$. È facile verificare che A è sottogruppo additivo di $\mathbb{R}^{2,2}$, però non è chiuso rispetto al prodotto, infatti ad esempio:

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = I_2 \notin A.$$

- (c) L'insieme B consiste in tutte e sole le matrici strettamente triangolari superiori, cioè della forma

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix}$$

per qualche $a \in \mathbb{R}$. Come prima, è facile verificare che B è sottogruppo additivo. Però stavolta osserviamo che il prodotto di due elementi di B

$$\begin{pmatrix} 0 & a \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$$

è la matrice nulla, che appartiene ancora a B . Quindi B è un sottoanello di $\mathbb{R}^{2,2}$: è commutativo, ma non unitario.

- (d) L'insieme C consiste in tutte e sole le matrici della forma

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

per qualche $a \in \mathbb{R}$. Ancora una volta, si verifica che B è sottogruppo additivo. Osserviamo che

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ab & 0 \\ 0 & 0 \end{pmatrix} \in C.$$

Quindi C è un sottoanello di $\mathbb{R}^{2,2}$: è commutativo ed unitario (ma con unità diversa da quella di $\mathbb{R}^{2,2}$).

5. Usiamo il criterio per sottoanelli: siano $a_1, a_2 \in Z(A)$. Allora per ogni $b \in A$:

$$(a_1 - a_2)b = a_1b + (-a_2)b = a_1b + (-a_2b) = a_1b - a_2b,$$

$$b(a_1 - a_2) = ba_1 + b(-a_2) = ba_1 + (-ba_2) = ba_1 - ba_2 :$$

dall'ipotesi $a_1, a_2 \in Z(A)$ deduciamo che $a_1b = ba_1$ e $a_2b = ba_2$, quindi $-a_2b = -ba_2$. Concludiamo che $(a_1 - a_2)b = b(a_1 - a_2)$, cioè $a_1 - a_2 \in Z(A)$.

Inoltre

$$(a_1a_2)b = a_1(a_2b) = a_1(ba_2) = (a_1b)a_2 = (ba_1)a_2 = b(a_1a_2),$$

quindi anche il prodotto $a_1a_2 \in Z(A)$. Concludiamo che $Z(A)$ è un sottoanello di A .

Non è difficile verificare che $Z(A)$ è unitario se A lo è.

6. (a) Come prima cosa, osserviamo che I_x è un sottoinsieme proprio di A^X ; presi $\varphi, \psi \in I_x$ si ha

$$(\varphi - \psi)(x) = \varphi(x) - \varphi(y) = 0_A - 0_A = 0_A,$$

quindi $\varphi - \psi \in I_x$. Se poi $f \in A^X$ è una qualsiasi altra applicazione $X \rightarrow A$:

$$(\varphi f)(x) = \varphi(x)f(x) = 0_A f(x) = 0_A,$$

$$(f\varphi)(x) = f(x)\varphi(x) = f(x)0_A = 0_A,$$

dunque $\varphi f, f\varphi \in I_x$, e quindi I_x è un ideale.

(b) Se consideriamo la funzione costante ω definita nell'esercizio 2, per ogni $\varphi \in J_x$ si ha

$$(\varphi\omega)(x) = \varphi(x)\omega(x) = 1_A \cdot 0_A = 0_A \neq 1_A,$$

$$(\omega\varphi)(x) = \omega(x)\varphi(x) = 0_A \cdot 1_A = 0_A \neq 1_A.$$

Quindi J_x non è un ideale.

(c) Consideriamo le funzioni

$$\varphi': X \rightarrow A$$

$$x \mapsto \begin{cases} 0_A & \text{se } x = x', \\ 1_A & \text{se } x \neq x'. \end{cases}$$

$$\varphi'': X \rightarrow A$$

$$x \mapsto \begin{cases} 1_A & \text{se } x = x', \\ 0_A & \text{se } x \neq x'. \end{cases}$$

Chiaramente $\varphi' \in I_{x'}$. Inoltre $x'' \neq x'$ dunque $\varphi''(x'') = 0_A$, cioè $\varphi'' \in I_{x''}$. Inoltre

$$(\varphi' + \varphi'')(x) = \varphi'(x) + \varphi''(x) = \begin{cases} 0_A + 1_A = 1_A & \text{se } x = x', \\ 1_A + 0_A = 1_A & \text{se } x \neq x'. \end{cases}$$

Quindi φ coincide con l'unità $\epsilon \in A^X$.

