ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ Ι

Ακαδημαϊκο Ετος 2023-2024

Επιλυση Ασκησεων - Φυλλαδιο 3

Διδασκων: Α. Μπελληγιάννης

ΙΣΤΟΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ

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

Πέμπτη 28 Μαρτίου 2024

Υπενθυμίζουμε ότι μια ομάδα $(G,\cdot)$ καλείται **κυκλική** αν υπάρχει ένα στοιχείο $a\in G$ έτσι ώστε η G συμπίπτει με την κυκλική υποομάδα $\langle a\rangle=\{a^n\in G\mid n\in\mathbb{Z}\}$ της G η οποία παράγεται από το a.

Σε μια κυκλική ομάδα G, κάθε στοιχείο $a\in G$ με την ιδιότητα $G=\langle a\rangle$ καλείται **γεννήτορας** της G.

Άσκηση 1. Αν $n\geqslant 1$ είναι ένας φυσικός αριθμός, να δειχθεί ότι το σύνολο U_n των n-οστών ριζών της μονάδας, δηλαδή

$$\mathsf{U}_n=\{z\in\mathbb{C}\mid z^n=1\}$$

αποτελεί υποομάδα της πολλαπλασιαστικής ομάδας $(\mathbb{C}^*,\cdot)$ των μη-μηδενικών μιγαδικών αριθμών. Ακολούθως να δειχθεί ότι η ομάδα $(\mathsf{U}_n,\cdot)$ είναι κυκλική τάξης n.

Λύση. Προφανώς $\mathsf{U}_n\subseteq\mathbb{C}^*$ διότι κάθε στοιχείο $z\in\mathsf{U}_n$ ικανοποιεί τη σχέση $z^n=1$ και άρα $z\neq 0$. Επιπλέον $\mathsf{U}_n\neq\varnothing$ διότι $1\in\mathsf{U}_n$. Αν $z_1,z_2\in\mathsf{U}_n$, τότε $z_1^n=1=z_2^n$ και επομένως $(z_1\,z_2^{-1})^n=z_1^n\,\frac{1}{z_2^n}=1$. Άρα $z_1\,z_2^{-1}\in\mathsf{U}_n$ και επομένως το υποσύνολο U_n είναι υποομάδα της $(\mathbb{C}^*,\cdot)$.

Για να δείξουμε ότι η ομάδα $(\mathsf{U}_n,\cdot)$ είναι κυκλική, δείχνουμε πρώτα ότι

$$\mathsf{U}_n=\left\{e^{\frac{2k\pi i}{n}}\in\mathbb{C}\mid 0\leqslant k<n\right\}=\left\{\cos(\frac{2k\pi}{n})+i\sin(\frac{2k\pi}{n})\in\mathbb{C}\mid 0\leqslant k<n\right\}\qquad(*)$$

Πράγματι, αν z είναι ένας μιγαδικός αριθμός, τότε θεωρούμε την πολική/τριγωνομετρική αναπαράστασή του

$$z=re^{i\theta}=r(\cos\theta+i\sin\theta),\qquad r=|z|\quad\&\quad\theta=\arg z$$

Υπενθυμίζουμε ότι αν z_1 και z_2 είναι μη-μηδενικοί μιγαδικοί αριθμοί με αναπαραστάσεις

$$z_1=r_1e^{i\theta_1}=r_1(\cos\theta_1+i\sin\theta_1)\quad\&\quad z_2=r_2e^{i\theta_2}=r_2(\cos\theta_2+i\sin\theta_2)$$

τότε:

$$z_1z_2=r_1r_2e^{i(\theta_1+\theta_2)}=r_1r_2(\cos(\theta_1+\theta_2)+i\sin(\theta_1+\theta_2))$$

και άρα $z^n=r^ne^{in\theta}=r^n(\cos(n\theta)+i\sin(n\theta))$. Επομένως αν $z\in\mathsf{U}_n$, θα έχουμε $z^n=1$ και άρα $|z|^n=1$, απ' όπου βλέπουμε $|z|=r=1$, και επίσης $z^n=e^{in\theta}=\cos(n\theta)+i\sin(n\theta)=e^0=1$. Τότε προφανώς θα έχουμε $n\theta=2k\pi$, για έναν ακέραιο $k\in\mathbb{Z}$. Επομένως αν $z\in\mathsf{U}_n$, τότε $z=e^{\frac{2k\pi i}{n}}=\cos(\frac{2k\pi}{n})+i\sin(\frac{2k\pi}{n})$. Αντίστροφα αν $z=e^{\frac{2k\pi i}{n}}=\cos(\frac{2k\pi}{n})+i\sin(\frac{2k\pi}{n})$, τότε $z^n=(e^{\frac{2k\pi i}{n}})^n=e^{\frac{2kn\pi i}{n}}=e^{2k\pi i}=\cos(2k\pi)+i\sin(2k\pi)=1$, δηλαδή $z\in\mathsf{U}_n$. Επομένως

$$\mathsf{U}_n=\left\{e^{\frac{2k\pi i}{n}}\in\mathbb{C}\mid k\in\mathbb{Z}\right\}=\left\{\cos(\frac{2k\pi}{n})+i\sin(\frac{2k\pi}{n})\in\mathbb{C}\mid k\in\mathbb{Z}\right\}$$

Από τις παραπάνω σχέσεις έπεται ότι $\left\{e^{\frac{2k\pi i}{n}} \in \mathbb{C} \mid 0 \leqslant k < n \in \mathbb{Z}\right\} = \left\{\cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n}) \in \mathbb{C} \mid 0 \leqslant k < n\right\} \subseteq \mathsf{U}_n$. Έστω τώρα $z \in \mathsf{U}_n$ και επομένως $z = e^{\frac{2k\pi i}{n}}$ για κάποιο $k \in \mathbb{Z}$. Από την Ευκλείδεια διαίρεση του k με το n, θα έχουμε $k = nq + r$, όπου $0 \leqslant r < n$, και επομένως

$$z = e^{\frac{2k\pi i}{n}} = e^{\frac{2(nq+r)\pi i}{n}} = e^{\frac{2nq\pi i + 2r\pi i}{n}} = e^{\frac{2nq\pi i}{n}} \cdot e^{\frac{2r\pi i}{n}} = e^{2q\pi i} \cdot e^{\frac{2r\pi i}{n}} = 1 \cdot e^{\frac{2r\pi i}{n}} = e^{\frac{2r\pi i}{n}}, \qquad 0 \leqslant r < n$$

Επομένως θα έχουμε:

$$\mathsf{U}_n = \left\{e^{\frac{2k\pi i}{n}} \in \mathbb{C} \mid 0 \leqslant k < n\right\} = \left\{\cos(\frac{2k\pi}{n}) + i\sin(\frac{2k\pi}{n}) \in \mathbb{C} \mid 0 \leqslant k < n\right\}$$

Θεωρούμε τώρα έναν φυσικό αριθμό k όπου $1 \leqslant k < n$ και $(k, n) = 1$. Θα δείξουμε ότι το στοιχείο $w = e^{\frac{2k\pi i}{n}}$ είναι ένας γεννήτορας της U_n, δηλαδή:

$$\mathsf{U}_n = \langle e^{\frac{2k\pi i}{n}} \rangle$$

Έστω $z = e^{\frac{2l\pi i}{n}} \in \mathsf{U}_n$, όπου $0 \leqslant l < n$. Θα δείξουμε ότι $z = e^{\frac{2l\pi i}{n}} = w^m = e^{\frac{2km\pi i}{n}}$, για κατάλληλο $m \in \mathbb{Z}$. Επειδή $(k, n) = 1$, υπάρχουν ακέραιοι x, y έτσι ώστε $1 = kx + ny$. Τότε $l = klx + nly$, και θέτοντας $m = lx$, θα έχουμε:

$$z = e^{\frac{2l\pi i}{n}} = e^{\frac{2(klx+nly)\pi i}{n}} = e^{\frac{2klx\pi i + 2nly\pi i}{n}} = e^{\frac{2klx\pi i}{n}} \cdot e^{\frac{2nly\pi i}{n}} = e^{\frac{2klx\pi i}{n}} \cdot e^{2ly\pi i} =$$
$$= e^{\frac{2klx\pi i}{n}} \cdot 1 = (e^{\frac{2k\pi i}{n}})^{lx} = w^{lx} = w^m$$

Άρα το τυχαίο στοιχείο $z \in \mathsf{U}_n$ ανήκει στην κυκλική υποομάδα $\langle w \rangle$ της U_n η οποία παράγεται από το w και επομένως $\mathsf{U}_n = \langle w \rangle$, δηλαδή η U_n είναι κυκλική. ■

Παρατήρηση. *Από την παραπάνω Άσκηση 1 έπεται ιδιαίτερα ότι θέτοντας* $\zeta_n = e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n} + i\sin(\frac{2\pi}{n}))$, *θα έχουμε:*

$$\mathsf{U}_n = \langle \zeta_n \rangle = \left\{\zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}, \zeta_n^n\right\} \quad ▲$$

Άσκηση 2. (1) Ας είναι T το σύνολο των μιγαδικών αριθμών με μέτρο ίσο με 1, δηλαδή

$$\mathsf{T} = \left\{z \in \mathbb{C} \mid |z| = 1\right\}$$

Να δειχθεί ότι το T αποτελεί υποομάδα τής ομάδας $(\mathbb{C}^\star, \cdot)$.

(2) Να δείξετε ότι το υποσύνολο U των μιγαδικών αριθμών z με $z^n = 1$, για κάποιο $n \in \mathbb{N}$, δηλαδή

$$\mathsf{U} = \left\{z \in \mathbb{C} \mid \exists\, n \in \mathbb{N} :\ z^n = 1\right\}$$

αποτελεί υποομάδα τής $(\mathsf{T}, \cdot)$.

(3) Να δείξετε ότι: (α) η ομάδα $(\mathsf{U}_n, \cdot)$ είναι υποομάδα της ομάδας $(\mathsf{U}, \cdot)$, (β) ισχύει ότι $\mathsf{U} = \bigcup_{n=1}^{\infty} \mathsf{U}_n$, και (γ) η ομάδα U δεν είναι κυκλική.

Λύση. (1) Προφανώς $\mathsf{T} \subseteq \mathbb{C}^*$, διότι $z \neq 0$, $\forall z \in \mathsf{T}$. Επιπλέον Θα έχουμε $\mathsf{T} \neq \varnothing$ διότι $1 \in \mathsf{T}$.
Έστω $z_1, z_2 \in \mathsf{T}$. Τότε $z_1 \neq 0 \neq z_2$, ιδιαίτερα $|z_2| \neq 0$, και θα έχουμε:

$$|z_1 \cdot z_2^{-1}| = |z_1| \cdot |z_2^{-1}| = |z_1| \cdot |\frac{1}{z_2}| = |z_1| \cdot \frac{1}{|z_2|} = 1 \cdot 1 = 1 \quad \Longrightarrow \quad z_1 \cdot z_2^{-1} \in \mathsf{T}$$

Άρα, σύμφωνα με γνωστό κριτήριο, το σύνολο T είναι υποομάδα τής ομάδας $(\mathbb{C}^\star, \cdot)$.

(2) Προφανώς $\mathsf{U} \neq \varnothing$ διότι $1 \in \mathsf{U}$. Επιπλέον αν $z \in \mathsf{U}$, τότε $z^n = 1$ για κάποιον θετικό ακέραιο n, και επομένως $|z^n| = |z|^n = 1$. Επειδή ο πραγματικός αριθμός $|z|$ είναι θετικός, έπεται ότι $|z| = 1$ και επομένως $z \in \mathsf{T}$. Άρα $\mathsf{U} \subseteq \mathsf{T}$.

