Φυλλάδιο Β

Β1. Έστω $G = \langle \alpha \rangle$ μια κυκλική ομάδα και έστω $H \leq G$.

- Αν $H = \{e\}$ τότε $H = \langle e \rangle$: κυκλική.
- Αν $H \neq \{e\}$ τότε υπάρχει $g \in H$ με $g \neq e$.

Επίσης, $g \in H \Rightarrow g \in G \Rightarrow g \in \langle \alpha \rangle$

$$\Rightarrow \exists \kappa \in \mathbb{Z} : g = \alpha^{\kappa}$$

Τότε, $\kappa \neq 0$ διότι αν $\kappa = 0$ θα είχαμε $g = \alpha^{\kappa} = \alpha^{0} = e$, το οποίο είναι άτοπο.

Αν $\kappa < 0$, τότε εφ' όσον $H \leq G$ και $g \in H$ έχουμε: $g^{-1} \in H \Rightarrow (\alpha^{\kappa})^{-1} \in H \Rightarrow \alpha^{-\kappa} \in H$ με $-\kappa > 0$. Επομένως, η υποομάδα H περιέχει θετικές δυνάμεις α^{κ}, με $\kappa > 0$, του γεννήτορα α της G.

Αυτό σημαίνει ότι το σύνολο φυσικών αριθμών $\{\lambda \in \mathbb{N} \mid \alpha^{\lambda} \in H\}$ είναι μη-κενό και από την Αρχή Καλής Διάταξης, έχει ελάχιστο στοιχείο. Έστω $n = \min\{\lambda \in \mathbb{N} \mid \alpha^{\lambda} \in H\}$, δηλαδή ο n είναι ο ελάχιστος φυσικός αριθμός με την ιδιότητα $\alpha^{n} \in H$. Θα αποδείξουμε ότι $H = \langle \alpha^{n} \rangle$ και άρα H: κυκλική.

Επειδή $\alpha^{n} \in H$ και $H \leq G$ έχουμε $\langle \alpha^{n} \rangle \subseteq H$.

Αντίστροφα, έστω $h \in H$. Τότε $h \in G \Rightarrow$
$\Rightarrow h \in \langle \alpha \rangle \Rightarrow \exists m \in \mathbb{Z} : h = \alpha^{m}$. Η Ευκλείδεια διαίρεση του m με το n δίνει ακέραιους q, r ώστε $m = nq + r$ με $0 \leq r \leq n-1$. Τότε: $h \in H \Rightarrow \alpha^{m} \in H \Rightarrow$
$\alpha^{nq+r} \in H \Rightarrow \alpha^{nq} \cdot \alpha^{r} \in H \Rightarrow$

$(\alpha^n)^q \cdot \alpha^r \in H \Rightarrow \exists\, x \in H : (\alpha^n)^q \cdot \alpha^r = x$,

οπότε: $\alpha^r = (\alpha^n)^{-q}$. (*)

▸ $\left\{\begin{array}{l} \alpha^n \in H \\ \text{και} \\ x \in H \end{array}\right. \xRightarrow{H \leq G} \left\{\begin{array}{l} (\alpha^n)^{-q} \in H \\ \text{και} \\ x \in H \end{array}\right. \xRightarrow[H \leq G]{} (\alpha^n)^{-q} x \in H$

$\xRightarrow{(*)} \alpha^r \in H$. Το r είναι είτε 0 ή φυσικός αριθμός με $r \leq n-1 < n$. Αν ο r είναι φυσικός με $r < n$ τότε το γεγονός ότι $\alpha^r \in H$ αντίκειται στο γεγονός ότι ο n είναι ο μικρότερος φυσικός αριθμός με την ιδιότητα $\alpha^n \in H$. Άρα, αναγκαστικά, $r = 0 \Rightarrow m = nq$, οπότε:

$$h = \alpha^m = \alpha^{nq} = (\alpha^n)^q \in \langle \alpha^n \rangle.$$

Συμπεραίνουμε ότι: $H \subseteq \langle \alpha^n \rangle$. Τελικά,

$H = \langle \alpha^n \rangle$, όπως θέλαμε. ∎

Συμπεράσματα της Άσκησης Β1

(I) Έστω $G = \langle a \rangle$ μια άπειρη κυκλική ομάδα. Τότε οι υποομάδες της G είναι οι ακόλουθες και μόνο αυτές:

