19/3/2018

▶ Άσκηση 1 $\mathbb{Z}_{10}$ $\quad H = \langle 2 \rangle$

• Βρείτε όλα τα αριστερά σύμπλοκα της $\langle 2 \rangle$ στο $\mathbb{Z}_{10}$

• <u>Έχω</u>: $H = \langle 2 \rangle = \{ [0]_{10}, [2]_{10}, [4]_{10}, [6]_{10}, [8]_{10} \}$

• <u>Επίσης</u>: • $[0]+H = H = \{[0], [2], [4], [6], [8]\}$

• $[1]+H = \{[1], [3], [5], [7], [9]\}$

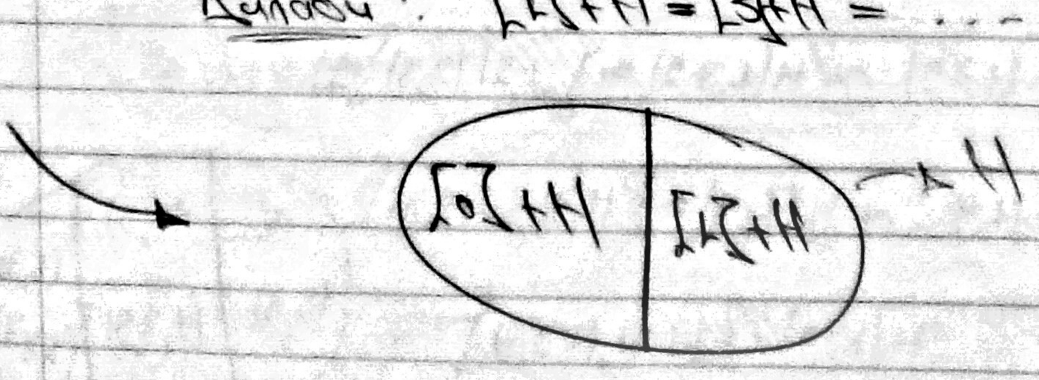
• <u>Άρα</u>: $\mathbb{Z}_{10} = ([0]+H) + ([1]+H)$

<u>και</u>: $([0]+H) \cap ([1]+H) = \emptyset$

• <u>Συνεπώς</u>, τα <u>αριστερά</u>, αλλά και τα <u>δεξιά</u> σύμπλοκα (λόγω <u>μεταθετικότητας</u> της πράξης σε $\mathbb{Z}_{10}$) είναι τα: $\boxed{[0]+H}$ και $\boxed{[1]+H}$.

⚠ Δύο κλάσεις ισοδυναμίας, αν έχουν ένα κοινό στοιχείο, τότε θα ταυτίζονται αναγκαστικά.

<u>Δηλαδή</u>: $[1]+H = [3]+H = \ldots = [9]+H$



Πρόταση: Κάθε αριστερό (δεξιό) σύμπλοκο αH, έχει ακριβώς τόσα στοιχεία όσα και η H!

$$H \xrightarrow{\varphi} \alpha H$$

Απόδειξη.

• Ορίζω απεικόνιση: $\boxed{\varphi(h)=\alpha h}$ και έχω:

• Η φ είναι καλά ορισμένη, αφού για $h\in H \Rightarrow \alpha h \in \alpha H$

• Έχω: $\varphi(h_1)=\varphi(h_2) \Rightarrow \alpha h_1=\alpha h_2 \Rightarrow \underbrace{\alpha^{-1}\alpha}_{e_H} h_1 = \underbrace{\alpha^{-1}\alpha}_{e_H} h_2 \Rightarrow$

$$\Rightarrow \boxed{h_1=h_2} \Rightarrow \boxed{\varphi: \text{"1-1"}}$$

• Έστω: $y\in\alpha H \Rightarrow y=\alpha h_0 \Rightarrow \varphi(h_0)=\alpha h_0 = y \Rightarrow$

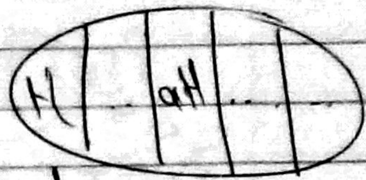
$$\Rightarrow \varphi(h_0)=y \Rightarrow \boxed{\varphi: \text{επί}}$$

• Άρα τα δύο σύνολα H και αH έχουν το ίδιο πλήθος στοιχείων.

