TRACCIA – 16 MARZO 2024

Esercizio 1

Facendo le tabelle di verità, si vede che è una tautologia.

Esercizio 2

(i)

f è suriettiva in quanto $im(f) = \mathbb{Z}$.

f non è iniettiva in quanto esistono elementi del dominio che hanno la stessa immagine. Ad esempio: $f((0,30)) = 30 = f((1,0))$.

(ii)

$[f(a,b)]_{45}$ è invertibile $\iff$ $f(a,b)$ e 45 sono coprimi.

$45 = 3^2 \cdot 5$. Quindi ci basta prendere valori in T che sono coprimi con 45 (non si dividono per 3 e 5). Quindi:

$S = \{(a,b) \,/\, a \in \mathbb{N} \wedge b \in \{61, 62, 64, 67, 68\}\}$

(iii)

Scelgo $a = 0$ e $b = 61$. $f(a,b) = f(0,61) = 61$.

$[61]_{45} = [16]_{45}$.

Troviamo una $x \in \mathbb{Z}_{45}$ t.c. $16x \equiv_{45} 1$. Usiamo l'algoritmo Euclideo:

$45 = (2)16 + 13 \Rightarrow 13 = (1)45 + (-2)16$

$16 = (1)13 + 3 \Rightarrow 3 = (1)16 + (-1)13$

$13 = (4)3 + 1 \Rightarrow 1 = (1)13 + (-4)3$

$3 = (3)1 + 0$

Sostituiamo:

$1 = (1)13 + (-4)3 = (1)45 + (-2)16 + (-4)16 + (4)13 =$

$= (1)45 + (-6)16 + (4)13 = (1)45 + (-6)16 + (4)45 + (-8)16 =$

$= (5)45 + (-14)16$

$\overline{-14} \equiv_{45} \overline{31}$.

Moltiplichiamo ambo i membri dell'equazione per $\overline{31}$:

$x \equiv_{45} 31$.

Esercizio 3

(i)

$|R| = |\mathbb{Z}_4| \times |\mathbb{Z}_6| = 4 \cdot 6 = 24$

(ii)

$0_R = (0,0)$. Infatti: $\forall (x,y) \in R \, ((x,y) + (0,0) = (x+0, y+0) = (x,y))$.
Vale anche a destra.

$1_R = (1,1)$. Infatti: $\forall (x,y) \in R \, ((x,y)(1,1) = (x \cdot 1, y \cdot 1) = (x,y))$.
Vale anche a destra.

$(x,y) \in R$ è invertibile $\Leftrightarrow \exists (\bar{x}, \bar{y}) \in R \, ((x,y)(\bar{x},\bar{y}) = (\bar{x},\bar{y})(x,y) = (1,1))$.

$(x,y)(\bar{x},\bar{y}) = (x \cdot \bar{x}, y \cdot \bar{y}) = (1,1)$

$$\begin{cases} x \cdot \bar{x} \equiv_4 1 & \Rightarrow \mathcal{U}(\mathbb{Z}_4) = \{1,3\} \\ y \cdot \bar{y} \equiv_6 1 & \Rightarrow \mathcal{U}(\mathbb{Z}_6) = \{1,5\} \end{cases} \Rightarrow \mathcal{U}(R) = \{(1,1),(1,5),(3,1),(3,5)\}.$$

Facendo un ragionamento analogo agli elementi invertibile, i divisori dello zero in $\mathbb{Z}_4$ sono $\{2\}$, mentre in $\mathbb{Z}_6$ sono $\{2,3,4\}$. Dunque i divisori dello zero i R sono: $\{(2,2),(2,3),(2,4)\}$.

$(x,y) \in R$ è idempotente se:

$$\begin{cases} x^2 \equiv_4 x & \Rightarrow \text{gli elementi idempotenti sono } \{0,1\} \\ y^2 \equiv_6 y & \Rightarrow \text{gli elementi idempotenti sono } \{0,3,1,4\}. \end{cases}$$

Dunque gli elementi idempotenti in R sono $\{(0,0),(0,3),(0,1),(0,4),(1,0),(1,1),(1,3),(1,4)\}$.

