5/3/2018

▸ Στο προηγούμενο μάθημα

• $H \leq G$ ⇝ H υποομάδα της G

• $H \leq G \iff$ (i) $H \subseteq G$

(ii) H κλειστό ως προς την πράξη (δηλ. αν $\alpha, \beta \in H \implies \alpha * \beta \in H$)

(iii) $(H, *)$ ομάδα.

▸ **Ορισμός** • Αν $H = \langle \alpha \rangle = \{\alpha^n \mid n \in \mathbb{Z}\}$, τότε η $\langle \alpha \rangle$ καλείται <u>κυκλική</u> υποομάδα της G, ή υποομάδα που παράγεται από το α.

• Το α λέγεται <u>γεννήτορας</u> της υποομάδας $\langle \alpha \rangle$

▸ **Ορισμός** Αν υπάρχει $\alpha \in G$, τέτοιο ώστε $G = \langle \alpha \rangle$, τότε η G καλείται <u>κυκλική ομάδα</u>

▸ **Θεώρημα** Έστω G ομάδα και H υποσύνολο της G.

Το <u>H είναι υποομάδα της G</u>, αν και μόνο αν:

(i) Το H είναι κλειστό, ως προς την πράξη της ομάδας G

(ii) Το ουδέτερο στοιχείο της G, ανήκει στο H

(iii) Για κάθε $\alpha \in H$, συνεπάγεται το $\alpha^{-1} \in H$.

▸ **Απόδειξη**: $(\longrightarrow)$ Το (i) είναι προφανές.

(ii) Έστω $\alpha \in H$ και e_H: το ουδέτερο στοιχείο της H.

Τότε:

$$\left.\begin{aligned} &\alpha * e_H = \alpha \\ \& \quad &\alpha \cdot e_G = \alpha \end{aligned}\right\} \Longrightarrow \alpha * e_H = \alpha * e_G \xrightarrow[\text{διαγραφής}]{\text{αριστερός νόμος}}$$

$$\Longrightarrow \boxed{e_H = e_G}$$

(iii) $\left.\begin{aligned} &\text{Για την } G: \ \alpha * \alpha^{-1} = e \\ &H: \text{ομάδα}: \ \alpha * \alpha' = e \end{aligned}\right\} \ \alpha * \alpha^{-1} = \alpha * \alpha' \Rightarrow \boxed{\alpha^{-1} = \alpha'}$

$(\longleftarrow)$ Είναι προφανής η απόδειξη!

▸ $\boxed{\text{Θεώρημα } 2}$ Έστω G ομάδα και H υποσύνολο της G. Το H είναι υποομάδα της G, αν και μόνο αν:

(i) $H \neq \emptyset$

(ii) για κάθε $\alpha, \beta \in H \Longrightarrow \alpha * \beta^{-1} \in H$

▸ **Απόδειξη**: $(\longrightarrow)$ (i) H: υποομάδα της $G \xRightarrow{(ii)} e_G = e_H$
$\Longrightarrow \boxed{e \in H} \Longrightarrow \boxed{H \neq \emptyset}$

(ii) $\alpha, \beta \in H \xRightarrow{(iii)} \left.\begin{aligned} &\alpha \in H \\ &\beta^{-1} \in H \end{aligned}\right\} \xRightarrow{(i)} \boxed{\alpha * \beta^{-1} \in H}$

$(\longleftarrow)$ (ii): $H \neq \emptyset \Longrightarrow (\exists\, h \in H)$

• Για $h \in H$ και $h \in H \Longrightarrow h * h^{-1} \in H \Longrightarrow \boxed{e \in H}$

(iii) Έστω $\alpha \in H \xRightarrow{(ii)}$ Για $e \in H$ και $\alpha \in H \Rightarrow e * \alpha^{-1} \in H \Rightarrow$

$\Rightarrow \boxed{\alpha^{-1} \in H}$.

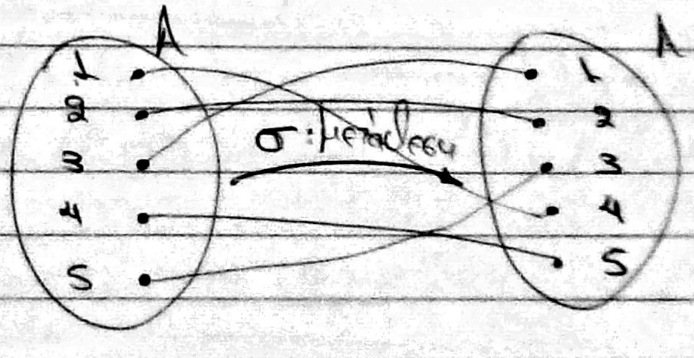
(i) Έστω $\alpha, \beta \in H \Rightarrow \boxed{\alpha \in H}$ & $\boxed{\beta^{-1} \in H} \Rightarrow$

$\xRightarrow{(ii)} \boxed{\alpha * \beta^{-1} \in H} \Rightarrow H$: κλειστό ως προς την πράξη της G!

