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

Svolgere i seguenti esercizi,

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

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

Esercizio 1. Le formule $A\colon \exists x(\forall y(\theta(x,y)))$ e $B\colon \forall y(\exists x(\theta(x,y)))$ sono (per un arbitrario predicato binario θ) tra loro equivalenti?

Esercizio 2. Definire le nozioni di applicazione, applicazione iniettiva, applicazione suriettiva da un insieme a ad un insieme b. Assumendo $|a| = 25$ e $|b| = 32$, indicare quante sono le applicazioni da a a b, quante tra queste sono iniettive e quante suriettive. (Per cortesia, non cercare di calcolare questi numeri.)

Esercizio 3. Sia ρ la relazione binaria definita in $\mathbb{Z}$ da $\forall a, b \in \mathbb{Z}(a \;\rho\; b \iff a + b \equiv_4 1)$. Stabilire se ρ è la relazione di adiacenza di un grafo (semplice) su $\mathbb{Z}$ e, nel caso lo sia, quante componenti connesse ha questo grafo e se esso è una foresta.

Esercizio 4. Siano $\oplus$ e $*$ le operazioni binarie definite in $\mathbb{Z}_{100}$ da: $\forall a, b \in \mathbb{Z}_{100}$,

$$a \oplus b = a + b - \bar{25} \qquad \text{e} \qquad a * b = \bar{7}ab + \bar{25}(a + b).$$

- (i) Dare la definizione di anello e, dando per noto che $*$ è associativa, verificare che $(\mathbb{Z}_{100}, \oplus, *)$ è un anello commutativo.
- (ii) Determinare tutti gli $a \in \mathbb{Z}_{100}$ tali che $a * \bar{4} = \bar{4}$; usando questa informazione decidere poi se $(\mathbb{Z}_{100}, \oplus, *)$ è un anello unitario specificando, nel caso, la sua unità.
- (iii) Di ciascuno degli elementi $\bar{0}$, $\bar{1}$, $\bar{2}$ di $\mathbb{Z}_{100}$ decidere se in questo anello è o non è invertibile, idempotente, cancellabile, un divisore dello zero.

Esercizio 5.

- (i) Siano α e β le relazioni binarie definite in $\mathcal{P}(\mathbb{Z})$ da: $\forall x, y \in \mathcal{P}(\mathbb{Z})$

$$(x \;\alpha\; y \iff x \cup y \in \mathcal{P}(\mathbb{N})) \qquad \wedge \qquad (x \;\beta\; y \iff x \bigtriangleup y \in \mathcal{P}(\mathbb{N})).$$

  Decidere quali tra α e β sono di equivalenza e, rispetto a quelle che lo sono, descrivere esplicitamente la classe di equivalenza di $\{2, 15, 87\}$, stabilendo anche se questa classe è finita o infinita.
- (ii) Siano γ e δ le relazioni binarie definite in $\mathbb{Q}$ da: $\forall x, y \in \mathbb{Q}$

$$(x \;\gamma\; y \iff x - y \in \mathbb{N}) \qquad \wedge \qquad (x \;\delta\; y \iff x + y \in \mathbb{N}).$$

  Decidere quali tra γ e δ sono di relazioni d'ordine e, rispetto a quelle che lo sono, determinare l'insieme dei minoranti di $\{0, 1/2\}$, gli eventuali elementi massimali, minimali, minimo, massimo dell'insieme ordinato descritto da questa relazione in $\mathbb{Q}$ ed infine se questo insieme ordinato è un reticolo.

Esercizio 6. Vero o falso (e perché)?

- (i) Per ogni parte finita T di $\mathbb{Q}$ esiste un polinomio $f \in \mathbb{Q}[x]$ tale che gli elementi di T siano tutte e sole le radici di f.
- (ii) Detto F l'insieme delle parti finite di $\mathbb{Q}$, l'applicazione $h\colon \mathbb{Q}[x] \smallsetminus \{0\} \to F$ che ad ogni $f \in \mathbb{Q}[x] \smallsetminus \{0\}$ associa l'insieme delle radici di f è suriettiva.
- (iii) L'applicazione h definita al punto precedente è iniettiva.
- (iv) Detto ancora F l'insieme delle parti finite di $\mathbb{Q}$, è ben definita l'applicazione $k\colon \mathbb{Q}[x] \to F$ che ad ogni $f \in \mathbb{Q}[x]$ associa l'insieme delle radici di f.
- (v) Ogni polinomio di grado dispari in $\mathbb{R}[x]$ ha radici in $\mathbb{R}$.
- (vi) Ogni polinomio in $\mathbb{R}[x]$ che sia privo di radici in $\mathbb{R}$ è irriducibile in $\mathbb{R}[x]$.
- (vii) Ogni polinomio irriducibile in $\mathbb{R}[x]$ è privo di radici in $\mathbb{R}$.

