ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ I

Ακαδημαϊκο Ετος 2023-2024

Επιλυση Ασκησεων - Φυλλαδιο 7

Διδασκων: Α. Μπεληγιάννης

ΙΣΤΟΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ

http://users.uoi.gr/abeligia/AlgebraicStructuresI/ASI2024/ASI2024.html

Παρασκευή 26 Απριλίου 2024

Άσκηση 1. *Έστω ότι G είναι μια κυκλική ομάδα. Να δεχθεί ότι μια απεικόνιση $f\colon G \longrightarrow G$ είναι ομομορφισμός ομάδων αν και μόνον αν υπάρχει ακέραιος $k \in \mathbb{Z}$ έτσι ώστε: $f(x) = x^k$, $\forall x \in G$.*

Είναι ο ακέραιος k μοναδικός;

Λύση. Επειδή η ομάδα G είναι κυκλική, υπάρχει $a \in G$ έτσι ώστε $G = \langle a \rangle$.

(1) Έστω ότι $f\colon G \longrightarrow G$ είναι ένας ομομορφισμός ομάδων. Τότε $f(a) \in \langle a \rangle = G$ και επομένως υπάρχει $k \in \mathbb{Z}$ έτσι ώστε: $f(a) = a^k$.

Αν $x \in G$, τότε υπάρχει $r \in \mathbb{Z}$ έτσι ώστε $x = a^r$ και τότε:

$$f(x) = f(a^r) = f(a)^r = (a^k)^r = a^{kr} = (a^r)^k = x^k$$

Άρα ο ομομορφισμός f είναι της μορφής $f(x) = x^k$, $\forall x \in G$.

(2) Έστω $k \in \mathbb{Z}$ ένας ακέραιος και θεωρούμε την απεικόνιση $f\colon G \longrightarrow G$, $f(x) = x^k$. Τότε, χρησιμοποιώντας ότι η G, ως κυκλική, είναι αβελιανή, θα έχουμε:

$$f(x \cdot y) = (x \cdot y)^k = x^k \cdot y^k = f(x) \cdot f(y)$$

και επομένως η απεικόνιση f είναι ομομορφισμός ομάδων.

Υποθέτουμε τώρα ότι $f\colon G \longrightarrow G$ είναι ένας ομομορφισμός ομάδων, και τότε από τα παραπάνω υπάρχει ακέραιος $k \in \mathbb{Z}$ έτυσι ώστε: $f(x) = x^k$, $\forall x \in G$.

• Έστω ότι η κυκλική ομάδα $G = \langle a \rangle$ είναι άπειρη, ισοδύναμα ο γεννήτορας a έχει άπειρή τάξη. Αν υπάρχουν ακέραιοι $k, l \in \mathbb{Z}$ έτσι ώστε: $f(x) = x^k = x^l$, $\forall x \in G$, τότε ιδιαίτερα θα έχουμε $f(a) = a^k = a^l$ και επομένως $a^{k-l} = e$. Επειδή το στοιχείο a έχει άπειρη τάξη, θα έχουμε $k - l = 0$ και άρα $k = l$, δηλαδή το στοιχείο k είναι μοναδικό.

• Έστω ότι η κυκλική ομάδα $G = \langle a \rangle$ είναι πεπερασμένη με τάξη n , ισοδύναμα ο γεννήτορας a έχει τάξη $\mathsf{o}(a) = n$. Αν υπάρχουν ακέραιοι $k, l \in \mathbb{Z}$ έτσι ώστε: $f(x) = x^k = x^l$, $\forall x \in G$, τότε ιδιαίτερα θα έχουμε $f(a) = a^k = a^l$ και επομένως $a^{k-l} = e$. Τότε $n = \mathsf{o}(a) \mid k - l$ και άρα $k \equiv l \,(\mathrm{mod}\, n)$. Αντίστροφα, αν $k \equiv l \,(\mathrm{mod}\, n)$, τότε $n \mid k - l$ και άρα $k - l = nr$ για κάποιον ακέραιο r. Έτσι $k = l + rn$ και, επειδή $x^n = e$, θα έχουμε:

$$f(x) = x^k = x^{l+rn} = x^l \cdot x^{rn} = x^l (x^n)^r = x^l \cdot e^r = x^l \cdot e = x^l$$

Άρα το στοιχείο k είναι μοναδικό $\mathrm{mod}\, n$, όπου $n = |G|$. ∎

Άσκηση 2. *Έστω* $\mathsf{GL}(n,\mathbb{R})$ *η ομάδα των αντιστρέψιμων* $n \times n$ *πινάκων πραγματικών αριθμών. Αν* $\mathsf{SL}(n,\mathbb{R}) = \big\{A \in \mathsf{GL}(n,\mathbb{R}) \mid \mathsf{det}(A) = 1\big\}$, *να δείξετε ότι το σύνολο* $\mathsf{SL}(n,\mathbb{R})$ *είναι μια κανονική υποομάδα της* $\mathsf{GL}(n,\mathbb{R})$, *και ακολούθως να περιγράψετε την ομάδα πηλίκο:*

$$\mathsf{GL}(n,\mathbb{R})\big/\mathsf{SL}(n,\mathbb{R})$$

Λύση. Ορίζουμε απεικόνιση

$$f:\ \mathsf{GL}(n,\mathbb{R}) \longrightarrow \mathbb{R}^*, \quad f(A) = \mathsf{det}(A)$$

Επειδή η απεικόνιση ορίζουσας ικανοποιεί τη σχέση $\mathsf{det}(A \cdot B) = \mathsf{det}(A) \cdot \mathsf{det}(B)$, έπεται ότι η απεικόνιση f είναι ένας ομομορφισμός ομάδων από την $\mathsf{GL}(n,\mathbb{R})$ στην πολλαπλασιαστική ομάδα $\mathbb{R}^*$ των μη-μηδενικών πραγματικών αριθμών.

Ο ομομορφισμός f είναι επιμορφισμός, διότι για κάθε μη-μηδενικό πραγματικό αριθμό x, έχουμε $f(A) = \mathsf{det}(A) = x$, όπου A είναι ο διαγώνιος πίνακας με στοιχεία στην διαγώνιο παντού 1, εκτός από την θέση (11), όπου έχουμε το στοιχείο x.

Προφανώς $\mathsf{Ker}(f) = \mathsf{SL}(n,\mathbb{R})$, και άρα η ομάδα $\mathsf{SL}(n,\mathbb{R})$ είναι μια κανονική υποομάδα της $\mathsf{GL}(n,\mathbb{R})$.

Τέλος από το Πρώτο Θεώρημα Ισομορφισμών, θα έχουμε έναν ισομορφισμό:

$$\mathsf{GL}(n,\mathbb{R})\big/\mathsf{SL}(n,\mathbb{R}) \ \xrightarrow{\cong}\ \mathbb{R}^* \qquad \blacksquare$$

Άσκηση 3. *Θεωρούμε την πολλαπλασιαστική ομάδα* $\mathsf{GL}(2,\mathbb{R})$ *των αντιστρέψιμων πινάκων με στοιχεία πραγματικούς αριθμούς.*

(1) *Να δείξετε ότι το υποσύνολο*

$$G = \big\{\left(\begin{smallmatrix} a & b \\ 0 & d\end{smallmatrix}\right) \ \in\ \mathsf{M}_{2\times 2}(\mathbb{R}) \ \mid\ ad \neq 0\big\}$$

είναι υποομάδα της $\mathsf{GL}(2,\mathbb{R})$.

(2) *Να δείξετε ότι το υποσύνολο*

$$H = \big\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1\end{smallmatrix}\right) \ \in\ \mathsf{M}_{2\times 2}(\mathbb{R}) \ \mid\ b \in \mathbb{R}\big\}$$

είναι κανονική (ορθόθετη) υποομάδα της G.

(3) *Να κατασκευάσετε έναν ισομορφισμό*

$$H \ \cong\ \mathbb{R}$$

(4) *Να δειχθεί ότι η ομάδα-πηλίκο* G/H *είναι αβελιανή.*

Λύση. (1) Έστω $\left(\begin{smallmatrix} a & b \\ 0 & d\end{smallmatrix}\right), \left(\begin{smallmatrix} x & y \\ 0 & z\end{smallmatrix}\right) \in G$. Τότε

$$\begin{pmatrix} a & b \\ 0 & d\end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & z\end{pmatrix} = \begin{pmatrix} ax & ay + bz \\ 0 & dz\end{pmatrix} \in G$$

διότι $axdz \neq 0$ αφού $ad \neq 0$ και $xz \neq 0$. Άρα το σύνολο G είναι κλειστό ως προς τη πράξη της $\mathsf{GL}_2(\mathbb{R})$. Προφανώς το ουδέτερο στοιχείο $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1\end{smallmatrix}\right)$ της $\mathsf{GL}_2(\mathbb{R})$ ανήκει και στη G. Έστω $\left(\begin{smallmatrix} a & b \\ 0 & d\end{smallmatrix}\right) \in G$. Τότε

$$\begin{pmatrix} a & b \\ 0 & d\end{pmatrix} \cdot \begin{pmatrix} \frac{1}{a} & \frac{-b}{da} \\ 0 & \frac{1}{d}\end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix} \implies \begin{pmatrix} a & b \\ 0 & d\end{pmatrix}^{-1} = \begin{pmatrix} \frac{1}{a} & \frac{-b}{da} \\ 0 & \frac{1}{d}\end{pmatrix} \in G$$

διότι $ad \neq 0$. Άρα $G \leq \mathsf{GL}(2,\mathbb{R})$.

(2) Έστω $\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) \in G$. Τότε

$$\begin{aligned}
\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} &= \begin{pmatrix} \frac{1}{x} & \frac{-y}{xz} \\ 0 & \frac{1}{z} \end{pmatrix} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \\
&= \begin{pmatrix} \frac{1}{x} & \frac{bz-y}{xz} \\ 0 & \frac{1}{z} \end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \\
&= \begin{pmatrix} 1 & \frac{bz}{x} \\ 0 & 1 \end{pmatrix} \in H
\end{aligned}$$

Συνεπώς $H \trianglelefteq \mathsf{GL}(2,\mathbb{R})$.

(3) Ορίζουμε απεικόνιση

$$g: H \longrightarrow \mathbb{R}, \qquad g\big(\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)\big) = b$$

Η απεικόνιση g είναι ομομορφισμός ομάδων, διότι:

$$g\big(\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} 1 & b' \\ 0 & 1 \end{smallmatrix}\right)\big) = g\big(\left(\begin{smallmatrix} 1 & b'+b \\ 0 & 1 \end{smallmatrix}\right)\big) = b' + b = b + b' = g\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) + g\left(\begin{smallmatrix} 1 & b' \\ 0 & 1 \end{smallmatrix}\right)$$

και φανερά ο ομομορφισμός g είναι επιμορφισμός. Τέλος ο ομομορφισμός g είναι μονομορφισμός διότι:

$$\begin{aligned}
\mathsf{Ker}(g) &= \big\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in H \mid g\big(\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)\big) = 0\big\} \\
&= \big\{\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in H \mid b = 0\big)\big\} \\
&= \big\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\big\} \\
&= \big\{I_2\big\}
\end{aligned}$$

Άρα η απεικόνιση g είναι ισομορφισμός.

(4) Η ομάδα πηλίκο G/H είναι αβελιανή αν και μόνο αν

$$\forall A, B \in G\colon AH \cdot BH = BH \cdot AH \iff (AB)H = (BA)H \iff AB \cdot (BA)^{-1} \in H$$

Έστω $A = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right) \in G$. Έχουμε:

$$\begin{cases}
AB = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay+bz \\ 0 & dz \end{pmatrix} \\[2ex]
BA = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} xa & xb+yd \\ 0 & zd \end{pmatrix} \\[2ex]
(BA)^{-1} = \begin{pmatrix} \frac{1}{xa} & \frac{-xb-yd}{xazd} \\ 0 & \frac{1}{zd} \end{pmatrix}
\end{cases}$$

και τότε

$$(AB) \cdot (BA)^{-1} = \begin{pmatrix} ax & ay+bz \\ 0 & dz \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{xa} & \frac{-xb-yd}{xazd} \\ 0 & \frac{1}{zd} \end{pmatrix} = \begin{pmatrix} 1 & \frac{-ax^2b-axyd+xa^2y+xabz}{xazd} \\ 0 & 1 \end{pmatrix} \in H$$

Άρα η ομάδα πηλίκο G/H είναι αβελιανή.

2ος Τρόπος: Θα δείξουμε τα (2) και (4) με χρήση του Πρώτου Θεωρήματος Ισομορφισμών:

Έχοντας δείξει ότι η G είναι μια υποομάδα της $\mathsf{GL}(2,\mathbb{R})$, θεωρούμε την ομάδα ευθύ γινόμενο $\mathbb{R}^* \times \mathbb{R}^*$ της πολλαπλασιαστικής ομάδας $(\mathbb{R}^*, \cdot)$ των μη-μηδενικών πραγματικών αριθμών, και ορίζουμε μια απεικόνιση

$$\varphi: \ G \longrightarrow \mathbb{R}^* \times \mathbb{R}^*, \quad \varphi(A) = \varphi\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) = (a,d)$$

Η απεικόνιση φ είναι ομομορφισμός ομάδων, διότι αν $A = \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$ και $B = \left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right)$ είναι δύο στοιχεία της G, θα έχουμε:

$$\varphi(A{\cdot}B) = \varphi\big(\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right){\cdot}\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right)\big) = \varphi\big(\left(\begin{smallmatrix} ax & ay+bz \\ 0 & dz \end{smallmatrix}\right)\big) = (ax, dz) = (a,d){\cdot}(x,z) = \varphi\big(\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\big){\cdot}\varphi\big(\left(\begin{smallmatrix} x & y \\ 0 & z \end{smallmatrix}\right)\big) = \varphi(A){\cdot}\varphi(B)$$

Επιπλέον η φ είναι επιμορφισμός, διότι:

$$\forall (a,d) \in \mathbb{R}^* \times \mathbb{R}^*, \quad A = \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \in G \quad \text{και} \quad \varphi(A) = \varphi\big(((\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) = (a,d)$$

Υπολογίζουμε τον πυρήνα του επιμορφισμού φ:

$$\mathsf{Ker}(\varphi) = \big\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G \mid \varphi\big(\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)\big) = (1,1)\big\} = \big\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in G \mid (a,d)) = (1,1)\big\} = \big\{ \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in G \mid b \in \mathbb{R}\big\} = H$$

Έτσι η απεικόνιση φ είναι ένας επιμορφισμός ομάδων με πυρήνα την υποομάδα H.

(2) Επειδή ο πυρήνας ενός ομομορφισμού είναι πάντα κανονική υποομάδα, έπεται ότι το σύνολο H είναι μια κανονική υποομάδα της G.

(4) Από το Πρώτο Θεώρημα Ισομορφισμών, θα έχουμε ότι η απεικόνιση φ επάγει έναν ισομορφισμό ομάδων

$$\widetilde{\varphi}: \ G/\,\mathsf{Ker}(\varphi) = G/H \ \xrightarrow{\cong} \ \mathbb{R}^* \times \mathbb{R}^*, \quad \widetilde{\varphi}(AH) = \varphi(A)$$

Επειδή η ομάδα $\mathbb{R}^* \times \mathbb{R}^*$ είναι αβελιανή (ως ευθύ γινόμενο αβελιανών ομάδων), έπεται ότι η ομάδα πηλίκο G/H είναι αβελιανή (ως ισόμορφη με μια αβελιανή ομάδα). ∎

Άσκηση 4. *Θεωρούμε το σύνολο απεικονίσεων*

$$G = \big\{\tau_{a,b}: \ \mathbb{R} \longrightarrow \mathbb{R} \ \mid \ \tau_{a,b}(x) = ax + b, \quad a,b \in \mathbb{R}, \ \ a \neq 0\big\}$$

το οποίο είναι ομάδα με πράξη την σύνθεση απεικονίσεων.

(1) *Να δείξετε ότι το υποσύνολο*

$$H = \big\{\tau_{1,b} \in G \ \mid \ b \in \mathbb{R}\big\}$$

είναι κανονική (ορθόθετη) υποομάδα της G.

(2) *Να προσδιορίσετε την ομάδα-πηλίκο G/H.*

Λύση. (1) Για κάθε $a,b,c,d,x \in \mathbb{R}$ με $a,c \neq 0$ έχουμε:

$$\begin{aligned} (\tau_{a,b} \circ \tau_{a^{-1},-a^{-1}b})(x) \quad &= \quad \tau_{a,b}\big(\tau_{a^{-1},-a^{-1}b}(x)\big) \quad = \quad \tau_{a,b}\big(\frac{x}{a} - \frac{b}{a}\big) \quad = \quad a\big(\frac{x}{a} - \frac{b}{a}\big) + b = x \\ \Longrightarrow \quad &\tau_{a,b} \circ \tau_{a^{-1},-a^{-1}b} = \mathrm{Id}_{\mathbb{R}} \end{aligned}$$

Όμοια δείχνουμε ότι

$$\tau_{a^{-1},-a^{-1}b} \circ \tau_{a,b} = \mathrm{Id}_{\mathbb{R}}$$

και άρα

$$(\tau_{a,b})^{-1} = \tau_{a^{-1},-a^{-1}b} \tag{1}$$

Ιδιαίτερα βλέπουμε ότι το σύνολο G αποτελείται από 1-1 και επί απεικονίσεις από το $\mathbb{R}$ στο $\mathbb{R}$, και άρα είναι υποσύνολο της συμμετρικής ομάδας $S(\mathbb{R})$ επί του συνόλου $\mathbb{R}$. Παρατηρούμε ότι η ταυτοτική απεικόνιση $\mathrm{Id}_{\mathbb{R}}\colon \mathbb{R} \longrightarrow \mathbb{R}$ ανήκει στο σύνολο G διότι $\mathrm{Id}_{\mathbb{R}} = \tau_{1,0}$.

Επίσης έχουμε

$$\begin{aligned}(\tau_{a,b}\circ\tau_{c,d})(x) &= \tau_{a,b}\big(\tau_{c,d}(x)\big) &=& \ \tau_{a,b}(cx+d)\\ &= a(cx+d)+b &=& \ acx+(ad+b)\\ &= \tau_{ac,ad+b}(x)\end{aligned}$$

Συνεπώς έπεται ότι

$$\tau_{a,b}\circ\tau_{c,d}=\tau_{ac,ad+b} \tag{2}$$

Να σημειώσουμε ότι επειδή η ταυτοτική απεικόνιση : $\mathbb{R}\longrightarrow\mathbb{R}$ ανήκει στο υποσύνολο G, οι σχέσεις (1) και (2) δείχνουν ότι το σύνολο G είναι υποομάδα της συμμετρικής ομάδας $S(\mathbb{R})$ (της οποίας η πράξη είναι η σύνθεση απεικονίσεων). Επομένως το σύνολο G εφοδιασμένο με τη πράξη της σύνθεσης είναι ομάδα.

