5/3/2018

1ο Έστω $n \geq 2$. Θέτουμε $SLn(\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} : \det A = 1\}$
(Special Linear ομάδα)

Ισχυρισμός $(SLn(\mathbb{R}), \cdot)$ ομάδα

ΑΠΟΔΕΙΞΗ — Έστω $A, B \in SLn(\mathbb{R})$. Τότε

$\det(A) = \det(B) = 1$. Από Γραμμική Άλγεβρα

$\det(AB) = (\det(A)\cdot\det(B)) = 1\cdot 1 = 1$

Άρα $AB \in SLn(\mathbb{R})$. Επομένως $\cdot$ πράξη στο $SLn(\mathbb{R})$

Φανερά $SLn(\mathbb{R}) \neq \emptyset$, γιατί για τον ταυτοτικό $n\times n$ πίνακα I_n ισχύει $\det(I_n) = \begin{vmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{vmatrix} = 1$.

Η πράξη $\cdot$ είναι προσεταιριστική, γιατί από Γρ. Άλγεβρα ο πολλαπλασιασμός πινάκων είναι προσεταιριστικός. Η πράξη έχει ουδέτερο στοιχείο το $I_n \in SLn(\mathbb{R})$.

Έστω $A \in SLn(\mathbb{R})$. Τότε $\det(A) = 1$, άρα A αντιστρέφεται σαν πίνακας. Έστω A^{-1} ο αντίστροφος. Τότε
$A\cdot A^{-1} = I_n \Rightarrow \det(A\cdot A^{-1}) = \det(I_n) \Rightarrow \det(A)\cdot\det(A^{-1}) = 1$
$\Rightarrow \det(A^{-1}) = 1$. Άρα $A^{-1} \in SLn(\mathbb{R})$.

11. Θέτουμε $S = \{A \in \mathbb{R}^{n\times n} : \det A \in \{1, 2, 2^2, 2^3, 2^4, \dots\}\}$
Είναι ο πολλαπλασιασμός καλά ορισμένος (δηλ. αν $A, B \in S$ ισχύει $AB \in S$); ΝΑΙ, γιατί αν $k_1, k_2 \in \mathbb{Z}$ με $k_1, k_2 \geq 1$ και $\det A = 2^{k_1}$, $\det B = 2^{k_2}$ τότε $\det(AB) = \det(A)\cdot\det(B) = 2^{k_1}\cdot 2^{k_2} = 2^{k_1+k_2}$. Άρα $AB \in S$
Είναι ο πολλαπλασιασμός στο S προσεταιριστικός; Ναι. Υπάρχει ουδέτερο στο S; Ναι, γιατί $I_n \in S$

Έχει κάθε στοιχείο του S αντίστροφο στο S; Όχι, για παράδειγμα $A = \begin{bmatrix} 2 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \in S$. Αλλά δεν

υπάρχει $B \in S$ με $AB = BA = I_n$

ΑΠΟΔΕΙΞΗ

Έστω $B \in S$ με $AB = BA = I_n$. Τότε $\det(AB) = \det(I_n) \Longrightarrow \det(A)\cdot\det(B) = 1 \Rightarrow 2\det(B) = 1 \Rightarrow \det(B) = \frac{1}{2}$, αντίφαση, γιατί $B \in S$

Άρα $(S, \cdot)$ όχι ομάδα.

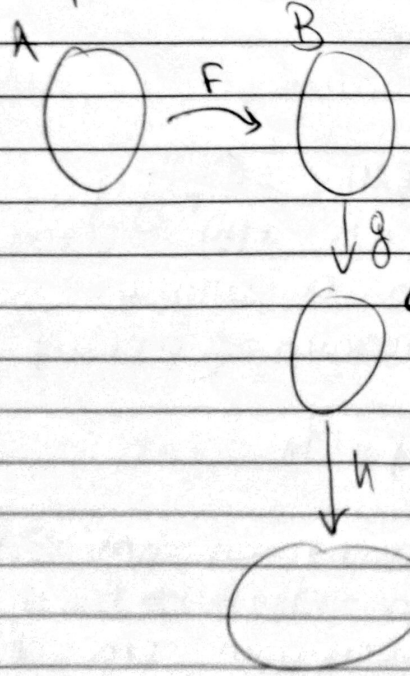
ΠΑΡΑΤΗΡΗΣΗ

Αν θέσουμε $S' \in \{A \in \mathbb{R}^{n\times n} : \det(A) \in \{\ldots, \frac{1}{2^3}, \frac{1}{2^2}, \frac{1}{2}, 2^0 = 1, 2^1, 2^2, 2^3, 2^4, \ldots\}\}$

