Istituzioni di Algebra e Geometria — Algebra, a.a. 2023-2024
Soluzioni foglio 5

1. (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 $\mathbb{R}^{2,2}$).

2. Usiamo il criterio per sottoanelli: siano $a', a'' \in Z(A)$. Allora

$$(a' - a'')b = a'b + (-a'')b = a'b + (-a''b) = a'b - a''b,$$

$$b(a' - a'') = ba' + b(-a'') = ba' + (-ba'') = ba' - ba'' :$$

dall'ipotesi $a', a'' \in Z(A)$ deduciamo che $a'b = ba'$ e $a''b = ba''$, quindi $-a''b = -ba''$. Concludiamo che $(a' - a'')b = b(a' - a'')$, cioè $a' - a'' \in A$.

Inoltre

$$(a'a'')b = a'(a''b) = a'(ba'') = (a'b)a'' = (ba')a'' = b(a'a''),$$

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

Provate a verificare che $Z(A)$ è unitario se A lo è.

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

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

4. (a) Lascio a voi questa verifica.
   (b) Se A è commutativo allora, in base alla definizione data per il prodotto, abbiamo

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

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

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

$$\begin{aligned} \varphi\colon X &\to A \\ x &\mapsto a, \end{aligned}$$

$$\begin{aligned} \psi\colon X &\to A \\ x &\mapsto b. \end{aligned}$$

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

$$\begin{aligned} \epsilon\colon X &\to A \\ x &\mapsto 1_A. \end{aligned}$$

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.

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

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

(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

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

Ciò si può verificare se e solo se $\operatorname{Im}(\varphi) \subseteq A^*$.

(b) Lascio a voi analizzare il caso in cui o X o A si riducono a un solo elemento. Supponiamo che sia X che A abbiano almeno due elementi distinti: sia $x_0 \in X$ fissato e si consideri

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

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.
Invece cosa si può dire su A se si sa che A^X è un campo?

(c) Di nuovo, a voi il caso in cui o X o A si riducono a un solo elemento. 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

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

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 $\varphi\psi = \omega$.

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 $X \to A$:

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

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

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 precedente, 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

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

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

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. Le affermazioni (a), (b), (c), sono tutte false se si ammette che l'applicazione nulla sia un omomorfismo. Se invece consideriamo solo gli omomorfismi di anelli unitari, la situazione cambia.

   (a) È vero che esiste un unico omomorfismo di anelli $\mathbb{Z} \to \mathbb{Z}$: esso è l'omomorfismo unitario (che abbiamo introdotto durante a lezione), che su $\mathbb{Z}$ coincide con l'identità.

   (b) Anche questa affermazione è vera: poiché $\mathbb{Q}$ è un campo, ogni omomorfismo $\varphi : \mathbb{Q} \to \mathbb{Q}$ non nullo è un isomorfismo. Poiché $\varphi(1) = 1$, per ogni $n \in \mathbb{Z}$ si ha $\varphi(n) = \varphi(n \cdot 1) = n$, quindi φ induce l'identità su $\mathbb{Z}$. Sia ora $\frac{a}{b}$ con $a, b \in \mathbb{Z}$: allora

   $$\varphi(\tfrac{a}{b}) = \varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = ab^{-1} = \tfrac{a}{b},$$

   quindi φ è l'identità.

   (c) Lascio a voi dimostrare, con lo stesso metodo utilizzato sopra, che φ induce l'identità su $\mathbb{Q} \subseteq \mathbb{R}$. Sia ora $x \in (0, +\infty)$: allora esiste $y \in \mathbb{R}$ tale che $x = y^2$, quindi

   $$\varphi(x) = \varphi(y^2) = \varphi(y)^2 \in (0, +\infty),$$

   cioè φ manda $(0, +\infty)$ in $(0, +\infty)$. Segue che se $x, y \in \mathbb{R}$ e $x > y$ allora $x - y > 0$, dunque

   $$\varphi(x) - \varphi(y) = \varphi(x - y) > 0 \quad \Rightarrow \quad \varphi(x) > \varphi(y).$$

   Supponiamo che esista $x \in \mathbb{R}$ tale che $\varphi(x) \neq x$: per fissare le idee supponiamo $x > \varphi(x)$. Prendiamo un razionale $q \in \mathbb{Q}$ tale che $\varphi(x) < q < x$. Applicando φ dovremmo avere $\varphi(q) < \varphi(x)$, ma $\varphi(q) = q > \varphi(x)$, una contraddizione. Quindi anche questa affermazione è vera, e l'unico omomorfismo $\mathbb{R} \to \mathbb{R}$ è l'identità.

