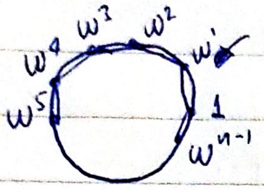
$U_n = \{a \in \mathbb{C} \mid a^n = 1\} \subseteq \mathbb{C}$

οι n-οστές ρίζες της μονάδας.

$= \left\{ \text{συν}\left(\frac{2k\pi}{n}\right) + i\,\text{ημ}\left(\frac{2k\pi}{n}\right) \mid 0 \le k \le n-1 \right\}.$



κανονικό n-γωνο. $= \left\{ \omega^k \mid 0 \le k \le n-1,\ \omega = \text{συν}\left(\frac{2\pi}{n}\right) + i\,\text{ημ}\left(\frac{2\pi}{n}\right) \right\}$

$= \{1, \omega, \omega^2, \omega^3, \dots, \omega^{n-1}\}$ με $|U_n| = n$

$U_1 = \{1\}$, $U_2 = \{1, -1\}$.

$\boxed{\text{Δευτέρα} \quad 25/02/2019}$

Άσκηση: Έστω G ομάδα τ.ω. $a * a = e$ για $\forall a \in G$. Δ.ό. η G είναι αβελιανή.

Έστω $a, b \in G$, τότε $(a*b)*(a*b) = e \Rightarrow a*a*(b*(a*b)) = a*e \Rightarrow e*(b*a)*b*b = a*b$

$a*b \in G$.

$\Rightarrow (b*a)*e = a*b \Rightarrow a*b = b*a.$

Υποομάδες μιας ομάδας G:

Παραδείγματα: (i) $SL_n(\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} \mid \det A = 1\}$

$GL_n(\mathbb{R}) = \{A \in \mathbb{R}^{n\times n} \mid \det A \neq 0\}$

$SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$ (υποομάδα)

(ii) $\mathbb{Q}$ ομάδα $= (\mathbb{Q}, +)$.

$\mathbb{Q}^* = (\mathbb{Q}^*, \cdot)$ ομάδα

$\mathbb{Q}^* \subset \mathbb{Q}$ (όχι υποομάδα διότι έχουν διαφορετικές πράξεις).

Ορισμός: Έστω $(G, *)$ ομάδα και S υποσύνολο του G. Αν $\forall a, b \in S$ ισχύει ότι το γινόμενο $a*b \in S$ τότε λέμε ότι το S είναι κλειστό ως προς την πράξη $*$ της G.

Παράδειγμα: $(\mathbb{Z}, +)$, $A = 2\mathbb{Z} = \{2k, k \in \mathbb{Z}\}$ άρτιοι

Το A είναι κλειστό ως προς την πρόσθεση +.

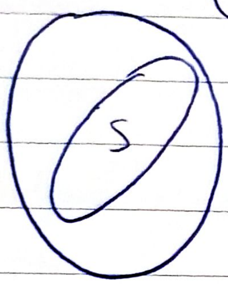
$B = 2\mathbb{Z}+1 = \{2k+1, k \in \mathbb{Z}\}$

Το B δεν είναι κλειστό ως προς την πράξη της πρόσθεσης.

Παράδειγμα: $(\mathbb{R}^{n\times n}, +)$ $GL_n(\mathbb{R})$ (σύνολο αντιστρέψιμων πινάκων). $\det A \neq 0$.

$\left.\begin{array}{l} I_n \in GL_n(\mathbb{R}) \\ -I_n \in GL_n(\mathbb{R}) \end{array}\right\}$ $I_n + (-I_n) = O_{n\times n} \notin GL_n(\mathbb{R})$. Άρα το $GL_n(\mathbb{R})$ δεν είναι κλειστό ως προς την πρόσθεση.

$(G, *)$ ομάδα



$S \subseteq G$ S κλειστό ως προς την πράξη της G

$S \times S \to S$

$(a, b) \to a*b$

η $*$ είναι διμελής πράξη στο

Η πράξη αυτή λέγεται η επαγόμενη πράξη στο S από τ πράξη στο G.

Ορισμός: Ένα υποσύνολο H μιας ομάδας G ονομάζεται υποομάδα τ G αν ισχύουν:

1) H κλειστό ως προς την πράξη της G.
2) Το e της G ανήκει στην H
3) Για κάθε $a \in H$ το $a^{-1} \in H$.

Θεώρημα: Έστω G ομάδα και H υποομάδα της G. Τότε το H με την επαγόμενη πράξη από την πράξη της G είναι ομάδα.

$(H, *)$ ↙ επαγόμενη πράξη.

$H \times H \to H$

$(a, b) \to a*b$.

(i) Έστω $a, b, \gamma \in H \subset G \Rightarrow a, b, \gamma \in G$, η G ομάδα $\Rightarrow a*(b*\gamma) = (a*b)*$

(ii) $e \in H$ (ορισμός). Έστω $a \in H \subset G$ $a*e = e*a = a$

ουδέτερο της G.

(iii) Για κάθε $a \in H$ το $a^{-1} \in H$ και $a * a^{-1} = a^{-1} * a = e$.