Για κάθε $\tau_{a,b}\in G$ έχουμε:

$$\begin{aligned}(\tau_{a,b}^{-1}\circ\tau_{1,r}\circ\tau_{a,b})(x) &= \tau_{a,b}^{-1}\big(\tau_{1,r}(ax+b)\big)\\ &= \tau_{a,b}^{-1}(ax+b+r)\\ &= \tau_{a^{-1},-a^{-1}b}(ax+(b+r))\\ &= a^{-1}(ax+b+r)-a^{-1}b\\ &= x+a^{-1}b+a^{-1}r-a^{-1}b\\ &= x+a^{-1}r\\ &= \tau_{1,a^{-1}r}(x)\end{aligned}$$

Άρα δείξαμε ότι

$$\tau_{a,b}^{-1}\circ\tau_{1,r}\circ\tau_{a,b}=\tau_{1,a^{-1}r} \quad\Longrightarrow\quad \tau_{a,b}^{-1}\circ\tau_{1,r}\circ\tau_{a,b}\ \in\ H, \qquad \forall\tau_{a,b}\in G$$

Επομένως έχουμε ότι η H είναι κανονική υποομάδα της G.

(2) Ορίζουμε την απεικόνιση

$$f:\ G/H\longrightarrow\mathbb{R}^*, \qquad \tau_{a,b}H\ \longmapsto\ f\big(\tau_{a,b}H\big)=a$$

Έχουμε

- Καλά ορισμένη: Έστω $\tau_{a,b}H=\tau_{c,d}H$. Τότε έχουμε

$$\begin{aligned}\tau_{a,b}\circ\tau_{c,d}^{-1}\in H \ \Longrightarrow\ \tau_{a,b}\circ\tau_{c^{-1},-c^{-1}d}\in H \ \Longrightarrow\ \tau_{ac^{-1},-ac^{-1}d+b}\in H &\ \Longrightarrow\ ac^{-1}=1\\ &\ \Longrightarrow\ a=c\\ &\ \Longrightarrow\ f\big(\tau_{a,b}H\big)=f\big(\tau_{c,d}H\big)\end{aligned}$$

Άρα η απεικόνιση f είναι καλά ορισμένη.

- Ομομορφισμός Ομάδων: Έστω $\tau_{a,b}H,\tau_{c,d}H\in G/H$. Τότε

$$f\big((\tau_{a,b}H)(\tau_{c,d}H)\big)=f\big(\tau_{a,b}\circ\tau_{c,d}H\big)=f\big(\tau_{ac,ad+b}H\big)=ac=f\big(\tau_{a,b}H\big)f\big(\tau_{c,d}H\big)$$

και άρα η f είναι ομομορφισμός ομάδων.

- Ένα προς ένα: Έστω $\tau_{a,b}H\in G/H$ έτσι ώστε $f\big(\tau_{a,b}H\big)=1$. Τότε

$$a=1\ \Longrightarrow\ \tau_{a,b}H=\tau_{1,b}H\ \Longrightarrow\ \tau_{a,b}H=H$$

και άρα ο πυρήνας της f είναι ο τετριμμένος. Συνεπώς η f είναι 1-1.

- Επί: Για κάθε $a\in\mathbb{R}^*$ υπάρχει το στοιχείο $\tau_{a,b}H\in G/H$ και από τον ορισμό της f έχουμε ότι $f\big(\tau_{a,b}H\big)=a$. Επομένως η f είναι επί.

Συνεπώς έχουμε ότι η απεικόνιση f είναι ισομορφισμός, και άρα:

$$G/H \ \simeq \ \mathbb{R}^*$$

2ος Τρόπος: Θα δείξουμε τα (1) και (2) με χρήση του Πρώτου Θεωρήματος Ισομορφισμών:

Δείχνουμε πρώτα ότι το σύνολο G εφοδιασμένο με την σύνθεση απεικονίσεων είναι ομάδα. Θεωρούμε την πολλαπλασιαστική ομάδα $(\mathbb{R}^*, \cdot)$ των μη-μηδενικών πραγματικών αριθμών, και ορίζουμε απεικόνιση

$$\phi : \ G \longrightarrow \mathbb{R}^*, \quad \phi(\tau_{a,b}) = a$$

Τότε η απεικόνιση ϕ είναι ένας ομομορφισμός ομάδων, διότι αν $\tau_{a,b}$ και $\tau_{c,d}$ είναι δύο στοιχεία της G, θα έχουμε:

$$\phi\big(\tau_{a,b} \circ \tau_{c,d}\big) = \phi\big(\tau_{ac,ad+b}\big) = ac = \phi(\tau_{a,b}) \cdot \phi(\tau_{c,d})$$

Επιπλέον η ϕ είναι επιμορφισμός, διότι:

$$\forall a \in \mathbb{R}^*, \quad \tau_{a,0} \in G \quad \text{και} \quad \phi(\tau_{a,0}) = a$$

Υπολογίζουμε τον πυρήνα του επιμορφισμού ϕ:

$$\mathsf{Ker}(\phi) = \big\{\tau_{a,b} \ \in \ G \mid \phi(\tau_{a,b}) = 1\big\} = \big\{\tau_{a,b} \ \in \ G \mid a = 1\big\} = \big\{\tau_{1,b} \ \in \ G \mid b \in \mathbb{R}\big\} = H$$

Έτσι η απεικόνιση ϕ είναι ένας επιμορφισμός ομάδων με πυρήνα την υποομάδα H.

(1) Επειδή ο πυρήνας ενός ομομορφισμού είναι πάντα κανονική υποομάδα, έπεται ότι το σύνολο H είναι μια κανονική υποομάδα της G.

(2) Από το Πρώτο Θεώρημα Ισομορφισμών, θα έχουμε ότι η απεικόνιση ϕ επάγει έναν ισομορφισμό ομάδων[1]

$$\widetilde{\phi} : \ G/\,\mathsf{Ker}(\phi) = G/H \ \xrightarrow{\cong} \ \mathbb{R}^*, \quad \widetilde{\phi}(\tau_{a,b}H) = \phi(\tau_{a,b}) = a$$

Επειδή η ομάδα $\mathbb{R}^*$ είνα αβελιανή (ως ευθύ γινόμενο αβελιανών ομάδων), έπεται ότι η ομάδα πηλίκο G/H είναι αβελιανή (ως ισόμορφη με μια αβελιανή ομάδα). ■

Άσκηση 5. *Έστω η πολλαπλασιαστική ομάδα $\mathbb{C}^*$ των μη-μηδενικών μιγαδικών αριθμών.*

(1) *Αν $\mathsf{T} = \{z \in \mathbb{C} \mid |z| = 1\} \leq \mathbb{C}^*$ είναι η ομάδα του κύκλου, να δειχθεί ότι η ομάδα-πηλίκο $\mathbb{C}^*/\mathsf{T}$ είναι ισόμορφη με την πολλαπλασιαστική ομάδα $\mathbb{R}^+$ των θετικών πραγματικών αριθμών.*

(2) *Να δείξετε ότι το σύνολο*

$$G = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \ \in \ \mathsf{M}_{2\times 2}(\mathbb{R}) \ \mid \ (a,b) \neq (0,0) \right\}$$

εφοδιασμένο με την πράξη πολλαπλασιασμού πινάκων είναι ομάδα και υπάρχει ισομορφισμός:

$$G \ \xrightarrow{\cong} \ \mathbb{C}^*$$

Λύση. (1) Ορίζουμε την απεικόνιση

$$f : \ \mathbb{C}^*/\mathsf{T} \longrightarrow \mathbb{R}^+, \ \ z\mathsf{T} \ \mapsto \ f(z\mathsf{T}) = |z|$$

Έχουμε

- <u>Καλά ορισμένη</u>: Έστω $z\mathsf{T} = w\mathsf{T}$. Τότε έχουμε

$$z^{-1}w \in \mathsf{T} \ \Longrightarrow \ |z^{-1}w| = 1 \ \Longrightarrow \ |z^{-1}| \cdot |w| = 1 \ \Longrightarrow \ |z| = |w| \ \Longrightarrow \ f(z\mathsf{T}) = f(w\mathsf{T})$$

Άρα η απεικόνιση f είναι καλά ορισμένη.

[1] Ο ισομορφισμός $\widetilde{\phi}$ συμπίπτει με τον ισομορφισμό f.

- <u>Ομομορφισμός Ομάδων</u>: Έστω $z\mathsf{T}, w\mathsf{T} \in \mathbb{C}^*/\mathsf{T}$. Τότε
$$f\big((z\mathsf{T})(w\mathsf{T})\big) \;=\; f(zw\mathsf{T}) \;=\; |zw| \;=\; |z|\cdot|w| \;=\; f(z\mathsf{T})f(w\mathsf{T})$$
και άρα η f είναι ομομορφισμός ομάδων.

- <u>Ένα προς ένα</u>: Έστω $z\mathsf{T} \in \mathsf{Ker}\, f$. Τότε
$$f(z\mathsf{T}) = 1 \quad\Longrightarrow\quad |z| = 1 \quad\Longrightarrow\quad z \in \mathsf{T} \quad\Longrightarrow\quad z\mathsf{T} = \mathsf{T}$$
Συνεπώς η f είναι ένα προς ένα διότι πυρήνας $\mathsf{Ker}\, f$ της f αποτελείται μόνο από το ουδέτερο στοιχείο T της ομάδας $\mathbb{C}^*/\mathsf{T}$.

- <u>Επί</u>: Για κάθε $r \in \mathbb{R}^+$ το στοιχείο $r\mathsf{T} \in \mathbb{C}^*/\mathsf{T}$ και $f(r\mathsf{T}) = |r| = r$. Επομένως η f είναι επί.

Άρα δείξαμε πράγματι ότι υπάρχει ένας ισομορφισμός:
$$\mathbb{C}^*/\mathsf{T} \;\simeq\; \mathbb{R}^+$$

2ος Τρόπος: Όπως και στις Ασκήσεις 1, 2, Θα δείξουμε τον ισχυρισμό με χρήση του Πρώτου Θεωρήματος Ισομορφισμών:

Ορίζουμε απεικόνιση
$$\varphi : \mathbb{C}^* \longrightarrow \mathbb{R}^+, \quad \varphi(z) = |z|$$
η οποία είναι ένας ομομορφισμός ομάδων, διότι αν $z, w \in \mathbb{C}^*$,θα έχουμε:
$$\varphi(z\cdot w) = |z\cdot w| = |z|\cdot|w| = \varphi(z)\cdot\varphi(w)$$
Επιπλέον ο ομομορφισμός φ είναι επιμορφισμός, διότι:
$$\forall r \in \mathbb{R}^+ : \quad z = r + 0i \in \mathbb{C}^* \quad \text{και} \quad \varphi(z) = |z| = |r| = r$$
Υπλογίζουμε τον πυρήνα του ομομορφισμού φ:
$$\mathsf{Ker}(\varphi) = \big\{z \in \mathbb{C}^* \mid \varphi(z) = 1\big\} = \big\{z \in \mathbb{C}^* \mid |z| = 1\big\} = \mathsf{T}$$
Από το Πρώτο Θεώρημα Ισομορφισμών, θα έχουμε ότι η απεικόνιση φ επάγει έναν ισομορφισμό ομάδων[2]
$$\widetilde{\varphi} : \mathbb{C}^*/\,\mathsf{Ker}(\varphi) = \mathbb{C}^*/\mathsf{T} \xrightarrow{\cong} \mathbb{R}^+, \quad \widetilde{\varphi}(zT) = \varphi(z) = |z|$$

(2) Έστω $\left(\begin{smallmatrix} a & b \\ -b & a\end{smallmatrix}\right) \in G$. Τότε παρατηρούμε ότι
$$\begin{vmatrix} a & b \\ -b & a \end{vmatrix} \;=\; a^2 + b^2 \neq 0$$
και άρα τα στοιχεία της G ανήκουν στην $\mathsf{GL}(2,\mathbb{R})$. Θα δείξουμε ότι η G είναι υποομάδα της $\mathsf{GL}(2,\mathbb{R})$. Είναι φανερό ότι το ουδέτερο στοιχείο της $\mathsf{GL}(2,\mathbb{R})$ ανήκει και στην G. Έστω $\left(\begin{smallmatrix} a & b \\ -b & a\end{smallmatrix}\right)$, $\left(\begin{smallmatrix} c & d \\ -d & c\end{smallmatrix}\right) \in G$. Τότε
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac - bd & ad + bc \\ -bc - ad & -bd + ac \end{pmatrix} \in G$$
διότι $ac - bd \neq 0$ και $ad + bc \neq 0$. Άρα το σύνολο G είναι κλειστό ως προς τη πράξη της $\mathsf{GL}_2(\mathbb{R})$. Επίσης για κάθε $\left(\begin{smallmatrix} a & b \\ -b & a\end{smallmatrix}\right) \in G$ το αντίστροφο στοιχείο
$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2}\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \begin{pmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} \in G$$
ανήκει στην G και άρα $G \leq \mathsf{GL}(2,\mathbb{R})$.

[2] Ο ισομορφισμός $\widetilde{\varphi}$ συμπίπτει με τον ισομορφισμό f.

Θα δείξουμε ότι η G είναι ισόμορφη με την $\mathbb{C}^*$. Ορίζουμε την απεικόνιση

$$f: G \longrightarrow \mathbb{C}^*, \quad \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \mapsto f\left(\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)\right) = a + bi$$

που είναι καλά ορισμένη. Έχουμε

- <u>Ομομορφισμός Ομάδων</u>: Έστω $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right), \left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right) \in G$. Τότε

$$\begin{aligned} f\left(\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right)\right) = f\left(\left(\begin{smallmatrix} ax-by & ay+bx \\ -bx-ay & -by+ax \end{smallmatrix}\right)\right) &= (ax - by) + (ay + bx)i \\ &= ax + ayi + bxi - by \\ &= (a + bi) \cdot (x + yi) \\ &= f\left(\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)\right) \cdot f\left(\left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right)\right) \end{aligned}$$

και άρα η f είναι ομομορφισμός ομάδων.

- <u>Ένα προς ένα</u>: Έστω $\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) \in \mathsf{Ker}\, f$. Τότε

$$\begin{aligned} f\left(\left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right)\right) = 1 \implies a + bi = 1 + 0i &\implies a = 1 \text{ και } b = 0 \\ &\implies \left(\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \\ &\implies \mathsf{Ker}\, f = \left\{\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\right\} \end{aligned}$$

Συνεπώς η f είναι ένα προς ένα διότι $\mathsf{Ker}\, f = 0_G$.

- <u>Επί</u>: Για κάθε μιγαδικό αριθμό $x + yi \in \mathbb{C}^*$ το στοιχείο $\left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right) \in G$ και $f\left(\left(\begin{smallmatrix} x & y \\ -y & x \end{smallmatrix}\right)\right) = x + yi$. Επομένως η f είναι επί.

Άρα έχουμε τον ισομορφισμό:

$$G \simeq \mathbb{C}^*$$

■

Άσκηση 6 (**Θεωρημα Cauchy για αβελιανες ομαδες**). *Έστω G μια πεπερασμένη αβελιανή ομάδα τάξης > 1 και p ένας πρώτος διαιρέτης της τάξης $\mathsf{o}(G)$ της ομάδας. Τότε η G έχει (τουλάχιστον) ένα στοιχείο τάξης p.*

Λύση. Η απόδειξη θα γίνει με επαγωγή στην τάξη $\mathsf{o}(G) = n \geq 2$ της ομάδας.

(1) Αν $\mathsf{o}(G) = 2$, τότε προφανώς κάθε στοιχείο της G εκτός του ταυτοτικού έχει τάξη 2 και το Θεώρημα ισχύει κατά τετριμμένο τρόπο.

(2) <u>Επαγωγικη Υποθεση</u>: Υποθέτουμε ότι για κάθε πεπερασμένη αβελιανή ομάδα K τάξης $< \mathsf{o}(G)$ και για κάθε πρώτο διαιρέτη p της τάξης της ομάδας K, η K έχει (τουλάχιστον) ένα στοιχείο τάξης p.

(3) Υποθέτουμε ότι η τάξη της G είναι $n \geq 3$.

   (α΄) Αν οι μόνες υποομάδες της G είναι η τετριμμένη $\{e\}$ και η ίδια η G, τότε όπως γνωρίζουμε η G είναι κυκλική με τάξη έναν πρώτο αριθμό, οποίος αναγκαστικά είναι ο πρώτος διαιρέτης p. Τότε ο γεννήτορας της G έχει προφανώς τάξη p, και άρα η G έχει ένα στοιχείο τάξης p.

   (β΄) Υποθέτουμε ότι η G έχει μια μη-τετριμμένη γνήσια υποομάδα N. Διακρίνουμε περιπτώσεις:

      (i) $p \mid \mathsf{o}(N)$.
      Τότε επειδή $G \neq N \neq \{e\}$, έπεται ότι $\mathsf{o}(N) < \mathsf{o}(G)$. Επειδή η N είναι αβελιανή ως υποομάδα αβελιανής ομάδας, από την Επαγωγική Υπόθεση, έπεται ότι η N έχει ένα στοιχείο τάξης p. Τότε όμως και η G έχει ένα στοιχείο τάξης p.

      (ii) $p \nmid \mathsf{o}(N)$.
      Επειδή η G είναι αβελιανή, η υποομάδα N είναι κανονική υποομάδα της G. Επομένως ορίζεται η ομάδα πηλίκο G/N, η οποία όπως γνωρίζουμε είναι αβελιανή. Επιπλέον η τάξη της είναι

$$1 < \mathsf{o}(G/N) = \frac{\mathsf{o}(G)}{\mathsf{o}(N)} < \mathsf{o}(G)$$

διότι αν $\mathsf{o}(G/N) = 1$, τότε $\mathsf{o}(G) = \mathsf{o}(N)$ απ' όπου $G = N$ το οποίο είναι άτοπο, και αν $\frac{\mathsf{o}(G)}{\mathsf{o}(N)} = \mathsf{o}(G)$, τότε $\mathsf{o}(N) = 1$ απ' όπου $N = \{e\}$ το οποίο είναι άτοπο. Επειδή ο αριθμός p είναι πρώτος, θα έχουμε:

$$p \mid \mathsf{o}(G) = \frac{\mathsf{o}(G)}{\mathsf{o}(N)} \cdot \mathsf{o}(N) \quad \& \quad p \nmid \mathsf{o}(N) \quad \Longrightarrow \quad p \mid \frac{\mathsf{o}(G)}{\mathsf{o}(N)} = \mathsf{o}(G/N)$$

Επειδή η ομάδα πηλίκο G/N είναι αβελιανή και $p \mid \mathsf{o}(G/N) < \mathsf{o}(G)$, από την Επαγωγική Υπόθεση, έπεται ότι η ομάδα $G/N)$ έχει ένα στοιχείο xN τάξης p, και ιδιαίτερα $(xN)^p = x^pN = N$.

