CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
18 GIUGNO 2019

Svolgere i seguenti esercizi,

⟶ **giustificando pienamente tutte le risposte.** ⟵

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

Esercizio 1. Enunciare il teorema di Bézout per numeri interi.

Esercizio 2. Si consideri l'operazione binaria $*$ definita in $\mathbb{Z}_9$ ponendo, per ogni $a, b \in \mathbb{Z}_9$,

$$a * b = \bar{5}(ab - a - b + \bar{3}).$$

Dando per noto che $*$ è associativa e commutativa.

- (i) Determinare tutti gli elementi $a \in \mathbb{Z}_9$ tali che $a * \bar{0} = \bar{0}$.
- (ii) Utilizzando quanto visto al punto precedente, dimostrare che $*$ ammette elemento neutro, determinandolo.
- (iii) Decidere se $\bar{4}$ è invertibile in $(\mathbb{Z}_9, *)$.
- (iv) Vero o falso: $\mathcal{U}(\mathbb{Z}_9, *) = \mathcal{U}(\mathbb{Z}_9, \cdot)$? (Qui $\cdot$ indica l'usuale operazione di moltiplicazione in $\mathbb{Z}_9$.)
- (v) Decidere se $T := \{\bar{3}, \bar{7}\}$ è o non è una parte chiusa di $(\mathbb{Z}_9, *)$.

Esercizio 3. Sia $S = \{n \in \mathbb{N} \mid n < 10\}$. In $\mathcal{P}(S)$ si consideri la relazione di equivalenza $\mathcal{R}$ definita ponendo, per ogni $X, Y \in \mathcal{P}(S)$,

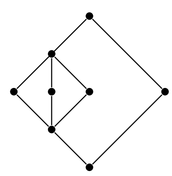
$$X \mathrel{\mathcal{R}} Y \iff X \smallsetminus \{1\} = Y \smallsetminus \{1\}.$$

- (i) Elencare gli elementi di $[\varnothing]_{\mathcal{R}}$ e quelli di $[\{1, 2\}]_{\mathcal{R}}$;
- (ii) in generale, per ogni $X \in \mathcal{P}(S)$, descrivere $[X]_{\mathcal{R}}$, e calcolare $|[X]_{\mathcal{R}}|$. Calcolare $|\mathcal{P}(S)/\mathcal{R}|$.

Sia ora σ la relazione d'ordine definita in $\mathcal{P}(S)$ ponendo, per ogni $X, Y \in \mathcal{P}(S)$,

$$X \mathrel{\sigma} Y \iff (X = Y \vee X \smallsetminus \{1\} \subset Y \smallsetminus \{1\}).$$

- (iii) Stabilire se σ è una relazione totale.
- (iv) Determinare in $(\mathcal{P}(S), \sigma)$, eventuali minimo, massimo, elementi minimali, elementi massimali.
- (v) $(\mathcal{P}(S), \sigma)$ è un reticolo? Se lo è, è distributivo?, è complementato?
- (vi) Il diagramma a destra rappresenta un reticolo? Nel caso, un reticolo distributivo?, complementato?, booleano?
- (vii) Trovare, se possibile, un sottoinsieme B di $\mathcal{P}(S)$ tale che (B, σ) sia rappresentato dal diagramma di Hasse a destra; se non è possibile farlo spiegare perché.



Esercizio 4. Nell'anello di polinomi $\mathbb{Z}_3[x]$ si consideri l'insieme A dei polinomi della forma $x^3 + ax + b$ al variare di a e b in $\mathbb{Z}_3$.

- (i) Quanto vale $|A|$?
- (ii) Se $b = \bar{0}$, il polinomio $x^3 + ax + b$ indicato sopra può essere irriducibile in $\mathbb{Z}_3[x]$? ...
- (iii) ... e se $a = b = \bar{1}$?
- (iv) Sia $g = (x + \bar{1})(x^2 - x - \bar{1}) \in \mathbb{Z}_3[x]$. $\quad g \in A$? $\quad g$ è irriducibile in $\mathbb{Z}_3[x]$?
- (v) Trovare tutti i polinomi irriducibili (in $\mathbb{Z}_3[x]$) appartenenti ad A. Quanti sono? Quanti sono i polinomi non irriducibili appartenenti ad A?