30/03/17.

$(S_n, \circ)$ n-οστή συμμετρική ομάδα.

$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ Π.χ. $n=5$, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}$

$\tau = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(1) & \tau(2) & \dots & \tau(n) \end{pmatrix}$ $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 3 & 4 \end{pmatrix}$

$\sigma \circ \tau \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \dots & & \sigma(\tau(5)) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}$

$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}$ || $\sigma^{-1} = \begin{pmatrix} 3 & 1 & 4 & 2 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} =$

$\sigma^{-1} \circ \sigma \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix} = i$ || $= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 1 & 3 & 5 \end{pmatrix}$

Δυνάμεις Στοιχείων

Έστω $(G, \cdot)$ ομάδα και $\alpha \in G$ και $n \in \mathbb{Z}$

Ορισμός: n-οστή δύναμη α^n του α ορίζεται ως εξής:

$$\alpha^n = \begin{cases} \underbrace{\alpha \cdot \alpha \cdot \dots \cdot \alpha}_{n-\text{φορές}}, & n \geq 1 \\ e, & n = 0 \\ \underbrace{\alpha^{-1} \cdot \alpha^{-1} \cdot \dots \cdot \alpha^{-1}}_{|n|-\text{φορές}}, & n \leq -1 \end{cases}$$

Για προσθετική ομάδα:

• $(G, +) \rightarrow$ $$n\alpha = \begin{cases} \overbrace{\alpha + \alpha + \dots + \alpha}^{n-\text{φορές}}, & n > 0 \\ 0, & n = 0 \\ \underbrace{(-\alpha) + (-\alpha) + \dots + (-\alpha)}_{|n|-\text{φορές}}, & n < 0 \end{cases}$$

$(G,+)$

Πρόταση: Έστω $(G,\cdot)$ ομάδα $\alpha \in G$, $n,m \in \mathbb{Z}$. Τότε:
① $\alpha^n \cdot \alpha^m = \alpha^{n+m}$, ② $(\alpha^n)^m = \alpha^{n\cdot m}$, ③ $\alpha^{-n} = (\alpha^{-1})^n$

$n\alpha + m\alpha = (n+m)\alpha$ $\quad m(n\alpha) = (nm)\alpha$ $\quad (-n)\alpha = n(-\alpha)$

Αποδ: ① • Αν $n=0$, τότε $\alpha^0 \cdot \alpha^m = e \cdot \alpha^m = \alpha^m = \alpha^{0+m}$

• Αν $n \geq 1$, τότε από Αρχή Μαθ. Επαγωγής:

$$\alpha^1 \cdot \alpha^m = \begin{cases} \underbrace{\alpha \cdot \underbrace{\alpha \cdot \alpha \cdots \alpha}_{m-\text{φορές}}}_{(m+1)-\text{φορές}} = \alpha^{m+1}, & m \geq 1 \\ \alpha^1 \cdot \alpha^0 = \alpha^1 \cdot e = \alpha^1 = \alpha^{1+0}, & m=0 \\ \alpha \cdot \underbrace{(\alpha^{-1}) \cdots (\alpha^{-1})}_{m-\text{φορές}} = (\alpha \cdot \alpha^{-1}) \cdot \underbrace{\alpha^{-1} \cdots \alpha^{-1}}_{|m+1|\ (\text{φορές})} = \alpha^{-1} \cdots \alpha^{-1} = \alpha^{m+1} & m<0 \end{cases}$$

• Αν $n>1$, θα υποθ. ότι $\alpha^n \cdot \alpha^m = \alpha^{n+m}$.
Τότε $\alpha^{n+1} \cdot \alpha^m = \alpha \cdot \alpha^n \cdot \alpha^m = \alpha \cdot \alpha^{n+m} = \alpha^{1+n+m}$

• Αν $n<0$ Τότε $n=-k$, $k>0$. Τότε θα έχουμε:
$\alpha^m = \alpha^{m+k-k} = \alpha^{-k} \cdot \alpha^{m+k} \Rightarrow \alpha^k \cdot \alpha^m = \alpha^k \cdot \alpha^{-k} \cdot \alpha^{m+k}$
$= e\alpha^{m+k} = \alpha^{m+k}$

Έστω $(G,\cdot)$ ομάδα και $\alpha \in G$. Θεωρούμε το σύνολο
$\langle \alpha \rangle = \{\alpha^n \in G \mid n \in \mathbb{Z}\}$

Πρόταση: Το ζεύγος $(\langle \alpha \rangle, \cdot)$ αποτελεί ομάδα.