7. (a) Applicando al caso $G = X$ l'esercizio 2 del foglio 2, sappiamo che G^G è un gruppo abeliano additivo. Osserviamo che $\text{End}(G) \subseteq G^G$ è in realtà un sottogruppo: infatti, date $\varphi, \psi \in \text{End}(G)$ allora $\varphi - \psi$ è ancora un endomorfismo, quindi la condizione del criterio per sottogruppi è verificata.

Osserviamo poi che se $\varphi, \psi \in \text{End}(G)$ allora risulta anche $\varphi \circ \psi \in \text{End}(G)$. Infatti la composizione di due endomorfismi è ancora un endomorfismo:

$$\begin{aligned}\varphi \circ \psi(g' + g'') &= \varphi(\psi(g' + g'')) = \varphi(\psi(g') + \psi(g'')) = \\ &= \varphi(\psi(g')) + \varphi(\psi(g'')) = \varphi \circ \psi(g') + \varphi \circ \psi(g'').\end{aligned}$$

Con questa operazione si verifica che $\text{End}(G)$ è un anello. Inoltre l'applicazione identica id è banalmente un omomorfismo, quindi è in $\text{End}(G)$ e si ha $\varphi \circ id = id \circ \varphi = \varphi$: deduciamo che id è l'unità di $\text{End}(G)$.

- (b) In generale è ben noto che $\varphi \circ \psi \neq \psi \circ \varphi$. Per esempio se G è il gruppo additivo \mathbb{R}^2 e consideriamo $A, B \in \mathbb{R}^{2,2}$, allora le applicazioni

$$\begin{aligned}\mu_A: \mathbb{R}^2 &\rightarrow \mathbb{R}^2 \\ X &\mapsto AX\end{aligned}$$

$$\begin{aligned}\mu_B: \mathbb{R}^2 &\rightarrow \mathbb{R}^2 \\ X &\mapsto BX\end{aligned}$$

commutano se e solo se $AB = BA$: è facile trovare esempi di matrici per cui ciò non accade.

- (c) Si noti che I è l'insieme degli endomorfismi di G contenenti nel loro nucleo il sottogruppo di torsione $T(G)$ (i dettagli sul sottogruppo di torsione li trovate nell'esercizio 7 del foglio 3). Se $\varphi \in I$, $\psi \in \text{End}(G)$ e $g \in T(G)$ ha ordine $n \in \mathbb{N}$ si ha $\varphi(g) = 0_G$ e

$$n\psi(g) = \psi(n g) = \psi(0_G) = 0_G,$$

quindi anche $\psi(g) \in T(G)$. Quindi per definizione di I

$$\varphi \circ \psi(g) = \varphi(\psi(g)) = 0_G, \quad \psi \circ \varphi(g) = \psi(\varphi(g)) = \psi(0_G) = 0_G.$$

Quindi I è un ideale di $\text{End}(G)$.

8. (a) Ricordiamo che la caratteristica di un anello unitario A coincide con l'ordine (additivo) dell'elemento 1_A . Da una parte, osserviamo che, poiché φ è un omomorfismo per ipotesi:

$$\varphi(2 \cdot 1_A) = \varphi(1_A + 1_A) = \varphi(1_A) + \varphi(1_A) = 1_A + 1_A = 2 \cdot 1_A.$$

D'altra parte, per definizione:

$$\varphi(2 \cdot 1_A) = (2 \cdot 1_A)^2 = 4 \cdot 1_A^2 = 4 \cdot 1_A.$$

Quindi $4 \cdot 1_A = 2 \cdot 1_A$, e, usando la legge di cancellazione, questo implica $2 \cdot 1_A = 0_A$, quindi $\text{char}(A) = 2$. Dati $a, b \in A$, da una parte si ha che

$$\varphi(a+b) = \varphi(a) + \varphi(b) = a^2 + b^2,$$

dall'altra:

$$\varphi(a+b) = (a+b)^2 = a^2 + ab + ba + b^2,$$

quindi necessariamente $ab + ba = 0_A$, cioè $ab = -ba$.

