TRACCIA - 15 FEBBRAIO 2024

Esercizio 1

$A \Rightarrow B$?
Sì. Se esiste un solo x che vale per tutti gli y, allora sicuramente per ogni y esiste un y t.c. $(\vartheta(x,y))$.

$B \Rightarrow A$?
No, perchè se per ogni y esiste una x t.c. $\vartheta(x,y)$, non è detto che esista una x che vada bene per tutte le y.

Esercizio 2

$f \in Corr(A,B)$ è un'applicazione se e solo se:

$$\forall x \in A (\exists! y \in B (f(x) = y))$$

$f: A \to B$ è iniettiva se $\forall x, y \in A (x \neq y \Rightarrow f(x) \neq f(y))$ oppure se $\forall x, y \in A (f(x) = f(y) \Rightarrow x = y)$.

$f: A \to B$ è suriettiva se e solo se $im(f) = B$.

Il numero di applicazioni da A a B è dato da $|B|^{|A|}$.

Le applicazioni iniettive saranno: $\dfrac{|B|!}{(|B|-|A|)!}$

Non ci sono funzioni suriettive in quanto $|A| < |B|$.

Esercizio 4

(i)

Un anello è una struttura algebrica del tipo $(\mathbb{Z}_{100}, \oplus, *)$ tale che:
- $(\mathbb{Z}_{100}, \oplus)$ è un gruppo abeliano
- $(\mathbb{Z}_{100}, *)$ è un semigruppo
- $*$ è distributiva rispetto a $\oplus$

$(\mathbb{Z}_{100}, \oplus, *)$ è commutativo se $*$ è commutativa, ovvero se per ogni $a,b \in \mathbb{Z}_{100}$: $a * b = b * a$.

$a * b = \overline{7}ab + 25(a+b)$

$b * a = \overline{7}ba + 25(b+a)$

Coincidono in quanto le operazioni definite moltiplicativamente e additivamente sono commutative.

(ii)

$a * 4 = \overline{7}a\overline{4} + \overline{25}(a+\overline{4}) = \overline{4} \iff$

$\overline{7}a\overline{4} + \overline{25}(a+\overline{4}) \equiv_{100} \overline{4} \iff \overline{28}a + \overline{25}a + \overline{100} \equiv_{100} 4 \iff$

$\iff \overline{53}a \equiv_{100} \overline{4}$

Dobbiamo risolvere l'equazione congruenziale ottenuta. Ha soluzione se e solo se $MCD(53, 100) / \overline{8}$. Vero dato che $\overline{53}$ e 100 sono coprimi. Usiamo l'algoritmo Euclideo per trovare l'inverso moltiplicativo di $\overline{53}$.

$100 = (1)\overline{53} + 47 \Rightarrow 47 = (1)100 + (-1)53$

$\overline{53} = (1)47 + 6 \Rightarrow 6 = (1)53 + (-1)47$

$47 = (7)6 + 5 \Rightarrow 5 = (1)47 + (-7)6$

$6 = (1)5 + 1 \Rightarrow 1 = (1)6 + (-1)5$

$5 = (5)1 + 0$

$1 = (1)53 + (-1)47 + (-1)47 + (7)6 =$

$= (1)53 + (-2)47 + (7)53 + (-7)47 = (8)53 + (-9)47 =$

$= (8)53 + (-9)100 + (9)53 = (17)53 + (-9)100$

Moltiplichiamo $\overline{17}$ per ambo i membri dell'equazione e otteniamo: $a \equiv_{100} \overline{68}$

Da questo possiamo intuire che $\overline{68}$ può essere l'elemento neutro a sinistra. Verifichiamolo:

$\overline{68} * a = a \iff \overline{7}\cdot\overline{68}\cdot a + \overline{25}(\overline{68}+a) \equiv_{100} a$

$\iff \overline{76}a + a \equiv_{100} a$

$\iff \overline{76}a \equiv_{100} 0 \neq a \Rightarrow$ non è un anello unitario.

(iii)

Dato che l'anello non è unitario, possiamo dire che nessuno dei tre è invertibile.

$\overline{0}$ è idempotente $\iff 0 * 0 = 0$.

