

Esercizio 1

Se $\varphi \rightarrow \psi$ è una tautologia, significa che l'implicazione è sempre vera. O meglio, se facciamo la tabella di verità, notiamo che il risultato è sempre vero. ψ è una contraddizione, il che significa che è sempre falsa. Per capire com'è fatta φ , dobbiamo considerare il fatto che l'implicazione è falsa solo se l'antecedente è vero e il conseguente è falso. Mettendo tutto insieme possiamo dire che anche $\varphi \rightarrow \psi$ è una contraddizione.

Esercizio 3.

(i) $(A, \oplus, *)$ è un anello se ~~è un gruppo abeliano~~ (A, \oplus) è un gruppo abeliano, $(A, *)$ è un semigruppo e l'operazione $*$ è distributiva rispetto a \oplus .

Controlliamo che (A, \oplus) è un gruppo abeliano.

1) L'operazione è associativa:

$$\oplus \text{ è associativa se } \forall x, y, a, b, \alpha, \beta, \in A ((x, y) \oplus ((a, b) \oplus (\alpha, \beta)) = ((x, y) \oplus (a, b)) \oplus (\alpha, \beta)).$$

Partiamo da:

$$((x, y) \oplus ((a, b) \oplus (\alpha, \beta))) = (x, y) \oplus (a + \alpha, b + \beta) = (x + a + \alpha, y + b + \beta)$$

$$((x, y) \oplus (a, b)) \oplus (\alpha, \beta) = (x + a, y + b) \oplus (\alpha, \beta) = (x + a + \alpha, y + b + \beta)$$

I due sono uguali in quanto l'operazione $+$ è commutativa. Quindi \oplus è associativa.

Vediamo se in (A, \oplus) c'è l'elemento neutro.

$(x, y) \in A$ è neutro se $\forall (a, b) \in A ((x, y) \oplus (a, b) = (a, b) \oplus (x, y) = (a, b))$.

$$(x, y) \oplus (a, b) = (x + a, y + b) = (a, b) \Leftrightarrow (x, y) = (0, 0)$$

$$(a, b) \oplus (x, y) = (a + x, b + y) = (a, b) \Leftrightarrow (x, y) = (0, 0).$$

Quindi l'elemento neutro esiste ed è $(0, 0) \in A$.

In questo caso l'elemento neutro sinistro e destro coincidono, ma non vale sempre.

Dobbiamo ora vedere se (A, \oplus) ogni elemento è invertibile.
 In
 Ogni ~~$(a, b) \in A$~~ è invertibile $\Leftrightarrow \exists (x, y) \in A$ t.c.
 $(a, b) \oplus (x, y) = (x, y) \oplus (a, b) = (0, 0)$.

$$(a, b) \oplus (x, y) = (a+x, b+y) = (0, 0) \Leftrightarrow (x, y) = (-a, -b)$$

$$(x, y) \oplus (a, b) = (x+a, b+y) = (0, 0) \Leftrightarrow (x, y) = (-a, -b).$$

Dunque ogni elemento è invertibile perché esiste l'inverso $(-a, -b)$.

In questo caso l'inverso sinistro e destro coincidono, ma non vale sempre.

Ora dobbiamo vedere che $(A, *)$ è un semigruppo. In particolare, dobbiamo vedere che $*$ è associativa.

$$\forall (a, b), (x, y), (\alpha, \beta) \in A ((a, b) * ((x, y) * (\alpha, \beta))) = ((a, b) * (x, y)) * (\alpha, \beta)$$

$$(a, b) * ((x, y) * (\alpha, \beta)) = (a, b) * (0, x\alpha) = (0, 0)$$

$$((a, b) * (x, y)) * (\alpha, \beta) = (0, a\alpha) = * (\alpha, \beta) = (0, 0)$$

Hanno lo stesso risultato, quindi è associativa.