$H_n = \langle a^n \rangle$ με $n \in \mathbb{N}_0$, δηλαδή οι:

$\langle a^0 \rangle = \langle e \rangle = \{e\}$, $\langle a^1 \rangle = \langle a \rangle = G$, $\langle a^2 \rangle$, $\langle a^3 \rangle$, $\langle a^4 \rangle$, ...

Επίσης για $H_n = \langle a^n \rangle$ και $H_m = \langle a^m \rangle$ με $n, m \in \mathbb{N}_0$ έχουμε:

(i) $H_n \leq H_m \iff m \mid n$

(ii) $H_n = H_m \iff n = m$

<u>ΑΡΑ</u>: Για την άπειρη κυκλική ομάδα $(\mathbb{Z}, +)$ με γεννήτορα το $1 \in \mathbb{Z}$

συμπεραίνουμε ότι οι μόνες υποομάδες της $(\mathbb{Z},+)$ είναι οι ακόλουθες:

- $H_0 = \langle 0\cdot 1 \rangle = \langle 0 \rangle = \{0\}$
- $H_1 = \langle 1\cdot 1 \rangle = \langle 1 \rangle = \mathbb{Z}$
- $H_2 = \langle 2\cdot 1 \rangle = \langle 2 \rangle = \{2k \in \mathbb{Z} \mid k \in \mathbb{Z}\} = 2\mathbb{Z}$
- $H_3 = \langle 3\cdot 1 \rangle = \langle 3 \rangle = \{3k \in \mathbb{Z} \mid k \in \mathbb{Z}\} = 3\mathbb{Z}$

$\vdots \quad \vdots \quad \vdots \quad \vdots$

- $H_n = \langle n\cdot 1 \rangle = \langle n \rangle = \{nk \in \mathbb{Z} \mid k \in \mathbb{Z}\} = n\mathbb{Z}$

$\vdots \quad \vdots$

Επιπλέον, για $n, m \in \mathbb{N}_0$ έχουμε

(i)' $n\mathbb{Z} \subseteq m\mathbb{Z} \iff m \mid n$

(ii)'' $n\mathbb{Z} = m\mathbb{Z} \iff n = m$

(II) Έστω $G = \langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ μια πεπερασμένη κυκλική ομάδα τάξης $n \in \mathbb{N}$, δηλαδή $|G| = |\langle a \rangle| = o(a) = n \in \mathbb{N}$.

▶ Έστω $H \leq G$. Σύμφωνα με τη B1 η H είναι επίσης κυκλική. Άρα $H = \langle a^m \rangle$ για κάποιο $m = 0, 1, 2, \dots, n-1$. Θα αποδείξουμε ότι $H = \langle a^d \rangle$, όπου $d = (n, m)$ και

$$o(H) = o(a^d) = \frac{o(a)}{(o(a), d)} = \frac{n}{(n, d)} = \frac{n}{d}$$

. Επειδή $d = (n, m)$ έπεται $d \mid m$, άρα $m = dk$ για κάποιο $k \in \mathbb{N}$, άρα:

$$a^m = a^{dk} = (a^d)^k \in \langle a^d \rangle \implies H = \langle a^m \rangle \underset{(*)}{\leq} \langle a^d \rangle$$

Αντίστροφα, έστω $x \in \langle a^d \rangle$. Τότε:

$x = (a^d)^q = a^{dq}$ για κάποιο $q \in \mathbb{Z}$.

Εφ' όσον $d=(n,m)$, υπάρχουν $\lambda, r \in \mathbb{Z}$ ώστε $d = n\lambda + mr$ και συνεπώς:

$$x = a^{dq} = a^{n\lambda q + rmq} = (a^n)^{\lambda q} \cdot (a^m)^{rq} \xlongequal[a^n = e]{o(a)=n}$$

$$e^{\lambda q} \cdot (a^m)^{rq} = e \cdot (a^m)^{rq} = (a^m)^{rq} \in \langle a^m \rangle = H.$$

Άρα, $\langle a^d \rangle \subseteq H$ $(**)$. Λόγω $(*)$, $(**)$ προκύπτει: $H = \langle a^d \rangle$.