• Συμβολισμός: $\boxed{|H| = \#\alpha H}$ ▸ Διότι δεν μπορούμε να αποφανθούμε αν η αH είναι ομάδα ή όχι

▸ Θεώρημα Lagrange: Έστω H μία υποομάδα μιας πεπερασμένης ομάδας G. Τότε η τάξη της H είναι διαιρέτης της τάξης της G.

▸ Απόδειξη:



• Έχω: $|G| = n$ και $|H| = d$

• Έστω r: το πλήθος των αριστερών συμπλόκων. Τότε:

$$n = |G| = r \cdot d \Rightarrow \boxed{d \mid n}$$ Αποδείχθηκε!!

(r: Το πλήθος των αριστερών συμπλόκων) (d: πλήθος στοιχείων κάθε συμπλόκου aH, με $\# aH = d = |H|$)

▸ Θεώρημα: Κάθε ομάδα με τάξη πρώτο αριθμό, είναι κυκλική!

▸ Απόδειξη: Έστω G: ομάδα με $|G| = p$, με p: πρώτο

• Έστω $a \in G$, με $a \neq 1$ (τέτοιο a υπάρχει διότι διαφορετικά: $G = \{1\} \Rightarrow \boxed{p = 1}$) Άτοπο

• Τότε, για $H < G$, με $H = \langle a \rangle$, έχω:

(Lagrange) $|H| \mid |G| = p \Rightarrow |H| = 1$ ή $|H| = p$.

• Όμως: $1 \in H$ και $1 \neq a \in H \Rightarrow \boxed{|H| \geq 2}$

$$\Rightarrow \boxed{|H| = p}$$

$$\Rightarrow \begin{cases} |H| = p \\ H \leq G \\ |H| = |G| = p \end{cases} \Rightarrow \langle \alpha \rangle = H = G \Rightarrow \boxed{G = \langle \alpha \rangle}$$

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

$\boxed{\blacktriangleright \text{Θεώρημα}}$ Η τάξη ενός στοιχείου είναι διαιρέτης της τάξης της ομάδας.

$\blacktriangleright$ Απόδειξη: $|G| = n$. Θεωρώ $\alpha \in G$. Τότε:

$$\begin{rcases} \cdot\ ord(\alpha) = |\langle \alpha \rangle| \\ \cdot\ \langle \alpha \rangle \leq G \end{rcases} \xrightarrow{\text{Lagrange}} |\langle \alpha \rangle| \,\big|\, |G| = n \Rightarrow$$

$$\Rightarrow \boxed{ord(\alpha) \mid n}.$$

$\boxed{\blacktriangleright \text{Θεώρημα Euler}}$ Έστω $\alpha \in \mathbb{Z}$, n: φυσικός και: $\text{μκδ}(\alpha, n) = 1$. Τότε: $\alpha^{\varphi(n)} \equiv 1 \mod n$

$\blacktriangleright$ Απόδειξη: $\text{μκδ}(\alpha, n) = 1 \Rightarrow [\alpha] \in U(\mathbb{Z}_n)$ και $|U(\mathbb{Z}_n)| = \varphi(n)$ $\Bigg\} \Rightarrow$

$$\xrightarrow{\text{Θεώρημα}} \boxed{ord([\alpha]) \mid \varphi(n)} \Rightarrow \boxed{\varphi(n) = ord([\alpha]) \cdot m} \quad (1)$$

$$\cdot\ [\alpha]_n^{ord([\alpha])} = 1 \Rightarrow \left([\alpha]_n^{ord([\alpha])}\right)^m = 1^m = 1 \mod n \Rightarrow$$

$$\Rightarrow [\alpha]_n^{ord([\alpha]) \cdot m} \overset{(1)}{=} 1 \mod n \Rightarrow \boxed{[\alpha]_n^{\varphi(n)} = 1 \mod n}$$

Άσκηση 1 ($S = \mathbb{R}\setminus\{0\}$, $S \times S \longrightarrow S$, με $\alpha * b = |\alpha| \cdot b$

(i) καλά ορισμένη (ii) Προσεταιριστική
(iii) ($\exists e \in S$) : $e * b = b$, $\forall b \in S$
(iv) αν $\alpha \in S$, τότε υπάρχει $b \in S$: $\alpha * b = e$
(v) Έχει η S ουδέτερο? Είναι ομάδα?