Dobbiamo concludere verificando che $*$ è distributiva rispetto a \oplus .

$$(\forall (a, b), (x, y), (\alpha, \beta) \in A ((a, b) * ((x, y) \oplus (\alpha, \beta)) = ((a, b) * (x, y)) \oplus ((a, b) * (\alpha, \beta)))$$

$$(a, b) * ((x, y) \oplus (\alpha, \beta)) = (a, b) * (x+\alpha, y+\beta) = (0, a(x+\alpha))$$

$$(a, b) * (x, y) = (0, ax)$$

$$(a, b) * (\alpha, \beta) = (0, a\alpha)$$

$$(0, a\alpha) \oplus (0, a\alpha) = (0, ax + a\alpha) = (0, a(x+\alpha))$$

Possiamo così concludere che è un anello.

(ii)

$(A, \oplus, *)$ è unitario se è verificato l'elemento neutro di $*$. ovvero se è verificata:

$$\forall (a, b) \in A (\exists (x, y) \in A ((a, b) * (x, y) = (x, y) * (a, b) = (a, b)))$$

$$(a, b) * (x, y) = (0, ax) \neq (a, b).$$

Facendo solo una parte, abbiamo potuto subito verificare che una tale coppia (x, y) non può mai esistere.

$(A, \oplus, *)$ è commutativo se è commutativo rispetto a $*$. Oppure se:

$$\forall (a, b), (x, y) \in A \quad ((a, b) * (x, y) = (x, y) * (a, b))$$

$$\left. \begin{array}{l} (a, b) * (x, y) = (0, a \cdot x) \\ (x, y) * (a, b) = (0, x \cdot a) \end{array} \right\} \text{coincidono in quanto } \cdot \text{ è commutativa.}$$

$(A, \oplus, *)$ è booleano se è unitario e ogni elemento è idempotente, ovvero ogni elemento coincide con il proprio quadrato. Abbiamo però verificato che non è unitario, quindi non è booleano.

$(A, \oplus, *)$ è integro se non ha divisori dello zero. Verifichiamo quindi se li ha.

$$(0, 0)$$

$$(x, y) \in A \text{ è un divisore dello zero se } \forall (a, b) \in A \cdot (x, y) * (a, b) = (0, 0)$$

Poiché $(x, y) * (a, b) = (0, x \cdot a)$, allora i divisori dello zero sono tutte le coppie la cui prima coordinata è nulla ma la seconda no.

(iii)

Per quanto detto prima, $(5, 3) \rightarrow$ è un divisore dello zero, ~~ma non~~ e $(5, 0) \downarrow$.

(iv)

$(B, \oplus, *)$ è ~~un~~ un sottoanello di $(A, \oplus, *)$ se e solo se è chiuso rispetto a \oplus e $*$. Vediamo:

$$\forall (0, b), (0, y) \in B \quad ((0, b) \oplus (0, y) \in B)$$

$$(0, b) \oplus (0, y) = (0, b + y) \in B \checkmark$$

$$\forall (0, b), (0, y) \in B \quad ((0, b) * (0, y) \in B)$$

$$(0, b) * (0, y) = (0, b \cdot y) \in B \checkmark$$

Quindi è un sottoanello di $(A, \oplus, *)$.

Ora dobbiamo vedere se B è isomorfo a $(\mathbb{Z}, +, \cdot)$. Questo significa verificare ~~se~~ esiste una biezione $f: \mathbb{Z} \rightarrow B$ t.c.

$$f(a+b) = f(a) \oplus f(b)$$

$$f(a \cdot b) = f(a) * f(b)$$

La somma in B è la stessa in \mathbb{Z} . Per il prodotto invece no in quanto in B è sempre nullo.