(iii)

Un elemento di R è radice del polinomio $x^2 - x$ se e solo se: $(a,b)^2 \cdot (a,b) \bar{=} (a,b) = (0,0)$

$\Leftrightarrow (a^2 - a, b^2 - b) = (0,0) \Leftrightarrow \begin{cases} a^2 - a = 0 \\ b^2 - b = 0 \end{cases} \Leftrightarrow \begin{cases} a^2 = a \\ b^2 = b \end{cases}$

Quindi le radici del polinomio sono tutti gli elementi idempotenti trovati nel punto precedente

(iv)

$mcm(4,6) = 12$, infatti $12(1,1) = (12,12) = (0,0)$. Quindi 12 è la caratteristica di R.

(v)

R è un dominio di integrità se è integro, commutativo e unitario. Dobbiamo verificare solo l'integrità, ovvero che sia privo di divisori dello zero. Nel punto (ii) abbiamo visto che esistono, quindi R non è un dominio di integrità.

(vi)

M è parte chiusa rispetto a + e $\cdot$ $\iff \forall (a,b),(c,d) \in M \, ((a,b)+(c,d) \wedge (a,b)(c,d)$ appartengono a M).

$(a,b)+(c,d) = (a+c, b+d)$ $\quad$ $(a,b)(c,d) = (ac, bd)$.

Affinché sia parte chiusa $b+d \in \{[0]_6, [3]_6\}$ e $bd \in \{[0]_6, [3]_6\}$ che è banalmente vero. Quindi $(M,+,\cdot)$ è un anello commutativo.

(vii)

$(x,y) \in M$ è neutro se $\forall (a,b) \in M \, ((x,y)(a,b) = (a,b)(x,y) = (a,b))$

$(x,y)(a,b) = (xa \cdot yb) = (a,b)$

$$\begin{cases} xa = a \\ yb = b \end{cases} \iff \begin{cases} x = 1 \\ y = 3 \end{cases} \Rightarrow (1,3) \text{ è neutro a sinistra.}$$

Facendo opportune verifiche notiamo che è neutro anche a destra.

$(M,\cdot)$ sarà quindi un monoide.

Esercizio 4

ρ è una relazione d'ordine se è riflessiva, antisimmetrica e transitiva.

ρ è riflessiva $\iff \forall x \in \mathbb{N} \, (x \rho x)$

$x \rho x \iff x - x \in 2x\mathbb{N}$ il che è vero.

ρ è antisimmetrica $\iff \forall a,b \in \mathbb{N} \, (a \rho b \wedge b \rho a \Rightarrow a = b)$

$a \rho b \iff b - a = 2ak$

$b \rho a \iff a - b = 2bh$

$$\begin{cases} b - a = 2ak \\ a - b = 2bh \end{cases} \quad \begin{cases} b = 2ak + a = a(2k+1) \\ a = 2bh + b = b(2h+1) \end{cases} \quad \begin{cases} b = b(2h+1)(2k+1) \\ '' \end{cases}$$

Questo implica che $(2h+1)(2k+1) = 1 \iff h,k = 0$. Quindi otteniamo:

$$\begin{cases} b - a = 2a \cdot 0 \\ a - b = 2b \cdot 0 \end{cases} \quad \begin{cases} b = a \\ a = b \end{cases} \quad \checkmark$$

ρ è transitiva $\Leftrightarrow \forall a,b,c \in \mathbb{N} (a \rho b \wedge b \rho c \Rightarrow a \rho c)$

