28/2/2018.

Υπενθύμιση από Θ. Αριθμών

Έστω $n\in\mathbb{Z}$ με $n\geq 2$. Ορίζουμε σχέση ισοδυναμίας $\sim_n$ στο $\mathbb{Z}$ ως εξής:

$a\sim_n b$, αν $a\equiv b \bmod n$, δηλ. $n|a-b$

Από Θ. Αριθμών $\sim_n$ ισοδυναμίας στο $\mathbb{Z}$.

Θέτουμε $\mathbb{Z}_n$ το σύνολο των κλάσεων ισοδυναμίας. Για $a\in\mathbb{Z}$ συμβολίζουμε $[a]_n\in\mathbb{Z}_n$ την αντίστοιχη κλάση

ΕΡΩΤΗΜΑ 1 Αν $a,b\in\mathbb{Z}$, τότε $[a]_n=[b]_n$

ΑΠΑΝΤΗΣΗ Αν και μόνο αν $n|a-b$.

π.χ. $[2]_5=[-3]_5$, ενώ $[1]_5\neq[-1]_5$

ΠΡΟΤΑΣΗ (Από Θεωρία Αριθμών)

Αν $a,a',b,b'\in\mathbb{Z}$ και $a\sim_n a'$, $b\sim_n b'$ τότε $a+b\sim_n a'+b'$ και $ab\sim_n a'b'$

Συμπέρασμα: Μπορούμε να ορίσουμε πράξεις

$+ : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

$\cdot : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$

ως εξής $[a]_n + [b]_n = [a+b]_n$

$[a]_n \cdot [b]_n = [ab]_n$

π.χ. $[9]_{12} + [5]_{12} = [14]_{12} = [2]_{12}$

Άρα έχουμε δύο πράξεις στο $\mathbb{Z}_n$: πρόσθεση και πολλαπλασιασμό.

ΠΡΟΤΑΣΗ (Από Θ. Αριθμών)

Το $\mathbb{Z}_n$ είναι πεπερασμένο σύνολο με ακριβώς n στοιχεία και ισχύει

$\mathbb{Z}_n = \{[0]_n, [1]_n, \dots, [n-1]_n\}$.

- - - - - - - - - - - - - -

ΠΙΝΑΚΑΣ ΜΙΑΣ ΠΡΑΞΗΣ

Ορισμός: Έστω (S, ϕ) σύνολο με πράξη, ώστε S πεπερασμένο σύνολο με $|S| = n$

δηλ. $S = \{s_1, s_2, \dots, s_n\}$ με $s_i \neq s_j$ για $i \neq j$

($|S|$ = αριθμός στοιχείων του S)

Ο πίνακας της πράξης ϕ στο S είναι ο (με στοιχεία στο S) πίνακας $n \times n$

Υπενθύμιση: $x \phi y = \phi(x, y)$

	s_1	s_2	s_3	$\dots$	s_n
s_1	$s_1 \phi s_1$	$s_1 \phi s_2$	$s_1 \phi s_3$	$\dots$	$s_1 \phi s_n$
s_2	$s_2 \phi s_1$	$s_2 \phi s_2$	$s_2 \phi s_3$		$s_2 \phi s_n$
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$
s_n	$s_n \phi s_1$	$s_n \phi s_2$	$s_n \phi s_3$	$\dots$	$s_n \phi s_n$.

ΠΑΡΑΔΕΙΓΜΑ $(\mathbb{Z}_3, \cdot)$ Θα βρούμε τον πίνακα της πράξης.

$$\mathbb{Z}_3 = \{ s_1 = [0]_3, s_2 = [1]_3, s_3 = [2]_3 \}$$

	$[0]_3$	$[1]_3$	$[2]_3$
$[0]_3$	$[0]_3$	$[0]_3$	$[0]_3$
$[1]_3$	$[0]_3$	$[1]_3$	$[2]_3$
$[2]_3$	$[0]_3$	$[2]_3$	$[4]_3 = [1]_3$

ΠΑΡΑΤΗΡΗΣΕΙΣ

1) Η πράξη ϕ στο $\{s_1, \ldots, s_n\}$ είναι μεταθετική δηλ. $s_i \phi s_j = s_j \phi s_i$, αν και μόνο αν ο πίνακας της πράξης ϕ είναι συμμετρικός ως προς την διαγώνιο, γιατί (i,j) στοιχείο του πίνακα είναι το $\phi(s_i, s_j)$, ενώ το (j,i) είναι το $s_j \phi s_i$

Δηλαδή ο πίνακας μας λέει αμέσως αν η πράξη είναι μεταθετική ή όχι.

