TRACCIA – 16 GENNAIO 2023

Esercizio 1

$\neg(p \Rightarrow q) \Leftrightarrow (\neg p \vee q)$ per la tautologia dell'implicazione come disgiunzione

$\Leftrightarrow (p \wedge \neg q)$ per De Morgan

Esercizio 2

$T : A \longrightarrow A \qquad S : B \longrightarrow A \qquad r : T \longrightarrow S$ (con $B \longrightarrow A$)

(i)

$|T| = |A|^{|A|} = 10^{10} \qquad |S| = |A|^{|B|} = 10^{9}$

(ii)

(a) Una applicazione può essere iniettiva $\Leftrightarrow$ la cardinalità del dominio è minore o uguale della cardinalità del codominio. Ricordiamo che $f : A \to A$ e $r : B \to A$.
Se f è iniettiva, allora essendo $B \subset A$, sicuramente l'iniettività è "conservata".

(b) Un'applicazione può essere suriettiva $\Leftrightarrow$ o dominio e codominio sono vuoti, o la cardinalità del codominio è minore o uguale del dominio. Poiché $|A| > |B|$, allora se f è suriettiva, non è detto che $r(f)$ lo sia.

(iii)

r è iniettiva $\Leftrightarrow \forall f_1, f_2 \in T\ (r(f_1) = r(f_2) \Rightarrow f_1 = f_2)$.
Poiché r è la restrizione di f, c'è il valore 9 che viene lasciato fuori. Quindi se $r(f_1) = r(f_2)$ allora non è detto che $f_1 = f_2$ in quanto non sappiamo cosa succede in 9.

r è suriettiva $\Leftrightarrow \forall g \in S\ (\exists f \in T\ (r(f) = g))$
$g : B \to A \quad f : A \to A$. Essendo r la restrizione di f, $r(f) : B \to A$. Quindi per ogni g è possibile trovare una applicazione f tale che $r(f) = g$.

(iv)

$[h]R$ è costituita da tutte le applicazioni f tali che $r(h) = r(f)$.
$r(h)(x)$ è la restrizione di h su B. Quindi significa che se $f : A \to A$ appartiene a $[h]R$ allora $r(f)(x) = 3 \quad \forall x \in B$. Il valore 9 però, che non è in B, deve comunque essere considerato, anche se non ha alcun tipo di restrizione, in quanto ci interessa sapere che $r(h) = r(f)$ per i valori in B. Dunque $|[h]R| = 10$. Avendo dimostrato che r è suriettiva $|T/R| = |S|$.

Esercizio 3

(i)

Dato che stiamo considerando $rest(a, 9)$, possiamo limitarci a ragionare sui valori $\{0, \dots, 8\}$

La classe di resto $[1]_p$ rappresenta l'insieme dei minimali, mentre la classe $[0]_p$ è l'insieme dei massimali.

Non ci sono minimo e massimo.

(ii)

$x \in \mathbb{Z}$ è minorante di $\{127, 721\} \Leftrightarrow x\, p\, 127 \wedge x\, p\, 721$.

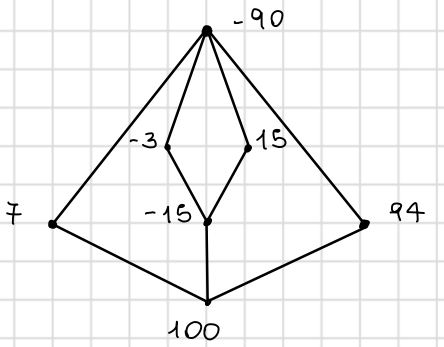
$x \,p\, 127 \Leftrightarrow x = 127 \lor rest(x,9)$ divide propriamente $rest(127,9) = 1$

$x \,p\, 721 \Leftrightarrow x = 721 \lor rest(x,9)$ divide propriamente $rest(721,9) = 1$

L'unico divisore di 1 è 1, ma non lo divide propriamente. Di conseguenza, non esistono minoranti di $\{127, 721\}$ e, in particolare, non esiste $\inf\{127, 721\}$.

(iii)
Per il punto precedente abbiamo visto che non per ogni $x, y \in \mathbb{Z}$ è determinato $\inf\{x, y\}$. Quindi non è un reticolo.

(v)
$rest(-90, 9) = 0$
$rest(-15, 9) = 3$
$rest(-3, 9) = 6$
$rest(7, 9) = 7$
$rest(15, 9) = 6$
$rest(94, 9) = 4$
$rest(100, 9) = 1$



E' un reticolo. Non è distributivo in quanto ha un sottoreticolo isomorfo al reticolo pentagonale. E' complementato.

