**CORSO DI LAUREA TRIENNALE IN INFORMATICA**
**PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)**
**10 OTTOBRE 2018**

Svolgere i seguenti esercizi,

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

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

**Esercizio 1.** Dare la definizione di *polinomio irriducibile* su un campo e rispondere alle domande:

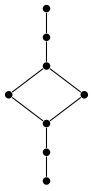
(*i*) Esistono un campo $K$ ed un polinomio irriducibile $f \in K[x]$ tali che $f$ abbia radici in $K$?
(*ii*) Esiste un campo $F$ tale che il polinomio $(x^2+1)(x^2+1)$ non abbia radici in $F$?
(*iii*) Esiste un campo $F$ tale che il polinomio $(x^2+1)(x^2+1)$ sia irriducibile in $F[x]$?
(*iv*) Esiste un campo $F$ tale che il polinomio $x^3+4x+1$ sia associato in $F[x]$ a $4x^2+x+1$?
(*v*) Esiste un polinomio $f \in \mathbb{Q}[x]$ che abbia grado 5, sia irriducibile in $\mathbb{Q}[x]$ ma non sia irriducibile in $\mathbb{R}[x]$? Nel caso esista, un tale polinomio ha radici in $\mathbb{R}$?

**Esercizio 2.** Siano $\mathbb{P}$ l'insieme dei numeri primi positivi e $A = \{5, 10, 18, 33\}$. Per ogni intero $n > 1$ poniamo $p_n = \max\{p \in \mathbb{P} \mid p \text{ divide } n\}$ e $q_n = \min\{p \in \mathbb{P} \mid p \text{ divide } n\}$. Descrivere, elencandone gli elementi, $P = \{p_a \mid a \in A\}$, $Q = \{q_a \mid a \in A\}$, $P \cup Q$, $P \triangle Q$, $D = \{p_a - q_a \mid a \in A\}$, $E = \{\frac{a}{p_a} \mid a \in A\}$, $S = E \triangle E \triangle D \triangle \varnothing$.

**Esercizio 3.** Definiamo in $\mathbb{N} \times \mathbb{N}$ la relazione d'ordine $\rho$ ponendo, per ogni $a, b, c, d \in \mathbb{N}$,

$$(a,b)\ \rho\ (c,d) \iff \big((a,b) = (c,d) \vee \text{rest}(a+b,7) \text{ divide propriamente } \text{rest}(c+d,7)\big).$$

(*i*) Determinare gli eventuali elementi minimali, massimali, minimo, massimo in $(\mathbb{N} \times \mathbb{N}, \rho)$.
(*ii*) Tra gli elementi di $\mathbb{N} \times \mathbb{N}$ che hanno 3 come seconda coordinata, determinare quelli che sono elementi massimali in $(\mathbb{N} \times \mathbb{N}, \rho)$.
(*iii*) $(\mathbb{N} \times \mathbb{N}, \rho)$ è un reticolo?
(*iv*) Il diagramma a destra rappresenta un reticolo? Nel caso, un reticolo distributivo?, complementato?, booleano?
(*v*) Se possibile, costruire una parte $V$ di $\mathbb{N} \times \mathbb{N}$ tale che $(V, \rho)$ sia rappresentato dal diagramma di Hasse a destra; se non è possibile farlo spiegare perché.



**Esercizio 4.** Sia $M$ l'insieme delle matrici $2 \times 2$ sull'anello $\mathbb{Z}_9$.

(*i*) Stabilire se la relazione binaria $\alpha$ definita in $M$ ponendo, per ogni $A, B \in M$, $A\ \alpha\ B$ se e solo se esistono $a, b, c, d \in \mathbb{Z}$ tali che $A = B + \begin{pmatrix} \overline{3a} & \overline{3b} \\ \overline{3c} & \overline{3d} \end{pmatrix}$ è una relazione di equivalenza.

Si considerino l'applicazione $f\colon (a,b) \in \mathbb{Z}_9 \times \mathbb{Z}_9 \mapsto \begin{pmatrix} a-b & a \\ a & a+b \end{pmatrix} \in M$, il suo insieme immagine $T = \vec{f}(\mathbb{Z}_9 \times \mathbb{Z}_9)$ e $S = \{\begin{pmatrix} a & a \\ a & a \end{pmatrix} \big| a \in \mathbb{Z}_9\}$,

(*ii*) $f$ è iniettiva? $f$ è suriettiva?; (*iii*) Quanto vale $|T|$?; (*iv*) Si ha $S \subseteq T$?

Si munisca $M$ della moltiplicazione $\cdot$ righe per colonne. Rispetto a questa operazione

(*v*) $S$ è una parte chiusa? $T$ è una parte chiusa?

Se una delle due lo è, chiamata questa $C$, si stabilisca (facendo esplicito uso dell'algoritmo risolutivo per le equazioni congruenziali, ove possa servire):

(*vi*) che tipo di struttura (commutativa o meno, semigruppo, monoide) è $(C, \cdot)$, specificandone eventuali elementi neutri a destra, neutri a sinistra, neutri;
(*vii*) se le domande hanno senso,
(a) $\begin{pmatrix} \overline{4} & \overline{4} \\ \overline{4} & \overline{4} \end{pmatrix}$ è invertibile in $(C, \cdot)$? Nel caso, calcolare l'inverso;
(b) $\begin{pmatrix} \overline{6} & \overline{6} \\ \overline{6} & \overline{6} \end{pmatrix}$ è invertibile in $(C, \cdot)$? Nel caso, calcolare l'inverso;
(c) quali e quanti sono gli elementi invertibili in $(C, \cdot)$?