ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ Ι

Ακαδημαϊκο Ετος 2023-2024

Επιλυση Ασκησεων - Φυλλαδιο 5

Διδασκων: Α. Μπεληγιάννης

ΙΣΤΟΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ

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

Πέμπτη 11 Απριλίου 2024

Υπενθύμιση: Έστω ότι G είναι μια ομάδα και $H \leq G$ είναι μια υποομάδα της.

- Ορίζοντας

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

αποκτούμε μια σχέση ισοδυναμίας «$\sim_H$» επί του συνόλου G (η σχέση ισοδυναμίας «$\sim_H$» συμβολίζεται και ως «$\mathcal{R}_H$». Η κλάση ισοδυναμίας $[x]_{\sim_H}$ του στοιχείου $x \in G$ ως προς τη σχέση ισοδυναμίας «$\sim_H$» θα συμβολίζεται απλούστερα με $[x]_H$ και θα έχουμε

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

Επομένως από τη γενική θεωρία σχέσεων ισοδυναμίας, θα έχουμε:

$$\forall x, y \in G: \quad [x]_H = [y]_H \iff x \in [y]_H \iff y \in [x]_H \iff x \sim_H y \iff x^{-1}y \in H$$

Επιπρόσθετα η οικογένεια $\{[a]_H = aH \mid a \in G\}$ των διακεκριμένων αριστερών πλευρικών κλάσεων (συμπλόκων) aH της H στη G αποτελεί μια διαμέριση της G, δηλαδή:

(1) $\forall a \in G: aH \neq \emptyset$, **(2)** $G = \bigcup_{a \in G} aH$, **(3)** $aH \cap bH \neq \emptyset \implies aH = bH$

Χρησιμοποιώντας αυτές τις παρατηρήσεις, προκύπτει η εξής γενική μέθοδος την οποία ακολουθούμε για τον προσδιορισμό όλων των αριστερών πλευρικών κλάσεων της H στην G:

(1) Πρώτα προσδιορίζουμε μια (οποιαδήποτε) αριστερή πλευρική κλάση a_1H, της H στην G.
Η προφανής επιλογή είναι να ξεκινήσουμε με το στοιχείο $a_1 = e$ και τότε έχουμε την πλευρική κλάση

$$a_1H = eH = H$$

(2) Κατόπιν βρίσκουμε (αν υπάρχει) ένα στοιχείο $a_2 \in G \setminus a_1H$. Τότε $a_1H \neq a_2H$, αφού $a_2 \notin a_1H$, γι' αυτό μια νέα πλευρική κλάση της H στην G είναι η a_2H.
Αν όπως παραπάνω επιλέξουμε $a_1 = e$, τότε βρίσκουμε (αν υπάρχει) ένα στοιχείο $a_2 \in G \setminus H$, και τότε μια νέα πλευρική κλάση της H στην G είναι είναι η a_2H. Έτσι μέχρι τώρα θα έχουμε τις αριστερές πλευρικές κλάσεις:

$$H, \quad a_2H$$

(3) Σχηματίζουμε την ένωση $a_1H \cup a_2H$, κατόπιν βρίσκουμε (αν υπάρχει) ένα στοιχείο $a_3 \in G \setminus (a_1H \cup a_2H)$, γι' αυτό μια νέα πλευρική κλάση είναι η a_3H.
Έτσι, επιλέγοντας $a_1 = e$ παραπάνω, μέχρι τώρα έχουμε τις αριστερές πλευρικές κλάσεις

$$H, \quad a_2H, \quad a_3H$$

(4) Σχηματίζουμε την ένωση $a_1H \cup a_2H \cup a_3H$, και κατόπιν βρίσκουμε (αν υπάρχει) κάποιο $a_4 \in G \setminus (a_1H \cup a_2H \cup a_3H)$. Τότε αποκτούμε μια νέα αριστερή πλευρική κλάση a_4H της H στην G.
Έτσι, επιλέγοντας $a_1 = e$ παραπάνω, μέχρι τώρα έχουμε τις αριστερές πλευρικές κλάσεις

$$H, \quad a_2H, \quad a_3H, \quad a_4H$$

(5) Συνεχίζοντας αυτή τη διαδικασία, επειδή η οικογένεια $\big\{[a]_H = aH \mid a \in G\big\}$ είναι μια διαμέριση της G, κάποια στιγμή η ένωση των διακεκριμένων αριστερών πλευρικών κλάσεων οι οποίες έχουν προκύψει θα είναι ίση με το σύνολο G, και τότε αυτές οι αριστερές πλευρικές κλάσεις θα συμπίπτουν με όλες τις διακεκριμένες αριστερέρς πλευρικές κλάσεις της H στην G.

