CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)
2 MARZO 2023

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. Si consideri l'operazione definita in $\mathbb{Z}_{16}$ definita da: per ogni $a, b \in \mathbb{Z}_{16}$, $a*b = a+b+\bar{3}ab$.

(i) Verificare che $(\mathbb{Z}_{16}, *)$ è un monoide e determinarne l'elemento neutro.
(ii) Determinare $U = \mathcal{U}(\mathbb{Z}_{16}, *)$.
(iii) Che tipo di struttura è $(U, *)$?
(iv) Determinare chi tra $\bar{2}$ e $\bar{3}$ è simmetrizzabile in $(\mathbb{Z}_{16}, *)$ e determinarne il simmetrico.

Esercizio 2. Sia $g = (v, l)$ un grafo (semplice) finito connesso senza circuiti. È possibile determinare la somma dei gradi di tutti i vertici, sapendo che $|v| = 8$? Se sì, determinarla.

Esercizio 3. Sia a un insieme tale che $|a| = 7$ e sia $P = \mathcal{P}_4(a)$ l'insieme delle sue parti costituite da (esattamente) quattro elementi.

(i) Quanti elementi ha P? Quante sono le applicazioni da a a P? (Rispondere senza eseguire i calcoli).
(ii) Quante sono le partizioni F di a tali che $F \cap P \neq \varnothing$?
(iii) Fissato un elemento c di a, quanti sono gli elementi di P a cui c non appartiene?

Esercizio 4. Di ciascuna delle seguenti relazioni binarie dire se è o non è d'ordine e, nel caso lo sia, determinare gli eventuali minimo, massimo, elementi minimali ed elementi massimali nell'insieme ordinato da essa definito.

(i) α definita su $\mathbb{Z}$ da: $\forall a, b \in \mathbb{Z}(a\ \alpha\ b \iff (a \leq b \wedge a \equiv_3 b))$;
(ii) β definita su $\mathbb{N}$ da: $\forall a, b \in \mathbb{N}(a\ \beta\ b \iff (a \leq b \wedge a \equiv_3 b))$;
(iii) γ definita su $\mathbb{Z}$ da: $\forall a, b \in \mathbb{Z}(a\ \gamma\ b \iff (a \leq b \vee a \equiv_3 b))$.

Esercizio 5. Si consideri l'applicazione $f\colon (a, b) \in \mathbb{Z}_7 \times \mathbb{Z}_7 \mapsto \max(a \smallsetminus \mathbb{N}^*) + \min(b \cap \mathbb{N}^*) \in \mathbb{Z}$.

(i) Determinare $\vec{f}(\mathbb{Z}_7 \times \mathbb{Z}_7)$.
(ii) f è iniettiva? È suriettiva?
(iii) Detto $\mathcal{R}_f$ il nucleo di equivalenza di f, determinare $|(\mathbb{Z}_7 \times \mathbb{Z}_7)/\mathcal{R}_f|$.
(iv) Determinare la classe di equivalenza di $[([1]_7, [6]_7)]_{\mathcal{R}_f}$.

Esercizio 6. Dando per noto che nell'anello $\mathbb{Z}_7[x]$ il polinomio $p = x^4 + \bar{3}x^2 - \bar{2}$ è irriducibile,

(i) scrivere $p^{100}(p - \bar{2})$ come prodotto di polinomi monici irriducibili in $\mathbb{Z}_7[x]$.
(ii) Quanti e quali sono i divisori monici di p^{100} in $\mathbb{Z}_7[x]$?
(iii) Quanti e quali sono i divisori, monici o non monici, di p^{100} in $\mathbb{Z}_7[x]$ che abbiano grado 57?

ES 1

$\forall a, b \in \mathbb{Z}_{16} \left(a * b = a + b + \overline{3}ab \right)$

i) MONOIDE: SI

COMMUTATIVA: SI

$+, \cdot$ sono commutativi

Trovata perchè facilita calcoli associatività e neutro

ASSOCIATIVA: SI

$(a*b)*c = a*(b*c)$

$(a+b+3ab)+c+3(ac+bc+3abc)$

$a+b+3ab+c+3ac+3bc+9abc$

$9abc+3ab+3ac+3bc+a+b+c$

$(b*c)*a$

$(b+c+3bc)+a+3(ab+ac+3abc)$

$9abc+3ab+3ac+3bc+a+b+c$

NEUTRO: SI : 0

$a*n = a$

$a+n+\overline{3}an = a$

$3an = a-a \Rightarrow \overline{3}an = 0 \Rightarrow n = 0$

poichè $\overline{3}$ non divide $\overline{16}$, non esistono altri n che moltiplicati per $\overline{3}$ sono uguali $[0]_{16}$

ii) $U = U(\mathbb{Z}_{16}, *) = \{0, 2, 4, 8, 10, 12, 14\}$

$a * i = \overline{0} \Rightarrow$

$a + i + 3ai = \overline{0} \Rightarrow i + 3ai = -a$

$a = 0 \quad i = 0$

$a = 1$

$i + 3i = 15 \qquad 4i = 15 \qquad MCD(4, 16) = 4 \quad \neg(4 \mid 15)$ no soluzioni

