(I) $\mathbb{N} = \{1, 2, 3, 4, \dots\}$: το σύνολο των φυσικών αριθμών

Πράξη : πρόσθεση φυσικών αριθμών

1) • $n, m \in \mathbb{N} \Longrightarrow n+m \in \mathbb{N}$ ✓

2) • $n, m, k \in \mathbb{N} \Longrightarrow n+(m+k) = (n+m)+k$ ✓

• Δεν υπάρχει $n_0 \in \mathbb{N}$ ώστε $n+n_0 = n = n_0+n$, $\forall n \in \mathbb{N}$

Αν όμως θεωρήσουμε το $\mathbb{N}_0 = \{0, 1, 2, 3, 4, \dots\}$ με την πράξη της πρόσθεσης, ισχύουν οι 1), 2) και επίσης υπάρχει το $0 \in \mathbb{N}_0$ ώστε

• $n+0 = n = 0+n$, $\forall n \in \mathbb{N}_0$

Όμως δεν υπάρχει ο αντίθετος (αντίστροφος) στο $\mathbb{N}_0$. Δηλαδή, αν $n \in \mathbb{N}_0$, $n \geq 1$ τότε δεν υπάρχει $m \in \mathbb{N}_0$ ώστε: $n+m = 0 = m+n$.

Πράγματι, αν υπήρχε, θα έπρεπε

$$m = -n \notin \mathbb{N}_0$$

Ομοίως, αν "δούμε" τα $\mathbb{N}$ και $\mathbb{N}_0$ με την πράξη του πολλαπλασιασμού, πάλι βλέπουμε ότι η ιδιότητα 4) του "αντίστροφου" (ή "αντίθετου") δεν ικανοποιείται.

. Ας το δούμε για το $\mathbb{N}_0$

1) $n, m \in \mathbb{N}_0 \Longrightarrow n \cdot m \in \mathbb{N}_0$

2) $n, m, k \in \mathbb{N}_0 \Longrightarrow n \cdot (m \cdot k) = (n \cdot m) \cdot k$

3) $(\exists 1 \in \mathbb{N}_0)(\forall n \in \mathbb{N}_0) : n \cdot 1 = n = 1 \cdot n$

Όμως, το $0 \in \mathbb{N}_0$ δεν "αντιστρέφεται" διότι

$0 \cdot n = 0 \neq 1, \forall n \in \mathbb{N}_0$

Για την ακρίβεια, κανένα $n \in \mathbb{N}_0$ δεν "αντιστρέφεται".

(II) $\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$

↳ το σύνολο των ακεραίων αριθμών

Πράξη: πρόσθεση ακεραίων αριθμών

1) $n, m \in \mathbb{Z} \Rightarrow n+m \in \mathbb{Z}$

2) $n, m, k \in \mathbb{Z} \Rightarrow n+(m+k) = (n+m)+k$ ✓

3) $(\exists 0 \in \mathbb{Z})(\forall n \in \mathbb{Z}),\ n+0 = n = 0+n$

4) $(\forall n \in \mathbb{Z})(\exists -n \in \mathbb{Z}),\ n+(-n) = 0 = (-n)+n$

Πράξη: πολλαπλασιασμός ακεραίων αριθμών

1) $n, m \in \mathbb{Z} \Rightarrow n \cdot m \in \mathbb{Z}$

2) $n, m, k \in \mathbb{Z} \Rightarrow n \cdot (m \cdot k) = (n \cdot m) \cdot k$

3) $(\exists 1 \in \mathbb{Z})(\forall n \in \mathbb{Z}),\ n \cdot 1 = n = 1 \cdot n$

Ωστόσο, τα μόνα στοιχεία που "αντιστρέφονται" είναι τα $-1, 1$.

(III) Αντιστοίχως μπορούμε να δούμε εύκολα ότι τα σύνολα $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$ με την πράξη της πρόσθεσης ρητών, πραγματικών και μιγαδικών αριθμών, αντιστοίχως, ικανοποιούν τις αντίστοιχες ιδιότητες 1)-4). Απ' την άλλη, αν στα σύνολα $\mathbb{Q}$, $\mathbb{R}$ και $\mathbb{C}$ θεωρήσουμε την πράξη του πολλαπλασιασμού τότε βλέπουμε ότι:

(στα ακόλουθα $\mathbb{F} = \mathbb{Q}, \mathbb{R}$ ή $\mathbb{C}$)

1) $x, y \in \mathbb{F} \Rightarrow x \cdot y \in \mathbb{F}$

2) $x, y, z \in \mathbb{F} \Rightarrow x \cdot (y \cdot z) = (x \cdot y) \cdot z$

3) $(\exists 1 \in \mathbb{F})(\forall x \in \mathbb{F}),\ x \cdot 1 = x = 1 \cdot x$

Όμως το $0 \in \mathbb{F}$ δεν έχει "αντίστροφο".