Αν η ομάδα G είναι πεπερασμένου δείκτη $[G : H] = k$, τότε οι διακεκριμένες αριστερές πλευρικές κλάσεις οι οποίες θα προκύψουν με την παραπάνω διαδικασία θα είναι σε πλήθος k, οι εξής:

$$a_1H = eH = H, \quad a_2H, \quad a_3H, \quad \cdots, \quad a_kH$$

- Ανάλογα εργαζόμαστε με δεξιές πλευρικές κλάσεις: ορίζοντας

$$\forall x, y \in G: \qquad x \,{}_H\!\sim y \iff xy^{-1} \in H$$

αποκτούμε μια σχέση ισοδυναμίας «${}_H\!\sim$» επί του συνόλου G (η σχέση ισοδυναμίας «${}_H\!\sim$» συμβολίζεται και ως «${}_H\!\mathcal{R}$». Η κλάση ισοδυναμίας ${}_H\!\sim[x]$ του στοιχείου $x \in G$ ως προς τη σχέση ισοδυναμίας «${}_H\!\sim$» θα συμβολίζεται απλούστερα με ${}_H[x]$ και θα έχουμε

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

Επομένως από τη γενική θεωρία σχέσεων ισοδυναμίας, θα έχουμε:

$$\forall x, y \in G: \quad {}_H[x] = {}_H[y] \iff x \in {}_H[y] \iff y \in {}_H[x] \iff x \,{}_H\!\sim y \iff xy^{-1} \in H$$

Επιπρόσθετα η οικογένεια $\big\{{}_H[a] = Ha \mid a \in G\big\}$ των διακεκριμένων δεξιών πλευρικών κλάσεων (συμπλόκων) Ha της H στην G αποτελεί μια διαμέριση της G, δηλαδή:

(1) $\forall a \in G:\ Ha \neq \emptyset$, **(2)** $G = \bigcup_{a \in G} Ha$, **(3)** $Ha \cap Hb \neq \emptyset \implies Ha = Hb$

Η μέθοδος την οποία ακολουθούμε για τον προσδιορισμό όλων των δεξιών πλευρικών κλάσεων της H στην G είναι ακριβώς ανάλογη με την μέθοδο που περιγράψαμε για τον προσδιορισμό όλων των αριστερών πλευρικών κλάσεων της H στην G.

Ορισμένες φορές η τάξη μιας ομάδας G συμβολίζεται και ως $\mathsf{o}(G)$.

Άσκηση 1. Θεωρούμε τις ακόλουθες (κυκλικές) υποομάδες της S_3:

$$H = \big\langle (2\,3) \big\rangle = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\rangle \quad \& \quad K = \big\langle (1\,2\,3) \big\rangle = \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle$$

Να βρεθούν οι δεξιές και αριστερές πλευρικές κλάσεις (δεξιά και αριστερά σύμπλοκα) των υποομάδων H, K στην S_3.

Λύση. Υπενθυμίζουμε ότι[1]:

$$\mathsf{S}_3 = \big\{\rho_0 = \iota,\ \mu_1,\ \mu_2,\ \mu_3,\ \rho_1,\ \rho_2\big\}$$

όπου:

$$\rho_0 = \iota = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \rho_2 = \rho_1^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Τα στοιχεία μ_1, μ_2, μ_3 έχουν τάξη 2 και τα στοιχεία ρ_1, ρ_2 έχουν τάξη 3. Άρα:

$$H = \langle \mu_2 \rangle = \big\{\rho_0, \mu_1\big\} \quad \text{και} \quad K = \langle \rho_1 \rangle = \big\{\rho_0, \rho_1, \rho_2\big\}$$

(1) Για την υποομαδα H: Επειδή το πλήθος των (αριστερών ή δεξιών) πλευρικών κλάσεων μιας υποομάδας σε μια πεπερασμένη ομάδα είναι ο δείκτης της υποομάδας στην ομάδα, και

$$[\mathsf{S}_3 : H] = \frac{6}{2} = 3$$

θα υπάρχουν τρεις (αριστερές ή δεξιές) πλευρικές κλάσεις της H στην S_3.

[1] Συνήθως οι μεταθέσεις μ_i συμβολίζονται και με σ_i, όπου $i = 1, 2, 3$.