Poiché $\text{char}(A) = 2$, $0_A = 2 \cdot (ba) = ba + ba$, quindi $ba = -ba$. Ma allora $ab = -ba = ba$, l'anello è commutativo.

- (b) Sia $a \in \text{Ker}(\varphi)$. Allora $\varphi(a) = a^2 = 0_A$. Calcoliamo

$$(1_A + a)(1_A - a) = 1_A^2 + 1_A(-a) + a1_A - a^2 = 1_A - a^2 = 1_A,$$

quindi $1_A - a = (1_A + a)^{-1}$

- (c) Visto che abbiamo dimostrato che se φ è omomorfismo allora A ha caratteristica 2, vediamo se il caso di \mathbb{Z}_2 può essere un esempio valido. Per mostrare che effettivamente lo è, siano $\bar{a}, \bar{b} \in \mathbb{Z}_2$, allora:

$$\varphi(\bar{a} + \bar{b}) = (\bar{a} + \bar{b})^2 = \bar{a}^2 + \bar{b}^2 + 2\bar{a}\bar{b} = \bar{a}^2 + \bar{b}^2 = \varphi(\bar{a}) + \varphi(\bar{b}),$$

$$\varphi(\bar{a}\bar{b}) = \varphi(\bar{a}\bar{b}) = \bar{a}\bar{b}^2 = \bar{a}^2\bar{b}^2.$$

9. (a) $(2a)^3 = (a+a)^3 = 8a^3 = 8a$, dove l'ultima uguaglianza segue dalla relazione $a^3 = a$.
 (b) Poiché $a^3 = a$ per ogni $a \in A$, si ha $2a = (2a)^3 = 8a$, dunque $6a = 0_A$ per ogni $a \in A$: in particolare preso $a = 1_A$ risulta $6 \cdot 1_A = 0_A$, quindi $\text{char}(A)$ (che è l'ordine additivo di 1_A) è un divisore di 6, cioè 2, 3 o 6.
 (c) Basta considerare gli anelli $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_6$.
10. (a) Per ogni $a \in I$, $a = a^1 \in I$, quindi $I \subseteq \sqrt{I}$.
 (b) Se $a \in \sqrt{I}$, per definizione esiste $n \in \mathbb{N}$ tale che $a^n \in I$. Poiché I è un ideale, per ogni $m \in \mathbb{N}$, $m \geq n$, vale che $a^m = a^{m-n} \cdot a^n$ è un prodotto di un elemento di A per uno di I , quindi appartiene a I .
 (c) Se $a \in \sqrt{I}$, per definizione esiste $n \in \mathbb{N}$ tale che $a^n \in I$, e vale che $(-a)^n = \pm a^n \in I$, cioè $-a \in \sqrt{I}$. Sia ora b un altro elemento di \sqrt{I} : esiste $m \in \mathbb{N}$ tale che $b^m \in I$. Sia $N = n + m$; poiché A è commutativo, vale che

$$(a+b)^N = \sum_{i=0}^N \binom{N}{i} a^i b^{N-i},$$

e tutti gli addendi di questa somma appartengono a I . Infatti, se $i < n$, allora $N - i > m$, e quindi

$$\binom{N}{i} a^i b^{N-i} = \binom{N}{i} a^i b^{N-i-m} b^m \in I.$$

Similmente, se $i \geq n$, allora

$$\binom{N}{i} a^i b^{N-i} = \binom{N}{i} a^{i-n} b^{N-i} a^n \in I.$$

In totale quindi $(a+b)^N \in I$, e quindi $a+b \in \sqrt{I}$.