• Αποδείξαμε λοιπόν και τις δύο κατευθύνσεις!
(Θεώρημα 1 $\Longleftrightarrow$ Θεώρημα 2)

▶ Ορισμός Έστω A σύνολο. Μετάθεση του A ονομάζεται μία απεικόνιση από το A στο A, που είναι "1-1" και επί.

▶ Παράδειγμα



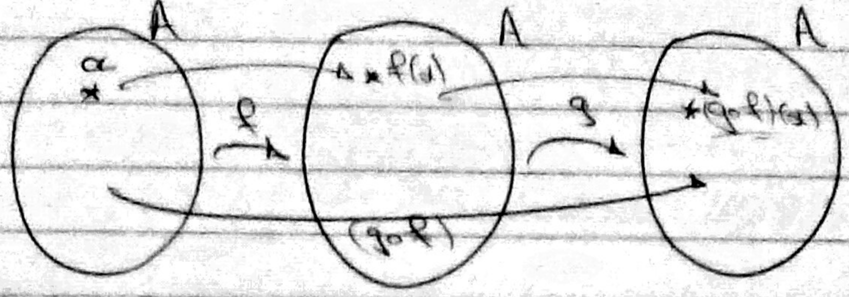
→ Συμβολισμός μίας μετάθεσης σ:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix}$$

→ στοιχεία του A

→ οι εικόνες αυτών

▸ **Ορισμός** | S_A: είναι το σύνολο των μεταθέσεων του A.



• $(g\circ f)(\alpha)=g(f(\alpha))$

• $A \longrightarrow A$

f: μετάθεση   g: μετάθεση

▸ f,g: "1-1" $\overset{?}{\Longrightarrow}$ $g\circ f$: "1-1"

• $g(\alpha)=g(b) \xRightarrow{g:\text{"1-1"}} \alpha=b$

• Έστω: $(g\circ f)(\alpha)=(g\circ f)(b) \xRightarrow{g:\text{"1-1"}} g(f(\alpha))=g(f(b)) \Rightarrow$

$\Rightarrow f(\alpha)=f(b) \xRightarrow{f:\text{"1-1"}} \boxed{\alpha=b} \Rightarrow (g\circ f)$: "1-1"

• Άρα, πράγματι: $\boxed{f,g:\text{"1-1"} \Longrightarrow (g\circ f):\text{"1-1"}}$

▸ f,g: επί $\overset{?}{\Longrightarrow}$ $(g\circ f)$: επί

• g: επί και $\omega\in A \Longrightarrow (\exists z\in A)$, τ.ω. $\boxed{g(z)=\omega}$ (1)

• f: επί και $z\in A \Longrightarrow (\exists x\in A)$, τ.ω. $\boxed{f(x)=z}$ (2)

• Από (1) και (2): $(g\circ f)(x)=g(f(x))=g(z)=\omega \Rightarrow$

$\Rightarrow \boxed{(g\circ f)(x)=\omega}$

$\Rightarrow \boxed{(g\circ f):\text{ επί}}$

• Άρα, η $g\circ f$ είναι μετάθεση!!!

• <u>Θεωρώ</u> $(S_A, \circ)$, όπου $(g,f) \longrightarrow g\circ f$

το σύνολο των μεταθέσεων — σύνθεση συναρτήσεων.

• Θα αποδείξω ότι είναι ομάδα!

(i) <u>Έστω</u> f, g, h μεταθέσεις. Τότε $f\circ(g\circ h) \overset{?}{=} (f\circ g)\circ h$

• <u>Έχω</u>: $\alpha \in A \Rightarrow \begin{cases} \cdot\ f\circ(g\circ h)(\alpha) = f((g\circ h)(\alpha)) = \underline{f(g(h(\alpha)))} \\ \cdot\ ((f\circ g)\circ h)(\alpha) = f\circ g(h(\alpha)) = \underline{f(g(h(\alpha)))} \end{cases}$

$$\Longrightarrow \boxed{f\circ(g\circ h) = (f\circ g)\circ h}$$

(ii) <u>Έχω</u>: $I_A : A \longrightarrow A$, με $\underline{I_A(\alpha) = \alpha}$.

• <u>Προφανώς</u>, η I_A είναι "1-1" και επί, ως ταυτοτική απεικόνιση.