H/W: Να δείξετε ότι τα $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ και $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ ικανοποιούν τις ιδιότητες 1)-4).

Ορισμός: Μια **ομάδα** είναι ένα ζεύγος $(G, \cdot)$, όπου G είναι ένα μη-κενό σύνολο και $\cdot$ είναι μια δυαδική πράξη επί του G, δηλαδή μια απεικόνιση $\cdot : G \times G \longrightarrow G$

$$(a,b) \longmapsto \cdot(a,b) := a \cdot b$$

για την οποία ικανοποιούνται τα ακόλουθα:

1) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $\forall a,b,c \in G$

(προσεταιριστικότητα της πράξης $\cdot$)

2) $(\exists e \in G)(\forall a \in G)$, $a \cdot e = a = e \cdot a$

(ύπαρξη ουδέτερου στοιχείου)

3) $(\forall a \in G)(\exists a' \in G)$, $a \cdot a' = e = a' \cdot a$

(ύπαρξη αντίστροφου στοιχείου)

(ή αντίθετου)

Μια ομάδα $(G, \cdot)$ λέγεται **αβελιανή**, αν

$$a \cdot b = b \cdot a, \ \forall a,b \in G.$$

Λήμμα: Έστω $(G, \cdot)$ μια ομάδα.

i) Μοναδικότητα ουδέτερου στοιχείου:
Αν $e, e' \in G$ είναι δύο ουδέτερα στοιχεία της G, δηλαδή ικανοποιούν την ιδιότητα 2) του ορισμού της ομάδας, τότε $e = e'$.

ii) Μοναδικότητα αντίστροφων (ή αντίθετων) στοιχείων:
Αν $a \in G$ και $a', a'' \in G$ είναι δύο αντίστροφα του a, δηλαδή ικανοποιούν την ιδιότητα 3) του ορισμού της ομάδας, τότε $a' = a''$.

Απόδειξη

i) Ισχύουν: $\begin{cases} e \cdot a = a = a \cdot e, \ \forall a \in G & (*) \\ e' \cdot a = a = a \cdot e', \ \forall a \in G & (**) \end{cases}$

Άρα: $e' \underset{a = e'}{\overset{(*)}{=}} e \cdot e' \underset{a = e}{\overset{(**)}{=}} e$.

ii) Ισχύουν: $\begin{cases} a \cdot a' = e = a' \cdot a & (*) \\ a \cdot a'' = e = a'' \cdot a & (**) \end{cases}$

Τότε: $a'' = a'' \cdot e \overset{(*)}{=} a''(a \cdot a')$

$= (a''a) \cdot a'$

$\overset{(**)}{=} e \cdot a'$

$= a'$ ∎

Παραδείγματα Ομάδων

(I) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ και $(\mathbb{C}, +)$

Σε όλες το ουδέτερο στοιχείο είναι το 0

(Στο $\mathbb{C}$: $0 = 0 + 0i$) [Αβελιανές ομάδες]

Για $x \in \mathbb{Z}$ ή $\mathbb{Q}$ ή $\mathbb{R}$ το αντίθετο είναι το $-x$. Στο $\mathbb{C}$: $x = a + bi$

$-x = -a - bi$

(II) Αν X είναι μη-κενό σύνολο, τότε το σύνολο $S(X) = \{f : X \to X \mid f: \text{απεικόνιση 1-1 κ' επί}\}$ εφοδιασμένο με την πράξη της σύνθεσης απεικονίσεων είναι μια ομάδα με ουδέτερο

στοιχείο την ταυτοτική απεικόνιση Id_X και για κάθε $f \in S(X)$ το αντίστροφο στοιχείο είναι η απεικόνιση $f^{-1}: X \to X$ (η αντίστροφη της f).