Επομένως υπάρχει ένα στοιχείο $e \neq x \in G$: $x^p \in N$. Έστω $m = \mathsf{o}(N)$. Τότε

$$(x^p)^m = (x^m)^p = e^p = e$$

Θέτουμε $y = x^m$. Τότε $y^p = e$, και άρα $\mathsf{o}(y) \mid p$. Επειδή p είναι πρώτος, είτε $\mathsf{o}(y) = 1$ ή $\mathsf{o}(y) = p$. Όμως αν $\mathsf{o}(y) = 1$, τότε $y = x^m = e$ και άρα $(xN)^m = N$ το οποίο σημαίνει ότι $p = \mathsf{o}(xN) \mid m = \mathsf{o}(N)$. Αυτό όμως είναι άτοπο διότι $p \nmid \mathsf{o}(N)$. Επομένως $\mathsf{o}(y) = p$, και άρα η G έχει ένα στοιχείο τάξης p. ■

Άσκηση 7. *Βρείτε την τάξη της δοθείσας ομάδας πηλίκο:*

(1) $\mathbb{Z}_6/\langle [3]_6 \rangle$
(2) $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/(\langle [2]_4 \rangle \times \langle [2]_{12} \rangle)$
(3) $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle ([2]_4, [1]_2) \rangle$
(4) $(\mathbb{Z}_3 \times \mathbb{Z}_5)/(\{[0]_3\} \times \mathbb{Z}_5)$
(5) $(\mathbb{Z}_2 \times S_3)/\langle ([1]_2, (123)) \rangle$

Λύση. (1) Η τάξη της ομάδας πηλίκο $\mathbb{Z}_6/\langle [3]_6 \rangle$ είναι:

$$\mathsf{o}(\mathbb{Z}_6/\langle [3]_6 \rangle) = \frac{\mathsf{o}(\mathbb{Z}_6)}{\mathsf{o}(\langle [3]_6 \rangle)} = \frac{\mathsf{o}(\mathbb{Z}_6)}{\mathsf{o}([3]_6)} = \frac{6}{\mathsf{o}([3]_6)}$$

Επειδή

$$\mathsf{o}([3]_6) = \mathsf{o}(3[1]_6) = \frac{\mathsf{o}([1]_6)}{(3, \mathsf{o}([1]_6)} = \frac{6}{(3,6)} = \frac{6}{3} = 2$$

θα έχουμε:

$$\mathsf{o}(\mathbb{Z}_6/\langle [3]_6 \rangle) = \frac{\mathsf{o}\mathbb{Z}_6}{\mathsf{o}([3]_6)} = \frac{6}{2} = 3$$

(2) Η τάξη της ομάδας πηλίκο $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/(\langle [2]_4 \rangle \times \langle [2]_{12} \rangle)$ είναι:

$$\mathsf{o}((\mathbb{Z}_4 \times \mathbb{Z}_{12})/(\langle [2]_4 \rangle \times \langle [2]_{12} \rangle)) = \frac{\mathsf{o}(\mathbb{Z}_4 \times \mathbb{Z}_{12})}{\mathsf{o}(\langle [2]_4 \rangle \times \langle [2]_{12} \rangle)} = \frac{48}{\mathsf{o}(\langle [2]_4 \rangle \times \langle [2]_{12} \rangle)}$$

Επειδή

$$\langle [2]_4 \rangle = \big\{[0]_2, [2]_4\big\} \quad \text{και} \quad \langle [2]_{12} \rangle = \big\{[0]_{12}, [2]_2, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\big\}$$

έπεται ότι

$$\mathsf{o}(\langle [2]_4 \rangle \times \langle [2]_{12} \rangle) = 2 \cdot 6 = 12$$

και επομένως

$$\mathsf{o}((\mathbb{Z}_4 \times \mathbb{Z}_{12})/(\langle [2]_4 \rangle \times \langle [2]_{12} \rangle)) = \frac{48}{\mathsf{o}(\langle [2]_4 \rangle \times \langle [2]_{12} \rangle)} = \frac{48}{12} = 4$$

(3) Η τάξη της ομάδας πηλίκο $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle([2]_4, [1]_2)\rangle$ είναι:

$$\begin{aligned}
\mathsf{o}\big((\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle([2]_4, [1]_2)\rangle\big) &= \frac{\mathsf{o}(\mathbb{Z}_4 \times \mathbb{Z}_2)}{\mathsf{o}(\langle([2]_4, [1]_2)}\rangle) \\
&= \frac{4 \cdot 2}{[(\mathsf{o}([2]_4), \mathsf{o}([1]_2)]} \\
&= \frac{8}{[2, 2]} \\
&= \frac{8}{2} = 4
\end{aligned}$$

(4) Η τάξη της ομάδας πηλίκο $(\mathbb{Z}_3 \times \mathbb{Z}_5)/(\{[0]_3\} \times \mathbb{Z}_5)$ είναι:

$$\mathsf{o}((\mathbb{Z}_3 \times \mathbb{Z}_5)/(\{[0]_3\} \times \mathbb{Z}_5)) = \frac{\mathsf{o}(\mathbb{Z}_3 \times \mathbb{Z}_5)}{\mathsf{o}(\{[0]_3\} \times \mathbb{Z}_5)} = \frac{3 \cdot 5}{5} = 3$$

διότι προφανώς $\mathsf{o}(\{[0]_3\} \times \mathbb{Z}_5) = \mathsf{o}(\mathbb{Z}_5) = 5$.

(5) Η τάξη της ομάδας πηλίκο $(\mathbb{Z}_2 \times S_3)/\langle([1]_2, (123))\rangle$ είναι:

$$\begin{aligned}
\mathsf{o}((\mathbb{Z}_2 \times S_3)/\langle([1]_2, (123))\rangle) &= \frac{\mathsf{o}(\mathbb{Z}_2 \times S_3)}{\mathsf{o}(\langle([1]_2, (123))\rangle)} \\
&= \frac{2 \cdot 6}{[\mathsf{o}([1]_2), \mathsf{o}((123))]} \\
&= \frac{12}{[2, 3]} \\
&= \frac{12}{6} \\
&= 2
\end{aligned}$$

■

Άσκηση 8. *Βρείτε την τάξη του στοιχείου:*

(1) $[5]_{12} + \langle[4]_{12}\rangle$ *στην ομάδα πηλίκο* $\mathbb{Z}_{12}/\langle[4]_{12}\rangle$
(2) $[26]_{60} + \langle[12]_{60}\rangle$ *στην ομάδα πηλίκο* $\mathbb{Z}_{60}/\langle[12]_{60}\rangle$
(3) $([2]_3, [1]_6) + \langle([1]_3, [1]_6)\rangle$ *στην ομάδα πηλίκο* $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle([1]_3, [1]_6)\rangle$
(4) $([2]_6, [0]_8) + \langle([4]_6, [4]_8)\rangle$ *στην ομάδα πηλίκο* $(\mathbb{Z}_6 \times \mathbb{Z}_8)/\langle([4]_6, [4]_8)\rangle$

Λύση. Οι τάξεις των στοιχείων μπορούν να υπολογισθούν με διάφορους τρόπους, συμπεριλαμβανομένου του ορισμού. Θα δούμε παρακάτω αρκετούς τέτοιους τρόπους.

(1) Η ομάδα $\mathbb{Z}_{12}$ είναι κυκλική με γεννήτορα την κλάση $[1]_{12}$. Επειδή η ομάδα $\mathbb{Z}_{12}/\langle[4]_{12}\rangle$ είναι πηλίκο της κυκλικής ομάδας $\mathbb{Z}_{12}$, έπεται ότι η ομάδα $\mathbb{Z}_{12}/\langle[4]_{12}\rangle$ είναι επίσης κυκλική και μάλιστα με γεννήτορα το στοιχείο $[1]_{12} + \langle[4]_{12}\rangle$. Έτσι θα έχουμε:

$$\mathsf{o}\big([5]_{12} + \langle[4]_{12}\rangle\big) = \mathsf{o}\big(5[1]_{12} + \langle[4]_{12}\rangle\big) = \mathsf{o}\big(5([1]_{12} + \langle[4]_{12}\rangle)\big) = \frac{\mathsf{o}\big([1]_{12} + \langle[4]_{12}\rangle\big)}{\big(5, \mathsf{o}\big([1]_{12} + \langle[4]_{12}\rangle\big)\big)}$$

Επειδή το στοιχείο $[1]_{12} + \langle[4]_{12}\rangle$ είναι γεννήτορας της κυκλικής μάδας, θα έχουμε

$$\mathsf{o}\big([1]_{12} + \langle[4]_{12}\rangle\big) = \mathsf{o}(\mathbb{Z}_{12}/\langle[4]_{12}\rangle) = \frac{\mathsf{o}(\mathbb{Z}_{12})}{\mathsf{o}(\langle[4]_{12}\rangle)} = \frac{12}{\mathsf{o}([4]_{12})} = \frac{12}{3} = 4$$

επειδή προφανώς $\mathsf{o}([4]_{12}) = 3$. Επομένως:

$$\mathsf{o}\big([5]_{12} + \langle [4]_{12}\rangle\big) = \frac{\mathsf{o}\big([1]_{12} + \langle [4]_{12}\rangle\big)}{(5, \mathsf{o}\big([1]_{12} + \langle [4]_{12}\rangle\big))} = \frac{4}{(5,4)} = \frac{4}{1} = 4$$

Παρατηρούμε ότι επειδή η τάξη του στοιχείου $[5]_{12} + \langle [4]_{12}\rangle$ στην ομάδα $\mathbb{Z}_{12}/\langle [4]_{12}\rangle$ είναι 4, δηλαδή όσο και η τάξη της ομάδας, το στοιχείο $[5]_{12} + \langle [4]_{12}\rangle$ είναι επίσης γεννήτορας της $\mathbb{Z}_{12}/\langle [4]_{12}\rangle$.

(2) Η ομάδα $\mathbb{Z}_{60}$ είναι κυκλική με γεννήτορα την κλάση $[1]_{60}$. Επειδή η ομάδα $\mathbb{Z}_{60}/\langle [12]_{60}\rangle$ είναι πηλίκο της κυκλικής ομάδας $\mathbb{Z}_{60}$, έπεται ότι η ομάδα $\mathbb{Z}_{60}/\langle [12]_{60}\rangle$ είναι επίσης κυκλική και μάλιστα με γεννήτορα το στοιχείο $[1]_{60} + \langle [12]_{60}\rangle$. Ιδιαίτερα θα έχουμε:

$$\mathsf{o}([1]_{60} + \langle [12]_{60}\rangle) = \mathsf{o}(\mathbb{Z}_{60}/\langle [12]_{60}\rangle) = \frac{\mathsf{o}(\mathbb{Z}_{60})}{\mathsf{o}(\langle [12]_{60}\rangle)} = \frac{60}{\mathsf{o}(\langle [12]_{60}\rangle)} = \frac{60}{\mathsf{o}([12]_{60})} = \frac{60}{5} = 12$$

διότι όπως μπορούμε να δούμε εύκολα $\mathsf{o}([12]_{60}) = 5$.

Έτσι θα έχουμε:

$$\mathsf{o}\big([26]_{60} + \langle [12]_{60}\rangle\big) = \mathsf{o}\big(26[1]_{60} + \langle [12]_{60}\rangle\big) = \mathsf{o}\big(26([1]_{60} + \langle [12]_{60}\rangle)\big) =$$

$$= \frac{\mathsf{o}\big([1]_{12} + \langle [4]_{12}\rangle\big)}{(26, \mathsf{o}\big([1]_{12} + \langle [12]_{60}\rangle\big))} = \frac{12}{(26,12)} = \frac{12}{2} = 6$$

(3) Η τάξη της ομάδας πηλίκο $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle ([1]_3, [1]_6)\rangle$ είναι:

$$\mathsf{o}((\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle ([1]_3, [1]_6)\rangle) = \frac{\mathsf{o}(\mathbb{Z}_3 \times \mathbb{Z}_6)}{\mathsf{o}(\langle ([1]_3, [1]_6)\rangle)} = \frac{3 \cdot 6}{\mathsf{o}(([1]_3, [1]_6))} = \frac{18}{[\mathsf{o}([1]_3, \mathsf{o}([1]_6])} = \frac{18}{[3,6]} = \frac{18}{6} = 3$$

Άρα η τάξη του στοιχείου $([2]_3, [1]_6) + \langle ([1]_3, [1]_6)\rangle$ στην ομάδα πηλίκο $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle ([1]_3, [1]_6)\rangle$ θα είναι διαιρέτης της τάξης 3 της ομάδας και άρα θα είναι 1 ή 3. Όμως η τάξη του στοιχείου δεν μπορεί να είναι 1 διότι αν είναι 1, τότε $([2]_3, [1]_6) \in \langle ([1]_3, [1]_6)\rangle$ και άρα $([2]_3, [1]_6) = k([1]_3, [1]_6)$, για κάποιον ακέραιο k. Δηλαδή $([2]_3, [1]_6) = k([k]_3, [k]_6)$ και επομένως $[2]_3 = [k]_3$ και $[1]_6 = [k]_6$. Τότε $3 \mid k-2$ και $6 \mid k-1$. Προφανώς οι δύο τελευταίες σχέσεις διαιρετότητας μας οδηγούν σε άτοπο. Επομένως:

$$\mathsf{o}(([2]_3, [1]_6) + \langle ([1]_3, [1]_6)\rangle) = 3$$

(4) Η τάξη του στοιχείου $([2]_6, [0]_8) + \langle ([4]_6, [4]_8)\rangle$ στην ομάδα πηλίκο $(\mathbb{Z}_6 \times \mathbb{Z}_8)/\langle (4,4)\rangle$ είναι 1, δηλαδή $([2]_6, [0]_8) + \langle ([4]_6, [4]_8)\rangle = \langle (4,4)\rangle$ διότι το στοιχείο $([2]_6, [0]_8)$ ανήκει στην υποομάδα $\langle ([4]_6, [4]_8)\rangle$. Παραγματικά: $8([4]_6, [4]_8) = ([32]_6, [32]_8) = ([2]_6, [0]_8)$. Έτσι

$$\mathsf{o}(([2]_6, [0]_8) + \langle ([4]_6, [4]_8)\rangle) = 1$$

■

Άσκηση 9. *Αποδείξτε την ύπαρξη των παρακάτω ισομορφισμών:*

(1) $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle ([0]_2, [1]_4)\rangle \;\cong\; \mathbb{Z}_2$
(2) $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle ([0]_2, [2]_4)\rangle \;\cong\; \mathbb{Z}_2 \times \mathbb{Z}_2$
(3) $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle ([1]_2, [2]_4)\rangle \;\cong\; \mathbb{Z}_4$
(4) $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8)/\langle (0, 4, [0]_8)\rangle \;\cong\; \mathbb{Z} \times \mathbb{Z}_4 \times \mathbb{Z}_8$
(5) $(\mathbb{Z} \times \mathbb{Z})/\langle (2,2)\rangle \;\cong\; \mathbb{Z}_2 \times \mathbb{Z}$

Λύση. (1) Ορίζουμε απεικόνιση

$$f : \mathbb{Z}_2 \times \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2, \qquad ([x]_2, [y]_4) \longmapsto f([x]_2, [y]_4)) = [x]_2 \,.$$

Πολύ εύκολα βλέπουμε ότι η απεικόνιση f είναι επιμορφισμός ομάδων. Ο πυρήνας της f είναι:

$$\begin{aligned}
\mathsf{Ker}(f) &= \big\{([x]_2,[y]_4)\in\mathbb{Z}_2\times\mathbb{Z}_4 \mid f([x]_2,[y]_4)=[0]_2\big\}\\
&= \big\{([x]_2,[y]_4)\in\mathbb{Z}_2\times\mathbb{Z}_4 \mid [x]_2=[0]_2\big\}\\
&= \big\{([0]_2,[y]_4)\in\mathbb{Z}_2\times\mathbb{Z}_4\big\}\\
&= \big\{y([0]_2,[1]_4)\in\mathbb{Z}_2\times\mathbb{Z}_4 \mid y\in\mathbb{Z}\big\}\\
&= \langle([0]_2,[1]_4)\rangle
\end{aligned}$$

Επομένως από το Πρώτο Θεώρημα Ισομορφισμών έχουμε ότι

$$(\mathbb{Z}_2\times\mathbb{Z}_4)\big/\mathsf{Ker}(f)\ \cong\ \mathbb{Z}_2 \qquad\Longrightarrow\qquad (\mathbb{Z}_2\times\mathbb{Z}_4)/\langle([0]_2,[1]_4)\rangle\ \cong\ \mathbb{Z}_2\ .$$

Ο παραπάνω ισομορφισμός ορίζεται ως εξής:

$$\overline{f}:\ (\mathbb{Z}_2\times\mathbb{Z}_4)/\langle([0]_2,[1]_4)\rangle\ \longrightarrow\ \mathbb{Z}_2,\qquad \overline{f}\big(([x]_2,[y]_4)+\langle([0]_2,[1]_4)\rangle\big)=[x]_2$$

(2) Ορίζουμε απεικόνιση

$$f:\ \mathbb{Z}_2\times\mathbb{Z}_4\longrightarrow\mathbb{Z}_2\times\mathbb{Z}_2,\qquad ([x]_2,[y]_4)\longmapsto f([x]_2,[y]_4)=([x]_2,[y]_2)$$

Η απεικόνιση f είναι καλά ορισμένη διότι αν $([x]_2,[y]_4)=([x']_2,[y']_4)$, τότε $([x]_2=[x']_2$ και $[y]_4=[y']_4$. Η τελευταία ισότητα δίνει ότι $4\mid y-y'$ και τότε $2\mid y-y'$, δηλαδή $[y]_2=[y']_2$. Επομένως $([x]_2,[y]_2)=([x']_2,[y']_2)$ δηλαδή: $f([x]_2,[y]_4)=f([x']_2,[y']_4)$ και η f είναι καλά ορισμένη.