<u>Άρα</u> I_A: μετάθεση $\Longrightarrow \boxed{I_A \in S_A}$

• <u>Έχω</u>: $\begin{rmatrix}\end{rmatrix}$

$\cdot\ (f\circ I_A)(\alpha) = f(I_A(\alpha)) = f(\alpha)$

$\cdot\ (I_A\circ f)(\alpha) = I_A(f(\alpha)) = f(\alpha)$ $\Rightarrow$

$$\Rightarrow \boxed{(f\circ I_A)(\alpha) = f(\alpha) = (I_A\circ f)(\alpha)}$$

(iii) <u>Έστω</u> $f \in S_A \Rightarrow \underline{f^{-1}\circ f = I_A = f\circ f^{-1}}$

$\Rightarrow f$: "1-1" και επί $\Longrightarrow f^{-1}$ υπάρχει και είναι και αυτή "1-1" και επί.

• <u>Άρα</u> $f^{-1} \in S_A \Longrightarrow$ <u>Άρα</u> $(S_A, \circ)$ είναι ομάδα!!!

$\boxed{\text{• Παραδείγματα}}$ • $A=\{1,2,3\}$

• Έχω: $S_A=\left\{\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\right\}$

• Προφανώς: $\boxed{|S_A|=6}$ — (Τάξη του S_A = πλήθος στοιχείων του S_A)

• $S_n = S_{\{1,2,\dots,n\}}$ και $|S_n| = n!$

• Θεωρώ $f*g = f\circ g$ και έχω:

• $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}*\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$

$\longrightarrow$ Π.χ. $g(2)=3$ κι $(f\circ g)(2)=f(3)=3$

$\Rightarrow \boxed{(f\circ g)(2)=3}$

• $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}*\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

$\longrightarrow$ Π.χ. $g(1)=2$ κι $(f\circ g)(1)=f(g(1))=f(2)=3$

$\Rightarrow \boxed{(f\circ g)(1)=3}$

⚠ Η S_3 και γενικώς η S_n, **ΔΕΝ** είναι αβελιανή, για $n\geq 3$, καθώς δεν ισχύει η μεταθετικότητα

(θα έπρεπε για $f,g\in S_3$: $f\circ g = g\circ f$)

S_{11}

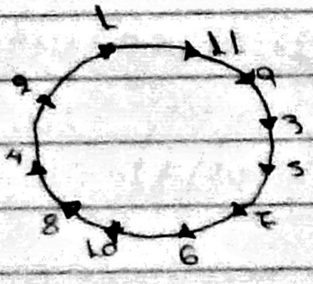
- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 4 & 11 & 1 & 5 & 2 & 3 & 7 & 9 & 10 & 8 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 3 & 4 & 5 & 7 & 9 & 11 & 1 & 6 & 10 & 8 \end{pmatrix}$

(Απ.) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 11 & 1 & 5 & 2 & 7 & 10 & 6 & 4 & 3 & 8 & 9 \end{pmatrix} = \sigma$

- Έχω: $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 4 & 9 & 8 & 3 & 7 & 5 & 10 & 11 & 6 & 1 \end{pmatrix}$

Διαφορετικός συμβολισμός για δήλωση μετάθεσης:

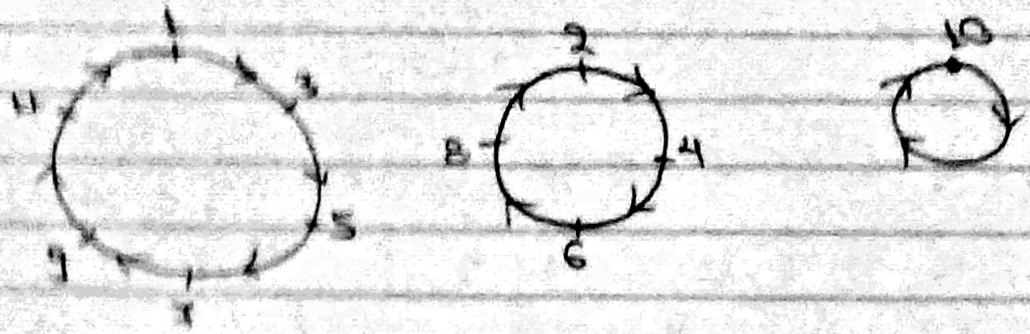
Π.χ. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) & \ldots & & & & & \sigma(10) & \sigma(11) \end{pmatrix}$



Συμβολισμός

$\sigma = (1, 11, 9, 3, 5, 7, 6, 10, 8, 4, 2)$ Το ένα στοιχείο πηγαίνει στο επόμενο

• $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 2 & 11 & 10 & 1 \end{pmatrix}$



→ <u>Έχω</u>: $\tau = (3,5,7,9,11,1)\cdot(6,8,2,4)\cdot(10)$

<u>και</u>: $\tau^{-1} = (1,11,9,7,5,3)\cdot(4,2,8,6)\cdot(10)$

⚠ Δεν έχει σημασία από ποιο στοιχείο θα ξεκινήσω τις μεταθέσεις που θα κάνω!!!

