CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
17 GIUGNO 2022

Svolgere i seguenti esercizi,

⟶ $\boxed{\textbf{\textit{giustificando pienamente tutte le risposte.}}}$ ⟵

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola**, **gruppo di appartenenza**.

Non è necessario consegnare la traccia.

NB: I simboli '$\leftrightarrow$' e '$\rightarrow$' sono anche usati per indicare i connettivi bicondizionale ('$\iff$') e condizionale ('$\Rightarrow$') rispettivamente.

Esercizio 1.

(*i*) Stabilire se le forme proposizionali $\big(p \to (p \leftrightarrow p)\big)$ e $\big((p \to p) \leftrightarrow p\big)$ sono logicamente equivalenti.

Sia ora φ la frase (del linguaggio ordinario): "x è la capitale della Francia".

(*ii*) Negare, formalmente e con una frase del linguaggio ordinario, la formula $(\exists! x)(\varphi(x))$.

(*iii*) Detta θ la formula $(\forall x)(\varphi(x))$, e assumendo l'interpretazione ordinaria per le parole che appaiono nella formula φ, decidere se le formule $\theta \to (\theta \leftrightarrow \theta)$ e $(\theta \to \theta) \leftrightarrow \theta$ sono logicamente equivalenti.

Esercizio 2. Quando, *per definizione*, dati tre interi a, b e m, si ha $a \equiv_m b$? Inoltre:

(*i*) per quali interi c si ha $3 \equiv_c -2$?

(*ii*) Per quali interi d si ha $5 \equiv_d 2$?

(*iii*) Esiste un intero negativo e tale che 2 sia nella stessa classe di equivalenza di 3 modulo e?

Esercizio 3. Si consideri l'operazione binaria $*$ definita in $\mathcal{P}(\mathbb{Z})$ ponendo, per ogni $a, b \in \mathcal{P}(\mathbb{Z})$,

$$a * b = (a \mathbin{\triangle} \mathbb{N}) \mathbin{\triangle} b.$$

Si decida se $*$ è commutativa, se è associativa, se in $(\mathcal{P}(\mathbb{Z}), *)$ esistono elementi neutri a destra o a sinistra, se $(\mathcal{P}(\mathbb{Z}), *)$ è un gruppo. Nel caso la domanda abbia senso, determinare il simmetrico di $\mathbb{Z}$ rispetto ad $*$.

Esercizio 4. Poniamo, per ogni $n \in \mathbb{Z}$, $\quad \bar{n} = [n]_5$.

(*i*) Descrivere $A := \{f \in \mathbb{Z}_5[x] \mid f(\bar{1}) = f(\bar{2}) = \bar{0} \wedge f \text{ ha grado } 3\}$ e calcolare $|A|$.

(*ii*) Posto $B = \{f \in \mathbb{Z}_5[x] \mid f(\bar{3}) = \bar{0}\}$, descrivere $A \cap B$ e calcolare $|A \cap B|$.

(*iii*) Descrivere esplicitamente $\overline{A} = \{f \in A \mid f \text{ è irriducibile}\}$ e $\overline{B} = \{f \in B \mid f \text{ è irriducibile}\}$; calcolare $|\overline{A}|$ e $|\overline{B}|$.

(*iv*) Elencare gli elementi di $C := \{a^2 \mid a \in \mathbb{Z}_5\}$; utilizzando questo elenco costruire un polinomio irriducibile di grado 2 in $\mathbb{Z}_5[x]$.

Esercizio 5. Sia S l'insieme delle parti finite e non vuote di $\mathbb{Z}$. Sia poi f l'applicazione $X \in S \mapsto \max X - \min X \in \mathbb{N}$.

(*i*) f è iniettiva? f è suriettiva?

(*ii*) Descrivere $\overleftarrow{f}(\{0\})$.

(*iii*) Detto σ il nucleo di equivalenza di f, descrivere $[\{4\}]_\sigma$ e decidere se l'insieme quoziente S/σ è finito o infinito.

Sia ρ la relazione d'ordine in S definita ponendo, per ogni $X, Y \in S$,

$$X \mathrel{\rho} Y \iff \big(X = Y \vee f(X) \text{ è un divisore proprio di } f(Y)\big).$$

(*iv*) Determinare gli eventuali elementi minimali, massimali, minimo, massimo in (S, ρ).

(*v*) Decidere se (S, ρ) è un reticolo.

(*vi*) Disegnare il diagramma di Hasse di (T, ρ), dove $T = \{A, B, C, D, E, F, G, H, I\}$, e $A = \{0, 1\}$, $B = \{1, -1\}$, $C = \{0, 1, 2, 3\}$, $D = \{0, 2, 4, 6\}$, $E = \{0, 100!\}$, $F = \{2, 10, 20\}$, $G = \{-2, 2\}$, $H = \{1, 5, 25\}$, $I = \{1, 10\}$ decidendo poi se (T, ρ) è un reticolo e, nel caso, se è distributivo, complementato, booleano.