Πολύ εύκολα βλέπουμε ότι η απεικόνιση f είναι επιμορφισμός ομάδων. Ο πυρήνας της f είναι:

$$\begin{aligned}
\mathsf{Ker}(f) &= \{([x]_2,[y]_4)\in\mathbb{Z}_2\times\mathbb{Z}_4 \mid f([x]_2,[y]_4)=([0]_2,[0]_2)\}\\
&= \{([x]_2,[y]_4)\in\mathbb{Z}_2\times\mathbb{Z}_4 \mid ([x]_2,[y]_2)=([0]_2,[0]_2)\}\\
&= \{([x]_2,[y]_4)\in\mathbb{Z}_2\times\mathbb{Z}_4 \mid [x]_2=[0]_2\ \text{ και }\ [y]_2=[0]_2\}\\
&= \{([x]_2,[y]_4)\in\mathbb{Z}_2\times\mathbb{Z}_4 \mid [x]_2=[0]_2\ \text{ και }\ [y]_4=[0]_4\ \text{ ή }\ [y]_4=[2]_4\}\\
&= \big\{([0]_2,[0]_4),([0]_2,[2]_4\big\}\\
&= \langle([0]_2,[2]_4)\rangle
\end{aligned}$$

Επομένως από το Πρώτο Θεώρημα Ισομορφισμών θα έχουμε ότι

$$(\mathbb{Z}_2\times\mathbb{Z}_4)\big/\mathsf{Ker}(f)\ \cong\ \mathbb{Z}_2\times\mathbb{Z}_2 \qquad\Longrightarrow\qquad (\mathbb{Z}_2\times\mathbb{Z}_4)/\langle([0]_2,[2]_4)\rangle\ \cong\ \mathbb{Z}_2\times\mathbb{Z}_2$$

Ο παραπάνω ισομορφισμός ορίζεται ως εξής:

$$\overline{f}:\ (\mathbb{Z}_2\times\mathbb{Z}_4)/\langle([0]_2,[2]_4)\rangle\ \longrightarrow\ \mathbb{Z}_2\times\mathbb{Z}_2,\qquad \overline{f}\big(([x]_2,[y]_4)+\langle([0]_2,[2]_4)\rangle\big)=([x]_2,[y]_2)$$

(3) Η τάξη της ομάδας πηλίκο $(\mathbb{Z}_2\times\mathbb{Z}_4)/\langle([1]_2,[2]_4)\rangle$ είναι

$$\mathsf{o}\big((\mathbb{Z}_2\times\mathbb{Z}_4)/\langle(1,2)\rangle\big)=\frac{\mathsf{o}(\mathbb{Z}_2\times\mathbb{Z}_4)}{\mathsf{o}(\langle([1]_2,[2]_4)\rangle)}=\frac{8}{2}=4$$

όπου παραπάνω χρησιμοποιήσαμε ότι:

$$\mathsf{o}(\langle([1]_2,[2]_4)\rangle)=\mathsf{o}([1]_2,[2]_4)=[\mathsf{o}([1])_2),\mathsf{o}([2]_4)]=[2,2]=2$$

Γνωρίζουμε ότι κάθε ομάδα τάξης 4 είναι ισόμορφη είτε με την κυκλική τάξης 4 ή με την ομάδα του Klein. Επειδή η ομάδα $(\mathbb{Z}_2\times\mathbb{Z}_4)/\langle([1]_2,[2]_4)\rangle$ έχει τάξη 4, θα είναι ισόμορφη με την $\mathbb{Z}_4$ αν έχει ένα στοιχείο τάξης 4. Παρατηρούμε ότι το στοιχείο

$$x=([1]_2,[1]_4)+\langle([1]_2,[2]_4)\rangle\in(\mathbb{Z}_2\times\mathbb{Z}_4)/\langle([1]_2,[2]_4)\rangle$$

έχει τάξη 4, διότι:

$$4x = 4\big(([1]_2,[1]_4) + \langle([1]_2,[2]_4)\rangle\big) = ([4]_2,[4]_4) + \langle([1]_2,[2]_4)\rangle = ([0]_2,[0]_4) + \langle([1]_2,[2]_4)\rangle = \langle([1]_2,[2]_4)\rangle$$

και όπως μπορούμε να δούμε εύκολα ο αριθμός $k = 4$ είναι ο μικρότερος φυσικός με την ιδιότητα $kx = 0$ στην ομάδα πηλίκο. Επομένως το στοιχείο $([1]_2,[1]_4) + \langle([1]_2,[2]_4)\rangle$ είναι γεννήτορας της ομάδας $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle([1]_2,[2]_4)\rangle$, και άρα:

$$\mathsf{o}\big(([1]_2,[1]_4) + \langle([1]_2,[2]_4)\rangle\big) = 4 \quad \Longrightarrow \quad (\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle([1]_2,[2]_4)\rangle \quad \cong \quad \mathbb{Z}_4$$

Ο παραπάνω ισομορφισμός μεταξύ κυκλικών ομάδων ίδιας τάξης, θα στέλνει τον γεννήτορα $([1]_2,[1]_4)+\langle([1]_2,[2]_4)\rangle$ της $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle([1]_2,[2]_4)\rangle$ στον γεννήτορα $[1]_4$ της $\mathbb{Z}_4$. Επομένως επειδή

$$(\mathbb{Z}_2 \times \mathbb{Z}_4)\big/\langle([1]_2,[2]_4)\rangle = \big\{k\big(([1]_2,[1]_4) + \langle([1]_2,[2]_4)\rangle\big) \mid 0 \leq k \leq 3\big\}$$

θα έχουμε ότι ο ζητούμενος ισομορφισμός θα είναι ο ακόλουθος

$$\overline{f} : (\mathbb{Z}_2 \times \mathbb{Z}_4)\big/\langle([1]_2,[2]_4)\rangle \longrightarrow \mathbb{Z}_4, \qquad \overline{f}\big(k\big(([1]_2,[1]_4) + \langle([1]_2,[2]_4)\rangle\big)\big) = k[1]_4 = [k]_4$$

(4) Ορίζουμε απεικόνιση

$$f : \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8 \longrightarrow \mathbb{Z} \times \mathbb{Z}_4 \times \mathbb{Z}_8, \quad f(m,n,[k]_8) = (m,[n]_4,[k]_8)$$

Είναι πολύ εύκολο να δούμε ότι η f είναι καλά ορισμένη και επιμορφισμός. Ο πυρήνας της f είναι:

$$\begin{aligned}
\mathsf{Ker}(f) &= \big\{(m,n,[k]_8) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8 \mid f(m,n,[k]_8) = (0,[0]_4,[0]_8)\big\} \\
&= \{(m,n,\overline{k}_8) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8 \mid (m,[n]_4,[k]_8) = (0,[0]_4,[0]_8)\} \\
&= \{(0,n,\overline{0}_8) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8 \mid 4 \mid n\} \\
&= \{(0,n,\overline{0}_8) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8 \mid n = 4r, \quad r \in \mathbb{Z}\} \\
&= \{(0,4r,\overline{0}_8) \in \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8 \mid \quad r \in \mathbb{Z}\} \\
&= \langle(0,4,[0]_8)\rangle
\end{aligned}$$

Επομένως από το Πρώτο θεώρημα Ισομορφισμών θα έχουμε ότι

$$(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8)\big/\mathsf{Ker}(f) \;\cong\; \mathbb{Z} \times \mathbb{Z}_4 \times \mathbb{Z}_8 \quad \Longrightarrow \quad (\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8)/\langle(0,4,[0]_8)\rangle \;\cong\; \mathbb{Z} \times \mathbb{Z}_4 \times \mathbb{Z}_8$$

Ο παραπάνω ισομορφισμός ορίζεται ως εξής:

$$\overline{f} : (\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8)\big/\langle(0,4,[0]_8)\rangle \longrightarrow \mathbb{Z} \times \mathbb{Z}_4 \times \mathbb{Z}_8, \qquad \overline{f}\big((m,n,[k]_8) + \langle(0,4,[0]_8)\rangle\big) = (m,[n]_4,[k]_8)$$

(5) Ορίζουμε απεικόνιση

$$f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}, \quad f(n,m) = ([n]_2, m-n)$$

Η f είναι προφανώς καλά ορισμένη και για κάθε $(n,m),(n',m') \in \mathbb{Z} \times \mathbb{Z}$ έχουμε:

$$\begin{aligned}
f((n,m) + (n',m')) &= f(n+n', m+m') \\
&= ([n+n']_2, (m+m') - (n+n')) \\
&= ([n]_2 + [n']_2, (m-n) + (m'-n')) \\
&= ([n]_2, m-n) + ([n']_2, m'-n') \\
&= f(n,m) + f(n',m')
\end{aligned}$$

Συνεπώς η f είναι ομομορφισμός ομάδων. Επίσης για κάθε $([n]_2, m) \in \mathbb{Z}_2 \times \mathbb{Z}$ υπάρχει το στοιχείο $(n, m+n) \in \mathbb{Z} \times \mathbb{Z}$ έτσι ώστε

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

και άρα η f είναι επιμορφισμός. Τέλος, ο πυρήνας της f είναι:

$$\begin{aligned}\mathsf{Ker}(f) &= \big\{(n,m)\in\mathbb{Z}\times\mathbb{Z} \mid f(n,m)=([0]_2,0)\big\}\\ &= \big\{(n,m)\in\mathbb{Z}\times\mathbb{Z} \mid ([n]_2,m-n)=([0]_2,0)\big\}\\ &= \big\{(n,m)\in\mathbb{Z}\times\mathbb{Z} \mid 2\mid n \ \text{ και } \ m=n\big\}\\ &= \big\{(2k,2k)\mid k\in\mathbb{Z}\big\}\\ &= \langle(2,2)\rangle\end{aligned}$$

Επομένως από το Πρώτο Θεώρημα Ισομορφισμών έχουμε ότι

$$(\mathbb{Z}\times\mathbb{Z})\big/\mathsf{Ker}(f) \ \cong\ \mathbb{Z}_2\times\mathbb{Z} \quad\Longrightarrow\quad (\mathbb{Z}\times\mathbb{Z})\big/\langle(2,2)\rangle \ \cong\ \mathbb{Z}_2\times\mathbb{Z}$$

Ο παραπάνω ισομορφισμός ορίζεται ως εξής:

$$\overline{f}:\ (\mathbb{Z}\times\mathbb{Z})\big/\langle(2,2)\rangle \ \longrightarrow\ \mathbb{Z}_2\times\mathbb{Z}, \qquad \overline{f}\big((n,m)+\langle(2,2)\rangle\big)=([n]_2,m)$$ ■

Άσκηση 10. (1) *Έστω G και H δύο ομάδες και $a\in G$ και $b\in H$. Τότε τα ακόλουθα είναι ισοδύναμα:*

(α΄) *Τα στοιχεία a και b των G και H αντίστοιχα έχουν πεπερασμένη τάξη.*

(β΄) *Το στοιχείο (a,b) της ομάδας ευθύ γινόμενο $G\times H$ έχει πεπερασμένη τάξη.*

Επιπλέον αν τα στοιχεία a και b των G και H αντίστοιχα έχουν πεπερασμένη τάξη, τότε:

$$\mathsf{o}((a,b))=[\mathsf{o}(a),\mathsf{o}(b)]$$

(2) *Αν G και H είναι πεπερασμένες κυκλικές ομάδες, να δείξετε ότι η ομάδα ευθύ γινόμενο $G\times H$ είναι κυκλική αν και μόνον αν:*

$$(\mathsf{o}(G),\mathsf{o}(H))=1 \tag{$\dagger$}$$

(3) *Να δείξετε ότι:*

$$\mathbb{Z}_n\times\mathbb{Z}_m\ \cong\ \mathbb{Z}_{nm} \quad\Longleftrightarrow\quad (n,m)=1 \tag{$\dagger\dagger$}$$

Λύση. (1) «$\Longrightarrow$» Έστω ότι τα στοιχεία a και b των G και H αντίστοιχα έχουν πεπερασμένη τάξη, και έστω ότι $n=\mathsf{o}(a)$ και $m=\mathsf{o}(b)$. Θα δείξουμε ότι το στοιχείο (a,b) έχει πεπερασμένη τάξη και μάλιστα $\mathsf{o}((a,b))=[n,m]$. Έστω $k=[n,m]$. Τότε υπάρχουν φυσικοί αριθμοί r,s έτσι ώστε $k=nr$ και $m=ms$. Τότε θα έχουμε:

$$(a,b)^k=(a^k,b^k)=(a^{nr},b^{ms})=((a^n)^r,(b^m)^s)=(e_G^r,e_H^s)=(e_G,e_H)$$

Επομένως το στοιχείο (a,b) έχει πεπερασμένη τάξη. Αν l είναι ένας φυσικός με την ιδιότητα $(a,b)^l=(e_G,e_H)$, τότε θα έχουμε:

$$(a,b)^l=(e_G,e_H) \implies (a^l,b^l)=(e_G,e_H) \implies a^l=e_G \ \&\ b^l=e_H \implies \mathsf{o}(a)=n\mid l \ \&\mathsf{o}(b)=m\mid l$$

Επομένως $[n,m]\mid l$ και άρα $k=[n,m]\leq l$. Αυτό δείχνει ότι $\mathsf{o}((a,b))=[n,m]=[\mathsf{o}(a),\mathsf{o}(b)]$.

«$\Longleftarrow$» Αντίστροφα αν το στοιχείο (a,b) της ομάδας ευθύ γινόμενο $G\times H$ έχει πεπερασμένη τάξη, έστω $\mathsf{o}((a,b))=k$, τότε θα έχουμε:

$$(a,b)^k=(e_G,e_H) \implies (a^k,b^k)=(e_G,e_H) \implies a^k=e_G \ \&\ b^k=e_H \implies \mathsf{o}(a)<\infty \ \&\ \mathsf{o}(b)<\infty$$

(2) Υποθέτουμε ότι οι κυκλικές ομάδες $G=\langle a\rangle$ και $H=\langle b\rangle$ είναι πεπερασμένες, και έστω:

$$\mathsf{o}(G)=\mathsf{o}(a)=n \qquad \text{και} \qquad \mathsf{o}(H)=\mathsf{o}(b)=m$$

Υποθέτουμε πρώτα ότι $(n,m)=1$. Τότε σύμφωνα με το μέρος (1) θα έχουμε ότι η τάξη του στοιχείου (a,b) είναι $[n,m]=nm$, διότι $(n,m)=1$. Άρα η κυκλική υποομάδα $\langle(a,b)\rangle$ της ομάδας $G\times H$ η οποία παράγεται από το στοιχείο (a,b) έχει τάξη $nm=\mathsf{o}(G)\cdot\mathsf{o}(H)=\mathsf{o}(G\times H)$. Αυτό σημαίνει ότι $\langle(a,b)\rangle=G\times H$ και άρα η ομάδα $G\times H$ είναι κυκλική με γεννήτορα το στοιχείο (a,b).

Αντίστροφα υποθέτουμε ότι η $G \times H$ είναι κυκλική και έστω $G \times H = \langle (x,y) \rangle$. Τότε $\mathsf{o}((x,y)) = nm$. Επειδή $x \in G$ και $y \in H$, και επειδή $|G| = n$ και $|H| = m$, από το Θεώρημα του Lagrange έπεται ότι $\mathsf{o}(x) \mid n$ και $\mathsf{o}(y) \mid m$ και άρα $n = \mathsf{o}(x) \cdot k$ και $m = \mathsf{o}(y) \cdot l$. Τότε[3]:

$$\frac{\mathsf{o}(x)\mathsf{o}(y)}{(\mathsf{o}(x),\mathsf{o}(y))} = [\mathsf{o}(x),\mathsf{o}(y)] = \mathsf{o}((x,y)) = n \cdot m = \mathsf{o}(x) \cdot k \cdot \mathsf{o}(y) \cdot l \quad \Longrightarrow \quad k \cdot l \cdot (\mathsf{o}(x),\mathsf{o}(y)) = 1$$

απ' όπου προφανώς έπεται ότι: $k = l = (\mathsf{o}(x),\mathsf{o}(y)) = 1$. Τότε $\mathsf{o}(x) = n$, $\mathsf{o}(y) = m$, και επομένως $(n,m) = 1$.

(3) Αν οι ομάδες $\mathbb{Z}_n \times \mathbb{Z}_m$ και $\mathbb{Z}_{nm}$ είναι ισόμορφες, τότε η ομάδα $\mathbb{Z}_n \times \mathbb{Z}_m$ είναι κυκλική και επομένως από την ισοδυναμία (†) θα έχουμε ότι $(n,m) = 1$. Αντίστροφα αν $(n,m) = 1$, από την ισοδυναμία (†) θα έχουμε ότι η ομάδα $\mathbb{Z}_n \times \mathbb{Z}_m$ είναι κυκλική. Επειδή κυκλικές ομάδες με την ίδια τάξη είναι ισόμορφες, έπεται ότι οι ομάδες $\mathbb{Z}_n \times \mathbb{Z}_m$ και $\mathbb{Z}_{nm}$ θα είναι ισόμορφες. ■

Παρατήρηση. *Είναι εύκολο να δει κανείς, με χρήση Μαθηματικής Επαγωγής, ότι αν $G_1, \cdots, G_k$ είναι ομάδες και $(a_1, \cdots, a_k)$ είναι ένα στοιχείο της ομάδας ευθύ γινόμενο $G_1 \times \cdots \times G_k$, τότε τα ακόλουθα είναι ισοδύναμα:*

(1) *Τα στοιχεία $a_1, a_2, \cdots, a_k$ των ομάδων $G_1, \cdots, G_k$ αντίστοιχα έχουν πεπερασμένη τάξη.*
(2) *Το στοιχείο $(a_1, \cdots, a_k)$ της ομάδας ευθύ γινόμενο $G_1 \times G_2 \cdots \times G_k$ έχει πεπερασμένη τάξη.*

Επιπλέον αν τα στοιχεία στοιχεία $a_1, a_2, \cdots, a_k$ έχουν πεπερασμένη τάξη, τότε:

$$\mathsf{o}((a_1, a_2, \cdots, a_k)) = [\mathsf{o}(a_1), \mathsf{o}(a_2, \cdots, \mathsf{o}(a_k)]$$

Επιπλέον αν οι ομάδες $G_1, \cdots, G_k$ είναι πεπερασμένες κυκλικές, τότε τα ακόλουθα είναι ισοδύναμα

(3) *Η ομάδα ευθύ γινόμενο $G_1 \times \cdots \times G_k$ είναι κυκλική.*
(4)
$$1 \leq i \neq j \leq n \quad \Longrightarrow \quad \big(\mathsf{o}(G_i), \mathsf{o}(G_j)\big) = 1$$

Ιδιαίτερα αν $n_1, \cdots, n_k$ είναι φυσικοί αριθμοί, τότε τα ακόλουθα είναι ισοδύναμα:

(5) *Η ομάδα ευθύ γινόμενο $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ είναι κυκλική.*
(6)
$$1 \leq i \neq j \leq n \quad \Longrightarrow \quad \big(n_i, n_j\big) = 1$$

Επομένως αν n είναι ένας φυσικός αριθμός με πρωτογενή ανάλυση

$$n = p_1^{a_1} \cdots p_k^{a_k}$$

τότε επειδή οι αριθμοί $p_i^{a_i}$, $1 \leq i \leq k$, είναι πρώτοι μεταξύ τους ανά δύο, έπεται ότι η ομάδα ευθύ γινόμενο $\mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$ θα είναι κυκλική τάξης $n = p_1^{a_1} \cdots p_k^{a_k}$. Επομένως θα έχουμε έναν ισομορφισμό

$$\mathbb{Z}_n \ \cong \ \mathbb{Z}_{p_1^{a_1}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}} \qquad \surd$$

Άσκηση 11. *Να εξετασθεί αν η ομάδα ευθύ γινόμενο $G_1 \times G_2$ δύο κυκλικών ομάδων G_1 και G_2 είναι επίσης κυκλική.*

Λύση. Διακρίνουμε περιπτώσεις:

[3]Υπενθυμιζουμε ότι:

$$\forall n, m \in \mathbb{N}: \quad (n,m) \cdot [n,m] = n \cdot m$$

(1) Οι κυκλικές ομάδες G_1 και G_2 είναι πεπερασμένες.