Ragioniamo adesso per con C e vediamo se è un sottoanello di $(A, \oplus, *)$.

$$\forall (a, 0), (x, 0) \in C \quad ((a, 0) \oplus (x, 0)) \in C$$

$$(a, 0) \oplus (b, 0) = (a+b, 0) \in C \quad \checkmark$$

$$\forall (a, 0), (x, 0) \in C \quad ((a, 0) * (x, 0)) \in C$$

$$(a, 0) * (x, 0) = (0, a \times) \notin C$$

Quindi non è un sottoanello di $(A, \oplus, *)$.

Esercizio 4

(i)

f non è iniettiva in quanto ci sono 2 parti di A che hanno la stessa immagine tramite f . Ad esempio $\{2, 3\}$ e $\{1, 4\}$ hanno immagine 2.

~~f è suriettiva in quanto ogni elemento del codominio è immagine di almeno un elemento del codominio. Ovvvero $\text{im}(f) = \mathbb{N}$~~

Non è neanche suriettiva in quanto $\text{inn}(f) < \mathbb{N}$ e non uguale.

(ii)

$$\text{im}(f) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

(iii)

~~P è il nucleo di equivalenza di f , ovvero $\forall x, y \in P(A) \quad (x \sim y \Leftrightarrow f(x) = f(y))$~~

La $[\{1, 2\}]_P$ è costituita da tutte le parti di A di cardinalità 2 che non contengono 5. Il numero di questi elementi è dato dal coefficiente binomiale

$$\binom{9}{2} = \frac{9!}{2!(9-2)!} = \frac{9!}{2!7!} = 36 \quad q = |\overset{A}{\sim} \{5\}|.$$

La $[\{5\}]_P$ è costituita da tutte le parti di A che contengono 5. Possiamo scriverlo come $\{5\} \cup x$ (dove $x \subseteq A \setminus \{5\}$). Il numero di questi insiemi sarà $2^9 = 512$.

(iv)

$$|P(A)/_P| = |\text{im}(f)| = |\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}| = 10.$$

Esercizio 5

(i)

Lavoriamo su σ .

- σ riflessiva $\Leftrightarrow \forall a, b \in \mathbb{N}^* (a \sigma a)$.

$$a \sigma a \Leftrightarrow (a = a \vee \forall p \in P (p/a \Rightarrow p^2/a))$$

Vero perché $a = a$ è sempre vero.

- σ antisimmetrica $\Leftrightarrow \forall a, b \in \mathbb{N}^* (a \sigma b \wedge b \sigma a \Rightarrow a = b)$

$$a \sigma b \Leftrightarrow (a = b \vee \forall p \in P (p/a \Rightarrow p^2/b))$$

$$b \sigma a \Leftrightarrow (\exists (b = a \vee \forall p \in P (p/b \Rightarrow p^2/a)))$$

Se $a = b \wedge b = a \Rightarrow$ allora la proprietà è banalmente verificata.
Dobbiamo quindi vedere se:

$$(\forall p \in P ((p/a \Rightarrow p^2/b) \wedge (p/b \Rightarrow p^2/a))).$$

Supponiamo che $a \neq b$ e che p/a ma $p^2 \nmid b$.

Sappiamo che $a \sigma b \Rightarrow p/a$ e segue che p^2/b .

Ma sappiamo anche che $b \sigma a \Rightarrow p^2/a$.

Perciò avremmo supposto non fosse vero, è un assurdo, quindi se $a \sigma b \wedge b \sigma a \Rightarrow a = b$.

- σ transitiva $\Leftrightarrow \forall a, b, c \in \mathbb{N}^* ((a \sigma b \wedge b \sigma c) \Rightarrow a \sigma c)$.

$$a \sigma b \Leftrightarrow (a = b \vee \forall p \in P (p/a \Rightarrow p^2/b))$$

$$b \sigma c \Leftrightarrow (b = c \vee \forall p \in P (p/b \Rightarrow p^2/c))$$

Se $a = b \wedge b = c \Rightarrow a = c$ e abbiamo finito. Per l'altra condizione, sapendo che $a \sigma b \Rightarrow p/a \Rightarrow p^2/b$ e al tempo stesso $b \sigma c$, otteniamo che $p^2/b \Rightarrow p^4/c$ che è una condizione più forte di quella richiesta - Dunque per forza $a \sigma c$ come volevamo.

