Κανονικές Υποομάδες

Ορισμός: Έστω $(G,\cdot)$ μια ομάδα. Μια υποομάδα H της G λέγεται **κανονική** αν $xHx^{-1} = H$, $\forall x \in G$, όπου

$$xHx^{-1} = \{ xhx^{-1} \in G \mid h \in H \}.$$

Τότε θα γράφουμε $H \trianglelefteq G$.

Πρόταση: Έστω $(G,\cdot)$ μια ομάδα και έστω $H \leq G$. Τα ακόλουθα ισοδυναμούν:

(i) $H \trianglelefteq G$ (ii) $\forall x \in G, \forall h \in H$, $xhx^{-1} \in H$

(iii) $\forall x \in G$, $xHx^{-1} \subseteq H$.

Απόδειξη: (i) $\Rightarrow$ (ii) Υποθέτω ότι $H \trianglelefteq G$. Τότε, $xHx^{-1} = H$, $\forall x \in G$ (*) Συνεπώς, αν $x \in G$ και $h \in H$ τότε $xhx^{-1} \in xHx^{-1}$ και λόγω της (*), $xhx^{-1} \in H$.

(ii) $\Rightarrow$ (iii) Έστω $x \in G$ και θα δείξουμε ότι $xHx^{-1} \subseteq H$. Έστω λοιπόν $g \in xHx^{-1}$. Τότε $g = xhx^{-1}$, όπου $h \in H$. Λόγω υπόθεσης (ii), $g \in H$. Συνεπώς, $xHx^{-1} \subseteq H$.

(iii) $\Rightarrow$ (i) Υποθέτουμε ότι $xHx^{-1} \subseteq H$, $\forall x \in G$. Θα αποδείξουμε ότι $H \trianglelefteq G$, δηλαδή ότι $xHx^{-1} = H$, $\forall x \in G$. Έστω λοιπόν $x \in G$. Από υπόθεση (iii), $xHx^{-1} \subseteq H$, οπότε αρκεί να δείξουμε ότι $H \subseteq xHx^{-1}$. Έστω $h \in H$.

Τότε: $h = xx^{-1}hxx^{-1}$ (1)

Λόγω υπόθεσης (iii), $x^{-1}hx \in x^{-1}Hx \subseteq H$
$(x \to x^{-1})$

άρα η (1) δίνει: $h = x\underbrace{(x^{-1}hx)}_{\in H}x^{-1} \in xHx^{-1}$,

όπως θέλαμε. ∎

Παραδείγματα

(1) Έστω $(G, \cdot)$ μια ομάδα. Προφανώς, η τετριμμένη υποομάδα $\{e\}$ καθώς και ίδια η G είναι κανονικές υποομάδες της G.

$$\{e\} \trianglelefteq G, \quad G \trianglelefteq G$$

(2) Αν $H \leq G$ με την ιδιότητα $H \subseteq Z(G)$ τότε η H είναι κανονική.

Πράγματι, λόγω της προηγούμενης πρότασης αρκεί να δείξουμε ότι $xhx^{-1} \in H$, $\forall x \in G, \forall h \in H$.

Για $x \in G$ και $h \in H$ έχουμε

$$x \in G,\ h \in Z(G) \Longrightarrow xhx^{-1} \in Z(G) \quad \left(\begin{matrix}\text{γνωστή} \\ \text{θεωρία}\end{matrix}\right)$$

άρα $(xhx^{-1})x = x(xhx^{-1}) \Rightarrow xh = xxhx^{-1}$

$\xRightarrow[\text{διαγραφής}]{\text{νόμος}} h = xhx^{-1}$, άρα $xhx^{-1} = h \in H$,

όπως θέλαμε.

(3) Από το (2) έπεται, $Z(G) \trianglelefteq G$.

(4) Αν η ομάδα $(G, \cdot)$ είναι αβελιανή τότε κάθε υποομάδα της είναι κανονική.

(5) Έστω G_1, G_2 δύο ομάδες και $f: G_1 \to G_2$ μορφισμός. Τότε $Ker(f) \trianglelefteq G_1$.

Απόδειξη: Έστω $x \in G_1$, $a \in Ker(f)$ και θα αποδείξουμε ότι $x a x^{-1} \in Ker(f)$. Ισχύει:

$$f(x a x^{-1}) = f(x) f(a) f(x^{-1}) \underset{a \in Ker(f)}{=\!=} f(x) e_2 (f(x))^{-1}$$

$$= f(x)(f(x))^{-1} = e_2, \text{ οπότε } x a x^{-1} \in Ker(f) \quad \blacksquare$$

(6) $S_3 = \left\{ \begin{matrix} Id, (1\ 2), (1\ 3), \\ (2\ 3), (1\ 2\ 3), (1\ 3\ 2) \end{matrix} \right\}$

Η $\sigma = (1\ 2\ 3)$ είναι 3-κύκλος, άρα $o(\sigma) = 3$ και έτσι:

$$\langle \sigma \rangle = \{ Id, \sigma, \sigma^2 \} = \{ Id, \sigma, (1\ 3\ 2) \}$$

Θα δείξουμε ότι $H = \langle \sigma \rangle \trianglelefteq S_3$.

Πράγματι, με εύκολους υπολογισμούς δείχνουμε

- $php^{-1} \in H$, $\forall p \in S_3$, $\forall h \in H$.

Άσκηση 1: Έστω $(G, \cdot)$ μια ομάδα και έστω $(H_i)_{i\in I}$ οικογένεια κανονικών υποομάδων της G. Τότε $H = \bigcap_{i\in I} H_i \trianglelefteq G$.