Άσκηση: Η $(S(X), \circ)$ είναι αβελιανή αν-ν το X έχει το πολύ δύο στοιχεία.

Λύση: "$\Leftarrow$" Αν $|X| = 1$ τότε $S(X) = \{Id_X\}$ με

$Id_X \circ Id_X = Id_X = Id_X \circ Id_X$ ✓

Αν $|X| = 2$ τότε $X = \{x, y\}$ και άρα $S(X) = \{Id_X, \sigma\}$, όπου $\sigma: X \to X$, $\sigma(x) = y$, $\sigma(y) = x$

- $Id_X \circ \sigma = \sigma = \sigma \circ Id_X$ ✓
- $\sigma \circ \sigma = \sigma \circ \sigma$ ✓
- $Id_X \circ Id_X = Id_X = Id_X \circ Id_X$

"$\Rightarrow$" Ας υποθέσουμε ότι $|X| \geq 3$ και έστω $a, b, c \in X$ με $a \neq b \neq c$

Ορίζουμε $f: X \to X$ με $f(x) = \begin{cases} b, & x = a \\ a, & x = b \\ x, & x \in X \setminus \{a, b\} \end{cases}$

και $g: X \to X$ με $g(x) = \begin{cases} b, & x = a \\ c, & x = b \\ a, & x = c \\ x, & x \in X \setminus \{a, b, c\} \end{cases}$

Προφανώς f, g: 1-1 και επί, οπότε $f, g \in S(X)$.

Όμως $(f \circ g)(a) = f(g(a)) = f(b) = a$

$(g \circ f)(a) = g(f(a)) = g(b) = c \neq a$

δηλαδή $f \circ g \neq g \circ f$

και συνεπώς $(S(X), \circ)$ όχι αβελιανή.

(III) Τα ζεύγη $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ και $(\mathbb{C}^*, \cdot)$ είναι αβελιανές ομάδες. Οι $(\mathbb{Q}^*, \cdot)$ και $(\mathbb{R}^*, \cdot)$ έχουν ουδέτερο στοιχείο το 1 και για κάθε $x \in \mathbb{Q}^*$ ή $\mathbb{R}^*$ το αντίστροφο είναι το $\frac{1}{x} \in \mathbb{Q}^*$ ή $\mathbb{R}^*$.

Η $(\mathbb{C}^*, \cdot)$ έχει ουδέτερο το $1 = 1+0i$ και για κάθε $z = a+bi \in \mathbb{C}^*$ ισχύει:

$$z^{-1} = \frac{1}{z} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i \in \mathbb{C}^*$$

(IV) Αν $\mathbb{F} = \mathbb{Q}, \mathbb{R}$ ή $\mathbb{C}$ και $m, n \in \mathbb{N}$ τότε το σύνολο $\mathbb{M}_{m\times n}(\mathbb{F})$ των $m\times n$ - πινάκων με στοιχεία από το $\mathbb{F}$ με την πράξη την πρόσθεση πινάκων είναι μια αβελιανή ομάδα με ουδέτερο (μηδενικό) στοιχείο τον μηδενικό πίνακα

$$\mathbb{O} = \begin{bmatrix} 0 & 0 \dots & 0 \\ \vdots & & \\ 0 & 0 \dots & 0 \end{bmatrix}$$ και για κάθε $A = [a_{ij}] \in \mathbb{M}_{m\times n}(\mathbb{F})$

ο αντίστροφος (αντίθετος) πίνακας είναι ο

$$-A = [-a_{ij}] \in M_{m\times n}(\mathbb{F})$$

(V) Αντίθετα, όπως είδαμε, τα σύνολα $(\mathbb{N},\cdot)$, $(\mathbb{N}_0,\cdot)$, $(\mathbb{Z},\cdot)$, $(\mathbb{Q},\cdot)$ και $(\mathbb{R},\cdot)$, $(\mathbb{C},\cdot)$ δεν αποτελούν ομάδες.

	Ουδέτερο	Αντίστροφο
Προσθ. συμβολισμός $(G,+)$	0 = μηδενικό	$-x$ = αντίθετο
Πολ/κός συμβολισμός $(G,\cdot)$	e = ταυτοτικό	x^{-1} = αντίστροφο

- Έστω $(G,\cdot)$ μια ομάδα, $x\in G$ και $n\in\mathbb{Z}$.