Passiamo ora a ρ .

- ρ riflessiva $\Leftrightarrow \forall a \in \mathbb{N}^* (a \rho a)$.

$$a \rho a \Leftrightarrow (\forall p \in P (p^{f_p(a)} / a) \wedge (a = a \vee f(a) < f(a)))$$

Dato che $f_p(a)$ è il massimo esponente di p che divide a , allora $p^{f_p(a)}$ divide sicuramente a . Il conseguente della congiunzione è sempre vero dato che $a = a$ vale sempre. Dunque ρ è riflessiva.

• **antisimmetrica** $\Leftrightarrow \forall a, b \in \mathbb{N}^* (a \succ b \wedge b \succ a \Rightarrow a = b)$

$$a \succ b \Leftrightarrow (\forall p \in P(p^{fp(a)} / b) \wedge (a = b \vee f(a) < f(b)))$$

$$b \succ a \Leftrightarrow (\forall p \in P(p^{fp(b)} / a) \wedge (a = b \vee f(b) < f(a)))$$

Se $a \succ b \wedge b \succ a$ allora possiamo dedurre che (per $a \neq b$) che, avendo $f(a) < f(b)$ e $f(b) < f(a)$, $f(a) = f(b)$. Inoltre se $p^{fp(a)} / b$ e $p^{fp(b)} / a$ allora a e b hanno gli stessi fattori in P . Questi fattori avranno gli stessi esponenti (per $f(a) = f(b)$), dunque $a = b$.

• **P transitiva** $\Leftrightarrow \forall a, b, c \in \mathbb{N}^* ((a \succ b \wedge b \succ c) \Rightarrow a \succ c)$.

$$a \succ b \Leftrightarrow (\forall p \in P(p^{fp(a)} / b) \wedge (a = b \vee f(a) \leq f(b)))$$

$$b \succ c \Leftrightarrow (\forall p \in P(p^{fp(b)} / c) \wedge (b = c \vee f(b) \leq f(c)))$$

• Banale il fatto che, per $a \neq b \neq c$, $f(a) < f(b) < f(c) \Rightarrow f(a) < f(c)$. Osserviamo che $p^{fp(a)}$ divide a , ma essendo $f_p(a)$ il massimo esponente di p che divide a , allora $p^{fp(a)} / a$. Lo stesso discorso vale per $p^{fp(b)}$. Dunque possiamo dire che $p^{fp(a)} / c$, che è quello che volevamo.

Possiamo concludere che sono entrambe relazioni d'ordine.

(ii)

Partiamo da σ .

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

$$m \sigma x \Leftrightarrow (m = x \vee \forall p \in P(p/m \Rightarrow p^2/x))$$

L'implicazione è sempre vera quando il suo antecedente è falso. Quindi dobbiamo trovare il valore di m che non viene mai diviso da $\{2, 3, 5\}$, ovvero un valore per cui $m \in \{2, 3, 5\}$ sono coprimi. L'unico valore possibile è $m=1$. Dunque 1 è il minimo.

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

Significa trovare un valore di M che viene sempre diviso da $\{2, 3, 5\}$. Poiché stiamo lavorando in \mathbb{N}^* , non esiste tale valore.

• **Minimale**: $m \in \mathbb{N}^*$ minimale $\Leftrightarrow \forall x \in \mathbb{N}^* (m \sigma x \wedge x \sigma m \Rightarrow m \sigma x)$

Se il minimo esiste è anche l'unico minimale. Dunque $m=1$ è minimale.

• **Massimale**: $M \in \mathbb{N}^*$ massimale $\Leftrightarrow \forall x \in \mathbb{N}^* (x \sigma M \wedge M \sigma x \Rightarrow x \sigma M)$.

