CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
15 LUGLIO 2024

Svolgere i seguenti esercizi,

$\longrightarrow$ ***giustificando pienamente tutte le risposte.*** $\longleftarrow$

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

Esercizio 1. Sia $A = \mathcal{P}_2(\mathbb{Z})$ l'insieme delle parti di $\mathbb{Z}$ di cardinalità 2. Sia σ la relazione d'ordine definita da: $\forall a, b \in A$

$$a \ \sigma \ b \iff \big(a = b \vee \forall x \in a (\forall y \in b \ (x \text{ divide } y))\big).$$

Sia $B = \{\{0, 12\}, \{0, 16\}, \{1, 2\}, \{2, 4\}, \{2, 8\}, \{4, 6\}\}$

- (i) Disegnare un diagramma di Hasse di (B, σ). Stabilire se (B, σ) è un reticolo e, nel caso, se è distributivo, complementato, booleano.
- (ii) Determinare un sottoinsieme C di B della cardinalità massima possibile tale che (C, σ) sia un reticolo complementato.
- (iii) Determinare in (A, σ) i minoranti di $\{\{1, 4\}\}$ e, se esistono, $\inf\{\{1, 4\}, \{1, 6\}\}$ e $\sup\{\{1, 4\}, \{1, 6\}\}$.
- (iv) Determinare, se ne esistono, gli elementi minimali, massimali, minimo, massimo in (A, σ).
- (v) Esiste $a \in A$ tale che $(B \cup \{a\}, \sigma)$ sia un reticolo?

Esercizio 2. Stabilire per quali $c \in \{1, 3, 20, 24, 55, 60\}$ l'equazione congruenziale $470x \equiv_{350} 3c$ ha soluzioni in $\mathbb{Z}$ e, per ciascun tale c, fornire l'insieme delle soluzioni.

Esercizio 3. Sia S un insieme tale che $|S| = 13$ e sia h un suo elemento. Indicare (ma non calcolare): (a) il numero delle parti di S di cardinalità 8; (b) il numero delle parti di S di cardinalità 18; (c) il numero delle parti T di S tali che $|T| = 7$ e $h \in T$; (d) il numero delle relazioni binarie in S.

Esercizio 4. Per ciascuno degli insiemi $\mathbb{Z}$, $\mathbb{Z}_6$ e $\mathbb{Z}_3$ si consideri l'operazione binaria (che indichiamo sempre con lo stesso simbolo) $*$ definita da: per ogni a, b appartenenti all'insieme, $a * b = 3a + b$. Che tipo di strutture algebriche (semigruppi, monoidi, gruppi; commutativi o no?) sono $(\mathbb{Z}, *)$, $(\mathbb{Z}_6, *)$ e $(\mathbb{Z}_3, *)$? In ciascuna di esse determinare gli eventuali elementi neutri a sinistra o a destra.

Esercizio 5. Siano $S = \mathbb{N} \smallsetminus \{0, 1\}$ ed $f \colon S \to S$ l'applicazione che ad ogni $n \in S$ associa la somma $\sum_{n \geq p \in \mathbb{P}} p$ dei numeri interi positivi primi minori o uguali a n (ad esempio, $f(4) = 2 + 3 = 5$). Sia poi $\Re$ il nucleo di equivalenza di f.

- (i) Determinare $\overleftarrow{f}(\{10\})$ e $\overleftarrow{f}(\{11\})$.
- (ii) f è iniettiva? f è suriettiva? f è biettiva?
- (iii) Elencare gli elementi di $[8]_\Re$.
- (iv) $|S/\Re|$ è finito o infinito?
- (v) Esiste $a \in S$ tale che $a \notin [a]_\Re$?
- (vi) Posto $T = \{n \in S \mid 10 \leq n \leq 20\}$, detta $\Re_T$ la relazione di equivalenza indotta da $\Re$ su T, descrivere esplicitamente le classi appartenenti a $T/\Re_T$, elencandone gli elementi. Quanto vale $|T/\Re_T|$?

Esercizio 6.

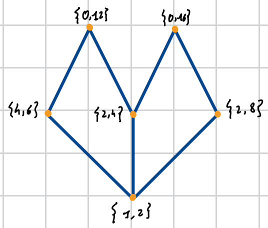
- (i) Quali tra queste affermazioni sono vere, e quali no, per tutte le possibili scelte di un anello commutativo unitario A, di $f \in A[x]$ e di due elementi distinti a e b di A:
  - (a) se a e b sono radici di f, allora $(x - a)$ e $(x - b)$ dividono f in $A[x]$;
  - (b) se a e b sono radici di f, allora $(x - a)(x - b)$ divide f in $A[x]$;
  - (c) se A è un campo e a e b sono radici di f, allora $(x - a)(x - b)$ divide f in $A[x]$.
- (ii) Esistono un anello commutativo unitario A ed un polinomio di grado 2 in $A[x]$ tali che f abbia infinite radici in A?
- (iii) Sia $f \in \mathbb{Z}_{13}[x]$. Supponiamo $f = pqr$ dove p, q ed r sono polinomi irriducibili in $\mathbb{Z}_{13}[x]$, p e q hanno grado 1 e r ha grado 4. Allora, in $\mathbb{Z}_{13}[x]$,
  - (a) quanti divisori monici di grado 3 ha f?
  - (b) quanti divisori monici di grado 2 ha f?
  - (c) assumendo p e q non associati tra loro, quanti divisori, monici o non monici, di grado 5 ha f?

