

TRACCIA - 20 FEBBRAIO 2025

Esercizio 1

(i)

Un numero intero è primo se non è invertibile e ha solo divisori banali.

(ii)

I numeri primi in S sono $\{2, 3\}$. Restano $\{-2, -1, 0, 1, 4\}$ che possiamo prendere o meno. Quindi il numero di sottoinsiemi richiesto è $2^5 = 32$.

(iii)

È dato dal coefficiente binomiale

$$\binom{7}{3} = \frac{7!}{3!(7-3)!} = 35$$

Esercizio 2

(i)

Sia A un anello commutativo unitario, $f \in A[x] \setminus \{0\}$. $c \in A$ è radice di f se e solo se $f(c) = 0$.

(ii)

Sia \mathbb{K} un campo, $f \in \mathbb{K}[x]$. Indichiamo con $n = \text{gr}(f)$. Allora f è ~~se~~ irriducibile se e solo se:

$$1) \forall g, h \in \mathbb{K}[x] (f = g \cdot h \Rightarrow \text{gr}(g) = n \oplus \text{gr}(h) = n)$$

$$2) \forall g, h \in \mathbb{K}[x] (f = g \cdot h \Rightarrow \text{gr}(g) = 0 \oplus \text{gr}(h) = 0).$$

(iii)

No, in quanto \mathbb{R} è un campo quindi ogni ~~non~~ coefficiente di un polinomio $f \in \mathbb{R}[x]$ sarà invertibile.

(iv)

• Grado 1:

$$\begin{array}{l} x \\ x+1 \\ x+2 \end{array}$$

• Grado 2:

$$\begin{array}{l} x^2 + 1 \\ x^2 + x + 2 \\ x^2 + 2x + 2 \end{array}$$

(v)

Il polinomio f non ha radici. Possiamo vedere se riusciamo ad ottenerlo tramite i polinomi irriducibili del punto precedente, ma neanche in questo caso otteniamo f . Dunque f non si può scomporre.

(vi)

Il polinomio f ha radice 1, dunque per Ruffini, è possibile dividerlo per $x-1$.

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

$x^3 + 2x^2 + 3x + 4$ è riducibile dato che ha radice 1:

$$\begin{array}{r|l} x^3 + 2x^2 + 3x + 4 & x - 1 \\ \hline -x^3 + x^2 & x^2 + 3x + 1 \\ \hline // 3x^2 + 3x + 4 & \\ -3x^2 + 3x & \\ \hline // 6x + 4 & \\ -x + 1 & \\ \hline // 0 & \end{array} \quad \begin{array}{r|l} x^2 + 3x + 1 & x - 1 \\ \hline -x^2 + x & x + 4 \\ \hline // 4x + 1 & \\ -4x + 4 & \\ \hline // 0 & \end{array}$$

$$\begin{array}{r|l} x + 4 & x - 1 \\ -x + 1 & 1 \\ \hline // 0 & \end{array}$$

Dunque $f = (x-1)(x-1)(x-1)(x+4)$

Esercizio 4

(i) (?)

f è ben definita perché, per il teorema fondamentale dell'aritmetica, ogni intero diverso da $\{-1, 0, 1\}$ o è primo o si può scrivere come prodotto di primi. Quindi ogni elemento del dominio avrà immagine. (importante che il prodotto è unico).

(ii)

f non è iniettiva in quanto, presi due elementi distinti del dominio, è possibile che abbiano la stessa immagine. Ad esempio:

$$f(10) = 2$$

$$f(6) = 2$$

f non è neanche suriettiva in quanto per esserlo $\text{im}(f) = \mathbb{N}$ ma $0 \notin \text{im}(f)$.

(iii)

$$\leftarrow f(\{0\}) = \emptyset \quad \text{per quanto detto prima.}$$

$$\leftarrow f(\{1\}) = \{p \in \mathbb{N}^* / p \text{ è primo}\}$$

$$\rightarrow f(\{8h / h \in \mathbb{N}^*\}) = \{x \in \mathbb{N}^* / x \geq 3\}$$

(iv)

f è un omomorfismo da (\mathbb{N}^*, \cdot) su $(\mathbb{N}, +)$ se $\forall x, y \in \mathbb{N}^* (f(x \cdot y) = f(x) + f(y))$.
Supponiamo che $x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ e che $f(x) = n$.
 $y = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_s^{\beta_s}$ e che $f(y) = m$.

$$f(x) + f(y) = n + m$$

$$f(x \cdot y) = f(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t} \cdot p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}) = \overbrace{\alpha_1 + \alpha_2 + \cdots + \alpha_t}^{n} + \overbrace{\beta_1 + \beta_2 + \cdots + \beta_s}^{m} = n + m.$$

(v)

$$[8]_{\mathbb{R}} = \{x \in \mathbb{N}^* / x = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_t^{\alpha_t} \wedge \sum_{i=1}^t \alpha_i = 3\}$$

(vi)

• Minimo: $m \in \mathbb{N}^*$ è minimo in $(\mathbb{N}^*, \sigma) \Leftrightarrow \forall x \in \mathbb{N}^* (m \sigma x)$.