Λύση Έστω $x \in G$ και $h \in H$. Τότε $h \in H_i$, $\forall i \in I$. Επειδή $H_i \trianglelefteq G$, $\forall i \in I$ προκύπτει $xhx^{-1} \in H_i$, $\forall i \in I$, οπότε $xhx^{-1} \in H$. Συνεπώς, $H \trianglelefteq G$. ∎

Άσκηση 2 (H/W): Έστω $H, K \trianglelefteq G$. Θέτω:

- $HK = \{hk \in G \mid h \in H, k \in K\} \subseteq G$
- $KH = \{kh \in G \mid k \in K, h \in H\} \subseteq G$

Να δείξετε ότι $HK = KH$ και $HK \trianglelefteq G$

Σχόλιο επί της Άσκησης 2: Στο Α Φυλλάδιο Ασκήσεων στην Άσκηση Α15 έχουμε το αποτέλεσμα που αναφέρεται στην Άσκηση 2 για αβελιανές ομάδες, όπου στις αβελιανές ομάδες κάθε υποομάδα είναι κανονική.

Ορισμός: Μια ομάδα $(G,\cdot)$ καλείται απλή αν οι μόνες κανονικές υποομάδες της είναι οι $\{e\}$ και G.

Παραδείγματα

(1) (SOS) Έστω $(G,\cdot)$ μια ομάδα τάξης $|G| = p$, όπου p: πρώτος αριθμός. Τότε η G είναι απλή.

(βλέπε απόδειξη αργότερα
Β φυλλάδιο Ασκήσεων)

(2) Η ομάδα $(\mathbb{Z},+)$ δεν είναι απλή.

Πράγματι, $\forall n \in \mathbb{N}$, $\{0\} \neq n\mathbb{Z} \trianglelefteq \mathbb{Z}$

(3) (SOS) (χωρίς απόδειξη)

Για $n \geq 5$, η $(A_n, \circ)$ είναι απλή.

<u>Άσκηση</u>: Έστω $f: G_1 \to G_2$ μορφισμός ομάδων με G_1: απλή. Τότε $Ker(f) = G_1$ (δηλαδή f: τετριμμένος μορφισμός) ή f: 1-1.

<u>Λύση</u>: Επειδή $f: G_1 \to G_2$ μορφισμός έχουμε δει ότι $Ker(f) \trianglelefteq G_1$. Εφ' όσον G_1: απλή ομάδα έπεται:

$$\left\{\begin{array}{l} Ker(f) = \{e_1\} \\ \quad\quad ή \\ Ker(f) = G_1 \end{array}\right. \Longrightarrow \left\{\begin{array}{l} f: 1-1 \\ \quad ή \\ f: \text{τετριμμένος} \end{array}\right.$$

$\blacksquare$

(4) $\forall n \in \mathbb{N}$, $n \geq 2$, $A_n \trianglelefteq S_n$ (έχουμε δείξει ότι $\rho \circ \sigma \circ \rho^{-1} \in A_n$, $\forall \rho \in S_n$, $\forall \sigma \in A_n$), οπότε

$(S_n, \circ)$: όχι απλή ομάδα.

<u>Υποομάδες - Σχέσεις Ισοδυναμίας - Πλευρικές Κλάσεις</u>

Έστω $(G,\cdot)$ μια ομάδα και $H \leq G$.

Θεωρούμε τις ακόλουθες σχέσεις επί του G:

- $\forall x,y \in G: \quad x \,{}_{H}{\sim}\, y \iff xy^{-1} \in H$

- $\forall x,y \in G: \quad x \sim_{H} y \iff x^{-1}y \in H$.

<u>Ισχυρισμός</u>: Η ${}_{H}{\sim}$ είναι σχέση ισοδυναμίας επί του G.

<u>Απόδειξη</u>: (i) $\forall x \in G$, $xx^{-1} = e \in H$, άρα $x \,{}_{H}{\sim}\, x$

(ii) Αν $x \,{}_{H}{\sim}\, y$ τότε $xy^{-1} \in H$ και αφού $H \leq G$ έχουμε $(xy^{-1})^{-1} \in H \Rightarrow yx^{-1} \in H$, δηλαδή $y \,{}_{H}{\sim}\, x$.

(iii) Αν $x \underset{H}{\sim} y$ και $y \underset{H}{\sim} z$ τότε

$$\left.\begin{array}{l} xy^{-1} \in H \\ yz^{-1} \in H \end{array}\right\} \xrightarrow{H \leq G} xy^{-1}yz^{-1} \in H \Rightarrow xz^{-1} \in H$$

οπότε $x \underset{H}{\sim} z$. ■

Ομοίως αποδεικνύεται ότι και η $\sim_H$ είναι σχέση ισοδυναμίας επί του G.

Σε κάθε περίπτωση ορίζονται οι αντίστοιχες κλάσεις ισοδυναμίας

$${}_H[x] := \{ y \in G \mid x \underset{H}{\sim} y \} \subseteq G, \quad \forall x \in G.$$

$$[x]_H = \{ y \in G \mid x \sim_H y \} \subseteq G$$

Λήμμα $\forall x \in G$, ${}_H[x] = Hx := \{hx \in G \mid h \in H\}$

$[x]_H = xH := \{xh \in G \mid h \in H\}$

Απόδειξη: Έστω $x \in G$ και θα δείξουμε ότι ${}_H[x] = Hx$.

Έστω $y \in {}_H[x]$. Τότε $x \,{}_H\!\sim y$ και άρα $xy^{-1} \in H$, οπότε $xy^{-1} = h$ για κάποιο $h \in H$, άρα: $y^{-1} = x^{-1}h \Rightarrow y = h^{-1}x \in Hx$.

Συνεπώς, ${}_H[x] \subseteq Hx$. (1) Αντίστροφα, έστω $y \in Hx$. Τότε $y = hx$ για κάποιο $h \in H$. Επειδή $xy^{-1} = xx^{-1}h^{-1} = h^{-1} \in H$ έπεται ότι $x \,{}_H\!\sim y$, δηλαδή: $y \in {}_H[x]$. Επομένως, $Hx \subseteq {}_H[x]$. (2)

Λόγω των (1), (2), ${}_H[x] = Hx$.

Ομοίως, $[x]_H = xH$. $\square$

<u>Ορισμός</u>: Η κλάση ισοδυναμίας ${}_H[x] = Hx$ ($[x]_H = xH$) του στοιχείου $x \in G$ ως προς τη σχέση ισοδυναμίας ${}_H\sim$ (αντ. $\sim_H$) λέγεται δεξιό σύμπλοκο (αντ. αριστερό σύμπλοκο) του x ως προς την υποομάδα H.