Ορίζουμε $x^n = \begin{cases} \underbrace{x\cdot x\cdot\ldots\cdot x}_{n\text{-φορές}}, & n\in\mathbb{N} \\ e, & n=0 \\ \underbrace{x^{-1}\cdot x^{-1}\cdots x^{-1}}_{-n\text{ φορές}}, & n<0 \end{cases}$

Στην περίπτωση προσθετικής ομάδας $(G,+)$:

$$nx := \begin{cases} \underbrace{x+x+\dots+x}_{n\text{ φορές}}, & n\in\mathbb{N} \\ 0, & n=0 \\ \underbrace{(-x)+(-x)+\dots+(-x)}_{-n\text{ φορές}}, & n<0 \end{cases}$$

και αν $x,y\in G$: $x+(-y) := x-y$

Πρόταση

Έστω $(G,\cdot)$ $((G,+))$ μια ομάδα. Για κάθε $x\in G$ και κάθε $n,m\in\mathbb{Z}$ ισχύουν

(i) $x^{n+m} = x^n\cdot x^m$ $\quad((n+m)x = nx+mx)$

(ii) $(x^n)^m = x^{nm}$ $\quad(n(mx) = (nm)x)$

(iii) $(x^n)^{-1} = x^{-n} = (x^{-1})^n$ $\quad(-(nx) = (-n)x = n(-x))$

Επίσης, αν $y\in G$ και $xy=yx$ $(x+y=y+x)$

τότε: $(xy)^n = x^n y^n$ $\quad(n(x+y) = nx+ny)$.

Πρόταση

Έστω $(G, \cdot)$ μια ομάδα και $a, b, c \in G$. Τότε:

1. $\begin{cases} ab = ac \Rightarrow b = c \\ ba = ca \Rightarrow b = c \end{cases}$ (Νόμος Διαγραφής)

2. $(ab)^{-1} = b^{-1}a^{-1}$ και $(a^{-1})^{-1} = a$

Απόδειξη

1. Θα αποδείξουμε ότι αν $ab = ac$ τότε $b = c$.

Πράγματι, $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow$

$(a^{-1}a)b = (a^{-1}a)c \Rightarrow e \cdot b = e \cdot c \Rightarrow b = c$

. $ba = ca \Rightarrow b = c$ (Η/ΙΝ)

2. Ισχύει: $(ab)b^{-1}a^{-1} = abb^{-1}a^{-1} = a \cdot e \cdot a^{-1} = aa^{-1} = e$

$b^{-1}a^{-1}(ab) = b^{-1}a^{-1}ab = b^{-1}eb = b^{-1}b = e$

Λόγω μοναδικότητας των αντιστρόφων, έπεται ότι

$(ab)^{-1} = b^{-1}a^{-1}$.

Επίσης, από τη μοναδικότητα των αντιστρόφων και το γεγονός ότι $a a^{-1} = e = a^{-1} a$, έχουμε

$$(a^{-1})^{-1} = a$$

Ορισμός: Μια ομάδα $(G, \cdot)$ καλείται **πεπερασμένη ομάδα** αν το πλήθος των στοιχείων του συόλου G είναι πεπερασμένο, $|G| < \infty$. Διαφορετικά η $(G, \cdot)$ καλείται **άπειρη ομάδα**. Η τάξη της ομάδας $(G, \cdot)$ ορίζεται να είναι το πλήθος $|G|$ των στοιχείων του συόλου G όταν η ομάδα είναι πεπερασμένη. Αν η ομάδα είναι άπειρη γράφουμε $|G| = \infty$.

▶ Τα περισσότερα παραδείγματα ομάδων που είδαμε μέχρι στιγμής ήταν άπειρες ομάδες.

Είναι κάθε ομάδα άπειρη;

Απάντηση: Όχι. Μάλιστα, αργότερα θα δούμε ότι για κάθε $n \in \mathbb{N}$ υπάρχει ομάδα τάξης n.

① **Η τετριμμένη ομάδα:**

G: μονοσύνολο. Τότε $G = \{e\}$ με πράξη

$$e \cdot e = e = e \cdot e$$

② $|G| = 2$: $G = \{e, a\}$, $\cdot : G \times G \to G$

$$G \times G = \{(e,e), (e,a), (a,e), (a,a)\}$$

$e \cdot e = e$, $e \cdot a = a$, $a \cdot e = a$, $a \cdot a = ;$

Έστω $a \cdot a = a$. Τότε $a^{-1}(a \cdot a) = a^{-1} \cdot a \Rightarrow$

$(a^{-1}a)a = e \Rightarrow e \cdot a = e \Rightarrow a = e$, άτοπο.

