CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
12 NOVEMBRE 2018

Svolgere i seguenti esercizi,

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

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

Esercizio 1. Dare la definizione di *gruppo* e dimostrare in dettaglio che, per ogni insieme S, $(\mathcal{P}(S), \triangle)$ è un gruppo.

(i) Verificare che la relazione binaria $\mathcal{R}$ definita in $\mathcal{P}(\mathbb{Z})$ ponendo, per ogni $A, B \in \mathcal{P}(\mathbb{Z})$,
$$A \,\mathcal{R}\, B \iff (\exists X \in \mathcal{P}(\{1,2\}))(A = B \triangle X)$$
è una relazione di equivalenza.

(ii) Elencare gli elementi di $[\mathbb{N}]_{\mathcal{R}}$. Quanto vale $|[\mathbb{N}]_{\mathcal{R}}|$?

(iii) Qual è la massima cardinalità possibile per $[A]_{\mathcal{R}}$, al variare di A in $\mathcal{P}(\mathbb{Z})$?

Esercizio 2. Risolvere l'equazione congruenziale $30x \equiv_{104} 8$, descrivendo l'insieme di tutte le sue soluzioni intere.

Esercizio 3. Vero o falso? Per ogni insieme ordinato $(S, \leq)$...

(i) ...se $(S, \leq)$ è un reticolo, in $(S, \leq)$ esistono $\inf S$ e $\sup S$;

(ii) ...se in $(S, \leq)$ esiste $\inf S$, allora $\inf S = \min S$;

(iii) ...se in $(S, \leq)$ esiste $\min S$, allora $\min S = \inf S$;

(iv) ...se $X \subseteq S$ e, in $(S, \leq)$, esiste $\inf X$, allora $\inf X = \min X$;

(v) ...se $X \subseteq S$ e, in $(S, \leq)$, esiste $\min X$, allora $\min X = \inf X$;

(vi) ...se $(S, \leq)$ è totalmente ordinato, allora è un reticolo;

(vii) ...se $(S, \leq)$ è un reticolo limitato, $0 = \min S$ e $1 = \max S$, allora $(S, \leq)$ è complementato se e solo se per ogni $a, b \in S$ si ha $a \wedge b = 0$ e $a \vee b = 1$.

Inoltre:

$(viii)$ Esistono reticoli non totalmente ordinati? Nel caso, fornire un esempio.

(ix) Dare le definizione di *minorante* di una parte X in un insieme ordinato $(S, \leq)$.

Esercizio 4. Sia $*$ l'operazione binaria definita in $\mathbb{Z} \times \mathbb{Z}$ ponendo, per ogni $a, b, c, d \in \mathbb{Z}$,
$$(a, b) * (c, d) = (a, b + d + 3).$$

(i) Come applicazione da $(\mathbb{Z} \times \mathbb{Z}) \times (\mathbb{Z} \times \mathbb{Z})$ a $\mathbb{Z} \times \mathbb{Z}$, $*$ è iniettiva? È suriettiva?

(ii) $*$ è commutativa? È associativa? Ammette elementi neutri a destra, a sinistra, neutri? Che tipo di struttura algebrica è $(\mathbb{Z} \times \mathbb{Z}, *)$?

(iii) Descrivere gli elementi di $X = \{-1\} \times \mathbb{Z}$. X è una parte chiusa di $(\mathbb{Z} \times \mathbb{Z}, *)$? Se lo è, stabilire che tipo di struttura algebrica è $(X, *)$.

Esercizio 5. Sia $f = \big(x^4 - (x + \bar{1})^2\big)(x^3 - x + \bar{2})^{100} \in \mathbb{Z}_3[x]$. *Senza eseguire moltiplicazioni,*

(i) scrivere f come prodotto di polinomi monici irriducibili in $\mathbb{Z}_3[x]$;

(ii) *dopo* averlo fatto, determinare le radici di f in $\mathbb{Z}_3$.