Infine:

- $(viii)$ Quali sono gli elementi di $A := \{n \in \mathbb{N} \mid \text{esiste un polinomio irriducibile di grado } n \text{ in } \mathbb{R}[x]\}$ e quali quelli di $B := \{n \in \mathbb{N} \mid \text{esiste un polinomio irriducibile di grado } n \text{ in } \mathbb{Q}[x]\}$?
- (ix) Per definizione, cosa è un polinomio irriducibile?

FEB-24 ES 1

Esercizio 1. Le formule $A\colon \exists x(\forall y(\theta(x, y)))$ e $B\colon \forall y(\exists x(\theta(x, y)))$ sono (per un arbitrario predicato binario θ) tra loro equivalenti?

No perchè

A dice che esiste almeno una x che per ogni y per cui vale θ

B dice che per ogni y esiste almeno una x per cui vale θ

FEB-24 ES2

Esercizio 2. Definire le nozioni di applicazione, applicazione iniettiva, applicazione suriettiva da un insieme a ad un insieme b. Assumendo $|a| = 25$ e $|b| = 32$, indicare quante sono le applicazioni da a a b, quante tra queste sono iniettive e quante suriettive. (Per cortesia, non cercare di calcolare questi numeri.)

APPLICAZIONI TOTALI:

$$|b|^{|a|}$$

INIETTIVE:

$$MAP(a,b) = \frac{|b|!}{(|b|-|a|)!}$$

SURIETTIVE:

$|b| > |a|$, non esistono

FEB-24 ES 3

Esercizio 3. Sia ρ la relazione binaria definita in $\mathbb{Z}$ da $\forall a, b \in \mathbb{Z}(a \rho b \iff a + b \equiv_4 1)$. Stabilire se ρ è la relazione di adiacenza di un grafo (semplice) su $\mathbb{Z}$ e, nel caso lo sia, quante componenti connesse ha questo grafo e se esso è una foresta.

GRAFO? SI

SIMMETRICA: SI

$a \rho b = b \rho a$ sì, perchè + è commutativo

ANTIRIFLESSIVA: SI

$\forall a \, (a \rho a)$

$a + a \equiv_4 1 \Rightarrow 2a \equiv_4 1$

$4 \mid a-1 \Rightarrow 4 \mid 1$ FALSO

COMPONENTI CONNESSE: 2

1 — 5   2 — 6
| /
8

FORESTA: NO

CI SONO CIRCUITI

FEB - 24
ES 4

Esercizio 4. Siano $\oplus$ e $*$ le operazioni binarie definite in $\mathbb{Z}_{100}$ da: $\forall a, b \in \mathbb{Z}_{100}$,

$$a \oplus b = a + b - \overline{25} \qquad \text{e} \qquad a * b = \overline{7}ab + \overline{25}(a+b).$$

(*i*) Dare la definizione di anello e, dando per noto che $*$ è associativa, verificare che $(\mathbb{Z}_{100}, \oplus, *)$ è un anello commutativo.

(*ii*) Determinare tutti gli $a \in \mathbb{Z}_{100}$ tali che $a * \overline{4} = \overline{4}$; usando questa informazione decidere poi se $(\mathbb{Z}_{100}, \oplus, *)$ è un anello unitario specificando, nel caso, la sua unità.

(*iii*) Di ciascuno degli elementi $\overline{0}$, $\overline{1}$, $\overline{2}$ di $\mathbb{Z}_{100}$ decidere se in questo anello è o non è invertibile, idempotente, cancellabile, un divisore dello zero.

i) ANELLO : $\oplus$: G. A $\quad$ $*$: Semigruppo

$*$ commutativo: SI perchè + e · sono commutativi

ii) $\overline{7} \cdot \overline{4} \cdot a + \overline{25}(a + \overline{4}) \Rightarrow \overline{28}a + \overline{25}a \equiv \overline{4} \Rightarrow \overline{53}\, a \equiv_{100} \overline{4}$

ALGORITMO EUCLIDEO

$100 = 53 \cdot 1 + 47$

$53 = 47 \cdot 1 + 6$

$47 = 6 \cdot 7 + 5$

$6 = 5 \cdot 1 + 1$

$\overline{1}\, a \equiv_{100} \overline{4} \cdot \overline{17}$

$a \equiv_{100} \overline{68}$

↳ possibile neutro

ESTESO

$1 = 6 + 5(-1)$

$6 + 47 \cdot (-1) + 6 \cdot 7 \Rightarrow 47 \cdot (-1) + 6 \cdot (8)$

$47 \cdot (-1) + 53(8) + 47 \cdot (-8) \Rightarrow 53(8) + 47(-9)$

$100 \cdot (-9) + 53(9) + 53(8) \Rightarrow 100(-9)$

$53(17) + 100(-9)$

NEUTRO 68

$\overline{7} \cdot \overline{68} \cdot x + \overline{25}(\overline{68} + x) = x$

$\overline{476} \cdot x + \overline{1700} + \overline{25}x = x$

$\overline{501}\, x = x \Rightarrow x = x$

FEB-24 ES 5

Esercizio 5.