❗ Για εφαρμογή του (II) βλέπε Άσκηση B4.

B2. Αφού $K \trianglelefteq G$ έπεται $axa^{-1} \in K$, $\forall a \in G$, $\forall x \in K$. Ιδιαίτερα, αφού $H \leq G$:

$\forall h \in H$, $\forall x \in K$: $hxh^{-1} \in K$.

Συνεπώς, $K \trianglelefteq H$. ∎

B3. Από το Θεώρημα Lagrange έχουμε:

$$o(g) \mid |G| \Rightarrow o(g) \mid p^2 \xrightarrow[\text{πρώτος}]{p:} o(g) \in \{1, p, p^2\}.$$

· Αν $o(g) = 1$ τότε $g^1 = e \Rightarrow g = e$, άτοπο.

· Αν $o(g) = p^2$ τότε: $|\langle g \rangle| = o(g) = p^2 = |G|$

και επειδή $\langle g \rangle \leq G$ προκύπτει: $G = \langle g \rangle$,

δηλαδή G: κυκλική, άτοπο. Τελικά, $o(g) = p$ ∎

B4. Ακολουθούμε την τακτική (II) της άσκησης B1. Η $(\mathbb{Z}_{12}, +)$ είναι πεπερασμένη κυκλική με γεννήτορα το $[1]_{12}$.

$$\mathbb{Z}_{12} = \{ [0]_{12}, [1]_{12}, [2]_{12}, \ldots [11]_{12} \}$$

$$= \left\{ \begin{array}{l} [0]_{12}, [1]_{12}, 2[1]_{12}, 3[1]_{12}, 4[1]_{12}, 5[1]_{12}, \\ 6[1]_{12}, 7[1]_{12}, 8[1]_{12}, 9[1]_{12}, 10[1]_{12}, \\ 11[1]_{12} \end{array} \right\}$$

- $H_0 = \langle 0 \cdot [1]_{12} \rangle = \langle [0]_{12} \rangle = \{ [0]_{12} \}$.

$|H_0| = 1 \mid 12$

- $H_1 = \langle 1 \cdot [1]_{12} \rangle = \langle [1]_{12} \rangle = \mathbb{Z}_{12}$

$|H_1| = 12 \mid 12$

- $H_2 = \langle 2 \cdot [1]_{12} \rangle = \langle d[1]_{12} \rangle$, όπου $d = (12, 2) = 2$

άρα $H_2 = \langle 2[1]_{12} \rangle = \langle [2]_{12} \rangle =$

$= \{ [0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12} \}$

$|H_2| = 6 \mid 12$

- $H_3 = \langle 3 \cdot [1]_{12} \rangle = \langle d'[1]_{12} \rangle$, όπου $d' = (12, 3) = 3$

άρα $H_3 = \langle 3[1]_{12} \rangle = \langle [3]_{12} \rangle =$

$= \{ [0]_{12}, [3]_{12}, [6]_{12}, [9]_{12} \}$

$|H_3| = 4 \mid 12$

- $H_4 = \langle 4 \cdot [1]_{12} \rangle = \langle d''[1]_{12} \rangle$, όπου $d'' = (12, 4) = 4$

άρα: $H_4 = \langle [4]_{12} \rangle = \{ [0]_{12}, [4]_{12}, [8]_{12} \}$.

$|H_4| = 3 \mid 12$.

- $H_5 = \langle 5[1]_{12} \rangle = \langle d'''[1]_{12} \rangle$, όπου

$d''' = (12, 5) = 1$, άρα:

$H_5 = \langle [1]_{12} \rangle = \mathbb{Z}_{12}$, $|H_5| = 12 | 12$.

