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

Svolgere i seguenti esercizi,

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

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

Esercizio 1. In ciascuna delle quattro forme proposizionali che seguono, si stabilisca quali tra i connettivi '$\Rightarrow$' e '$\Leftarrow$' (ovvero '$\rightarrow$' e '$\leftarrow$') possono essere sostituiti all'asterisco in modo da ottenere una tautologia (risposte possibili: '$\Rightarrow$', '$\Leftarrow$', 'entrambi', 'nessuno dei due'):
(a) $\big(p\wedge(\neg p)\big)*q$; (b) $q*\big((p\wedge q)\vee q\big)$; (c) $(p\vee q)*\big((p\wedge q)\vee q\big)$; (d) $\big(p \Rightarrow (q\wedge p)\big)*(p \Rightarrow q)$.

Esercizio 2. Siano α, β, γ e δ le relazioni binarie definite in $\mathbb{Z}$ da: $\forall a, b \in \mathbb{Z}$,

$$a\ \alpha\ b \iff 5a+8 \equiv_{15} 5b-7 \qquad a\ \beta\ b \iff 5a+8 \equiv_{15} 8b+5$$
$$a\ \gamma\ b \iff 5a+8 \equiv_{15} 5b-8 \qquad a\ \delta\ b \iff (\forall p \in \mathbb{P})(p|a \Leftrightarrow p|b)$$

dove $\mathbb{P}$ è l'insieme dei numeri primi positivi. Per ciascuna di esse decidere se è o non è di equivalenza e, nel caso lo sia, descrivere la classe di equivalenza di 0.

Esercizio 3. Si consideri la relazione d'ordine ρ definita in $\mathbb{Z}$ ponendo, per ogni $a, b \in \mathbb{Z}$,

$$a\ \rho\ b \iff \big((a \le 0 \le b) \vee (a, b < 0\ \wedge\ a|b) \vee (a, b > 0\ \wedge\ a \le b)\big)$$

(*i*) Determinare gli eventuali minimo, massimo, elementi minimali ed elementi massimali in $(\mathbb{Z}, \rho)$.
(*ii*) $(\mathbb{Z}, \rho)$ è un reticolo?
(*iii*) Posto $A = \{n \in \mathbb{Z} \mid -4 \le n \le 1\}$, disegnare il diagramma di Hasse di (A, ρ), stabilire se (A, ρ) è un reticolo e, nel caso, se è distributivo e se è complementato.

Esercizio 4. Indicando, per ogni $n \in \mathbb{Z}$, con $\bar{n}$ la classe $[n]_{24} \in \mathbb{Z}_{24}$,
(*i*) giustificare, senza fare calcoli, le uguaglianze: $\bar{9}\cdot\overline{16} = \bar{0}$, $(\bar{9})^2 = \bar{9}$ e $(\overline{16})^2 = \overline{16}$. Per farlo utilizzare le uguaglianze $24 = 3\cdot 8$, $9^2 = 9 + 9\cdot 8$ e $16^2 = 16 + 16\cdot 15$.

Sia $*$ l'operazione binaria definita in $\mathbb{Z}_{24}$ da: $\forall a, b \in \mathbb{Z}_{24}$ $(a * b = \overline{16}(a+b) + \bar{9}ab)$.
(*ii*) Stabilire se $*$ è commutativa e, *usando quanto al punto precedente*, se è associativa.
(*iii*) $(\mathbb{Z}_{24}, *)$ ammette elemento neutro? Nel caso, calcolarlo. [*Suggerimento: per quali* $c \in \mathbb{Z}_{24}$ *si ha* $\bar{1} * c = \bar{1}$*?*]
(*iv*) Se la domanda ha senso, di ciascuno di $\bar{0}$ e $\bar{1}$ decidere se è simmetrizzabile in $(\mathbb{Z}_{24}, *)$ e, nel caso, determinarne il simmetrico.

Esercizio 5. Per ogni intero primo positivo p, sia f_p il polinomio $x^2(\bar{3}x-\bar{1})(x^2-\bar{1})-\bar{2}x^3+\bar{2}x+\overline{21} \in \mathbb{Z}_p[x]$.
(*i*) Determinare l'insieme A degli interi primi positivi p per i quali f_p abbia sia $\bar{1}$ che $-\bar{1}$ come radice.
(*ii*) Detto q il massimo elemento di A, si scriva f_q come prodotto di polinomi irriducibili in $\mathbb{Z}_q[x]$.