<u>Παρατήρηση</u>: $He = eH = H$ αλλά δεν ισχύει γενικά $Hx = xH$ για $x \in G$.

<u>Σχόλιο</u>: Ορίζονται οι αντίστοιχοι χώροι-πηλίκα

· $G/{}_H\sim = \{ {}_H[x] \subseteq G \mid x \in G \} = \{ Hx \subseteq G \mid x \in G \}$

· $G/\sim_H = \{ [x]_H \subseteq G \mid x \in G \} = \{ xH \subseteq G \mid x \in G \}$

Άρα τα σύμπλοκα ${}_H[x]$, $x \in G$ (αντ. $[x]_H$, $x \in G$) αποτελούν διαμέριση του συνόλου G και συνεπώς ισχύουν τα ακόλουθα:

1. $\forall x \in G, \quad Hx \neq \emptyset \; (xH \neq \emptyset)$

2. $\forall x, y \in G$, είτε $Hx = Hy$ ή $Hx \cap Hy = \emptyset$
$(xH = yH$ ή $xH \cap yH = \emptyset)$

3. $G = \bigcup_{x \in G} Hx \quad \left(G = \bigcup_{x \in G} xH \right)$

διακεκριμμένη ένωση

Λήμμα

Ⓐ Τα σύμπλοκα Hx και xH έχουν το ίδιο πλήθος στοιχείων για κάθε $x \in G$.

Ⓑ Τα σύνολα πηλίκα $G/{}_{H}\!\sim$ και $G/\sim_H$ έχουν το ίδιο πλήθος στοιχείων.

Απόδειξη

Ⓐ Έστω $x \in G$. Θεωρούμε την απεικόνιση $f : xH \to Hx$ με $f(xh) = hx$ η οποία είναι καλά ορισμένη.

f: επί : Έστω $y \in Hx$. Τότε $y = hx$ για κάποιο $h \in H$. Έτσι, $xh \in xH$ και $f(xh) = hx = y$.

f: 1-1 : Έστω $f(xh_1) = f(xh_2)$. Τότε

$h_1 x = h_2 x \xrightarrow[\text{διαγραφής}]{\text{νόμος}} h_1 = h_2$, άρα $xh_1 = xh_2$

Εφ' όσον, f: 1-1 και επί: $|Hx| = |xH|$

(B) Θεωρούμε απεικόνιση

$$\psi : G/\underset{H}{\sim} \to G/\underset{H}{\sim} \text{ με } \psi(Hx) = x^{-1}H$$

Βήμα 1 : ψ: καλά ορισμένη : Έστω $Hx = Hy$ και θα δείξουμε ότι $\psi(Hx) = \psi(Hy)$.

Πράγματι, αφού: $Hx = Hy$ έχουμε: $_H[x] = {}_H[y]$

$\Rightarrow x \underset{H}{\sim} y \Rightarrow xy^{-1} \in H$, άρα $xy^{-1} = h$ για κάποιο $h \in H$. Τότε $(xy^{-1})^{-1} = h^{-1} \Rightarrow$

$\Rightarrow yx^{-1} = h^{-1} \in H \Rightarrow (y^{-1})^{-1}x^{-1} \in H$

$\Rightarrow y^{-1} \underset{H}{\sim} x^{-1} \Rightarrow [x^{-1}]_H = [y^{-1}]_H \Rightarrow$

$x^{-1}H = y^{-1}H \implies \psi(Hx) = \psi(Hy)$.

<u>Βήμα 2</u>: <u>ψ 1-1</u>: Έστω $\psi(Hx) = \psi(Hy)$ και θα δείξουμε $Hx = Hy$. Πράγματι:

$\psi(Hx) = \psi(Hy) \implies x^{-1}H = y^{-1}H \implies x^{-1} \sim_H y^{-1}$

$\iff (x^{-1})^{-1}y^{-1} \in H \implies xy^{-1} \in H \implies x \,_H\!\sim y$

$\implies Hx = Hy$.

<u>Βήμα 3</u>: <u>ψ: επί</u>: Έστω $xH \in G/\sim_H$.

Τότε $Hx^{-1} \in G/_H\!\sim$ και

$\psi(Hx^{-1}) = (x^{-1})^{-1}H = xH$.

Επομένως, $|G/_H\!\sim| = |G/\sim_H|$.

$\blacksquare$

Από εδώ και κάτω: Σταθεροποιούμε όπως και πριν μια υποομάδα $H \leq G$ της ομάδας $(G,\cdot)$ και εργαζόμαστε με τη σχέση ισοδυναμίας $\underset{H}{\sim}$: $\forall x,y \in G,\ x \underset{H}{\sim} y \iff x^{-1}y \in H$.

Σύνολο πηλίκο:

$$G/_{\underset{H}{\sim}} := G/_H = \{ [x]_H \subseteq G \mid x \in G \}$$
$$= \{ xH \subseteq G \mid x \in G \}$$

Σχόλιο: $xH = H \iff xH = eH \iff$

$x \underset{H}{\sim} e \iff x^{-1}e \in H \iff x^{-1} \in H \underset{H \leq G}{\iff} x \in H.$

Λήμμα: Ισχύει ότι για κάθε $x,y \in G$ τα xH και yH έχουν το ίδιο πλήθος στοιχείων.

Απόδειξη: Η απεικόνιση $f: xH \to yH$ με $f(xh) = yh$ είναι 1-1 και επί.

Πόρισμα: $\forall x \in G$, $o(H) = |H| = |xH|$

Απόδειξη: $\forall x \in G$, $|H| = |eH| \underset{y=e}{\overset{\text{Λήμμα}}{=}} |xH|$ ∎

Ορισμός: Το πλήθος των στοιχείων του συνόλου - πηλίκου G/H καλείται ο δείκτης της H στην G και συμβολίζεται με

$$[G:H].$$

Παραδείγματα

(1) Αν $H = \{e\} \leq G$ τότε:

$\forall x \in G$, $xH = \{xe \in G\} = \{x\}$, οπότε

$G/_{\{e\}} = \{xH \subseteq G \mid x \in G\} = \{\{x\} \subseteq G \mid x \in G\}$

$\Longrightarrow [G:\{e\}] = |G|$

(2) Αν $H = G$, τότε $xH = xG = \{xy \in G \mid y \in G\}$

$= G$, $\forall x \in G$.