$0 * 0 = 0 + 0 = 0$ ✓

$\overline{1}$ è idempotente $\iff \overline{1} * \overline{1} = 1$

$\overline{1} * \overline{1} = \overline{7} + \overline{50} = \overline{57} \neq 1$ ✗

$\overline{2}$ è idempotente $\iff \overline{2} * \overline{2} = \overline{2}$

$\overline{2} * \overline{2} = \overline{28} + \overline{0} = \overline{28} \neq 2$ ✗

$\bar{0}$ è cancellabile $\underbrace{}_{}$ a sx $\iff \forall a,b \in (0 * a = 0 * b \Rightarrow a = b)$

$0 * a = \bar{0} + \overline{25}a = \overline{25}a$

$0 * b = \overline{25}b$

$\overline{25}a = \overline{25}b \Rightarrow a = b$ ✓

Vale anche a destra, quindi 0 è cancellabile.

$\bar{1}$ è cancellabile a sinistra $\iff \forall a,b \in \mathbb{Z}_{100} (1 * a = 1 * b \Rightarrow a = b)$

$1 * a = \bar{7}a + \overline{25} + \overline{25}a = \overline{32}a + \overline{25}$

$1 * b = \overline{32}b + \overline{25}$

$\overline{32}a + \overline{25} = \overline{32}b + \overline{25} \iff \overline{32}a = \overline{32}b \Rightarrow a = b$ ✓

Vale anche a destra, quindi 1 è cancellabile.

2 è cancellabile a sinistra $\iff \forall a,b \in \mathbb{Z}_{100} (2 * a = 2 * b \Rightarrow a = b)$

$2 * a = \overline{14}a + \overline{50} + \overline{25}a = \overline{39}a + \overline{50}$

$2 * b = \overline{39}b + \overline{50}$

$\overline{39}a + 50 = \overline{39}b + 50 \iff \overline{39}a = \overline{39}b \Rightarrow a = b$ ✓

$\bar{0}$ non può essere un divisore dello zero in quanto, per definizione, dovrebbe essere diverso da se stesso.

$\bar{1}$ è un divisore dello zero se $\forall x \in \mathbb{Z}_{100} \setminus \{0\} (\bar{1} * x = x * \bar{1} = 0)$

$\bar{1} * x = \bar{0} \iff \bar{7}x + \overline{25}x + \overline{25} \equiv_{100} 0$

$\iff \overline{32}x + \overline{25} \equiv_{100} 0 \iff \overline{32}x \equiv_{100} 75$

L'equazione ha soluzione $\iff MCD(32, 100) / 75$. Non è così quindi $\bar{1}$ non è un divisore dello zero.

Facciamo il ragionamento analogo per 2:

$\bar{2} * x = \bar{0} \iff \overline{14}x + \overline{50} + \overline{25}x \equiv_{100} 0$

$\iff \overline{39}x \equiv_{100} \overline{50}$

Usiamo l'algoritmo euclideo per trovare l'inverso moltiplicativo di $\overline{39}$.

$100 = (2)39 + 22 \Rightarrow 22 = (1)100 + (-2)39$ $\quad 5 = (2)2 + 1 \Rightarrow 1 = (1)5 + (-2)2$

$39 = (1)22 + 17 \Rightarrow 17 = (1)39 + (-1)22$ $\quad 2 = (2)1 + 0$

$22 = (1)17 + 5 \Rightarrow 5 = (1)22 + (-1)17$

$17 = (3)5 + 2 \Rightarrow 2 = (1)17 + (-3)5$

$1 = (1)5 + (-2)2 = (1)22 + (-1)17 + (-2)17 + (6)5 =$

$= (1)100 + (-2)39 + (-3)17 + (6)22 + (-6)17 =$

$= (1)100 + (-2)39 + (-9)17 + (6)22 = (1)100 + (-2)39 + (-9)39 + (9)22 + (6)22 =$

$= (1)100 + (-11)39 + (15)22 = (1)100 + (-11)39 + (15)100 + (-30)39 =$

$= (16)100 + (-41)39$

Otteniamo $-\overline{41} = \overline{59}$. Moltiplichiamo ambo i membri per $\overline{89}$ e otteniamo:

$x \equiv_{100} 0$. Dunque non è un divisore dello zero.

Esercizio 5

(i)

Una relazione binaria è di equivalenza se è: riflessiva, simmetrica e transitiva. Verifichiamo queste proprietà per α e β.

- Riflessività: $\forall x \in P(\mathbb{Z}) \, (x \, \alpha \, x)$

$x \, \alpha \, x \iff x \cup x \in P(\mathbb{N}) \iff x \in P(\mathbb{N})$.

Non vale per ogni $x \in P(\mathbb{Z})$, dunque α non è una relazione di equivalenza. Passiamo a β e verifichiamo la riflessività:

$\forall x \in P(\mathbb{Z}) \, (x \beta x)$

$x \beta x \iff x \Delta x \in P(\mathbb{N})$ il che è vero in quanto $x \Delta x = \emptyset \in P(\mathbb{N})$.

