# Εις άτοπον απαγωγή

**Απόδειξη "διά τῆς εἰς ἄτοπον απαγωγῆς"/ proof by contradiction**

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

$$\{P \Rightarrow Q \text{ αληθεύει}\} \equiv \{P \vee \neg Q \ \text{ δεν αληθεύει}\}$$

($\vee =$ και, $\neg Q =$ όχι $Q$ )

Παραδείγματα

{ Αν $n \in \mathbb{N}$ τότε $n \geq 1$} $\Leftrightarrow$ { Δεν υπάρχει φυσικός αριθμός μικρότερος από το $1$}

Αποδ: Εστω $\mathcal{K} =${ φυσικοί $< 1$} και Peano (v) $\rightsquigarrow M \backslash \mathcal{K} = \mathbb{N}$ άτοπο.

{ Αν $n \in \mathbb{N}$ και $n \geq 2$ } $\Rightarrow n - 1 \in \mathbb{N}$

Αποδ: Εστω $\mathcal{K} =${ το 1 και οι φυσικοί που έχουν προηγούμενο} και Peano (iii) και Peano (v) $\rightsquigarrow M \backslash \mathcal{K} = \mathbb{N}$ άτοπο.

# Αρχή Επαγωγής

## Απόδειξη με επαγωγή/ Proof by induction

Αν $P(m)$ είναι μια πρόταση η οποία εξαρτάται από το $m \in \mathbb{N}$

(i) $P(1)$ αληθεύει

(ii) για ένα $n \in \mathbb{N}$ η πρόταση $P(n)$ αληθεύει $\rightsquigarrow P(n+1)$ αληθεύει

συνεπάγεται ότι **η πρόταση $P(n)$ είναι αληθινή για κάθε $n \in \mathbb{N}$**

## Απόδειξη με επαγωγή/ Proof by induction

Αν $P(m)$ είναι μια πρόταση η οποία εξαρτάται από το $m \in \mathbb{N}$

(i) $P(1)$ αληθεύει

(ii) $\left\{ \begin{array}{c} \text{για ένα } n \in \mathbb{N} \\ \text{η πρόταση } P(k) \text{ αληθεύει} \\ \text{για } k = 1,\, 2,\, \ldots,\, n \end{array} \right\} \rightsquigarrow P(n+1)$ αληθεύει

συνεπάγεται ότι **η πρόταση $P(n)$ είναι αληθινή για κάθε $n \in \mathbb{N}$**

## Απόδειξη με επαγωγή/ Proof by induction

Αν $P(m)$ είναι μια πρόταση η οποία εξαρτάται από το $m \in \mathbb{N}$

(i) $P(1)$ αληθεύει

(ii) $\left\{ \begin{array}{c} \text{για ένα } n \in \mathbb{N} \\ \text{η πρόταση } P(k) \text{ αληθεύει} \\ \text{για } k = 1,\, 2,\, \ldots,\, n \end{array} \right\} \rightsquigarrow P(n+1)$ αληθεύει

συνεπάγεται ότι **η πρόταση $P(n)$ είναι αληθινή για κάθε $n \in \mathbb{N}$**

{ Μεταξύ των φυσικών αριθμών $n$ και $n+1$ δεν υπάρχει άλλος φυσικός αριθμός} $\leftrightsquigarrow$ { **Το σύνολο $\mathbb{N}$ δεν είναι πυκνό** }

# 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

$$\left.\begin{array}{lll} A_1 & \alpha + \beta = \beta + \alpha & \text{αβελιανή ιδιότητα} \\ A_2 & \alpha + 0 = \alpha & \exists \text{ ουδέτερο στοιχείο} \\ A_3 & \alpha + (-\alpha) = 0 & \exists \text{ αντίθετο στοιχείο} \\ A_4 & \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma & \text{προσεταιριστική ιδιότητα} \end{array}\right\} \begin{array}{c} \text{Ιδιότητες} \\ \text{αβελιανής} \\ \text{ομάδας} \end{array}$$

Αλλα σύνολα που έχουν την δομή μιας αβελιανής ομάδας:
$\mathbb{Q}$ (ρητοί αριθμοί), $\mathbb{R}$ (πραγματικοί αριθμοί), $\mathbb{C}$ (μιγαδικοί αριθμοί), διανύσματα στο χώρο

