Αλγεβρικές Δομές 26/2/2018

1ο μάθημα

Ομάδα: η πιο απλή αλγεβρική δομή και έχουμε μόνο 1 πράξη $\rightarrow \begin{pmatrix} +, - \\ \cdot, / \end{pmatrix}$

Δακτύλιος $\rightarrow (+, -, \cdot)$

Σώμα $\rightarrow (+, -, \cdot, /)$

• Ορισμός: Ομάδα $(G, *)$ είναι ένα σύνολο G μαζί με μια (διμελή) πράξη $\begin{pmatrix} G \times G \rightarrow G \\ (a, b) \rightarrow a*b \end{pmatrix}$ τέτοια ώστε να ισχύουν τα ακόλουθα αξιώματα.

1) Η πράξη είναι προσεταιριστική
δηλ. $\forall a, b, \gamma \in G$: $a*(b*\gamma) = (a*b)*\gamma$

2) Υπάρχει ένα στοιχείο $e \in G$ τέτοιο ώστε
$a*e = e*a = a \quad \forall a \in G$

3) Για κάθε $a \in G$, υπάρχει $a' \in G$ τ.ω.
$a'*a = a*a' = e$
(a' αντίστροφο του a)

• Παραδείγματα:

- $(\mathbb{N}, +)$ δεν είναι ομάδα γιατί δεν έχει ουδέτερο στοιχείο (το μηδέν)

- $(\mathbb{N}_0, +)$ $n \in \mathbb{N}$ $n+0 = 0+n = n$
αλλά τα στοιχεία του $\mathbb{N}_0$ δεν έχουν αντίστροφο άρα δεν είναι ομάδα.

! Το κενό σύνολο δεν είναι ποτέ ομάδα.

- $(\mathbb{Z},+)$ 1) ισχύει η προσετ.
  2) έχει ουδέτερο το 0.
  3) έχει αντίθετο

  Άρα $(\mathbb{Z},+) \to$ ομάδα.

- $(\mathbb{Z},\cdot)$ 1) ισχύει προσετ. $(a\cdot b)\cdot \gamma = a\cdot(b\cdot\gamma)$
  2) έχει ουδέτερο το 1 $(n\cdot 1 = 1\cdot n = n)$
  3) δεν έχει αντίστροφο (τα μόνα στοιχεία που έχουν αντιστρ. : 1, -1)

  Άρα δεν είναι ομάδα

- $(\mathbb{Q},+) \to$ ομάδα
- $(\mathbb{Q},\cdot) \to$ όχι ομάδα

- $(\mathbb{Q}^*,\cdot) \to$ ομάδα με $\mathbb{Q}^* = \mathbb{Q}-0$

- $(\mathbb{Q}^*,\odot)$ με $a\odot b = \frac{a\cdot b}{2}$ είναι ομάδα;

1) $a\odot(b\odot\gamma) = a\odot\left(\frac{b\cdot\gamma}{2}\right) = \frac{a\cdot\frac{b\cdot\gamma}{2}}{2} = \frac{ab\gamma}{4}$

$(a\odot b)\odot\gamma = \left(\frac{a\cdot b}{2}\right)\odot\gamma = \frac{\frac{a\cdot b}{2}\cdot\gamma}{2} = \frac{ab\gamma}{4}$

Άρα ισχύει η προσετ.

2) $a\odot\boxed{2} = \boxed{2}\odot a = a$.

Άρα ουδέτερο στοιχείο το 2.

3) Έστω $a\in\mathbb{Q}^*$. $a\odot\boxed{\frac{4}{a}} = \boxed{\frac{4}{a}}\odot a = 2$

Άρα υπάρχει αντίστροφο και $(\mathbb{Q}^*,\odot) \to$ ομάδα

Παράδειγμα:

Έστω $(V, K, +, \cdot)$ ένας K-διανυσματικός χώρος, τότε:

περιορίζομαι στο $(V,+)$

- $\forall \vec{a}, \vec{b}, \vec{\gamma} \in V$ ισχύει $\vec{a}+(\vec{b}+\vec{\gamma}) = (\vec{a}+\vec{b})+\vec{\gamma}$
- υπάρχει $0+\vec{a} = \vec{a}+0 = a$
- $(\forall \vec{a} \in V)\ (\exists (-\vec{a}) \in V)$ τέτοιο ώστε $\vec{a}+(-\vec{a}) = \vec{0}$

ιδιότητες διαν. χώρου

Άρα το $(V,+)$ είναι ομάδα.