Esercizio 1

$A = P_2(\mathbb{Z})$ $\quad \forall a,b \in A (a = b \vee \forall x \in a (\forall y \in b (x | y))$

$B = \{\{0,12\}, \{0,16\}, \{1,2\}, \{2,4\}, \{2,8\}, \{4,6\}\}$

i)



Non è un reticolo perchè non esiste un $\sup(\{0,12\}, \{0,16\})$

ii) $C = \{\{0,16\}, \{1,2\}, \{2,4\}, \{2,8\}\}$

iii) $\text{Minoranti}(\{1,4\}) = \{1, -1\}$
$\inf(\{\{1,4\}, \{1,6\}\}) = \{1, -1\}$
$\sup(\{\{1,4\}, \{1,6\}\}) = \{12, -12\}$

iv) minimali: $\{\{1,-1\}\}$
min: $\{1, -1\}$
massimali: $\{0, n \in \mathbb{Z} \setminus \{0\}\}$

v) non esiste

Esercizio 2

$470x \equiv_{350} 3c$

$120x \equiv_{350} 3c$ $\qquad 12x \equiv_{35} 3c$

$\text{MCD}(350, 120) = 10$

$c \in \{1, 3, 20, 24, 55, 60\}$
ammettono soluzioni solo le c divisibili per 10, quindi $c \in \{20, 60\}$

$35 = 12 \cdot 2 + 11$
$12 = 11 \cdot 1 + 1$

$c = 20$	$120x \equiv_{350} 60$	$12x \equiv_{35} 6$	$3 \cdot 12x \equiv_{35} 6 \cdot 12$	$x \equiv_{35} 2$
$c = 60$	$120x \equiv_{350} 180$	$12x \equiv_{35} 18$	$3 \cdot 12x \equiv_{35} 18 \cdot 12$	$x \equiv_{35} 6$

$1 = 12 + 11 \cdot (-1)$
$1 = 12 + (35 + 12(-2))(-1)$
$1 = 12 + 35(-1) + 12(2)$
$1 = 35(-1) + 12(3)$

ESERCIZIO 4

$\forall a, b \in \mathbb{Z}_x \, (a * b = 3a + b)$

ASSOCIATIVA

$(a*b)*c = a*(b*c)$
$3(3a+b)+c = 3a+(3b+c)$
$9a+3b+c = 3a+3b+c$

$(\mathbb{Z}, *)$ FALSO, non è associativa quindi non è una struttura algebrica

$(\mathbb{Z}_6, *)$ $\bar{9}a+\bar{3}b+c = \bar{3}a+\bar{3}b+c$
$\bar{3}a+\bar{3}b+c = \bar{3}a+\bar{3}b+c$
VERO, è associativa

$(\mathbb{Z}_3, *)$ $\bar{9}a+\bar{3}b+c = \bar{3}a+\bar{3}b+c$
$\bar{3}a+\bar{3}b+c = \bar{3}a+\bar{3}b+c$
VERO, è associativa

ELEMENTO NEUTRO

$a*b = a \Rightarrow 3a+b = a$
$b*a = a \Rightarrow 3b+a = a$

$(\mathbb{Z}_6, *)$ $\bar{3}b + a = a$ $\qquad b = [0]_6$

$\bar{3}a+b = a \Rightarrow b = -\bar{3}a+a \Rightarrow b = -\bar{2}a = b = 4a$

Neutro sx: $[0]$
Neutro dx: nessuno

$(\mathbb{Z}_3, *)$ $\bar{3}b+a = a$
b è un qualunque elemento di $\mathbb{Z}_3$

$\bar{3}a+b = a$
$b = a$, non esiste neutro

ESERCIZIO 5

$S = \mathbb{N} \setminus \{0,1\}$ $\qquad f: S \to S \, (\forall n \in S \, (f(n) = \text{somma interi positivi} < n)$

i) $\overleftarrow{f}(\{10\}) = \{6\}$ $\qquad \overleftarrow{f}(\{11\}) = \varnothing$

ii) INIETTIVA: NO
$\forall x, y \in S \, (f(x) = f(y) \Leftrightarrow x = y)$

$f(8) = 2+3+5+7 = 17$
$f(9) = 2+3+5+7 = 17$

Suriettiva: NO

$$\forall x \in S \ \exists x \in S \ (y = f(x))$$

10 non è immagine di nessun elemento

Biettiva: NO

iii) $[8]_R = \{8, 9, 10\}$

iv) $|S \setminus R| = \infty$, perchè infiniti sono i numeri

v) No, ogni elemento di S ha una somma di primi minori

vi) $T = \{n \in S \mid 10 \leq n \leq 20\}$

$$\left.f(10) = 17\right\} \quad [10]_{R_T} = \{10\}$$

$$\left.\begin{array}{l} f(11) = 28 \\ f(12) = 28 \end{array}\right\} \quad [11]_{R_T} = \{11, 12\}$$

$$\left.\begin{array}{l} f(13) = 41 \\ f(14) = 41 \\ f(15) = 41 \\ f(16) = 41 \end{array}\right\} \quad [13]_{R_T} = \{13, 14, 15, 16\}$$

$$\left.\begin{array}{l} f(17) = 58 \\ f(18) = 58 \end{array}\right\} \quad [17]_{R_T} = \{17, 18\}$$

$$\left.\begin{array}{l} f(19) = 78 \\ f(20) = 78 \end{array}\right\} \quad [19]_{R_T} = \{19, 20\}$$