Έστω $z_1, z_2 \in \mathsf{U}$. Τότε υπάρχουν $n_1 \in \mathbb{N}$ και $n_2 \in \mathbb{N}$ έτσι ώστε $z_1^{n_1} = 1$ και $z_2^{n_2} = 1$. Τότε $z_2 \neq 0$ και θέτοντας $n = n_1 \cdot n_2$, θα έχουμε:

$$(z_1 z_2^{-1})^n = (z_1 \cdot \frac{1}{z_2})^{n_1 \cdot n_2} = \big((z_1)^{n_1}\big)^{n_2} \cdot \big((\frac{1}{z_2})^{n_2}\big)^{n_1} = 1^{n_2} \cdot 1^{n_1} = 1 \cdot 1 = 1 \quad \Longrightarrow \quad z_1 \cdot z_2^{-1} \in \mathsf{U}$$

Άρα, σύμφωνα με γνωστό κριτήριο, το σύνολο U αποτελεί υποομάδα τής $(\mathsf{T}, \cdot)$.

(3) Επειδή $\mathsf{U}_n \subseteq \mathsf{U} \subseteq \mathsf{T}$ και η U_n είναι υποομάδα της T, έπεται άμεσα ότι η U_n είναι υποομάδα της U.

Επειδή $\mathsf{U}_n \subseteq \mathsf{U}$, $\forall n \geqslant 1$, έπεται ότι $\bigcup_{n=1}^{\infty} \mathsf{U}_n \subseteq \mathsf{U}$. Αν $z \in \mathsf{U}$, τότε εξ' ορισμού υπάρχει θετικός ακέραιος n έτσι ώστε $z^n = 1$. Τότε προφανώς $z \in \mathsf{U}_n \subseteq \bigcup_{n=1}^{\infty} \mathsf{U}_n$ και επομένως $\mathsf{U} \subseteq \bigcup_{n=1}^{\infty} \mathsf{U}_n$. Έτσι τελικά θα έχουμε $\mathsf{U} = \bigcup_{n=1}^{\infty} \mathsf{U}_n$.

Υποθέτουμε ότι η ομάδα U είναι κυκλική, δηλαδή υπάρχει ένας μιγαδικός αριθμός $w \in \mathsf{U}$ έτσι ώστε $\mathsf{U} = \langle w \rangle$. Τότε προφανώς $w \in \mathsf{U}$ και επομένως $w \in \mathsf{U}_n$ για κάποιον θετικό ακέραιο n. Επειδή $\langle w \rangle \subseteq \mathsf{U}_n \subseteq \mathsf{U} = \langle w \rangle$, θα έχουμε $\mathsf{U} = \mathsf{U}_n = \langle w \rangle$. Τότε για κάθε $m > n$, και για κάθε στοιχείο $z \neq 1$ της U_m έτσι ώστε $\langle z \rangle = \mathsf{U}_m$, θα έχουμε ότι $z \in \mathsf{U} = \mathsf{U}_n$ και επομένως $z^n = 1$. Τότε όπως γνωρίζουμε από γνωστή Πρόταση, $\langle z \rangle = \{1, z \cdots, z^{n-1}\}$ και επομένως $m = |\mathsf{U}_m| = |\langle z \rangle| \leqslant n$ και αυτό είναι άτοπο. Άρα η ομάδα U δεν είναι κυκλική. ■

Παρατήρηση. (1) *Η ομάδα* T *καλείται η* **ομάδα του κύκλου**.

(2) *Ένας μιγαδικός αριθμός* z *καλείται* n-**οστή ρίζα της μονάδας**, *όπου* n *είναι ένας θετικός ακέραιος, αν* $z^n = 1$.

Μια n-**οστή ρίζα της μονάδας** z *καλείται* **πρωταρχική** n-**οστή ρίζα της μονάδας**, *όπου* n *είναι ένας θετικός ακέραιος, αν* $z^m \neq 1$, *για κάθε* $m < n$.

(3) *Η ομάδα* U_n *καλείται η ομάδα των* n-**οστών ριζών της μονάδας**. *Η ομάδα* U_n *είναι κυκλική, και μια* n-**οστή ρίζα της μονάδας** z *είναι γεννήτορας της* U_n, *δηλαδή* $\mathsf{U}_n = \langle z \rangle$, *αν και μόνον αν το* z *είναι πρωταρχική* n-**οστή ρίζα της μονάδας** *αν και μόνον αν υπάρχει* $1 \leqslant k < n$ *και* $(k, n) = 1$, *έτσι ώστε:* $z = e^{\frac{2k\pi i}{n}} = \cos(\frac{2k\pi i}{n}) + i \sin(\frac{2k\pi i}{n})$.

(4) *Η ομάδα* $\mathsf{U} = \bigcup_{n=1}^{\infty} \mathsf{U}_n$ *καλείται η* **ομάδα των ριζών της μονάδας**.

(5) *Ισχύουν οι εξής σχέσεις,* $\forall n \geqslant 1$*:*

$$\mathsf{U}_n \leqslant \mathsf{U} \leqslant \mathsf{T} \leqslant \mathbb{C}^* \quad \blacktriangle$$

Άσκηση 3. Έστω $(G, \cdot)$ μια ομάδα. Να δειχθεί ότι αν η ομάδα G είναι πεπερασμένη, τότε κάθε υποομάδα της είναι πεπερασμένη και η τάξη κάθε στοιχείου της είναι πεπερασμένη.

Να δοθεί παράδειγμα άπειρης ομάδας, κάθε στοιχείο της οποίας έχει πεπερασμένη τάξη.

Λύση. Έστω $|G| < \infty$ και $H \leqslant G$ μια υποομάδα της G. Τότε επειδή $H \subseteq G$, θα έχουμε $|H| \leqslant |G|$ και επομένως η H είναι επίσης πεπερασμένη ομάδα. Αν $a \in G$, τότε επειδή $\mathsf{o}(a) = |\langle a \rangle|$ και $\langle a \rangle \leqslant G$, θα έχουμε $\mathsf{o}(a) = |\langle a \rangle| \leqslant |G|$ και επομένως το στοιχείο a έχει πεπερασμένη τάξη.

Θεωρούμε την ομάδα $\mathsf{U} = \bigcup_{n=1}^{\infty} \mathsf{U}_n$ των ριζών της μονάδας. Τότε προφανώς η ομάδα U είναι άπειρη. Αν $a \in \mathsf{U}$, τότε υπάρχει $n \in \mathbb{N}$ έτσι ώστε $a \in \mathsf{U}_n$, και τότε $a^n = 1$. Αυτό, όπως γνωρίζουμε, σημαίνει ότι $\mathsf{o}(a) < \infty$, ακριβέστερα $\mathsf{o}(a) \mid n$. ■

Άσκηση 4. Για κάθε μια από τις παρακάτω ομάδες να βρεθούν τουλάχιστον δύο μη-τετριμμένες γνήσιες υποομάδες.

(1) $(\mathbb{Z}, +)$, (2) $(\mathbb{Q}, +)$, (3) $(\mathbb{C}^\star, \cdot)$, (4) $(8\mathbb{Z}, +)$, (5) $(\mathsf{S}_3, \circ)$, (6) $(\mathsf{GL}(2, \mathbb{Q}), \cdot)$.

Λύση. Θα έχουμε:

(1) Για την $(\mathbb{Z}, +)$:

$$H_1 = 2\mathbb{Z} = \langle 2 \rangle \quad \& \quad H_2 = 3\mathbb{Z} = \langle 3 \rangle$$

(2) Για την $(\mathbb{Q}, +)$:

$$H_1 = \mathbb{Z} \quad \& \quad H_2 = \Big\langle \frac{1}{2} \Big\rangle = \Big\{ \frac{n}{2} \in \mathbb{Q} \mid n \in \mathbb{Z} \Big\}$$

(3) Για την $(\mathbb{C}^\star, \cdot)$:

$$H_1 = \mathsf{T} \quad \& \quad H_2 = \mathsf{U}_n$$

(4) Για την $(8\mathbb{Z}, +)$:

$$H_1 = 16\mathbb{Z} = \langle 16 \rangle \quad \& \quad H_2 = 24\mathbb{Z} = \langle 24 \rangle$$

(5) Για την $(\mathsf{S}_3, \circ)$:

$$H_1 = \left\{ \iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\} = \langle \mu_1 \rangle$$

$$H_2 = \left\{ \iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} = \langle \rho_1 \rangle$$

(6) Για την $(\mathsf{GL}(2, \mathbb{Q}), \cdot)$:

$$H_1 = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\} = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$$

$$H_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\} = \left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$$

■

Άσκηση 5. Να προσδιορισθεί η κυκλική υποομάδα $\langle A \rangle$ της γενικής γραμμικής ομάδας $\mathsf{GL}(2, \mathbb{R})$ η οποία παράγεται από τον πίνακα A, όπου A είναι ένας εκ των πινάκων:

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

Είναι οι κυκλικές υποομάδες $\langle A \rangle$ υποομάδες της γενικής γραμμικής ομάδας $\mathsf{GL}(2, \mathbb{Z})$;

Λύση. (1) Για τον πίνακα $A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$, θα έχουμε:

$$A^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad A^3 = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \quad A^4 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad A^5 = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad A^6 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Επομένως, σύμφωνα με γνωστή Πρόταση[1]:

$$\langle A \rangle = \{ I_2,\ A,\ A^2,\ A^3,\ A^4,\ A^5 \}$$

(2) Για τον πίνακα $A = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$, θα έχουμε:

$$A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Επομένως, σύμφωνα με γνωστή Πρόταση:

$$\langle A \rangle = \{ I_2,\ A \}$$

(3) Για τον πίνακα $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, θα έχουμε:

$$A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \quad A^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}, \quad \text{και με επαγωγή:} \quad A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, \ \forall n \geqslant 0$$

Επειδή ο πίνακας A είναι αντιστρέψιμος και $A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, θα έχουμε

$$A^{-2} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}, \quad A^{-3} = \begin{pmatrix} 1 & -3 \\ 0 & 1 \end{pmatrix}, \quad \text{και με επαγωγή:} \quad A^{-n} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}, \ \forall n \geqslant 0$$

[1] Αν $(G = \langle a \rangle, \cdot)$ είναι μια κυκλική ομάδα και $\mathsf{o}(a) = n$, δηλαδή n είναι ο μικρότερος θετικός ακέραιος, ή 0 αν $G = \{e\}$, έτσι ώστε $a^n = e$, τότε $G = \{e, a, a^2, \cdots, a^{n-1}\}$.