Significa trovare un valore di M t.c. non esiste alcun $x \in \mathbb{N}^*$ per cui $M \sigma x$. In questo caso però non è possibile trovare massimali perché è sempre possibile trovare valori maggiori aumentando gli esponenti dei fattori.

Lavoriamo ora sul p.

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

$$m \leq x \Leftrightarrow (\forall p \in P (p^{\frac{m}{f_p(x)}} / x) \wedge (m = b \vee f(m) < f(x)))$$

$f_p(m)$ è il massimo esponente di p che divide m , per ogni p . L'unico valore possibile è 1, in quanto $p^{\frac{m}{f_p(1)}} / x$ e $f(1) < f(x)$ per ogni x .

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

Dato che passiamo sempre aumentare gli esponenti di p , non esiste alcun massimo.

• Minimale: $m \in \mathbb{N}^*$ è minimale $\Leftrightarrow \forall x \in \mathbb{N}^* (x \geq m \wedge m \leq x \Rightarrow m \leq x)$

Il minimo è l'unico minimale, dunque 1 è minimale.

• Massimale: $M \in \mathbb{N}^*$ massimale $\Leftrightarrow \forall x \in \mathbb{N}^* (x \geq M \wedge M \leq x \Rightarrow x \geq M)$

Per lo stesso discorso del massimo, non esiste alcun massimale.

(iii)

• (\mathbb{N}^*, σ) è un reticolo se $\forall x, y \in \mathbb{N}^* (\exists \inf_{(\mathbb{N}^*, \sigma)}(\{x, y\}), \exists \sup_{(\mathbb{N}^*, \sigma)}(\{x, y\}))$. Lo stesso vale per (\mathbb{N}^*, p) . Nessuno dei due è un reticolo perché non è possibile determinare l'estremo inferiore e superiore per ogni coppia di elementi.

(iv)

$$\begin{aligned} 3 &= 2^0 \cdot 3^1 \cdot 5^0 & f(3) &= 1 \\ 4 &= 2^2 \cdot 3^0 \cdot 5^0 & f(4) &= 2 \\ 10 &= 2^1 \cdot 3^0 \cdot 5^1 & f(10) &= 2 \\ 26 &= 2^1 \cdot 3^0 \cdot 5^0 & f(26) &= 1 \\ 49 &= 2^0 \cdot 3^0 \cdot 5^0 & f(49) &= 0 \\ 90 &= 2^1 \cdot 3^2 \cdot 5^1 & f(90) &= 4 \\ 660 &= 2^2 \cdot 3^1 \cdot 5^1 & f(660) &= 4 \\ 900 &= 2^{+2} \cdot 3^2 \cdot 5^2 & f(900) &= 6 \end{aligned}$$

Diagramma rispetto a σ

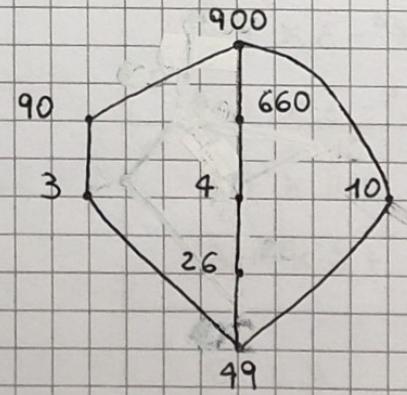
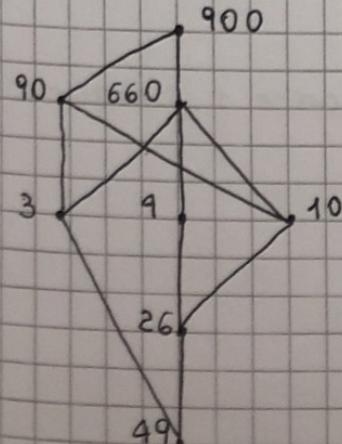


Diagramma rispetto a p



(v)

• In (\mathbb{N}^*, σ) sono 900 e 49

• In (\mathbb{N}^*, p) sono 900, 660, 90, 26, 49

(vi)

Analizzando i rispettivi diagrammi di Hasse vediamo che sia (X, σ) sia (X, ρ) non sono reticolati in quanto non è possibile per ogni coppia di elementi non confrontabili determinare l'estremo inferiore e superiore.