Άρα, $a \cdot a = a^2 = e$

$\cdot$	e	a
e	e	a
a	a	e

← πίνακας πράξης.

↖ Κάθε στοιχείο εμφανίζεται ακριβώς μια φορά σε κάθε γραμμή και κάθε στήλη.

③ $|G|=3$, $G=\{e,a,b\}$, $\cdot : G\times G \to G$

$$G\times G = \begin{Bmatrix} (e,e), (e,a), (e,b) \\ (a,e), (a,a), (a,b) \\ (b,e), (b,a), (b,b) \end{Bmatrix}$$

$e\cdot e = e$, $e\cdot a = a$, $e\cdot b = b = b\cdot e$

$= a\cdot e$

Χρησιμοποιώντας το νόμο της διαγραφής αποκλείουμε τις περιπτώσεις: $a\cdot a = a^2 = a$

$a\cdot a = a^2 = e$

και $b^2 = b\cdot b = e$, $b^2 = b\cdot b = b$

Συνεπώς, $a^2 = b$ και $b^2 = a$

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

④ $|G| = 4$, $G = \{e, a, b, c\}$

Στην περίπτωση αυτή υπάρχουν δύο "διαφορετικές" ομάδες με πλήθος στοιχείων ίσο με 4. Παρουσιάζουμε τους αντίστοιχους πίνακες:

Α

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

← V_4: η ομάδα του Klein

αβελιανή και

$x^2 = e, \ \forall x \in G$

(βλέπε $\mathbb{Z}_2 \times \mathbb{Z}_2$)

Β

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

← αβελιανή

$G = \{e, b, b^2, b^3\}$

(κυκλική, βλέπε $\mathbb{Z}_4$)

Ασκήσεις

① Έστω $n \in \mathbb{N}$ και έστω το σύνολο

$$GL(n,\mathbb{R}) = \{ A \in M_n(\mathbb{R}) \mid \det(A) \neq 0 \}$$

Να αποδείξετε ότι το $GL(n,\mathbb{R})$ με την πράξη πολλαπλασιασμού πινάκων είναι ομάδα. Είναι άπειρη ή πεπερασμένη; Να δείξετε ότι:

$(GL(n,\mathbb{R}), \cdot)$: αβελιανή $\iff n = 1$

(Τα ίδια ισχύουν και για $GL(n,\mathbb{Q})$, $GL(n,\mathbb{C})$).

② $X \neq \emptyset$, $F(X,\mathbb{R}) = \{ f : X \to \mathbb{R} \mid f : \text{απεικόνιση} \}$

$\forall f, g \in F(X,\mathbb{R})$, $f+g, f \cdot g : X \to \mathbb{R}$ όπου

$(f+g)(x) := f(x) + g(x)$ και $(f \cdot g)(x) = f(x) g(x)$

Να αποδείξετε ότι

(i) $(F(X,\mathbb{R}), +)$: αβελιανή άπειρη ομάδα.

(ii) $(F(X,\mathbb{R}), \cdot)$: όχι ομάδα.

Υποομάδες

Ορισμός: Έστω $(G,\cdot)$ μια ομάδα και H ένα μη-κενό υποσύνολο του G. Το H λέγεται **υποομάδα** της $(G,\cdot)$ αν το H είναι ομάδα ως προς την πράξη της G. Τότε γράφουμε $H \leq G$. Αν $H \neq G$ τότε $H < G$.

Παρατήρηση: Για κάθε ομάδα $(G,\cdot)$ ισχύει $\{e\} \leq G$ και $G \leq G$.