Επομένως, σύμφωνα με γνωστή Πρόταση:

$$\langle A\rangle = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\}$$

(4) Για τον πίνακα $A = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$, θα έχουμε:

$$A^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}, \quad A^3 = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}, \quad A^4 = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}, \quad A^5 = \begin{pmatrix} 8 & 5 \\ 5 & 3 \end{pmatrix}, \quad \cdots$$

Θεωρούμε την ακολουθία Fibonacci $\{F_n\}_{n\geqslant 1}$:

$$F_1 = 1, \quad F_2 = 1, \quad F_3 = 2, \quad F_4 = 3, \quad F_5 = 5, \quad F_6 = 8, \quad \text{και γενικά}: \quad F_{n+1} = F_n + F_{n-1}, \quad \forall n \geqslant 2$$

Τότε εύκολα υπολογίζουμε με επαγωγή ότι:

$$A^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}, \quad \forall n \geqslant 1$$

όπου, χάριν ευκολίας, θέσαμε $F_0 = 0$. Υπολογίζουμε εύκολα ότι:

$$A^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}, \quad A^{-2} = \begin{pmatrix} 1 & -1 \\ -1 & 2 \end{pmatrix}, \quad A^{-3} = \begin{pmatrix} -1 & 2 \\ 2 & -3 \end{pmatrix}, \quad A^{-4} = \begin{pmatrix} 2 & -3 \\ -3 & 5 \end{pmatrix}, \quad \cdots$$

Χρησιμοποιώντας τη σχέση (η οποία είναι γνωστή από τη Θεωρία Αριθμών)

$$F_{n-1}F_{n+1} - F_n^2 = (-1)^n$$

και επαγωγή εύκολα βλέπουμε ότι:

$$A^{-n} = \begin{pmatrix} (-1)^n F_{n-1} & (-1)^{n+1} F_n \\ (-1)^{n+1} F_n & (-1)^n F_{n+1} \end{pmatrix} = (-1)^n \begin{pmatrix} F_{n-1} & -F_n \\ -F_n & F_{n+1} \end{pmatrix}, \quad \forall n \geqslant 1$$

Επομένως, θέτοντας χάριν ευκολίας $F_{-1} = 1$, θα έχουμε:

$$\langle A\rangle = \left\{ \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}, \ (-1)^m \begin{pmatrix} F_{m-1} & -F_m \\ -F_m & F_{m+1} \end{pmatrix}, \ \forall n \geqslant 0, \ \forall m \geqslant 1 \right\}$$

Παρατηρούμε ότι οι πίνακες A είναι πίνακες ακεραίων αριθμών, έχουν ορίζουσα ± 1 και άρα είναι αντιστρέψιμοι, και οι αντίστροφοι πίνακες A^{-1} είναι επίσης πίνακες ακεραίων αριθμών. Επειδή τα υποσύνολα $\langle A\rangle \subseteq \mathsf{GL}(2,\mathbb{Z})$ είναι μη-κενά, και είναι κλειστά στον πολλαπλασιασμό πινάκων, αυτό σημαίνει ότι $\langle A\rangle \leqslant \mathsf{GL}(2,\mathbb{Z})$. ■

Παρατήρηση. *Ο πίνακας* $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ *είναι ένας πίνακας ακέραιων αριθμών με ορίζουσα* $|A| = 3 \neq 0$, *αλλά ο αντίστροφός του* A^{-1}, *ο οποίος υπάρχει πάντα ως πίνακας ρητών αριθμών, δεν είναι πίνακας ακέραιων αριθμών διότι*

$$A^{-1} = \begin{pmatrix} \frac{2}{3} & -\frac{1}{3} \\ -\frac{1}{3} & \frac{2}{3} \end{pmatrix}$$

Έτσι $A^{-1} \in \mathsf{GL}(2,\mathbb{Q})$ *και* $A^{-1} \notin \mathsf{GL}(2,\mathbb{Z})$.

Γενικά, αν A *είναι ένας πίνακας με στοιχεία ακέραιους αριθμούς με* $|A| \neq 0$, *τότε*[2] *ο πίνακας* A^{-1}, *ο οποίος υπάρχει πάντα ως πίνακας ρητών αριθμών, είναι πίνακας ακέραιων αριθμών αν και μόνον αν* $|A| = \pm 1$. ▲

[2] Να δειχθεί σαν Άσκηση.

Άσκηση 6. (1) Δείξτε ότι αν H και K είναι δύο υποομάδες μιας αβελιανής ομάδας $(G,\cdot)$, τότε το υποσύνολο[3]

$$H\cdot K=\big\{h\cdot k\in G\mid h\in H\ \ \&\ \ k\in K\big\}$$

είναι μια υποομάδα της G.

(2) Να αποδείξετε με τη βοήθεια ενός αντιπαραδείγματος ότι ο ισχυρισμός του (1) δεν αληθεύει όταν η ομάδα $(G,\cdot)$ δεν είναι αβελιανή.

(3) Έστω $n,m\geqslant 1$ δύο φυσικοί αριθμοί και $H=n\mathbb{Z}=\langle n\rangle$ και $K=m\mathbb{Z}=\langle m\rangle$ οι κυκλικές υποομάδες της προσθετικής ομάδας $(\mathbb{Z},+)$, οι οποίες παράγονται από τους φυσικούς αριθμούς n και m αντίστοιχα. Να προσδιορισθεί η ομάδα $H+K$.

Λύση. Παραλείπουμε χάριν απλότητας το σύμβολο της πράξης «$\cdot$» και θα γράφουμε $H\cdot K=HK$.

(1) Προφανώς $HK\neq\varnothing$, διότι $e=e^2=ee\in HK$. Έστω $a,b\in HK$, δηλαδή

$$a=h_1k_1\quad\&\quad b=h_2k_2\qquad\text{όπου}\qquad h_1,h_2\in H\quad\&\quad k_1,k_2\in K$$

Θα δείξουμε ότι: $ab^{-1}\in HK$. Έχουμε:

$$\begin{aligned}ab^{-1}&=(h_1k_1)(h_2k_2)^{-1}\\&=(h_1k_1)(k_2^{-1}h_2^{-1})\\&=(h_1k_1)(h_2^{-1}k_2^{-1})\\&=h_1(k_1h_2^{-1})k_2^{-1}\\&=h_1(h_2^{-1}k_1)k_2^{-1}\\&=(h_1h_2^{-1})(k_1k_2^{-1})\end{aligned}$$

Επειδή $H\leqslant G$, έχουμε ότι $h_1h_2^{-1}\in H$, και επειδή $K\leqslant G$ έπεται ότι $k_1k_2^{-1}\in K$. Άρα το στοιχείο ab^{-1} ανήκει στο υποσύνολο HK και επομένως $HK\leqslant G$.

(2) Θεωρούμε τη συμμετρική ομάδα S_3 και έστω οι μεταθέσεις

$$\mu_1=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}\qquad\text{και}\qquad\mu_2=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

Τότε έχουμε τις υποομάδες

$$H=\langle\mu_1\rangle=\big\{\iota,\ \mu_1\big\}\ \leqslant\ \mathsf{S}_3\qquad\&\qquad K=\langle\mu_2\rangle=\big\{\iota,\ \mu_2\big\}\ \leqslant\ \mathsf{S}_3$$

Το σύνολο HK σε αυτή τη περίπτωση είναι το ακόλουθο:

$$H\cdot K=\big\{\iota,\ \mu_2,\ \mu_1,\ \mu_1\mu_2\big\}$$

και

$$\mu_1\circ\mu_2=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\rho_1$$

Το υποσύνολο HK δεν είναι υποομάδα της S_3, διότι για παράδειγμα

$$\rho_1\circ\rho_1=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\circ\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\rho_2\ \notin\ HK$$

Μια διαφορετική απόδειξη[4] μπορεί να γίνει με γνώση του Θεωρήματος του Lagrange το οποίο θα αποδειχθεί αργότερα.

(3) Έστω $d=(n,m)$ ο Μέγιστος Κοινός Διαιρέτης των n και m. Τότε $n=dx$ και $m=dy$ για κάποιους φυσικούς αριθμούς x,y.

---

[3] Αν η ομάδα έχει δοθεί με προσθετικό συμβολισμό $(G,+)$ τότε θα γράφουμε:

$$H+K=\big\{h+k\in G\mid h\in H\ \ \&\ \ k\in K\big\}$$

[4] Από το Θεώρημα του Langrange (με το οποίο θα ασχοληθούμε σε επόμενο φυλλάδιο) γνωρίζουμε ότι η τάξη μιας υποομάδας μιας πεπερασμένης ομάδας διαιρεί τη τάξη της ομάδας. Άρα το σύνολο $H\cdot K$ δεν είναι υποομάδα της S_3 διότι $|H\cdot K|=4\nmid 6=|\mathsf{S}_3|$.

(α΄) Αν $z \in n\mathbb{Z} + m\mathbb{Z}$, τότε $z = nk + ml$, όπου $k, l \in \mathbb{Z}$, και άρα $z = dxk + dyl = d(xk + yl) \in d\mathbb{Z}$. Επομένως

$$n\mathbb{Z} + m\mathbb{Z} \subseteq d\mathbb{Z}$$

(β΄) Αν $z \in d\mathbb{Z}$, τότε $z = dr$ για κάποιον ακέραιο $r \in \mathbb{Z}$. Όπως γνωρίζουμε, υπάρχουν ακέραιοι a, b έτσι ώστε $d = na + mb$, και τότε: $z = dr = (na + mb)r = nar + mbr \in n\mathbb{Z} + m\mathbb{Z}$. Επομένως

$$d\mathbb{Z} \subseteq n\mathbb{Z} + m\mathbb{Z}$$

Επομένως θα έχουμε

$$n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z} = \langle (n, m) \rangle$$

και έτσι η υποομάδα $n\mathbb{Z} + m\mathbb{Z}$ είναι κυκλική με γεννήτορα τον αριθμό (n, m). ■

Άσκηση 7. (1) Να δειχθεί ότι κάθε μη-κενό πεπερασμένο υποσύνολο H μιας ομάδας G το οποιο είναι κλειστό στην πράξη της ομάδας είναι υποομάδα της G.

(2) Να δειχθεί με ένα αντιπαράδειγμα ότι γενικά το παραπάνω αποτέλεσμα δεν ισχύει αν το υποσύνολο είναι άπειρο.

Λύση. (1) Επειδή το υποσύνολο H είναι μη-κενό και πεπερασμένο, μπορούμε να γράψουμε

$$H = \{h_1, h_2, \cdots, h_n\}$$

όπου $h_1, h_2, \cdots, h_n$ είναι διακεκριμένα στοιχεία της G, $n \geqslant 1$.

Έστω x ένα τυχόν στοιχείο του H. Τότε

$$\forall i = 1, 2, \cdots, n: \quad xh_i = xh_j \implies x^{-1}xh_i = x^{-1}xh_j \implies h_i = h_j \implies i = j$$

Επομένως τα στοιχεία $xh_1, xh_2, \cdots, xh_n$ της G είναι διακεκριμένα και άρα επειδή το σύνολο H είναι κλειστό στην πράξη της ομάδας G, και $x, h_1, \cdots, h_n \in H$, έπεται ότι

$$H = \{xh_1, xh_2, \cdots, xh_n\} \qquad (*)$$

Τότε το στοιχείο x θα είναι της μορφής xh_i για κάποιο $i = 1, 2, \cdots, n$, δηλαδή: $xh_i = x$. Επομένως $xh_i = xe$ και ο Νόμος Διαγραφής σε Ομάδες δίνει ότι $h_i = e$. Επομένως το ουδέτερο στοιχείο e της G ανήκει στην H.

Μένει να δείξουμε ότι αν $x \in H$, τότε $x^{-1} \in H$. Όπως και πριν, επειδή το e ανήκει στην H, από την σχέση $(*)$, θα έχουμε ότι το e είναι της μορφής xh_k για κάποιο $k = 1, 2, \cdots, n$, δηλαδή: $xh_k = e$. Από την τελευταία σχέση έχουμε $x^{-1}xh_k = x^{-1}e = x^{-1}$ και επομένως $x^{-1} = h_k \in H$. Άρα αν $x \in H$, τότε και $x^{-1} \in H$.

Επομένως σύμφωνα με γνωστλό κριτήριο, το υποσύνολο H είναι μια υποομάδα της G.