Άρα. $G/_G = \{G\} \Rightarrow [G:G] = 1$.

(3) $(\mathbb{Z},+)$, $n \in \mathbb{N}$ και $H = n\mathbb{Z} \leq \mathbb{Z}$

Προσοχή εδώ: προσθετικός συμβολισμός

$\forall k,m \in \mathbb{Z}$: $k \underset{H}{\sim} m \iff -k+m \in H$

$(x \underset{H}{\sim} y)$ $\quad (x^{-1}y \in H)$

$\iff m-k \in n\mathbb{Z} \iff n \mid m-k$

$\iff \exists t \in \mathbb{Z} \quad m = k+nt$

Άρα, $\forall m \in \mathbb{Z}$ $[m]_H = m+H = m+n\mathbb{Z}$

Από Ευκλείδεια Διαίρεση του m με το n έχουμε $m = nq+r$, $0 \leq r \leq n-1$, άρα:

$[m]_H = m+n\mathbb{Z} = (nq+r)+n\mathbb{Z}$.

δηλαδή: αν $k \in [m]_H$ τότε: $k = nq+r+nt$

για κάποιο $t \in \mathbb{Z}$ ή ισοδύναμα:

$k = r+n(q+t) \in r+n\mathbb{Z}$, με $0 \leq r \leq n-1$.

Συνεπώς, $\mathbb{Z}/_{n\mathbb{Z}} = \{ m + n\mathbb{Z} \subseteq \mathbb{Z} \mid m \in \mathbb{Z} \}$

$= \{ r + n\mathbb{Z} \subseteq \mathbb{Z} \mid 0 \leq r \leq n-1 \}$

$\Longrightarrow [\mathbb{Z} : n\mathbb{Z}] = n$

(4) $S_3 = \{ Id, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2) \}$

$H = \{ Id, (1\ 2) \} = \langle (1\ 2) \rangle \leq S_3$

• $Id\, H = H = \{ Id, (1\ 2) \}$

• $(1\ 2) H = \{ (1\ 2) \circ Id, (1\ 2) \circ (1\ 2) \}$

$= \{ (1\ 2), Id \}$ (διότι $(1\ 2)^2 = (1\ 2) \circ (1\ 2) = Id$)

$= H$

(λογικό διότι: $(1, 2)^{-1} \circ Id = (1\ 2) \in H$)

• $(1\ 3) H = \{ (1\ 3) \circ Id, (1\ 3) \circ (1\ 2) \}$

$= \{ (1\ 3), (1\ 2\ 3) \}$

• $(2\ 3) H = \{ (2\ 3) \circ Id, (2\ 3) \circ (1\ 2) \}$

$$= \{(2\ 3), (1\ 3\ 2)\}$$

- $(1\ 2\ 3)H = \{(1\ 2\ 3) \circ Id, (1\ 2\ 3) \circ (1\ 2)\}$
$$= \{(1\ 2\ 3), (1\ 3)\} = (1\ 3)H$$

$$\left(\begin{array}{l} (1\ 2\ 3)^{-1} \circ (1\ 3) = (1\ 3\ 2) \circ (1\ 3) = \\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2) \in H \end{array} \right)$$

- $(1\ 3\ 2)H = \{(1\ 3\ 2) \circ Id, (1\ 3\ 2) \circ (1\ 2)\}$
$$= \{(1\ 3\ 2), (2\ 3)\} = (2\ 3)H$$

$$\left(\begin{array}{l} (1\ 3\ 2)^{-1} \circ (2\ 3) = (1\ 2\ 3) \circ (2\ 3) = \\ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1\ 2) \in H \end{array} \right)$$

Άρα, $S_3/H = \{\sigma H \subseteq S_3 \mid \sigma \in S_3\} =$

$$= \{IdH, (1\ 2)H, (1\ 3)H, (2\ 3)H, (1\ 2\ 3)H, (1\ 3\ 2)H\}$$

$$= \{H, H, (1\ 3)H, (2\ 3)H, (1\ 3)H, (2\ 3)H\}$$

$= \{ H, (1\ 3)H, (2\ 3)H \}$.

Επομένως, $[S_3 : H] = 3$

Ασκήσεις H/W: (1) Να βρείτε τον δείκτη $[S_3 : H]$, όπου $H = \langle (1\ 2\ 3) \rangle$

(2) Να βρείτε τον δείκτη $[\mathbb{Z}_{12} : H]$, όπου $H = \langle [8]_{12} \rangle$

Θεώρημα Lagrange

Έστω $(G, \cdot)$ μια πεπερασμένη ομάδα και $H \leq G$. Τότε $|G| = |H| \cdot [G:H]$

Συνεπώς, $|H| \mid |G|$.

Απόδειξη: Έχουμε $G = \bigcup\limits_{i=1}^{k} [x_i]_H = \bigcup\limits_{i=1}^{k} x_i H$ (1),

όπου τα $x_1 H, \ldots, x_k H$ είναι τα διακεκριμμένα αριστερά σύμπλοκα της H στην G, δηλαδή

$$G/_H = \{ x_1 H, \ldots, x_k H \}, \text{ άρα } [G:H] = k$$

Επειδή $|x_i H| = |H|$, $\forall i = 1, \ldots, k$ και η (1) είναι διακεκριμμένη ένωση, παίρνουμε:

$$|G| = \left| \bigcup_{i=1}^{k} x_i H \right| = \sum_{i=1}^{k} |x_i H| = \sum_{i=1}^{k} |H| =$$

$$k|H| = |H| \cdot [G:H].$$

Πρόταση: Έστω $(G, \cdot)$ πεπερασμένη ομάδα.

