14/3/17 Μάθημα 4.

Με Σ_ν συμβολίζουμε το σύνολο των 1-1 απεικονίσεων από $\{1, 2, \dots \nu\}$ στον εαυτό του. Με την σύνθεση αυτό αποτελεί ομάδα και καλείται η συμμετρική ομάδα σε ν στοιχεία. Είδαμε ότι $|\Sigma_\nu| = \nu!$

Με D_ν το σύνολο των συμμετριών ενός κανονικού ν-γώνου. Με την σύνθεση αυτό αποτελεί ομάδα η οποία "ζει" μέσα στην Σ_ν, διότι μεταθέτει τις ν κορυφές.

Είδαμε ότι $D_3 = \Sigma_3$ ενώ $D_4 \subseteq \Sigma_4$ διότι $|D_4| = 8$ και $|\Sigma_4| = 24$. Θα δείξουμε ότι $|D_\nu| = 2\nu$ και καλείται <u>διεδρική</u> ομάδα τάξης 2ν.

Δείξαμε ότι $\Sigma_3 = \{1, f, f^2, g, fg, f^2 g\}$ όπου:

$f : (1, 2, 3) \to (2, 3, 1)$

$g : (1, 2, 3) \to (1, 3, 2)$

<u>ΚΑΙ</u> $f^3 = 1$ ταυτοτική $= g^2$, $gf = f^2 g$

Η $gf = f^2 g$ δεν είναι αβελιανή γιατί $gf \neq fg$ γεννάται από δύο στοιχεία f και g. Είναι η ομάδα που θα χρησιμοποιούμε, μη εύκολη για παραδείγματα.

Είδαμε ότι $D_4 = \{1, f, f^2, f^3, g, fg, f^2 g, f^3 g\}$ με

$f : (1, 2, 3, 4) \to (2, 3, 4, 1)$

$g : (1, 2, 3, 4) \to (1, 4, 3, 2)$

Και αυτή γεννάται από δύο στοιχεία και δεν είναι αβελιανή.

Γενικά ισχύει $D_\nu = \{1, f, f^{\nu-1}, g, fg, f^2 g, \dots, f^{\nu-1} g\}$ με $f^\nu = 1 = g^2$ και $f^i g = g f^{\nu-i}$ χωρίς απόδειξη.

G ομάδα, $\alpha \in G$, $o(\alpha)$ μικρότερος φυσικός ώστε $\alpha^{o(\alpha)} = 1$,
Αν υπάρχει αλλιώς $o(\alpha) = \infty$

G κυκλική $= \langle \alpha \rangle \Leftrightarrow$ κάθε στοιχείο της είναι δύναμη του α.

<u>π.χ.</u> $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$
$\mathbb{Z}_\nu = \langle [1]_\nu \rangle$ στροφές κατά γωνία πολ/σιο του $\frac{2\pi}{\nu}$
$\mathbb{Q}$ όχι κυκλική
Σ_3 όχι κυκλική
D_ν όχι κυκλική

<u>Θεώρημα</u>: 1) $o(\alpha) = o(\alpha^{-1})$
2) Αν $\alpha^m = 1$, τότε $o(\alpha) \mid m$
3) Αν $o(\alpha) = k$, τότε $o(\alpha^m) = \frac{k}{(k,m)}$ ΜΚΔ

απόδειξη:
2) Αν $\alpha^m = 1 \Rightarrow o(\alpha) \leq m$. Θέτουμε $o(\alpha) = k$.
Υποθέτουμε ότι $k \nmid m \Rightarrow m = \pi k + u$ με $0 < u < k$
$\alpha^m = 1 \Rightarrow \alpha^{\pi k + u} = 1 \Rightarrow (\alpha^k)^\pi \alpha^u = 1 \xRightarrow{o(\alpha)=k}$
$\Rightarrow 1^\pi \alpha^u = 1$ και $\alpha^u = 1$ με $u < k$ <u>άτοπο!</u>

<u>π.χ.</u> $\mathbb{Z}_6 = \langle [1]_6 \rangle$ $o([1]) = 6$
$o([2]) = 3 \mid 6$
$2 \cdot 1$ $2 \cdot 2 \cdot 2 = 2 \cdot 3 = 6$.