(2) Έστω $G = (\mathbb{Z}, +)$ η προσθετική ομάδα των ακεραίων και $H = \mathbb{N} \subseteq \mathbb{Z}$. Τότε το υποσύνολο H είναι ένα μη-κενό άπειρο υποσύνολο του $\mathbb{Z}$ το οποίο είναι προφανώς κλειστό στην πράξη πρόσθεσης της ομάδας G. Όμως το H δεν είναι υποομάδα της $\mathbb{Z}$ διότι αν $x \in \mathbb{N}$, τότε το αντίστροφό του ως προς την πράξη της ομάδας δεν ανήκει στο υποσύνολο: $-x \notin \mathbb{N}$. ■

Άσκηση 8. Έστω η ομάδα

$$\mathsf{S}(A) = \{f: A \longrightarrow A \mid \text{η } f \text{ είναι «1-1» και «επί»}\}$$

των μεταθέσεων, δηλαδή των «1-1» και «επί» απεικονίσεων, επί ενός μη κενού συνόλου A, με πράξη την σύνθεση «$\circ$» απεικονίσεων. Αν X είναι ένα πεπερασμένο μη κενό υποσύνολο του A, να δειχθεί ότι το υποσύνολο

$$H = \{f \in \mathsf{S}(A) \mid f(X) \subseteq X\}$$

είναι μια υποομάδα της $\mathsf{S}(A)$.

Αληθεύει ο ισχυρισμός αν το υποσύνολο X είναι άπειρο;

Λύση. • Το υποσύνολο H είναι μη-κενό διότι $\mathrm{Id}_A(X) = X$ και άρα $\mathrm{Id}_A \in H$.

• Αν $f, g \in H$, τότε $f(X) \subseteq X$ και $g(X) \subseteq X$ και επομένως $(f \circ g)(X) = f(g(X)) \subseteq f(X) \subseteq X$. Άρα $f \circ g \in H$ και το υποσύνολο H είναι κλειστό στην πράξη της ομάδας $\mathsf{S}(A)$.

• Έστω $f \in H$. Τότε $f(X) \subseteq X$ και άρα η «1-1» και «επί» απεικόνιση $f\colon A \longrightarrow A$ επάγει μια απεικόνιση $f\colon X \longrightarrow X$ η οποία είναι προφανώς «1-1». Επειδή το σύνολο X είναι πεπερασμένο έπεται ότι η απεικόνιση $f\colon X \longrightarrow X$ είναι «επί», δηλαδή $f(X) = X$, ή ισοδύναμα $f^{-1}(X) = X$. Επομένως η αντίστροφη απεικόνιση $f^{-1}\colon A \longrightarrow A$ ικανοποιεί τη σχέση $f^{-1}(X) \subseteq X$, και άρα $f^{-1} \in H$.

Από τα παραπάνω, σύμφωνα με γνωστό κριτήριο έπεται[5] ότι το ζεύγος $(H, \circ)$ είναι μια υποομάδα της $\mathsf{S}(A)$.

Έστω $A = \mathbb{Z}$ και $X = \mathbb{N}$. Θεωρούμε την απεικόνιση $f\colon \mathbb{Z} \longrightarrow \mathbb{Z}$, $f(n) = n + 1$, η οποία είναι «1-1» και «επί», άρα ανήκει στην ομάδα $\mathsf{S}(\mathbb{Z})$ των μεταθέσεων επί του $\mathbb{Z}$, και προφανώς $f(\mathbb{N}) \subseteq \mathbb{N}$, άρα $f \in H$. Εύκολα βλέπουμε ότι η αντίστροφη f^{-1} της f είναι η συνάρτηση $f^{-1}\colon \mathbb{Z} \longrightarrow \mathbb{Z}$, $f(n) = n - 1$. Τότε $f^{-1} \notin H$ διότι $f^{-1}(1) = 0 \notin \mathbb{N}$. Άρα το υποσύνολο H της ομάδας $\mathsf{S}(\mathbb{Z})$ δεν είναι υποομάδα. ■

Άσκηση 9. Έστω $(G, \cdot)$ μια αβελιανή ομάδα με ταυτοτικό στοιχείο e. Ας είναι $n \in \mathbb{N}$ ένας σταθερά δοσμένος φυσικός αριθμός. Να δειχθεί ότι το υποσύνολο

$$G_n = \big\{ g \in G \mid g^n = e \big\}$$

της G το οποίο αποτελείται από τα στοιχεία $g \in G$ με την ιδιότητα $g^n = e$ είναι μια υποομάδα της G.

Ισχύει το παραπάνω αποτέλεσμα αν η ομάδα δεν είναι αβελιανή; Αν ισχύει να το αποδείξετε, διαφορετικά να δώσετε αντιπαράδειγμα.

Λύση. • Το σύνολο $G_n = \big\{ g \in G \mid g^n = e \big\}$ δεν είναι το κενό διότι $e^n = e \in H$.

• Έστω $a, b \in G_n$. Θα δείξουμε ότι το στοιχείο $ab^{-1} \in G_n$, δηλαδή θα δείξουμε ότι $(ab^{-1})^n = e$. Επειδή η G είναι αβελιανή, έπεται άμεσα ότι

$$(g_1 g_2)^n = g_1^n g_2^n$$

Επομένως θα έχουμε:

$$(ab^{-1})^n = a^n (b^{-1})^n = a^n (b^n)^{-1} = e e^{-1} = e$$

και άρα πράγματι $ab^{-1} \in G_n$. Συνεπώς $G_n \leqslant G$.

Το αποτέλεσμα της Άσκησης δεν ισχύει γενικά, αν η ομάδα δεν είναι αβελιανή. Πράγματι θεωρούμε τη συμμετρική ομάδα $G = \mathsf{S}_3$ η οποία δεν είναι αβελιανή, και έστω $n = 2$. Τότε όπως μπορούμε να δούμε εύκολα,

$$G_2 = \left\{ \iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},\ \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$$

η οποία δεν είναι υποομάδα της S_3, διότι:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \notin G_2$$

■

Άσκηση 10. (1) Αν H και K είναι υποομάδες μιας ομάδας G, να δειχθεί ότι η ένωση $H \cup K$ είναι υποομάδα της G αν και μόνον αν είτε $H \subseteq K$ είτε $K \subseteq H$.

(2) Δεν υπάρχει ομάδα η οποία είναι ένωση δύο γνήσιων υποομάδων της.

(3) Υπάρχει ομάδα η οποία είναι ένωση τριών γνήσιων υποομάδων της;

[5] Διαφορετικά: επειδή το σύνολο X είναι πεπερασμένο, έπεται ότι η ομάδα μεταθέσεων

$$\mathsf{S}(X) = \big\{ f\colon X \longrightarrow X \mid \text{η } f \text{ είναι «1-1» και «επί»} \big\}$$

είναι πεπερασμένη ομάδα. Επειδή όπως δείξαμε παραπάνω κάθε στοιχείο f του υποσυνόλου H είναι μια απεικόνιση $f\colon X \longrightarrow X$ η οποία είναι «1-1» και «επί», έπεται ότι $H \subseteq \mathsf{S}(X)$, και επομένως το υποσύνολο H είναι πεπερασμένο. Επειδή όπως δείξαμε παραπάνω το υποσύνολο H είναι μη κενό και κλειστό στην πράξη της ομάδας $\mathsf{S}(A)$, από την Άσκηση 7 έπεται ότι το υποσύνολο H είναι μια υποομάδα της $\mathsf{S}(A)$.

Λύση. (1) «$\Longleftarrow$» Υποθέτουμε ότι είτε $H \subseteq K$ είτε $K \subseteq H$. Τότε:

$$\begin{cases} H \subseteq K \implies H \cup K = K \implies H \cup K \leqslant G \\ \\ \text{είτε} \\ \\ K \subseteq H \implies H \cup K = H \implies H \cup K \leqslant G \end{cases}$$

Επομένως σε κάθε περίπτωση έχουμε ότι η ένωση $H \cup K$ είναι υποομάδα της G.

«$\Longrightarrow$» Έστω ότι $H \cup K \leqslant G$ και υποθέτουμε αντίθετα ότι $H \nsubseteq K$ και $K \nsubseteq H$. Τότε αφού $H \nsubseteq K$ έχουμε ότι υπάρχει $x \in H$ με $x \notin K$ και όμοια αφού $K \nsubseteq H$ έπεται ότι υπάρχει $y \in K$ με $y \notin H$. Τότε $x, y \in H \cup K$ και επομένως επειδή το υποσύνολο $H \cup K$ είναι υποομάδα, θα έχουμε $xy \in H \cup K$. Τότε, χρησιμοποιώντας ότι τα υποσύνολα H και K είναι υποομάδες της G και $x \in H$ και $y \in K$, οπότε θα έχουμε $x^{-1} \in H$ και $y^{-1} \in K$, θα έχουμε:

$$xy \in H \cup K \implies \begin{cases} xy \in H \\ \text{ή} \\ xy \in K \end{cases} \implies \begin{cases} x^{-1}xy \in H \\ \text{ή} \\ xyy^{-1} \in K \end{cases} \implies \begin{cases} y \in H \quad \text{το οποίο είναι άτοπο διότι } y \notin H \\ \text{ή} \\ x \in K \quad \text{το οποίο είναι άτοπο διότι } x \notin K \end{cases}$$

και άρα σε κάθε περίπτωση έχουμε καταλήξει σε άτοπο. Επομένως είτε $H \subseteq K$ είτε $K \subseteq H$.

(2) Αν για την ομάδα G ισχύει ότι $G = H \cup K$, όπου H και K είναι γνήσιες υποομάδων της G, τότε η ένωση των υποομάδων H και K είναι ομάδα και άρα από το (1) θα έχουμε είτε $H \subseteq K$ ή $K \subseteq H$. Τότε όμως θα έχουμε $G = H \cup K = K$ ή $G = H \cup K = H$ αντίστοιχα. Και οι δύο περιπτώσεις μας οδηγούν σε άτοπο διότι οι υποομάδες H και K είναι γνήσιες. Άρα η τυχούσα ομάδα G δεν μπορεί να είναι ένωση δύο γνήσιων υποομάδων της.

(3) Θεωρούμε την ομάδα του Klein $G = \{e, a, b, c\}$. Τότε γνωρίζουμε ότι τα υποσύνολα

$$H_1 = \{e, a\}, \quad H_1 = \{e, b\}, \quad H_1 = \{e, c\}$$

είναι (γνήσιες) υποομάδες της G και

$$G = H_1 \cup H_2 \cup H_3$$ ■

Άσκηση 11. Σημειώστε αν είναι σωστό ή λάθος.

(1) Ο προσεταιριστικός νόμος ισχύει σε κάθε ομάδα.
(2) Είναι δυνατόν να υπάρξει ομάδα στην οποία να μην ισχύει ο νόμος της διαγραφής.
(3) Κάθε ομάδα είναι υποομάδα του εαυτού της.
(4) Κάθε ομάδα έχει ακριβώς δύο μη γνήσιες υποομάδες.
(5) Σε κάθε κυκλική ομάδα, κάθε στοιχείο είναι γεννήτορας.
(6) Στο μάθημα, δεν έχουμε δώσει ακόμα παράδειγμα ομάδας που να μην είναι αβελιανή.
(7) Κάθε σύνολο αριθμών που είναι ομάδα με πράξη την πρόσθεση είναι και ομάδα με πράξη τον πολλαπλασιασμό.
(8) Μπορούμε να ορίσουμε την υποομάδα ως «υποσύνολο μιας ομάδας».
(9) Η $(\mathbb{Z}_4, +)$ είναι κυκλική ομάδα.
(10) Κάθε υποσύνολο οποιασδήποτε ομάδας είναι υποομάδα με την επαγόμενη πράξη.