Συνεχίζοντας με το ίδιο σκεπτικό έχουμε:

- $H_6 = \langle [6]_{12} \rangle = \{ [0]_{12}, [6]_{12} \}$
- $H_7 = \langle [7]_{12} \rangle = \mathbb{Z}_{12}$
- $H_8 = \langle [8]_{12} \rangle = \{ [0]_{12}, [8]_{12}, [4]_{12} \}$
- $H_9 = \langle [9]_{12} \rangle = \{ [0]_{12}, [9]_{12}, [6]_{12}, [3]_{12} \}$
- $H_{10} = \langle [10]_{12} \rangle = \{ [0]_{12}, [10]_{12}, [8]_{12}, [6]_{12}, [4]_{12}, [2]_{12} \}$
- $H_{11} = \langle [11]_{12} \rangle = \mathbb{Z}_{12}$.

- Για εσάς η $(\mathbb{Z}_8, +)$.

B5. Αφού $|G| = p \geq 2$, υπάρχει $a \in G$ με $a \neq e$. Από Θεώρημα Lagrange,

$$o(a) \mid |G| \Rightarrow o(a) \mid p \xRightarrow[\text{πρώτος}]{p:} o(a) \in \{1, p\}.$$

Αν $o(a) = 1$ τότε $a^1 = e \Rightarrow a = e$, άτοπο.

Άρα, $o(a) = p \Rightarrow |\langle a \rangle| = p = |G|$

$$\xRightarrow{\langle a \rangle \leq G} G = \langle a \rangle : \text{κυκλική.}$$

Έστω $H \trianglelefteq G$. Από Θεώρημα Lagrange,

$$|H| \mid |G| \Rightarrow |H| \mid p \xRightarrow[\text{πρώτος}]{p:} |H| \in \{1, p\}$$

$$\Rightarrow \begin{cases} |H| = 1 \\ \text{ή} \\ |H| = p \end{cases} \Rightarrow \begin{matrix} H = \{e\} \\ \text{ή} \\ H = G \end{matrix}$$

Συνεπώς, $(G, \cdot)$: απλή.

Τέλος, επειδή η $(G, \cdot)$ είναι πεπερασμένη κυκλική τάξης p, από Ταξινόμηση Κυκλικών Ομάδων έπεται: $(G, \cdot) \cong (\mathbb{Z}_p, +)$. ∎

B6. $H = \langle [6]_{15} \rangle = \langle 6[1]_{15} \rangle$, άρα

$|H| = o(6[1]_{15}) = \dfrac{o([1]_{15})}{(o([1]_{15}), 6)}$ (*). Επειδή το $[1]_{15}$ είναι ο γεννήτορας της $(\mathbb{Z}_{15}, +)$ έπεται $o([1]_{15}) = |\mathbb{Z}_{15}| = 15$, άρα:

$$|H| \overset{(*)}{=} \frac{15}{(15,6)} = \frac{15}{3} = 5,$$ οπότε:

$$H = \{0 \cdot [6]_{15}, 1 \cdot [6]_{15}, 2 \cdot [6]_{15}, 3 \cdot [6]_{15}, 4 \cdot [6]_{15}\}$$

$$= \{[0]_{15}, [6]_{15}, [12]_{15}, [18]_{15}, [24]_{15}\}$$

$$= \{[0]_{15}, [3]_{15}, [6]_{15}, [9]_{15}, [12]_{15}\}$$

Άρα: $[\mathbb{Z}_{15} : H] = \dfrac{|\mathbb{Z}_{15}|}{|H|} = \dfrac{15}{5} = 3$,

δηλαδή υπάρχουν τρία διακεκριμένα σύμπλοκα της H στην $\mathbb{Z}_{15}$.