# Πεδίο/Σώμα - Field

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

$$\begin{array}{lll}
A_1 & \alpha + \beta = \beta + \alpha & \text{αβελιανή ιδιότητα} \\
A_2 & \alpha + 0 = \alpha & \exists\,\text{ουδέτερο} \\
A_3 & \alpha + (-\alpha) = 0 & \exists\,\text{αντίθετο} \\
A_4 & \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma & \text{προσεταιριστικότητα}
\end{array}$$

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

$$\begin{array}{lll}
A_5 & \alpha \cdot \beta = \beta \cdot \alpha & \text{αβελιανή ιδιότητα} \\
A_6 & \alpha \cdot 1 = \alpha & \exists\,\text{ουδέτερο} \\
A_7 & \alpha \cdot (\alpha^{-1}) = 1 & \exists\,\text{αντίθετο} \\
A_8 & \alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma & \text{προσεταιριστικότητα}
\end{array}$$

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

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

- $\sqrt{2} \notin Q$ (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)

$$\begin{aligned}
(\alpha + \sqrt{2}\beta) + (\alpha' + \sqrt{2}\beta') &= (\alpha + \alpha') + \sqrt{2}\,(\beta + \beta') \\
(\alpha + \sqrt{2}\beta) \cdot (\alpha' + \sqrt{2}\beta') &= (\alpha\alpha' + 2\beta\beta') + \sqrt{2}\,(\alpha\beta' + \alpha'\beta) \\
\left(\alpha + \sqrt{2}\beta\right)^{-1} &= \frac{\alpha}{\alpha^2 - 2\beta^2} - \frac{\sqrt{2}\beta}{\alpha^2 - 2\beta^2}
\end{aligned}$$

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

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

| | |
|---|---|
| $\overline{0}+\overline{0}=\overline{0}$ | $\overline{0}\cdot\overline{0}=\overline{0}$ |
| $\overline{0}+\overline{1}=\overline{1}+\overline{0}=\overline{1}$ | $\overline{0}\cdot\overline{1}=\overline{1}\cdot\overline{0}=\overline{0}$ |
| $\overline{1}+\overline{1}=\overline{0}$ | $\overline{1}\cdot\overline{1}=\overline{1}$ |

$$\rightsquigarrow \left\{ \begin{array}{ll} a \neq 0 & \Rightarrow a = -a \\ & \Rightarrow a^1 = \overline{1} \end{array} \right\}$$

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

| | |
|---|---|
| $\overline{0}+\overline{0}=\overline{0}$ | $\overline{0}\cdot\overline{0}=\overline{0}$ |
| $\overline{0}+\overline{1}=\overline{1}+\overline{0}=\overline{1}$ | $\overline{0}\cdot\overline{1}=\overline{1}\cdot\overline{0}=\overline{0}$ |
| $\overline{1}+\overline{1}=\overline{2}$ | $\overline{1}\cdot\overline{1}=\overline{1}$ |
| $\overline{0}+\overline{2}=\overline{2}+\overline{0}=\overline{2}$ | $\overline{0}\cdot\overline{2}=\overline{2}\cdot 0=\overline{0}$ |
| $\overline{1}+\overline{2}=\overline{2}+\overline{1}=\overline{0}$ | $\overline{1}\cdot\overline{2}=\overline{2}\cdot\overline{1}=\overline{2}$ |
| $\overline{2}+\overline{2}=\overline{1}$ | $\overline{2}\cdot\overline{2}=\overline{1}$ |

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

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

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

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

$$\begin{aligned} \overline{0} &= \{0, 5, 10, 15, 20, \dots\} \\ \overline{1} &= \{1, 6, 11, 16, 21, \dots\} \\ \overline{2} &= \{2, 7, 12, 17, 22, \dots\} \\ \overline{3} &= \{3, 8, 13, 18, 23, \dots\} \\ \overline{4} &= \{4, 9, 14, 19, 24, \dots\} \end{aligned}$$

| $+$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $\overline{1}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ |
| $\overline{2}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ |
| $\overline{3}$ | $\overline{3}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{4}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ |

| $\cdot$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
|---|---|---|---|---|---|
| $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ | $\overline{0}$ |
| $\overline{1}$ | $\overline{0}$ | $\overline{1}$ | $\overline{2}$ | $\overline{3}$ | $\overline{4}$ |
| $\overline{2}$ | $\overline{0}$ | $\overline{2}$ | $\overline{4}$ | $\overline{1}$ | $\overline{3}$ |
| $\overline{3}$ | $\overline{0}$ | $\overline{3}$ | $\overline{1}$ | $\overline{4}$ | $\overline{2}$ |
| $\overline{4}$ | $\overline{0}$ | $\overline{4}$ | $\overline{3}$ | $\overline{2}$ | $\overline{1}$ |