Τότε, $\forall x \in G$, 1. $x^{|G|} = e$

2. $o(x) \mid |G|$.

Απόδειξη: Έστω $x \in G$ και θεωρούμε την κυκλική υποομάδα $H = \langle x \rangle$ που παράγεται από το x. Τότε, $o(x) = |H|$.

Από Θεώρημα Lagrange, $o(x) \mid |G|$ (2.)

και $|G| = o(x)[G:H]$, άρα:

$$x^{|G|} = x^{o(x)[G:H]} = \left(x^{o(x)}\right)^{[G:H]} = e^{[G:H]} = e. \ (1$$

■

Εφαρμογή: Για $n \in \mathbb{N}$, $n \geq 2$ έχουμε: $A_n \leq S$

άρα από Θεώρημα Lagrange:

$$|S_n| = |A_n| \cdot [S_n : A_n] \Rightarrow n! = \frac{n!}{2}[S_n : A_n]$$

$$\Rightarrow \boxed{[S_n : A_n] = 2}$$

■

Πρόταση: Έστω $H \leq G$ με $[G:H] = 2$.

Τότε, $H \trianglelefteq G$.

Απόδειξη: Για κάθε $x \in G \setminus H$, τα αριστερά σύμπλοκα H και xH είναι διαφορετικά (διότι $H = xH \iff x \in H$). Επιπλέον, το $\{H, xH\}$ είναι μια διαμέριση του G (αφού $[G:H] = 2$) και άρα: $\begin{cases} G = H \cup xH \\ \text{και} \\ H \cap xH = \emptyset \end{cases}$,

οπότε $xH = G \setminus H$. Παρόμοια θα έχουμε: $Hx = G \setminus H$. Συνεπώς, $xH = Hx$, $\forall x \in G \setminus H$.

Απ' την άλλη, $xH = Hx$, $\forall x \in H$ αφού $H \leq G$.

Αυτά δίνουν: $xH = Hx$, $\forall x \in G$, ή ισοδύναμα: $xHx^{-1} = H$, $\forall x \in G$, που σημαίνει ότι $H \trianglelefteq G$, όπως θέλαμε. ∎

ΟΜΑΔΕΣ - ΠΗΛΙΚΑ / ΘΕΩΡΗΜΑΤΑ ΙΣΟΜΟΡΦΙΣΜΩΝ

Έστω $(G, \cdot)$ μια ομάδα και $H \leq G$.

Έχουμε ορίσει τις εξής σχέσεις ισοδυναμίας επί του G:

- $\forall x, y \in G: \quad x \underset{H}{\sim} y \iff xy^{-1} \in H$

Εδώ: $G/_H = \{ Hx \subseteq G \mid x \in G \}$

- $\forall x, y \in G: \quad x \underset{H}{\sim} y \iff x^{-1}y \in H$

Εδώ: $G/_H = \{ xH \subseteq G \mid x \in G \}$

Γενικά, δεν ισχύει: $xH = Hx$ για $x \in G$.

Αν όμως $H \trianglelefteq G$ τότε $xHx^{-1} = H$, $\forall x \in G$, άρα $xH = Hx$, $\forall x \in G$ και μπορούμε να ασχοληθούμε μόνο με τα αριστερά σύμπλοκα της H στην G

▶ Έστω $H \trianglelefteq G$ και θεωρούμε το σύνολο-πηλίκο $G/_H = \{ xH \subseteq G \mid x \in G \}$ ως προς τη σχέση ισοδυναμίας $\sim_H$.

Στο μη-κενό σύνολο G/H ορίζουμε:

$$\cdot : G/_H \times G/_H \to G/_H$$
$$(xH, yH) \mapsto xH \cdot yH = xyH$$

<u>Ισχυρισμός</u>: Η $\cdot$ είναι καλά ορισμένη πράξη επί του $G/_H$

Απόδειξη : Προφανώς, για κάθε

$(xH, yH) \in G/_H \times G/_H$ ισχύει :

$\cdot (xH, yH) = xH \cdot yH = (xy)H \in G/H$.

Μένει να δείξουμε ότι αν $(xH, yH) = (zH, wH)$

τότε $xH \cdot yH = zH \cdot wH$, δηλαδή ισοδύναμα

ότι : $(xy)H = (zw)H$. Πράγματι, επειδή

$$(xH, yH) = (zH, wH) \Rightarrow \left\{ \begin{array}{c} xH = zH \\ \text{και} \\ yH = wH \end{array} \right. , \text{ άρα}$$

$x^{-1}z \in H$ και $y^{-1}w \in H$. Έτσι,

$$(xy)H = (zw)H \Leftrightarrow (xy)^{-1}zw \in H \Leftrightarrow \underbrace{y^{-1}x^{-1}zw \in H}_{\substack{\text{αρκεί να} \\ \text{αποδείξουμε αυτό.}}}$$

Πράγματι, $y^{-1}x^{-1}zw = (y^{-1}x^{-1}zy)\, y^{-1}w \quad (*)$

Επειδή $x^{-1}z \in H$ και $H \trianglelefteq G$, προκύπτει

$y^{-1}x^{-1}zy \in y^{-1}Hy = H$

Από την άλλη, $y^{-1}w \in H$ και εφ' όσον $H \leq G$ παίρνουμε $(y^{-1}x^{-1}zy)y^{-1}w \in H$

$\Rightarrow y^{-1}x^{-1}zw \in H$, όπως θέλαμε.

• Για κάθε $xH, yH, zH \in G/H$ έχουμε:

$(xH \cdot yH) \cdot zH = (xy)H \cdot zH = (xy) \cdot zH =$

$x(yz)H = xH \cdot (yz)H) = xH \cdot (yH\, zH)$

δηλαδή η $\cdot$ είναι προσεταιριστική πράξη στο G/H

• Υπάρχει το $eH = H \in G/H$ ώστε:

$xH \cdot eH = xeH = xH$, $\forall xH \in G/H$

$eH \cdot xH = exH = xH$

δηλαδή το σύμπλοκο $eH = H$ είναι ουδέτερο στοιχείο του G/H ως προς την $\cdot$

• Για κάθε $xH \in G/H$ υπάρχει το $x^{-1}H \in G/H$

ώστε $xH \cdot x^{-1}H = xx^{-1}H = eH = H$

$x^{-1}H \cdot xH = x^{-1}xH = eH = H$

<u>Συμπέρασμα</u>: Το ζεύγος $(G/H, \cdot)$ είναι ομάδα με ουδέτερο στοιχείο το $eH = H$ και $\forall xH \in G/H$ έχουμε $(xH)^{-1} = x^{-1}H$.