Τότε όπως γνωρίζουμε από την Άσκηση 10:

$$\text{η ομάδα } \ G_1 \times G_2 \ \text{ είναι κυκλική} \quad \Longleftrightarrow \quad \big(\mathsf{o}(G_1), \mathsf{o}(G_2)\big) = 1$$

(2) Μια εκ των κυκλικών ομάδων G_1 και G_2 είναι άπειρη.

(α΄) Αν η G_1 είναι άπειρη κυκλική, και η $G_2 = \{e\}$ είναι η τετριμμένη υποομάδα, τότε η ομάδα ευθύ γινόμενο $G_1 \times G_2$ είναι προφανώς ισόμορφη με την G_1, μέσω του ισομορφισμού

$$f: \ G_1 \times \{e\} \longrightarrow G_1, \quad f(g_1, e) = g_1$$

και άρα είναι κυκλική.

(β΄) Υποθέτουμε ότι η G_1 είναι άπειρη κυκλική, και $G_2 \neq \{e\}$

Έστω ότι η ομάδα $G_1 \times G_2$ είναι κυκλική. Επειδή η G_1 είναι άπειρη έπεται ότι η $G_1 \times G_2$ είναι μια άπειρη κυκλική ομάδα. Επειδή σε μια άπειρη κυκλική ομάδα το μόνο στοιχείο πεπερασμένης τάξης είναι το ταυτοτικό στοιχείο, έπεται ότι η κυκλική ομάδα G_2 είναι άπειρη. Πράγματι, αν η G_2 είναι πεπερασμένη, τότε υπάρχει γεννήτορας $e_2 \neq g_2 \in G_2$ και $\mathsf{o}(g_2) = n < \infty$, και τότε καταλήγουμε σε άτοπο

$$(e_1, g_2)^n = (e_1^n, g_2^n) = (e_1, e_2) \implies \mathsf{o}(e_1, g_2) < \infty \implies (e_1, g_2) = (e_1, e_2) \implies g_2 = e_2$$

Άρα και η G_2 είναι άπειρη κυκλική. Υποθέτουμε ότι:

$$G_1 = \langle a \rangle \quad \text{και} \quad G_2 = \langle b \rangle$$

Έστω $(x, y) \in G_1 \times G_2$ ένας γεννήτορας της: $G_1 \times G_2 = \langle (x, y) \rangle$. Τότε:

$$(x, y) = (a^r, b^s), \qquad \text{όπου} \qquad r \in \mathbb{Z} \quad \text{και} \quad s \in \mathbb{Z}$$

Τότε υπάρχει ακέραιος $n \in \mathbb{Z}$:

$$(a, e) = (x, y)^n = (x^n, y^n) = ((a^r)^n, (b^s)^n = (a^{rn}, b^{sn}) \implies a = a^{rn} \quad \text{και} \quad b^{sn} = e_2$$

Άρα

$$a^{rn-1} = e_1 \quad \text{και} \quad b^{sn} = e_2$$

Επειδή το μόνο στοιχείο της G_2 με πεπερασμένη τάξη είναι το ταυτοτικό στοιχείο της, έπεται ότι είτε $b = e_2$ ή $sn = 0$. Αν $b = e_2$, τότε επειδή $G_2 = \langle b \rangle$ και η G_2 είναι άπειρη καταλήγουμε σε άτοπο. Άρα $sn = 0$ και επομένως $s = 0$ ή $n = 0$. Από την άλλη πλευρά, επειδή $a^{rn-1} = e_1$ για τον ίδιο λόγο θα έχουμε ότι είτε $a = e_1$ ή $rn = 1$. Η εκδοχή $a = e_1$ απορρίπτεται διότι το στοιχείο $G_1 = \langle a \rangle$ και η G_1 είναι άπειρη. Άρα ισχύει $rn = 1$ και επομένως θα έχουμε και $s = 0$. Τότε όμως $y = e_2$ και θα υπάρχει $m \in \mathbb{Z}$ έτσι ώστε:

$$(e_1, b) = (x, y)^m = (x^m, y^m) = (x^m, e_2^m) = (x^m, e_2) \implies b = e_2$$

το οποίο είναι άτοπο διότι $G_2 = \langle b \rangle$ και η ομάδα G_2 είναι άπειρη.

Άρα καταλήξαμε σε άτοπο και επομένως η ομάδα $G_1 \times G_2$ δεν είναι κυκλική.

Συνοψίζουμε: η ομάδα ευθύ γινόμενο $G_1 \times G_2$ είναι κυκλική αν και μόνον αν:

(1) Είτε οι ομάδες G_1 και G_2 είναι πεπερασμένες και $\big(\mathsf{o}(G_1), \mathsf{o}(G_2)\big) = 1$,
(2) ή μία εκ των ομάδων G_1 και G_2 είναι η τετριμμένη ομάδα.

Ιδιαίτερα έπεται ότι το ευθύ γινόμενο δύο άπειρων κυκλικών ομάδων δεν είναι ποτέ κυκλική ομάδα. ■

Άσκηση 12. *Έστω $G = \langle a \rangle$ μια κυκλική ομάδα. Να βρεθούν όλοι οι ομομορφισμοί ομάδων $f: G \longrightarrow G$.*

Λύση. Από την Άσκηση 1, γνωρίζουμε ότι οι ομομορφισμοί ομάδων $f\colon G \longrightarrow G$ είναι της μορφής $f_k\colon G \longrightarrow G$, $f_k(x) = x^k$, όπου $k \in \mathbb{Z}$. Άρα αρκεί να εξετάσουμε ποιοί από τους ομομορφισμούς f_k, $k \in \mathbb{Z}$, συμπίπτουν.

Διακρίνουμε περιπτώσεις:

(1) Η G είναι άπειρη ομάδα. Τότε: $k = l \Longleftrightarrow f_k = f_l$.

Πράγματι, αν $k = l$, τότε προφανώς $f_k = f_l$. Αντίστροφα, αν $f_k = f_l$, τότε $f(x) = x^k = x^l$, $\forall x \in G$, και επομένως από την Άσκηση 1 θα έχουμε $k = l$.

Άρα όλοι οι, ανά δύο διαφορετικοί, ομομορφισμοί $f\colon G \longrightarrow G$ είναι οι άπειροι σε πλήθος ομομορφισμοί

$$f_k\colon G \longrightarrow G, \quad f_k(x) = x^k, \qquad \text{όπου} \quad k \in \mathbb{Z}$$

(2) Η G είναι πεπερασμένη ομάδα τάξης n. Τότε: $f_k = f_l \Longleftrightarrow k \equiv l \,(\mathrm{mod}\, n)$.

Πράγματι, αν $k \equiv l \,(\mathrm{mod}\, n)$, τότε όπως είδαμε στην Άσκηση 1 θα έχουμε $f_k = f_l$. Αντίστροφα, αν $f_k = f_l$, τότε $f(x) = x^k = x^l$, $\forall x \in G$, και επομένως από την Άσκηση 1 θα έχουμε $k \equiv l \,(\mathrm{mod}\, n)$.

Άρα όλοι οι, ανά δύο διαφορετικοί, ομομορφισμοί $f\colon G \longrightarrow G$ είναι οι n σε πλήθος ομομορφισμοί

$$f_k\colon G \longrightarrow G, \quad f_k(x) = x^k, \qquad \text{όπου} \quad k = 0, 1, 2, \cdots, n-1$$ ■

Παρατήρηση. *Από την παραπάνω Άσκηση έπεται ότι:*

(1) *οι ανα δύο διαφορετικοί ομομορφισμοί ομάδων* $: \mathbb{Z} \longrightarrow \mathbb{Z}$ *είναι οι απεικονίσεις*

$$f_k\colon \mathbb{Z} \longrightarrow \mathbb{Z}, \quad f_k(x) = kx, \qquad k \in \mathbb{Z}$$

(2) *οι ανα δύο διαφορετικοί ομομορφισμοί ομάδων* $: \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ *είναι οι απεικονίσεις*

$$f_k\colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \quad f_k([x]_n) = [kx]_n, \qquad k = 0,\ 1,\ 2,\ \cdots,\ n-1$$

Η επόμενη Άσκηση περιγράφει όλους τους ανά δύο διαφορετικούς ομομορφισμούς ομάδων $: \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$. ▲

Άσκηση 13. *Να βρεθούν όλοι οι ομομορφισμοί ομάδων* $f\colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$.

Λύση. (1) Αν $f\colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ είναι ένας ομομορφισμός ομάδων, τότε υπάρχει $k \in \mathbb{Z}$ έτσι ώστε: $f([x]_n) = [kx]_m$, $\forall [x]_n \in \mathbb{Z}_n$.

Πράγματι, τότε $f([1]_n) \in \mathbb{Z}_m$ και επομένως υπάρχει ακέραιος $k \in \mathbb{Z}$ έτσι ώστε $f([1]_n) = [k]_n$. Προφανώς, για κάθε στοιχείο $[x]_m \in \mathbb{Z}_m$ θα έχουμε $[kx]_m = k[x]_m = [k]_m \cdot [x]_m$. Για κάθε $[x]_n \in \mathbb{Z}_n$, θα έχουμε:

$$f([x]_n) = f(x[1]_n) = xf([1]_n) = x[k]_m = [xk]_m$$

(2) Έστω $k \in \mathbb{Z}$. Θα δείξουμε ότι η απεικόνιση

$$f_k\colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_m, \quad f([x]_n) = [kx]_m$$

είναι ομομορφισμός ομάδων[4] αν και μόνον αν $m \mid kn$.

Πράγματι, αν $m \mid kn$, τότε υπάρχει $r \in \mathbb{Z}$ έτσι ώστε $kn = mr$. Έστω $[x]_n = [y]_n$. Τότε $n \mid x - y$ και επομένως $x - y = ns$ για κάποιον ακέραιο $s \in \mathbb{Z}$. Τότε $kx - ky = kns = mrs$ και επομένως $kx - ky \equiv 0 \,(\mathrm{mod}\, m)$, δηλαδή $[kx]_m = [ky]_m$. Άρα $f_k([x]_n) = f_k([y]_n)$ και η f_k είναι καλά ορισμένη απεικόνιση. Τέλος η f_k είναι ομομορφισμός διότι

$$f_k([x]_n + [y]_n) = f_k([x+y]_n) = [k(x+y)]_m = [kx+ky]_m = [kx]_m + [ky]_m = f_k([x]_n) + f_k([y]_n)$$

[4]Το κρίσιμο σημείο στον ισχυρισμό είναι αν η απεικόνιση f_k είναι καλά ορισμένη.

Αντίστροφα, αν η απεικόνιση f_k είναι ομομορφισμός ομάδων, τότε θα έχουμε:

$$[0]_m = f_k([0]_n) = f_k([n]_n) = f_k(n[1]_n) = nf_k([1]_m) = n[k\cdot 1]_m = n[k]_m = [nk]_m \quad \Longrightarrow \quad kn \equiv 0 \pmod m$$

και επομένως: $m \mid kn$.

(3) Έστω $k, l \in \mathbb{Z}$ είναι δύο ακέραιοι έτσι ώστε $m \mid kn$ και $m \mid ln$. Τότε από το μέρος (2) έπεται ότι ορίζονται οι ομομορφισμοί ομάδων f_k και f_l.

Θα δείξουμε ότι: $f_k = f_l \iff k \equiv l \pmod m$.

Πράγματι, αν $k \equiv l \pmod m$, τότε υπάρχει $r \in \mathbb{Z}$ έτσι ώστε $k - l = rm$ και άρα $k = l + rm$. Τότε θα έχουμε, $\forall [x]_n$:

$$f_k([x]_n) = [kx]_m = [(l+rm)x]_m = [lx + rmx]_m = [lx]_m + [rmx]_m = [lx]_m = f_l([x]_n)$$

και άρα $f_k = f_l$.

Αντίστροφα, έστω $f_k = f_l$. Τότε:

$$f_k([1]_n) = f_l([1]_n) \quad \Longrightarrow \quad [k\cdot 1]_m = [l \cdot 1]_m \quad \Longrightarrow \quad [k]_m = [l]_m \quad \Longrightarrow \quad k \equiv l \pmod m$$

(4) Από τα μέρη (1) και (2) οι δυνατοί ομομορφισμοί ομάδων $f\colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ είναι όλες οι διαφορετικές ανά δύο απεικονίσεις $f_k\colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$, όπου $k \in \mathbb{Z}$ και $m \mid kn$. Λαμβάνοντας υπ' όψιν το μέρος (3), αναζητούμε μεταξύ των m σε πλήθος διαφορετικών ανά δύο απεικονίσεων f_k για τις οποίες ισχύει ότι $m \mid kn$. Με άλλα λόγια ζητάμε τα ανά δύο διαφορετικά στοιχεία $[k]_n \in \mathbb{Z}_m$ για τα οποία $m \mid kn$. Επομένως αναζητούμε τις διακεκριμένες λύσεις k στο $\mathbb{Z}_m$ της γραμμικής ισοτιμίας

$$kn \equiv 0 \pmod m$$

Από την Θεωρία Αριθμών γνωρίζουμε ότι οι ανά δύο ανισότιμες $\bmod m$ λύσεις της παραπάνω ισοτιμίας είναι οι

$$k = 0, 1, 2, \cdots, d-1, \qquad \text{όπου} \qquad d = (n, m)$$

Άρα, καταλήγουμε, όλοι οι ανά δύο διαφορετικοί, ομομορφισμοί $f\colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_m$ είναι οι εξής:

$$f_k\colon \mathbb{Z}_n \longrightarrow \mathbb{Z}_m, \quad f_k([x]_n) = [kx]_m, \qquad \text{όπου} \quad k = 0,\ \frac{m}{d},\ 2\frac{m}{d},\ 3\frac{m}{d},\ \cdots,\ (d-1)\frac{m}{d}, \quad d = (n,m) \qquad \blacksquare$$

Άσκηση 14. (1) *Δείξτε ότι το σύνολο* $\mathsf{Aut}(G)$ *όλων των αυτομορφισμών*[5] *μιας ομάδας* G *είναι ομάδα με πράξη τη σύνθεση απεικονίσεων.*

(2) *Να προσδιορισθεί η ομάδα αυτομορφισμών* $\mathsf{Aut}(G)$, *όταν:*

(α') G *είναι μια άπειρη κυκλική ομάδα.*

(β') G *είναι μια πεπερασμένη κυκλική ομάδα.*

Λύση. (1) Επειδή η σύνθεση αυτομορφισμών είναι αυτομορφισμός, και επειδή η σύνθεση απεικονίσεων ικανοποιεί την προσεταιριστική ιδιότητα, αρκεί να δείξουμε την ύπαρξη ταυτοτικού στοιχείου και την ύπαρξη αντίστροφου στοιχείου. Όμως προφανώς η ταυτοτική απεικόνιση είναι αυτομορφισμός, και επειδή η αντίστροφη απεικόνιση ενός αυτομορφισμού είναι προφανώς αυτομορφισμός, έπεται ότι το σύνολο $\mathsf{Aut}(G)$ όλων των αυτομορφισμών μιας ομάδας G είναι ομάδα με πράξη τη σύνθεση απεικονίσεων.

(2) (α') Υποθέτουμε ότι η G είναι μια άπειρη κυκλική ομάδα.

Έστω $G = \langle a \rangle$ ένας γεννήτορας της G. Τότε προφανώς για κάθε αυτομορφισμό $f\colon G \longrightarrow G$ της G, το στοιχείο $f(a)$ είναι επίσης γεννήτορας της G. Επειδή η G είναι άπειρη κυκλική, γνωρίζουμε ότι η G έχει ακριβώς δύο γεννήτορες: το στοιχείο a και το στοιχείο a^{-1}. Έτσι $f(a) = a$ ή $f(a) = a^{-1}$.

[5] Υπενθυμίζουμε ότι μια απεικόνιση $f\colon G \longrightarrow G$ καλείται **αυτομορφισμός** της G, αν η f είναι ισομορφισμός.

Επειδή $G = \langle a \rangle$, αν $f(a) = a$, έπεται ότι $f = \mathrm{Id}_G$, και αν $f(a) = a^{-1}$, τότε $f(x) = x^{-1}$, $\forall x \in G$. Αντίστροφα οι απεικονίσεις Id_G και $\varphi\colon G \longrightarrow G, \varphi(x) = x^{-1}$ είναι αυτομορφισμοί της G. Άρα $\mathsf{Aut}(G) = \{\mathrm{Id}_G, \varphi\}$, όπου προφανώς $\varphi^2 = \mathrm{Id}_G$. Επομένως η $\mathsf{Aut}(G)$ είναι ισόμορφη με την κυκλική ομάδα $\mathbb{Z}_2$, μέσω του ισομορφισμού $\mathrm{Id}_G \longmapsto [0]_2$ και $\varphi \longmapsto [1]_2$:

$$\mathsf{Aut}(G) \ \cong \ \mathbb{Z}_2$$

(β΄) Υποθέτουμε ότι η G είναι μια πεπερασμένη κυκλική ομάδα.

