**CORSO DI LAUREA TRIENNALE IN INFORMATICA**
**PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III) — 27 OTTOBRE 2025**

Svolgere i seguenti esercizi,

$\longrightarrow$ $\boxed{\textit{giustificando pienamente tutte le risposte.}}$ $\longleftarrow$

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola**, **gruppo di appartenenza**.
**Non** è necessario consegnare la traccia.

**Esercizio 1.** Siano $P$ e $Q$ predicati unari, e sia $\varphi$ la formula $\big(\forall x(P(x) \wedge Q(x))\big) \to \big(\exists y(P(y))\big)$.

- (*i*) Scrivere una formula logicamente equivalente a $\neg\varphi$ in cui non appaia il connettivo $\wedge$.
- (*ii*) Dare, quando possibile, un esempio di struttura in cui $\varphi$ è sempre (cioè per ogni scelta di $P$ e $Q$) vera e un esempio in cui $\varphi$ è sempre falsa.

**Esercizio 2.** Data l'applicazione $f\colon (a,b) \in \mathbb{N}^* \times \mathbb{N} \mapsto (a^b, ab) \in \mathbb{N}^* \times \mathbb{N}$, dove $\mathbb{N}^* = \mathbb{N} \smallsetminus \{0\}$, determinare:

- (*i*) $\overleftarrow{f}(\{(2,3)\})$, $\overleftarrow{f}(\{(1,1)\})$ e $\overleftarrow{f}(\{(3,3)\})$;
- (*ii*) $\overrightarrow{f}(\{1\} \times \mathbb{N})$ e $\overrightarrow{f}(\mathbb{N}^* \times \{1\})$.
- (*iii*) $f$ è iniettiva? È suriettiva? È invertibile?
- (*iv*) Indicata con $\Re_f$ la relazione di equivalenza associata ad $f$ (cioè il nucleo di equivalenza di $f$), determinare $[(5,1)]_{\Re_f}$.

**Esercizio 3.** Si consideri l'insieme ordinato $(\mathbb{N}^* \times \mathbb{N}, \sigma)$, dove, per ogni $a, c \in \mathbb{N}^*$ e $b, d \in \mathbb{N}$,

$$(a,b)\ \sigma\ (c,d) \iff \big((a,b) = (c,d) \vee ab \text{ è un divisore proprio di } cd\big).$$

Determinare, in $(\mathbb{N}^* \times \mathbb{N}, \sigma)$:

- (*i*) eventuali minimo, massimo, elementi minimali, elementi massimali;
- (*ii*) l'insieme dei minoranti e l'eventuale estremo inferiore di $X := \{(4,1), (2,2)\}$;
- (*iii*) $(\mathbb{N}^* \times \mathbb{N}, \sigma)$ è un reticolo?
- (*iv*) Sia $L = \{(1,144), (4,1), (2,2), (12,1), (6,2), (36,1), (144,1), (30,4)\}$. Si disegni il diagramma di Hasse di $(L, \sigma)$. $(L, \sigma)$ è un reticolo? Se lo è, è distributivo? È complementato? È booleano?

**Esercizio 4.** In $\mathbb{Z}_{25}$ si consideri l'operazione definita da $a * b = \bar{5}ab + a + b$ per ogni $a, b \in \mathbb{Z}_{25}$.

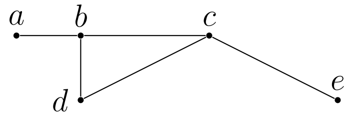
- (*i*) Determinare in $(\mathbb{Z}_{25}, *)$ l'eventuale elemento neutro e l'insieme di quelli simmetrizzabili. Che tipo di struttura (semigruppo, monoide, gruppo) è $(\mathbb{Z}_{25}, *)$?
- (*ii*) Determinare, se la domanda ha senso, il simmetrico di $\bar{5}$ in $(\mathbb{Z}_{25}, *)$.

**Esercizio 5.** Sia $A = \{x \in \mathbb{N} \mid x \leq 10\}$ e sia $\mathbb{P}$ l'insieme dei numeri interi positivi primi.

- (*i*) Elencare gli elementi di $A \cap \mathbb{P}$ e quelli di $A \smallsetminus \mathbb{P}$.
- (*ii*) Quanti sono i sottoinsiemi di $A$ che contengono solo numeri primi?
- (*iii*) Quanti sono i sottoinsiemi di $A$ che non contengono nessun numero primo?
- (*iv*) Quanti sono i sottoinsiemi di $A$ che contengono esattamente due numeri primi e due numeri non primi?
- (*v*) Vero o falso (e, come per tutte le domande, perché)?
  - a) ogni elemento di $A$ è (primo o) prodotto di primi;
  - b) detti $n$ il numero descritto in (*ii*) ed $m$ il numero descritto in (*iii*), $|\mathcal{P}(A)| = n + m$.

Solo per studenti immatricolati prima dell'a.a. 2024/25

**Esercizio 6.** Disegnare tutti i sottoalberi massimali (alberi di supporto) del grafo a destra. Tra questi stabilire quali sono e quali non sono isomorfi tra loro.




**Esercizio 7.** (*i*) Enunciare il teorema di Ruffini ed il teorema generalizzato di Ruffini.

- (*ii*) Per quali interi primi positivi $p$, il polinomio $f_p = x^4 + \bar{3}x^3 - \bar{5}x^2 + \bar{2}x - \overline{10} \in \mathbb{Z}_p[x]$ ha sia $\bar{2}$ che $-\bar{2}$ come radici?
- (*iii*) Detto $q$ il minimo di tali primi, decomporre $f_q$ in prodotto di polinomi irriducibili in $\mathbb{Z}_q[x]$.
- (*iv*) Esiste un polinomio associato ad $f_q$ in $\mathbb{Z}_q[x]$ che abbia termine noto $\bar{3}$? In caso di risposta affermativa, determinarlo.