Για το $(V,\cdot)$ δεν ισχύει γιατί έχω βαθμωτό πολ/σμό, άρα δεν είναι ομάδα.

Με πρόσθεση:

$(K^n,+)$ $(\mathbb{R}^n,+)$ $(\mathbb{C}^n,+)$ → ομάδες (n-άδες αριθμών)

$K^{m\times n} = M_{m\times n}(K)$
$\mathbb{R}^{m\times n} = M_{m\times n}(\mathbb{R})$
} (σύνολα πινάκων) → αποτελούν ομάδες

$\mathbb{R}_n[x]$ (σύνολο πολυωνύμων το πολύ βαθμού n) → ομάδες.

<u>Ας δούμε για πολ/σμό</u>

$(M_{m\times m}(\mathbb{R}) = \mathbb{R}^{m\times n}, \cdot)$ → πολ/σμός πινάκων (μόνο σε τετραγωνικούς)

Είναι ομάδα;

1) $A, B, \Gamma \in M_{m\times m}(\mathbb{R})$ $(A\cdot B)\cdot\Gamma = A(B\cdot\Gamma)$ ισχύει η προσετ.
2) $A\cdot \boxed{I_n} = \boxed{I_n}\cdot A = A$ έχει ουδέτερο στοιχείο
3) $A\cdot \boxed{} = \boxed{}\, A = I_n$ (ο μηδενικός πίνακας δεν έχει αντίστροφο άρα δεν ισχύει η ιδιότητα)

Συνεπώς, δεν είναι ομάδα.

- $(GL(m,\mathbb{R}),\cdot)$

$(GL(m,\mathbb{R}),\cdot) = \{A \in \mathbb{R}^{m\times m} \mid \det A \neq 0\}$ δηλ. υπάρχει αντίστροφος.

και εφόσον είναι υποσύνολο του προηγούμενου συνόλου και υπάρχει και αντίστροφο στοιχείο, είναι ομάδα

- $(GL(m,\mathbb{R}),+) \to$ όχι ομάδα

γιατί δεν είναι πράξη (δεν ξέρω αν η + 2 πινάκων με det ≠ 0 μου δίνει επίσης πίνακα με det ≠ 0)

- $SL(m,\mathbb{R}) = \{A \in \mathbb{R}^{m\times m} \mid \det A = 1\}$

$(SL(m,\mathbb{R}),\cdot)) \to$ ομάδα

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

$[0]_n = n\cdot\mathbb{Z}$, $[1]_n = 1+n\cdot\mathbb{Z}$, $[n-1]_n \to n-1+n\cdot\mathbb{Z}$

1) $([a]_n + [b]_n) + [\gamma]_n = (a+b) + [\gamma]_n = [(a+b)+\gamma]_n$

$[a]_n + ([b]_n + [\gamma]_n) = [a+(b+\gamma)]_n$

Άρα ισχύει η προσεταιριστική.

2) $[a]_n + [0]_n = [0]_n + [a]_n = [a]_n$

Άρα $[0]_n$ ουδέτερο στοιχείο. (δηλ. όλα τα πολλαπλ. του n)

3) $[a]_n + [n-a]_n = [n-a]_n + [a]_n = [0]_n$

Υπάρχει αντίθετος

Άρα $(\mathbb{Z},+)$ είναι ομάδα.

- $(\mathbb{Z}_7,+)$ έχει 7 στοιχεία.

Το Z_n έχει n στοιχεία, αυτά που γράψαμε πριν.
$|Z_n| = n$ (⤳ τάξη = σύνολο των στοιχείων σε πεπερασμένο σύνολο)

- $(Z_n, \cdot)$ 1) προσεταιριστική
2) $[a]_n \cdot [1]_n = [1]_n \cdot [a]_n = [a]_n$
Άρα ουδέτερο το $[1]_n$
3) $[a]_n \cdot [\ ]_n = [\ ]_n \cdot [a]_n = [1]_n$.
Για $a=0$ δεν ισχύει.
Άρα δεν είναι ομάδα.

- $U(Z_n)$: τα αντιστρέψιμα στοιχεία του Z_n
$(U(Z_n), \cdot) \subseteq Z_n$ και ισχύει και η 3η ιδιότητα άρα είναι ομάδα.