⚠ Όταν κάποιο στοιχείο "πάει" στον εαυτό του, μπορώ να το παραλείψω!!!

$\boxed{\sigma\cdot\tau}$

• <u>Έχω</u>: $(1,11,9,3,5,7,6,10,8,4,2)(3,5,7,9,11,1)(6,8,2,4)(10)$

$= (1,5,6,4,10,8)(2)(3,7)(9)(11)$

⚠ Ξεκινάω από αριστερά, και <u>εφαρμόζω</u> από 1 έως 11, παραλείποντας τα στοιχεία που θα έχω <u>βρει</u>!!

• $f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 3 & 5 & 7 & 1 & 4 & 8 & 6 & 10 & 9 \end{pmatrix}$

$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 2 & 5 & 4 & 7 & 8 & 9 & 10 & 6 \end{pmatrix}$

Έχω: $f = (1,2,3,5)(4,7,8,6)(9,10)$ → Μορφή κύκλου

και: $g = (1,3,2)(4,5)(6,7,8,9,10)$

$$\boxed{f * g = (1,5,7,6,8,10,4)(2)(3)(9)}$$

▸**Θεώρημα** Κάθε κυκλική ομάδα, είναι αβελιανή

▸Απόδειξη: G: κυκλική $\Rightarrow \boxed{\exists\, \alpha \in G}$, τέτοιο ώστε:

$$G = \langle \alpha \rangle = \{\alpha^n, n \in \mathbb{Z}\}$$

• Έστω $x, y \in G = \langle \alpha \rangle \Rightarrow \boxed{x = \alpha^n}$ και $\boxed{y = \alpha^m}$

• Έχω: $x \cdot y = \alpha^n \cdot \alpha^m = \alpha^{n+m} = \alpha^{m+n} = \alpha^m \cdot \alpha^n = y \cdot x$

• Άρα, για $n, m \in \mathbb{Z}$, η G είναι αβελιανή!!!

(Ισχύει η μεταθετικότητα)

Θεώρημα Κάθε υποομάδα κυκλικής ομάδας, είναι κυκλική

Απόδειξη: G: κυκλική $\Rightarrow G = \langle \alpha \rangle$

- Έστω H: υποομάδα της G. Διακρίνω τις περιπτώσεις:

(i) $H = \{1\} \Rightarrow H = \langle 1 \rangle \Rightarrow \boxed{H: \text{κυκλική}}$ (όλα της τα στοιχεία παράγονται από το 1)

(ii) $H \neq \{1\} \Rightarrow$ Ισχύει ότι $\alpha^u \in H$ και $\alpha^{-u} \in H$, για $u \neq 0$

- Άρα, υπάρχουν φυσικοί αριθμοί, τέτοιοι, ώστε $\alpha^u \in H$.
- Έστω d: ο μικρότερος φυσικός τέτοιος, ώστε $\alpha^d \in H$.
- Ισχυριζόμαστε, ότι: $H \overset{?}{=} \langle \alpha^d \rangle$

$\longrightarrow$ Έχω $\begin{cases} \alpha^d \in H \Rightarrow (\alpha^d)^u \in H \Rightarrow \boxed{\langle \alpha^d \rangle \subseteq H} \\ \alpha^{-d} \in H \Rightarrow (\alpha^{-d})^u \in H \Rightarrow \boxed{\langle \alpha^d \rangle \subseteq H} \end{cases}$

Για $u \in \mathbb{N}$

$\longrightarrow$ Έστω $h \in H \subseteq G \Rightarrow h \in G = \langle \alpha \rangle \Rightarrow \boxed{h = \alpha^u}$

- Να δείξω ότι το u είναι πολλαπλάσιο του d.
- Έχω $\boxed{u = q \cdot d + r}$, με $0 \leq r < d$. Θέλω $\boxed{r = 0}$
- Έχω $\alpha^u = \alpha^{qd+r} = (\alpha^d)^q \cdot \alpha^r \Rightarrow \alpha^r = (\alpha^d)^{-q} \cdot \alpha^u \xrightarrow[(\alpha^d)^{-q} \in H]{\alpha^u \in H}$

$\Rightarrow \boxed{\alpha^r \in H}$. Διακρίνω περιπτώσεις:

(i) Αν r: φυσικός: $\alpha^r \in H$ και $r < d$

· Άτοπο, καθώς ο d είναι ο μικρότερος φυσικός!!!

· Άρα: $\boxed{r=0} \Rightarrow \boxed{u = g \cdot d} \Rightarrow$

$\Rightarrow h = \alpha^u = \alpha^{g \cdot d} = (\alpha^d)^g \in \langle \alpha^d \rangle$

$\Rightarrow \boxed{H \subseteq \langle \alpha^d \rangle} \Rightarrow \boxed{H = \langle \alpha^d \rangle}$

$\Rightarrow \boxed{H: \text{κυκλική}}$