Έστω

$$G = \langle a \rangle = \big\{e,\ a,\ a^2,\ \cdots,\ a^{n-1}\big\}$$

Αν $n = 1$, τότε $G = \{e\}$ και $\mathbb{Z}_1 = [0]_1$ και τότε προφανώς $\mathsf{Aut}(G) = \{\mathrm{Id}_G\} \cong \{\mathrm{Id}_{\mathbb{Z}_1}\} \cong \mathsf{U}(\mathbb{Z}_1)$.

Υποθέτουμε ότι $n > 1$. Έστω $f\colon G \longrightarrow G$ ένας αυτομορφισμός της G. Τότε το στοιχείο $f(a) \in G$ είναι γεννήτορας της G. Γνωρίζουμε από την Θεωρία ότι οι γεννήτορες μιας κυκλικής ομάδας τάξης n με γεννήτορα το στοιχείο a, είναι της μορφής a^k, όπου $1 \leq k \leq n-1$ και $(k, n) = 1$. Επομένως θα έχουμε $f(a) = a^k$, για ένα μοναδικό στοιχείο k, όπου $1 \leq k \leq n-1$ και $(k, n) = 1$ (αν $k = 0$, τότε $f(a) = e$ και άρα $a = e$ διότι η f αυτομορφισμός, δηλαδή $G = \{e\}$ το οποίο είναι άτοπο). Έτσι θα έχουμε $[k]_n \in \mathsf{U}(\mathbb{Z}_n)$, και επομένως μπορούμε να ορίσουμε μια απεικόνιση

$$\Phi:\ \mathsf{Aut}(G) \ \longrightarrow\ \mathsf{U}(\mathbb{Z}_n), \quad \Phi(f) = [k]_n, \qquad \text{όπου} \qquad f(a) = a^k$$

• Έστω $f, g \in \mathsf{Aut}(G)$ και έστω ότι $\Phi(f) = \Phi(g)$, δηλαδή: $[k]_n = [l]_n$, όπου $f(a) = a^k$ και $g(a) = a^l$. Τότε $n \mid k - l$ και επειδή $1 \leq k, l \leq n$ και $(k, n) = 1 = (l, n)$, έπεται ότι $k = l$. Επομένως $f(a) = g(a)$ και τότε προφανώς $f = g$, διότι επειδή οι f, g είναι ομομορφισμοί και $\forall x \in G$, $x = a^m$, θα έχουμε: $f(x) = f(a^m) = f(a)^m = g(a)^m = g(a^m) = g(x)$. Επομένως η απεικόνιση Φ είναι 1-1.

• Έστω $[k]_n \in \mathsf{U}(\mathbb{Z}_n)$, δηλαδή $1 \leq k \leq n-1$ και $(k, n) = 1$. Ορίζουμε μια απεικόνιση

$$f_k:\ G \ \longrightarrow\ G, \quad f(a^m) = a^{km}$$

Η απεικόνιση f_k είναι ομομορφισμός, διότι:

$$f_k(a^{m_1}a^{m_2}) = f_k(a^{m_1+m_2}) = a^{(m_1+m_2)k} = a^{m_1k+m_2k} = a^{m_1k}a^{m_2k} = f_k(a^{m_1})f(a^{m_2})$$

Αν $f_k(a^m) = e$, τότε $a^{mk} = e$, και άρα $n \mid mk$. Επειδή $(n, k) = 1$, έπεται ότι $n \mid m$. Τότε όμως αναγκαστικά $m = 0$, διότι $0 \leq m \leq n-1$. Άρα $a^m = a^0 = e$ και ο ομομορφισμός f_k είναι μονομορφισμός. Τότε όμως ο ομομορφισμός f_k είναι αυτομορφισμός διότι $\mathsf{o}(G) = n < \infty$. Τέλος, εξ' ορισμού θα έχουμε $\Phi(f_k) = [k]_n$, διότι $f_k(a) = a^k$, και άρα η απεικόνιση Φ είναι επί.

• Μένει να δείξουμε ότι η Φ είναι ομομορφισμός ομάδων. Έστω $f, g \in \mathsf{Aut}(G)$. Τότε θα έχουμε $\Phi(f) = a^k$, $\Phi(g) = a^l$, όπου $f(a) = a^k$, $g(a) = a^l$, και $1 \leq k, l \leq n-1$ και $(k, n) = 1 = (l, n)$. Υποθέτουμε ότι $\Phi(f \circ g) = a^m$, όπου $1 \leq m \leq n-1$, $(n, m) = 1$, και $(f \circ g)(a) = a^m$. Όμως $(f \circ g)(a) = f(g(a)) = f(a^l) = f(a)^l = (a^k)^l = a^{kl}$. Τότε: $a^{kl} = a^m$ και επομένως $a^{kl-m} = e$. Επειδή $\mathsf{o}(a) = n$, θα έχουμε $n \mid kl - m$ και επομένως $[kl]_n = [m]_n$, δηλαδή: $[k]_k[l]_n = [m]_n$. Τότε:

$$\Phi(f \circ g) = [m]_n = [kl]_n = [k]_n[l]_n = \Phi(f)\Phi(g)$$

και άρα η απεικόνιση Φ είναι ομομορφισμός. Επομένως η Φ είναι ισομορφισμός, και άρα:

$$\mathsf{Aut}(G) \ \cong \ \mathsf{U}(\mathbb{Z}_n) \qquad \blacksquare$$

Υπενθυμίζουμε ότι αν A είναι ένα μη-κενό σύνολο, τότε $\mathcal{S}(A)$ συμβολίζει την ομάδα μεταθέσεων επί του συνόλου A, δηλαδή το σύνολο των «1-1» και «επί» απεικονίσεων $: A \longrightarrow A$, το οποίο αποτελεί ομάδα με πράξη την σύνθεση απεικονίσεων.

Άσκηση 15. *Έστω X και Y δύο μη-κενά σύνολα με το ίδιο πλήθος στοιχείων: $|X| = |Y|$. Τότε υπάρχει ένας ισομορφισμός ομάδων*

$$\widetilde{\varphi} : \mathcal{S}(X) \xrightarrow{\cong} \mathcal{S}(Y)$$

Λύση. Επειδή $|X| = |Y|$, έπεται ότι υπάρχει μια «1-1» και «επί» απεικόνιση $\varphi \colon X \longrightarrow Y$. Ορίζουμε μια απεικόνιση:

$$\widetilde{\varphi} \colon \mathcal{S}(X) \longrightarrow \mathcal{S}(Y), \quad \widetilde{\varphi}(f) = \varphi \circ f \circ \varphi^{-1}$$

Δηλαδή η απεικόνιση $\widetilde{\varphi}$ στέλνει την «1-1» και «επί» απεικόνιση $f \colon X \longrightarrow X$ στην απεικόνιση $\widetilde{\varphi}(f)$ η οποία ορίζεται ως η εξής σύνθεση:

$$\begin{tikzcd}
Y \arrow[r, dashed, "\widetilde{\varphi}(f)"] \arrow[d, "\varphi^{-1}"'] & Y \\
X \arrow[r, "f"] & Y \arrow[u, "\varphi"']
\end{tikzcd}$$

(1) <u>*Η $\widetilde{\varphi}$ είναι καλά ορισμένη*</u>: Έστω $f \in \mathcal{S}(X)$. Θα δείξουμε ότι η απεικόνιση $\widetilde{\varphi}(f)$ ανήκει στο σύνολο $\mathcal{S}(Y)$, δηλαδή είναι «1-1» και «επί». Αυτό όμως είναι άμεσο διότι $\widetilde{\varphi}(f) = \varphi \circ f \circ \varphi^{-1}$ είναι «1-1» και «επί» ως σύνθεση απεικονίσεων οι οποίες είναι «1-1» και «επί».

(2) <u>*Η $\widetilde{\varphi}$ είναι «1-1»*</u>: Έστω $f, g \in \mathcal{S}(X)$, και υποθέτουμε ότι $\widetilde{\varphi}(f) = \widetilde{\varphi}(g)$. Τότε συνθέτοντας από αριστερά με την φ^{-1} και από τα δεξιά με την φ, θα έχουμε:

$$\widetilde{\varphi}(f) = \widetilde{\varphi}(g) \implies \varphi \circ f \circ \varphi^{-1} = \varphi \circ g \circ \varphi^{-1} \implies f \circ \varphi^{-1} = g \circ \varphi^{-1} \implies f = g$$

Επομένως η $\widetilde{\varphi}$ είναι «1-1».

(3) <u>*Η $\widetilde{\varphi}$ είναι «επί»*</u>: Αν $h \colon Y \longrightarrow Y$ είναι μια «1-1» και «επί» απεικόνιση, δηλαδή ένα στοιχείο της ομάδας $\mathcal{S}(Y)$, τότε θεωρούμε την απεικόνιση

$$\varphi^{-1} \circ h \circ \varphi : X \longrightarrow X$$

η οποία είναι «1-1» και «επί» ως σύνθεση απεικονίσεων οι οποίες είναι «1-1» και «επί», και άρα ανήκει στην ομάδα $\mathcal{S}(X)$. Επιπλέον

$$\widetilde{\varphi}(\varphi^{-1} \circ h \circ \varphi) = \varphi \circ \varphi^{-1} \circ h \circ \varphi \circ \varphi^{-1} = h$$

Επομένως η απεικόνιση $\widetilde{\varphi}$ είναι επί.

(4) <u>*Η $\widetilde{\varphi}$ είναι ομομορφισμός*</u>: Έστω $f, g \in \mathcal{S}(X)$. Τότε:

$$\widetilde{\varphi}(f \circ g) = \varphi \circ (f \circ g) \circ \varphi^{-1} = \varphi \circ f \circ g \circ \varphi^{-1} = \varphi \circ f \circ \mathrm{Id}_Y \circ g \circ \varphi^{-1} =$$
$$= \varphi \circ f \circ \varphi^{-1} \circ \varphi \circ g \circ \varphi^{-1} = \widetilde{\varphi}(f) \circ \widetilde{\varphi}(g)$$

Συνοψίζοντας, δείξαμε ότι η απεικόνιση $\widetilde{\varphi} \colon \mathcal{S}(X) \longrightarrow \mathcal{S}(Y)$ είναι ένας ισομορφισμός ομάδων. ■

Εφαρμογή: Αν X είναι ένα σύνολο με πλήθος στοιχείων $|X| = n$, τότε από την Άσκηση 15, έπεται ότι υπάρχει ένας ισομορφισμός ομάδων

$$\mathcal{S}(X) \xrightarrow{\cong} \mathsf{S}_n$$

Σύμφωνα με το Θεώρημα του Cayley, για κάθε ομάδα G υπάρχει μονομορφισμός ομάδων

$$\mathsf{L} : G \longrightarrow \mathcal{S}(G), \quad \mathsf{L}(g) := l_g, \quad \text{όπου} \quad l_g : G \longrightarrow G, \quad l_g(x) = gx$$

και επομένως η G είναι ισόμορφη με την υποομάδα $\mathsf{Im}(\mathsf{L}) = \big\{l_g \in \mathcal{S}(G) \mid g \in G\big\} \leq \mathcal{S}(G)$. Η υποομάδα $\mathsf{Im}(\mathsf{L})$ καλείται η **αριστερή κανονική αναπαράσταση** της G.

Η **δεξιά κανονική αναπαράσταση** της G είναι η υποομάδα $\mathsf{Im}(\mathsf{R}) \leq \mathcal{S}(G)$, όπου R είναι ο μονομορφισμός ομάδων

$$\mathsf{R} : G \longrightarrow \mathcal{S}(G), \quad \mathsf{R}(g) := r_g, \quad \text{όπου} \quad r_g : G \longrightarrow G, \quad r_g(x) = xg^{-1}$$

Άσκηση 16. *Να βρεθεί η αριστερή κανονική αναπαράσταση της κυκλικής ομάδας τάξης* 3.

Λύση. Θα υπολογίσουμε την αριστερή κανονική αναπαράσταση της κυκλικής ομάδας τάξης 3:

$$G = \langle a \rangle = \big\{e,\ a,\ b\big\}$$

όπου $\mathsf{o}(a) = 3$, και άρα $b = a^2$ και $e = a^3$.

Επειδή $\mathsf{o}(G) = 3$, έπεται ότι η G θα είναι ισόμορφη με την υποομάδα $\mathsf{Im}(\mathsf{L})$ της ομάδας μεταθέσεων $\mathcal{S}(\{e,a,b\})$ επί του συνόλου $G = \{e,a,b\}$, και η οποία με τη σειρά της είναι ισόμορφη με την τρίτη συμμετρική ομάδα S_3. Θα έχουμε:

$$\mathsf{Im}(\mathsf{L}) = \big\{l_e,\ l_a,\ l_b\big\} \ \leq\ \mathcal{S}(\{e,a,b\}) \ \cong\ S_3$$

Ο πίνακας Cayley του πολλαπλασιασμού της ομάδας G είναι:

$G = \big\{e,\ a,\ b\big\}$:

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Θα προσδιορίσουμε τις μεταθέσεις $l_e,\ l_a,\ l_b$:

(1) Η μετάθεση

$$l_e : G \longrightarrow G, \quad l_e(x) = ex$$

Άρα:

$$l_e(e) = ee = e, \qquad l_e(a) = ea = a, \qquad l_e(b) = eb = b$$

Επομένως η απεικόνιση l_e είναι η ταυτοτική μετάθεση του συνόλου $G = \{e,a,b,c\}$:

$$l_e = \begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}$$

(2) Η μετάθεση

$$l_a : G \longrightarrow G, \quad l_a(x) = ax$$

Άρα:

$$l_a(e) = ae = a, \qquad l_a(a) = aa = a^2 = b, \qquad l_a(b) = ab = e, \qquad \mathsf{l}_a(c) = ac = b$$

Επομένως η απεικόνιση l_a είναι η ακόλουθη μετάθεση του συνόλου $G = \{e,a,b\}$:

$$l_a = \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}$$

(3) Η μετάθεση

$$l_b : G \longrightarrow G, \quad l_b(x) = bx$$

Άρα:

$$l_b(e) = be = b, \qquad l_b(a) = ba = e, \qquad l_b(b) = b^2 = a$$

Επομένως η απεικόνιση l_b είναι η ακόλουθη μετάθεση του συνόλου $G = \{e,a,b,c\}$:

$$l_b = \begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix}$$

Από μτα παραπάνω έπεται ότι η G είναι ισόμορφη με τη ακόλουθη ομάδα μεταθέσεων (υποομάδα της $\mathsf{S}(G)$):

$$\mathsf{Im}(\mathsf{L}) = \left\{ \begin{pmatrix} e & a & b \\ e & a & b \end{pmatrix}, \ \begin{pmatrix} e & a & b \\ a & b & e \end{pmatrix}, \ \begin{pmatrix} e & a & b \\ b & e & a \end{pmatrix} \right\}$$

Χρησιμοποιώντας την «1-1» και «επί» απεικόνιση

$$G = \{e, a, b\} \longrightarrow \{1, 2, 3\}, \qquad \text{όπου} \quad e \leftrightarrows 1, \ \ a \leftrightarrows 2, \ \ b \leftrightarrows 3$$

από την Άσκηση 15 θα έχουμε ότι η $\mathsf{S}(G)$ είναι ισόμορφη με την S_3.

Επομένως η G είναι ισόμορφη με τη ακόλουθη ομάδα μεταθέσεων (υποομάδα της S_3):

$$\left\{ \iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 1 \end{pmatrix}, \ \ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \ \ \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

Άρα:

$$\mathsf{L} \, : \, G \xrightarrow{\ \cong\ } \left\{ \iota, \ \rho_1, \ \rho_2 \right\} = \langle \rho_1 \rangle \ \leq \ S_3$$

Απο τα παραπάνω μπορούμε να σχηματίσουμε τον πίνακα Cayley της αριστερής κανονικής αναπαράστασης $\mathsf{Im}\,\mathsf{L}$ της G:

$\mathsf{Im}\,\mathsf{L} = \left\{ l_e, \ l_a, \ l_b \right\}$:

$\cdot$	l_e	l_a	l_b
l_e	l_e	l_a	l_b
l_a	l_a	l_e	l_c
l_b	l_b	l_c	l_e

■

Άσκηση 17. *Να βρεθεί η αριστερή κανονική αναπαράσταση της ομάδας* $\mathcal{V} = \left\{ e, a, b, c \right\}$ *του Klein.*

Λύση. Θα υπολογίσουμε την αριστερή κανονική αναπαράσταση της ομάδας του Klein τάξης 4:

$$G = \left\{ e, \ a, \ b, \ c \right\}$$

όπου $a^2 = b^2 = c^2 = e$, και $c = ab$.