Λύση: (i) Έστω $(\alpha, b) \in S \times S \Rightarrow \alpha \neq 0$ και $b \neq 0$

• Έστω : $\alpha * b = |\alpha| \cdot b = 0 \Longrightarrow \alpha = 0$ ή $b = 0$

$\Longrightarrow \alpha \notin S$ ή $b \notin S$. Άτοπο! αφού $(\alpha, b) \in S \times S$.

• Άρα $\alpha * b \in S$ $\Longrightarrow$ Άρα η $*$: καλά ορισμένη!

(ii) Για $\alpha, b, c \in S$, έχω:

$$\cdot\ \alpha * (b * c) = \alpha * (|b| \cdot c) = \boxed{|\alpha| \cdot |b| \cdot c}$$

$$\|$$

και :

$$\cdot\ (\alpha * b) * c = (|\alpha| \cdot b) * c = \boxed{|\alpha||b| \cdot c}$$

• Άρα η $*$: Προσεταιριστική!

(iii) Για $e = \pm 1 \in S \Rightarrow e * b = |e| \cdot b = 1 \cdot b = \boxed{b}$

(Όχι, ομάδα λόγω μοναδικότητας ουδετέρου.)

(iv) Για $\alpha \in S$, έχω: $\alpha * 1/|\alpha| = |\alpha| \cdot \frac{1}{|\alpha|} = \boxed{1} = e$

(ii): $\alpha * \left(-\frac{1}{|\alpha|}\right) = |\alpha| \cdot \left(-\frac{1}{|\alpha|}\right) = \boxed{-1} = e$

(v) Το S, δεν έχει ουδέτερο, καθώς:

$$\alpha * e = \alpha \Rightarrow |\alpha| \cdot e = \alpha \Rightarrow \boxed{e=1} \text{ ή } \boxed{e=-1}$$

Άτοπο!, λόγω μοναδικότητας.

• Καθώς η S δεν έχει ουδέτερο στοιχείο, δεν θα είναι ομάδα!!!

▶ Άσκηση Έστω G: σύνολο και $*$: μία πράξη στο G, τέτοια, ώστε:

Είναι δίχαρα, καλά ορισμένη

(i) Η $*$ είναι προσεταιριστική

(ii) Υπάρχει $e \in G$: $e * \alpha = \alpha$, $(\forall \alpha \in G)$

(iii) Για κάθε $\alpha \in G$, υπάρχει $\alpha' \in G$, τέτοιο ώστε:

$$\alpha' * \alpha = e$$

• Τότε η G είναι ομάδα!

▶ Απόδειξη: (iii) Έστω $\alpha \in G$. Υπάρχει $\alpha' \in G$, όπου:

$(\alpha')' \in G \Longrightarrow \alpha'' \in G$ να ο αντίστροφος του αντιστρόφου!!

• Έχω: $\alpha * \alpha' = e * (\alpha * \alpha') = (\alpha'' * \alpha') * (\alpha * \alpha') =$

$= \alpha'' * (\alpha' * \alpha) * \alpha' = \alpha'' * (e * \alpha') = \alpha'' * \alpha' = \boxed{e}$

$\Rightarrow \boxed{\alpha * \alpha' = e} \Rightarrow \boxed{\alpha' * \alpha = \alpha * \alpha' = e}$

(ii) • Έχω: $\alpha * e = \alpha * (\alpha' * \alpha) = (\alpha * \alpha') * \alpha = e * \alpha = \boxed{\alpha}$

$\Rightarrow \boxed{\alpha * e = e * \alpha = \alpha}$

• Συνεπώς, η G πληροί τις προϋποθέσεις μιας ομάδας.

• Άρα $\boxed{G: \text{ομάδα}}$

$\boxed{\blacktriangleright \text{Άσκηση}}$ $G = (-1, 1) \subset \mathbb{R}$ και $x * y = \dfrac{x+y}{1+xy}$.

• Κλειστότητα: Έστω ότι: $x * y \notin G$, για $x, y \in G$

Τότε: $x * y = 1 \notin G \Rightarrow \dfrac{x+y}{1+xy} = 1 \Rightarrow x + y = 1 + xy \Rightarrow$

$\Rightarrow (x-1)(y-1) = 0 \Rightarrow \boxed{x = 1}$ ή $\boxed{y = 1}$ Άτοπο, διότι $x, y \in G$!