$|U(Z_n)| = \phi(n)$

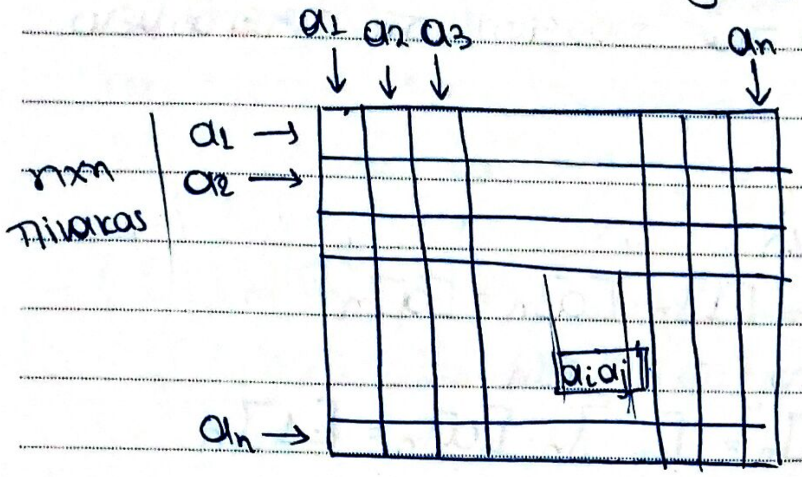
- $U(Z_8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$ $\quad Z_8 = \{[0]_8, [1]_8 \ldots, [6]_8, [7]_8\}$

μκδ με το 8 να είναι το 1

$|U(Z_8)| = \phi(8) = \phi(2^3) = 2^2 \cdot (2-1) = 4$ (άρα το περίμενα να έχει 4 στοιχεία).

$(U(Z_8), \cdot) \to$ ομάδα

Πίνακας του Cayley



$G = \{a_1, a_2, \dots, a_n\}$

Δεν είναι απαραίτητα συμμετρικός ο πίνακας γιατί μπορεί $a_i \cdot a_j \neq a_j a_i$

- $U(\mathbb{Z}_8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$

Πίνακας Cayley της $U(\mathbb{Z}_8)$

	[1]	[3]	[5]	[7]
[1]	[1]	[3]	[5]	[7]
[3]	[3]	[1]	[7] (=[3][5])	[5] (=[3][7])
[5]	[5]	[7]	[1]	[3]
[7]	[7]	[5]	[3]	[1]

Αν θέσω [1]=α, [3]=β, [5]=γ, [7]=δ

	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	α	β
δ	δ	γ	β	α

- $U(\mathbb{Z}_{12}) = \{ [1]_{12}, [5]_{12}, [7]_{12}, [11]_{12} \}$

Πίνακας Cayley της $U(\mathbb{Z}_{12})$

	[1]	[5]	[7]	[11]
[1]	[1]	[5]	[7]	[11]
[5]	[5]	[1]	[11]	[7]
[7]	[7]	[11]	[1]	[5]
[11]	[11]	[7]	[5]	[1]

Αν θέσω $[1]=a$, $[5]=b$, $[7]=\gamma$, $[11]=\delta$ θα έχω:

	a	b	γ	δ
a	a	b	γ	δ
b	b	a	δ	γ
γ	γ	δ	a	b
δ	δ	γ	b	a

Οι δύο πίνακες είναι ίδιοι!

- $\{1, -1, i, -i\} \subset \mathbb{C}$

$(\{1,-1,i,-i\}, \cdot) \to$ ομάδα

1) προσεταιριστική
2) ουδέτερο στοιχείο το 1.
3) 1 αντιστρ. -1, -1 το 1, i το $-i$, $-i$ το i.

Πίνακας Cayley της $(\{1,-1,i,-i\}, \cdot)$

1	−1	i	−i
−1	1	−i	i
i	−i	−1	1
−i	i	1	−1

- **Ορισμός**: Μια ομάδα G ονομάζεται αβελιανή αν για κάθε $a, b \in G$ ισχύει:

$a * b = b * a$

(δηλαδή ο πίνακας Cayley είναι συμμετρικός ως προς την διαγώνιο)

Όλες οι ομάδες που είδαμε πριν ήταν αβελιανές.

- $(\mathbb{R}^{m\times n}, +) \to$ Αβελιανές.

