Istituzioni di Algebra e Geometria — Algebra, a.a. 2024-2025

# Soluzioni foglio 1

1. Le mappe e gli insiemi dell'esercizio possono essere illustrati così:

$$X \underset{\varphi'}{\overset{\varphi}{\rightleftarrows}} Y \underset{\psi'}{\overset{\psi}{\rightleftarrows}} Z$$

   (a) Siano $x_1, x_2 \in X$ tali che $(\psi \circ \varphi)(x_1) = (\psi \circ \varphi)(x_2)$. Allora $\psi(\varphi(x_1)) = \psi(\varphi(x_2))$; siccome $\psi$ è iniettiva, deve valere $\varphi(x_1) = \varphi(x_2)$. Siccome anche $\varphi$ è iniettiva, deve valere $x_1 = x_2$.

   (b) Sia $z \in Z$ un elemento qualsiasi. Poiché $\psi$ è suriettiva, esiste $y \in Y$ tale che $z = \psi(y)$; poiché $\varphi$ è suriettiva, esiste $x \in X$ tale che $y = \varphi(x)$. Quindi $z = \psi(y) = \psi(\varphi(x)) = (\psi \circ \varphi)(x)$.

   (c) Supponiamo che $\psi$ sia biettiva e che la composizione $\psi \circ \varphi$ sia iniettiva, e siano $x_1, x_2 \in X$ tali che $\varphi(x_1) = \varphi(x_2)$, e quindi $(\psi \circ \varphi)(x_1) = \psi(\varphi(x_1)) = \psi(\varphi(x_2)) = (\psi \circ \varphi)(x_2)$. Siccome la composizione $\psi \circ \varphi$ è iniettiva, segue che $x_1 = x_2$, e quindi $\varphi$ è iniettiva. Il viceversa segue direttamente dalla parte (a), perché biettiva implica iniettiva.

   (d) Supponiamo che $\varphi$ sia biettiva e che la composizione $\psi \circ \varphi$ sia suriettiva, e sia $z \in Z$. Poiché $\psi \circ \varphi$ è suriettiva, $\exists\, x \in X$ tale che $z = \psi(\varphi(x))$: ma allora $z = \psi(y)$ appartiene all'immagine di $\psi$, cioè $\psi$ è suriettiva. Il viceversa segue direttamente dalla parte (b), perché biettiva implica suriettiva.

   (e) Sia $x \in X$, e consideriamo i due elementi $\varphi(x), \varphi'(x) \in Y$. Sappiamo che $(\psi \circ \varphi)(x) = (\psi \circ \varphi')(x)$, e quindi $\psi(\varphi(x)) = \psi(\varphi'(x))$. Poiché $\psi$ è iniettiva, questo implica $\varphi(x) = \varphi'(x)$, cioè $\varphi = \varphi'$.

   (f) Sia $y \in Y$, e consideriamo i due elementi $\psi(y), \psi'(y) \in Z$. Siccome $\varphi$ è suriettiva, sappiamo che $\exists\, x \in X$ tale che $y = \varphi(x)$. Ma allora $(\psi \circ \varphi)(x) = (\psi' \circ \varphi)(x)$, e quindi $\psi(y) = \psi'(y)$, cioè $\psi = \psi'$.

2. (a) Sia $y \in Y$; ci domandiamo se $(\varphi \circ \psi_i)(y) = y$. Se $y \neq \bar{y}$, allora $(\varphi \circ \psi_i)(y) = (\varphi \circ \psi)(y) = y$, mentre se $y = \bar{y}$ allora $(\varphi \circ \psi_i)(\bar{y}) = \varphi(\psi_i(\bar{y})) = \varphi(x_i) = \bar{y}$, quindi siamo a posto.

   (b) Semplicemente, se $\varphi$ non fosse iniettiva allora esisterebbero $x_1, x_2 \in X$ tali che $x_1 \neq x_2$ e $\varphi(x_1) = \varphi(x_2)$, quindi applicando quanto visto nella parte (a) riusciremmo a costruire due inverse destre diverse di $\varphi$.

3. (a) La verifica che le $\psi_i$ sono entrambe inverse sinistre di $\varphi$ è immediata, si fa come la parte (a) dell'esercizio 2 qua sopra.

(b) Similmente all'esercizio precedente, se esistesse $y \in Y \setminus \mathrm{Im}(\varphi)$ potremmo costruire due inverse sinistre distinte come nella parte (a).