Τότε εύκολα βλέπουμε $(S', \cdot)$ ομάδα.

ΟΜΑΔΕΣ ΜΕΤΑΘΕΣΕΩΝ

Υπενθύμιση από Θ. Συνόλων. Έστω A, B, C, D μη κενά σύνολα $f: A \to B$, $g: B \to C$, $h: C \to D$ συναρτήσεις.



ΙΣΧΥΡΙΣΜΟΣ

$(h\circ g)\circ f = h\circ(g\circ f)$ όπου $\circ$ σύνθεση συναρτήσεων.
(Με άλλα λόγια η σύνθεση συναρτήσεων είναι προσεταιριστική)

ΑΠΟΔΕΙΞΗ

Έστω $a \in A$

$[(h\circ g)\circ f](a) = (h\circ g)(f(a)) = h(g(f(a)))$

$[h\circ(g\circ f)](a) = h(g\circ f)(a) = h(g(f(a)))$

Άρα $(h\circ g)\circ f = h\circ(g\circ f)$

Υπενθύμιση Αν $g\circ f$ 1-1, τότε και $g\circ f$ 1-1

(Δηλαδή, η σύνθεση δύο 1-1 συναρτήσεων είναι 1-1

ΑΠΟΔΕΙΞΗ

Έστω $a, a' \in A$. Υποθέτουμε $(g \circ f)(a) = (g \circ f)(a')$

Θα δείξουμε ότι $a = a'$

Παρατηρούμε $(g \circ f)(a) = (g \circ f)(a') \Rightarrow$

$g(f(a)) = g(f(a')) \xrightarrow{g\ 1-1} f(a) = f(a') \xrightarrow{f\ 1-1} a = a'$

Άρα $g \circ f$ 1-1.

ΙΣΧΥΡΙΣΜΟΣ. Αν g επί και f επί τότε η $g \circ f$ είναι επί. (Δηλαδή σύνθεση επί συναρτήσεων είναι επί)

ΑΠΟΔΕΙΞΗ Έστω $c \in C$. Αφού g επί υπάρχει $b \in B$ με $c = g(b)$. Αφού f επί, υπάρχει $a \in A$ με $b = f(a)$.

Άρα, $c = g(b) = g(f(a)) = (g \circ f)(a)$

Συνεπώς $g \circ f$ επί.

- Έστω $f: A \to B$ 1-1 και επί. Ορίζουμε $r: B \to A$ ως εξής: Για $b \in B$ $r(b)$ είναι το μοναδικό $a \in A$ με $f(a) = b$. (Το a υπάρχει διότι f επί και είναι μοναδικό διότι f 1-1)

Τότε ισχύει $for = id_B$, $rof = id_A$

όπου $id_A: A \to A$ η ταυτοτική, δηλ $id_A(a) = a$ $\forall a \in A$ και ομοίως για $id_B: B \to B$. Η r λέγεται αντίστροφη συνάρτηση της f και συμβολίζεται με f^{-1}.

ΟΡΙΣΜΟΣ Έστω $M \neq \phi$ σύνολο. Θέτουμε

$$S_M = \{ f : M \to M \mid f \ 1-1 \text{ και επί} \}$$

Αφού από υπενθύμιση η σύνθεση δύο $1-1$ συναρτήσεων είναι $1-1$ και η σύνθεση δύο επί συναρτήσεων, έχουμε ότι $(S_M, \circ)$ (σύνθεση) είναι πράξη στο S_M.