<u>Υπενθύμιση</u>: Για προσθετική ομάδα $(G,+)$ και $H \leq G$ έχουμε:

$\forall x \in G: \quad x+H = \{ x+h \in G \mid h \in H \}$ και:

$\forall x, y \in G: \quad x+H = y+H \iff (-x)+y \in H$

Σε περίπτωση όπου η $(G,+)$ είναι αβελιανή, όπως στην B7, τότε:

$$x+H = y+H \iff (-x)+y \in H \iff y-x \in H$$
$$\iff x-y \in H$$

- $[0]_{15} + H = H$ ✓ $([0]_{15} \in H)$
- $[1]_{15} + H = \{ [1]_{15}+[0]_{15}, [1]_{15}+[3]_{15}, [1]_{15}+[6]_{15}, [1]_{15}+[9]_{15}, [1]_{15}+[12]_{15} \}$

$= \{ [1]_{15}, [4]_{15}, [7]_{15}, [10]_{15}, [13]_{15} \}$

- $[2]_{15} + H = \{ [2]_{15}+[0]_{15}, [2]_{15}+[3]_{15}, [2]_{15}+[6]_{15}, [2]_{15}+[9]_{15}, [2]_{15}+[12]_{15} \}$

$= \{ [2]_{15}, [5]_{15}, [8]_{15}, [11]_{15}, [14]_{15} \}$

- $[3]_{15} + H = H$ (αφού $[3]_{15} \in H$)

- $[4]_{15}+H = [1]_{15}+H$ διότι:

  $[4]_{15}-[1]_{15} = [3]_{15} \in H$

- $[5]_{15}+H = [2]_{15}+H$ διότι:

  $[5]_{15}-[2]_{15} = [3]_{15} \in H$

- $[6]_{15}+H = H$ διότι $[6]_{15} \in H$

- $[7]_{15}+H = [1]_{15}+H$ αφού $[7]_{15}-[1]_{15} = [6]_{15} \in H$

- $[8]_{15}+H = [2]_{15}+H$

  αφού $[8]_{15}-[2]_{15} = [6]_{15} \in H$

- $[9]_{15}+H = [12]_{15}+H = H$ διότι: $[9]_{15}, [12]_{15} \in H$

- $[10]_{15}+H = [1]_{15}+H$

- $[11]_{15}+H = [2]_{15}+H$

- $[13]_{15}+H = [1]_{15}+H$, $[14]_{15}+H = [2]_{15}+H$

Τελικά: $\mathbb{Z}_{15}/H = \{ H, [1]_{15}+H, [2]_{15}+H \}$ ∎

B7: (i) $\Rightarrow$ (ii) Αν G: αβελιανή τότε $G = Z(G)$ και άρα $G/Z(G) = G/G \cong \{e\} = \langle e \rangle$: κυκλική

(ii) $\Rightarrow$ (i) Έστω $G/Z(G)$: κυκλική.
Τότε $G/Z(G) = \langle gZ(G) \rangle$ για κάποιο $g \in G$.
Έστω $x \in G$. Τότε $xZ(G) \in G/Z(G) \Rightarrow$
$\Rightarrow xZ(G) \in \langle gZ(G) \rangle \Rightarrow \exists n \in \mathbb{Z} : xZ(G) = (gZ(G))^n$
$\Rightarrow \exists n \in \mathbb{Z} : xZ(G) = g^n Z(G) \Rightarrow x^{-1} g^n \in Z(G)$
$\xRightarrow{Z(G) \leq G} (x^{-1} g^n)^{-1} \in Z(G) \Rightarrow (g^n)^{-1} x \in Z(G)$.
Δηλαδή, υπάρχει $z(x) \in Z(G)$ ώστε $(g^n)^{-1} x = z(x)$
$\Rightarrow x = g^n z(x)$.
Έτσι, αν y είναι ένα άλλο στοιχείο της G τότε $y = g^m z(y)$ για κάποιο $m \in \mathbb{Z}$ και $z(y) \in Z(G)$.

Τότε: $xy = g^n z(x) g^m z(y) \overset{z(x)\in Z(G)}{=\!=} g^n g^m z(x) z(y)$

$= g^{n+m} z(x) z(y) = g^{m+n} z(x) z(y) = g^m g^n z(x) z(y)$

$\underset{z(y)\in Z(G)}{=} g^m g^n z(y) z(x) \overset{z(y)\in Z(G)}{=\!=} g^m z(y) g^n z(x) = yx.$

Άρα, $xy = yx$, $\forall x, y \in G$ και έτσι η $(G, \cdot)$: αβελιανή.