- (d) Intanto, $0_A \in \sqrt{I}$, che è quindi diverso dal vuoto. Inoltre, se $a, b \in \sqrt{I}$ per quanto dimostrato nella parte precedente anche $a + (-b) = a - b \in \sqrt{I}$, che quindi è un sottogruppo additivo. Infine, siano $a \in \sqrt{I}$ e $x \in A$. Sappiamo che esiste $n \in \mathbb{N}$ tale che $a^n \in I$, e quindi: $(ax)^n = a^n x^n \in I$, cioè $ax = xa \in I$.

11. (a) Si tratta di una verifica immediata. Sappiamo già che con l'operazione componente per componente il prodotto cartesiano di due gruppi abeliani è un gruppo abeliano a sua volta. Verifichiamo che il prodotto è associativo: dati $a_1, a_2, a_3 \in A$ e $b_1, b_2, b_3 \in B$, abbiamo che

$$\begin{aligned} ((a_1, b_1) \cdot (a_2, b_2)) \cdot (a_3, b_3) &= (a_1 a_2, b_1 b_2) \cdot (a_3, b_3) = ((a_1 a_2) a_3, (b_1 b_2) b_3) \\ &= (a_1 (a_2 a_3), b_1 (b_2 b_3)) = (a_1, b_1) \cdot ((a_2, b_2) \cdot (a_3, b_3)). \end{aligned}$$

Inoltre:

$$\begin{aligned} (a_1, b_1) \cdot ((a_2, b_2) + (a_3, b_3)) &= (a_1, b_1) \cdot (a_2 + a_3, b_2 + b_3) = (a_1 (a_2 + a_3), b_1 (b_2 + b_3)) \\ &= (a_1 a_2 + a_1 a_3, b_1 b_2 + b_1 b_3) = (a_1, b_1) \cdot (a_2, b_2) + (a_1, b_1) \cdot (a_3, b_3), \end{aligned}$$

e l'altra proprietà distributiva è analoga.

Inoltre $A \times B$ è unitario, e la sua unità è l'elemento $(1_A, 1_B)$.

- (b) Questa è un conto diretto: $(a, b) \cdot (a', b') = (a', b') \cdot (a, b)$ se e solo se $aa' = a'a$ e $bb' = b'b$.
(c) Sia le immersioni i_A e i_B che le proiezioni p_A e p_B sono omomorfismi di anelli, infatti:

$$\begin{aligned} i_A(a + a') &= (a + a', 0_B) = (a, 0_B) + (a', 0_B) = i_A(a) + i_A(a'), \\ i_A(aa') &= (aa', 0_B) = (a, 0_B) \cdot (a', 0_B) = i_A(a) \cdot i_A(a'), \end{aligned}$$

e lo stesso identico ragionamento si applica a i_B , p_A e p_B . La differenza è che i_A e i_B non sono omomorfismi di anelli unitari, visto che $i_A(1_A) = (1_A, 0_B) \neq 1_{A \times B}$ e $i_B(1_B) = (0_A, 1_B) \neq 1_{A \times B}$, mentre $p_A(1_A, 1_B) = 1_A$ e $p_B(1_A, 1_B) = 1_B$.

- (d) Da quanto visto a lezione, sappiamo che $\text{Im}(i_A) \subseteq A \times B$, essendo immagine di un omomorfismo di anelli, è un sottoanello. Inoltre, dato un qualsiasi elemento $(a, b) \in A \times B$ e un qualsiasi $(a', 0_B) \in \text{Im}(i_A)$, abbiamo che $(a, b) \cdot (a', 0_B) = (aa', b0_B) = (aa', 0_B) \in \text{Im}(i_A)$, cioè l'immagine è un ideale. L'osservazione banale che ogni elemento di $\text{Im}(i_A)$ si scrive come $(a, 0_B) = (a1_A, 0_B) = (a, 0_B) \cdot (1_A, 0_B)$ mostra che $\text{Im}(i_A)$ è generato da $(1_A, 0_B)$.
Il ragionamento per $\text{Im}(i_B)$ è identico.

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!