10/3/17 Μαθημα 3ο

• $(\mathbb{N}, +, \cdot)$

$\mathbb{N} \times \mathbb{N} /_{\Sigma\chi\epsilon\sigma\eta} \rightarrow$ κλασεις ισοδυναμιας $= \{ [\overset{n}{\underset{\uparrow}{(n,0)}}], [\overset{-m}{\underset{\uparrow}{(0,m)}}] \mid n, m \in \mathbb{N} \} =$

$= \mathbb{Z} = \{0, \pm 1, \ldots\}$

Πράξη στο $\mathbb{N}$ περνάει στο $\mathbb{Z} \equiv$ Η πράξη δεν εξαρτάται απο τον αντιπρόσωπο της κλάσης (όπως στα modula). Η πράξη καλείται συμβιβαστή με την σχέση.

$[(n,0)] \oplus [(n',0)] = [(n+n',0)]$

$[(n,0)] \oplus [(0,m)] = [(n,m)]$

Η πράξη του πολ/σμου: $[(n,0)] \odot [(n',0)] = [(nn',0)]$

$[(n,0)] \odot [(0,m)] = [(0,nm)]$

$[(0,m)] \odot [(0,m')] = [(mm',0)]$

- $(\mathbb{Z}, +)$ είναι αβελιανή ομάδα
- $(\mathbb{Z}, \cdot)$ είναι μονοειδές, αβελιανό

$\mathbb{Z} \times \mathbb{Z}^*$ σχέση ισοδυναμίας

$(\alpha, \beta) R (\alpha', \beta') \Leftrightarrow \alpha\beta' = \beta\alpha'$

κλάσεις ισοδυναμίας:

$[(\alpha, \beta)]$ $\beta \in \mathbb{N}^*$, α, β πρώτοι μεταξύ τους.

$\downarrow$

$\frac{\alpha}{\beta} = \frac{\kappa\alpha}{\kappa\beta}$, $\kappa \neq 0$

$\mathbb{Q} = \{ [(\alpha,\beta)] \ \beta \in \mathbb{N}^*, \ \alpha, \beta$ πρώτοι μεταξύ τους $\} =$
$= \{ \frac{r}{q} \mid r \in \mathbb{Z}, q \in \mathbb{N}^*, (r,q) = 1 \}$
$[(r,q)]$

$(\mathbb{Q}, +)$ αβελιανή ομάδα
$(\mathbb{Q}^*, \cdot)$ αβελιανή ομάδα
Οι πράξεις εδώ συνδέονται με την επιμεριστική ιδιότητα.

Ορισμός: Έστω μια πράξη $\odot$ στο σύνολο $A : \odot \ A \times A \to A$ $(\alpha, \beta) \mapsto \alpha \odot \beta$ και μια σχέση ισοδυναμίας R στο A. Θα λέμε ότι η σχέση R είναι συμβιβαστή με την πράξη $\odot$, αν ισχύει $\alpha R b \Rightarrow \alpha \odot \gamma \, R \, b \odot \gamma$ (δεξιά συμβ.) και $\gamma \odot \alpha R \gamma \odot b$ (αριστερά συμβιβαστή) $\forall \alpha, b, \gamma \in A$.

π.χ. Οι πράξεις πρόσθεσης και πολλαπλασιασμού του $\mathbb{Z}$ στα modulo $\bmod n$ = σχέση στο $\mathbb{Z}$ πως; έτσι $\alpha R b$ ή $\alpha \equiv b \bmod n \Leftrightarrow \alpha - b$ διαιρείται από τον n.

Πράξεις: Να βρεθούν πραγματικοί α και b ώστε η πράξη $* : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ με τύπο $(x,y) \mapsto x * y = \alpha x + b y$ να είναι προσεταιριστική.