Σχόλιο: Έστω $(G,\cdot)$ μια ομάδα και $H \leq G$. Το H με την πράξη $\cdot$ είναι ομάδα, άρα διαθέτει ουδέτερο στοιχείο $e_H \in H$ και ισχύει $x \cdot e_H = x = e_H \cdot x$, $\forall x \in H$. Επιπλέον για κάθε $x \in H$ υπάρχει το $x_H^{-1} \in H$ με

$$x \cdot x_H^{-1} = e_H = x_H^{-1} \cdot x$$

Λήμμα

Έστω $(G, \cdot)$ ομάδα με ουδέτερο στοιχείο e και έστω $H \leq G$. Τότε:

(i) $e_H = e$ (ii) $\forall x \in H: \; x_H^{-1} = x_G^{-1}$

Απόδειξη

(i) Ισχύουν $e_H \cdot e_H = e_H$ και $e_H \cdot e = e_H$, οπότε:

$e_H \cdot e_H = e_H \cdot e \xrightarrow[\text{διαγραφής στην } G]{\text{νόμος}} e_H = e$

(ii) Έστω $x \in H$. Από (i), $e_H = e$, άρα $x \cdot x_H^{-1} = e$. Επίσης, $x \cdot x_G^{-1} = e$ και συνεπώς

$x \cdot x_H^{-1} = x \cdot x_G^{-1} \xrightarrow[\text{διαγραφής στην } G]{\text{νόμος}} x_H^{-1} = x_G^{-1}$

■

Πρόταση

Αν $(G,\cdot)$ είναι ομάδα και $\emptyset \neq H \subseteq G$, τότε τα ακόλουθα ισοδυναμούν:

(1) $H \leq G$ (2) Το H είναι κλειστό στην πράξη $\cdot$ της G, $e \in H$ και $\forall a \in H,\ a^{-1} \in H$.

(3) $H \neq \emptyset$ και $ab^{-1} \in H,\ \forall a,b \in H$.

Απόδειξη

(1) $\Rightarrow$ (2) Έστω $H \leq G$. Εξ' ορισμού το H είναι ομάδα ως προς την πράξη $\cdot$ της G, άρα είναι κλειστό ως προς την πράξη. Επίσης, από το προηγούμενο λήμμα, $e = e_H \in H$ και για κάθε $a \in H$: $a^{-1} = a^{-1}_H \in H$.

(2) $\Rightarrow$ (3) Από υπόθεση, $e \in H$, άρα $H \neq \emptyset$. Έστω $a,b \in H$. Τότε λόγω (2), $b^{-1} \in H$ και επειδή H κλειστό στην πράξη $\cdot$ της G έχουμε $\left.\begin{matrix} a \in H \\ b^{-1} \in H \end{matrix}\right\} \Rightarrow ab^{-1} \in H$.

(3) $\Rightarrow$ (1) Επειδή $H \neq \emptyset$, υπάρχει $a \in H$.
Από (3), $aa^{-1} \in H \Rightarrow e \in H$. Επίσης, για
κάθε $x \in H$, ισχύει: $ex^{-1} = x^{-1} \in H$.
Έστω τώρα $x, y \in H$. Επειδή $x \in H, y^{-1} \in H$
έχουμε $x(y^{-1})^{-1} = xy \in H$. Συνεπώς, το H
είναι κλειστό στην πράξη $\cdot$ της G, η
πράξη $\cdot$ είναι προσεταιριστική επί των H,
υπάρχει το ουδέτερο στοιχείο $e \in H$ και
τέλος για κάθε $x \in H$ έχουμε $x^{-1} \in H$.
Άρα H ομάδα με την πράξη της G, που
σημαίνει ότι $H \leq G$.

∎

Σχόλιο: $(G,\cdot)$ ομάδα και $\emptyset \neq K \subseteq H \subseteq G$.

(1) $H \leq G$ και $K \leq H \Rightarrow K \leq G$

(2) $K \leq G$ και $H \leq G \Rightarrow K \leq H$.

Παραδείγματα

(I) $(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$

(II) Έστω η ομάδα $(\mathbb{Z},+)$ και έστω $n \in \mathbb{N}$.
Τότε $n\mathbb{Z} := \{ nx \in \mathbb{Z} \mid x \in \mathbb{Z} \} \leq \mathbb{Z}$

Απόδειξη: $0 = n \cdot 0 \Rightarrow 0 \in n\mathbb{Z}$. Επίσης

αν $nx, ny \in n\mathbb{Z}$ τότε:

$nx - ny = n(x-y) \in n\mathbb{Z}$.