Λύση. (1) Σωστό, από τον ορισμό της ομάδας.
(2) Λάθος. Έχουμε δείξει ότι ο Νόμος Διαγραφής ισχύει σε κάθε ομάδα.
(3) Σωστό, από τον ορισμό της (υπο)ομάδας.
(4) Λάθος, προφανώς.
(5) Λάθος. Στην ομάδα $(\mathbb{Z}, +)$ το στοιχείο 2 δεν είναι γεννήτορας.
(6) Λάθος, η συμμετρική ομάδα S_3 δεν είναι αβελιανή.
(7) Λάθος, για παράδειγμα το ζεύγος $(\mathbb{Z}, +)$ είναι ομάδα ενώ αντίθετα το $(\mathbb{Z}, \cdot)$ δεν είναι ομάδα.

(8) Λάθος, αρκεί να θημηθούμε τον ορισμό της υποομάδας.
(9) Σωστό. Το στοιχείο $[1]_4$ είναι γεννήτορας της $\mathbb{Z}_4$: $\mathbb{Z}_4 = \langle [1]_4 \rangle$.
(10) Λάθος, σκεφτείτε πάλι τον ορισμό της υποομάδας καθώς και διάφορα υποσύνολα γνωστών σας ομάδων που δεν είναι υποομάδες με την επαγόμενη πράξη, για παράδειγμα το υποσύνολο $\mathbb{N}$ στην ομάδα $(\mathbb{Z}, +)$. ■

Άσκηση 12. Έστω $(G, \cdot)$ μια ομάδα, και $\mathcal{H} = \{H_i \mid H_i \leqslant G\}_{i \in I}$ μια οικογένεια υποομάδων της G, όπου I είναι ένα σύνολο δεικτών.

(1) Να δειχθεί ότι η τομή
$$H = \bigcap_{i \in I} H_i$$
είναι μια υποομάδα της G.
(2) Έστω $n, m \geqslant 1$ δύο φυσικοί αριθμοί και
$$H_1 = n\mathbb{Z} = \langle n \rangle \quad \& \quad H_2 = m\mathbb{Z} = \langle m \rangle$$
οι κυκλικές υποομάδες της προσθετικής ομάδας $(\mathbb{Z}, +)$, οι οποίες παράγονται από τους φυσικούς αριθμούς n και m αντίστοιχα. Να προσδιορισθεί η ομάδα $n\mathbb{Z} \cap m\mathbb{Z}$.

Λύση. (1) Θα έχουμε:
(α΄) Επειδή $H_i \leqslant G$, $\forall i \in I$, έπεται ότι $e \in H_i$, $\forall i \in I$ και άρα $e \in H = \bigcap_{i \in I} H_i$. Ιδιαίτερα $H \neq \varnothing$.
(β΄) Έστω $a, b \in H$. Τότε $a, b \in H_i$, $\forall i \in I$. Επειδή $H_i \leqslant G$, $\forall i \in I$, έπεται ότι $ab^{-1} \in H_i$, $\forall i \in I$. Τότε όμως $ab^{-1} \in H = \bigcap_{i \in I} H_i$.
Επομένως συμφωνα με γνωστό κριτήριο το υποσύνολο $H = \bigcap_{i \in I} H_i$ είναι μια υποομάδα της G.
(2) Έστω $r = [n, m]$ το ελάχιστο κοινό πολλαπλάσιο των ακεραίων n, m. Τότε $r = nx$ και $r = my$.
(α΄) Έστω $z \in n\mathbb{Z} \cap m\mathbb{Z}$. Τότε $z \in n\mathbb{Z}$ και $z \in m\mathbb{Z}$, και άρα $z = nk$ και $z = ml$ για κάποιους ακέραιους k, l. Τότε όμως από την Θεωρία Αριθμών γνωρίζουμε ότι $r = [n, m] \mid z$ και άρα $z = rt$ για κάποιον ακέραιο t. Αυτό σημαίνει ότι $z \in r\mathbb{Z}$ και άρα:
$$n\mathbb{Z} \cap m\mathbb{Z} \subseteq r\mathbb{Z}$$
(β΄) Έστω $z \in r\mathbb{Z}$ και άρα $z = rt$ για κάποιον ακέραιο t. Τότε $z = nxt$ και $z = myt$, και άρα $z \in n\mathbb{Z}$ και $z \in m\mathbb{Z}$, δηλαδή $z \in n\mathbb{Z} \cap m\mathbb{Z}$. Έτσι
$$r\mathbb{Z} \subseteq n\mathbb{Z} \cap m\mathbb{Z}$$
Συνοψίζοντας, θα έχουμε:
$$n\mathbb{Z} \cap m\mathbb{Z} = [n, m]\mathbb{Z} = \langle [n, m] \rangle$$
και άρα η ομάδα $n\mathbb{Z} \cap m\mathbb{Z}$ είναι κυκλική με γεννήτορα τον αριθμό $[n, m]$. ■

Άσκηση 13. Έστω ότι $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι δύο ομάδες. Να δειχθεί ότι το καρτεσιανό γινόμενο $G_1 \times G_2$ εφοδιασμένο με την πράξη
$$\star : (G_1 \times G_2) \times (G_1 \times G_2) \longrightarrow G_1 \times G_2, \qquad ((a_1, a_2), (b_1, b_2)) \longmapsto (a_1 \star_1 b_1, a_2 \star_2 b_2)$$
αποτελεί μια ομάδα. (Η συγκεκριμένη ομάδα ονομάζεται το **ευθύ γινόμενο** των ομάδων G_1 και G_2.)

Λύση. Κατ' αρχήν παρατηρούμε ότι $G_1 \times G_2 \neq \varnothing$ διότι $G_i \neq \varnothing$ επειδή $e_i \in G_i$, $i = 1, 2$.

Έστω $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$. Έχουμε:

- Η πράξη «$\star$» είναι προσεταιριστική:

$$(a_1, a_2) \star \big[(b_1, b_2) \star (c_1, c_2)\big] = (a_1, a_2) \star (b_1 \star_1 c_1, b_2 \star_2 c_2) = \big(a_1 \star_1 (b_1 \star_1 c_1), a_2 \star_2 (b_2 \star_2 c_2)\big)$$

και

$$\big[(a_1, a_2) \star (b_1, b_2)\big] \star (c_1, c_2) = (a_1 \star_1 b_1, a_2 \star_2 b_2) \star (c_1, c_2) = \big((a_1 \star_1 b_1) \star_1 c_1, (a_2 \star_2 b_2) \star_2 c_2\big)$$

Επειδή οι πράξεις «$\star_1$» και «$\star_2$» είναι προσεταιριστικές, έπεται ότι $a_1 \star_1 (b_1 \star_1 c_1) = (a_1 \star_1 b_1) \star_1 c_1$ και $a_2 \star_2 (b_2 \star_2 c_2) = (a_2 \star_2 b_2) \star_2 c_2$. Άρα η πράξη «$\star$» είναι προσεταιριστική.

• Ουδέτερο στοιχείο: Έστω $e_{G_1} = e_1$ το ουδέτερο στοιχείο της G_1 και $e_{G_2} = e_2$ το ουδέτερο στοιχείο της G_2. Τότε για κάθε $(g_1, g_2) \in G_1 \times G_2$ έχουμε:

$$(g_1, g_2) \star (e_1, e_2) = (g_1 \star_1 e_1, g_2 \star_2 e_2) = (g_1, g_2) = (e_1 \star_1 g_1, e_2 \star_2 g_2) = (e_1, e_2) \star (g_1, g_2)$$

Συνεπώς το στοιχείο $(e_1, e_2) \in G_1 \times G_2$ είναι το ουδέτερο στοιχείο της $G_1 \times G_2$ ως προς τη πράξη «$\star$»:

$$e_{G_1 \times G_2} = (e_{G_1}, e_{G_2})$$

• Αντίστροφο στοιχείο: Έστω $(g_1, g_2) \in G_1 \times G_2$. Τότε υπάρχουν αντίστροφα στοιχεία $g_1^{-1} \in G_1$ και $g_2^{-1} \in G_2$ έτσι ώστε

$$g_1^{-1} \star_1 g_1 = e_1 = g_1 \star_1 g_1^{-1} \quad \text{και} \quad g_2^{-1} \star_2 g_2 = e_2 = g_2 \star_2 g_2^{-1}$$

Τότε έχουμε:

$$(g_1, g_2) \star (g_1^{-1}, g_2^{-1}) = (g_1 \star_1 g_1^{-1}, g_2 \star_2 g_2^{-1}) = (e_1, e_2) = (g_1^{-1} \star_1 g_1, g_2^{-1} \star_2 g_2) = (g_1^{-1}, g_2^{-1}) \star (g_1, g_2)$$

και άρα το στοιχείο $(g_1^{-1}, g_2^{-1}) \in G_1 \times G_2$ αποτελεί το αντίστροφο στοιχείο του (g_1, g_2):

$$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$$

Επομένως το ζεύγος $(G_1 \times G_2, \star)$ είναι ομάδα. ■

Παρατήρηση. *Αν $\{G_i \mid i \in I\}$ είναι μια συλλογή από ομάδες, όπου το ουδέτερο στοιχείο της ομάδας $(G_i, \star_i)$ συμβολίζεται με e_i, $i \in I$, τότε παρόμοια με την παραπάνω Άσκηση, το καρτεσιανό γινόμενο συνόλων*

$$\bigtimes_{i \in I} G_i = \{(g_i)_{i \in I} \mid g_i \in G_i,\ \forall i \in I\}$$

εφοδιασμένο με την πράξη

$$(g_i)_{i \in I} \star (g_i')_{i \in I} = (g_i \star_i g_{i \in I}')_{i \in I}$$

είναι ομάδα με ουδέτερο στοιχείο $(e_i)_{i \in I}$, και αντίστροφο του στοιχείου $(g_i)_{i \in I}$ το στοιχείο $(g_i)_{i \in I}^{-1} = (g_i^{-1})_{i \in I}$.

Αν $I = \{1, 2, \cdots, n\}$, τότε θα γράφουμε $\times_{i \in I} G_i = G_1 \times G_2 \cdots \times G_n$.

Για παράδειγμα, για κάθε $n \in \mathbb{N}$, θέτοντας $(G_i, \star_i) = (\mathbb{Z}_n, +)$, για κάθε $i = 1, 2, 3, \cdots$, αποκτούμε την ομάδα ευθύ γινόμενο

$$\mathbb{Z}_n \times \mathbb{Z}_n \times \cdots = \{([x]_n)_{i \in \mathbb{N}} \mid x \in \mathbb{Z},\ i = 1, 2, 3, \cdots\}$$

η οποία είναι προφανώς άπειρης τάξης, αλλά κάθε στοιχείο της $([x]_n)_{i \in \mathbb{N}}$ έχει πεπερασμένη τάξη:

$$n([x]_n)_{i \in \mathbb{N}} = (n[x]_n)_{i \in \mathbb{N}} = ([nx]_n)_{i \in \mathbb{N}} = ([0]_n)_{i \in \mathbb{N}}$$

η οποία είναι διαρέτης του n. ▲

Άσκηση 14. Έστω ότι $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι δύο ομάδες, και θεωρούμε την ομάδα ευθύ γινόμενο, όπως στην Άσκηση 13. Αν

$$H = G_1 \times \{e_2\} = \{(g_1, e_2) \in G_1 \times G_2 \mid g_1 \in G_1\} \quad \text{και} \quad K = \{e_1\} \times G_2 = \{(e_1, g_2) \in G_1 \times G_2 \mid g_2 \in G_2\}$$

(1) Να δειχθεί ότι

$$H \leqslant G_1 \times G_2 \quad \text{και} \quad K \leqslant G_1 \times G_2$$

(2) $H \bigcap K = \{e_{G_1 \times G_2}\} = \{(e_1, e_2)\}$.