$a \rho b \Leftrightarrow b - a = 2ah$

$b \rho c \Leftrightarrow c - b = 2bk$

$\cancel{\begin{cases} b - a = 2ah \\ c - b = 2bk \end{cases}} \quad \cancel{\begin{cases} c - 2bk - a = 2ah \\ b = c - 2bk \end{cases}} \quad \cancel{\begin{cases} a = c - 2bk - 2ah \\ '' \end{cases}}$

$$\begin{cases} b - a = 2ah \\ c - b = 2bk \end{cases} \quad \begin{cases} b = a(2h+1) \\ c = b(2k+1) \end{cases} \quad \begin{cases} '' \\ c = a(2h+1)(2k+1) \end{cases}$$

$$\begin{aligned} c - a &= a(2h+1)(2k+1) - a \\ &= a((2h+1)(2k+1) - 1) \\ &= a(2hk + 2h + 2k + 1 - 1) \\ &= a(2\underbrace{(hk + h + k)}_{s}) = a2s \in 2a\mathbb{N} \checkmark \end{aligned}$$

(i)

L'insieme dei minoranti è $\{n \in \mathbb{N} \mid n \rho 12\}$

$$\begin{aligned} n \rho 12 &\Leftrightarrow 12 - n = 2 \cdot n \cdot \mathbb{N} \Leftrightarrow \\ &\Leftrightarrow \exists k \in \mathbb{N} (12 - n = 2nk) \\ &\Leftrightarrow \exists k \in \mathbb{N} (12 = n(2k+1)) \Leftrightarrow n \mid 12 \text{ e } 12/n \text{ è dispari.} \end{aligned}$$

Quindi i divisori di 12 sono $\{1, 3, 4, 6, 12\}$. Vediamo che per $n = 12$ si ha $12/12 = 1$ e per $n = 4$ si ha $12/4 = 3$. Dunque l'insieme dei minoranti è $\{4, 12\}$.

(ii)

- Minimo: m è minimo $\Leftrightarrow \forall x \in \mathbb{N} (m \rho x)$

$m \rho x \Leftrightarrow x - m = 2m\mathbb{N} \Leftrightarrow \exists k \in \mathbb{N} (x - m = 2mk) \Leftrightarrow \exists k \in \mathbb{N} (x = m(2k+1))$.

Non è presente un minimo in quanto 1 (candidato per essere minimo) vale solo per x dispari e non quelli pari.

- Massimo: M è massimo $\Leftrightarrow \forall x \in \mathbb{N} (x \rho M)$.

$x \rho M \Leftrightarrow \exists k \in \mathbb{N} (M = x(2k+1))$.

Possiamo prendere però valori di x arbitrariamente grandi. Quindi non esiste un massimo.

• Minimali = m è minimale $\iff \forall x \in \mathbb{N} \, (x \rho m \wedge m \rho x \Rightarrow m \rho x)$.

Ovvero non esiste alcun elemento tale che $x \rho m$. Seguendo un ragionamento analogo a quanto fatto per il minimo, possiamo dire che gli elementi minimali sono... ?

• Massimali = M è massimale $\iff \forall x \in \mathbb{N} \, (x \rho M \wedge M \rho x \Rightarrow x \rho M)$.

Per lo stesso motivo del massimo, non esistono elementi massimali.

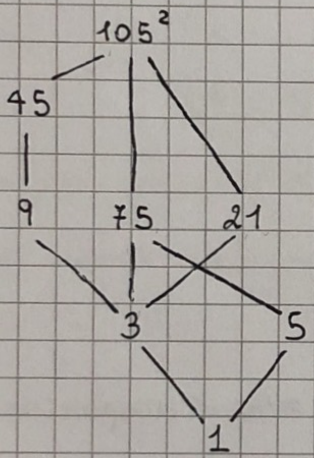
(iii)

$(\mathbb{N}, \rho)$ è un reticolo $\iff \forall x, y \in \mathbb{N} \, (\exists \inf(\{x, y\}) \wedge \exists \sup(\{x, y\}))$.

Non è possibile determinare estremo inferiore e/o superiore per ogni coppia di elementi, dunque non è un reticolo.

(iv)

Il diagramma di Hasse è:



E' un reticolo in quanto per ogni elemento non confrontabile è possibile determinare l'estremo inferiore e superiore.