(III) $\mathbb{T} = S^1 = \{ z \in \mathbb{C}^* \mid |z| = 1 \} \leq (\mathbb{C}^*, \cdot)$

Απόδειξη: $1 = 1 + 0i \in S^1$ διότι $|1| = 1$

Επίσης, αν $z, w \in S^1$ τότε:

$|zw^{-1}| = |z||w^{-1}| = |z||w|^{-1} = 1 \cdot 1^{-1} = 1$, οπότε

$zw^{-1} \in S^1$

(IV) (HW) $U_3 = \{ z \in \mathbb{C}^* \mid z^3 = 1 \} \leq (\mathbb{C}^*, \cdot)$

Μάλιστα, $U_3 \leq S^1 \leq (\mathbb{C}^*, \cdot)$. Να κάνετε τον πίνακα πολλαπλασιασμού της $(U_3, \cdot)$. Ποια ομάδα σας θυμίζει;

(V) $SL(n, \mathbb{R}) = \{ A \in M_n(\mathbb{R}) \mid \det(A) = 1 \} \leq GL(n, \mathbb{R})$

Αρχικά, αν $A \in SL(n, \mathbb{R})$ τότε $\det(A) = 1 \neq 0$, οπότε $A \in GL(n, \mathbb{R})$. Επομένως, $SL(n, \mathbb{R}) \subseteq GL(n, \mathbb{R})$.

Ισχύει $I_n \in SL(n, \mathbb{R})$ αφού $\det(I_n) = 1$.

Επιπλέον, αν $A, B \in SL(n, \mathbb{R})$ τότε:

$\det(AB^{-1}) = \det(A) \det(B^{-1}) = \det(A) (\det(B))^{-1} =$

$= 1 \cdot 1^{-1} = 1$, δηλαδή $AB^{-1} \in SL(n, \mathbb{R})$.

Άρα, $SL(n, \mathbb{R}) \leq GL(n, \mathbb{R})$. ∎

(VI) (Η/Ν) Να βρείτε όλες τις υποομάδες των ομάδων $(G,\cdot)$ με $|G| \leq 3$

(VII) Οι υποομάδες της ομάδας V_4 του Klein:

$V_4 = \{e, a, b, c\}$ όπου $a^2 = b^2 = c^2 = e$.

Πιθανές υποομάδες: $H_1 = \{e\}$ ✓ $H_2 = \{e, a\}$,
$H_3 = \{e, b\}$, $H_4 = \{e, c\}$, $H_5 = \{e, a, b\}$,
$H_6 = \{e, a, c\}$, $H_7 = \{e, b, c\}$, $H_8 = V_4$ ✓

· Οι H_2, H_3, H_4 είναι κλειστές στην πράξη της V_4 και κάθε στοιχείο των έχει αντίστροφο εντός των υποομάδων

$$\left[\begin{array}{c} e^{-1} = e \in H_2, H_3, H_4 \\ a^{-1} = a \in H_2,\ b^{-1} = b \in H_3 \\ c^{-1} = c \in H_4 \end{array}\right]$$

οπότε $H_2, H_3, H_4 \leq V_4$

Για H_5: $ab = c \notin H_5 \Rightarrow H_5 \nleq V_4$

H_6: $ac = b \notin H_6 \Rightarrow H_6 \nleq V_4$

H_7: $bc = a \notin H_7 \Rightarrow H_7 \nleq V_4$

Τελικά: $\{e\}, \{e, a\}, \{e, b\}, \{e, c\}$ και V_4

είναι όλες οι διακεκριμένες υποομάδες της ομάδας V_4 του Klein:

• Στην περίπτωση της $G=\{e,a,b,c\}$ με $G=\{e,b,b^2,b^3\}$ (2η ομάδα με 4 στοιχεία διαφορετική της V_4) εύκολα βλέπουμε ότι οι διακεκριμένες υποομάδες της είναι οι:

$\{e\}$, $\{e,b^2\}$ και G.

Πρόταση

Έστω $(G,\cdot)$ μια ομάδα και έστω $(H_i)_{i\in I}$ μια οικογένεια υποομάδων της G. Τότε η τομή $H=\bigcap_{i\in I} H_i$ είναι υποομάδα της G.

Απόδειξη: Εφ' όσον $H_i \leq G$, $\forall i\in I$ έχουμε: $e\in H_i$, $\forall i\in I$, οπότε $e\in \bigcap_{i\in I} H_i = H$.

Θεωρούμε τυχόντα στοιχεία $x,y\in H$.