Το γινόμενο $\alpha \cdot b$ στην αβελιανή γίνεται άθροισμα $\alpha + b$
α^m $\underbrace{\alpha + \alpha + \dots + \alpha}_{m} = m \cdot a$

3) $o(\alpha) = k$, έστω $o(\alpha^m) = l$ θέλουμε $l = \frac{k}{(k,m)}$
Παίρνω α^m και το υψώνω στο $\frac{k}{(k,m)}$
$(\alpha^m)^{\frac{k}{(k,m)}} = \alpha^{\frac{mk}{(k,m)}} = (\alpha^k)^{\frac{m}{(k,m)}} = 1^{\frac{m}{(k,m)}} \xRightarrow{②}$ θέλουμε $l' = 1$
$(+)$

$\Rightarrow l \mid \frac{k}{(k,m)} = l l'$

$(\alpha^m)^l = 1 \Rightarrow \alpha^{ml} = 1 \overset{(2)}{\Rightarrow} k \mid ml = kk' \Rightarrow \frac{m}{(k,m)} l = \frac{k}{(k,m)} k'$

Άρα $\left(\frac{m}{(k,m)}, \frac{k}{(k,m)}\right) = 1$ πρώτοι μεταξύ τους.

Και $\frac{k}{(k,m)} \Big| \frac{m}{(k,m)} l \Rightarrow \frac{k}{(k,m)} \Big| l'$ (++)

Από (+), (++) $\Rightarrow l = \frac{k}{(k,m)}$

<u>π.χ.</u> $\mathbb{Z}_{14}$

$o([1]) = 14$ ένας γεννήτορας

$o([2]) = \frac{14}{(2,14)} = \frac{14}{2} = 7$

$o([3]) = \frac{14}{(3,14)} = \frac{14}{1} = 14$ άλλοι ένας γεννήτορας

$o([4]) = \frac{14}{(4,14)} = \frac{14}{2} = 7$

$o([6]) = \frac{14}{(6,14)} = \frac{14}{2} = 7$

$o([7]) = \frac{14}{(7,14)} = \frac{14}{7} = 2$

$o([10]) = \frac{14}{(10,14)} = \frac{14}{4}$.

όμοια.

$\mathbb{Z}_{14} = \langle [1] \rangle = \langle [3] \rangle$

Γεννήτορας είναι αυτοί που είναι πρώτοι με το 14

δηλ. $\phi(14) = \phi(2\cdot 7) = \phi(2)\cdot\phi(7) = 6$.

<u>Θεώρημα</u>: Έστω $G = \langle \alpha \rangle$ κυκλική. Αν $o(\alpha) = \infty$ τότε $\alpha^k \neq \alpha^l$ για $k \neq l$. Αν $o(\alpha) = n$, τότε $\alpha^k = \alpha^l \iff k \equiv l \bmod n$.

απόδειξη: Έστω $k \neq l$. Αν είχαμε $\alpha^k = \alpha^l$ με $k<l$ $\Rightarrow \alpha^k \cdot \alpha^{-k} = \alpha^l \cdot \alpha^{-k}$
$\Rightarrow \alpha^0 = \alpha^{l-k} \Rightarrow 1 = \alpha^{l-k} \Rightarrow o(\alpha) \mid l-k > 0$ και $o(\alpha) = \infty$
Αδύνατο

Έστω $o(\alpha) = n$ και $\alpha^k = \alpha^l$ με $k < l \Rightarrow \alpha^k \cdot \alpha^{-k} = \alpha^l \cdot \alpha^{-k} \Rightarrow$

$\Rightarrow 1 = a^{l-k} \Rightarrow n \mid l-k \Leftrightarrow l-k \equiv 0 \bmod n \Leftrightarrow l \equiv k \bmod n.$

<u>Προταση</u>: Αν G κυκλική, τοτε G αβελιανή.

<u>Προσοχή</u>! $\mathbb{Q}$ αβελιανή αλλα δεν ειναι κυκλική.