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

Svolgere i seguenti esercizi,

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

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.** Si consideri l'applicazione $f\colon X \in \mathcal{P}(\mathbb{Z}) \mapsto \{x+2 \mid x \in X\} \in \mathcal{P}(\mathbb{Z})$.

(*i*) Calcolare $f(\{-2,2,4\})$, $f(\mathbb{Z})$ e $\overleftarrow{f}(\{\{-2,3,5\}\})$.

(*ii*) Verificare che f è biettiva e calcolare f^{-1}.

(*iii*) Siano $h\colon x \in \mathbb{Q} \mapsto 2x+1 \in \mathbb{Q}$ e $g\colon y \in \mathbb{Z} \mapsto y/3 \in \mathbb{Q}$; descrivere $k := h \circ g$ e decidere se k è suriettiva.

Esercizio 2. Si consideri l'operazione binaria definita in $S := \mathbb{Z} \times \mathbb{Z}_{64}$ da: per ogni $(a,\bar{b}),(c,\bar{d}) \in S$,

$$(a,\bar{b}) * (c,\bar{d}) = (ac, \overline{bc} + \bar{d}).$$

★ (*i*) Decidere se $*$ è commutativa, se è associativa, se ammette elementi neutri a destra e/o a sinistra.

★ (*ii*) Nel caso la domanda abbia senso, descrivere gli elementi simmetrizzabili in $(S,*)$. Quanti sono? Che tipo di struttura (semigruppo, monoide, gruppo) è $(S,*)$?

★ (*iii*) Detti $V = 64\mathbb{Z} \times \mathbb{Z}_{64}$ e $W = \{65\} \times \mathbb{Z}_{64}$, si dica se per ciascuna di V e W se è una parte chiusa in $(S,*)$ e, dove la domanda abbia senso, che tipo di strutture siano $(V,*)$ e $(W,*)$.

(*iv*) Determinare, nel caso esistano, gli elementi $(u,\bar{v})$ di S tali che $(u,\bar{v}) * (8,\overline{15}) = (-8,\bar{2})$.

Esercizio 3. Sia $A = \{n \in \mathbb{N} \mid n < 14\}$. Quante sono le parti X di A che verificano contemporaneamente le condizioni $6 \in X$, $\quad 7 \notin X \quad$ e $\quad |X| = 5$?

Esercizio 4. Enunciare il teorema fondamentale che lega relazioni di equivalenza e partizioni in un insieme. Dimostrare che la relazione binaria $\sim$ definita in $A := \{n \in \mathbb{N} \mid n < 14\}$ da

$$\forall a,b \in A(a \sim b \iff a^2 + 3 \equiv_6 b^2 - 3)$$

è di equivalenza (suggerimento: ragionare sulle classi di a^2 e b^2 modulo 6; la condizione $a^2+3 \equiv_6 b^2-3$ equivale a…?) e descrivere, elencando gli elementi di ciascuna classe, $A/\!\sim$.

Esercizio 5. Sia S l'insieme delle parti finite e non vuote di $\mathbb{N}$. Si definisca la relazione binaria ρ in S ponendo, per ogni $X,Y \in S$

$$X \,\rho\, Y \iff \big(X = Y \vee \forall x \in X(\forall y \in Y(x \leq y))\big).$$

Dando per noto che ρ è una relazione d'ordine,

(*i*) stabilire se ρ è una relazione totale.

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

(*iii*) Posto $X = \{1,2,3,4\}$ e $Y = \{2,5\}$, determinare in (S,ρ) l'insieme dei maggioranti di $\{X,Y\}$ e decidere se esiste $\sup\{X,Y\}$;

(*iv*) Sia $T = \{A,B,C,D,E,F,G,H\}$, dove $A = \{0\}$, $B = \{0,4\}$, $C = \{0,6\}$, $D = \{4,5,7\}$, $E = \{6\}$, $F = \{6,9\}$, $G = \{7\}$, $H = \{9\}$. Disegnare il diagramma di Hasse di (T,ρ) e decidere se (T,ρ) è un reticolo, un reticolo distributivo, un reticolo complementato.

(*v*) Esiste in S un elemento I tale che $(T \cup \{I\},\rho)$ sia un reticolo non distributivo? Indicarne uno o spiegare perché non ne esistono.

Esercizio 6. Si determini il massimo primo p tale che $f := x^3 - \bar{3}x^2 + \bar{4}x + \bar{2} \in \mathbb{Z}_p[x]$ abbia $\bar{3}$ come radice. Si scriva poi f come prodotto di polinomi monici irriducibili in $\mathbb{Z}_p[x]$. Inoltre:

(*i*) in $\mathbb{Z}_p[x]$, un polinomio associato a $x - \bar{3}$ deve dividere f? Quanti sono, in tutto, i polinomi di primo grado in $\mathbb{Z}_p[x]$ che dividono f?

(*ii*) *Senza eseguire calcoli,* decidere se $f + (x-\bar{3})^5$ è o non è irriducibile in $\mathbb{Z}_p[x]$.

(*iii*) Si determini, nel caso esista, un polinomio g associato a f in $\mathbb{Z}_p[x]$ che abbia coefficiente direttore $\bar{4}$.

(*iv*) Si determini, nel caso esista, un polinomio h associato a f in $\mathbb{Z}_p[x]$ tale che $h(\bar{0}) = \bar{4}$.