Λύση
$(x * y) * z = x * (y * z)$
$(x * y) * z = (\alpha x + b y) * z = \alpha(\alpha x + b y) + b z = \alpha^2 x + \alpha b y + b z$

$x * (y * z) = x * (\alpha y + b z) = \alpha x + b(\alpha y + b z) =$
$= \alpha x + b \alpha y + b^2 z$

$\alpha^2 x + \cancel{\alpha b y} + b z = \alpha x + \cancel{b \alpha y} + b^2 z \Rightarrow$
$\alpha(\alpha - 1)x + b(1 - b)z = 0.$

Πρέπει $\alpha(\alpha-1)=0 \Rightarrow \alpha=0$ ή $\alpha=1$

$\beta(\beta-1)=0 \Rightarrow \beta=0$ ή $\beta=1$

Έχω 4 πράξεις $\alpha=0$ κ $\beta=0$

$\alpha=0$ κ $\beta=1$

$\alpha=1$ κ $\beta=1$

$\alpha=1$ κ $\beta=0$.

$a=b=0$	αν $\alpha=0,\ \beta=1$	αν $\alpha=1,\ b=0$	$\alpha=\beta=1$
$x*y=0$	$x*y=y$	$x \cdot y=x$	$x*y=x+y$

Π.χ.

Δίνεται το $A=\{\alpha,\beta,\gamma,\delta\}$ και μια πράξη $*$ η οποία περιγράφεται από το ακόλουθο πινακάκι. Εξετάστε αν είναι αντιμεταθετική, έχει ουδέτερο-μοναδιαίο είναι προσεταιριστική.

$*$	α	β	γ	δ
α	α	β	γ	δ
β	β	γ	δ	α
γ	γ	δ	α	β
δ	δ	α	β	γ

π.χ. $\gamma*\delta=\beta$

$\delta*\gamma=\beta$

Λύση

Ο πίνακας είναι συμμετρικός ως προς την διαγώνιο, άρα είναι αντιμεταθετικός.

Το α είναι μοναδιαίο (αφού $\alpha\cdot\alpha=\alpha$, $\alpha\cdot\beta=\beta$, $\alpha\cdot\gamma=\gamma$, $\alpha\cdot\delta=\delta$)

Βασικές ιδιότητες: Το ζεύγος $(G,*)$ θα είναι ομάδα. Τότε ισχύουν:

1) Το μοναδιαίο είναι μοναδικό.

2) Το αντίστροφο είναι μοναδικό

3) Αν g^{-1} είναι ο αντίστροφος του g, τότε $(g^{-1})^{-1} = g$ $\forall g \in G$.

4) Ισχύει $(g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1}$

5) Αν είναι αβελιανή ισχύει: $(g_1 * g_2)^{-1} = g_1^{-1} * g_2^{-1}$

6) Αν $\left.\begin{array}{l} g_1 * g_2 = g_1 * g_3 \Rightarrow g_2 = g_3 \\ g_2 * g_1 = g_3 * g_1 \Rightarrow g_2 = g_3 \end{array}\right\}$ ιδιότητα διαγραφής

Απόδειξη

1) Έστω ότι υπάρχουν δυο μοναδιαία: e κ e'. Δηλαδή $\forall g \in G$ ισχύει: $g = g * e = e * g = e' * g = g * e'$

$\underset{g}{e'} = e' \cdot e = e$

$\uparrow$ e μοναδ. ; e' μοναδ.

2) Έστω ότι $g_1 * g = e = g * g_1 = g_2 * g = g * g_2$ για τυχαίο g. Θ.δ.ο $g_1 = g_2$.

$g_1 = g_1 * e = g_1 * (g * g_2) \overset{\text{προσεταιριστική}}{=} (g_1 * g) * g_2 = e * g_2 \overset{\text{μοναδ.}}{=} g_2$

3) Εφόσον ο αντίστροφος είναι μοναδικός, συμβολίζουμε με g^{-1}. Άρα $g * g^{-1} = e$. Ο αντίστροφος του (g^{-1}) είναι ο $(g^{-1})^{-1}$ και ισχύει $g^{-1} * (g^{-1})^{-1} = e$ και επίσης ισχύει $g^{-1} * g = e$. Ο αντίστροφος είναι μοναδικός άρα $g = (g^{-1})^{-1}$.