2) Το στοιχείο s_i (για κάποιο i) είναι ουδέτερο στοιχείο της (S, ϕ) αν και μόνο αν η i-γραμμή του πίνακα είναι $s_1, s_2, \ldots, s_n$ ΚΑΙ η i-στήλη του πίνακα είναι
s_1
s_2
$\vdots$
s_n

3) Υποθέτουμε s_i ουδέτερο στοιχείο. Τότε το στοιχείο s_k αναστρέψιμο αν και μόνο αν υπάρχει j ώστε τα (k,j) και (j,k) στοιχεία του πίνακα είναι ίσα με s_i.

Στο παράδειγμα ο πίνακας μας λέει S_3 είναι αντίστροφο του S_3.

4) <u>ΠΡΟΣΟΧΗ</u> : Ο πίνακας πράξης δεν βοηθάει πολύ στο να αποφανθούμε αν η πράξη είναι προσεταιριστική ή όχι.

<u>Υπενθύμιση</u> Το ζεύγος (S, ϕ) όπου S μη κενό σύνολο και ϕ πράξη στο S λέγεται ΟΜΑΔΑ αν η ϕ είναι προσεταιριστική, έχει ουδέτερο στοιχείο και κάθε στοιχείο της S αντιστρέφεται.

<u>ΣΥΜΒΟΛΙΣΜΟΣ</u> : Συνήθως θα συμβολίζουμε μια ομάδα με G την πράξη με $\cdot$ (που κάποιες φορές θα παραλείπεται) το ουδέτερο στοιχείο με e και το αντίστροφο στοιχείο του a με a^{-1}.
Κάποιες φορές θα συμβολίζουμε την πράξη με $+$ το ουδέτερο στοιχείο με 0, και το αντίστροφο στοιχείο του a με $-a$.

<u>ΠΑΡΑΔΕΙΓΜΑΤΑ</u>

1) $(\mathbb{Z}, +)$ όπου $+$ η συνηθισμένη πρόσθεση στους ακεραίους είναι ομάδα με ουδέτερο το 0 και αντίστροφο ως προς $+$ του $a \in \mathbb{Z}$ το $-a \in \mathbb{Z}$

2) Ομοίως $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ είναι ομάδες και μάλιστα μεταθετικές.

3) Έστω $n \geq 2$. Τότε το $(\mathbb{Z}_n, +)$ είναι επίσης μεταθετική ομάδα.

4) Έστω $G = \{e\}$ με πράξη $e \cdot e = e$. Τότε η G είναι ομάδα με ένα στοιχείο. και πίνακα

	e
e	e

Από 3) το $(\mathbb{Z}_2,+)$ είναι ομάδα με δύο στοιχεία και πίνακα πράξης

	$[0]_2$	$[1]_2$
$[0]_2$	$[0]_2$	$[1]_2$
$[1]_2$	$[1]_2$	$[2]_2=[0]_2$

ΕΡΩΤΗΜΑ Στο $\mathbb{Z}_2$ ποιο είναι το αντίθετο ως προς + του $[1]_2$ Απάντηση: $[1]_2$.

Μια άλλη ομάδα με 2 στοιχεία είναι $G=\{1,-1\}\subseteq\mathbb{R}$ με πράξη τον συνηθισμένο πολλαπλασιασμό στο $\mathbb{R}$. Ο πίνακας είναι:

	1	-1
1	1	-1
-1	-1	1

Άρα το αντίστροφο του -1 ως προς τον · είναι το -1

Θα δούμε ότι οι ομάδες $(\mathbb{Z}_2,+)$ και $(\{1,-1\},\cdot)$ είναι "ισόμορφες".

Παρατήρηση Αν $n\geq 2$ η $(\mathbb{Z}_n,+)$ είναι ομάδα μεταθετική με n στοιχεία.

5) Έστω V διαν. χώρος επί του σώματος $\mathbb{F}$ π.χ. $(\mathbb{F}=\mathbb{R})$ Τότε από τα αξιώματα διαν. χώρων το $(V,+)$ είναι ομάδα (και μάλιστα μεταθετική)

Άρα π.χ. $(\mathbb{R}^n,+)$, $(\mathbb{R}^{\nu\times\nu},+)$ $\mathbb{R}_d[x]=\{$πολυώνυμα επί του $\mathbb{R}$ βαθμού $\leq d\}$

$(\mathbb{R}_d[x],+)$ αβελιανές ομάδες.

6. Τα ζεύγη $(\mathbb{Q}\setminus\{0\},\cdot)$, $(\mathbb{R}\setminus\{0\},\cdot)$ είναι αβελιανές ομάδες.

7. <u>ΠΡΟΣΟΧΗ</u> Το ζεύγος $(\mathbb{Q}, \cdot)$ δεν είναι ομάδα.

