

## Esercizi

**Settimana 0** - 29/09/2025

Ex.1 - Determinare tutti gli elementi del gruppo  $S_3$  e scrivere la tabella moltiplicativa.

Ex.2 - Determinare la composizione  $\sigma \circ \tau$  delle seguenti permutazioni in  $S_6$ :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}.$$

Ex.3 - Supponiamo che in un gruppo valga l'equazione  $xyz = 1$ . È vero che  $yzx = 1$ ? È vero che  $yxz = 1$ ?

Ex.4 - Sia  $G$  un gruppo con prodotto  $\cdot$ . Definiamo il *gruppo opposto*  $G^\circ$  come l'insieme  $G$  dotato del prodotto opposto  $a \circ b = b \cdot a$ . Dimostrare che  $G^\circ$  è un gruppo.

Ex.5 - Siano  $a, b$  elementi di un gruppo. Assumendo che  $a$  ha ordine 5 e  $a^3b = ba^3$ , mostrare che  $ab = ba$ .

Ex.6 - Quali dei seguenti sono sottogruppi?

(a)  $GL_n(\mathbb{R}) \subset GL_n(\mathbb{C})$ ;

(b)  $\{\pm 1\} \subset \mathbb{R}^\times$ ;

(c)  $\{n > 0\} \subset \mathbb{Z}$ ;

(d)  $\{a > 0\} \subset \mathbb{R}^\times$ ;

(e)  $\left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a \neq 0 \right\} \subset GL_2(\mathbb{R})$ .

(Ricordiamo la definizione del gruppo  $GL_n(\mathbb{K})$  come l'insieme delle matrici  $n \times n$  invertibili a coefficienti nel campo  $\mathbb{K}$ .)

Ex.7 - Mostrare che le  $n$  radici  $n$ -sime di 1 in  $\mathbb{C}$  formano un gruppo ciclico di ordine  $n$ .

Ex.8 - Mostrare che l'insieme  $\text{Mat}_{m \times n}(\mathbb{R})$  delle matrici  $m \times n$  a coefficienti reali è un anello commutativo con unità rispetto alla somma di matrici.

Ex.9 - Mostrare che un dominio d'integrità finito è necessariamente un campo. (Ricordiamo che un dominio di integrità è un anello commutativo unitario con la proprietà che se  $ab = 0$  allora necessariamente  $a = 0$  o  $b = 0$ .)

Ex.10 - Esiste un campo con esattamente 15 elementi?

Ex.11 - Sia  $A$  un insieme che soddisfa tutti gli assiomi di anello con l'eccezione della commutatività della somma. Mostrare allora che la somma è commutativa calcolando  $(1+1)(x+y)$  in due modi diversi.

## Esercizi

**Settimana 0** - per il 6/10/2025

Ex.1 - Nel gruppo simmetrico  $S_7$  risolvere l'equazione  $\alpha x = \beta$ , dove

$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 1 & 5 & 7 & 4 & 6 \end{pmatrix}, \quad \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 2 & 5 & 4 & 3 & 1 \end{pmatrix}.$$

Ex.2 - Dimostrare per induzione che  $1 + 3 + 5 + \dots + (2n - 1) = n^2$ .

Ex.3 - Dimostrare per induzione che  $5^n - 1$  è divisibile per 4, qualunque sia  $n \geq 1$ .

Ex.4 - Sia  $F_n$  la successione di Fibonacci, definita per ricorrenza da  $F_1 = F_2 = 1$ ,  $f_n = F_{n-1} + F_{n-2}$ . Dimostrare per induzione che  $\sum_{i=1}^n F_i^2 = F_n F_{n+1}$ .

Ex.5 - Si diano esempi di relazioni:

- (a) riflessiva, simmetrica, non transitiva,
- (b) riflessiva, non simmetrica, transitiva,
- (c) non riflessiva, simmetrica, transitiva.

Ex.6 - Siano  $I, J$  ideali di un anello  $A$  che soddisfano  $I + J = A$ .

- Mostrare che  $IJ = I \cap J$ .
- Dimostrare il Teorema cinese dei resti: per ogni scelta di  $a, b \in A$  esiste  $x \in A$  tale che  $x \equiv a \pmod{I}$  e  $x \equiv b \pmod{J}$ . (Per  $x \equiv a \pmod{I}$  si intende che  $x - a \in I$ ).