Επιπλέον, $|G/H| = [G : H]$

<u>Παρατηρήσεις</u>: (1) $(xH)^k = x^k H, \ \forall k \in \mathbb{Z}$

(2) Αν $g \in G$ με $o(g) = n \in \mathbb{N}$ τότε

$o(gH) \mid n$

Πράγματι, $g^n = e$, άρα $(gH)^n = g^n H = eH = H$

$\Rightarrow o(gH) \mid n$

<u>Ορισμός</u>: Η $(G/H, \cdot)$ λέγεται <u>ομάδα-πηλίκο</u> της G ως προς την H.

<u>Πρόταση</u>: Έστω $(G,\cdot)$ μια κυκλική ομάδα. Τότε για κάθε υποομάδα H της G η ομάδα-πηλίκο G/H είναι κυκλική.

<u>Απόδειξη</u>: Έστω $H \leq G$. Επειδή η G είναι κυκλική, είναι και αβελιανή, άρα $H \trianglelefteq G$, οπότε ορίζεται η ομάδα-πηλίκο G/H.

Έστω $G = \langle a \rangle$. Θα αποδείξουμε ότι $G/H = \langle aH \rangle$. Επειδή $\langle aH \rangle \leq G/H$, αρκεί να δείξουμε ότι $G/H \subseteq \langle aH \rangle$. Έστω $xH \in G/H$. Τότε $x \in G = \langle a \rangle \Rightarrow \exists\, k \in \mathbb{Z} : x = a^k$

άρα: $xH = a^k H = (aH)^k \in \langle aH \rangle$, όπως θέλαμε.

Ώστε, G/H : κυκλική. ∎

Σχόλιο: Σε προσθετικές ομάδες $(G,+)$ για $H \trianglelefteq G$ γράφουμε:

- $G/H = \{x+H \subseteq G \mid x \in G\}$
- $(x+H)+(y+H) = (x+y)+H$
- **ουδέτερο**: $H = 0+H$
- **αντίθετο**: $-(x+H) = (-x)+H$
- $n \in \mathbb{Z}$, $n(x+H) = nx+H$

Σχόλιο: Αν $(G,\cdot)$ είναι μια ομάδα και $H \trianglelefteq G$ τότε ορίζεται η απεικόνιση

$\pi : G \longrightarrow G/H$ με $\pi(x) = xH$.

$\forall x,y \in G$: $\pi(xy) = (xy)H = xH \cdot yH = \pi(x)\cdot\pi(y)$

άρα π: μορφισμός ομάδων.

Επίσης, η π είναι επί του G/H,

δηλαδή π: επιμορφισμός.

Τέλος $Ker(\pi) = \{ x \in G \mid \pi(x) = e_{G/H} \} =$

$\{ x \in G \mid xH = H \} = \{ x \in G \mid x \in H \} = H$

Η απεικόνιση π ονομάζεται <u>προβολή</u>.

<u>1ο ΘΕΩΡΗΜΑ ΙΣΟΜΟΡΦΙΣΜΩΝ ΟΜΑΔΩΝ</u>

Έστω $f : G_1 \to G_2$ μορφισμός ομάδων.

Τότε $G_1 / \ker(f) \cong Im(f)$.

<u>Απόδειξη</u>: Επειδή $f : G_1 \to G_2$ μορφισμός προκύπτει ότι $Ker(f) \trianglelefteq G_1$ και άρα ορίζεται η ομάδα-πηλίκο $G_1 / \ker(f)$. Θεωρούμε απεικόνιση

$$\tilde{f} : G_1 / \ker(f) \longrightarrow Im(f)$$
$$x \, Ker(f) \longmapsto f(x)$$

Υπενθυμίζουμε ότι $Im(f) = \{ f(x) \in G_2 \mid x \in G_1 \}$

$$\leq G_2$$

1. Η $\tilde{f}$ είναι καλά ορισμένη : Αρχικά, για κάθε $xKer(f) \in G_1/Ker(f)$ ισχύει

$$\tilde{f}(xKer(f)) = f(x) \in Im(f).$$

Θα δείξουμε τώρα ότι αν $xKer(f) = yKer(f)$ τότε $\tilde{f}(xKer(f)) = \tilde{f}(yKer(f))$, δηλαδή θα δείξουμε ότι $f(x) = f(y)$. Πράγματι,

$$xKer(f) = yKer(f) \Rightarrow x^{-1}y \in Ker(f) \Rightarrow$$

$$f(x^{-1}y) = e_2 \xrightarrow[\text{μορφ.}]{f} f(x^{-1})f(y) = e_2 \xrightarrow[\text{μορφ.}]{f} (f(x))^{-1}f(y) = e_2$$

$$\Rightarrow f(x)(f(x))^{-1}f(y) = f(x)e_2 \Rightarrow f(y) = f(x),$$ όπως θέλαμε.

2. Η $\tilde{f}$ είναι μορφισμός ομάδων : Για κάθε $xKer(f), yKer(f) \in G_1/Ker(f)$ έχουμε:

$$\tilde{f}(xKer(f) \cdot yKer(f)) = \tilde{f}((xy)Ker(f)) = f(xy) \underset{\text{μορφ.}}{\overset{f}{=}}$$

$$f(x)f(y) = \tilde{f}(xKer(f))\tilde{f}(yKer(f)).$$

3. <u>Η $\tilde{f}$ είναι επιμορφισμός</u> : Έστω $y \in Im(f)$

Τότε $y = f(x)$ για κάποιο $x \in G_1$. Έτσι,

$x Ker(f) \in G_1/_{Ker(f)}$ και $\tilde{f}(x Ker(f)) = f(x) = y$.