Significa che $f(m)$ deve essere divisore proprio di tutti gli $f(x)$. Non esiste però tale elemento.

• Massimo: $M \in \mathbb{N}^*$ è massimo in $(\mathbb{N}^*, \sigma) \Leftrightarrow \forall x \in \mathbb{N}^* (x \sigma M)$.

~~Bonelli~~ Non esiste neanche il massimo dato che è possibile prendere valori di x arbitrariamente grandi.

• Minimali = $m \in \mathbb{N}^*$ è minimale in $(\mathbb{N}^*, \sigma) \Leftrightarrow \forall x \in \mathbb{N}^* (m \sigma x \wedge x \neq m \Rightarrow m \sigma x)$.

Il valore più piccolo che m può assumere è 2, in quanto $f(2) = 1$. Non essendo iniettiva, ci saranno altri elementi la cui immagine fa 1, ovvero i numeri primi. Questi sono gli elementi minimali.

• Massimali = $H \in \mathbb{N}^*$ è massimale in $(\mathbb{N}^*, \sigma) \Leftrightarrow \forall x \in \mathbb{N}^* (x \sigma H \wedge H \sigma x \Rightarrow x \sigma H)$

Significa che non deve mai succedere che $f(H)$ è un divisore proprio di $f(x)$. Il caso più plausibile è quello in cui $f(x)$ è primo perché avrebbe solo divisori banali. Dunque gli elementi massimali sono quelli che hanno come immagine, tramite f , un numero primo.

(vii)

$m \in \mathbb{N}^*$ è minorante $\Leftrightarrow \forall x \in \{4, 9\} (m \sigma x)$.

$$f(4) = 2 = f(9)$$

Dobbiamo quindi trovare $f(m)$ che divide propriamente 2, ovvero 1 (è l'unico divisore banale di 2). Gli elementi che hanno come immagine 1 sono i numeri propri.

(viii)

Un insieme ordinato (S, σ) è un reticolo se e solo se
 $\forall x, y \in S (\exists \inf(\{x, y\}), \exists \sup(\{x, y\}))$.

Considerando (\mathbb{N}^*, σ) e $x, y \in \mathbb{N}^*$:

• $\sup(\{x, y\}) = \minimo \text{ comune multiplo } f(\overset{x}{\cancel{x}}) \text{ e } f(\overset{y}{\cancel{y}})$

• $\inf(\{x, y\}) = \massimo \text{ comune divisore di } f(x) \text{ e } f(y)$

Non è sempre garantita la loro esistenza, quindi (\mathbb{N}^*, σ) non è un reticolo.

(ix)

$$f(1) = 0 \quad f(9) = 2 \quad f(30) = 3$$

$$f(2) = 1 \quad f(12) = 3$$

$$f(6) = 2 \quad f(25) = 2$$

Possiamo togliere il valore 25. Quindi $(\mathbb{N}^* \setminus \{25\}, \sigma)$ è un reticolo.

Esercizio 5

(i)

* è commutativa se $\forall x, y \in P(\mathbb{N}) (x * y = y * x)$.

$$x * y = x \cup (y \setminus \{3\}) \quad y * x = y \cup (x \setminus \{3\})$$

Supponiamo che $x \neq y$ e $x = \{2, 4\}$ e $y = \{1, 2, 3\}$.

$$x * y = \{1, 2, 4\} \quad y * x = \{1, 2, 3, 4\}$$

Sono diversi, dunque non è commutativa.

* è associativa se $\forall x, y, z \in P(\mathbb{N}) (x * (y * z) = (x * y) * z)$

$$\begin{aligned} x * (y * z) &= x * (y \cup (z \setminus \{3\})) = x \cup ((y \cup (z \setminus \{3\})) \setminus \{3\}) = \\ &= x \cup \{(y \setminus \{3\}) \cup (z \setminus \{3\})\} \end{aligned}$$

$$(x * y) * z = (x \cup (y \setminus \{3\})) * z = x \cup (y \setminus \{3\}) \cup (z \setminus \{3\})$$

Sono uguali, dunque è associativa.

(ii)

$n \in P(\mathbb{N})$ è neutro a sinistra se $\forall x \in P(\mathbb{N}) (n * x = x)$.

$$n * x = n \cup (x \setminus \{3\}) = x \Leftrightarrow n = \emptyset.$$

Questo non va bene, in quanto n ~~dipende~~ dipende dal valore di x . Dunque non c'è neutro a sinistra.