Ex.7 - Trovare tutti gli  $x$  interi tali che

$$\begin{cases} 2x \equiv 3 & (\text{mod } 15) \\ 3x \equiv 5 & (\text{mod } 8) \\ 4x \equiv 2 & (\text{mod } 7) \end{cases}$$

Ex.8 - Trovare tutti gli  $y$  interi tali che

$$\begin{cases} 7y \equiv 4 & (\text{mod } 12) \\ 5y \equiv 6 & (\text{mod } 26) \end{cases}$$

Ex.9 - (Artin 11.1.6) Calcolare il massimo comun divisore dei seguenti polinomi  $p, q$  a coefficienti razionali  $p := x^3 - 6x^2 + x + 4$ ,  $q := x^5 - 6x + 1$ .

Ex.10 - Usare l'algoritmo Euclideo per il calcolo del  $MCD(3522, 321)$  e del  $MCD(413, 173)$ . Esprimere in entrambi i casi il  $MCD(a, b)$  nella forma  $pa + qb$ .

## Esercizi

**Settimana 3** - per il 20/10/2025

Ex.1 - Calcolare il MCD e l'identità di Bezout per le seguenti coppie di numeri:

14743 e 8915,    10000 e 642,    5785 e 546

Ex.2 - Determinare gli elementi invertibili (e per ciascuno di tali elementi il suo inverso) negli anelli  $\mathbb{Z}/7$ ,  $\mathbb{Z}/14$ ,  $\mathbb{Z}/20$ .

Ex.3 - Trovare tutte le soluzioni (se esistono) delle seguenti congruenze:

(a)  $3x \equiv 5 \pmod{4}$ ,

(b)  $3x \equiv 9 \pmod{6}$ ,

(c)  $4x \equiv 7 \pmod{9}$ ,

(d)  $6x \equiv 8 \pmod{9}$ .

Ex.4 - Risolvere i seguenti sistemi alle congruenze

(a) 
$$\begin{cases} x \equiv 2 & \pmod{5} \\ x \equiv 1 & \pmod{3} \end{cases}$$

(b) 
$$\begin{cases} x \equiv 2 & \pmod{5} \\ x \equiv 1 & \pmod{3} \\ x \equiv 6 & \pmod{14} \end{cases}$$

Ex.5 - Risolvere il sistema alle congruenze 
$$\begin{cases} 2x \equiv 8 & \pmod{9} \\ 2x \equiv 6 & \pmod{15} \end{cases}$$

Ex.6 - Determinare le ultime tre cifre di  $46^{14}$ .

Ex.7 - Determinare, se esiste, il minimo intero positivo  $n$  tale che  $7123^n$  abbia come ultima cifra 1.

Ex.8 - Determinare un criterio di divisibilità per 11.

## Esercizi

**Settimana 4** - per il 27/10/2025

- Ex.1 - Calcolare le tabelle additive e moltiplicative di  $\mathbb{Z}/2\mathbb{Z}$ ,  $\mathbb{Z}/3\mathbb{Z}$ ,  $\mathbb{Z}/5\mathbb{Z}$  e verificare che queste strutture soddisfano gli assiomi di campo.
- Ex.2 - Elencare gli elementi invertibili di  $\mathbb{Z}/9\mathbb{Z}$  e  $\mathbb{Z}/7\mathbb{Z}$  e, per ciascuno di essi, determinarne l'inverso.
- Ex.3 - Calcolare i seguenti elementi del campo  $\mathbb{Z}/5\mathbb{Z}$ :
- $$3 \cdot 4^{-1}, \quad 3^5 \cdot 2^{-2}, \quad (1 + 2 + \dots + 9) \cdot 3^{-10}$$
- Ex.4 - Sia  $\mathcal{A}$  un anello. Due elementi  $a, b$  si dicono *divisori dello zero* se  $a, b \neq 0$  e  $ab = 0$ . Calcolare i divisori dello zero di  $\mathbb{Z}/8\mathbb{Z}$ .
- Ex.5 - Sia  $\mathcal{A}$  un anello privo di divisori dello zero. Provare che  $\mathcal{A}$  soddisfa le *leggi di cancellazione*:
- $$\forall a, b, c \in \mathcal{A}, a \neq 0, \quad ab = ac \implies b = c;$$
- $$\forall a, b, c \in \mathcal{A}, a \neq 0, \quad ba = ca \implies b = c$$
- Ex.6 - dimostrare che  $\sqrt{2}$  e  $\sqrt{3}$  non sono numeri razionali (usando il teorema fondamentale dell'Aritmetica).
- Ex.7 - Calcolare  $3^{31} \bmod 7$  e  $128^{129} \bmod 17$  (usando il piccolo Teorema di Fermat).
- Ex.8 - Risolvere l'equazione alle congruenze  $x^{103} \equiv 4 \bmod 11$ .