(3) $H \star K = K \star H = G_1 \times G_2$.

(4) Να δειχθεί ότι[6], $\forall h \in H$, $\forall k \in K$, $\forall g \in G_1 \times G_2$:

$$g \star h \star g^{-1} \ \in \ H \qquad \text{και} \qquad g \star k \star g^{-1} \ \in \ K$$

Λύση. (1) Προφανώς $H \neq \varnothing$ διότι $(e_1, e_2) \in G_1 \times \{e_2\} = H$. Έστω $x = (a_1, e_2)$ και $y = (b_1, e_2)$ δύο στοιχεία του υποσυνόλου H. Τότε

$$x \star y^{-1} = (a_1, e_2) \star (b_1, e_2)^{-1} = (a_1, e_2) \star (b_1^{-1}, e_2^{-1}) = (a \star_1 b_1^{-1}, e_2 \star_2 e_2^{-1}) = (a \star_1 b_1^{-1}, e_2) \ \in \ G_1 \times \{e_2\} = H$$

Επομένως $H \leqslant G_1 \times G_2$.

Παρόμοια $K \neq \varnothing$ διότι $(e_1, e_2) \in \{e_1\} \times G_2 = K$. Έστω $z = (e_1, a_2)$ και $w = (e_1, b_2)$ δύο στοιχεία του υποσυνόλου K. Τότε

$$z \star w^{-1} = (e_1, a_2) \star (e_1, b_2)^{-1} = (e_1, a_2) \star (e_1^{-1}, b_2^{-1}) = (e_1 \star_1 e_1^{-1}, a_2 \star_2 b_2^{-1}) = (e_1, a_2 \star_2 b_2^{-1}) \ \in \ \{e_1\} \times G_2 = K$$

Επομένως $K \leqslant G_1 \times G_2$.

(2) Αν $x = (a, b) \in H \bigcap K$, τότε θα έχουμε αναγκαστικά $(a, b) \in H$ και επομένως $b = e_2$ και $(a, b) \in K$ και επομένως $a = e_1$. Άρα $x = (e_1, e_2) = e_{G_1 \times G_2}$, δηλαδή $H \bigcap K = \{e_{G_1 \times G_2}\}$.

(3) Έστω $x = (a, e_2) \in H$ και $y = (e_1, b) \in K$. Τότε:

$$x \star y = (a, e_2) \star (e_1, b) = (a \star_1 e_1, e_2 \star_2 b) = (a, b) = (e_1 \star_1 a, b \star_2 e_2) = (e_1, b) \star (a, e_2) = y \star x$$

Επομένως $H \star K = K \star H \subseteq G_1 \times G_2$. Αν $(a, b) \in G_1 \times G_2$, τότε

$$(a, b) = (e_1 \star_1 a, b \star_2 e_2) = (e_1, b) \star (a, e_2) \ \in \ K \star H$$

Άρα $H \star K = K \star H = G_1 \times G_2$.

(4) Έστω $h = (a, e_2) \in H$, $k = (e_1, b) \in K$, και $g = (g_1, g_2) \in G_1 \times G_2$. Τότε:

$$g \star h \star g^{-1} = (g_1, g_2) \star (a, e_2) \star (g_1, g_2)^{-1} = (g_1, g_2) \star (a, e_2) \star (g_1^{-1}, g_2^2) = (g_1 \star_1 a \star_1 g_1^{-1}, g_2 \star_2 e_2 \star_2 g_2^{-1}) =$$
$$= (g_1 \star_1 a \star_1 g_1^{-1}, g_2 \star_2 g_2^{-1}) = (g_1 \star_1 a \star_1 g_1^{-1}, e_2) \ \in \ H$$

Παρόμοια θα έχουμε:

$$g \star k \star g^{-1} = (g_1, g_2) \star (e_1, b) \star (g_1, g_2)^{-1} = (g_1, g_2) \star (e_1, b) \star (g_1^{-1}, g_2^{-1}) = (g_1 \star_1 e_1 \star_1 g_1^{-1}, g_2 \star_2 b \star_2 g_2^{-1}) =$$
$$= (g_1 \star_1 g_1^{-1}, g_2 \star_2 b \star_2 g_2^{-1}) = (e_1, g_2 \star_2 b \star_2 g^{-1}) \ \in \ K$$ ■

Άσκηση 15. Θεωρούμε την ομάδα ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_2$ της προσθετικής ομάδας $(\mathbb{Z}_2, +)$ με τον εαυτό της, βλέπε Άσκηση 13. Να σχηματιστεί ο πίνακας Cayley της $\mathbb{Z}_2 \times \mathbb{Z}_2$ και να αποδειχτεί ότι δεν πρόκειται για κυκλική ομάδα.

Λύση. Παρακάτω, χάριν απλότητας, γράφοντας $[k]$ εννοούμε την κλάση ισοτιμίας $[k]_2$ του ακεραίου k.

Η ομάδα $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$ έχει τέσσερα στοιχεία:

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \big\{([0],[0]),\ ([0],[1]),\ ([1],[0]),\ ([1],[1])\big\}$$

και ο πίνακας πράξης της είναι ο ακόλουθος:

$+$	$([\mathbf{0}],[\mathbf{0}])$	$([\mathbf{1}],[\mathbf{0}])$	$([\mathbf{0}],[\mathbf{1}])$	$([\mathbf{1}],[\mathbf{1}])$
$([\mathbf{0}],[\mathbf{0}])$	$([0],[0])$	$([1],[0])$	$([0],[1])$	$([1],[1])$
$([\mathbf{1}],[\mathbf{0}])$	$([1],[0])$	$([0],[0])$	$([1],[1])$	$([0],[1])$
$([\mathbf{0}],[\mathbf{1}])$	$([0],[1])$	$([1],[1])$	$([0],[0])$	$([1],[0])$
$([\mathbf{1}],[\mathbf{1}])$	$([1],[1])$	$([0],[1])$	$([1],[0])$	$([0],[0])$

Αν η ομάδα $\mathbb{Z}_2 \times \mathbb{Z}_2$ ήταν κυκλική θα έπρεπε κάποιο από τα μη-τετριμμένα στοιχεία της να παράγει ολόκληρη την ομάδα. Ισοδύναμα θα έπρεπε κάποιο από τα στοιχεία $([1],[0]), ([1],[0]), ([1],[1]) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ να έχει τάξη 4. Όμως από τον παραπάνω πίνακα διαπιστώνουμε ότι κανένα από τα μη-τετριμμένα στοιχεία δεν είναι γεννήτορας της $\mathbb{Z}_2 \times \mathbb{Z}_2$, αφού καθένα από αυτά έχει τάξη δύο. Άρα η ομάδα $\mathbb{Z}_2 \times \mathbb{Z}_2$ δεν είναι κυκλική. ■

[6] Μια υποομάδα H μιας ομάδας G η οποία ικανοποιεί την ιδιότητα: $g \cdot h \cdot g^{-1} \ \in \ H$, $\forall g \in G$, $\forall h \in H$, καλείται **κανονική υποομάδα** της G. Έτσι στην Άσκηση 14, οι υποομάδες H και K είναι κανονικές υποομάδες της ομάδας ευθύ γινόμενο $G_1 \times G_2$. Όπως θα δούμε αργότερα, οι κανονικές υποομάδες διαδραματίζουν σημαντικό ρόλο στη θεωρία ομάδων.

Άσκηση 16. Θεωρούμε τις ομάδες $(\mathbb{Z}_2, +)$, $(\mathbb{Z}_3, +)$ και το ευθύ γινόμενό τους $\mathbb{Z}_2 \times \mathbb{Z}_3$. Να σχηματιστεί ο πίνακας Cayley της ομάδας ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_3$ και να αποδειχτεί ότι πρόκειται για κυκλική ομάδα. Ακολούθως να εξετάσετε, αν ο ισχυρισμός

«**Σε κάθε κυκλική ομάδα, κάθε στοιχείο είναι γεννήτορας**»

είναι αληθής ή όχι.

Λύση. Παρακάτω, χάριν απλότητας, γράφοντας $([n], [m])$ εννοούμε το ζεύγος των κλάσεων ισοτιμίας $([n]_2, [m]_3)$.

Η ομάδα $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ έχει τα ακόλουθα έξι στοιχεία:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \big\{([0],[0]),\ ([0],[1]),\ ([0],[2]),\ ([1],[0]),\ ([1],[1]),\ ([1],[2])\big\}$$

και ο πίνακας Cayley της είναι ο εξής:

$+$	$([\mathbf{0}],[\mathbf{0}])$	$([\mathbf{0}],[\mathbf{1}])$	$([\mathbf{0}],[\mathbf{2}])$	$([\mathbf{1}],[\mathbf{0}])$	$([\mathbf{1}],[\mathbf{1}])$	$([\mathbf{1}],[\mathbf{2}])$
$([\mathbf{0}],[\mathbf{0}])$	$([0],[0])$	$([0],[1])$	$([0],[2])$	$([1],[0])$	$([1],[1])$	$([1],[2])$
$([\mathbf{0}],[\mathbf{1}])$	$([0],[1])$	$([0],[2])$	$([0],[0])$	$([1],[1])$	$([1],[2])$	$([1],[0])$
$([\mathbf{0}],[\mathbf{2}])$	$([0],[2])$	$([0],[0])$	$([0],[1])$	$([1],[2])$	$([1],[0])$	$([1],[1])$
$([\mathbf{1}],[\mathbf{0}])$	$([1],[0])$	$([1],[1])$	$([1],[2])$	$([0],[0])$	$([0],[1])$	$([0],[2])$
$([\mathbf{1}],[\mathbf{1}])$	$([1],[1])$	$([1],[2])$	$([1],[0])$	$([0],[1])$	$([0],[2])$	$([0],[0])$
$([\mathbf{1}],[\mathbf{2}])$	$([1],[2])$	$([1],[0])$	$([1],[1])$	$([0],[2])$	$([0],[0])$	$([0],[1])$

Στη συνέχεια υπολογίζουμε τις τάξεις των στοιχείων της $\mathbb{Z}_2 \times \mathbb{Z}_3$. Έχουμε:

$$([0],[1]) + ([0],[1]) = ([0],[2]) \implies ([0],[1]) + ([0],[2]) = ([0],[0]) \implies \mathrm{o}\big(([0],[1])\big) = 3$$

$$([0],[2]) + ([0],[2]) = ([0],[1]) \implies ([0],[2]) + ([0],[1]) = ([0],[0]) \implies \mathrm{o}\big(([0],[2])\big) = 3$$

$$([1],[0]) + ([1],[0]) = ([0],[0]) \implies \mathrm{o}\big(([1],[0])\big) = 2$$

$$\begin{aligned} ([1],[1]) + ([1],[1]) = ([0],[2]) &\implies ([1],[1]) + ([0],[2]) = ([1],[0]) \\ &\implies ([1],[1]) + ([1],[0]) = ([0],[1]) \\ &\implies ([1],[1]) + ([0],[1]) = ([1],[2]) \\ &\implies ([1],[1]) + ([1],[2]) = ([0],[0]) \\ &\implies \mathrm{o}\big(([1],[1])\big) = 6 \end{aligned}$$

$$\begin{aligned} ([1],[2]) + ([1],[2]) = ([0],[1]) &\implies ([1],[2]) + ([0],[1]) = ([1],[0]) \\ &\implies ([1],[2]) + ([1],[0]) = ([0],[2]) \\ &\implies ([1],[2]) + ([0],[2]) = ([1],[1]) \\ &\implies ([1],[2]) + ([1],[1]) = ([0],[0]) \\ &\implies \mathrm{o}\big(([1],[2])\big) = 6 \end{aligned}$$