ΠΡΟΤΑΣΗ Το $(S_M, \circ)$ είναι ομάδα

ΑΠΟΔΕΙΞΗ προσεταιριστικότητα. Έστω $f, g, h \in S_M$. Τότε $f \circ (g \circ h) = (f \circ g) \circ h$ αφού όπως είπαμε η σύνθεση συναρτήσεων είναι προσεταιριστική.

Ουδέτερο στοιχείο: Ταυτοτική απεικόνιση $id_M : M \to M$ με $id_M(m) = m$ για κάθε m είναι το ουδέτερο στοιχείο.

Πράγματι, έστω $f \in S_M$ θα δείξουμε ότι $f \circ id_M = id_M \circ f = f$. Αυτό ισχύει γιατί για $m \in M$

$(f \circ id_M)(m) = f(id_M(m)) = f(m)$ και
$(id_M \circ f)(m) = id_M(f(m)) = f(m)$

Αντίστροφο, Έστω $f \in S_M$ άρα $f : M \to M$ $1-1$ και επί

Θέτουμε $r = f^{-1} : M \to M$. Τότε $r \in S_M$ και $r \circ f = f \circ r = id_M$

Άρα r αντίστροφο ως προς την σύνθεση της f. Συνεπώς $(S_M, \circ)$ ΟΜΑΔΑ.

Συμβολισμός: Αν $M = \{1, 2, \ldots, n\}$ συμβολίζουμε το S_n επίσης με S_n. Το S_n λέγεται ομάδα μεταθέσεων σε n στοιχεία

ΕΡΩΤΗΜΑ Έστω $n \geq 1$. Πόσα στοιχεία έχει το S_n και ποια είναι αυτά;

ΠΕΡΙΠΤΩΣΕΙΣ

S_1 $M = \{1\}$ Τότε $S_1 = \{id_M\}$ και $|S_1| = 1$

S_2 $M = \{1, 2\}$ Τότε $S_2 = \{f_0 = id_M, f_1 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\}$

αυτό σημαίνει $f(1) = 2$, $f(2) = 1$

Πράγματι έστω $f: M \to M$ 1-1 και επί

Θεωρούμε τα $f(1)$, $f(2)$

Αν $f(1) = 1$ τότε $f(2) = 2$ άρα $f = f_0$

Αν $f(1) = 2$ τότε $f(2) = 1$ άρα $f = f_1$

S_3 $M = \{1, 2, 3\}$ $f = \begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}$

Πόσες επιλογές έχουμε για το $f(1)$; Τρεις.

Υποθέτουμε ότι το $f(1)$ έχει επιλεγεί. Πόσες επιλογές έχουμε για το $f(2)$; Δύο.

Υποθέτουμε ότι τα $f(1), f(2)$ έχουν επιλεγεί. Πόσες επιλογές έχουμε για το $f(3)$; Μία.

Στοιχεία της S_3 $\sigma_0 = id_M = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$ $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

Συμβολ. σημαίνει $\sigma_0(1) = 1$, $\sigma_0(2) = 2$, $\sigma_0(3) = 1$.

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

$\sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$. Άρα $S_3 = \{\sigma_i : 0 \leq i \leq 5\}$ και

$|S_3| = 6 = 3!$

(Η δεύτερη γραμμή στον συμβολισμό σι είναι μια διαταξη των 1,2,3)

Ταυτοτικό στοιχείο της S_3; Το $\sigma_0 = id_H = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$

Πίνακας πράξης (Λέγεται και πίνακας Cauley)

	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
σ_0	σ_0	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	σ_0	σ_4	σ_5	σ_2	σ_3
σ_2	σ_2	σ_5	σ_0	σ_4	σ_3	σ_1
σ_3	σ_3	σ_4	σ_5	σ_0	σ_1	σ_2
σ_4	σ_4	σ_3	σ_1	σ_2	σ_5	σ_0
σ_5	σ_5	σ_2	σ_3	σ_1	σ_0	σ_4

$$\sigma_1 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \sigma_0$$

$$\sigma_1 \circ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \sigma_2$$

$$\sigma_4 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \sigma_3$$

Συμπέρασμα S_3 όχι μεταθετική, γιατί
$\sigma_1 \circ \sigma_4 \neq \sigma_4 \circ \sigma_1$