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

$$\left(\overline{2} + \overline{4}\right) + \overline{3} = \overline{2} + \left(\overline{4} + \overline{3}\right), \; -\overline{3} = \overline{2}, \; \left(\overline{3}\right)^{-1} = \overline{2}$$

Ορισμός:

Το σύνολο $\mathbb{X}$ είναι $\boxed{\text{ολικά διατεταγμένο}}$ αν $\exists$ μια $\boxed{\text{σχέση διάταξης}}$ $\leq$

$A_{10}$ $\forall x \;\; y \in : \mathbb{X} \;\Rightarrow\; x \leq y$ ή $y \leq x$

$A_{11}$ $\forall x \;\rightsquigarrow\; x \leq x$ $\boxed{\text{αυτοπαθής}}$ ιδιότητα

$A_{12}$ $x \leq y$ και $y \leq x \;\rightsquigarrow\; x = y$ $\boxed{\text{(αντι)συμμετρική}}$ ιδιότητα

$A_{13}$ $x \leq y$ και $y \leq z; \rightsquigarrow\; x \leq z$ $\boxed{\text{μεταβατική}}$ ιδιότητα

Παραδείγματα:

- Τα $\mathbb{Q}$ και $\mathbb{Z}$ είναι ολικά διατεταγμένα σύνολα
- Το $\mathbb{X} = \{(m, n) \;:\; m, n \in \mathbb{N}\}$ με την σχέση διάταξης

$$(m, n) \preceq (m', n') \;\Leftrightarrow m \leq m' \;\text{ και }\; n \leq n'$$

  δεν είναι ολικά διατεταγμένο.
- $\mathbb{X} =$ Ελληνικές λέξεις στο λεξικό, είναι ολικά διατεταγμένο σύνολο.

Ορισμός:

Το πεδίο $\mathbb{F}$, που είναι ολικά διατεταγμένο ονομάζεται διατεταγμένο πεδίο αν

$A_{14}$ $x \leq y \rightsquigarrow x + z \leq y + z$

$A_{15}$ $0 \leq x$ και $0 \leq y \rightsquigarrow 0 \leq x \cdot y$

Παραδείγματα:

- Το $\mathbb{Q}$ είναι ένα ολικά διατεταγμένο πεδίο.
- Το $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ είναι μη διατεταγμένο.
  (τα πεπερασμένα πεδία $\boxed{\text{δεν}}$ είναι ολικά διατεταγμένα !)

## ΑΞΙΩΜΑΤΑ $\mathbb{R}$

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

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

| | | |
|---|---|---|
| $(A_9)$ | $(\alpha+\beta)\cdot\gamma=(\alpha\cdot\gamma)+(\beta\cdot\gamma)$ | επιμεριστικότητα |

| | | |
|---|---|---|
| $(A_{10})$ | $\forall x, y \in: \mathbb{R} \Rightarrow x\le y$ ή $y\le x$ | |
| $(A_{11})$ | $\forall x \rightsquigarrow x\le x$ | αυτοπαθής ιδιότητα |
| $(A_{12})$ | $x\le y$ και $y\le x; \rightsquigarrow x=y$ | αντισυμμετρική ιδιότητα |
| $(A_{13})$ | $x\le y$ και $y\le z; \rightsquigarrow x\le z$ | μεταβατική ιδιότητα |

| | |
|---|---|
| $(A_{14})$ | $x\le y \rightsquigarrow x+z\le y+z$ |
| $(A_{15})$ | $0\le x$ και $0\le y \rightsquigarrow 0\le x\cdot y$ |

**Παρατήρηση**

Ολες αυτές οι ιδιότητες είναι κοινές και για το $\mathbb{Q}$ και για το $\mathbb{R}$