Συνεπώς η ομάδα $\mathbb{Z}_2 \times \mathbb{Z}_3$ είναι κυκλική διότι

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \big\langle([1],[1])\big\rangle = \big\langle([1],[2])\big\rangle$$

και τα στοιχεία $([1],[1])$, $([1],[2])$ είναι γεννήτορες της $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Ο ισχυρισμός

«**Σε κάθε κυκλική ομάδα, κάθε στοιχείο είναι γεννήτορας**»

δεν είναι αληθής, διότι για παράδειγμα στην ομάδα $(\mathbb{Z}_{10}, +)$ το στοιχείο $[2]$ δεν είναι γεννήτορας. Δείτε την επόμενη άσκηση για περαιτέρω εξήγηση. ■

Σχόλιο 0.1. Από την Άσκηση 16 βλέπουμε ότι η ομάδα ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_3$ είναι κυκλική, και από την Άσκηση 15 βλέπουμε ότι η ομάδα ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_2$ δεν είναι κυκλική. Όπως θα δούμε αργότερα σε γενικότερο πλαίσιο η παραπάνω διαφοροποίηση οφείλεται στο ότι $(2,3) = 1$ και $(2,2) = 2 \neq 1$. Ειδικότερα θα αποδείξουμε ότι η ομάδα ευθύ γινόμενο $\mathbb{Z}_n \times \mathbb{Z}_m$ είναι κυκλική αν και μόνον αν $(n,m) = 1$. ▲

Άσκηση 17. Να προσδιοριστούν όλοι οι γεννήτορες της ομάδας $(\mathbb{Z}_{10}, +)$.

Λύση. Παρακάτω, χάριν απλότητας, γράφοντας $[\cdot]$ εννοούμε $[\cdot]_{10}$.

Υπολογίζουμε τις κυκλικές υποομάδες που παράγονται από τα στοιχεία της $\mathbb{Z}_{10}$:

$$\mathbb{Z}_{10} = \{[0], [1], [2], [3], [4], [5], [6], [7], [8], [9]\}$$

Έχουμε:

$$\begin{aligned}
\langle [1] \rangle &= \{[1], [2], [3], [4], [5], [6], [7], [8], [9], [0]\} &&= \mathbb{Z}_{10} \\
\langle [2] \rangle &= \{[2], [4], [6], [8], [0]\} &&\neq \mathbb{Z}_{10} \\
\langle [3] \rangle &= \{[3], [6], [9], [2], [5], [8], [1], [4], [7], [0]\} &&= \mathbb{Z}_{10} \\
\langle [4] \rangle &= \{[4], [8], [2], [6], [0]\} &&\neq \mathbb{Z}_{10} \\
\langle [5] \rangle &= \{[5], [0]\} &&\neq \mathbb{Z}_{10} \\
\langle [6] \rangle &= \{[6], [2], [8], [4], [0]\} &&= \mathbb{Z}_{10} \\
\langle [7] \rangle &= \{[7], [4], [1], [8], [5], [2], [9], [6], [3], [0]\} &&\neq \mathbb{Z}_{10} \\
\langle [8] \rangle &= \{[8], [6], [4], [2], [0]\} &&\neq \mathbb{Z}_{10} \\
\langle [9] \rangle &= \{[9], [8], [7], [6], [5], [4], [3], [2], [1], [0]\} &&= \mathbb{Z}_{10}
\end{aligned}$$

Άρα οι γεννήτορες της $\mathbb{Z}_{10}$ είναι τα στοιχεία $[1], [3], [7], [9]$ αφού

$$\mathbb{Z}_{10} = \langle [1] \rangle = \langle [3] \rangle = \langle [7] \rangle = \langle [9] \rangle$$

Παρατηρήστε ότι οι γεννήτορες της $\mathbb{Z}_{10}$ είναι ακριβώς οι κλάσεις ισοτιμίας $\bmod 10$ των οποίων οι αντιπρόσωποι είναι πρώτοι προς το δέκα. ■

Άσκηση 18. Θεωρούμε το σύνολο $G = \{e, a, b, c, d, f\}$. Να συμπληρωθεί ο ακόλουθος πίνακας έτσι ώστε να αποτελεί τον πίνακα Cayley μιας αβελιανής ομάδας $(G, \cdot)$.

$\cdot$	**e**	**a**	**b**	**c**	**d**	**f**
e	e	a	b	c	d	f
a	a	e	f			b
b	b		c		a	
c	c		e	b		a
d	d	c			b	
f	f					c

Είναι η ομάδα η οποία προκύπτει κυκλική;

Λύση. Λαμβάνοντας υπ' όψιν ότι η ομάδα $(G, \cdot)$ είναι αβελιανή, θα πρέπει τα στοιχεία του πίνακα Cayley να είναι συμμετρικά ως προς την κύρια διαγώνιο. Επομένως θα προκύψει ο πίνακας:

$\cdot$	**e**	**a**	**b**	**c**	**d**	**f**
e	e	a	b	c	d	f
a	a	e	f		c	b
b	b	f	c	e	a	
c	c		e	b		a
d	d	c	a		b	
f	f	b		a		c

Επειδή κάθε στήλη του πίνακα Cayley μιας ομάδας περιέχει τα στοιχεία της ομάδας ακριβώς μια φορά, η δεύτερη στήλη του παραπάνω πίνακα θα συμπληρωθεί με το στοιχείο b και θα προκύψει ο πίνακας

$\cdot$	**e**	**a**	**b**	**c**	**d**	**f**
e	e	a	b	c	d	f
a	a	e	f		c	b
b	b	f	c	e	a	
c	c	d	e	b		a
d	d	c	a		b	
f	f	b		a		c

και τότε λόγω συμμετρίας ως προς την κύρια διαγώνιο θα προκύψει ο πίνακας

$\cdot$	**e**	**a**	**b**	**c**	**d**	**f**
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	f	c	e	a	
c	c	d	e	b		a
d	d	c	a		b	
f	f	b		a		c

Επειδή κάθε στήλη του πίνακα Cayley μιας ομάδας περιέχει τα στοιχεία της ομάδας ακριβώς μια φορά, η τρίτη στήλη του παραπάνω πίνακα θα συμπληρωθεί με το στοιχείο d και θα προκύψει ο πίνακας

$\cdot$	**e**	**a**	**b**	**c**	**d**	**f**
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	f	c	e	a	
c	c	d	e	b		a
d	d	c	a		b	
f	f	b	d	a		c

και τότε λόγω συμμετρίας ως προς την κύρια διαγώνιο θα προκύψει ο πίνακας

·	**e**	**a**	**b**	**c**	**d**	**f**
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	f	c	e	a	d
c	c	d	e	b		a
d	d	c	a		b	
f	f	b	d	a		c

Επειδή κάθε στήλη του πίνακα Cayley μιας ομάδας περιέχει τα στοιχεία της ομάδας ακριβώς μια φορά, η τελευταία στήλη του παραπάνω πίνακα θα συμπληρωθεί με το στοιχείο e και θα προκύψει ο πίνακας

·	**e**	**a**	**b**	**c**	**d**	**f**
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	f	c	e	a	d
c	c	d	e	b		a
d	d	c	a		b	e
f	f	b	d	a		c

και τότε λόγω συμμετρίας ως προς την κύρια διαγώνιο θα προκύψει ο πίνακας

·	**e**	**a**	**b**	**c**	**d**	**f**
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	f	c	e	a	d
c	c	d	e	b		a
d	d	c	a		b	e
f	f	b	d	a	e	c

Επειδή κάθε στήλη του πίνακα Cayley μιας ομάδας περιέχει τα στοιχεία της ομάδας ακριβώς μια φορά, η τέταρτη και η πέμπτη στήλη του παραπάνω πίνακα θα συμπληρωθεί αναγκαστικά με τα στοιχεία με το στοιχείο f και θα προκύψει ο πίνακας

·	**e**	**a**	**b**	**c**	**d**	**f**
e	e	a	b	c	d	f
a	a	e	f	d	c	b
b	b	f	c	e	a	d
c	c	d	e	b	f	a
d	d	c	a	f	b	e
f	f	b	d	a	e	c

Όπως βλέπουμε άμεσα από τον παραπάνω πίνακα, θα έχουμε:

$$d^2 = b,\ \ d^3 = a,\ \ d^4 = c,\ \ d^5 = f,\ \ d^6 = e$$

Άρα

$$G = \langle d \rangle$$

και επομένως η $(G, \cdot)$ είναι κυκλική τάξης 6. ■

Άσκηση 19. (1) Να δειχθεί ότι κάθε κυκλική ομάδα είναι αβελιανή,

(2) Να δειχθεί ότι υπάρχουν αβελιανές ομάδες οι οποίες δεν είναι κυκλικές.

(3) Να δοθεί παράδειγμα μιας μη-αβελανής ομάδας με την ιδιότητα ότι κάθε γνήσια υποομάδα της είναι κυκλική.

Λύση. (1) Έστω ότι $(G,\cdot)$ είναι μια κυκλική ομάδα, δηλαδή υπάρχει στοιχείο $\alpha\in G$ έτσι ώστε

$$G=\langle\alpha\rangle=\{\alpha^n\mid n\in\mathbb{Z}\}$$

Έστω $g_1,g_2\in G$. Τότε $g_1=\alpha^r,\ g_2=\alpha^s\in G$ και άρα έχουμε

$$g_1g_2=a^ra^s=a^{r+s}=a^{s+r}=a^sa^r=g_2g_1$$

Επομένως η G είναι αβελιανή.

(2) Η ομάδα του Klein $G=\{e,a,b,c\}$ είναι μια αβελιανή ομάδα τάξης 4 κάθε στοιχείο της οποίας έχει τάξη 2 και επομένως η G δεν μπορεί να είναι κυκλική.

(3) Θεωρούμε τη συμμετρική ομάδα S_3, η οποία είναι μια μη-αβελιανή ομάδα τάξης 6. Εύκολα μπορούμε να δούμε[7] ότι η S_3 δεν διαθέτει υποομάδες τάξης 4 ή 5, και διαθέτει, εκτός της τετριμμένης, τρεις υποομάδας τάξης 2 και μια υποομάδα τάξης 3. Επειδή, όπως γνωρίζουμε, κάθε ομάδα με τάξη $\leqslant 3$ είναι κυκλική έπεται ότι κάθε γνήσια υποομάδα της S_3 είναι κυκλική. ■

Άσκηση 20. Θεωρούμε το ακόλουθο υποσύνολο της συμμετρικής ομνάδας $(\mathsf{S}_4,\circ)$:

$$G=\{\iota,\ \ \rho_1,\ \ \rho_2,\ \ \rho_3,\ \ \delta_1,\ \ \delta_2,\ \ \mu_1,\ \ \mu_2\}$$

όπου:

$$\iota=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\ \ \rho_1=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix},\ \ \rho_2=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\ \ \rho_3=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}$$

$$\delta_1=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix},\ \ \delta_2=\begin{pmatrix}1&2&3&4\\2&4&3&2\end{pmatrix},\ \ \mu_1=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\ \ \mu_2=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

Να δειχθεί ότι το υποσύνολο G είναι μια μη-αβελιανή υποομάδα της S_4 και κάθε γνήσια υποομάδα της είναι αβελιανή αλλά όχι απαραίτητα κυκλική.