Από πίνακα σ_0 ουδέτερο Άρα $\sigma_0^{-1} = \sigma_0$
$(\sigma_1)^{-1} = \sigma_1$, $(\sigma_2)^{-1} = \sigma_2$ $(\sigma_3)^{-1} = \sigma_3$
$(\sigma_4)^{-1} = \sigma_5$ $(\sigma_5)^{-1} = \sigma_4$

Κάθε ομάδα με το πολύ 5 στοιχεία είναι μεταθετική. Ενώ η S_3 έχει 6 και δεν είναι μεταθετική

ΠΑΡΑΤΗΡΗΣΗ. Είδαμε ότι η S_3 είναι ομάδα μη μεταθετική με έξι στοιχεία. Υπάρχει μεταθετική ομάδα με 6 στοιχεία;
Ναι η ομάδα $(\mathbb{Z}_6, +)$ των ακεραίων mod6 ως προς την πρόσθεση. (Πιο γενικά, για $n \geq 2$ η $(\mathbb{Z}_n, +)$

αβελιανή ομάδα με n στοιχεία.)

Πίνακας πράξης της $(\mathbb{Z}_6, +)$

$\mathbb{Z}_6 = \{[0]_6, [1]_6, [2]_6, [3]_6, [4]_6, [5]_6\}$

	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[0]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$
$[1]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$
$[2]_6$	$[2]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$
$[3]_6$	$[3]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$
$[4]_6$	$[4]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$
$[5]_6$	$[5]_6$	$[0]_6$	$[1]_6$	$[2]_6$	$[3]_6$	$[4]_6$

ΠΑΡΑΤΗΡΗΣΕΙΣ Πίνακας συμμετρικός ως προς την κύρια διαγώνιο, γιατί + μεταθετική.

12. Για $n \geq 2$, η ομάδα $U(\mathbb{Z}_n)$ = αντιστρέψιμα ως προς τον πολλαπλασιασμό στοιχεία του $\mathbb{Z}_n$

ΥΠΕΝΘΥΜΙΣΕΙΣ (Από Θ. Αριθμών)

1. Αν $a, b \in \mathbb{Z}$ με $a \neq 0$ ή $b \neq 0$ και $ΜΚΔ(a,b) = 1$ τότε υπάρχουν $x, y \in \mathbb{Z}$ με $1 = xa + yb$

2. Συνάρτηση $\phi: \mathbb{Z}_{\geq 1} \to \mathbb{Z}$ Euler.

ΟΡΙΣΜΟΣ. Για $n \geq 1$

$\phi(n) = \#\{k \in \mathbb{Z} : 1 \leq k \leq n$ και $ΜΚΔ(k,n) = 1\}$

αριθμός στοιχείων συνόλου.

ΥΠΕΝΘΥΜΙΣΗ

i) $\phi(1) = 1$

ii) Αν $n \geq 2$ και $n = p_1^{a_1} \cdots p_r^{a_r}$ με p_i πρώτοι $p_i \neq p_j$ για $i \neq j$ και $a_i > 0$ $\forall i$ τότε

$$\phi(n) = p_1^{a_1 - 1}(p_1 - 1) \cdot p_2^{a_2 - 1}(p_2 - 1) \cdots p_r^{a_r - 1}(p_r - 1)$$

π.χ. $\phi(16) = \phi(2^4) = 2^{4-1}(2-1) = \cdots = 2^3 \cdot 1 = 8$

$\phi(80) = \phi(2^4 \cdot 5) = 2^{4-1} \cdot (2-1) \cdot 5^{1-1}(5-1) = 2^3 \cdot 1 \cdot 4 = 32$

Ορισμός $U(\mathbb{Z}_n) = \{ [a]_n : 1 \le a \le n \text{ και } \text{ΜΚΔ}(a,n) = 1 \} \subseteq \mathbb{Z}_n$