Επειδή $\mathsf{o}(G) = 4$, έπεται ότι η G θα είναι ισόμορφη με την υποομάδα $\mathsf{Im}(\mathsf{L}_G)$ της συμμετρικής ομάδας $\mathsf{S}(\{e, a, b, c\})$ η οποία με τη σειρά της είναι ισόμορφη με την S_4. Θα έχουμε:

$$\mathsf{Im}(\mathsf{L}_G) = \left\{ \mathsf{l}_e, \ \mathsf{l}_a, \ \mathsf{l}_b, \ \mathsf{l}_c \right\} \ \leq \ \mathsf{S}(\{e, a, b, c\}) \ \ \cong \ \ \mathsf{S}_4$$

Ο πίνακας Cayley του πολλαπλασιασμού της ομάδας G είναι:

$G = \left\{ e, \ a, \ b, \ c \right\}$:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Θα προσδιορίσουμε τις μεταθέσεις $\mathsf{l}_e, \ \mathsf{l}_a, \ \mathsf{l}_b, \ \mathsf{l}_c$:

(1) Η μετάθεση

$$\mathsf{l}_e : \ G \longrightarrow G, \qquad \mathsf{l}_e(x) = ex$$

Άρα:

$$\mathsf{l}_e(e) = ee = e^2 = e, \qquad \mathsf{l}_e(a) = ea = a, \qquad \mathsf{l}_e(b) = eb = b, \qquad \mathsf{l}_e(c) = ec = c$$

Επομένως η απεικόνιση l_e είναι η ταυτοτική μετάθεση του συνόλου $G = \{e, a, b\}$:

$$\mathsf{l}_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}$$

(2) Η μετάθεση

$$\mathsf{l}_a : G \longrightarrow G, \quad \mathsf{l}_a(x) = ax$$

Άρα:

$$\mathsf{l}_a(e) = ae = a, \quad \mathsf{l}_a(a) = aa = a^2 = e, \quad \mathsf{l}_a(b) = ab = c, \quad \mathsf{l}_a(c) = ac = b$$

Επομένως η απεικόνιση l_a είναι η ακόλουθη μετάθεση του συνόλου $G = \{e, a, b, c\}$:

$$\mathsf{l}_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix} = (e\,a)(b\,c)$$

(3) Η μετάθεση

$$\mathsf{l}_b : G \longrightarrow G, \quad \mathsf{l}_b(x) = bx$$

Άρα:

$$\mathsf{l}_b(e) = be = b, \quad \mathsf{l}_b(a) = ba = c, \quad \mathsf{l}_b(b) = b^2 = e, , \quad \mathsf{l}_b(c) = bc = a$$

Επομένως η απεικόνιση l_b είναι η ακόλουθη μετάθεση του συνόλου $G = \{e, a, b, c\}$:

$$\mathsf{l}_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix} = (e\,b)(a\,c)$$

(4) Η μετάθεση

$$\mathsf{l}_c : G \longrightarrow G, \quad \mathsf{l}_c(x) = cx$$

Άρα:

$$\mathsf{l}_c(e) = ce = c, \quad \mathsf{l}_c(a) = ca = b, \quad \mathsf{l}_c(b) = cb = a, \quad \mathsf{l}_c(c) = c^2 = e$$

Επομένως η απεικόνιση l_c είναι η ακόλουθη μετάθεση του συνόλου $G = \{e, a, b, c\}$:

$$\mathsf{l}_c = \begin{pmatrix} e & a & b & c \\ c & b & c & e \end{pmatrix} = (e\,c)(a\,b)$$

Επομένως η G είναι ισόμορφη με τη ακόλουθη ομάδα μεταθέσεων (υποομάδα της $\mathsf{S}(G)$):

$$\mathsf{Im}(\mathsf{L}_G) = \big\{(e),\ (e\,a)(b\,c),\ (e\,b)(a\,c),\ (e\,c)(a\,b)\big\}$$

Χρησιμοποιώντας την 1-1 και επί απεικόνιση

$$G = \{e, a, b, c\} \longrightarrow \{1, 2, 3, 4\}, \qquad \text{όπου} \quad e \leftrightarrows 1, \;\; a \leftrightarrows 2, \;\; b \leftrightarrows 3, \;\; c \leftrightarrows 4$$

από την Άσκηση 15 θα έχουμε ότι η $\mathsf{S}(G)$ είναι ισόμορφη με την S_4.

Επομένως η G είναι ισόμορφη με τη ακόλουθη ομάδα μεταθέσεων (υποομάδα της S_4):

$$\mathsf{Im}(\mathsf{L}_G) = \big\{(e),\ (12)(34),\ (13)(24),\ (14)(23)\big\}$$

Άρα:

$$\mathsf{L} : G \xrightarrow{\cong} \big\{(e),\ (12)(34),\ (13)(24),\ (14)(23)\big\} \ \leq\ \mathsf{S}_4$$

Απο τα παραπάνω μπορούμε να σχηματίσουμε τον πίνακα Cayley της $\mathsf{Im}\,\mathsf{L}_G$:

$\mathsf{Im}\,\mathsf{L}_G = \big\{\mathsf{l}_e,\ \mathsf{l}_a,\ \mathsf{l}_b,\ \mathsf{l}_c\big\}$:

$\cdot$	l_e	l_a	l_b	l_c
l_e	l_e	l_a	l_b	l_c
l_a	l_a	l_e	l_c	l_b
l_b	l_b	l_c	l_e	l_a
l_c	l_c	l_b	l_a	l_e

■

Άσκηση 18. *Έστω $f : G \longrightarrow G'$ ένας ομομορφισμός ομάδων.*

(1) *Αν H είναι μια κανονική υποομάδα της G, να δείξετε ότι η $f(H)$ είναι μια κανονική υποομάδα της $\mathsf{Im}(f) = f(G)$.*

(2) *Αν K είναι μια κανονική υποομάδα της G', να δείξετε ότι η $f^{-1}(K)$ είναι κανονική υποομάδα της G.*

Λύση. (1) Έστω H μια κανονική υποομάδα της G και έστω $y \in \mathsf{Im}(f)$. Τότε $y = f(g)$ για κάποιο στοιχείο $g \in G$. Επειδή η f είναι ομομορφσιμός, για κάθε στοιχείο $f(h) \in f(H)$, θα έχουμε:

$$y^{-1}f(h)y = f(g)^{-1}f(h)f(g) = f(g^{-1})f(h)f(g) = f(g^{-1}hg) \in f(H)$$

διότι επειδή η H είναι κανονοκή υποομάδα της G, έπεται ότι θα έχουμε: $g^{-1}hg \in H$, για κάθε $g \in G$ και για κάθε $h \in H$. Άρα δείξαμε ότι $\forall y \in f(G)$, $\forall f(h) \in f(H)$: $y^{-1}f(h)y \in f(H)$, και επομένως η υποομάδα $f(H)$ είναι κανονική υποομάδα της $f(G)$.

(2) Έστω K μια κανονική υποομάδα της G', και έστω $g \in G$ και $h \in f^{-1}(K)$. Τότε $f(h) = k \in K$, και λόγω κανονικότητας της K στην G', θα έχουμε:

$$f(g^{-1}hg) = f(g^{-1})f(h)f(g) = f(g)^{-1}kf(g) \in K$$

Αυτό όμως σημαίνει ότι: $g^{-1}hg \in f^{-1}(K)$. Επομένως η υποομάδα $f^{-1}(K)$ είναι μια κανονική υποομάδα της G. ∎

Άσκηση 19. (Δευτερο Θεωρημα Ισομορφισμων) *Έστω G μια ομάδα, $H \leq G$ μια υποομάδα της G, και $N \trianglelefteq G$ μια κανονική υποομάδα της G. Να δείξετε ότι:*

(1) *Το υποσύνολο $HN = \{hn \in G \mid h \in H \ \ \& \ \ n \in N\}$ είναι μια υποομάδα της G και $N \trianglelefteq HN$.*

(2) *$H \cap N \trianglelefteq H$, και υπάρχει ένας ισομορφισμός ομάδων:*

$$HN \,/\, N \ \cong \ H \,/\, (H \cap N)$$

Αν η ομάδα G είναι προσθετική, τότε ο παραπάνω ισομορφισμός έχει την ακόλουθη μορφή:

$$H + N \,/\, N \ \cong \ H \,/\, (H \cap N)$$

Ως εφαρμογή να δείξετε ότι, αν $G = \mathbb{Z}$, $H = 3\mathbb{Z}$, $N = 4\mathbb{Z}$, τότε υπάρχει ισομορφισμός:

$$3\mathbb{Z}/12\mathbb{Z} \ \cong \ \mathbb{Z}_4$$

Λύση. (1) Προφανώς $e = ee \in HN$.

Έστω $g_1, g_2 \in HN$. Τότε $g_1 = h_1n_1$ και $g_2 = h_2n_2$, και επομένως:

$$g_1g_2^{-1} = h_1n_1(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2^{-1} = h_1n_1en_2^{-1}h_2^{-1} = h_1n_1h_2^{-1}h_2n_2^{-1}h_2^{-1} = h_1n_1h_2^{-1}n'$$

$$\text{όπου} \quad n' = h_2n_2^{-1}h_2^{-1} = (h_2^{-1})^{-1}n_2^{-1}h_2^{-1} \in N \quad \text{διότι} \quad N \trianglelefteq G$$

Παρόμοια:

$$h_1n_1h_2^{-1}n' = h_1en_1h_2^{-1}n' = h_1h_2^{-1}h_2n_1h_2^{-1}n' = h_1h_2^{-1}n''n' \in HN$$

$$\text{όπου} \quad n'' = h_2n_1h_2^{-1} = (h_2^{-1})^{-1}n_1h_2^{-1} \in N \quad \text{διότι} \quad N \trianglelefteq G$$

Επομένως θα έχουμε:

$$g_1g_2^{-1} \in HN \qquad \text{και άρα} \qquad HN \leq G$$

Έστω τώρα $hn \in HN$ και $n' \in N$, Τότε θα έχουμε:

$$(hn)^{-1}n'(hn) = n^{-1}h^{-1}n'hn = n^{-1}(h^{-1}n'h)n \in N$$

διότι, επειδή $N \trianglelefteq G$, το στοιχείο $h^{-1}n'h \in N$ και $n^{-1}, n \in N$. Άρα $N \trianglelefteq HN$.

(2) Ορίζουμε απεικόνιση

$$f:\ H \longrightarrow HN/N, \qquad f(h) = hN$$

θεωρώντας το στοιχείο $h \in H \subseteq HN$.

Η f είναι προφανώς ομομορφισμός ομάδων. Ο πυρήνας της f είναι:

$$\mathsf{Ker}(f) = \big\{h \in H \mid f(h) = N\big\} = \big\{h \in H \mid hN = N\big\} = \big\{h \in H \mid h \in N\big\} = H \cap N$$

και επομένως η υποομάδα $H \cap N$ είναι κανονική υποομάδα της H.

Η απεικόνιση f είναι επιμορφισμός, διότι:

$$\forall (hn)N \in HN/N:\quad (hn)N = hN \quad \text{διότι} \quad h^{-1}(hn) = (h^{-1}h)n = en = n \in N \quad \text{και άρα}$$

$$f(h) = hN = (hn)N$$

Από το Πρώτο Θεώρημα Ισομορφισμών θα έχουμε ότι ο επιμορφισμός f ορίζει έναν ισομορφισμό

$$\overline{f}:\ H/H \cap N \xrightarrow{\cong} HN/N, \qquad \overline{f}(h(H \cap N)) = hN$$

Εφαρμογή: Τέλος έστω $G = \mathbb{Z}$, $H = 3\mathbb{Z}$, και $N = 4\mathbb{Z}$. Χρησιμοποιώντας προσθετικό συμβολισμό (επειδή όλες οι εμπλεκόμενες ομάδες είναι προσθετικές), θα έχουμε:

$$3\mathbb{Z} + 4\mathbb{Z} = \big\{3m + 4n \in \mathbb{Z} \mid m, n \in \mathbb{Z}\big\}$$

και έτσι από ότι αποδείξαμε πριν θα έχουμε έναν ισομορφισμό ομάδων:

$$3\mathbb{Z}/(3\mathbb{Z} \cap 4\mathbb{Z}) \ \cong\ (3\mathbb{Z} + 4\mathbb{Z})/4\mathbb{Z} \tag{$*$}$$

Θα ταυτοποιήσουμε πρώτα τις ομάδες $3\mathbb{Z} + 4\mathbb{Z}$ και $3\mathbb{Z} \cap 4\mathbb{Z}$.

Επειδή $(3, 4) = 1$, έπεται ότι υπάρχουν $x, y \in \mathbb{Z}$ έτσι ώστε $3x + 4y = 1$. Επομένως αν $k \in \mathbb{Z}$, τότε

$$k = k1 = k(3x + 4y) = 3(kx) + 4(ky) \in 3\mathbb{Z} + 4\mathbb{Z}$$

και άρα:

$$3\mathbb{Z} + 4\mathbb{Z} = \mathbb{Z}$$

Επομένως

$$(3\mathbb{Z} + 4\mathbb{Z})/4\mathbb{Z} = \mathbb{Z}/4\mathbb{Z} \ \cong\ \mathbb{Z}_4 \tag{$**$}$$

Από την άλλη πλευρά, $3\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z}$. Πραγματικά, έστω $x \in 3\mathbb{Z} \cap 4\mathbb{Z}$, και άρα $x = 3n = 4m$, δηλαδή $3 \mid x$ και $4 \mid x$. Επειδή $(3, 4) = 1$, θα έχουμε $12 = 3 \cdot 4 \mid x$ και άρα $x = 12k$ για κάποιο $k \in \mathbb{Z}$, δηλαδή $x \in 12\mathbb{Z}$ και έτσι: $3\mathbb{Z} \cap 4\mathbb{Z} \subseteq 12\mathbb{Z}$. Αντίστροφα, έστω $x \in 12\mathbb{Z}$, δηλαδή $x = 12k$ για κάποιο $k \in \mathbb{Z}$. Τότε $x = 3(4k)$ και άρα $x \in 3\mathbb{Z}$ και $x = 4(3k)$ και άρα $x \in 4\mathbb{Z}$. Επομένως $x \in 3\mathbb{Z} \cap 4\mathbb{Z}$ και έτσι $12\mathbb{Z} \subseteq 3\mathbb{Z} \cap 4\mathbb{Z}$.

Συνοψίζοντας θα έχουμε

$$3\mathbb{Z} \cap 4\mathbb{Z} = 12\mathbb{Z} \qquad \text{και άρα} \qquad 3\mathbb{Z}/(3\mathbb{Z} \cap 4\mathbb{Z}) = 3\mathbb{Z}/12\mathbb{Z} \tag{$***$}$$

Συνδυάζοντας τις σχέσεις $(*), (**), (***)$ θα έχουμε έναν ισομορφισμό:

$$3\mathbb{Z}/12\mathbb{Z} \ \cong\ \mathbb{Z}_4 \qquad \surd$$

■

Πρόβλημα. *Ως γενίκευση της Εφαρμογής της Άσκησης 19, να εξετάσετε αν υπάρχει ισομορφισμός*

$$[n, m]\mathbb{Z} \,/\, m\mathbb{Z} \ \cong\ n\mathbb{Z} \,/\, (n, m)\mathbb{Z}$$

όπου $n, m \in \mathbb{Z}^+$. $\surd$

Άσκηση 20. (1) *Έστω G μια ομάδα και $g \in G$. Να δείξετε ότι η απεικόνιση*

$$\mathsf{i}_g : G \longrightarrow G, \quad x \longmapsto \mathsf{i}_g(x) = gxg^{-1}$$

είναι αυτομορφισμός, ο οποίος καλείται **ο εσωτερικός αυτομορφισμός της** G **ο οποίος αντιστοιχεί στο** g.

(2) *Υπολογίστε τις υποομάδες $i_{(123)}(H)$ και $\mathsf{i}_{(23)}(K)$ για τις υποομάδες $H = \langle(12)\rangle$ και $K = \langle(132)\rangle$ της ομάδας S_3.*

Λύση. (1) • Η απεικόνιση i_g είναι ομομορφισμός, διότι:

$$\mathsf{i}_g(xy) = g(xy)g^{-1} = gxyg^{-1} = gxeyg^{-1} = gxg^{-1}gyg^{-1} = \mathsf{i}_g(x)\mathsf{i}_g(y)$$

• Η απεικόνιση i_g είναι επιμορφισμός, διότι:

$$\forall y \in G, \ \ \exists\, g^{-1}yg \in G : \ \ \mathsf{i}_g(g^{-1}yg) = g(g^{-1}yg)g^{-1} = (gg^{-1})y(gg^{-1}) = eye = y$$

• Η απεικόνιση i_g είναι μονομορφισμός, διότι:

$$\mathsf{Ker}(\mathsf{i}_g) = \big\{x \in G \mid \mathsf{i}_g(x) = e\big\} = \big\{x \in G \mid gxg^{-1} = e\big\} = \big\{x \in G \mid gx = g\big\} = \big\{x \in G \mid x = e\big\} = \{e\}$$

Επομένως η απεικόνιση i_g είναι αυτομορφισμός της G.

(2) Θα υπολογίσουμε τον εσωτερικό αυτομορφισμό $\mathsf{i}_{(123)}(H)$ για την υποομάδα $H = \{(1), (12)\}$ της ομάδας S_3. Έχουμε:
- $\mathsf{i}_{(123)}((1)) = (123)(1)(123)^{-1} = (123)(123)^{-1} = (1)$
- $\mathsf{i}_{(123)}((12)) = (123)(12)(123)^{-1} = (13)(123)^{-1} = (13)(132) = (23)$

Άρα $\mathsf{i}_{(123)}(H) = \big\{(1), (23)\big\}$

Θα υπολογίσουμε τον εσωτερικό αυτομορφισμό $i_{(23)}(K)$ για την υποομάδα $K = \{(1), (132)\}$ της ομάδας S_3. Έχουμε:
- $\mathsf{i}_{(23)}((1)) = (23)(1)(23)^{-1} = (23)(23)^{-1} = (1)$
- $\mathsf{i}_{(23)}((132)) = (23)(132)(23)^{-1} = (23)(132)(23) = (12)(23) = (123)$

Άρα $\mathsf{i}_{(123)}(K) = \big\{(1), (123)\big\}$. ∎

Άσκηση 21. *Έστω G μια πολλαπλασιαστική ομάδα και $\emptyset \neq S \subseteq G$ ένα μη-κενό υποσύνολο της G.*

(1) *Το υποσύνολο*

$$\langle S\rangle = \bigcap \big\{H \leq G \mid S \subseteq H\big\}$$

είναι η μικρότερη υποομάδα της G η οποία περιέχει το S.

Η υποομάδα $\langle S\rangle$ καλείται **η υποομάδα της** G **η οποία παράγεται από το** S.

(2) *Να δείξετε ότι:*

$$\langle S\rangle = \big\{s_1^{a_1}s_2^{a_2}\cdots s_n^{a_n} \in G \ \mid \ n \geq 0, \ \ a_i \in \mathbb{Z}, \ \ s_i \in S\big\}$$

Αν η ομάδα G είναι προσθετική, τότε η παραπάνω ισότητα έχει την ακόλουθη μορφή:

$$\langle S\rangle = \big\{a_1s_1 + a_2s_2 + \cdots + a_ns_n \in G \ \mid \ n \geq 0, \ \ a_i \in \mathbb{Z}, \ \ s_i \in S\big\}$$

Λύση. (1) Η συλλογή υποομάδων $\big\{H \leq G \mid S \subseteq H\big\}$ της G είναι μη-κενή διότι διότι περιέχει την υποομάδα G. Έτσι το σύνολο $\langle S\rangle = \bigcap\big\{H \leq G \mid S \subseteq H\big\}$, ως τομή υποομάδων της G είναι μια υποομάδα της G. Αν $K \leq G$ και $S \subseteq K$, τότε η υποομάδα K ανήκει στην συλλογή $\big\{H \leq G \mid S \subseteq H\big\}$ και αρα $\langle S\rangle = \bigcap\big\{H \leq G \mid S \subseteq H\big\} \subseteq K$. Επομένως πράγματι η υποομάδα $\langle S\rangle$ είναι η μικρότερη υποομάδα της G η οποία περιέχει το υποσύνολο S.