ES 1

i) $(p \land \neg p) \; ? \; q$ $\qquad \Rightarrow$

ii) $q \; ? \; ((p \land q) \lor q)$ $\qquad$ entrambi

q	$p \land q$	$(p \land q) \lor q$
V	V	V
F	F	F
V	F	V
F	F	F

iii) $(p \lor q) \; ? \; ((p \land q) \lor q)$ $\qquad \Leftarrow$

$p \lor q$	$(p \land q) \lor q$
V	V
V	F
V	V
F	F

iv) $(p \Rightarrow (q \land p)) \; ? \; (p \Rightarrow q)$ $\qquad$ entrambi

$p \Rightarrow (q \land p)$	$p \Rightarrow q$
V	V
F	F
V	V
V	V

ES 2

α: $5a + 8 \equiv_{15} 5b - 7 \Rightarrow 5a + 8 \equiv_{15} 5b + 8 \Rightarrow a \equiv_{15} b$

SIMMETRIA

$a \,\alpha\, b \Rightarrow b \,\alpha\, a$

$a \equiv_{15} b \Rightarrow b \equiv_{15} a$ vero

TRANSITIVITÀ

$a \,\alpha\, b \wedge b \,\alpha\, c \Rightarrow a \,\alpha\, c$

$a \equiv_{15} b \wedge b \equiv_{15} c \Rightarrow a \equiv_{15} c$ vero

SIMMETRIA

$a \,\alpha\, a$ $\quad a \equiv_{15} a$ vero

C.E $[0]_{15}$

β: $5a + 8 \equiv_{15} 8b + 5$

RIFLESSIVA NO

$x \not\beta\, x$

$x = 3 \quad 5x + 8 \equiv_{15} 8x + 5$

$\overline{8} \equiv_{15} \overline{14}$

$r: 5a+8 \equiv_{15} 5b-8 \Rightarrow 5a+8 \equiv_{15} 5b+7$

RIFLESSIVA NO

$a=3$

$5a+8 \equiv_{15} 5a-8$ $\qquad 5\cdot 3+8 \equiv_{15} 5\cdot 3-8$

$\overline{8} \qquad \overline{7}$

$s: \forall p \in \mathbb{P}\ (p \mid a \Leftrightarrow p \mid b)$

nessun numero è divisibile per tutti primi, tranne 0.
ogni numero è in relazione con tutti i numeri tranne che con 0, e 0 è in rel solo con se stesso

Riflessiva

$a\ s\ a$ = vero

Transitiva

$a\ s\ b \wedge b\ s\ c \Rightarrow a\ s\ c$ vero

Simmetria

$a\ s\ b \Rightarrow b\ s\ a$ vero

$[0]_s = \{0\}$

ES 3

1) $a \leq 0 \leq b \Rightarrow \forall a \in \mathbb{Z}^- \cup \{0\}\ \forall b \in \mathbb{Z}^+ \cup \{0\}\ (a \rho b)$

2) $a, b < 0 \wedge a | b \Rightarrow \forall b \in \mathbb{Z}^-\ \exists a \in \mathbb{Z}^-\ (a \rho b \Leftrightarrow a | b)$

3) $0 < a \leq b \Rightarrow \forall a \in \mathbb{Z}^+\ \exists b \in \mathbb{Z}^+\ (a \rho b)$

i) minimali $= \{-1\}$, massimali $= \emptyset$
minimo $= -1$

ii) RETICOLO: RELAZIONE DI ORDINE LARGO: SI

ANTISIMMETRICA $a \rho b \wedge b \rho a \Rightarrow a = b$: Si

1) tutti i negativi sono in rel con tutti i positivi, ma non viceversa

2) i negativi se sono in rel $a \rho b$, $a | b$, e $b | a$ oltre per forza essere $a = b$

3) i positivi son in rel $\geq$ tra loro, e $a \rho b$ e $b \rho a$ è vero solo se $a = b$

TRANSITIVA $a \rho b \wedge b \rho c \Rightarrow a \rho c$: SI

- a è positivo e b è in rel con a, b è positivo, c è positivo, per lo stesso motivo e allora $a \rho c$. (3)

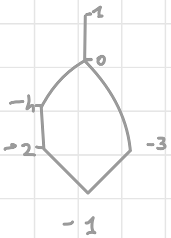
- a è negativo e b è positivo,(1) c è positivo(3), allora a è in rel. con c (1)