4) $(g_1 * g_2)^{-1} (g_1 * g_2) = e$

$(g_1 * g_2) \cdot (g_2^{-1} * g_1^{-1}) \overset{\text{προσ.}}{=} g_1 \cdot (g_2 * (g_2^{-1} * g_1^{-1})) \overset{\text{προσ.}}{=}$

$= g_1 * ((g_2 * g_2^{-1}) * g_1^{-1}) \overset{\text{μοναδ.}}{=} g_1 * (e * g_1^{-1}) \overset{\text{μοναδ.}}{=} g * g_1^{-1} = e.$

Αντιστροφος μοναδικος $\Rightarrow (g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1}$

6) $g_1 * g_2 = g_1 * g_3 \Rightarrow g_1^{-1} * (g_1 * g_2) = g_1^{-1} * (g_1 * g_3)$

$\overset{\text{προσ.}}{\Rightarrow} (g_1^{-1} * g_1) * g_2 = (g_1^{-1} * g_1) * g_3 \Rightarrow g_2 = g_3$

Ομαδα: Προσεταιριστική
Μοναδιαιο-Ουδετερο $g * e = g = e * g$
Αντιστροφο-Αντιθετο $\forall g \; \exists g^{-1} : g * g^{-1} = e = g^{-1} * g$

Συμβολισμός: Αν η πράξη είναι αβελιανή:
$g * g' = g' * g$, τοτε θα συμβολίζουμε την πράξη με +.
Σ' αυτην την περίπτωση το μοναδιαιο θα συμβολίζεται
με 0. Αν δεν γνωρίζουμε θα χρησιμοποιούμε το
συμβολο του πολ/μου και μοναδιαιο το επί 1.

π.χ

$\left.\begin{array}{l}(\mathbb{Z},+) \subseteq (\mathbb{Q},+) \subseteq (\mathbb{R},+) \subseteq (\mathbb{C},+) \\ (\mathbb{Q}^*,\cdot) \subseteq (\mathbb{R}^*,\cdot) \subseteq (\mathbb{C}^*,\cdot)\end{array}\right\}$ Απειρες

$(\mathbb{Z}_3,+) \dots, (\mathbb{Z}_n,+)$ ομάδες αβελιανες πεπερασμενες

$(\mathbb{Z}_3^*, \cdot)$ αβελιανή ομάδα : ΟΧΙ $(\mathbb{Z}_4^*, \cdot)$
ΝΑΙ $(\mathbb{Z}_p^*, \cdot)$

μονο οταν $\mathbb{Z}_n^*$ το n είναι πρωτος.

$q = p_1^{k_1} \cdots p_\ell^{k_\ell}$ πρώτοι $\neq p_i$

το $\frac{1}{p}$ δεν γίνεται να γραφεί ως $\frac{kr}{q}$ αδύνατον.

Ορισμός: Μια ομάδα $(O,+)$ καλείται κυκλική, αν υπάρχει στοιχείο $\alpha \in O$ ώστε $\forall b \in O$ ισχύει $b = \underbrace{\alpha + \dots + \alpha}_{k\text{-φορές}}$.
Δηλ. κάθε στοιχείο δημιουργείται από το α, τότε γράφουμε $O = \langle a \rangle$ και ο α καλείται γεννήτορας

π.χ. $(Z_n,+)$ είναι κυκλική με $Z_n = \langle 1_n \rangle$ πεπερασμένη

$(Z_n,+)$ » $Z = \langle 1 \rangle = \langle -1 \rangle$ άπειρη

$(Z_3,+)$ $Z_3 = \langle 1_3 \rangle$ $0 \xrightarrow{+1} 1 \xrightarrow{+1} 2$

γι' αυτό λέγεται κυκλική

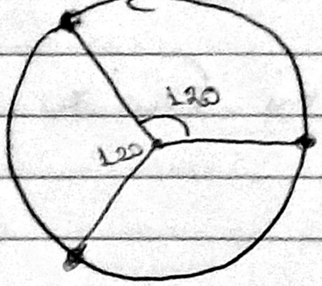
C: Μιγαδικοί

$\alpha + bi \to k(\alpha + bi) = 0$ με $k = 1, 2, \dots$

↳ ή $k = 0$ αδύνατο

ή $\alpha + bi = 0$ αδύνατο

$S' = \{(\cos\theta + i\sin\theta) \mid 0 \le \theta \le 2\pi\}$



αν πάρω $\cos\theta + i\sin\theta$ και το πολ/ω με $(\cos\theta' + i\sin\theta')$ έχω:

$(\cos\theta + i\sin\theta)(\cos\theta' + i\sin\theta') = \cos(\theta+\theta') + i\sin(\theta+\theta')$

$x_0 = \cos 120 + i\sin 120$

$x_0^2 = \cos 240 + i\sin 240$

$x_0^3 = 1$

$\{1, (\cos 120 + i\sin 120), (\cos 240 + i\sin 240)\} \le S'$

είναι ομάδα.