B8. (i) Έστω μορφισμός $f: \mathbb{Z}_{12} \to \mathbb{Z}_5$.

Από 1º θεώρημα Ισομορφισμών έχουμε:

$$\mathbb{Z}_{12}/\ker(f) \cong \mathrm{Im}(f).$$

Επειδή $\mathrm{Im}(f) \leq \mathbb{Z}_5$, από θεώρημα Lagrange, $|\mathrm{Im}(f)| \mid |\mathbb{Z}_5| \Rightarrow |\mathrm{Im}(f)| \mid 5$

$\underset{\text{πρώτος}}{\overset{5:}{\Longrightarrow}} |\mathrm{Im}(f)| = 1$ ή $|\mathrm{Im}(f)| = 5$

· Αν $|Im(f)| = 1$ τότε $Im(f) = \{[0]_5\}$, άρα $f([x]_{12}) = [0]_5, \forall [x]_{12} \in \mathbb{Z}_{12}$, δηλαδή

f: τετριμμένος.

· Αν $|Im(f)| = 5$ τότε $Im(f) = \mathbb{Z}_5$.

Έτσι: $\mathbb{Z}_{12}/ker(f) \cong \mathbb{Z}_5 \Rightarrow |\mathbb{Z}_{12}/ker(f)| = |\mathbb{Z}_5|$

$$\xRightarrow[\text{Lagrange}]{\text{Θεώρημα}} \frac{|\mathbb{Z}_{12}|}{|Ker(f)|} = 5 \Rightarrow \frac{12}{|Ker(f)|} = 5$$

$$\Rightarrow |Ker(f)| = \frac{12}{5} \notin \mathbb{N}, \text{ άτοπο.}$$

Τελικά, δεν υπάρχει μη-τετριμμένος μορφισμός από την $\mathbb{Z}_{12}$ στην $\mathbb{Z}_5$.

(ii) Έστω μορφισμός $f: \mathbb{Z}_7 \to S_5$.

Από 1ο θεώρημα Ισομορφισμών έχουμε:

$$\mathbb{Z}_7 / \ker(f) \cong \operatorname{Im}(f), \quad \text{άρα:}$$

$$|\mathbb{Z}_7/\ker(f)| = |\operatorname{Im}(f)| \xrightarrow[\text{Lagrange}]{\text{Θεώρημα}} \frac{|\mathbb{Z}_7|}{|\ker(f)|} = |\operatorname{Im}(f)|$$

$$\Rightarrow \frac{7}{\ker(f)} = |\operatorname{Im}(f)| \quad (*)$$

- $\ker(f) \leq \mathbb{Z}_7 \xrightarrow[\text{Lagrange}]{\text{Θεώρημα}} |\ker(f)| \mid |\mathbb{Z}_7|$

$$\Rightarrow |\ker(f)| \mid 7 \xrightarrow[\text{πρώτος}]{7:} |\ker(f)| = 1 \text{ ή } |\ker(f)| = 7$$

(α) Αν $|\ker(f)| = 1$ τότε λόγω της $(*)$:
$|\operatorname{Im}(f)| = 7$. Αλλά, $\operatorname{Im}(f) \leq S_5$, οπότε από θεώρημα Lagrange: $|\operatorname{Im}(f)| \mid |S_5|$

$$\Rightarrow 7 \mid 5! \Rightarrow 7 \mid 120, \text{ άτοπο.}$$

• Αν $|Ker(f)| = 7$ τότε λόγω $(*)$

$|Im(f)| = 1 \rightarrow Im(f) = \{Id\}$ και

τότε $f([x]_7) = Id$, $\forall [x]_7 \in \mathbb{Z}_7$, δηλαδή

f τετριμμένος.

Τελικά, δεν υπάρχει μη-τετριμμένος μορφισμός

$f: \mathbb{Z}_7 \rightarrow S_5$.

