

Το $(\mathbb{Z}, +)$ είναι αβελιανή ομάδα

Το σύνολο \mathbb{Z} είναι το μικρότερο σύνολο, που περιέχει το \mathbb{N} και έχει δομή αβελιανής ομάδας

ή

είναι το μικρότερο σύνολο το οποίο περιέχει το \mathbb{N} και τις λύσεις της εξίσωσης $x + p = 0$ όπου το $p \in \mathbb{Z}$.

Το σύνολο \mathbb{Z} είναι ένα σύνολο στοιχείων όπου έχουμε ορίσει την πράξη της πρόσθεσης

$$\mathbb{Z} \times \mathbb{Z} \ni (\alpha, \beta) \longrightarrow \alpha + \beta \in \mathbb{Z}$$

με τις ιδιότητες

A_1	$\alpha + \beta = \beta + \alpha$	αβελιανή ιδιότητα	} Ιδιότητες αβελιανής ομάδας
A_2	$\alpha + 0 = \alpha$	\exists ουδέτερο στοιχείο	
A_3	$\alpha + (-\alpha) = 0$	\exists αντίθετο στοιχείο	
A_4	$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$	προσεταιριστική ιδιότητα	

Αλλα σύνολα που έχουν την δομή μιας αβελιανής ομάδας:

\mathbb{Q} (ρητοί αριθμοί), \mathbb{R} (πραγματικοί αριθμοί), \mathbb{C} (μιγαδικοί αριθμοί), το σύνολο $\mathbb{Z} + \sqrt{2}\mathbb{Z}$, τα διανύσματα στο χώρο,

Σύνολο \mathbb{Z}_2

$$\begin{aligned}\bar{0} &= \{0, 2, 4, 6 \dots\} = \text{άρτιοι αριθμοί} \\ \bar{1} &= \{1, 3, 5, 7 \dots\} = \text{περιττοί αριθμοί}\end{aligned}$$

Το σύνολο $\mathbb{Z}_2 \equiv \{\bar{0}, \bar{1}\}$ είναι αβελιανή ομάδα.

$$\bar{0} + \bar{0} = \bar{0}$$

$$\bar{0} + \bar{1} = \bar{1} + \bar{0} = \bar{1}$$

$$\bar{1} + \bar{1} = \bar{0}$$

$$\rightsquigarrow a \neq 0 \Rightarrow a = -a$$

Εις άτοπον απαγωγή

Ορισμός ρητών αριθμών

Το \mathbb{Q} είναι ένα σύνολο που είναι 'κλειστό' ως προς την πρόσθεση και τον πολλαπλασιασμό και περιέχει το σύνολο των λύσεων της εξίσωσης $qx + p = 0$, όπου p και q στοιχεία του \mathbb{Z}

ή

$$\mathbb{Q} = \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\}$$

Απόδειξη “διά τῆς εἰς ἄτοπον ἀπαγωγῆς” / proof by contradiction

Για να αποδείξουμε την συνεπαγωγή των προτάσεων $P \Rightarrow Q$ αρκεί να αποδείξουμε ότι η υπόθεση $\{ P \text{ αληθής και } Q \text{ αναληθής} \}$ συνεπάγεται μια αντίφαση (“άτοπον”)

Παράδειγμα: Ο $\sqrt{2}$ δεν είναι ρητός αριθμός

Πεδίο / Σώμα - Field

Το $(\mathbb{F}, +)$ είναι αβελιανή ομάδα

A_1	$\alpha + \beta = \beta + \alpha$	αβελιανή ιδιότητα
A_2	$\alpha + 0 = \alpha$	\exists ουδέτερο
A_3	$\alpha + (-\alpha) = 0$	\exists αντίθετο
A_4	$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$	προσεταιριστικότητα

Το $(\mathbb{F} \setminus \{0\}, \cdot)$ είναι αβελιανή ομάδα

A_5	$\alpha \cdot \beta = \beta \cdot \alpha$	αβελιανή ιδιότητα
A_6	$\alpha \cdot 1 = \alpha$	\exists ουδέτερο
A_7	$\alpha \cdot (\alpha^{-1}) = 1$	\exists αντίθετο
A_8	$\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$	προσεταιριστικότητα

Η επιμεριστικότητα - distributivity συνδέει πρόσθεση και πολλαπλασιασμό

$$A_9 \quad (\alpha + \beta) \cdot \gamma = (\alpha \cdot \gamma) + (\beta \cdot \gamma)$$