<u>ΑΠΟΔΕΙΞΗ</u> Το $(\mathbb{Q}, \cdot)$ έχει ουδέτερο το 1. Το $0 \in \mathbb{Q}$ δεν έχει αντίστροφο ως προς $\cdot$, γιατί $0 \cdot a = 0 \neq 1$ για κάθε $a \in \mathbb{Q}$.

Ομοίως, το $(\mathbb{R}, \cdot)$ δεν είναι ομάδα.

8. Θέτουμε $\mathbb{R}_{>0} = \{a \in \mathbb{R} : a > 0\}$

Αν $a, b \in \mathbb{R}_{>0}$ τότε $ab > 0$. Επομένως $(\mathbb{R}_{>0}, \cdot)$ πράξη. Είναι ομάδα;

Προσεταιριστικότητα: Ναι, γιατί ο πολλαπλ. στο $\mathbb{R}$ είναι προσεταιριστικός.

Υπάρχει ουδέτερο: Ναι, το 1.

Έχει κάθε στοιχείο αντίστροφο; Ναι, γιατί αν $a \in \mathbb{R}_{>0}$ τότε και το $\frac{1}{a} \in \mathbb{R}_{>0}$

Άρα $(\mathbb{R}_{>0}, \cdot)$ ομάδα και μάλιστα αβελιανή.

9. Έστω $n \geq 2$. Θέτουμε $GL_n(\mathbb{R}) = \{A \in \mathbb{R}^{\nu \times \nu} : A \text{ αντιστρέψιμος}\}$

General Linear

<u>ΙΣΧΥΡΙΣΜΟΣ 1.</u> Αν $A, B \in GL_n(\mathbb{R})$ τότε $AB \in GL_n(\mathbb{R})$

<u>Απόδ.</u> ΠΡΑΓΜΑΤΙ Θέτουμε $C = B^{-1} \cdot A^{-1}$. Τότε $(AB)C = (AB)(B^{-1} \cdot A^{-1})$

$$= A \cdot (B \cdot B^{-1}) \cdot A^{-1} = A \cdot I_n \cdot A^{-1} = A \cdot A^{-1} = I_n.$$

$$C(AB) = (B^{-1} \cdot A^{-1}) \cdot (AB) = B^{-1} \cdot (A^{-1} \cdot A) \cdot B = B^{-1} \cdot I_n \cdot B = B^{-1} \cdot B = I_n.$$

Επομένως το ζεύγος $(GL_n(\mathbb{R}), \cdot)$ είναι σύνολο με πράξη.

<u>ΙΣΧΥΡΙΣΜΟΣ 2</u> G ΟΜΑΔΑ

<u>ΑΠΟΔ.</u> Προσεταιριστικότητα; Ναι, γιατί πολλαπλ. πινάκων είναι προσεταιριστικός.

Ουδέτερο στοιχείο; Ναι, γιατί το $I_n \in GL_n(\mathbb{R})$

Έστω $A \in GL_n(\mathbb{R})$. Φανερά $A^{-1} \in GL_n(\mathbb{R})$

Άρα G ομάδα.

<u>ΙΣΧΥΡΙΣΜΟΣ 3.</u> Για κάθε $n \geq 2$ η $(GL_n(\mathbb{R}), \cdot)$

είναι ομάδα ΜΗ ΜΕΤΑΘΕΤΙΚΗ.

<u>ΠΡΟΤΑΣΗ</u> Για $n=2$ Έστω $A = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$ $B = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$

Τότε $AB = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ $BA = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq AB$

Θέτουμε $A' = I_2 + A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = I_2 + B = \begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$

Φανερά $A', B' \in GL_n(\mathbb{R})$

$A'B' - B'A' = (I_2 + A)(I_2 + B) - (I_2 + B)(I_2 + A) =$

$(I_2 + A + B + AB) - (I_2 + B - A + AB) = BA - AB \neq O_{2\times 2}$

Άρα G όχι μεταθετική

Έστω $n \geq 3$ Θέτουμε $\tilde{A} = \begin{bmatrix} 1 & 1 & \cdots & 0 \\ & 1 & & \\ 0 & & \ddots & 1 \end{bmatrix} = \begin{bmatrix} A' & 0 \\ 0 & I_{n-2} \end{bmatrix}$

$\tilde{B} = \begin{bmatrix} 2 & & 0 \\ & 1 & \\ & & 1 \\ 0 & & \ddots & 1 \end{bmatrix}$

Τότε $\tilde{A}, \tilde{B} \in GL_n(\mathbb{R})$ και εύκολα βλέπουμε $\tilde{A}\tilde{B} \neq \tilde{B}\tilde{A}$