Τότε $x, y \in H_i$, $\forall i \in I$ και επειδή $H_i \leq G$, $\forall i \in I$, προκύπτει ότι $xy^{-1} \in H_i$, $\forall i \in I$, που σημαίνει ότι $xy^{-1} \in \bigcap_{i \in I} H_i = H$. Συνεπώς $H \leq G$. ∎

Σχόλιο: Σε αντίθεση με την τομή υποομάδων, η ένωση υποομάδων μιας ομάδας δεν είναι απαραίτητα υποομάδα.

πχ: Θεωρούμε την ομάδα $V_4 = \{e, a, b, c\}$ του Klein. Όπως είδαμε, οι $H_1 = \{e, a\}$ και $H_2 = \{e, b\}$ είναι υποομάδες της V_4 αλλά η $H = H_1 \cup H_2 = \{e, a, b\}$ δεν είναι υποομάδα της V_4 καθώς $a, b \in H$ αλλά $ab = c \notin H$.

▶ Μια πολύ σημαντική κατηγορία υποομάδων είναι οι λεγόμενες κυκλικές υποομάδες.

Βασική Πρόταση

Έστω $(G,\cdot)$ μια ομάδα και $a \in G$. Τότε

(i) η $\langle a \rangle := \{a^k \in G \mid k \in \mathbb{Z}\} \subseteq G$ είναι μια υποομάδα της $(G,\cdot)$ και επιπλέον ισχύει ότι $\langle a \rangle = \langle a^{-1} \rangle$.

(ii) η $\langle a \rangle$ είναι η μικρότερη υποομάδα της $(G,\cdot)$ η οποία περιέχει το a.

Απόδειξη

(i) Ισχύει $e = a^0$, άρα $e \in \langle a \rangle$. Έστω $x, y \in \langle a \rangle$. Τότε $x = a^k$ και $y = a^\lambda$ για κάποιοι $k, \lambda \in \mathbb{Z}$ και συνεπώς:

$$xy^{-1} = a^k (a^\lambda)^{-1} = a^k a^{-\lambda} = a^{k-\lambda} \in \langle a \rangle$$

Άρα, $\langle a \rangle \leq G$

Επίσης: $\langle a^{-1} \rangle = \{(a^{-1})^k \in G \mid k \in \mathbb{Z}\} =$

$\{a^{-k} \in G \mid k \in \mathbb{Z}\} = \{a^\lambda \in G \mid \lambda \in \mathbb{Z}\} = \langle a \rangle$.

(ii) Όπως αποδείξαμε στο (i) έχουμε $\langle a\rangle \leq G$ με $a = a^1 \in \langle a\rangle$. Έστω $H \leq G$ με $a \in H$ και θα αποδείξουμε ότι $\langle a\rangle \leq H$. Πράγματι, έστω $x \in \langle a\rangle$. Τότε $x = a^k$ για κάποιο $k \in \mathbb{Z}$.

- Αν $k = 0$, τότε $x = a^0 = e \in H$
- Αν $k \in \mathbb{N}$, τότε επειδή $a \in H$ και $H \leq G$ έχουμε $x = a^k = \underbrace{a \cdot a \cdots a}_{k\text{-φορές}} \in H$.
- Αν $k < 0$, τότε επειδή $a \in H$ και $H \leq G$, ισχύει $a^{-1} \in H$, άρα: $x = a^k = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{-k\text{: φορές}} \in H$.

Σε κάθε περίπτωση, $x \in H$.

Επομένως, $\langle a\rangle \leq H$. ∎

Ορισμός: Έστω $(G, \cdot)$ μια ομάδα και $a \in G$. Η υποομάδα $\langle a \rangle$ της G καλείται η κυκλική υποομάδα της G η οποία παράγεται από το στοιχείο a.

Η $(G, \cdot)$ λέγεται κυκλική ομάδα αν υπάρχει $a \in G$ ώστε $G = \langle a \rangle$. Σε αυτή την περίπτωση το a καλείται γεννήτορας της κυκλικής ομάδας G.

Σχόλιο: Όταν η G είναι προσθετική και $a \in G$, τότε $\langle a \rangle = \{ na \in G \mid n \in \mathbb{Z} \}$

! Η ταξινόμηση των κυκλικών ομάδων θα γίνει αργότερα.