$H \leq G \Leftrightarrow H \neq \emptyset$ και $\forall a \in H \Rightarrow a^{-1} \in H$.
πράξη κλειστή

$(\mathbb{Z},+) \leq (\mathbb{Q},+) \leq (\mathbb{R},+) \leq (\mathbb{C},+)$

$(\mathbb{Q}^*,\cdot) \leq (\mathbb{R}^*,\cdot) \leq (\mathbb{C}^*,\cdot)$

Παράδειγμα

Ας βρούμε τις υποομάδες του $(\mathbb{Z},+)$

Έστω $H \leq \mathbb{Z}$. Έστω $k = \min H \cap \mathbb{Z}^+$. Θ.δ.ο $H = k\mathbb{Z}$

$k \in H \Rightarrow$ κάθε πολ/σιο του $k \in H$ (γιατί η πράξη είναι κλειστή)

Άρα $k\mathbb{Z} \leq H$. Θέλουμε $H \leq k\mathbb{Z}$

Έστω $m \in H$ και $m \in k\mathbb{Z}$ $\quad m = k\pi + u$ με $0 < u < k$

$\left.\begin{matrix} m \in H \\ k\pi \in H \end{matrix}\right\} \Rightarrow m - k\pi \in H \Rightarrow u \in H \quad u < k$

Κάθε υποομάδα της $\mathbb{Z}$ είναι μορφής $k\mathbb{Z}$. Άρα κυκλική με γεννήτορες k ή $-k$.

Παράδειγμα

Ο τυχαία και $a \in (0,\cdot)$

Έστω $H = \{a^k \mid k \in \mathbb{Z}\}$

$H \leq O$ Είναι η υποομάδα που γεννάται από το a

$\emptyset \neq H$. Πράξη κλειστή $a^k a^l = a^{k+l} \in H$

$a^k \in H$ και $a^{-k} \in H \Rightarrow H \leq O$

<u>Μη τετριμμένη μη-κυκλική και μικρότερη.</u>

$|O| = 4$ (Προσοχή $|\mathbb{Z}_4| = 4$ αλλά είναι κυκλική)

$O = \{1, a, b, ab\}$ ← Ομάδα του <u>Klein</u>

$$\boxed{\begin{array}{l} a^2 = 1 = b^2 \\ ba = ab \end{array}}$$
← Σχέσεις

Αβελιανή, 2 γεννήτορες (a, b)

Αν έχω γεννήτορες χωρίς σχέσεις τότε ελεύθερη. π.χ. $\mathbb{Z}$

Ενώ $\mathbb{Z}_4 = \langle [1], \oplus \rangle$ όχι ελεύθερη αφού έχω την σχέση

$$\underbrace{[1] \oplus \dots \oplus [1]}_{4\text{-φορές}} = [0]$$

Πόσες υποομάδες έχει η ομάδα του Klein?

→ $\{1\}$ τετριμμένη

→ $\{a, a^2 = 1\}$

→ $\{b, b^2 = 1\}$

→ $\{ab, (ab)^2 = abab = abba = ab^2a = a1a = a^2 = 1\}$

→ O

Ερώτημα: Ποιες είναι οι υποομάδες της $(\mathbb{Z}_n, \oplus)$

ΘΕΩΡΗΜΑ

Έστω $G = \langle a \rangle$ κυκλική, τότε κάθε υποομάδα της θα είναι επίσης κυκλική

Απόδειξη

$G = \langle a \rangle = \{ a^k / k \in \mathbb{Z} \}$

$H \leq G$. Έστω l ο μικρότερος θετικός εκθέτης με $a^l \in H$

Θ.δ.ο $H = \langle a^l \rangle$

$a^l \in H \Rightarrow a^{lk} \in H \Rightarrow \langle a^l \rangle \leq H$

Έστω $a^m \in H - \langle a^l \rangle \Rightarrow m \neq kl \Rightarrow$

$m = nl + u \quad 0 < u < l \Rightarrow \underset{\in H}{a^m} \cdot \underset{\in H}{a^{-nl}} \in H \Rightarrow a^u \in H$