$n \in P(\mathbb{N})$ è neutro a destra se $\forall x \in P(\mathbb{N}) (x * n = x)$

$$x * n = x \cup (n \setminus \{3\}) = x \Leftrightarrow n = \emptyset.$$

Dunque \emptyset è neutro a destra.

Non ha neutro, in quanto dovrebbe esistere neutro a destra e sinistra.

(iii)

È un semigruppo dato che * è associativa. Non è un monoido per l'assenza di elemento neutro e, di conseguenza, non è neanche un gruppo.

(iv)

$x \in P(\mathbb{N})$ è cancellabile a sinistra se $\forall a, b \in P(\mathbb{N})$ ($x * a = x * b \Rightarrow a = b$).

$$x * a = x \cup (a \setminus \{3\}) \quad x * b = x \cup (b \setminus \{3\})$$

$$x \cup (a \setminus \{3\}) = x \cup (b \setminus \{3\})$$

Affinché $a \setminus \{3\} = b \setminus \{3\}$, $x = \emptyset$. Quindi \emptyset è cancellabile a sinistra.

$x \in P(\mathbb{N})$ è cancellabile a destra se $\forall a, b \in P(\mathbb{N})$ ($a * x = b * x \Rightarrow a = b$).

$$a * x = a \cup (x \setminus \{3\}) \quad b * x = b \cup (x \setminus \{3\})$$

Affinché $a = b$, $x \setminus \{3\} = \emptyset$, il che significa che $x \subseteq \{3\}$.

Un elemento $x \in P(\mathbb{N})$ se $x = x * x$.

$$x * x = x \cup (x \setminus \{3\})$$

$x \cup (x \setminus \{3\})$ sarà sempre uguale a x in quanto $(x \setminus \{3\}) \subseteq x$. Dunque tutti gli elementi di $P(\mathbb{N})$ sono idempotenti rispetto a $*$.

(v)

\cap in $P(\mathbb{N})$ è distributiva a sinistra rispetto a $*$ se $\forall x, y, z \in P(\mathbb{N})$:

$$x \cap (y * z) = (x \cap y) * (x \cap z)$$

$$x \cap (y * z) = x \cap (y \cup (z \setminus \{3\})) = (x \cap y) \cup (x \cap (z \setminus \{3\})) = (x \cap y) \cup ((x \cap z) \setminus \{3\})$$

$$(x \cap y) * (x \cap z) = (x \cap y) \cup ((x \cap z) \setminus \{3\})$$

Dunque è distributiva a sinistra.

A destra invece dovremmo avere: $(y * z) \cap x = (y \cap x) * (z \cap x)$

$$(y * z) \cap x = (y \cup (z \setminus \{3\})) \cap x = (y \cap x) \cup ((x \cap z) \setminus \{3\})$$

$$(y \cap x) * (z \cap x) = (y \cap x) \cup ((z \cap x) \setminus \{3\})$$

Dunque è distributiva anche a destra.

Esercizio 6

$$84n + 5 \equiv_{92} 14n - 1 \Leftrightarrow 70n \equiv_{92} -6 \Leftrightarrow 70n \equiv_{92} 86$$

L'equazione congruenziale ottenuta ha soluzione se e solo se $\text{MCD}(70, 92) | 86$.
E' vero in quanto $2 | 86$. Possiamo dividere tutto per 2 e ottenere così
 $35n \equiv_{46} 43$

Per risolvere l'equazione, troviamo l'inverso moltiplicativo di 35 in modulo 46. Significa risolvere l'equazione $35n \equiv_{46} 1$. Usiamo l'algoritmo Euclideo.

$$1 = 46x + 35y$$

$$46 = (1)35 + 11 \Rightarrow 11 = (1)46 + (-1)35$$

$$35 = (3)11 + 2 \Rightarrow 2 = (1)35 + (-3)11$$

$$11 = (5)2 + 1 \Rightarrow 1 = (1)11 + (-5)2$$

$$2 = (2)1 + 0$$

Paretiamo da $1 = (1)11 + (-5)2$ e sostituiamo:

$$\begin{aligned} 1 &= (1)46 + (-1)35 + (-5)35 + (15)11 \\ &= (1)46 + (-6)35 + (15)46 + (-15)35 \\ &= (16)46 + (-21)35 \end{aligned}$$

Dunque $n = -\overline{21} = \overline{25}$. Moltiplichiamo ambo i membri di $35n \equiv_{46} 43$ per n ottenuto.

$$n \equiv_{46} 43 \cdot \overline{25} = \overline{17}$$

Dunque l'insieme delle soluzioni è $\{n \in \mathbb{Z} \mid n = 17 + 46k, k \in \mathbb{Z}\}$