Ο διάδα $H \leq O$

$Ha = \{ha \mid h \in H\}$ δεξί σύμπλοκο

$Ha = Hb \Leftrightarrow ba^{-1} \in H \Leftrightarrow ab^{-1} \in H$

$O = \bigsqcup_{i=1}^{k} Ha_i$

Αν $|O| < \infty \Rightarrow |O| = |H|\,[O:H]$ Από Lagrange

όπου $[O:H]$ είναι ο δείκτης (το πλήθος των συμπλόκων)

$\forall a \in O \Rightarrow o(a) \mid |O|$

ΘΕΩΡΗΜΑ

Αν $|O| = p$ πρώτος τότε O κυκλική και κάθε μη ταυτοτικό στοιχείο είναι γεννήτορας

παράδειγμα

$(\mathbb{Z}_p, \oplus)$ $[a] \neq [0] \Rightarrow [a]$ γεννήτορας της $\mathbb{Z}_p = \langle [a] \rangle$

Απόδειξη

Αν δεν ήταν: $\exists\, a, b \in O$ με $b \neq a^k$ $\forall k \in \mathbb{Z}$ $\Rightarrow$

$\Rightarrow o(a), o(b) \mid p$

$o(a), o(b) = p$, $b \neq a^k$ $\Rightarrow |O| > p$ Άδικο

Παράδειγμα

$\mathbb{Z}_{12}$ $\quad H = \langle [3] \rangle$

$$|H| = o([3]) = \frac{o(1)}{(o(1),3)} = \frac{12}{(12,3)} = \frac{12}{3} = 4 \quad \Rightarrow |H| = 4 \Rightarrow$$

$$\Rightarrow [\mathbb{Z}_{12} : H] = \frac{|\mathbb{Z}_{12}|}{|H|} = \frac{12}{4} = 3$$

$[0] + H = H$

$[1] + H = \{[1], [4], [7], [10]\}$

$[2] + H = \{[2], [5], [8], [11]\}$

$$\mathbb{Z}_{12} = H \sqcup ([1] + H) \sqcup ([2] + H)$$

ΠΡΟΤΑΣΗ

Κάθε ομάδα με τάξη μικρότερη από 6 είναι αβελιανή

$|\Sigma_3| = 6 \rightarrow$ όχι αβελιανή

ΘΕΩΡΗΜΑ Fermat - Euler

Έστω m φυσικός και a ακέραιος πρώτος με τον m Τότε $a^{\varphi(m)} \equiv 1 \bmod m$

Ερώτημα: Ισχύει $aH = Ha$;;; Δεν ισχύει πάντα

Αν H αβελιανή ισχύει προφανώς

Υπάρχουν άλλες περιπτώσεις?

Έστω $aH = Ha$ 1) Ισχύει για κάθε a ?

2) Ισχύει για μεμονωμένα a?

ΟΡΙΣΜΟΣ

Έστω $H \leq O$ και ισχύει ότι $aH = Ha$ $\forall a \in O$. Τότε η H καλείται κανονική υποομάδα της O. Συμβολισμός: $H \lhd O$

$aH = Ha \iff aHa^{-1} = Haa^{-1} \iff aHa^{-1} = H$

Έστω $h \in H \Rightarrow aha^{-1} \in H \not\Longrightarrow aha^{-1} = h$

$aha^{-1} \in H \Longrightarrow \exists\, h'$ με $aha^{-1} = h'$

Παράδειγμα

$\Sigma_3 = \{1, f, f^2, g, fg, f^2g\}$, $H = \langle g \rangle$

$[\Sigma_3 : H] = 3$ Συμπλοκα: H, fH, f^2H

$fH = \{f, fg\}$

$Hf = \{f, gf\}$

Όμως $fg \neq gf \Longrightarrow Hf \neq fH \Rightarrow H \not\lhd \Sigma_3$

- $H' = \langle f \rangle \Rightarrow |H'| = 3 \Rightarrow [\Sigma_3 : H] = 2$

Συμπλοκα: H', gH' $\Sigma_3 = H' \sqcup gH'$

Αν $gH' \neq H'g \Rightarrow H'g = H'$ Αδύνατο. Άρα $gH' = H'g \Rightarrow$

$\Rightarrow H' \lhd \Sigma_3$

- $H'' = \langle fg \rangle$

$fgfg = ff^2 = 1$

$[\mathbb{Z}_3 : H''] = 3$ Συλλογικά: H'', fH'', f^2H''

$fH'' = \{f, ffg\} = \{f, f^2g\}$

$f^2H'' = \{f^2, f^2fg\} = \{f^2, g\}$

$H''f = \{f, fgf\}$

$gfg = f^2 \Rightarrow fgfg = f^3 = 1 \Rightarrow fgfgg = g \Rightarrow fgf = g$ $\Big\} \Rightarrow H''f = \{f, g\}$

Άρα $fH'' \neq H''f \Rightarrow H'' \not\lhd \mathbb{Z}_3$

$H'' = \{1, fg\}$ $\quad gH'' = \{g, gfg\} = \{g, f^2g\}$ $\Big\} \Rightarrow gH'' \neq H''g$

$H''g = \{g, fg\}$

ΠΡΟΤΑΣΗ

Έστω $H \leq O$. Τα επόμενα είναι ισοδύναμα:

(i) $H \lhd O \iff gHg^{-1} = H \quad \forall g \in O$

(ii) $gHg^{-1} \subseteq H, \quad \forall g \in O$

(iii) $gH = Hg, \quad \forall g \in O$

Απόδειξη

(i) $\Rightarrow$ (ii) προφανές.