• Άρα $*$: καλά ορισμένη!

• **Προσεταιριστικότητα**: Για $x, y, z \in G$, έχω:

• $(x*y)*z = \frac{x+y}{1+xy} * z = \frac{\frac{x+y}{1+xy}+z}{1+\frac{x+y}{1+xy}\cdot z} = \frac{\frac{x+y+z(1+xy)}{\cancel{1+xy}}}{\frac{1+xy+xz+yz}{\cancel{1+xy}}} =$

$$= \boxed{\frac{x+y+z+xyz}{1+xy+xz+yz}}$$

• **Ομοίως**:

$$x*(y*z) = \boxed{\frac{x+y+z+xyz}{1+xy+xz+yz}}$$

• **Άρα**, ισχύει η προσεταιριστική ιδιότητα!

• Θα δείξω ότι είναι **αβελιανή**:

$$x*y = \frac{x+y}{1+xy} = y*x$$ (διότι η πρόσθεση και ο πολ/μός είναι μεταθετικές στους πραγματικούς)

• **Ουδέτερο στοιχείο**: Αναζητώ $e \in G$, τέτοιο ώστε:

$$e*x = x \Rightarrow \frac{e+x}{1+ex} = x.$$

Για $\boxed{e = 0 \in G}$, έχω ότι $e*x = x = x*e$

• **Αντίστροφος**: Αναζητώ $a' \in G$, τέτοιο ώστε:

$$a*a' = e = 0 \Rightarrow \frac{a+a'}{1+aa'} = 0.$$

• Για $\boxed{a' = -a \in G}$, έχω ότι: $a*a' = e = a'*a$

• **Άρα**, η G είναι ομάδα!!!

▶ Άσκηση Έστω $(G,*)$ ομάδα, με e, το ουδέτερο.

Αν $|G| = 2\nu$, τότε υπάρχει α, με $\alpha \neq e$, τ.ω.:

$$\boxed{\alpha * \alpha = e}$$

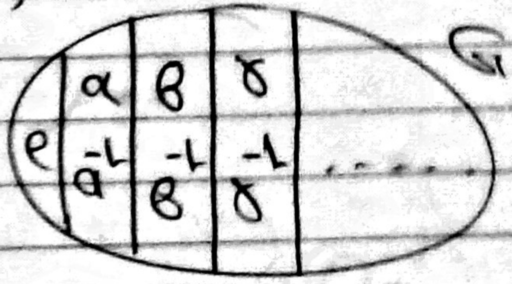
▶ Λύση: Έστω ότι δεν υπάρχει α, με $\alpha \neq e$, τ.ω.:

$$\boxed{\alpha * \alpha = e.} \Longrightarrow$$

$\Longrightarrow$ Για κάθε $\alpha \in G$, με $\alpha \neq e$, το $\boxed{\alpha^{-1} \neq \alpha}$

• Μπορώ να γράψω την G, ως εξής:

$$\boxed{G = \{e\} \cup \Big(\bigcup_{\substack{\alpha \in G \\ \alpha \neq e}} \{\alpha, \alpha^{-1}\} \Big)}$$



• **Έχω**: $\underbrace{2\nu}_{\text{άρτιος}} = |G| = 1 + 2\lambda$, **Άτοπο!!!**

• **Άρα**, υπάρχει $\alpha \in G$, τέτοιο ώστε: $\boxed{\alpha \neq e}$ & $\boxed{\alpha * \alpha = e}$

▶ Άσκηση 5 $(G,*)$, $a,b,c \in G$. Ν.δ.ο. είναι ισοδύναμα τα:

(i) $a*b*c = e$

(ii) $b*c*a = e$

(iii) $c*a*b = e$

▸ **Λύση**: • **Έχω**: $a*(b*c) = e = (b*c)*a \Rightarrow$

$\Rightarrow$ i $\Leftrightarrow$ ii

• **Έχω**: $(a*b)*c = e = c*(a*b) \Rightarrow$

$\Rightarrow$ i & $\Rightarrow$ iii

• **Και**: Αφού: i $\Leftrightarrow$ ii & i & $\Rightarrow$ iii $\Rightarrow$

$\Rightarrow$ $\boxed{\text{ii} \ \& \Rightarrow \text{iii}}$

▸ **Άσκηση 6**: $\mathbb{C} = \mathbb{R}^2$ και:

$$\cdot (a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$$

$$\cdot (a_1, b_1) \cdot (a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1)$$

▸ **Λύση**: (α) ▸ Για την $(\mathbb{C}, +)$:

• **Προφανώς**: $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1, b_2) \in \mathbb{R}^2$.