(iii) Θεωρούμε την απεικόνιση

$f: (\mathbb{Z} \times \mathbb{Z}, +) \rightarrow (\mathbb{Z}_2 \times \mathbb{Z}, +)$ με

$f(n, m) = ([n]_2, m-n)$

• Για κάθε $(n, m), (n', m') \in \mathbb{Z} \times \mathbb{Z}$ έχουμε

$$f((n,m)+(n',m')) = f(n+n', m+m')$$
$$= ([n+n']_2, m+m' - (n+n'))$$
$$= ([n]_2 + [n']_2, (m-n) + (m'-n'))$$

$= ([n]_2, m-n) + ([n']_2, m'-n') = f(n,m) + f(n',m')$.

Άρα η f είναι μορφισμός ομάδων.

• Η f είναι επί του $\mathbb{Z}_2 \times \mathbb{Z}$: Έστω

$([a]_2, x) \in \mathbb{Z}_2 \times \mathbb{Z}$. Αν $[a]_2 = [0]_2$ τότε

για το $(0,x) \in \mathbb{Z} \times \mathbb{Z}$ έχουμε:

$$f(0,x) = ([0]_2, x-0) = ([a]_2, x)$$

Αν $[a]_2 = [1]_2$ τότε για το $(1, x+1) \in \mathbb{Z} \times \mathbb{Z}$

έχουμε: $f(1, x+1) = ([1]_2, x+1-1) = ([a]_2, x)$.

• $\mathrm{Ker}(f) = \{ (n,m) \in \mathbb{Z} \times \mathbb{Z} \mid f(n,m) = ([0]_2, 0) \}$

$= \{ (n,m) \in \mathbb{Z} \times \mathbb{Z} \mid ([n]_2, m-n) = ([0]_2, 0) \}$

$= \{ (n,m) \in \mathbb{Z} \times \mathbb{Z} \mid [n]_2 = [0]_2 \text{ και } m-n = 0 \}$

$= \{ (n,m) \in \mathbb{Z} \times \mathbb{Z} \mid 2 \mid n \text{ και } m = n \}$

$= \{ (n,n) \in \mathbb{Z} \times \mathbb{Z} \mid 2 | n \}$

$= \{ (2\kappa, 2\kappa) \in \mathbb{Z} \times \mathbb{Z} \mid \kappa \in \mathbb{Z} \}$

$= \{ \kappa(2,2) \in \mathbb{Z} \times \mathbb{Z} \mid \kappa \in \mathbb{Z} \} = \langle (2,2) \rangle.$

Από το 1ο Θεώρημα Ισομορφισμών έχουμε:

$$\mathbb{Z} \times \mathbb{Z} / \ker(f) \cong \operatorname{Im}(f)$$

$$\xrightarrow[\text{επί}]{f:} \boxed{\mathbb{Z} \times \mathbb{Z} / \langle (2,2) \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}}$$

B9. (i) $HK \leq G$, $HK = \{hk \in G \mid h \in H, k \in K\}$.

(α) $\underline{\underline{HK \leq G}}$: Επειδή $H, K \leq G$ έχουμε ότι $e \in H$, $e \in K$ και άρα $e = e \cdot e \in HK$. Έστω τώρα $x, y \in HK$ και θα δείξουμε ότι $xy^{-1} \in HK$.

$$\left.\begin{array}{l} \cdot\ x \in HK \\ \cdot\ y \in HK \end{array}\right\} \Rightarrow \begin{array}{l} \exists h_1 \in H, \exists k_1 \in K:\ x = h_1 k_1 \\ \exists h_2 \in H, \exists k_2 \in K:\ y = h_2 k_2 \end{array}$$

Τότε $xy^{-1} = h_1 k_1 (h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} =$

$= h_1 k_1 h_2^{-1} \underbrace{h_2 k_2^{-1} h_2^{-1}}_{u'} = h_1 k_1 h_2^{-1} u'$, όπου

$u' = h_2 k_2^{-1} h_2^{-1} = (h_2^{-1})^{-1} \underbrace{k_2^{-1}}_{\in K} h_2^{-1} \in K$ διότι $K \trianglelefteq G$.