Άρα κάθε υποομάδα της G είναι ομάδα με την επαγόμενη πράξη.

Η υποομάδα της G το συμβολίζουμε με $H \leq G$ $\left(H < G \Leftrightarrow H \leq G \text{ και } H \neq G \right)$

Παραδείγματα: $G \leq G$

$\{e\} \leq G$

$\{e\} \leq G$. Έστω $a, \beta \in \{e\} \Rightarrow a = e$ και $b = e$: $a * b = e * e = e$

$a * b \in \{e\}$.

(i) Άρα $\{e\}$ κλειστό ως προς την πράξη της G.

(ii) Το $e \in \{e\}$.

(iii) Για κάθε $a \in \{e\} \Rightarrow a = e \Rightarrow a^{-1} = e \in \{e\}$.

$\mathbb{Z}$: $\mathbb{Z} \leq \mathbb{Z}$ $\quad \{0\} \leq \mathbb{Z}$

$2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\} = \{-2k, -6, -4, \dots, 0, 2, 4, 6, \dots, 2k\}$

άρτιοι

(i) $2\mathbb{Z}$ κλειστό ως προς την πρόσθεση

(ii) $0 \in 2\mathbb{Z}$

(iii) Έστω $2k \in 2\mathbb{Z} \Rightarrow -2k = 2(-k) \in 2\mathbb{Z}$

$2\mathbb{Z} \leq \mathbb{Z}$

$3\mathbb{Z} = \{3k \mid k \in \mathbb{Z}\} = \{-3k, -9, -6, -3, 0, 3, 6, 9, 3k\}$

(i) $3\mathbb{Z}$ κλειστό ως προς την πράξη (αφού αν $3k \in 3\mathbb{Z}$ και $3\lambda \in 3\mathbb{Z}$ $\} \Rightarrow 3k + 3\lambda = 3(k+\lambda) \in 3\mathbb{Z}$

(ii) $0 = 3 \cdot 0 \in 3\mathbb{Z}$

(iii) $3k \in 3\mathbb{Z} \Rightarrow -3k = 3(-k) \in 3\mathbb{Z}$ $\quad$ Άρα $3\mathbb{Z} \leq \mathbb{Z}$

Παραδείγματα: Έστω $n \in \mathbb{Z}$ τότε $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$. $(-2\mathbb{Z} = 2\mathbb{Z})$

(i) $na \in n\mathbb{Z}$, $nb \in n\mathbb{Z} \Rightarrow na + nb = n(a+b) \in n\mathbb{Z} \Rightarrow n\mathbb{Z}$ είναι κλειστό ως προς $+$

(ii) $0 = n \cdot 0 \in n\mathbb{Z}$

(iii) Αν $nk \in n\mathbb{Z} \Rightarrow -nk = n(-k) \in n\mathbb{Z}$ $\quad n\mathbb{Z} \leq \mathbb{Z}$.

Παράδειγμα: $U(\mathbb{Z}_8) = \{[1]_8, [3]_8, [5]_8, [7]_8\}$

> Τάξη ~~...~~ καθορίζεται από τα στοιχεία της ομάδας

Έστω $H \leq U(\mathbb{Z}_8)$

(i) $|H| = 1 \Rightarrow H_1 = \{[1]_8\}$.

(ii) $|H| = 2 \Rightarrow H_2 = \{[1]_8, [3]_8\}$ (i) $[1]_8[1]_8 = [1]_8$, $[1]_8[3]_8 = [3]_8[1]_8 = [3]_8$, $[3]_8[3]_8 = [1]_8$ κλειστό

$H_3 = \{[1]_8, [5]_8\} \leq U(\mathbb{Z}_8)$ (ii) $[1] \in H_2$

$H_4 = \{[1]_8, [7]_8\} \leq U(\mathbb{Z}_8)$ (iii) $[1]_8^{-1} = [1]_8$, $[3]^{-1} = [3]_8$.

$H_2 \leq U(\mathbb{Z}_8)$.

(iii) $|H| = 3$

$H_5 = \{[1]_8, [5]_8, [7]_8\} \not\leq U(\mathbb{Z}_8)$ $[5]_8[7]_8 = [3]_8$. Άρα H_5 δεν είναι κ[λειστό]

$H_6 = \{[1]_8, [3]_8, [7]_8\} \not\leq U(\mathbb{Z}_8)$ $[3]_8[7]_8 = [5]_8$. Άρα H_6 δεν είναι κ[λειστό]

$H_7 = \{[1]_8, [3]_8, [5]_8\} \not\leq U(\mathbb{Z}_8)$ $[3]_8[5]_8 = [7]_8$. Άρα H_7 δεν είναι κλειστό.

(iv) $|H| = 4$ $H_8 = U(\mathbb{Z}_8) \leq U(\mathbb{Z}_8)$.

