CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
14 FEBBRAIO 2020

Svolgere i seguenti esercizi,

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

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola**, **gruppo di appartenenza**. Chi usufruisce dell'esonero non deve rispondere ad esercizi e domande marcate con ★.

Non è necessario consegnare la traccia.

★ **Esercizio 1.** In $\mathbb{Z}_{10}$ si consideri l'operazione binaria $*$ definita da: per ogni $a, b \in \mathbb{Z}_{10}$,
$$a * b = a + \bar{6}b.$$

★ (i) Decidere se $*$ è commutativa e se è associativa.

★ (ii) Verificare se in $(\mathbb{Z}_{10}, *)$ esistono elementi neutri a destra, neutri a sinistra, neutri.

Sia $P = \{\overline{2n} \mid n \in \mathbb{Z}\}$.

★ (iii) Verificare che, per ogni $x \in P$, si ha $\bar{6}x = x$.

★ (iv) P è chiusa rispetto a $*$?

★ (v) Se le domande hanno senso, decidere se l'operazione indotta da $*$ su P è commutativa, se $(P, *)$ è un semigruppo, se è un monoide, se è un gruppo.

Esercizio 2.

★ (i) Si spieghi perché è ben definita l' applicazione $f\colon X \in \mathcal{P}(\mathbb{N}) \smallsetminus \{\varnothing\} \mapsto \min X \in \mathbb{N}$.

★ (ii) f è iniettiva? f è suriettiva?

★ (iii) $\overleftarrow{f}(\{3\})$ è un insieme finito o infinito?

(iv) Indicato con $\mathcal{R}$ il nucleo di equivalenza di f, si descrivano in modo esplicito $\big[\{0,5\}\big]_{\mathcal{R}}$ e $\big[\{2^n \mid n \in \mathbb{N}^*\}\big]_{\mathcal{R}} \cap \mathcal{P}(\{1,2,3\})$.

Esercizio 3. Si dica quando, per definizione, una relazione binaria ρ definita su in insieme S è antisimmetrica. Si stabilisca poi quali delle seguenti relazioni binarie sono e quali non sono antisimmetriche:

(i) α, definita in $\mathcal{P}(\mathbb{Z})$ ponendo, per ogni $A, B \in \mathcal{P}(\mathbb{Z})$, $A \;\alpha\; B \iff A \cap \mathbb{N} \subseteq B \cap \mathbb{N}$.

(ii) β, definita in $\mathbb{N}$ ponendo, per ogni $a, b \in \mathbb{N}$, $a \;\beta\; b \iff a|2b$;

Esercizio 4. Sia σ la relazione d'ordine definita in $\mathbb{N}$ ponendo, per ogni $a, b \in \mathbb{N}$,
$$a \;\sigma\; b \iff \big(a|b \wedge \operatorname{rest}(a,5) \le \operatorname{rest}(b,5)\big).$$

(i) Determinare l'insieme dei maggioranti di $\{5\}$ in $(\mathbb{N}, \sigma)$.

(ii) Verificare che, per ogni $n \in \mathbb{N}$, i numeri n e $6n$ sono confrontabili rispetto a σ.

(iii) Determinare in $(\mathbb{N}, \sigma)$ eventuali minimo, massimo, elementi minimali, elementi massimali.

(iv) Si trovino in $(\mathbb{N}, \sigma)$ gli insiemi dei minoranti e dei maggioranti di $X := \{2, 10\}$ e, se esistono, $\inf X$ e $\sup X$.

(v) $(\mathbb{N}, \sigma)$ è un reticolo?

(vi) Trovare in $\mathbb{N}$, o spiegare perché non esiste, un sottoinsieme infinito su cui σ induca una relazione d'ordine totale.

(vii) Trovare due sottoinsiemi A e B di $\mathbb{N}$, tali che $B \subseteq A$, $|A| = 5$, $|B| = 4$, (A, σ) sia un reticolo non distributivo e (B, σ) sia un sottoreticolo booleano di (A, σ).

Esercizio 5. Vero o falso (*e perché?*)

(i) In $\mathbb{Z}_{11}[x]$, un polinomio f ammette $\bar{2}$ e $\bar{3}$ come radici se e solo $x^2 - \bar{5}x - \bar{5}$ divide f.

(ii) $x^2 - \bar{5}x - \bar{5}$ è irriducibile in $\mathbb{Z}_{11}[x]$.

(iii) Per ogni primo positivo p, il polinomio $x^2 - \bar{5}x - \bar{5}$ in $\mathbb{Z}_p[x]$ non è irriducibile.

(iv) In $\mathbb{Z}_3[x]$, $(x^3 - x + \bar{1})(x^3 - x + \bar{2})$ è irriducibile.

(v) In $\mathbb{Z}_{11}[x]$, i polinomi $g = \bar{7}x^2 + \bar{3}$ e $h = \bar{3}x^2 - \bar{5}$ sono associati (per rispondere, utilizzare e risolvere esplicitamente un'equazione congruenziale).