4. (a) Questa dimostrazione è l'esempio 3.15 nelle note di Casnati sul principio di induzione.
`https://staff.polito.it/ada.boralevi/didattica/note/GfC_lez3.pdf`
È un po' lunga, ma non difficile; il trucco è usare l'uguaglianza

$$\binom{n}{h-1} + \binom{n}{h} = \binom{n+1}{h}.$$

(b) Dobbiamo dimostrare che per ogni $n \geq 1$ e per ogni $a \in [-1, +\infty)$ si ha $(1+a)^n \geq 1 + na$.
Se $n = 1$ allora $(1+a)^1 = 1 + a = 1 + 1a$ ✓
Se $n > 1$ allora $(1+a)^{n+1} = (1+a)(1+a)^n$. Ora $1 + a \geq 0$ perchè per ipotesi $a \geq 1$, mentre $(1+a)^n \geq 1 + na$ per ipotesi induttiva. In totale quindi

$$(1+a)^{n+1} = (1+a)(1+a)^n \geq (1+a)(1+na) = 1 + (n+1)a + na^2 \geq 1 + (n+1)a,$$

dove l'ultima disuguaglianza segue dal fatto che $na^2 \geq 0$. ✓

(c) Se $n = 0$ allora $1 + a^{2^0} = 1 + a = \frac{1-a^2}{1-a}$ ✓
Se $n > 0$, allora calcoliamo

$$\prod_{h=0}^{n+1}(1 + a^{2^h}) = (1 + a^{2^{n+1}}) \prod_{h=0}^{n}(1 + a^{2^h}) = (1 + a^{2^{n+1}})(\frac{1 - a^{2^{n+1}}}{1-a}) = \frac{1 - (a^{2^{n+1}})^2}{1-a} = \frac{1 - a^{2^{n+2}}}{1-a}.$$ ✓

(d) La dimostrazione che $\sum_{h=1}^{n} h = \frac{n(n+1)}{2}$ per $n \geq 1$ l'abbiamo vista insieme a lezione il 24/9/24.
Dimostriamo che per $n \geq 1$: $\sum_{h=1}^{n}(2h-1) = n^2$.
Se $n = 1$ allora $2 \cdot 1 - 1 = 1^2$ ✓
Se $n > 1$,

$$\sum_{h=1}^{n+1}(2h-1) = \sum_{h=1}^{n}(2h-1) + (2(n+1)-1) = n^1 + 2n + 1 = (n+1)^2$$ ✓

(e) Infine, dimostriamo che per $n \geq 1$, $\sum_{h=1}^{n} h^2 = \frac{n(n+1)(2n+1)}{6}$.
Se $n = 1$ allora $1^2 = \frac{1(1+1)(2\cdot 1+1)}{6}$ ✓
Se $n > 1$,

$$\begin{aligned}\sum_{h=1}^{n+1} h^2 &= \sum_{h=1}^{n} h^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 \\ &= \frac{n(n+1)(2n+1) + 6(n+1)^2}{6} = \frac{(n+1)(n+2)(2n+3)}{6}\end{aligned}$$ ✓

5. (a) Questa è una relazione di equivalenza, in quanto è riflessiva ($a \sim a$ perché 0 è pari), transitiva (se $a \sim b$ e $b \sim c$ allora $a - c = (a - b) + (b - c)$ è pari) e ovviamente simmetrica ($a - b$ è pari se e solo se $b - a$ è pari). Osserviamo che $\sim$ è semplicemente la relazione di congruenza modulo 2!

   (b) L'unica proprietà di cui gode questa relazione è la simmetria: $a - b$ è dispari se e solo se $b - a$ è dispari, le altre falliscono tutte (a voi i dettagli).

   (c) Questa relazione è riflessiva ($a \sim a$ perché $a = 1a$) e transitiva (se $a \sim b$ e $b \sim c$ significa che esistono $p, q \in \mathbb{N}$ tali che $a = pb$ e $b = qc$, quindi $a = (pq)c$, cioè $a \sim c$). Però non è simmetrica: se $a \sim b$ allora $a = qb$, e quindi $b = (1/q)a$, ma in generale se $q \in \mathbb{N}$ allora $q \notin \mathbb{N}$. Questo ragionamento però ci fa capire che la relazione è antisimmetrica: se $a \sim b$ e $b \sim a$ significa che sia $q$ che $1/q$ sono numeri naturali, e questo succede se e solo se $q = 1$.