Esercizio 6

(i)

$$x^2 - 1 = (x+1)(x-1).$$

f_m è divisibile per $x^2 - 1$ se e solo se, per il teorema di Ruffini, 1 e -1 sono radici di f_m , ovvero se e solo se $f(1) = 0$ e $f(-1) = 0$.

$$f_1 = \overline{11} \quad f_{-1} = \overline{11} \Rightarrow f(1) \equiv_m 0 \Rightarrow \overline{11} \equiv_m 0.$$

Questo accade per ogni $m \in \{11, 22, 33, \dots\}$ ovvero $m = \{x \in \mathbb{N}^* \text{ t.c. } x = 11 \cdot h\}$.

(ii)

Fissato $m = 11$, dobbiamo dividere f_{11} per $x-1$ o $x+1$.

$$\begin{array}{r} 5x^4 + 3x^3 + x^2 - 3x + 5 \\ \hline -5x^4 - 5x^3 \\ \hline \end{array} \quad \begin{array}{r} x+1 \\ \hline 5x^3 - 2x^2 + 3x - 6 \\ \hline \end{array}$$
$$\begin{array}{r} 11 - 2x^3 + x^2 - 3x + 5 \\ \hline + 2x^3 + 2x^2 \\ \hline \end{array}$$
$$\begin{array}{r} 11 \quad \overline{3}x^2 - 3x + 5 \\ \hline - 3x^2 - 3x \\ \hline \end{array}$$
$$\begin{array}{r} 11 - 6x + 5 \\ \hline + 6x + 6 \\ \hline \end{array}$$
$$\begin{array}{r} 11 \quad 0 \\ \hline \end{array}$$

$\overline{5}x^3 - \overline{2}x^2 + \overline{3}x - \overline{6}$ è ancora un polinomio riducibile con radice 1. Dunque possiamo dividerlo per $x-1$.

$$\begin{array}{r}
 5x^3 - 2x^2 + 3x - 6 \\
 - 5x^3 + 5x^2 \\
 \hline
 // \quad 3x^2 + 3x - 6 \\
 - 3x^2 + 3x \\
 \hline
 // \quad 6x - 6 \\
 - 6x + 6 \\
 \hline
 // \quad 0
 \end{array}$$

Il polinomio $5x^3 + 3x + 6$ non ha radici, dunque è irriducibile.
Possiamo concludere dicendo che

$$f_{11} = (x+1)(x-1)(5x^2 + 3x + 6)$$

(iii)

Un polinomio è monico quando il coefficiente direttore è 1. Per f_{11} , abbiamo quindi risolvere la seguente equazione congruenziale: $5x^3 \equiv 1 \pmod{11}$. Il valore di x sarà 9. Otteniamo, moltiplicando 9 per f_{11} , ~~$5x^3 + 3x + 6$~~

$$x^4 + 5x^3 + 9x^2 - 5x + 1.$$

(iv)

Abbiamo visto che $f_{11} = (x+1)(x-1)(5x^2 + 3x + 6)$. Quest'ultimo non è monico, quindi troviamo il polinomio monico associato usando lo stesso ragionamento del punto precedente. Otteniamo così: $x^2 + 5x + 10$.

(v)

No, dato che $5x^2 + 3x + 6$ è di grado 2.

(vi)

No, dato che $5x^2 + 3x + 6$ è di grado 2 e $x-1$ e $x+1$ sono di grado 1.