(ii) $\Rightarrow$ (i) : Θέλουμε $gHg^{-1} = H$ $\forall g \in O$ όταν έχουμε $gHg^{-1} \leq H$ $\forall g \in O$

Θέλουμε δοιπόν $H \leq gHg^{-1}$ $\forall g \in O$

Αρκεί $\forall h \in H \Rightarrow h \in gHg^{-1} \Leftrightarrow \exists\, h' \in H$ με $h = g h' g^{-1} \Leftrightarrow$

$\Leftrightarrow g^{-1} h g = h'$ ισχύει $\Leftrightarrow \underbrace{g^{-1} h g}_{(g^{-1})^{-1} h (g^{-1})} \in H$

ΠΡΟΤΑΣΗ

Αν O αβελιανή τότε κάθε υποομάδα της είναι κανονική

Απόδειξη

$H \leq O$ τυχαία. Πρέπει $gHg^{-1} = H$, O αβελιανή $\Rightarrow H$ αβελιανή

$ghg^{-1} = gg^{-1}h = h$ $\forall g \in O$ και $\forall h \in H$

ΠΡΟΤΑΣΗ

Έστω G, O ομάδες και η ομάδα $G \times O$. Τότε η $\{1\} \times O$ και $G \times \{1\}$ είναι κανονικές : $\{1\} \times O \triangleleft G \times O$

$G \times \{1\} \triangleleft G \times O$

Απόδειξη

Τυχαίο της $G \times O$ το (g, a)

$(g,a)\, \{1\} \times O\, (g,a)^{-1} \stackrel{?}{=} \{1\} \times O$

$(g, a) \in \mathbb{Z} \times O \; (g^{-1}, a^{-1}) = (g 1 g^{-1}, a O a^{-1}) = (1, O)$ ισχύει (αφού $a, a^{-1} \in O$)

ΘΕΩΡΗΜΑ

Αν ο δείκτης της H στον O είναι 2 $\left([O : H] = 2\right)$ τότε η H είναι κανονική $H \triangleleft O$

Στην $\mathbb{Z}_v$ η ευκλείδεια A_v (όλες οι άρτιες μεταθέσεις) έχει δείκτη 2. Γιατί $|A_v| = \frac{|\mathbb{Z}_v|}{2}$

Απόδειξη

$[O : H] = 2 \Rightarrow O = H \sqcup aH$ με $a \notin H$ αλλά και $O = H \sqcup Ha$

Θέλουμε $gHg^{-1} = H \Leftrightarrow gH = Hg$

Αν $g \in H \Rightarrow gH = H = Hg$

Αν $g \notin H \Rightarrow gH \sqcup H = O \Rightarrow gH \neq H$ $\left.\begin{matrix} \\ Hg \sqcup H = O \end{matrix}\right\} \Rightarrow gH = Hg$

Πόρισμα

$A_v \triangleleft \mathbb{Z}_v$

π.χ $O = \mathbb{Z}_3$ $H = \langle g \rangle$ $[O : H] = 3$ και $H \not\triangleleft O$

ΠΡΟΤΑΣΗ

Έστω $H \leq O$ και $g \in O$. Τότε $gHg^{-1} \leq O$ και $|gHg^{-1}| = |H|$

$(H \neq \{0\})$

Απόδειξη

$gHg^{-1} \leq O$

Πράξη: $(ghg^{-1})(gh'g^{-1}) = ghg^{-1}gh'g^{-1} = ghh'g^{-1} \in gHg^{-1}$ αφού $hh' \in H$

$ghg^{-1} \in gHg^{-1} \Rightarrow (ghg^{-1})^{-1} = gh^{-1}g^{-1} \in gHg^{-1}$

Ορίζουμε $\varphi : H \to gHg^{-1}$ με τύπο $\varphi(h) = ghg^{-1}$

$h \mapsto ghg^{-1}$

φ 1-1 : $ghg^{-1} = gh'g^{-1} \Rightarrow h = h'$

φ επί : $ghg^{-1} = \varphi(h) \Rightarrow |H| = |gHg^{-1}|$

Χρησιμότητα των κανονικών υποομάδων

$\mathbb{Z}$ ομάδα πηλίκο $k\mathbb{Z} \trianglelefteq \mathbb{Z}$

Σύμπλοκα της $k\mathbb{Z}$

$$\left.\begin{matrix} k\mathbb{Z}, & 1+k\mathbb{Z}, & 2+k\mathbb{Z}, & \dots, & (k-1)+k\mathbb{Z} \\ [0] & [1] & [2] & & [k-1] \end{matrix}\right\} = \mathbb{Z}_k \text{ ομάδα.}$$

$(a + k\mathbb{Z}) \oplus (b + k\mathbb{Z}) = (a+b) + k\mathbb{Z}$

$[a] \oplus [b] = [a+b]$

Ο ομάδα $H \leq 2$

Σύμπλοκα της H : $H, g_1H, g_2H, \dots, g_kH$ (δεν ξέρω αν τα σύμπλοκα είναι άπειρα ή πεπερασμένα)

(Αν είναι άπειρα ή όχι τα σύμπλοκα εξαρτάται από τον δείκτη)

$$[O:H] = \begin{cases} k \to \infty \\ \infty \end{cases}$$

$$\{H, g_1H, g_2H, \dots, g_kH\} = O/H$$

Ψάχνω πράξη : $g_iH \odot g_jH = g_ig_jH$ είναι καλά ορισμένη?

Θέλω να δείξω για να είναι καλά ορισμένη ότι δεν εξαρτάται από τον αναπαραστάτη. Αν είχα δηλαδή $g_iH \odot g_jH = g_i'g_j'H$ τότε $g_ig_jH = g_i'g_j'H$