• **Επίσης**, για $e = (0,0) \in \mathbb{R}^2$, έχω:

$$\cdot (a_1, b_1) + (0,0) = (a_1, b_1) \ ✓$$

• **Και**: για $(a_1, b_1)^{-1} = (-a_1, -b_1)$, έχω:

$$\cdot (a_1, b_1) + (a_1, b_1)^{-1} = (a_1, b_1) - (a_1, b_1) = (0,0) = e \ ✓$$

• Η προσεταιριστικότητα είναι προφανής!!!

· **Άρα**, η $(\mathbb{C},+)$ είναι **αβελιανή ομάδα**, καθώς η **πρόσθεση $(+)$** είναι μεταθετική πράξη!

▶ **Για την $(\mathbb{C}\setminus\{(0,0)\},\cdot)$:**

Απόσπασμα

· **Έστω** ότι: $(a_1a_2-b_1b_2,\ a_1b_2+a_2b_1)=(0,0) \Rightarrow$

$$\Rightarrow \begin{cases} a_1a_2-b_1b_2=0 \\ a_1b_2+a_2b_1=0 \end{cases}$$

· Παίρνω τους συζυγείς των (a_1,b_1) & (a_2,b_2):

Έχω: $(a_1,-b_1)(a_2,-b_2)=(0,0) \Rightarrow (a_1a_2-b_1b_2,\ a_1(-b_2)+a_2(-b_1))$
$=(0,0)$

$$\Rightarrow \begin{cases} a_1a_2-b_1b_2=0 \\ a_1b_2+a_2b_1=0 \end{cases}$$

· **Όμως**: $(a_1,b_1)\cdot(a_2,b_2)\cdot(a_1,-b_1)(a_2,-b_2)=(0,0) \Rightarrow$

$\Rightarrow (a_1,b_1)(a_1,-b_1)\cdot(a_2,b_2)(a_2,-b_2)=(0,0) \Rightarrow$

$\Rightarrow (a_1^2+b_1^2,\ -a_1b_1+a_1b_1)\cdot(a_2^2+b_2^2,\ -a_2b_2+a_2b_2)=(0,0)$

$\Rightarrow (a_1^2+b_1^2,0)\cdot(a_2^2+b_2^2,0)=(0,0) \Rightarrow$

$\Rightarrow ((a_1^2+b_1^2)\cdot(a_2^2+b_2^2)+0,\ 0)=(0,0) \Rightarrow \boxed{(a_1^2+b_1^2)(a_2^2+b_2^2)=0}$

$$\Rightarrow \begin{cases} a_1^2+b_1^2=0 \\ a_2^2+b_2^2=0 \end{cases} \Rightarrow \begin{cases} |(a_1,b_1)|=0 \\ |(a_2,b_2)|=0 \end{cases}$$

Άτοπο!!!

• **Προσεταιριστική**: Είναι προφανής μέσω πράξεων...

, για $(\alpha_1,b_1),(\alpha_2,b_2),(\alpha_3,b_3) \in \mathbb{C} = \mathbb{R}^2$

• **Μεταθετική**: Για $(\alpha_1,b_1),(\alpha_2,b_2) \in \mathbb{R}^2$:

$$(\alpha_1,b_1)\cdot(\alpha_2,b_2) = (\alpha_2,b_2)\cdot(\alpha_1,b_1) \Rightarrow \ldots$$

• **Ουδέτερο**: Για $e=(1,0) \in \mathbb{R}^2$, έχω ότι:

για $(\alpha,b) \in \mathbb{R}^2$: $(\alpha,b)\cdot(1,0) = (\alpha,b)$

• **Αντίστροφος**: Για $\left(\frac{\alpha}{\alpha^2+\beta^2}, -\frac{\beta}{\alpha^2+\beta^2}\right) \in \mathbb{R}^2$, έχω:

$$(\alpha,\beta)\cdot\left(\frac{\alpha}{\alpha^2+\beta^2}, -\frac{\beta}{\alpha^2+\beta^2}\right) = (1,0) = e$$