## Esercizi

**Settimana 5** - per il 3/11/2025

Ex.1 - Sia  $G$  un gruppo.

- (a) Verificare che  $G$  ammetta esattamente un elemento neutro.
- (b) Verificare che ogni elemento in  $G$  ammetta esattamente un elemento inverso
- (c) Verificare che  $ax = ay \implies x = y$  e  $xa = ya \implies x = y$

Ex.2 - Sia  $G$  un gruppo. Un elemento  $x$  di  $G$  si dice *idempotente* se  $x^2 = x$ . Si dimostri che l’unico idempotente di  $G$  è il suo elemento neutro.

Ex.3 - Sia  $Z_m = \langle \mathbb{Z}/m\mathbb{Z}; +, \cdot \rangle$  l’anello delle classi resto modulo  $m$  e si denoti con  $U_m$  l’insieme degli elementi invertibili della parte moltiplicativa di  $Z_m$ . Si verifichi che per  $m = 14, 20$ ,  $\langle U_m, \cdot \rangle$  è un gruppo.

Ex.4 - Si consideri l’insieme  $S = \{(a, b) : a, b \in \mathbb{R}, a \neq 0\}$  munito dall’operazione di prodotto  $(\circ)$  definita come

$$(a, b) \circ (c, d) = (ac, bc + d).$$

Si verifichi se  $\langle S, \circ \rangle$  è un gruppo

Ex.5 - Si consideri l’insieme  $S = \{a, b, c\}$  e si consideri su di esso l’operazione di prodotto  $(\circ)$  definita dalla tavola seguente

$\circ$	<b>a</b>	<b>b</b>	<b>c</b>
<b>a</b>	$a$	$b$	$c$
<b>b</b>	$b$	$c$	$a$
<b>c</b>	$c$	$a$	$b$

Si verifichi se  $\langle S, \circ \rangle$  è un gruppo

Ex.6 - Determinare i sottogruppi di  $\mathbb{Z}$  che contengono 18

Ex.7 - Siano  $H, K \leq G$  sottogruppi di un gruppo  $G$ .

- (a) Dimostrare che la loro intersezione ‘è ancora un sottogruppo.
- (b) Dimostrare che  $H \cup K$  è sottogruppo di  $G$  se e solo se  $H \subseteq K$  oppure  $K \subseteq H$ .

Ex.8 - Sia  $G$  un gruppo tale che ogni elemento diverso dall’identità ha ordine 2. Dimostrare che  $G$  è commutativo.

Ex.9 - Sia  $G$  un gruppo e  $g \in G$  un suo elemento. Verificare che la funzione  $h \mapsto ghg^{-1}$  è un isomorfismo di gruppo.

Ex.10 - Provare che se un gruppo ha un numero pari di elementi allora ha almeno un elemento di ordine 2. (*Suggerimento:* considerare le coppie  $(x, x^{-1})$  al variare di  $x \in G$ ; quante sono tali coppie? da quanti elementi sono composte?)

## Esercizi

**Settimana 6** - per il 17/11/2025

Ex.1 - Sia  $f : G_1 \rightarrow G_2$  un omomorfismo di gruppi i cui elementi neutri siano denotati  $e_1$  ed  $e_2$ , rispettivamente. Si considerino i seguenti insiemi definiti come:

$$\text{Ker}(f) = \{g \in G_1 \mid f(g) = e_2\} \quad (\text{nucleo di } f)$$

$$\text{Im}(f) = \{g_2 \in G_2 \mid \exists g_1 \in G_1 \mid f(g_1) = g_2\} \quad (\text{immagine di } f).$$

Mostrare che  $\text{Ker}(f) \leq G_1$  e  $\text{Im}(f) \leq G_2$ . Mostrare inoltre che  $f$  è iniettiva se e solo se  $\text{Ker}(f) = \{e_1\}$  e che  $f$  è suriettiva se e solo se  $\text{Im}(f) = G_2$ .