$(GL(n,\mathbb{R}), \cdot) \to$ Δεν είναι αβελιανή (ο πολ/μος σε πίνακα δεν είναι μεταθετικός)

Παράδειγμα

$$\left\{ \underset{M(1,2,3)}{\begin{pmatrix} 1&0&0\\0&1&0\\0&0&1\end{pmatrix}}, \underset{M(2,1,3)}{\begin{pmatrix} 0&1&0\\1&0&0\\0&0&1\end{pmatrix}}, \underset{M(1,3,2)}{\begin{pmatrix} 1&0&0\\0&0&1\\0&1&0\end{pmatrix}}, \underset{M(3,1,2)}{\begin{pmatrix} 0&1&0\\0&0&1\\1&0&0\end{pmatrix}}, \underset{M(3,2,1)}{\begin{pmatrix} 0&0&1\\0&1&0\\1&0&0\end{pmatrix}}, \underset{M(2,3,1)}{\begin{pmatrix} 0&0&1\\1&0&0\\0&1&0\end{pmatrix}} \right\}$$

Πίνακας Cayley

	M(1,2,3)	M(2,1,3)	M(1,3,2)	M(3,1,2)	M(3,2,1)	M(2,3,1)
M(1,2,3)	M(1,2,3)	M(2,1,3)	M(1,3,2)	M(3,1,2)	M(3,2,1)	M(2,3,1)
M(2,1,3)	M(2,1,3)	M(1,2,3)	M(2,3,1)	M(3,2,1)	M(3,1,2)	M(1,3,2)
M(1,3,2)	M(1,3,2)	M(3,1,2)	M(1,2,3)	M(2,1,3)	M(2,3,1)	M(3,2,1)
M(3,1,2)	M(3,1,2)					
M(3,2,1)	M(3,2,1)					
M(2,3,1)	M(2,3,1)					

Η ομάδα δεν είναι αβελιανή (ο πίνακας δεν είναι συμμετρικός)

• ΘΕΩΡΗΜΑ: Ο αριστερός και ο δεξιός νόμος διαγραφής ισχύουν σε κάθε ομάδα G, δηλ. αν $\alpha * \beta = \alpha * \gamma \Rightarrow$
$\Rightarrow \beta = \gamma$

και αν $\beta * \alpha = \gamma * \alpha \Rightarrow \beta = \gamma$

Απόδειξη

$a*b=a*\gamma \implies$

(έστω a' το αντίστροφο του a)

$\implies a'*(a*b) = a'*(a*\gamma)$ έχει σημασία που πολ/ζω από αριστερά

$\implies (a'*a)*b = (a'*a)*\gamma$

$\implies e*b = e*\gamma \implies b=\gamma$

Όμοια το άλλο.

Συμβολισμός: αντίστροφο του $a = a'$
- αν η πράξη μοιάζει με πολ/σμό: a^{-1}
- αν μοιάζει με πρόσθεση: $-a$

• **ΘΕΩΡΗΜΑ**: Έστω G ομάδα και $a, b \in G$. Οι γραμμικές εξισώσεις $ax=b$ και $xa=b$ έχουν μοναδικές ρίζες.

Απόδειξη

Θέλω ν.δ.ο. 1) έχουν λύση και 2) είναι μοναδική.

1) $a * \square = \dots = b$

a' ο αντίστροφος του a

$a*\boxed{a'*b} = (a*a')*b = e*b = b$

Έχει λύση την $\gamma_1 = a'*b$

2) Έστω γ_2 μια λύση με $\gamma_1 \neq \gamma_2$

Τότε έχω: $\left.\begin{array}{l} a*\gamma_1 = b \\ a*\gamma_2 = b \end{array}\right\} \implies$

$\implies a*\gamma_1 = a*\gamma_2 \implies (a'*a)*\gamma_1 = (a'*a)*\gamma_2 \implies e*\gamma_1 = e*\gamma_2$

$\implies \gamma_1 = \gamma_2$ Άτοπο άρα έχει μοναδική λύση.

• ΘΕΩΡΗΜΑ : Έστω G ομάδα και $a \in G$. Τότε
$G = a * G$, όπου $a * G = \{a * g / g \in G\}$

Απόδειξη

1) $a * G = \{a * g \,|\, g \in G\} \subseteq G$

2) Έστω $g_1 \in G \Rightarrow g_1 = a * \boxed{a' \cdot g_1} \Rightarrow g_1 \in a * G$.
$\Rightarrow G \subseteq a * G$.

Από (1), (2) $G = a * G$.