   (d) Quasi uguale al punto precedente.

   (e) Ricordiamo che $Y^X := \{f : X \to Y \mid f \text{ funzione}\}$. È immediato verificare che si tratta di una relazione di equivalenza, e che valgono le tre proprietà riflessiva, transitiva, simmetrica.

   (f) Anche in questo caso la verifica che si tratta di una relazione di equivalenza è immediata.

   (g) Diversamente dal punto (f), l'unica proprietà di cui gode questa relazione è la simmetria: $\ell \perp \ell'$ se e solo se $\ell' \perp \ell$. La relazione non è riflessiva (una retta non è perpendicolare a se stessa), né transitiva (se $\ell \perp \ell'$ e $\ell' \perp \ell''$ nel piano, allora $\ell \parallel \ell''$), né antisimmetrica.

   (h) Ancora una relazione di equivalenza, detta *coniugio* (e che avete probabilmente visto nel corso di Algebra Lineare). Infatti vale la riflessività ($A \sim A$ con $P = I_n$), la transitività (se $A \sim B$ allora $A = P^{-1}BP$, se $B \sim C$ allora $B = Q^{-1}CQ$, e quindi

   $$A = P^{-1}BP = P^{-1}Q^{-1}CQP = (QP)^{-1}C(QP),$$

   dove $QP$ è invertibile), e la simmetria (se $A \sim B$ allora $A = P^{-1}BP$ e quindi $B = PAP^{-1} = (P^{-1})^{-1}A(P^{-1})$ cioè $B \sim A$ tramite $P^{-1}$).

   (i) Anche questa è una relazione di equivalenza, detta *congruenza* (e dovreste aver visto anche questa ad Algebra Lineare). Vale la riflessività ($A \sim A$ con $P = I_n$), la transitività (se $A \sim B$ allora $A = {}^tPBP$, se $B \sim C$ allora $B = {}^tQCQ$, e quindi

   $$A = {}^tPBP = {}^tP{}^tQCQP = {}^t(QP)C(QP),$$

   dove $QP$ è invertibile), e la simmetria (se $A \sim B$ allora $A = {}^tPBP$ e quindi $B = {}^t(P^{-1})AP^{-1}$ cioè $B \sim A$ tramite $P^{-1}$, usando il fatto che $({}^tP)^{-1} = {}^t(P^{-1})$).

   (j) La verifica che si tratta di una relazione di equivalenza (che poi corrisponde alla relazione di isomorfismo tra spazi vettoriali finitamente generati su un campo dato) è immediata .

6. (a) La relazione è riflessiva ($x \leq x$ perché $x = 1\,x$), transitiva (se $x \leq y$ e $y \leq z$ allora $x = ay$ e $y = bz$, e quindi $x = (ab)z$, cioè $x \leq z$), e antisimmetrica (se $x \leq y$ e $y \leq x$ allora $x = ay$ e $y = bx$, ma se $a, b \in \mathbb{N}$ l'unico caso in cui questo è vero è quando $x = y$), quindi è una relazione d'ordine. Non tutti gli interi sono multipli gli uni degli altri, quindi l'ordinamento è parziale.

(b) Anche questa è una relazione d'ordine, anche questa parziale non appena l'insieme $A$ ha almeno 2 elementi distinti (abbiamo visto i dettagli a lezione).

(c) Idem come sopra.

(d) Anche quest'ultima è una relazione d'ordine, ma stavolta l'ordine è totale: data una qualsiasi coppia di elementi di $A^{\mathbb{N}}$, guardando le loro componenti ad una a una, o sono tutte uguali o ad un certo punto una è associata ad un numero più piccolo dell'altra.

7. (a) Osservazione immediata.

(b) Fissiamo $i \in I_n$; se $j \neq i, n+1$ l'applicazione $\tau_i$ coincide con l'identità, quindi è biettiva su $I_n \setminus \{i, n+1\}$. Se $j = i, n+1$ allora l'applicazione $\tau_i$ scambia i due numeri, quindi anche sull'insieme $\{i, n+1\}$ l'applicazione è biettiva.