- a è negativo e b è negativo, e $a \rho b$,(2) $a | b$:
  - c positivo, allora $a \rho c$ è vero. (1)
  - c negativo, allora $a \rho c$ è vero. (2)

RIFLESSIVA: $a \rho a$: SI

- I positivi sono in rel con se stessi per la 3
- I negativi sono in rel con se stessi per la 2
- 0 è in rel con se stesso per la 1

iii) $A = \{-4, -3, -2, -1, 0, 1\}$



min $= -1$, max $= 1$

Complementato: NO

$\forall x, y \in A \left(x \wedge_\rho y = 1 \wedge x \wedge_\rho y = -1 \right)$

Distributiva: NO

$a \wedge_\rho (b \wedge_\rho c) = (a \wedge_\rho b) \wedge_\rho (b \wedge_\rho c)$

Es 4

$\overline{0} = \overline{24} = \overline{3} \cdot \overline{8}$

i) $\overline{9} \cdot \overline{16} \equiv_{24} \overline{0}$

$9 \cdot 16$ è multiplo di $\overline{3} \cdot \overline{8}$, allora $\overline{9} \cdot \overline{16} \mid \overline{24}$, quindi $\overline{9} \cdot \overline{16} = \overline{0}$

$(\overline{9})^2 = 9$ $\qquad \overline{9} \cdot \overline{8} \mid \overline{3} \cdot \overline{8}$, quindi è 0

$(\overline{9})^2 = \overline{9} + \overline{9} \cdot \overline{8} = 9$

$(\overline{16})^2 = 16$

$(\overline{16})^2 = \overline{16} + \overline{16} \cdot \overline{15} = 16$ $\qquad \overline{16} \cdot \overline{15} \mid \overline{8} \cdot \overline{3}$, quindi 0

$\forall a, b \in \mathbb{Z}_{24} \left(a * b = \overline{16}(a+b) + \overline{9}\, ab \right)$

ii) COMMUTATIVA: SI

perché $\cdot$ e $+$ sono commutative

ASSOCIATIVA: SI

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

$(a * b) * c = 16(16a + 16b + 9ab) + 16c + 9(16ac + 16bc + 9abc)$

$16a + 16b + 16c + 9abc$

$(b * c) * a = 16(16b + 16c + 9bc) + 16a + 9(16ab + 16ac + 9abc$

$16a + 16b + 16c + 9abc$

iii) NEUTRO : 9

$$a * c = a$$

$$16(1+c) + 9 \cdot 1 \cdot c = 1$$
$$16 + 16c + 9c = 1$$
$$25c = 1 - 16 = -15 = 9 \implies c = 9$$

$$16(a+9) + 9a \cdot 9 = a$$
$$16a + 9a = a \implies 25a = a$$

iv)

$$a * s = 9$$

$$a = 0$$

$$0 * s = 9$$
$$16 \cdot 0 + 16s + 9 \cdot 0 \cdot s = 9$$
$$16s \equiv_{24} 9$$

$MCD(16, 24) = 4$ $\quad \neg(4 \mid 9)$, non ammette risultati

$$a = 1$$

$$1 * a = 9$$
$$16 + 16s + 9s = 9$$
$$25s = 9 - 16$$
$$s \equiv_{24} 17$$

$$16 + 16 \cdot 17 + 9 \cdot 17 = 9$$
$$16 + 8 + 9 = 9$$
$$24 + 9 = 9 \implies 9 = 9$$

TROVARE RADICE SOSTITUISCO IN 0

1 è radice di 3 $\quad 3 \in A$

-1 è radice di 3

radice

$-(1)$

$7 \in A$

$$\begin{array}{l|l} 2x^3 + 0x^2 + 2x + 0 & x-1 \\ \hline -2x^3 + 2x^2 \quad + 0 + 0 & 2x^2 - 2x \\ // \quad -2x^2 \quad -2x + 0 & \end{array}$$

ii) q il max di A = 7

rag in mod 7

$-(-1)$

$$x^2(3x-1)(x^2-1) - 2x^3 + 2x + 21$$

$$\begin{array}{l|l} 2x^2 - 2x + 0 & x+1 \\ \hline -2x^2 \quad -2x & 2x \end{array}$$

$$x^2(3x-1)(x-1)(x+1) - (2x^2-2x)(x-1)$$

$$x^2(3x-1)(x-1)(x+1) - 2x(x+1)(x-1)$$