Απόδειξη: $\forall x,y \in \langle \alpha \rangle$, $: x = \alpha^n$, $y = \alpha^m$, για κάποια $m,n \in \mathbb{Z}$.

Τότε $x \cdot y = \alpha^n \cdot \alpha^m = \alpha^{n+m} \in \langle \alpha \rangle \Rightarrow$
- η πράξη $\cdot$ της G είναι καλά ορισμένη στο $\langle \alpha \rangle$.

① $\alpha^n(\alpha^m \cdot \alpha^k) = \alpha^n(\alpha^{m+k}) = \alpha^{n+m+k} = \alpha^{n+m} \cdot \alpha^k = (\alpha^n \cdot \alpha^m)\alpha^k$
άρα $\cdot$: προσεταιριστική
② $e = \alpha^0 \in \langle \alpha \rangle$ και προφανώς το e: ουδ. στοιχ. στο $\langle \alpha \rangle$.
③ $\forall x \in \langle \alpha \rangle$ $x = \alpha^m$ είναι: $\alpha^{-m} \in \langle \alpha \rangle$ και
$\alpha^m \cdot \alpha^{-m} = \alpha^{m+(-m)} = \alpha^0 = e \in \langle \alpha \rangle$
$\quad\quad\quad\quad\quad\quad\quad\quad \| \ \alpha^{-m} \cdot \alpha^m$ $\longrightarrow$

Άρα $\forall x = \alpha^{\mu} \in \langle \alpha \rangle$, $\exists\, x^{-1} = \alpha^{-\mu}$

Άρα $(\langle \alpha \rangle, \cdot)$ αποτελεί ομάδα.

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

Πόρισμα: Για κάθε στοιχείο $\alpha \in G$, $(G, \cdot)$, η ομάδα η οποία παράγεται από το α, δηλαδή η $\langle \alpha \rangle$, είναι αβελιανή.

Αποδ: $\forall x, y \in \langle \alpha \rangle$, $x = \alpha^{n}$ $y = \alpha^{\mu}$ είναι:

$$x \cdot y = \alpha^{n} \cdot \alpha^{\mu} = \alpha^{n+\mu} = \alpha^{\mu+n} = \alpha^{\mu} \cdot \alpha^{n} = y \cdot x \Rightarrow \langle \alpha \rangle : \text{αβελιανή}$$

Ορισμός: Μία ομάδα $(G, \cdot)$ θα καλείται κυκλική $\Leftrightarrow (\exists \alpha \in G) : G = \langle \alpha \rangle$.

$(G, +)$, $\langle \alpha \rangle = \{(n\alpha) \in G \mid n \in \mathbb{Z}, \alpha \in G\}$

Αν $G = \langle \alpha \rangle \Rightarrow \alpha$: γεννήτορας της G.

Π.χ.: ① Αν $(G, \cdot)$ ομάδα τότε $\langle e \rangle = \{e\}$.

② Στην ομάδα $(\mathbb{Z}, +)$ και έστω $\kappa \in \mathbb{Z}$, τότε
$\langle \kappa \rangle = \{(n\kappa) \in \mathbb{Z} \mid n \in \mathbb{Z}\} = \{\dots, -3\kappa, -2\kappa, -\kappa, 0, \kappa, 2\kappa, 3\kappa, \dots\}$

Αν $\kappa = 1 \Rightarrow \langle 1 \rangle = \{n1 \in \mathbb{Z} \mid n \in \mathbb{Z}\} = \mathbb{Z} \Rightarrow (\mathbb{Z}, +)$: κυκλική

$\kappa = -1 \Rightarrow \langle -1 \rangle = \{n(-1) \in \mathbb{Z} \mid n \in \mathbb{Z}\} = \mathbb{Z} \Rightarrow \{1, -1\}$ γεννήτορες της $(\mathbb{Z}, +)$.

③ Στην ομάδα $(\mathbb{C}^*, \cdot)$: $\langle i \rangle = \{i^n \in \mathbb{C} \mid n \in \mathbb{Z}\} = \{1, -1, i, -i\}$

$i^1 = i$, $i^2 = -1$, $i^3 = -i$, $i^4 = 1$, ...