Το πεδίο \mathbb{F} είναι χαρακτηριστικής n αν

$$\forall \alpha \in \mathbb{F}, \alpha \neq 0; \rightsquigarrow \alpha^n = 1$$

Ορισμός ρητών αριθμών

Το \mathbb{Q} είναι το μικρότερο πεδίο/σώμα χαρακτηριστικής 0, που περιέχει \mathbb{Z}

ή

Το \mathbb{Q} είναι το σύνολο των λύσεων της εξίσωσης $qx + p = 0$, όπου p και q στοιχεία του \mathbb{Z}

ή

$$\mathbb{Q} = \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\}$$

- $\sqrt{2} \notin \mathbb{Q}$ (απαγωγή σε άτοπο)
- Το σύνολο $\{a + b\sqrt{2} : a \text{ και } b \in \mathbb{Q}\}$
($\Rightarrow a^2 - 2b^2 \neq 0$) είναι πεδίο χαρακτηριστικής 0 (ευθεία απόδειξη)

$$(a + \sqrt{2}b) + (a' + \sqrt{2}b') = (a + a') + \sqrt{2}(b + b')$$

$$(a + \sqrt{2}b) \cdot (a' + \sqrt{2}b') = (aa' + 2bb') + \sqrt{2}(ab' + a'b)$$

$$(a + \sqrt{2}b)^{-1} = \frac{a}{a^2 - 2b^2} - \frac{\sqrt{2}b}{a^2 - 2b^2}$$

$$(a + b\sqrt{2})^n = 1 \rightsquigarrow n = 0$$

- Το σύνολο $\mathbb{Z}_2 \equiv \{\bar{0}, \bar{1}\}$ είναι πεδίο. Με χαρακτηριστική 1.

$\bar{0} + \bar{0} = \bar{0}$	$\bar{0} \cdot \bar{0} = \bar{0}$
$\bar{0} + \bar{1} = \bar{1} + \bar{0} = \bar{1}$	$\bar{0} \cdot \bar{1} = \bar{1} \cdot \bar{0} = \bar{0}$
$\bar{1} + \bar{1} = \bar{0}$	$\bar{1} \cdot \bar{1} = \bar{1}$

$$\rightsquigarrow \left\{ \begin{array}{l} a \neq 0 \Rightarrow a = -a \\ \Rightarrow a^1 = \bar{1} \end{array} \right\}$$

- Το σύνολο $\mathbb{Z}_3 \equiv \{\bar{0}, \bar{1}, \bar{2}\}$ είναι πεδίο. Με χαρακτηριστική 2.

$\bar{0} + \bar{0} = \bar{0}$	$\bar{0} \cdot \bar{0} = \bar{0}$
$\bar{0} + \bar{1} = \bar{1} + \bar{0} = \bar{1}$	$\bar{0} \cdot \bar{1} = \bar{1} \cdot \bar{0} = \bar{0}$
$\bar{1} + \bar{1} = \bar{2}$	$\bar{1} \cdot \bar{1} = \bar{1}$
$\bar{0} + \bar{2} = \bar{2} + \bar{0} = \bar{2}$	$\bar{0} \cdot \bar{2} = \bar{2} \cdot \bar{0} = \bar{0}$
$\bar{1} + \bar{2} = \bar{2} + \bar{1} = \bar{0}$	$\bar{1} \cdot \bar{2} = \bar{2} \cdot \bar{1} = \bar{2}$
$\bar{2} + \bar{2} = \bar{1}$	$\bar{2} \cdot \bar{2} = \bar{1}$

$$\rightsquigarrow \left\{ \begin{array}{l} a \neq 0 \Rightarrow a^2 = \bar{1} \\ -\bar{1} = \bar{2}, -\bar{2} = \bar{1}, \bar{2}^{-1} = \bar{2} \end{array} \right\}$$

$$\bar{2} + \bar{2} \cdot \bar{2}^{-1} - \bar{1} = \bar{2}$$

- Το σύνολο \mathbb{Z}_4 δεν είναι πεδίο. ($\bar{2} \cdot \bar{2} = \bar{0}$)

Παράδειγμα $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$$\bar{0} = \{0, 5, 10, 15, 20, \dots\}$$

$$\bar{1} = \{1, 6, 11, 16, 21, \dots\}$$

$$\bar{2} = \{2, 7, 12, 17, 22, \dots\}$$

$$\bar{3} = \{3, 8, 13, 18, 23, \dots\}$$

$$\bar{4} = \{4, 9, 14, 19, 24, \dots\}$$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Το \mathbb{Z}_5 είναι πεδίο/σώμα χαρακτηριστικής 4

$$(\bar{2} + \bar{4}) + \bar{3} = \bar{2} + (\bar{4} + \bar{3}), \quad -\bar{3} = \bar{2}, \quad (\bar{3})^{-1} = \bar{2}$$