$a = 2$

$i + 3 \cdot 2i = 14 \qquad 7i = 14 \qquad MCD(7, 16) = 1$, è invertibile

$a = 3$

$i + 3 \cdot 3i = 13 \qquad 10i = 13 \qquad MCD(10, 16) = 2$

$a = 4$

$i + 3 \cdot 4i = 12 \qquad 13i = 12 \qquad MCD(13, 16) = 1$

$a = 5$

$i + 3 \cdot 5i = 11 \qquad 16i \equiv 11 \qquad MCD(16, 16) = 16$

iii) $(U, *)$ è un gruppo abeliano

iv) $\overline{3}$ non è simmetrizzabile

$\overline{2}$ è simmetrizzabile $\qquad \overline{7}i = 14$

$16 = 7 \cdot 2 + 2$

$7 = 2 \cdot 3 + 1 \leftarrow MCD$

$1 = 7 + 2(-3) =$

$= 7 + (16 + 7(-2))(-3)$

$= 7 + 16(-3) + 7(6) =$

$= 7(7) + 16(-3)$

$\overline{7} \cdot \overline{7}i = \overline{14} \cdot \overline{7} \Rightarrow \overline{49}i = \overline{98} \Rightarrow i = 2$

Es 2

$\mathcal{G} = (V, \mathcal{E})$ albero. $|V| = 8$

La somma dei gradi di tutti i vertici (α) è $2 \cdot |\mathcal{E}|$, e poiché $\mathcal{G}$ è un albero, $|\mathcal{E}| = |V - 1|$.

$|\mathcal{E}| = |V| - 1 = 7$

$\alpha = 2 \cdot 7 = 14$

Es 3

$|\alpha| = 7$, $P = P_4(\alpha)$

i) $|P| = \binom{7}{4}$

$|P|^{|\alpha|}$

ii)

iii) $\binom{6}{4}$

ES 4

i) $\alpha: \forall a,b \in \mathbb{Z}\,(a \alpha b \iff (a \le b \land a \equiv_3 b))$ REL D'ORDINE: SI

Antisimmetrica: SI

$\forall a,b \in \mathbb{Z}\,(a \alpha b \land b \alpha a \Rightarrow a = b)$

$a \le b \land a \equiv_3 b \land b \le a \land b \equiv_3 a \Rightarrow a = b$

è vero perchè $a \le b \land b \le a \iff a = b$

$a = b \Rightarrow a \equiv_3 b \land b \equiv_3 a$

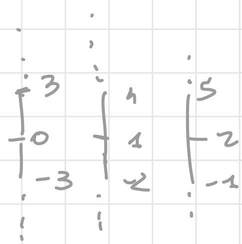
Transitiva: SI

$\forall a,b,c \in \mathbb{Z}\,(a \alpha b \land b \alpha c \Rightarrow a \alpha c)$

perchè se $a \alpha b \land b \alpha c$: $a \le b \le c \land a \equiv_3 b \equiv c$, quindi $a \alpha c$

Massimali $= \emptyset$ max $\nexists$

Minimali $= \emptyset$ min $\nexists$



ii) $\beta: \forall a,b \in \mathbb{N}\,(a \beta b \iff (a \le b \land a \equiv_3 b))$ REL D'ORDINE: SI

Antisimmetria come i)

Transitiva come i)

Massimali $= \emptyset$ max $\nexists$

Minimali $= \{0, 1, 2\}$ min $\nexists$

iii) $\gamma : \forall a,b \in \mathbb{Z} \, (a \gamma b \iff (a \leq b \lor a \equiv_3 b))$ REL D'ORDINE : NO

ASIMMETRIA : NO

$a \gamma b \land b \gamma a \Rightarrow a = b$

$a = 3$ e $b = 0$

$3 \gamma 0 \land 0 \gamma 3 \Rightarrow 3 = 0$, FALSO

$3 \gamma 0$, $3 \equiv_3 0$

$0 \gamma 3$, $0 \equiv_3 3$

Es 5

Il valore più piccolo > 0 di $[b]_7$

$$f(a,b) = \max(a \setminus \mathbb{N}^*) + \min(b \land \mathbb{N}^*)$$

Il valore più grande ≤ 0 di $[a]_7$

	max(...)	min(...)
$\bar{0}$	0	7
$\bar{1}$	-6	1
$\bar{2}$	-5	2
$\bar{3}$	-4	3
$\bar{4}$	-3	4
$\bar{5}$	-2	5
$\bar{6}$	-1	6

i) $\vec{f}(\mathbb{Z}_7 \times \mathbb{Z}_7) = \{ x \in \mathbb{Z} \mid -5 \leq x \leq 7 \}$

ii) Iniettiva : NO

$$\forall (a,b),(c,d) \in \mathbb{Z}_7 \times \mathbb{Z}_7 \, (f(a,b) = f(c,d) \Rightarrow (a,b) = (c,d))$$

$(a,b) = (\bar{1}, \bar{6})$, $(c,d) = (\bar{2}, \bar{5})$

$f(\bar{1}, \bar{6}) = 0$ $\quad f(\bar{2}, \bar{5}) = 0$

Suriettiva : NO

$$\forall y \in \mathbb{Z} \; \exists (a,b) \in \mathbb{Z}_7 \times \mathbb{Z}_7 \, (y = f(a,b))$$

falso: le $y < -5 \wedge y > 7$ non sono immagine di nessun (a,b)

iii) $|(\mathbb{Z}_7 \times \mathbb{Z}_7)/R_f| = |\vec{f}(\mathbb{Z}_7 \times \mathbb{Z}_7)| = 13$

iv) $f(\bar{1},\bar{6}) = 0$

$[(\bar{1},\bar{6})]_{R_f} = \{(\bar{1},\bar{6}),(\bar{2},\bar{5}),(\bar{3},\bar{4}),(\bar{4},\bar{3}),(\bar{5},\bar{2}),(\bar{6},\bar{1})\}$