Ex.2 - Siano  $G$  un gruppo e  $H$  un suo sottogruppo. Verificare che, per  $a \in G$ , si abbia

$$aH = H \quad \Longleftrightarrow \quad a \in H$$

(analogamente per le classi laterali destre).

Ex.3 - Siano  $G$  un gruppo e  $H$  un suo sottogruppo. Dato  $a \in G$ , si consideri la funzione  $\varphi : Ha \rightarrow aH$  data da  $\varphi(ha) = ah$ . Verificare che  $\varphi$  è una funzione biunivoca.

Ex.4 - Sia  $G$  un gruppo abeliano ed  $H$  un suo sottogruppo. Verificare che  $\rho_d = \rho_s$ , dove  $\rho_d$  e  $\rho_s$  denotano, rispettivamente, la congruenza destra e sinistra di  $H$ . (Ricordiamo che  $\rho_s$  e  $\rho_d$  sono definite da  $a \rho_s b \Leftrightarrow a^{-1}b \in H$  e  $a \rho_d b \Leftrightarrow ba^{-1} \in H$ .)

Ex.5 - Sia  $G = (\mathbb{Z}, +)$  il gruppo additivo dei numeri interi, sia  $m \in \mathbb{Z}, m \geq 1$  un intero positivo fissato e sia  $\rho_d$  la congruenza destra relativa al sottogruppo  $m\mathbb{Z}$ . Verificare che, per ogni  $a, b \in \mathbb{Z}$ , si abbia:

$$a \rho_d b \quad \Longleftrightarrow \quad a \equiv b \pmod{m}.$$

Ex.6 - Verificare che il gruppo additivo  $(\mathbb{Z}_4, +)$  delle classi resto mod 4, è isomorfo al gruppo moltiplicativo  $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$  delle classi resto mod 5 non nulle.

Ex.7 - Determinare i sottogruppi generati dagli elementi di  $(\mathbb{Z}_6, +)$ .

Ex.8 - Sia  $G$  il gruppo moltiplicativo  $(\mathbb{Z}_{20})^\times$  delle classi resto mod 20 invertibili. Determinare:

- (a) per ogni elemento di  $G$  il suo ordine;
- (b) i sottogruppi di  $G$ ;
- (c) il diagramma di Hasse dei sottogruppi di  $G$ , rispetto alla relazione d'ordine  $H \leq K$ , con  $H, K \leq G$ .

Ex.9 - Sia  $G$  un gruppo di ordine  $p$  con  $p$  primo. Verificare che  $G$  è ciclico e non possiede sottogruppi non banali.

Ex.10 - Classificare i gruppi di ordine  $\leq 5$ , a meno di isomorfismo.

## Esercizi

**Settimana 7** - per il 24/11/2025

Ex.1 - Si verifichi che i seguenti insiemi, con le usuali operazioni di somma e prodotto per scalari, sono spazi vettoriali su  $\mathbb{R}$ :

- (a) l'insieme delle matrici  $M_{m,n}(\mathbb{R})$ ;
- (b) l'insieme  $\mathbb{R}[x]$  dei polinomi a coefficienti reali in una variabile  $x$ ;
- (c) l'insieme  $\mathbb{R}^{\mathbb{N}}$  delle successioni  $(a_i)_{i \in \mathbb{N}}$  di elementi di  $\mathbb{R}$ :

$$(a_0, a_1, a_2, \dots).$$

Per ognuno di essi, si determinino (se esistono) una base e la dimensione.

Ex.2 - Si consideri il sottoinsieme di matrici dello spazio vettoriale  $M_{2,2}(\mathbb{R})$  definito come:

$$U = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a + b + c = 0 \right\}.$$

Si verifichi che  $U$  è un sottospazio vettoriale di  $M_{2,2}(\mathbb{R})$ . Si determini una sua base e la sua dimensione.