- Simmetria: $\forall x, y \in P(\mathbb{N}) \, (x \beta y \Rightarrow y \beta x)$

$x \beta y \iff x \Delta y \in P(\mathbb{N})$. Supponiamo sia vero. $x \Delta y \iff (x \setminus y) \cup (y \setminus x)$
Dato che l'operazione di unione è commutativa, equivale a $(y \setminus x) \cup (x \setminus y) \iff y \beta x$. Dunque è simmetrica.

- Transitività: $\forall x, y, z \in P(\mathbb{Z}) \, ((x \beta y \wedge y \beta z) \Rightarrow x \beta z)$

$x \beta y \iff x \Delta y \in P(\mathbb{N})$

$y \beta z \iff y \Delta z \in P(\mathbb{N})$

In generale non vale sempre, quindi anche β non è una relazione d'equivalenza.

(ii)

Una relazione binaria è d'ordine se è riflessiva, antisimmetrica e transitiva.

- γ è riflessiva se $\forall x \in \mathbb{Q} \, (x \gamma x)$

$x \gamma x \iff x - x = 0 \in \mathbb{N}$ ✓

- δ è riflessiva se $\forall x \in \mathbb{Q} \, (x \delta x)$

$x \delta x \iff x + x \in \mathbb{N}$ ma non è sempre vero $(-2 + (-5) = -7 \notin \mathbb{N})$.

Quindi sicuramente δ non è una relazione d'ordine.

- γ è antisimmetrica se $\forall x, y \in \mathbb{Q} \; (x \gamma y \wedge y \gamma x \Rightarrow x = y)$

$$\left.\begin{array}{l} x \gamma y \iff x - y \in \mathbb{N} \\ y \gamma x \iff y - x \in \mathbb{N} \end{array}\right\} \text{Se valgono entrambe allora sicuramente i due sono uguali.}$$

- γ è transitiva se $\forall x, y, z \in \mathbb{Q} \; ((x \gamma y \wedge y \gamma z) = x \gamma z)$

$$\left.\begin{array}{l} x \gamma y \iff x - y \in \mathbb{N} \\ y \gamma z \iff y - z \in \mathbb{N} \end{array}\right\} \text{Non sempre è vero}$$

Dunque, anche δ non è una relazione d'ordine.

Esercizio 6

(i)

VERO: Dato un insieme $T = \{q_1, q_2, \dots, q_n\} \subseteq \mathbb{Q}$, possiamo costruire esplicitamente un polinomio in $\mathbb{Q}[x]$ che ha esattamente queste radici, ad esempio:

$$f(x) = \prod_{i=1}^{n} (x - q_i).$$

Questo polinomio ha coefficienti razionali, ed è di grado n. Inoltre non ha radici diverse da quelle, perché i fattori lineari sono tutti e soli quelli associati a T.

(ii)

VERO: discorso fatto per il punto 1.

(iii)

FALSO: polinomi non nulli distinti possono avere le stesse radici

(iv)

FALSO: il problema nasce dal fatto che l'applicazione considera anche il polinomio nullo, che ha come radici tutto $\mathbb{Q}$. Quest'ultimo è infinito, ma l'applicazione ha come codominio un insieme finito. Dunque $\mathbb{Q}$ non appartiene ad $F \Rightarrow K$ non è ben definita.

(v)

VERO: in quanto le radici o restano negative (o positive) o diventano positive. Non è vero se il polinomio avesse grado pari. (es. x^2+1 non ha radici).

(vi)

FALSO: non è detto che sia irriducibile in $\mathbb{R}$. Ad esempio $x^4 + 5x^2 + 4$ non ha radici ma si può ridurre a $(x^2+1)(x^2+4)$.

(vii)

Vero.

(viii)

$A = \{1, 2\}$ $B = \{1, 2, 3, \dots\}$

(ix)

Sia $\mathbb{K}$ un campo e $f \in \mathbb{K}[x]$. Sia $n = gr(f)$. Allora f è irriducibile in $\mathbb{K}[x]$ se e solo se $n > 0$ e vale una delle due:
1) $\exists\, g, h \in \mathbb{K}[x]$ t.c. $(f = g \cdot h \Rightarrow gr(g) = n \oplus gr(h) = n)$
2) $\exists\, g, h \in \mathbb{K}[x]$ t.c. $(f = g \cdot h \Rightarrow gr(g) = 0 \oplus gr(h) = 0)$.