Από τον ορισμό $|U(\mathbb{Z}_n)| = \phi(n)$

Παράδειγμα $n = 8 = 2^3$ $1, 2, 3, 4, 5, 6, 7, 8$

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

$n = 12 = 2^3 \cdot 3$ $U(\mathbb{Z}_{12}) = \{[1]_{12}, [5]_{12}, [7]_{12}, [11]_{12}\}$

ΠΡΟΤΑΣΗ Ορίζουμε : $U(\mathbb{Z}_n) \times U(\mathbb{Z}_n) \to U(\mathbb{Z}_n)$

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

Τότε i) Η πράξη $\cdot$ είναι καλά ορισμένη

ii) Το ζεύγος είναι μεταθετική ομάδα με $\phi(n)$ στοιχεία.

ΑΠΟΔΕΙΞΗ

καλά ορισμένο : Έστω $[a]_n = [a']_n$, $[b]_n = [b']_n$

Τότε $n | a - a'$ Αφού $ab - a'b' = ab - a'b + a'b - a'b' =$

$n | b - b'$

$b(a-a') + a'(b-b')$. Άρα, $n | ab - a'b' \Rightarrow$

$[a]_n [b]_n = [a']_n \cdot [b']_n$.

Επίσης, αν $\text{ΜΚΔ}(a,n) = 1$ και $\text{ΜΚΔ}(b,n) = 1$

τότε $\text{ΜΚΔ}(ab,n) = 1$

(Απδ. Έστω $\text{ΜΚΔ}(ab,n) > 1$. Τότε υπάρχει πρώτος p με $p|n$ και $p|ab \Rightarrow (p|n$ και $p|a)$ ή $(p|n$ και $p|b)$

$\Rightarrow \text{ΜΚΔ}(n,a) > 1$ ή $\text{ΜΚΔ}(n,b) > 1$, αντίφαση

ii) Ουδέτερο : προσεταιριστικός, διότι

$([a]_n)([b]_n \cdot [c]_n) = [a]_n [bc]_n = [a(bc)]_n = [(ab)c]_n =$

$([ab]_n \cdot [c]_n) = ([a]_n [b]_n) \cdot [c]_n$

Αφού $\text{ΜΚΔ}(1,n) = 1$ έχουμε $[1]_n \in U(\mathbb{Z}_n)$ και

$[1]_n$ ουδέτερο του $(U(\mathbb{Z}_n), \cdot)$

Ύπαρξη Αντιστρόφου. Έστω $a \in \mathbb{Z}$ με $1 \le a \le n$

και $\text{ΜΚΔ}(a,n) = 1$. Ψάχνουμε $x \in \mathbb{Z}$ με $\text{ΜΚΔ}(x,n) = 1$

και $[a]_n [x]_n = [x]_n \cdot [a]_n = [1]_n$

(ισοδύναμα $ax \equiv 1 \bmod n$)

Από υπεν. $\text{ΜΚΔ}(a,n) = 1 \Rightarrow$ Υπάρχουν $x, y \in \mathbb{Z}$ με

$1 = xa + yn$ (1)

Η σχέση (1) μας δίνει $ΜΚΔ(x,n) = 1$

(γιατί αν $ΜΚΔ(x,n) = d > 1$ τότε $d|x$ και $d|n \Rightarrow$
$d|xa+yn = 1$ άνειφαση)

Επίσης, η (1) μας λέει

$$[1]_n = [xa]_n + [yn]_n = [x]_n \cdot [a]_n + [0]_n = [x]_n \cdot [a]_n.$$

Αφού (φανερά) η πράξη $\cdot$ είναι μεταθετική, έχουμε $[a]_n \in U(Z_n)$ αντιστρέψιμο με αντίστροφο
$([a]_n)^{-1} = [x]_n$

Παράδειγμα. $n=5$ $\quad U(Z_5) = \{[1]_5, [2]_5, [3]_5, [4]_5\}$

	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

$([1]_5)^{-1} = [1]_5$ Άρα $([2]_5)^{-1} = [3]_5$

$([3]_5)^{-1} = [2]_5$ $\quad ([4]_5)^{-1} = [4]_5$