   (d) L'analisi dell'applicazione coniugio $\mathbb{C} \to \mathbb{C}$ la lascio a voi.

8. (a) Dall'Esercizio 4 del foglio 2, sappiamo che G^X è un gruppo abeliano additivo. Osserviamo che $\mathrm{End}(G) \subseteq G^X$: verificate che si tratta di un sottogruppo. Osserviamo poi che se $\varphi, \psi \in \mathrm{End}(G)$ allora risulta anche $\varphi \circ \psi \in \mathrm{End}(G)$. Infatti

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

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

   (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

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

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

   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 $T(G)$. Se $\varphi \in I$, $\psi \in \mathrm{End}(G)$ e $g \in T(G)$ ha ordine $n \in \mathbb{N}$ si ha $\varphi(g) = 0_G$ e

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

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

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

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

9. (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 $\mathrm{char}(A) = 2$.

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

(c) Sia $a \in \mathrm{Ker}(\varphi)$. 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 $1_A - a = (1_A + a)^{-1}$

(d) 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:

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

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

10. Lo svolgimento di questo esercizio è una serie di verifiche più o meno dirette, le lascio a voi.

11. (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 $ax = xa \in I$.

12. (a) Lascio a voi questa prima parte.

    (b) È una conseguenza del fatto che le applicazioni p_A e p_B definite nell'esercizio precedente sono epimorfismi: a lezione abbiamo visto che questo implica che l'immagine di un ideale è un ideale.

    (c) Sempre a lezione, abbiamo visto che il fatto che p_A e p_B sono omomorfismi implica che $p_A^{-1}(I)$ e $p_B^{-1}(J)$ sono ideali, dunque lo stesso vale per $p_A^{-1}(I) \cap p_B^{-1}(J)$. Se $(a, b) \in H$ allora $a \in I$ e $b \in J$, dunque

$$p_A^{-1}(a) = \{(a, y) \mid y \in B\}, \qquad p_B^{-1}(b) = \{(x, b) \mid x \in A\}.$$

In particolare $(a, b) \in p_A^{-1}(I) \cap p_B^{-1}(J)$, quindi $H \subseteq p_A^{-1}(I) \cap p_B^{-1}(J)$.

    (d) La prima parte dell'affermazione è ovvia. Inoltre $(1, 0)(a, b') = (a, 0)$ e $(0, 1)(a', b) = (0, b)$.

    (e) Se $(a, b) \in p_A^{-1}(I) \cap p_B^{-1}(J)$, allora $a \in I$ e $b \in J$, dunque per quanto abbiamo appena dimostrato ci sono $a' \in A$ e $b' \in B$ tali che $(a, b'), (a', b) \in H$. Allora $(a, 0) \in (1, 0)(a, b') \in H$ e $(0, b) = (0, 1)(a', b) \in H$ perché H è un ideale. Per lo stesso motivo

$$(a, b) = (a, 0) + (0, b) = (1, 0)(a, b') + (0, 1)(a', b) \in H,$$

quindi $H \subseteq p_A^{-1}(I) \cap p_B^{-1}(J)$.

(f) Se $I \subseteq A$ e $J \subseteq B$ sono ideali, per la parte (a) anche $I \times J \subseteq A \times B$ lo è. Viceversa, se $H \subseteq A \times B$ è un ideale, allora per la parte (b) anche $I = p_A(H) \subseteq A$ e $J = p_B(H) \subseteq B$ sono ideali tali che $H \subseteq p_A^{-1}(I) \cap p_B^{-1}(J)$ (per la parte (c)) e $p_A^{-1}(I) \cap p_B^{-1}(J) \subseteq H$ (per la parte (e)), dunque $p_A^{-1}(I) \cap p_B^{-1}(J) = H$. Verificate che $p_A^{-1}(I) = I \times B$ e $p_B^{-1}(J) = A \times J$, dunque

$$H = (I \times B) \cap (A \times J) = I \times J.$$

13. (a) Dati due interi $n, m \in \mathbb{Z}$, esistono $x, y \in \mathbb{Z}$ tali che $z = xn + ym$ se e solo se z è multiplo di $d = \mathrm{MCD}(n, m)$. Quindi

$$\begin{aligned}(n) + (m) &= \{z \in \mathbb{Z} \mid z = z_1 + z_2, z_1 \in (n), z_2 \in (m)\} \\ &= \{z \in \mathbb{Z} \mid z = xn + ym, \text{per qualche } x, y \in \mathbb{Z}\} \\ &= \{z \in \mathbb{Z} \mid z = kd, d = \mathrm{MCD}(n, m), k \in \mathbb{Z}\} = (d).\end{aligned}$$

(b) Questa è una verifica abbastanza facile, la lascio a voi.

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!