Παράδειγμα

$Q_8 = \{ I, -I, J, -J, K, -K, L, -L \}$

$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \quad K = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad L = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$

$J^2 = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = \begin{pmatrix} i^2 & 0 \\ 0 & i^2 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$

$J^3 = J J^2 = J(-I) = -J$

$J^4 = J J^3 = J(-J) = -J^2 = -(-I) = I$

$o(J) = 4 = o(K) = o(L)$

$$JK = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = L$$

$KJ = -L$ όχι αβελιανή

$$JL = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \begin{pmatrix} 0 & i^2 \\ -i^2 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = -K$$

$LJ = K$

$|Q_8| = 4$ όχι αβελιανή, όχι κυκλική

έχω 2 γεννήτορες και σχέσεις

<u>ΠΡΟΤΑΣΗ</u>

Έστω H πεπερασμένο υποσύνολο μιας ομάδας G το οποίο να είναι κλειστό ως προς την πράξη. Τότε $H \leq G$

<u>Απόδειξη</u>

$H = \{h_1, h_2, \ldots, h_k\}$ πράξη κλειστή

Αρκεί $\forall\, h_i \in H \Rightarrow h_i^{-1} \in H$

$1_G \in H$. Έστω $h_i \in H \Rightarrow h_i H = \{h_i h_1, h_i h_2, \ldots, h_i h_k\} \Rightarrow$

πράξη κλειστή

$h_iH \subseteq H$ Αν είχαμε $h_iH \subsetneq H \Leftrightarrow$

$\Leftrightarrow \exists\ t$ και s $(t \neq s)$ ώστε $h_ih_t = h_ih_s \xRightarrow{\text{Ο ομάδα}}$

$\Rightarrow h_i^{-1}(h_ih_t) = h_i^{-1}(h_ih_s) \Rightarrow h_t = h_s^{*} \Rightarrow h_ih_t = h_ih_s$ Άρα $h_iH = H$

$\{h_ih_1, h_ih_2, \dots h_ih_r\} = \{h_1, h_2, \dots, h_r\}$

$\boxed{\begin{array}{l} * \Rightarrow t = s \\ \text{Άτοπο αφού } t \neq s \\ \text{από υπόθεση} \end{array}}$

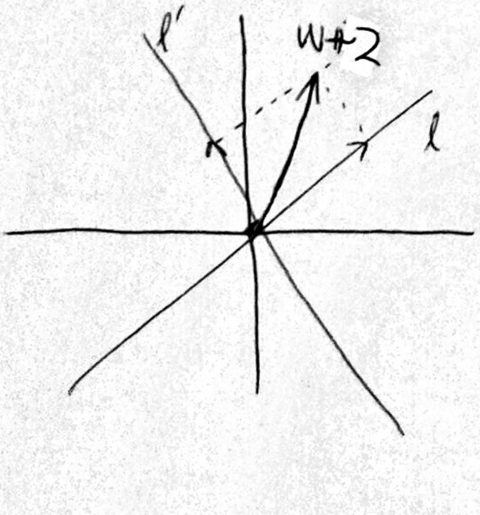
Συνεπώς $h_ih_j \longleftarrow h_i$

$h_ih_j = h_i \Rightarrow h_j = 1_0$ Άρα $1_0 \in h_iH \Rightarrow 1_0 = h_ih_t$ για κάποιο t

Άρα $1_0 = h_ih_t \Rightarrow h_t = h_i^{-1}$ & $h_t \in H \Rightarrow h_i^{-1} \in H$

<u>Παράδειγμα</u>

$\mathbb{R}^2$



Υπόχωροι του $\mathbb{R}^2$: - 0

- ευθείες που διέρχονται από την αρχή των αξόνων
- όλος ο χώρος

$W, Z \leq V$ δ.χ. $W \cap Z \leq V$

$W \cup Z \to W + Z$ (δεν ισχύει πάντα)