$\mathbb{C}^*$ $\exists \alpha+\beta i$ ώστε $(\alpha+\beta i)^k = 1$.

Ορισμός: Έστω $(O, \cdot)$ ομάδα και $\alpha \in O$.
Ο μικρότερος φυσικός k αν υπάρχει ώστε $\alpha^k = 1_O = e_O$ καλείται
τάξη του α και συμβολίζεται $o(\alpha) = k$ (order).
π.χ. 1) Το μοναδιαίο είναι το μοναδικό με τάξη 1

$$\left[\alpha^k = \alpha \cdot \alpha \cdots \alpha = 1 \rightarrow \alpha + \alpha + \dots + \alpha = 0 \Leftrightarrow k\alpha = 0\right]$$

2) Το 1 στο $\mathbb{Z}_n$ έχει τάξη n.
3) Το 1 στο $\mathbb{Z}$ έχει άπειρη τάξη
4) Το 1 στο $\mathbb{Q}^*$ $o(1) = 1$
5) $o(2) = \infty$ στο $\mathbb{C}^*$.
6) $o(i) = 4$ στο $\mathbb{C}^*$.
$i, i^2 = -1, i^3 = -i, i^4 = 1$.

Ορισμός: Μια ομάδα θα λέμε ότι έχει πεπερασμένη τάξη αν έχει πεπερασμένο πλήθος στοιχείων. Αλλιώς είναι άπειρης τάξης. Γράφουμε $|O| = \begin{cases} \to k \\ \to \infty \end{cases}$.

Παρατήρηση: Το $(\mathbb{Q}, +)$ δεν είναι κυκλική. Ενώ το $\mathbb{Z} \leq \mathbb{Q}$ είναι κυκλική.

Ιδιότητες: Έστω $(O, \cdot)$ ομάδα και $\alpha \in O$.
1) $\alpha^k \cdot \alpha^m = \alpha^{k+m}$
2) $(\alpha^k)^m = \alpha^{km}$
3) $(\alpha^{-1})^k = \alpha^{-k} = (\alpha^k)^{-1}$, $k, m \in \mathbb{Z}$

Προταση: Εστω $(O, \cdot)$ ομαδα και $\alpha \in O$.

α) $O(\alpha) = O(\alpha^{-1})$

β) Αν $O(\alpha) = n$ και $\alpha^m = 1_O = e_O$, τοτε ο n διαιρει τον m

γ) Αν $O(\alpha) = n$, τοτε $O(\alpha^m) = \frac{n}{(n,m)}$ ← ΜΚΔ.

αποδειξη:

α) Υποθετω οτι $O(\alpha) = k < \infty \Leftrightarrow \alpha^k = e \Leftrightarrow \alpha^{-k} = e^{-1} = e$

$(\alpha^{-1})^k = e \Rightarrow O(\alpha^{-1}) \leq k.$

Αν ειχαμε $O(\alpha^{-1}) = m < k \Rightarrow (\alpha^{-1})^m = e \Rightarrow \alpha^m = e^{-1} = e$

$\Rightarrow O(\alpha) < m < k = O(\alpha)$ αδυνατο.

Υποθετουμε οτι $O(\alpha) = \infty$ και $O(\alpha^{-1}) = k < \infty$

$(\alpha^{-1})^k = e \Rightarrow (\alpha^{-k}) = e \Rightarrow \alpha^k = e^{-1} = e \Rightarrow O(\alpha) < k$ αδυνατο

∞

π.χ. $O(1) = O(-1) = \infty$ στο $\mathbb{Z}$.