Παρόμοια, $h_1 k_1 k_2^{-1} u' = h_1 h_2^{-1} h_2 k_1 h_2^{-1} u'$

$= h_1 h_2^{-1} u'' u'$, όπου $u'' = h_2 \underbrace{k_1}_{\in K} h_2^{-1} \in K$ αφού $K \trianglelefteq G$. Τελικά, επειδή $h_1 h_2^{-1} \in H$ και $u'' u' \in K$ έπεται: $xy^{-1} \in HK$.

(β) $K \trianglelefteq HK$: Αρχικά $K \subseteq HK$ διότι:

$\forall k \in K: \ k = ek \in HK$.

Για $x \in K$ και $hk \in HK$ έχουμε:

$$(hk)^{-1} x \, hk = k^{-1} h^{-1} x \, hk = k^{-1} \underbrace{(h^{-1} x h)}_{\in K} k \in K.$$

(διότι $K \trianglelefteq G$)

Άρα, $K \trianglelefteq HK$.

(ii) Ορίζουμε $f: H \to HK/K$ με $f(x) = xK$

(σκέψου ότι: $H \subseteq HK$, άρα: $x \in H \Rightarrow x \in HK$)

• $\forall x, y \in H: \ f(xy) = (xy)K = xK \cdot yK = f(x) f(y)$,

άρα η f είναι μορφισμός ομάδων

• $\operatorname{Im}(f) = HK/K$: Πράγματι, έστω $y \in HK/K$

Τότε $y = zK$ για κάποιο $z \in HK$.

Εφ' όσον $z \in HK$, έχουμε $z = hk$ για κάποιους $h \in H$, $k \in K$. Τότε $f(h) = hK = hK \cdot eK =$
$hK \cdot kK = (hk)K = zK = y$.

$(eK = kK$ διότι $k \in K)$.

. $Ker(f) = \{x \in H \mid f(x) = e_{HK/K}\} =$
$= \{x \in H \mid xK = K\} = \{x \in H \mid x \in K\} = H \cap K$.

Από 1ο Θεώρημα Ισομορφισμών Ομάδων,

$$H/_{Ker(f)} \cong Im(f) \iff H/_{H \cap K} \cong HK/K$$

■

B10. Θεωρούμε την απεικόνιση
$f : G/K \to G/H$ με $f(xK) = xH$

. Σχόλιο: Επειδή $H, K \trianglelefteq G$, ορίζονται οι ομάδες πηλίκα G/K και G/H, αντίστοιχα, με πράξεις:

- $xK \cdot yK = (xy)K$, $\forall xK, yK \in G/K$
- $uH \cdot vH = (uv)H$, $\forall uH, vH \in G/H$.

(1) __f: καλά ορισμένη__ : Έστω $xK = yK \in G/K$ και θα αποδείξουμε ότι $f(xK) = f(yK)$, δηλαδή $xH = yH$. Πράγματι,

$$xK = yK \Rightarrow x^{-1}y \in K \xrightarrow{K \leq H} x^{-1}y \in H \Rightarrow xH = yH.$$

(2) __f: μορφισμός ομάδων__ : Για κάθε $xK, yK \in G/K$ ισχύει: $f(xK \cdot yK) = f((xy)K) = (xy)H = xH \cdot yH = f(xK) f(yK)$

(3) __f: επί του G/H__, δηλαδή: $Im(f) = G/H$.
Έστω $\tilde{y} \in G/H$. Τότε $\tilde{y} = xH$ για κάποιο $x \in G$. Άρα $xK \in G/K$ και: $f(xK) = xH = \tilde{y}$

(4) Θα υπολογίσουμε τώρα τον πυρήνα $Ker(f)$ της f.

$$\cdot \ \mathrm{Ker}(f) = \{ xK \in G/K \mid f(xK) = e_{G/H} \} =$$

$$= \{ xK \in G/K \mid xH = H \}$$

$$= \{ xK \in G/K \mid x \in H \}$$

$$= H/K \trianglelefteq G/K.$$

Από το 1º θεώρημα Ισομορφισμών Ομάδων, $G/K \big/ \mathrm{Ker}(f) \cong \mathrm{Im}(f)$

άρα: $\boxed{G/K \big/ H/K \cong G/H}$

■