④ $(GL_2(\mathbb{R}), \cdot)$ και $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R})$

$\langle A \rangle = \{A^n \in GL_2(\mathbb{R}) \mid n \in \mathbb{Z}\}$

• $n = 0$, $A^0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$, $n \geq 1$: $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$

$A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \Rightarrow \forall n \geq 1 \quad A^{-n} = (A^{-1})^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$

Άρα $\langle A \rangle = \{ A^n \in GL_2(\mathbb{R}) \mid n \in \mathbb{Z} \} = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{R}) \mid n \in \mathbb{Z} \right\}$

Π.χ.: $(S_3, \circ)$, $S_3 = \{ i = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$

$\mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \}.$

$\langle i \rangle = \{ i \}$

$\langle \mu_1 \rangle = \{ \mu_1^n \in S_3 \mid n \in \mathbb{Z} \} \overset{(*)}{=} \{ i, \mu_1 \}$

$(*)\ \mu_1^2 = \mu_1 \circ \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = i \Rightarrow \mu_1^{-1} = \mu_1$

Όμοια $\langle \mu_2 \rangle = \{ \mu_2^n \in S_3 \mid n \in \mathbb{Z} \} = \{ i, \mu_2 \}$

$\langle \mu_3 \rangle = \{ \mu_3 \in S_3 \mid n \in \mathbb{Z} \} = \{ \mu_3, i \}$

Είναι: $\rho_1^2 = \rho_1 \cdot \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \rho_2$

$\rho_1^3 = \rho_1^2 \cdot \rho_1 = \rho_2 \cdot \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = i \Rightarrow$

$\Rightarrow \boxed{\rho_1^{-1} = \rho_2}$

Άρα $\langle \rho_1 \rangle = \{ i, \rho_1, \rho_2 \} = \langle \rho_2 \rangle$ (όμοια)

Ορισμός: Έστω $(G, \cdot)$ ομάδα και $H \subseteq G$. Το H καλείται υποομάδα της $G \Leftrightarrow$:

1. Το H κλειστό στην πράξη $\cdot$ της ομάδας (δηλ. $\forall x, y \in H \Rightarrow (x \cdot y) \in H$)
2. Το ζεύγος $(H, \cdot)$ είναι ομάδα.

Λήμμα: Αν H: υποομάδα της $(G, \cdot)$ και e_H: ουδ. στοιχ. της $(H, \cdot)$ και $\forall h \in H$: h_H^{-1}: αντίστροφο του h στην $(H, \cdot)$ τότε:
(1) $e_H = e$, (2) $\forall h \in H$: $h_H^{-1} = h^{-1}$

Απόδ: (1) $\left.\begin{array}{l} e_H \cdot e = e_H \\ e_H \cdot e_H = e_H \end{array}\right\| \xrightarrow[\text{Διαγρ. } G]{\text{Νόμος}} \boxed{e = e_H}$

(2) Έστω $h \in H$, $h^{-1}, h_H^{-1} \in G$, $h_H \in G$

$h \in G: h \cdot h^{-1} = e = h^{-1} \cdot h$ $\longrightarrow$

Scanned by CamScanner

$h \in H : h \cdot h_H^{-1} = e = h_H^{-1} \cdot h$

Από Νόμο Διαγραφής στην G:

$$\boxed{h^{-1} = h_H^{-1}}$$

Θεώρημα: Έστω $(G, \cdot)$ ομάδα και $H \subseteq G$. Τότε τα ακόλουθα είναι ισοδύναμα:

① Το H είναι υποομάδα της $(G, \cdot)$.

② • $e \in H$

• $\forall x, y \in H : x \cdot y \in H$

• $\forall x \in H : x^{-1} \in H$

③ • $H \neq \emptyset$

• $\forall x, y \in H : x \cdot y^{-1} \in H$

Απόδ: ① $\Rightarrow$ ② : Αφού H υποομάδα $\Rightarrow$ η πράξη $\cdot$ είναι κλειστή στο H δηλ $\forall x, y \in H \Rightarrow x \cdot y \in H$.

Από λήμμα $e_H = e \Rightarrow e \in H$ και $\forall x \in H \Rightarrow x^{-1} \in H$.

Άρα το ② ισχύει

② $\Rightarrow$ ③ Αφού $e \in H \Rightarrow H \neq \emptyset$.

Έστω $x, y \in H \Rightarrow x, y^{-1} \in H \Rightarrow x \cdot y^{-1} \in H$

③ $\Rightarrow$ ①