Παράδειγμα

$(\mathbb{Z},+)$ $\quad 2\mathbb{Z}, 3\mathbb{Z} \leq \mathbb{Z}$

$$2\mathbb{Z} \cap 3\mathbb{Z} = \{ \underset{\substack{\Downarrow \\ k=2l}}{k \in 2\mathbb{Z}} \text{ και } \underset{\substack{\Downarrow \\ k=3n}}{k \in 3\mathbb{Z}} \}$$

$$k=2l = 3n$$

$$k = 2l = 3n \Rightarrow \left.\begin{matrix} 2 \mid 3n \\ 2 \nmid 3 \end{matrix}\right\} \Rightarrow 2 / n$$

$k = 3 \cdot 2n' = 6n' \quad n' \in \mathbb{Z}$

$6\mathbb{Z} \leq \mathbb{Z}$

$2\mathbb{Z} \cup 3\mathbb{Z} = \{ 2k, 3l \,/\, k, l \in \mathbb{Z} \}$ είναι υποομάδα του $\mathbb{Z}$?

$2 + 3 = 5 \notin 2\mathbb{Z} \cup 3\mathbb{Z}$ Άρα δεν είναι υποομάδα.

ΠΡΟΤΑΣΗ

Έστω H_1 και H_2 υποομάδες μιας ομάδας G. Τότε

1) $H_1 \cap H_2 \leq G$

2) $H_1 \cup H_2 \leq G \iff H_1 \leq H_2$ ή $H_2 \leq H_1$

(Άσκηση σαν τους διαν. χώρους) → Απόδειξη

ΘΕΩΡΗΜΑ

Έστω $G=\langle a \rangle$ κυκλική τάξης n. Τότε

α) για οποιονδήποτε ακέραιο m, n G έχει υποομάδα τάξης m ανν m/n

β) Αν $n=km$ τότε ο G έχει μοναδική υποομάδα τάξης m

γ) $\langle a^r \rangle = \langle a^s \rangle$ ανν $\overset{\text{Μ.Κ.Δ.}}{(n,r)} = (n,s)$

Απόδειξη

α) • G κυκλική τάξης n. $H \leq G$ τάξης m. Άρα H κυκλική $\Rightarrow$ $H = \langle a^r \rangle$ για κάποιον φυσικό r με $a^r \in G$

$$o(a^r) = \frac{o(a)}{(o(a), r)} = \frac{n}{(n,r)} = m \iff n = m(n,r) \Rightarrow m/n$$

• Έστω $|H| = m$ θέλαμε το m/n

$H \leq G \Rightarrow H$ κυκλική τάξης m $H = \langle a^r \rangle$ για κάποιο r

$$|H| = o(a^r) = \frac{n}{(n,m)} = m$$

Αν $m/n \Rightarrow n = mm'$

$H = \langle a^{m'} \rangle$

$$|H| = o(a^{m'}) = \frac{n}{(n,m')} = \frac{mm'}{(mm', m')} = \frac{mm'}{m'} = m$$

β) Αν $n=km$ και $H_1, H_2 \le G$

ώστε $|H_1|=|H_2|=m$ (1) θέλουμε $H_1=H_2$

$H_1, H_2 \le G \Rightarrow \exists\, a^r$ και $a^s \in G$ με $H_1=\langle a^r\rangle$ και $H_2=\langle a^s\rangle$

(1) $\Rightarrow o(a^r)=m=o(a^m) \iff \dfrac{n}{(n,r)} = m = \dfrac{n}{(n,s)} \iff (n,r)=(n,s)$

Δεν συνεπάγεται ότι $r=s$ αφού πχ $(5,2)=(5,3)$ ενώ $2\neq 3$

Έστω $(n,r)=(n,s)=k \Rightarrow k/n,r,s \Rightarrow (a^k)^{r'}=a^r$ (2)

$H=\langle a^k\rangle \Rightarrow |H| = \dfrac{n}{(n,k)} = \dfrac{n}{k} = m$ (αφού $n=mk$)

Άρα $|H|=|H_1|=|H_2|$

Από (2) έχω $a^r \in H$, ομοίως $a^s \in H \Rightarrow$

$$\left.\begin{array}{r} H_1=\langle a^r\rangle \le H \\ H_2=\langle a^s\rangle \le H \\ |H_1|=|H_2|=|H| \end{array}\right\} \Rightarrow$$

$\Rightarrow H_1=H_2=H$.