(c) Anche questa è una verifica immediata: se $A \neq \emptyset$, significa che esiste $1 \leq i \leq n$ tale che $i \in A$, e proprio per quel valore $i$ avremo $\tau_i(i) = n+1$, cioè $n+1 \in \tau_i(A)$.

8. (a) Poiché $\mathbb{Z}$ è numerabile, esiste una biezione $\varphi : \mathbb{N} \to \mathbb{Z}$. Definiamo allora

$$\begin{aligned} \bar{\varphi} : \mathbb{N} &\to q\mathbb{Z} \\ i &\mapsto q\varphi(i); \end{aligned}$$

la verifica che $\bar{\varphi}$ è una biezione è immediata: se $i \neq j$ allora $\varphi(i) \neq \varphi(j)$, e quindi, siccome $q \neq 0$, $\bar{\varphi}(i) = q\varphi(i) \neq q\varphi(j) = \bar{\varphi}(j)$, cioè $\bar{\varphi}$ è iniettiva. D'altra parte, un qualsiasi elemento di $q\mathbb{Z}$ si scrive come $qz$ per qualche $z \in \mathbb{Z}$, e quindi come $q\varphi(i) = \bar{\varphi}(i)$ per qualche $i \in \mathbb{N}$, cioè $\bar{\varphi}$ è suriettiva.

(b) Una possibile biezione $\mathbb{N} \to X \times Y$ è $n \mapsto (\varphi(n), \psi(n))$: l'iniettività e la suriettività vengono in un certo senso "ereditate" da quelle di $\varphi$ e $\psi$. Osserviamo che questo implica, con un ragionamento per induzione, che il prodotto cartesiano finito di un numero finito di insiemi numerabili è ancora numerabile.

(c) L'enunciato è vero non solo per $I_2$, ma più in generale per ogni $I_m$. La biezione cercata è

$$\begin{aligned} \bar{\varphi} : \mathbb{N} &\to X \cup I_m \\ i &\mapsto \begin{cases} i & \text{se } 1 \leq i \leq m \\ \varphi(i-m) & \text{se } i > m \end{cases} \end{aligned}$$

9. (a) Sia $A' \subseteq A \subseteq B$ e $\varphi\colon A \to A'$. Definiamo

$$\begin{aligned} \psi\colon B &\longrightarrow B' = A' \cup (B \setminus A) \\ b &\longrightarrow \begin{cases} \varphi(b) & \text{se } b \in A, \\ b & \text{se } b \notin A. \end{cases} \end{aligned}$$

Supponiamo che $\varphi$ sia iniettiva e siano $b_1, b_2 \in B$ tali che $\psi(b_1) = \psi(b_2)$. Se $b_1, b_2 \in A$ allora $\psi(b_1) = \varphi(b_1) = \varphi(b_2) = \psi(b_2)$ e siccome $\varphi$ è iniettiva, $b_1 = b_2$. Se $b_1, b_2 \notin A$ allora $\psi(b_1) = b_1 = b_2 = \psi(b_2)$. Infine se $b_1 \in A$ e $b_2 \notin A$ allora $\psi(b_1) = \varphi(b_1) = b_2 = \psi(b_2)$ implica $b_2 = \varphi(b_1) \in A' \subseteq A$, quindi questo caso non può capitare.

Viceversa, supponiamo che $\psi$ sia iniettiva, e siano $a_1, a_2 \in A$ tali che $\varphi(a_1) = \varphi(a_2)$. Ma in questo caso $\varphi(a_1) = \psi(a_1) = \psi(a_2) = \varphi(a_2)$, e siccome $\psi$ è iniettiva, $a_1 = a_2$.

(b) Osserviamo che se $A \subseteq B$, si ha un'applicazione naturale iniettiva $\iota : A \hookrightarrow B$, $a \mapsto \iota(a) = a$. Durante la lezione del 24/9/24 abbiamo dimostrato che se un insieme $A$ è infinito, allora esiste un'applicazione iniettiva $f : \mathbb{N} \hookrightarrow A$. Ora, se $B$ fosse finito, esisterebbe un certo $n \in \mathbb{N}$ e una funzione biettiva $g : B \to I_n$. Componendo le funzioni iniettive $f$ e $\iota$ con quella biettiva $g$ otterremmo una funzione iniettiva (cf. l'esercizio 1) $g \circ \iota \circ f : \mathbb{N} \hookrightarrow I_n$, che è ovviamente assurdo.