ΔΙΑΓΡΑΜΜΑ HASSE:

$$\begin{tikzcd}
 & U(\mathbb{Z}_8) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\{[1]_8, [3]_8\} \arrow[dr, dash] & \{[1]_8, [5]_8\} \arrow[d, dash] & \{[1]_8, [7]_8\} \arrow[dl, dash] \\
 & \{[1]_8\} &
\end{tikzcd}$$

Ομάδα του Klein

ΘΕΩΡΗΜΑ: Ένα υποσύνολο H μιας ομάδας G είναι υποομάδα της G αν-ν:

1) $H \neq \emptyset$
2) Για κάθε $a, b \in H \Rightarrow a * b^{-1} \in H$

ΠΑΡΑΤΗΡΗΣΗ: Αν η πράξη της G δεν είναι πρόσθεση θα χρησιμοποιούμε στις αποδείξεις ως πράξη τον πολλ/σμό, το 1 ως ουδέτερο και το a^{-1} ως αντίστροφο

($\longrightarrow$) i) $H \leq G \xRightarrow[\text{ορισμού}]{(ii)} 1 \in H \Rightarrow H \neq \emptyset$.

ii) Έστω $a, b \in H \xRightarrow[\text{ορισμού}]{(iii)} a, b^{-1} \in H \xRightarrow[\text{ορισμού}]{(i)} a \cdot b^{-1} \in H$

($\longleftarrow$) $H \neq \emptyset \Rightarrow \exists$ τουλάχιστον ένα στοιχείο $a \in H$.

$a, a \in H \xRightarrow[\text{ορισμού}]{(ii)} a \cdot a^{-1} \in H \Rightarrow 1 \in H$.

(iii) Έστω $a \in H$ $\quad 1, a \in H \Rightarrow 1 \cdot a^{-1} \in H \Rightarrow a^{-1} \in H$.
(i) Έστω $a, b \in H \Rightarrow a, b^{-1} \in H \Rightarrow a(b^{-1})^{-1} \in H \Rightarrow ab \in H$

Άρα H κλειστό ως προς την πράξη του G.

$a^0 = 1$	$0a = 0$
$a^n = \underbrace{a \cdot a \cdots a}_{n\text{-φορές}}$ $\quad n \in \mathbb{N}$	$n \cdot a =$
$a^n = \underbrace{a \cdot a \cdots a}_{-n\text{ φορές}}$ $\quad n \in \mathbb{Z}$, $n \notin \mathbb{N}$	

Πολλαπλασιασμός	Πρόσθεση
$(a^n)^{-1} = a^{-n}$	$-(na) = -na$
$(a^n)^m = a^{n \cdot m}$	$m(na) = (m \cdot n) \cdot a$
$(a^n) \cdot (a^m) = a^{n+m}$	$n \cdot a + ma = (n+m) \cdot a$

<u>Πρόταση</u>: Έστω G ομάδα και $a \in G$. Τότε το σύνολο $H_a = \{a^n \mid n \in \mathbb{Z}\}$ είναι υποομάδα της G.

1) $1 = a^0 \in H_a \Rightarrow H_a \neq \emptyset$
2) Έστω $\gamma, b \in H_a \Rightarrow b = a^k, \gamma = a^\lambda \Rightarrow b \cdot \gamma^{-1} = a^k (a^\lambda)^{-1} = a^k a^{-\lambda} = a^{k-\lambda} \in H_a$

Άρα $H_a \leq G$.

<u>Ορισμός</u>: Η υποομάδα $\{a^n \mid n \in \mathbb{Z}\}$ ονομάζεται κυκλική υποομάδα που παράγεται από το a και συμβολίζεται με $\langle a \rangle$.

<u>Ορισμός</u>: Μια ομάδα G ονομάζεται κυκλική αν υπάρχει $a \in G$ τ.ω. $G = \langle a \rangle$.

<u>Παραδείγματα</u>: $U(\mathbb{Z}_{17}) = \{[1]_{17}, [2]_{17}, [3]_{17}, \ldots, [16]_{17}\}$.

$\langle [2]_{17} \rangle = \{[2]_{17}^n \mid n \in \mathbb{Z}\} = \{[1]_{17}, [2]_{17}, [4]_{17}, [8]_{17}, [16]_{17}, [15]_{17}, [13]_{17}, [9]_{17}\}$.

Πρωταρχική ρίζα είναι γεννήτορες κυκλικών ομάδων

$$<[3]_{17}> = \{[3]_{17}^{n} \mid n \in \mathbb{Z}\} = <[1]_{17}, [3]_{17}, [9]_{17}, [10]_{17}, [13]_{17}, [5]_{17}, [15]_{17}, [11]_{17}, [16]_{17}, [14]_{17}, [8]_{17}, [7]_{17}, [4]_{17}, [12]_{17}, [2]_{17}, [6]_{17}>.$$

$<[3]_{17}> = U(\mathbb{Z}_{17})$ Άρα κυκλική ομάδα το $U(\mathbb{Z}_{17})$.

$$\mathbb{Z}_8 = \{[0]_8, [1]_8, \dots, [7]_8\}$$

$$<[2]_8> = \{[0]_8, [2]_8, [4]_8, [6]_8\}$$

$$<[1]_8> = \{[1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8, [8]_8 = [0]_8\}$$

Άρα $\mathbb{Z}_8$ κυκλική $\mathbb{Z}_8 = <[1]_8> = <[3]_8>$