Ex.3 - Sia  $\mathbb{R}$  il campo dei numeri reali. Si dica quali dei seguenti sottoinsiemi dello spazio vettoriale  $\mathbb{R}^n$  siano suoi sottospazi vettoriali:

- (a)  $H_1 = \{(x_1, \dots, x_n) \in \mathbb{R}^n : x_1 = 1\}$ ,
- (b)  $H_2 = \{(x_1, \dots, x_n) \in \mathbb{R}^n : x_1 + \dots + x_n = 0\}$ ,
- (c)  $H_3 = \{(x_1, \dots, x_n) \in \mathbb{R}^n : x_n \neq 0\}$ ,
- (d)  $H_4 = \{(x_1, \dots, x_n) \in \mathbb{R}^n : x_1 = x_2 = \dots = x_n\}$ .

Nel caso siano sottospazi, si determini una loro base e la loro dimensione.

Ex.4 - Sia  $n \in \mathbb{N}$  e si consideri l'insieme  $\mathbb{R}[x]_{\leq n}$  dei polinomi a coefficienti reali in una variabile  $x$  di grado non superiore ad  $n$ . Si verifichi che  $\mathbb{R}[x]_{\leq n}$  è un sottospazio vettoriale di  $\mathbb{R}[x]$ . Si determini una sua base e la sua dimensione.

Ex.5 - Verificare quali dei seguenti sono insiemi di vettori linearmente indipendenti, insiemi di generatori e/o basi di  $\mathbb{R}^3$ :

- (a)  $\left\{ \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 2 \\ 0 \\ 1 \end{pmatrix} \right\}$
- (b)  $\left\{ \begin{pmatrix} 1 \\ -3 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ -3 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$
- (c)  $\left\{ \begin{pmatrix} 1 \\ 1 \\ 3 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 6 \\ 8 \end{pmatrix} \right\}$
- (d)  $\left\{ \begin{pmatrix} 1 \\ -3 \\ 3 \end{pmatrix}, \begin{pmatrix} 0 \\ 2 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \\ -3 \end{pmatrix} \right\}$

Ex.6 - Calcolare le coordinate del vettore  $\mathbf{v} \in \mathbb{R}^3$  nella base  $\mathcal{B}$ :

$$\mathbf{v} = \begin{pmatrix} 3 \\ 4 \\ 1 \end{pmatrix}, \quad \mathcal{B} = \left\{ \begin{pmatrix} 1 \\ -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} \right\}$$

Ex.7 - Sia  $p(x)$  un polinomio fissato e sia  $\Gamma = \{(x, p(x)) \mid x \in \mathbb{R}\} \subset \mathbb{R}^2$  il grafico di  $p(x)$ . Determinare per quali polinomi  $p(x)$ ,  $\Gamma$  risulta essere un sottospazio vettoriale di  $\mathbb{R}^2$ .

- Ex.8 - Si considerino i polinomi  $p_1(x) = 1 + x$ ,  $p_2(x) = 1 + 2x + x^2$ ,  $p_3(x) = x - x^2$ . Verificare che formano una base di  $\mathbb{R}[x]_{\leq 2}$  (lo spazio dei polinomi di grado minore o uguale a 2) e determinare le coordinate di  $q(x) = 2 - x + x^2$  in questa base.
- Ex.9 - Trovare un sottoinsieme non vuoto  $S_+ \subset \mathbb{R}^2$  che sia chiuso rispetto alla somma ed a prendere gli elementi opposti, ma che non sia un sottospazio vettoriale. Trovare un sottoinsieme non vuoto  $S_- \subset \mathbb{R}^2$  che sia chiuso rispetto al prodotto per gli scalari, ma che non sia un sottospazio vettoriale.
- Ex.10 - Nello spazio vettoriale  $\mathbb{R}[x]$  dei polinomi in  $x$ , dire quali dei seguenti sottoinsiemi sono sottospazi vettoriali:
- (a)  $\{p(x) \in \mathbb{R}[x] \mid p(0) = 0\}$ ,
  - (b)  $\{p(x) \in \mathbb{R}[x] \mid p(0) = 1\}$ ,
  - (c)  $\{p(x) \in \mathbb{R}[x] \mid p(1) = 0\}$ ,
  - (d)  $\{p(x) \in \mathbb{R}[x] \mid p(0) = p(1) = 0\}$ ,
  - (e)  $\{p(x) \in \mathbb{R}[x] \mid p(0)p(1) = 0\}$ .