4. <u>Η $\tilde{f}$ είναι μονομορφισμός</u> :

Έστω $\tilde{f}(x Ker(f)) = \tilde{f}(y Ker(f))$ και θα δείξουμε

ότι $x Ker(f) = y Ker(f)$. Πράγματι, έχουμε

$\tilde{f}(x Ker(f)) = \tilde{f}(y Ker(f)) \Rightarrow f(x) = f(y) \Longrightarrow$

$(f(x))^{-1} f(x) = (f(x))^{-1} f(y) \underset{\text{μορφ.}}{\overset{f}{\Rightarrow}} e_2 = f(x^{-1}) f(y) \underset{\text{μορφ.}}{\overset{f}{\Longrightarrow}}$

$e_2 = f(x^{-1}y) \Rightarrow x^{-1}y \in Ker(f) \Rightarrow x Ker(f) = y Ker(f)$.

Από τα 1.-4. συμπεραίνουμε ότι η $\tilde{f}$ είναι

ισομορφισμός ομάδων και επομένως

$$G_1/_{Ker(f)} \cong Im(f)$$

$\blacksquare$

Σχόλια: Έστω $f: G_1 \to G_2$ μορφισμός ομάδων.

Ⓐ Αν ο f είναι μονομορφισμός τότε $Ker(f) = \{e_1\}$, οπότε

$$G_1/\{e_1\} \cong Im(f) \Rightarrow G_1 \cong G_1/\{e_1\} \cong Im(f).$$

Ⓑ Αν ο f είναι επιμορφισμός τότε $Im(f) = G_2$, οπότε $G_1/_{Ker(f)} \cong G_2$

ΕΦΑΡΜΟΓΕΣ

(I) Έστω $n \in \mathbb{N}$ και θεωρούμε τον επιμορφισμό $\pi: (\mathbb{Z}, +) \to (\mathbb{Z}_n, +)$ με $\pi(x) = [x]_n$.

$$Ker(\pi) = \{x \in \mathbb{Z} \mid \pi(x) = [0]_n\} = \{x \in \mathbb{Z} \mid [x]_n = [0]_n\}$$

$$= \{x \in \mathbb{Z} \mid n|x\} = \{nk \in \mathbb{Z} \mid k \in \mathbb{Z}\} = n\mathbb{Z}.$$

Από 1º Θεώρημα Ισομορφισμών έχουμε

$$\boxed{\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n}$$

(II) Έστω $n \in \mathbb{N}$, $n \geq 2$ και θεωρούμε τον επιμορφισμό $\varepsilon : (S_n, \circ) \to (\mathbb{Z}_2, +)$ με

$$\varepsilon(\sigma) = \begin{cases} [0]_2, & \sigma : \text{άρτια} \\ [1]_2, & \sigma : \text{περιττή} \end{cases}$$

$$Ker(\varepsilon) = \{\sigma \in S_n \mid \varepsilon(\sigma) = [0]_2\} = A_n$$

Από 1º Θεώρημα Ισομορφισμών έχουμε

$$\boxed{S_n / A_n \cong \mathbb{Z}_2}$$

(III) Ορίζουμε $f : (GL(2, \mathbb{R}), \cdot) \to (\mathbb{R}^*, \cdot)$ με

$f(A) = det(A)$

- Η f είναι καλά ορισμένη διότι αν $A \in GL(2, \mathbb{R})$ τότε $det(A) \neq 0 \Rightarrow f(A) = det(A) \in \mathbb{R}^*$
- Για κάθε $A, B \in GL(2, \mathbb{R})$ έχουμε

$f(AB) = det(AB) = det(A) det(B) = f(A) f(B)$, οπότε

f: μορφισμός ομάδων.

• $Im(f) = \mathbb{R}^*$: Πράγματι, αν $a \in \mathbb{R}^*$ τότε

$$A = \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in GL(2,\mathbb{R}) \text{ διότι } \det(A) = a \neq 0$$

και συνεπώς $f(A) = \det(A) = a$

• $Ker(f) = \{ A \in GL(2,\mathbb{R}) \mid f(A) = 1 \} =$

$= \{ A \in GL(2,\mathbb{R}) \mid \det(A) = 1 \} = SL(2,\mathbb{R})$

Από 1º Θεώρημα Ισομορφισμών έχουμε

$$GL(2,\mathbb{R}) / SL(2,\mathbb{R}) \cong \mathbb{R}^*$$

Σχόλιο επί των (II), (III) : Αν $(G, \cdot)$ είναι αβελιανή ομάδα και $H \leq G$ τότε $H \trianglelefteq G$. Άρα ορίζεται η ομάδα - πηλίκο G/H και είναι και αυτή αβελιανή. Πράγματι, $\forall xH, yH \in G/H$ $\quad xH \cdot yH = xyH \underset{\text{αβελιανή}}{\overset{G}{=}} yxH =$

$= yH \cdot xH$

Συνεπώς, πηλίκο αβελιανής ομάδος είναι επίσης αβελιανή. Το αντίστροφο δεν ισχύει: Για παράδειγμα, στην Εφαρμογή (ΙΙ), αν $n \geq 3$, τότε η $(S_n, \circ)$ δεν είναι αβελιανή. Ωστόσο: $S_n / A_n \cong \mathbb{Z}_2$ και επειδή η $\mathbb{Z}_2$ είναι αβελιανή, έπεται S_n/A_n αβελιανή.

(IV) Έστω $m, n \in \mathbb{N}$ με $(m,n) = 1$. Ορίζουμε $f : (\mathbb{Z}_{mn}, +) \to (\mathbb{Z}_m \times \mathbb{Z}_n, +)$ με

$$f([x]_{mn}) = ([x]_m, [x]_n)$$

• Για κάθε $[x]_{mn}, [y]_{mn} \in \mathbb{Z}_{mn}$ έχουμε:

$$f([x]_{mn} + [y]_{mn}) = f([x+y]_{mn}) = ([x+y]_m, [x+y]_n)$$

$$= ([x]_m + [y]_m, [x]_n + [y]_n) = ([x]_m, [x]_n) + ([y]_m, [y]_n)$$

$$= f([x]_{mn}) + f([y]_{mn})$$

Ώστε, f μορφισμός ομάδων.