(*i*) Siano α e β le relazioni binarie definite in $\mathcal{P}(\mathbb{Z})$ da: $\forall x, y \in \mathcal{P}(\mathbb{Z})$

$$(x \; \alpha \; y \iff x \cup y \in \mathcal{P}(\mathbb{N})) \qquad \wedge \qquad (x \; \beta \; y \iff x \triangle y \in \mathcal{P}(\mathbb{N})).$$

Decidere quali tra α e β sono di equivalenza e, rispetto a quelle che lo sono, descrivere esplicitamente la classe di equivalenza di $\{2, 15, 87\}$, stabilendo anche se questa classe è finita o infinita.

(*ii*) Siano γ e δ le relazioni binarie definite in $\mathbb{Q}$ da: $\forall x, y \in \mathbb{Q}$

$$(x \; \gamma \; y \iff x - y \in \mathbb{N}) \qquad \wedge \qquad (x \; \delta \; y \iff x + y \in \mathbb{N}).$$

Decidere quali tra γ e δ sono di relazioni d'ordine e, rispetto a quelle che lo sono, determinare l'insieme dei minoranti di $\{0, 1/2\}$, gli eventuali elementi massimali, minimali, minimo, massimo dell'insieme ordinato descritto da questa relazione in $\mathbb{Q}$ ed infine se questo insieme ordinato è un reticolo.

i) REL. EQUIVALENZA: SOLO β

SIMMETRICA: ENTRAMBE

α: $x \alpha y = y \alpha x$, VERO, unione è commutativa

β: $\forall x,y \in P(\mathbb{Z}) (x \Delta y = y \Delta x)$, VERO, Δ è commutativa

TRANSITIVA: ENTRAMBE

α: $x \alpha y \wedge y \alpha z \Rightarrow x \alpha z$

è VERO perché per essere in relazione, nessuno dei due elementi deve contenere numeri negativi

β: $x \beta y \wedge y \beta z \Rightarrow x \beta z$

è VERO perché due num. per essere in relazione se hanno elementi negativi devono essere gli stessi

RIFLESSIVA: SOLO β

α: $x \alpha x$ è FALSO se x ha numeri negativi non è in rel con se stesso

β: $x \beta x$ è VERO il risultato è $\emptyset$ che appartiene a $P(\mathbb{N})$

CLASSE EQ. $\{2, 15, 87\}$

$P(\mathbb{N}) \setminus \{2, 15, 87\}$ è la c.E., ed è infinita

ii) REL. D'ORDINE γ è DI ORDINE LARGO

ANTISIMMETRIA SOLO γ

$x+y \in \mathbb{N}$ $\quad$ $y+x \in \mathbb{N}$

δ: FALSO $\quad$ + è commutativo

γ: VERO $\quad$ − non è commutativo $\quad$ $x-y \in \mathbb{N}$ $\quad$ $y-x \in \mathbb{N}$

TRANSITIVITÀ SOLO γ

γ: $\forall x,y,z\ (x\gamma y \wedge y\gamma z \Rightarrow x\gamma z)$

è VERO perchè − è transitivo

RIFLESSIVITÀ SOLO γ

γ: VERO $\quad x\gamma x \Rightarrow x-x \in \mathbb{N} \quad 0 \in \mathbb{N}$

MINORANTI $T=\{0, \frac{1}{2}\}$ NESSUNO

$m \in \mathbb{Q}$

$\forall a \in T\ (a\gamma m \Longleftrightarrow a-m \in \mathbb{N})$, nessun elemento.

MASSIMALE NON C'È

$M \in \mathbb{Q}$

$\forall a \in \mathbb{Q}\ ((a\gamma M \vee M\gamma a) \Rightarrow a\gamma M)$

$((a-M \in \mathbb{N} \vee M-a \in \mathbb{N}) \Rightarrow a-M \in \mathbb{N})$

MINIMALE NON C'È

$m \in \mathbb{Q}$

$\forall a \in \mathbb{Q}\ ((a\gamma m \vee m\gamma a) \Rightarrow a\gamma m)$

$((a-m \in \mathbb{N} \vee m-a \in \mathbb{N}) \Rightarrow m-a \in \mathbb{N})$

MINIMO e MASSIMO NON CI SONO

RETICOLO NO

Nonostante sia antisimmetrica, transitiva e riflessiva, non ha sup ed inf

$\square$