Esercizio 4

(i)
• Associatività:
$\forall x, y, z \in \mathbb{Z}_{16} \ (x * (y * z) = (x * y) * z)$
$x * (y * z) = x * (\overline{3} y z) = \overline{9} x y z$
$(x * y) * z = (\overline{3} x y) * z = \overline{9} x y z$

• Commutatività:
$\forall x, y \in \mathbb{Z}_{16} \ (x * y = y * x)$
$x * y = \overline{3} x y = \overline{3} y x = y * x$

• Elemento neutro a sinistra:
$x \in \mathbb{Z}_{16}$ è neutro a sinistra $\Leftrightarrow \forall a \in \mathbb{Z} \ (x * a = a)$
$x * a = \overline{3} x a = a \Leftrightarrow 3 \overline{x} a \equiv_{16} a \Rightarrow 3 \overline{x} \equiv_{16} 1 \Rightarrow x = 11$.

• Elemento neutro a destra
$x \in \mathbb{Z}_{16}$ è neutro a destra $\Leftrightarrow \forall a \in \mathbb{Z}_{16} \ (a * x = a)$
Proviamo $x = 11$.
$a * 11 = \overline{3} \cdot \overline{11} a = a$ ✓.

• Simmetrizzabili
$\forall a \in \mathbb{Z}_{16} \ (\exists x \in \mathbb{Z}_{16} \ (x * a = a * x = \overline{11})$
$x * a = \overline{3} x a = \overline{11} \Rightarrow x a = 9$ (moltiplicando per l'inverso moltiplicativo di 3).
$x a \equiv_{16} 9$ ha soluzione $\Leftrightarrow$ $MCD(a, 16) / 9$. I divisori di 16 minori di 9 sono: 1, 2, 4, 8 e solo 1 divide 9. Quindi se $a = \{1, 3, 5, 6, 7, 9\}$ allora $MCD(a, 16) = 1 / 9$.

Possiamo quindi dire che $(\mathbb{Z}_{16}, *)$ è un monoide commutativo.

Troviamo l'inverso di 1, ovvero $x \in \mathbb{Z}_{16}$ tale che $1 * x = x * 1 = \overline{11}$
$1 * x = \overline{3} x = \overline{11} \Leftrightarrow \overline{3} x \equiv_{16} \overline{11} \Rightarrow x = 9$.
Vale anche a destra.

(ii)
H è una parte chiusa $\iff \forall x, y \in H\ (x * y \in H)$
$7 * 7 = 3 \notin H$ Quindi non è una parte chiusa

(iii)
$x \in \mathbb{Z}_{16} \setminus \{0\}$ è un divisore dello zero $\iff \forall y \in \mathbb{Z}_{16} \setminus \{0\}\ (x * y = y * x = 0)$
$x * y = 3xy = 3yx = y * x$
Quindi $xy = 0$. Gli unici elementi che possono essere divisori dello zero sono quelli non simmetrizzabili, ovvero gli elementi che non sono coprimi con 16. Sono $\{0, 2, 4, 6, 8, 10, 12, 14\}$.

Esercizio 6

(i)
Considerando il criterio di Einstein, possiamo dire che f è irriducibile in $\mathbb{Q}$.

(ii)
$f_5 = \bar{4}x + \bar{2}$
Per trovare il polinomio monico associato, dobbiamo moltiplicare f_5 per l'inverso moltiplicativo di 4. Lo troviamo risolvendo l'equazione $\bar{4}x \equiv_5 1 \Rightarrow x = 4$.
Otteniamo così il polinomio $x + \bar{3}$.

Facciamo lo stesso discorso per f_{32}. Poiché 32 è molto grande, trovo l'inverso moltiplicativo di 5 usando l'algoritmo Euclideo:

$32 = (6)5 + 2 \Rightarrow 2 = (1)32 + (-6)5$
$5 = (2)2 + 1 \Rightarrow 1 = (1)5 + (-2)2$
$2 = (2)1 + 0$

$$\begin{aligned} 1 &= (1)5 + (-2)2 \\ &= (1)5 + (-2)32 + (12)5 \\ &= (13)5 + (-2)32 \end{aligned}$$

Moltiplichiamo tutto per 13 e otteniamo: $x^4 + \bar{2}x^2 + \overline{20}x + \overline{26}$.

(iii)
Se $\mathbb{Z}_n[x]$ è un dominio di integrità, ogni elemento è cancellabile.
$\mathbb{Z}_n[x]$ è un dominio di integrità $\iff n$ è primo.
Quindi per $n \in \{2, 3, 5, 7\}$, f_n non nullo è cancellabile.