• Έστω $[x]_{mn} \in Ker(f)$. Τότε

$f([x]_{mn}) = ([0]_m, [0]_n)$, άρα $([x]_m, [x]_n) = ([0]_m, [0]_n)$

$\Rightarrow \begin{cases} [x]_m = [0]_m \\ \text{κ'} \\ [x]_n = [0]_n \end{cases} \Rightarrow m|x$ και $n|x$

$\Rightarrow [m,n] | x \xrightarrow[\text{Αριθμών}]{\text{Θεωρία}} \frac{mn}{(m,n)} | x \xRightarrow{(m,n)=1}$

$mn|x \Rightarrow [x]_{mn} = [0]_{mn}$

Ώστε, $Ker(f) \subseteq \{[0]_{mn}\}$. Απ' την άλλη,

$\{[0]_{mn}\} \subseteq Ker(f)$ και άρα $Ker(f) = \{[0]_{mn}\}$,

δηλαδή f: μονομορφισμός.

Από 1º Θεώρημα Ισομορφισμών:

$\mathbb{Z}_{mn} \cong Im(f)$. Άρα $|Im(f)| = |\mathbb{Z}_{mn}| = mn$.

Επειδή $Im(f) \leq \mathbb{Z}_m \times \mathbb{Z}_n$ και

$mn = |Im(f)| = |\mathbb{Z}_m \times \mathbb{Z}_n|$, παίρνουμε:

$Im(f) = \mathbb{Z}_m \times \mathbb{Z}_n$. Τελικά: $\boxed{\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n \text{ για } (m,n)=1}$

(V) Θεωρούμε το σύνολο $G = \{ e^{2\pi i \theta} \in \mathbb{C} \mid \theta \in \mathbb{Q} \}$

(i) Να δείξετε ότι το σύνολο G εφοδιασμένο με την πράξη πολ/μού μιγαδικών αριθμών είναι ομάδα

(ii) Να δείξετε ότι $\mathbb{Q}/\mathbb{Z} \cong G$

<u>Λύση</u>: (i) Γενικά: $\boxed{e^{ix} = \cos x + i \sin x, \ x \in \mathbb{R}}$

Τύπος Euler

$e^0 = 1$. Από στοιχειώδεις ιδιότητες τριγωνομετρίας προκύπτει εύκολα: $e^{i(x+y)} = e^{ix+iy} = e^{ix} \cdot e^{iy}$ $\forall x, y \in \mathbb{R}$

και: $e^{ix} \in \mathbb{C}^*$, $\forall x \in \mathbb{R}$.

Τώρα, $G \neq \emptyset$, $1 = e^0 = e^{2\pi i \cdot 0} \in G$, $G \subseteq \mathbb{C}^*$

και αν $e^{2\pi i \theta}, e^{2\pi i \varphi} \in G$, με $\theta, \varphi \in \mathbb{Q}$, τότε

$$e^{2\pi i \theta} \left(e^{2\pi i \varphi} \right)^{-1} = e^{2\pi i \theta} e^{-2\pi i \varphi} = e^{2\pi i (\theta - \varphi)} \in G$$

(αφού $\theta - \varphi \in \mathbb{Q}$) $\left\{ \text{Χρησιμοποιήσαμε το γεγονός ότι: } (e^{ix})^{-1} = e^{-ix}, \ x \in \mathbb{R} \right\}$

Συνεπώς, $G \leq (\mathbb{C}^*, \cdot)$ και άρα $(G, \cdot)$ ομάδα.

(ii) Θεωρούμε την απεικόνιση $f : (\mathbb{Q}, +) \to (G, \cdot)$ με $f(\theta) = e^{2\pi i \theta}$ η οποία είναι προφανώς επί του G.

Για κάθε $\theta, \varphi \in \mathbb{Q}$ έχουμε:

$$f(\theta+\varphi) = e^{2\pi i(\theta+\varphi)} = e^{2\pi i\theta + 2\pi i\varphi}$$
$$= e^{2\pi i\theta} \cdot e^{2\pi i\varphi} = f(\theta) f(\varphi),$$

οπότε f: επιμορφισμός ομάδων. Επίσης,

$$Ker(f) = \{\theta \in \mathbb{Q} \mid f(\theta) = 1\} = \{\theta \in \mathbb{Q} \mid e^{2\pi i\theta} = 1 + 0i\}$$
$$= \{\theta \in \mathbb{Q} \mid \cos(2\pi\theta) + i\sin(2\pi\theta) = 1 + 0i\} =$$
$$= \{\theta \in \mathbb{Q} \mid \cos(2\pi\theta) = 1 \text{ και } \sin(2\pi\theta) = 0\}$$

$$\cdot \begin{cases} \cos(2\pi\theta) = 1 \\ \sin(2\pi\theta) = 0 \end{cases} \iff \begin{matrix} \exists \kappa \in \mathbb{Z} : 2\pi\theta = 2\kappa\pi \\ \exists \lambda \in \mathbb{Z} : 2\pi\theta = \lambda\pi \end{matrix}$$

Άρα, πρέπει $\lambda = 2\kappa$ και

$2\pi\theta = 2\kappa\pi \Rightarrow \theta = \kappa \in \mathbb{Z}$.

Από την άλλη, αν $\kappa \in \mathbb{Z}$ τότε:

$e^{2\pi i \kappa} = \cos(2\pi\kappa) + i\sin(2\pi\kappa) = 1 \Rightarrow f(\kappa) = 1$

$\Rightarrow \kappa \in Ker(f)$.

Τελικά, $Ker(f) = \mathbb{Z}$.

Από 1ο θεώρημα Ισομορφισμών, έχουμε:

$$\boxed{\mathbb{Q}/\mathbb{Z} \cong G}$$

■