(c) Usiamo di nuovo il fatto visto a lezione che se un insieme $A$ è infinito, allora esiste un'applicazione iniettiva $f : \mathbb{N} \hookrightarrow A$; quindi se $A$ è infinito, il sottoinsieme numerabile di $A$ cercato è semplicemente $A' = f(\mathbb{N})$. Viceversa, $A$ contiene un sottoinsieme numerabile $A'$ se e solo se esiste una biezione $g : \mathbb{N} \to A'$, e quindi anche un'applicazione iniettiva $\mathbb{N} \hookrightarrow A$, ottenuta componendo $g$ con l'iniezione naturale $A' \hookrightarrow A$.

10. L'applicazione cercata è semplicemente

$$\begin{aligned} \varphi : A \times B &\to B \times A \\ (a, b) &\mapsto (b, a); \end{aligned}$$

la verifica che $\varphi$ è biettiva è immediata.

11. Abbiamo visto la soluzione di questo esercizio durante la lezione del 24/9/24.

12. (a) È sufficiente osservare che un qualsiasi elemento di $\mathbb{Q}[x]_m$ è della forma

$$p(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m;$$

questo ci permette di stabilire una biezione tra $\mathbb{Q}[x]_m$ e $\mathbb{Q}^m$ (il prodotto cartesiano di $\mathbb{Q}$ per se stesso $m$ volte), tramite $p(x) \mapsto (a_0, a_1, \ldots, a_m)$. Poiché $\mathbb{Q}^m$ è numerabile (si veda l'esercizio 8 (b)), segue che lo stesso vale per $\mathbb{Q}[x]_m$.

(b) È una conseguenza immediata della parte (a) di questo esercizio insieme alla parte (c) dell'esercizio 8.

(c) Per dimostrare che $\mathbb{Z}[x]$ è numerabile basta osservare che $\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$.

(d) È chiaramente falso che l'insieme $\mathbb{C}[x]$ è numerabile, poiché contiene come sottoinsieme $\mathbb{C}$ stesso, che non è numerabile.

13. (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: $2 * 3 = 8 \neq 9 = 3 * 2$.

(b) $G = \mathbb{R}$ è chiuso rispetto all'operazione $a * b = a + b + 3$.
Siccome la somma è commutativa, lo stesso vale per $*$. Non solo: l'operazione $*$ eredita anche l'associatività della somma su $\mathbb{R}$. L'elemento neutro è $-3$, infatti per ogni $a \in \mathbb{R}$: $a * (-3) = (-3) * a = a + (-3) - 3 = a$. L'inverso di un elemento $a$ è $b = -a - 6$, infatti $a * (-6 - a) = a + (-6 - a) + 3 = -3$.

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

(d) $G = \mathbb{N}$ è chiuso rispetto all'operazione $a * b = \max\{a, b\}$.
L'elemento neutro è 1, infatti $a * 1 = 1 * a = \max\{a, 1\} = a$ per ogni $a \in \mathbb{N}$. Invece non esistono inversi: dato $a \in \mathbb{N}$, non è possibile trovare un naturale $b \in \mathbb{N}$ tale che $a * b = \max\{a, b\} = 1$. L'operazione è associativa, basta osservare che per ogni $a, b, c \in \mathbb{N}$ vale $\max\{\max\{a, b\}, c\} = \max\{a, b, c\} = \max\{a, \max\{b, c\}\}$, ed è anche commutativa.
(Un insieme non vuoto dotato di un'operazione associativa è detto *semigruppo*; un semigruppo dotato di elemento neutro è detto *monoide*. Quindi $(\mathbb{N}, \max)$ è un monoide.)

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

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

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

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

Verifichiamo che vale la proprietà associativa; siano $\varphi, \psi, \chi \in G^X$ e sia $a \in X$, allora, sfruttando l'associatività dell'operazione del gruppo $G$, abbiamo che:

$$\varphi(\psi\chi)(a) = \varphi(a)\big((\psi\chi)(a)\big) = \varphi(a)\big(\psi(a)\chi(a)\big) = \big(\varphi(a)\psi(a)\big)\chi(a) = \big((\varphi\psi)(a)\big)\chi(a) = (\varphi\psi)\chi(a).$$

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 $\varphi_g\colon a \mapsto g$ e $\varphi_h\colon a \mapsto h$ sono in $G^X$, dunque commutano, cioè $G$ è abeliano:

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

**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!