Λύση. Εύκολα βλέπουμε ότι ισχύουν οι σχέσεις

$$\rho_1^2=\rho_2,\quad \rho_1^3=\rho_3,\quad \rho_1^4=\iota,\quad \mu_1^2=\mu_2^2=\delta_1^2=\delta_2^2=\iota,\quad \rho_1\circ\mu_1=\delta_1,\quad \mu_1\circ\rho_1=\delta_2$$

$$\rho_1\circ\delta_1=\mu_2,\quad \delta_1\circ\rho_1=\mu_1,\quad \mu_1\circ\delta_1=\rho_3=\delta_2\circ\mu_1,\quad \delta_1\circ\mu_1=\rho_1=\mu_1\circ\delta_2,\quad \cdots$$

Συνεχίζοντας κατ' αυτό τον τρόπο μπορούμε εύκολα να δούμε ότι το σύνολο G είναι κλειστό στην πράξη της S_4. Επειδή $8=|G|<\infty$, από γνωστό κριτήριο επέται ότι το σύνολο G είναι μια υποομάδα της S_4, η οποία είναι μη-αβελιανή διότι για παράδειγμα $\rho_1\circ\mu_1=\delta_1\neq\delta_2=\mu_1\circ\rho_1$.

Από το Θεώρημα του Lagrange[8] το οποίο θα δούμε αργότερα, έπεται ότι η τάξη κάθε γνήσιας υποομάδας της G είναι ένας εκ των αριθμών 1, 2, 3, 4. Επειδή, όπως έχουμε δει κάθε ομάδα με τάξη $\leqslant 4$ είναι αβελιανή, έπεται ότι κάθε γνήσια υποομάδα της G είναι αβελιανή.

Τέλος έστω το υποσύνολο

$$H=\{\iota,\ \ \rho_2,\ \ \delta_1,\ \ \delta_2\}$$

Εύκολα βλέπουμε ότι το υποσύνολο H είναι κλειστό στην πράξη της G και επομένως αποτελεί υποομάδα της G, η οποία δεν είναι κυκλική διότι $\rho_2^2=\delta_1^2=\delta_2^2=\iota$ και επομένως κανένα στοιχείο της H δεν μπορεί να είναι γεννήτοεράς της. ■

Άσκηση 21. Να δειχθεί ότι μια ομάδα η οποία δεν έχει γνήσιες μη τετριμμένες υποομάδες είναι κυκλική.

Λύση. Έστω G μια ομάδα η οποία δεν έχει γνήσιες μη τετριμμένες υποομάδες, δηλαδή οι μόνες υποομάδες της G είναι: η τετριμμένη υποομάδα $\{e\}$, και η ίδια η ομάδα G.

Διακρίνουμε τις παρακάτω περιπτώσεις:

[7] Ο ισχυρισμός αυτός προκύπτει άμεσα από το Θεώρημα του Lagrange το οποίο θα μελετήσουμε αργότερα. Εδώ ο ισχυρισμός μπορεί να προκύψει δείχνοντας οτι δεν υπάρχει υποσύνολο της S_3 με 4 ή 5 στοιχεία το οποίο είναι κλειστό στην πράξη της ομάδας.

[8] «*Η τάξη κάθε υποομάδας μιας πεπερασμένης ομάδας διαιρεί την τάξη της ομάδας*».

- Αν $G = \{e\}$, τότε $G = \langle e \rangle$ και άρα η G είναι κυκλική.
- Έστω ότι $G \neq \{e\}$. Τότε υπάρχει ένα στοιχείο $a \in G$ με $a \neq e$.

  Θεωρούμε την κυκλική υποομάδα $\langle a \rangle$ της G που παράγεται από το a, δηλαδή $\langle a \rangle \leqslant G$, η οποία δεν είναι η τετριμμένη υποομάδα $\{e\}$ διότι $a \neq e$. Επειδή από την υπόθεση οι μόνες υποομάδες της G είναι η υποομάδα που παράγεται από το $\{e\}$ και η ίδια η ομάδα G, αναγκαστικά θα έχουμε ότι
  $$G = \langle a \rangle$$
  και άρα η ομάδα G είναι κυκλική με γεννήτορα το a. ■

Θα αποδείξουμε αργότερα ότι μια ομάδα G δεν έχει γνήσιες μη τετριμμένες υποομάδες αν και μόνον αν η G είναι πεπερασμένη κυκλική με τάξη έναν πρώτο αριθμό.

Άσκηση 22. Έστω H ένα μη-κενό υποσύνολο μιας ομάδας $(G, \cdot)$. Να δειχθεί ότι το H είναι υποομάδα της G αν και μόνον αν η ακόλουθη σχέση:
$$\forall a, b \in H : \quad a \sim_H b \iff ab^{-1} \in H$$
είναι μια σχέση ισοδυναμίας στο σύνολο H.

Λύση. (1) «$\Longleftarrow$» Υποθέτουμε ότι σχέση «$\sim_H$» είναι μια σχέση ισοδυναμίας επί του μη-κενού υποσυνόλου H της G.

Έστω $h_1, h_2 \in H$. Επειδή $e^{-1} = e$, θα έχουμε $h_1 = h_1 e = h_1 e^{-1} \in H$ και $h_2 = h_2 e = h_2 e^{-1} \in H$, δηλαδή $h_1 \sim_H e$ και $h_2 \sim_H e$. Από την συμμετρική ιδιότητα, θα έχουμε και $e \sim_H h_2$ και τότε η μεταβατική ιδιότητα δίνει $h_1 \sim_H h_2$, δηλαδή $h_1 h_2^{-1} \in H$. Επομένως το H είναι μια υποομάδα της G.

(2) «$\Longrightarrow$» Υποθέτουμε ότι το μη-κενό υποσύνολο H της G είναι υποομάδα.

(α΄) Για κάθε $h \in H$ θα έχουμε $hh^{-1} = e \in H$, και άρα $h \sim_H h$, δηλαδή ισχύει η ανακλαστική ιδιότητα.

(β΄) Έστω $h_1, h_2 \in H$, και υποθέτουμε ότι $h_1 \sim_H h_2$, δηλαδή $h_1 h_2^{-1} \in H$. Επειδή το υποσύνολο H είναι υποομάδα της G, θα έχουμε $(h_1 h_2^{-1})^{-1} = (h_2^{-1})^{-1} h_1^{-1} = h_2 h_1^{-1} \in H$, δηλαδή $h_2 \sim_H h_1$, και άρα ισχύει η συμμετρική ιδιότητα.

(γ΄) Έστω $h_1, h_2, h_3 \in H$, και υποθέτουμε ότι $h_1 \sim_H h_2$ και $h_2 \sim_H h_3$. Τότε $h_1 h_2^{-1} \in H$ και $h_2 h_3^{-1} \in H$. Επειδή το υποσύνολο H είναι υποομάδα, έπεται ότι $h_1 h_2^{-1} h_2 h_3^{-1} = h_1 e h_3^{-1} = h_1 h_3^{-1} \in H$, δηλαδή $h_1 \sim_H h_3$ και άρα ισχύει η μεταβατική ιδιότητα.

Επομένως η σχέση «$\sim_H$» είναι μια σχέση ισοδυναμίας επί του H. ■

Παρατήρηση. *Παρόμοια αποδεικνύεται ότι αν H είναι ένα μη-κενό υποσύνολο μιας ομάδας G, τότε το υποσύνολο H είναι υποομάδα της G αν και μόνον αν η ακόλουθη σχέση:*
$$\forall a, b \in H : \quad a \sim^H b \iff a^{-1} b \in H$$
είναι μια σχέση ισοδυναμίας στο σύνολο H. ▲

Άσκηση 23. Έστω $(G, \cdot)$ μια κυκλική ομάδα και a ένας γεννήτορας της G, δηλαδή $G = \langle a \rangle$. Να δείξετε ότι και το στοιχείο a^{-1} είναι γεννήτορας της G. Ακολούθως να δείξετε ότι μια ομάδα G έχει ακριβώς έναν γεννήτορα αν και μόνον αν είτε η G είναι η τετριμμένη ομάδα ταξης 1 είτε η G είναι η κυκλική ομάδα τάξης 2.

Λύση. Αν $G = \langle a \rangle$, τότε $G = \{a^n \in G \mid n \in \mathbb{Z}\}$. Προφανώς τότε $G = \{a^{-n} \in G \mid n \in \mathbb{Z}\}$. Επειδή $a^{-n} = (a^{-1})^n$, θα έχουμε $G = \{(a^{-1})^n \in G \mid n \in \mathbb{Z}\} = \langle a^{-1} \rangle$ το οποίο σημαίνει ότι το στοιχείο a^{-1} είναι γεννήτορας της G.

Αν η ομάδα G έχει ακριβώς έναν γεννήτορα, έστω a, τότε από την παραπάνω ανάλυση έπεται ότι αναγκαστικά θα έχουμε $a = a^{-1}$, και επομένως $a^2 = e$. Αν $a = e$, τότε $G = \{e\} = \langle e \rangle$ είναι η τετριμμένη

ομάδα. Αν $a \neq e$, τότε, $\forall n \in \mathbb{Z}$: $a^n = e$ αν n είναι άρτιος και $a^n = a$ αν n είναι περιττός. Επομένως $G = \{a^n \in G \mid n \in \mathbb{Z}\} = \{e, a\} = \langle a \rangle$ είναι κυκλική με πλήθος στοιχείων ίσο με δύο.

Αντίστροφα αν η G έχει πλήθος στοιχείων ίσο με 1, τότε προφανώς $G = \{e\} = \langle e \rangle$. Αν η G έχει πλήθος στοιχείων ίσο με 2, τότε $G = \{e, a\}$, και προφανώς $a^2 = e$, δηλαδή $G = \langle a \rangle$ και το a είναι γεννήτορας της G. Προφανώς το a είναι ο μοναδικός γεννήτορας, διότι το άλλο στοιχείο e της G παράγει μόνο την τετριμμένη υποομάδα $\{e\}$. ■

Άσκηση 24. Έστω $(G, \cdot)$ μια κυκλική ομάδα. Τότε το πλήθος των γεννητόρων της G είναι άρτιο αν και μόνον αν $|G| \geqslant 3$.

Λύση. Αν $|G| \geqslant 3$, τότε από την Άσκηση 23 έπεται ότι η G δεν μπορεί να έχει ακριβώς έναν γεννήτορα. Επειδή από την Άσκηση 23 έπεται ότι οι γεννήτορες μιας κυκλικής ομάδας εμφανίζονται ως ζεύγη (a, a^{-1}), όπου $a \neq a^{-1}$ (διότι διαφορετικά αν το στοιχείο a ήταν γεννήτορας και $a = a^{-1}$ θα είχαμε $G = \{e, a\}$ και άρα $|G| \leqslant 2$ το οποίο είναι άτοπο από την υπόθεση), έπεται ότι το πλήθος των γεννητόρων της G είναι άρτιο.

Αντίστροφα αν το πλήθος των γεννητόρων της G είναι άρτιο, και $|G| \leqslant 2$, τότε από την Άσκηση 23 έπεται ότι η G έχει ακριβώς έναν γεννήτορα το οποίο είναι άτοπο από την υπόθεση. Άρα $|G| \geqslant 3$. ■