Non è complementato, ad esempio 75 non ha complemento: $75 \wedge 21 = 3$ (?)

Non è distributivo perché ha un sottoreticolo isomorfo al reticolo pentagonale.

Esercizio 5

Una relazione binaria φ è una corrispondenza del tipo, preso a un insieme, $\varphi = (a, a, G)$, con $G \subseteq a \times a$.

(i)

Considerando $a = \{0, 1, 2, 3, 4, 5, 6, 7\}$, dobbiamo trovare tutte le relazioni di equivalenza tali che: $\{(0,7), (1,4), (2,3), (2,4), (2,7)\} \subseteq G$. Inoltre, se $(1,3) \in G$ allora anche $(5,0) \in G$.

Per la proprietà transitiva, $(1 \sim 4) \wedge (4 \sim 2) \Rightarrow (1 \sim 2)$. Per lo stesso motivo $(0 \rho 7) \wedge (7 \rho 2) \Rightarrow (0 \rho 2)$. Inoltre, se $(3 \sim 2) \wedge (2 \sim 0) \Rightarrow (3 \sim 0) \Rightarrow (5 \sim 0)$.

L'unico elemento rimasto è 6 in quanto $[2]_\rho = \{0, 1, 2, 3, 4, 5, 7\}$.

- Se 6 è in relazione con un elemento di $[2]_\rho$, allora $\sim_1 = \tilde{\iota}$ è la relazione totale.
- In caso contrario, 6 sarà in relazione solo con se stesso con $\sim_2$.

(ii)

Per il teorema fondamentale delle partizioni e delle relazioni di equivalenza, sappiamo che esiste una biezione tra gli insiemi $Eq(a)$ e $Part_2(a)$. Otteniamo quindi le partizioni =

- $a/\sim_1 = a/\tau = \{a\}$
- $a/\sim_2 = \{[2]_\sim, [6]_\sim\}$ dove $[6]_\sim = \{6\}$.

Esercizio 6

$g(\bar{1}) = \overline{11} = \bar{0}$ $\qquad g(\overline{-1}) = \overline{11} = \bar{0}$

Possiamo riscrivere $(x^2-5) = (x-4)(x+4) = (x-7)(x+7)$ in quanto $\bar{4}$ e $\bar{7}$ sono le radici.

Abbiamo visto che $\bar{1}$ e $\overline{-1}$ sono le radici di g, quindi per il teorema di Ruffini $x-1/g$ e $x+1/g$.

$$
\begin{array}{l|l}
x^5+0+0+\bar{4}x^2-x+\bar{7} & x-1 \\
\hline
-x^5+x^4 & x^4+x^3+x^2+\bar{5}x+\bar{4} \\
\hline
// \quad x^4+0+\bar{4}x^2-x+\bar{7} & \\
-x^4+x^3 & \\
\hline
// \quad x^3+\bar{4}x^2-x+\bar{7} & \\
-x^3+x^2 & \\
\hline
// \quad \bar{5}x^2-x+\bar{7} & \\
-\bar{5}x^2+5x & \\
\hline
// \quad \bar{4}x+\bar{7} & \\
-\bar{4}x+\bar{4} & \\
\hline
// \quad \bar{0} &
\end{array}
$$

Il risultato ottenuto è ancora divisibile per $x+1$:

$$
\begin{array}{l|l}
x^4+x^3+x^2+\bar{5}x+\bar{4} & x+1 \\
\hline
-x^4-x^3 & x^3+x+4 \\
\hline
// \quad // \quad x^2+\bar{5}x+\bar{4} & \\
-x^2-x & \\
\hline
// \quad \bar{4}x+\bar{4} & \\
-\bar{4}x-\bar{4} & \\
\hline
// \quad \bar{0} &
\end{array}
$$

Otteniamo quindi che:

$f = (x-4)(x+4)(x-1)(x+1)(x^3+x+4)$

(i)

No.

(ii)

No.