(2) Θέτουμε: $R = \big\{ s_1^{a_1} s_2^{a_2} \cdots s_n^{a_n} \in G \ \mid \ n \geq 0, \ \ a_i \in \mathbb{Z}, \ \ s_i \in S \big\}$.

Αν H είναι μια υποομάδα της G η οποία περιέχει το S, τότε προφανώς η H θα περιέχει και κάθε στοιχείο της μορφής $s_1^{a_1} s_2^{a_2} \cdots s_n^{a_n}$, όπου $n \geq 0$, $a_i \in \mathbb{Z}$, και $s_i \in S$. Επομένως κάθε στοιχείο του συνόλου R ανήκιε σε κάθε υποομάδα H της G η οποία περιέχει το S, και άρα:

$$R \ \subseteq \ \langle S \rangle$$

Αντίστροφα, αν δείξουμε ότι το υποσύνολο R αποτελεί μια υποομάδα της G, τότε επειδή προφανώς $S \subseteq R$, θα έχουμε ότι $\langle S \rangle \subseteq R$, και επομένως $R = \langle S \rangle$. Το υποσύνολο R είναι υποομάδα, διότι:

- Είναι $R \neq \emptyset$, διότι $S \subseteq R$.
- Έστω $x, y \in R$. Τότε

  $$x = s_1^{a_1} s_2^{a_2} \cdots s_n^{a_n} \quad \text{και} \quad y = t_1^{b_1} t_2^{b_2} \cdots t_m^{b_m}, \quad \text{όπου} \quad n, m \geq 0, \ \ a_i, b_j \in \mathbb{Z}, \ \ s_i, t_j \in S$$

  Τότε:

  $$xy^{-1} = s_1^{a_1} s_2^{a_2} \cdots s_n^{a_n} (t_m^{b_m})^{-1} \cdots (t_2^{b_2})^{-1} (t_1^{b_1})^{-1} = s_1^{a_1} s_2^{a_2} \cdots s_n^{a_n} t_m^{-b_m} \cdots (t_2^{-b_2} t_1^{-b_1} \ \ \in \ \ R$$

  Επομένως το υποσύνολο R αποτελεί μια υποομάδα της G. ∎

Άσκηση 22. (1) *Έστω S ένα πεπερασμένο σύνολο στοιχείων της προσθετικής αβελιανής ομάδας $\mathbb{Q}$. Να δείξετε ότι η υποομάδα $\langle S \rangle$ η οποία παράγεται από το S είναι άπειρη κυκλική.*

(2) *Έστω T ένα πεπερασμένο σύνολο στοιχείων της προσθετικής αβελιανής ομάδας $\mathbb{Q}/\mathbb{Z}$. Να δείξετε ότι η υποομάδα $\langle T \rangle$ η οποία παράγεται από το T είναι πεπερασμένη κυκλική.*

Λύση. (1) Θεωρούμε ένα πεπερασμένο υποσύνολο

$$S = \Big\{ \frac{a_1}{b_1}, \ \frac{a_2}{b_2}, \ \cdots \ , \ \frac{a_k}{b_k} \Big\} \ \subseteq \ \mathbb{Q}$$

Τότε η υποομάδα της $\mathbb{Q}$ η οποία παράγεται από το S είναι:

$$\langle S \rangle = \left\{ n_1 \frac{a_1}{b_1} + n_2 \frac{a_2}{b_2} + \cdots + n_k \frac{a_k}{b_k} \ \in \ \mathbb{Q} \ \mid \ \ n_i \in \mathbb{Z} \right\}$$

Έστω

$$x = n_1 \frac{a_1}{b_1} + n_2 \frac{a_2}{b_2} + \cdots + n_k \frac{a_k}{b_k}$$

ένα τυχόν στοιχείο της $\langle S \rangle$. Θέτουμε:

$$c_1 = b_2 b_3 \cdots b_k, \quad c_2 = b_1 b_3 \cdots b_k, \quad \cdots \ , \quad c_k = b_1 b_2 \cdots b_{k-1}$$

Τότε

$$x = n_1 \frac{a_1}{b_1} + n_2 \frac{a_2}{b_2} + \cdots + n_k \frac{a_k}{b_k} = \frac{n_1 c_1 a_1 + n_2 c_2 a_2 + \cdots + n_k c_k a_k}{b_1 b_2 \cdots b_k} \tag{†}$$

Ο αριθμητής του παραπάνω κλάσματος ανήκει στην υπομμάδα της $\mathbb{Z}$ η οποία παράγεται από τα στοιχεία $\big\{ c_1 a_1, \ c_2 a_2, \ \cdots \ , \ c_k a_k \big\}$:

$$n_1 c_1 a_1 + n_2 c_2 a_2 + \cdots + n_k c_k a_k \ \in \ \langle c_1 a_1, \ c_2 a_2, \ \cdots \ , \ c_k a_k \rangle$$

Επειδή όλες οι υποομάδες της προσθετικής ομάδας $\mathbb{Z}$ είναι κυκλικές, έπεται ότι υπάρχει $\xi \in \mathbb{Z}$:

$$\langle c_1 a_1, \ c_2 a_2, \ \cdots \ , \ c_k a_k \rangle \ = \ \langle \xi \rangle$$

και άρα ο αριθμητής στο κλάσμα (†) γράφεται:

$$n_1 c_1 a_1 + n_2 c_2 a_2 + \cdots + n_k c_k a_k = \rho \, \xi \qquad \text{για κάποιο} \quad \rho \in \mathbb{Z} \tag{$*$}$$

και επομένως η σχέση (†) γράφεται

$$x = n_1 \frac{a_1}{b_1} + n_2 \frac{a_2}{b_2} + \cdots + n_k \frac{a_k}{b_k} = \rho \, \frac{\xi}{b_1 b_2 \cdots b_k}$$

Αυτό σημαίνει ότι το τυχόν στοιχείο $x \in \langle S \rangle$ ανήκει στην κυκλική υποομάδα της $\mathbb{Q}$ η οποία παράγεται από το στοιχείο

$$\frac{\xi}{b_1 b_2 \cdots b_k} \ \in \ \mathbb{Q}$$

και άρα:

$$\langle S \rangle = \Big\{ n_1 \frac{a_1}{b_1} + n_2 \frac{a_2}{b_2} + \cdots + n_k \frac{a_k}{b_k} \ \in \ \mathbb{Q} \ \mid \ n_i \in \mathbb{Z} \Big\} \ \subseteq \ \Big\langle \frac{\xi}{b_1 b_2 \cdots b_k} \Big\rangle$$

Αντίστροφα αν

$$x \ \in \ \Big\langle \frac{\xi}{b_1 b_2 \cdots b_k} \Big\rangle$$

τότε υπάρχει $z \in \mathbb{Z}$ έτσι ώστε:

$$x = z \frac{\xi}{b_1 b_2 \cdots b_k} = \frac{z\xi}{b_1 b_2 \cdots b_k}$$

Από την σχέση $(*)$, θα έχουμε ότι $\xi \in \langle c_1 a_1, \ c_2 a_2, \ \cdots, \ c_k a_k \rangle$ και άρα υπάρχουν ακέραιοι $m_1, m_2, \cdots, m_k$ έτσι ώστε:

$$\xi = m_1 c_1 a_1 + m_2 c_2 a_2 + \cdots + m_k c_k a_k$$

και τότε:

$$\begin{aligned}
x = \frac{z\xi}{b_1 b_2 \cdots b_k} \ &= \ \frac{z m_1 c_1 a_1 + z m_2 c_2 a_2 + \cdots + z m_k c_k a_k}{b_1 b_2 \cdots b_k} \\
&= \ \frac{z m_1 c_1 a_1}{b_1 b_2 \cdots b_k} + \frac{z m_2 c_2 a_2}{b_1 b_2 \cdots b_k} + \cdots + \frac{z m_k c_k a_k}{b_1 b_2 \cdots b_k} \\
&= \ \frac{z m_1 b_2 b_3 \cdots b_k a_1}{b_1 b_2 \cdots b_k} + \frac{z m_2 b_1 b_3 \cdots b_k a_2}{b_1 b_2 \cdots b_k} + \cdots + \frac{z m_k b_1 b_2 \cdots b_{k-1} a_k}{b_1 b_2 \cdots b_k} \\
&= \ \frac{z m_1 a_1}{b_1} + \frac{z m_2 a_2}{b_2} + \cdots + \frac{z m_k a_k}{b_k} \\
&= \ z m_1 \, \frac{a_1}{b_1} + z m_2 \, \frac{a_2}{b_2} + \cdots + z m_k \, \frac{a_k}{b_k} \ \in \ \Big\langle \frac{a_1}{b_1}, \ \frac{a_2}{b_2}, \ \cdots, \ \frac{a_k}{b_k} \Big\rangle
\end{aligned}$$

Άρα:

$$\Big\langle \frac{\xi}{b_1 b_2 \cdots b_k} \Big\rangle \ \subseteq \ \langle S \rangle = \Big\{ n_1 \frac{a_1}{b_1} + n_2 \frac{a_2}{b_2} + \cdots + n_k \frac{a_k}{b_k} \ \in \ \mathbb{Q} \ \mid \ n_i \in \mathbb{Z} \Big\}$$

και επομένως καταλήγουμε ότι:

$$\langle S \rangle = \Big\{ n_1 \frac{a_1}{b_1} + n_2 \frac{a_2}{b_2} + \cdots + n_k \frac{a_k}{b_k} \ \in \ \mathbb{Q} \ \mid \ n_i \in \mathbb{Z} \Big\} \ = \ \Big\langle \frac{\xi}{b_1 b_2 \cdots b_k} \Big\rangle$$

δηλαδή η υποομάδα της προσθετικής ομάδας $\mathbb{Q}$ η οποία παράγεται από το σύνολο S είναι κυκλική με γεννήτορα τον ρητό αριθμό $\frac{\xi}{b_1 b_2 \cdots b_k}$. Επειδή από την σχέση $(*)$ ο ακέραιος ξ είναι γεννήτορας μιας κυκλικής υποομάδας της προσθετικής ομάδας $\mathbb{Z}$ και επειδή κάθε μη-τετριμμένη (κυκλική) υποομάδα της $\mathbb{Z}$ είναι άπειρη, έπεται ότι το στοιχείο $\frac{\xi}{b_1 b_2 \cdots b_k}$ έχει άπειρη τάξη και άρα η υποομάδα $\langle S \rangle$ είναι άπειρη.

(2) Θεωρούμε ένα πεπερασμένο υποσύνολο

$$T = \left\{\frac{a_1}{b_1} + \mathbb{Z},\ \frac{a_2}{b_2} + \mathbb{Z},\ \cdots,\ \frac{a_k}{b_k} + \mathbb{Z}\right\} \subseteq \mathbb{Q}/\mathbb{Z}$$

Θέτοντας

$$S = \left\{\frac{a_1}{b_1},\ \frac{a_2}{b_2},\ \cdots,\ \frac{a_k}{b_k}\right\} \subseteq \mathbb{Q}$$

έπεται ότι θα έχουμε:

$$\langle T\rangle = \langle S\rangle + \mathbb{Z}$$

και άρα σύμφωνα με το (1), θα έχουμε ότι η υποομάδα της $\mathbb{Q}$ η οποία παράγεται από το S είναι η κυκλική ομάδα:

$$\langle S\rangle = \left\langle \frac{\xi}{b_1 b_2 \cdots b_k}\right\rangle$$

για κάποιο $\xi \in \mathbb{Z}$.

Αυτό όμως προφανώς σημαίνει ότι το στοιχείο $\frac{\xi}{b_1 b_2 \cdots b_k} + \mathbb{Z}$ είναι γεννήτορας της ομάδας $\langle T\rangle$, και επομένως:

$$\langle T\rangle = \left\langle \frac{\xi}{b_1 b_2 \cdots b_k} + \mathbb{Z}\right\rangle$$

Άρα η υποομάδα $\langle T\rangle$ της $\mathbb{Q}/\mathbb{Z}$ η οποία παράγεται από το σύνολο T είναι κυκλική με γεννήτορα το στοιχείο $\frac{\xi}{b_1 b_2 \cdots b_k} + \mathbb{Z}$. Επειδή

$$b_1 b_2 \cdots b_k \cdot \big(\frac{1}{b_1 b_2 \cdots b_k} + \mathbb{Z}\big) = 1 + \mathbb{Z} = \mathbb{Z}$$

ο γεννήτορας της $\langle T\rangle$ έχει πεπερασμένη τάξη και επομένως η κυκλική υποομάδα $\langle T\rangle$ είναι πεπερασμένη. ■

Παρατήρηση. *Μια (προσθετική) αβελιανή ομάδα G καλείται* **τοπικά κυκλική** *αν η υποομάδα η οποία παράγεται από κάθε πεπερασμένο υποσύνολο της G είναι κυκλική.*

Σύμφωνα με την Άσκηση 22, οι αβελιανές ομάδες $\mathbb{Q}$ και $\mathbb{Q}/\mathbb{Z}$ είναι τοπικά κυκλικές. Αντίστροφα αποδεικνύεται ότι κάθε τοπικά κυκλική ομάδα είνα υποομάδα είτε της $\mathbb{Q}$ ή της $\mathbb{Q}/\mathbb{Z}$.

Αν G είναι μια τοπικά κυκλική (αβελιανή) ομάδα, τότε:

(1) *είτε κάθε στοιχείο της G έχει πεπερασμένη τάξη*
(2) *ή κάθε μη-ταυτοτικό στοιχείο της G έχει άπειρη τάξη.*

Βλέπετε γιατί; ▲

Άσκηση 23. *Να δοθούν παραδείγματα:*

(1) *Άπειρης ομάδας G, όλα τα στοιχεία της οποίας έχουν πεπερασμένη τάξη.*
(2) *Ομάδας G η οποία να μην έχει στοιχεία πεπερασμένης τάξης > 1 αλλά να έχει μια ομάδα-πηλίκο G/H, της οποίας όλα τα στοιχεία να έχουν πεπερασμένη τάξη.*
(3) *Άπειρης ομάδας G η οποία να έχει μια κανονική υποομάδα H όλα τα στοιχεία της οποίας έχουν πεπερασμένη τάξη, και η ομάδα πηλίκο G/H να μην έχει στοιχεία πεπερασμένης τάξης.*

Λύση. (1) Θεωρούμε την προσθετική αβελιανή ομάδα $\mathbb{Q}/\mathbb{Z}$.

Τότε η ομάδα $\mathbb{Q}/\mathbb{Z}$ είναι άπειρη διότι, όπως μπορούμε να δούμε πολύ εύκολα, το σύνολο

$$\{\frac{1}{n} + \mathbb{Z} \ \in \ \mathbb{Q}/\mathbb{Z} \mid n \in \mathbb{N}\}$$

είναι άπειρο. Από την άλλη πλευρά θεωρούμε τυχόν μη-μηδενικό στοιχείο $x+\mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$, όπου $x \in \mathbb{Q}$ και προφανώς μπορούμε να υποθέσουμε ότι $x = \frac{p}{q}$, όπου $q > 0$, $p \in \mathbb{Z}$. Τότε:

$$q(\frac{p}{q} + \mathbb{Z}) = q\frac{p}{q} + \mathbb{Z} = p + \mathbb{Z} = \mathbb{Z} \quad \Longrightarrow \quad \mathsf{o}(\frac{p}{q} + \mathbb{Z}) < \infty$$

Άρα κάθε στοιχείο της $\mathbb{Q}/\mathbb{Z}$ έχει πεπερασμένη τάξη.

(2) Η προσθετική ομάδα $\mathbb{Q}$ των ρητών αριθμών, δεν έχει προφανώς κανένα μη-ταυτοτικό στοιχείο πεπερασμένης τάξης. Η υποομάδα $\mathbb{Z}$ της $\mathbb{Q}$ είναι κανονική διότι η $\mathbb{Q}$ είναι αβελιανή, και όπως είδαμε στο (1), κάθε στοιχείο της ομάδας πηλίκο $\mathbb{Q}/\mathbb{Z}$ έχει πεπερασμένη τάξη.

(3) Θεωρούμε την ομάδα πηλίκο $\mathbb{R}/\mathbb{Z}$ η οποία είναι προφανώς άπειρη. Έστω $r + \mathbb{Z}$ ένα τυχόν στοιχείο της $\mathbb{R}/\mathbb{Z}$. Τότε:

$$\mathsf{o}(r + \mathbb{Z}) < \infty \iff \exists\, n \geq 1 : \ n(r + \mathbb{Z}) = Z \iff \exists\, n \geq 1 : \ nr + \mathbb{Z} = \mathbb{Z} \iff$$
$$\exists\, n \geq 1 : \ nr \in \mathbb{Z} \iff \exists\, n \geq 1 : nr = s \in \mathbb{Z} \iff \exists\, n \geq 1 : r = \frac{s}{n} \iff r \ \in \ \mathbb{Q}$$

Άρα κάθε στοιχείο της υποομάδας $\mathbb{Q}/\mathbb{Z}$ της $\mathbb{R}/\mathbb{Z}$ έχει πεπερασμένη τάξη. Από το Τρίτο Θεώρημα Ισοιμορφισμών, για την ομάδα πηλίκο θα έχουμε:

$$\mathbb{R}/\mathbb{Z}/\mathbb{Q}/\mathbb{Z} \ \cong \ \mathbb{R}/\mathbb{Q}$$

Τότε:

$$\mathsf{o}(r + \mathbb{Q}) < \infty \iff \exists\, n \geq 1 : \ n(r + \mathbb{Q}) = \mathbb{Q} \iff \exists\, n \geq 1 : \ nr + \mathbb{Q} = \mathbb{Q} \iff$$
$$\exists\, n \geq 1 : \ nr \in \mathbb{Q} \iff \exists\, n \geq 1 : nr = \frac{p}{q} \in \mathbb{Q} \iff \exists\, n \geq 1 : r = \frac{p}{nq} \iff r \ \in \ \mathbb{Q}$$

και επομένως το μόνο στοιχείο της ομάδας πηλίκο $\mathbb{R}/\mathbb{Q}$ με πεπερασμένη τάξη είναι το μηδενικό. ■