(α΄) Αριστερές πλευρικές κλάσεις:

$$\rho_0 H = H = \{\rho_0, \mu_1\} \quad \& \quad \rho_1 H = \{\rho_1\rho_0, \rho_1\mu_1\} = \{\rho_1, \mu_3\} \quad \& \quad \rho_2 H = \{\rho_2\rho_0, \rho_2\mu_1\} = \{\rho_2, \mu_2\}$$

Οι παραπάνω αριστερές πλευρικέ κλάσεις, όπως βλέπουμε είναι ανά δύο ξένες και άρα είναι όλες οι αριστερές πλευρικές κλάσεις της H στην S_3. Όπως περιμένουμε $\mathsf{S}_3 = H \cup \rho_1 H \cup \rho_2 H$.

(β΄) Δεξιές πλευρικές κλάσεις:

$$H\rho_0 = H = \{\rho_0, \mu_1\} \quad \& \quad H\rho_1 = \{\rho_0\rho_1, \mu_1\rho_1\} = \{\rho_1, \mu_2\} \quad \& \quad H\rho_2 = \{\rho_0\rho_2, \mu_1\rho_2\} = \{\rho_2, \mu_3\}$$

Οι παραπάνω δεξιές πλευρικές κλάσεις, όπως βλέπουμε είναι ανά δύο ξένες και άρα είναι όλες οι αριστερές πλευρικές κλάσεις, της H στην S_3. Όπως περιμένουμε $\mathsf{S}_3 = H \cup H\rho_1 \cup H\rho_2$.

Παρατηρούμε ότι:

$$\rho_1 H \neq H\rho_1 \quad \text{και} \quad \rho_2 H \neq H\rho_2$$

(2) Για την υποομαδα K: Επειδή το πλήθος των (αριστερών ή δεξιών) πλευρικών κλάσεων, μιας υποομάδας σε μια πεπερασμένη ομάδα είναι ο δείκτης της υποομάδας στην ομάδα, και

$$[\mathsf{S}_3 : K] = \frac{6}{3} = 2$$

θα υπάρχουν δύο (αριστερές ή δεξιές) πλευρικές κλάσεις της K στην S_3.

(α΄) Αριστερές πλευρικές κλάσεις:

$$\rho_0 K = K = \{\rho_0, \rho_1, \rho_2\} \quad \& \quad \mu_1 K = \{\mu_1\rho_0, \mu_1\rho_1, \mu_1\rho_2\} = \{\mu_1, \mu_2, \mu_3\}$$

Οι παραπάνω αριστερές πλευρικές κλάσεις, όπως βλέπουμε είναι ανά δύο ξένες και άρα είναι όλες οι αριστερές πλευρικές κλάσεις της K στην S_3. Όπως περιμένουμε $\mathsf{S}_3 = K \cup H\mu_1$.

(β΄) Δεξιές πλευρικές κλάσεις:

$$K\rho_0 = K = \{\rho_0, \rho_1, \rho_2\} \quad \& \quad K\mu_1 = \{\rho_0\mu_1, \rho_1\mu_1, \rho_2\mu_1\} = \{\mu_1, \mu_2, \mu_2\}$$

Οι παραπάνω δεξιές πλευρικές κλάσεις, όπως βλέπουμε είναι ανά δύο ξένες και άρα είναι όλα οι δεξιές πλευρικές κλάσεις της K στην S_3. Όπως περιμένουμε $\mathsf{S}_3 = K \cup K\mu_1$.

Παρατηρούμε ότι:

$$\mu_1 K = K\mu_1$$

□

Αν η ομάδα G είναι αβελιανή, και $H \leq G$ είναι μια υποομάδα της G, τότε επειδή οι αριστερές πλευρικές κλάσεις συμπίπτουν με τις δεξιές πλευρικές κλάσεις, $\forall a \in G$:

$$aH = \{ah \in G \mid h \in H\} = \{ha \in G \mid h \in H\} = Ha$$

δεν υπάρχει ανάγκη διάκρισης μεταξύ δεξιών και αριστερών πλευρικών κλάσεων. Έτσι σ' αυτή την περίπτωση θα μιλάμε απλά για πλευρικές κλάσεις.

Άσκηση 2. (1) Να ευρεθούν οι πλευρικές κλάσεις (τα σύμπλοκα) της υποομάδας $\langle 5\rangle = 5\mathbb{Z}$ στην ομάδα $(\mathbb{Z}, +)$.

(2) Να ευρεθούν οι πλευρικές κλάσεις (τα σύμπλοκα):
   (α΄) της υποομάδας $\langle 9\rangle = 9\mathbb{Z}$ στην ομάδα $(\mathbb{Z}, +)$,
   (β΄) της υποομάδας $\langle 9\rangle = 9\mathbb{Z}$ στην (υπο)ομάδα $\langle 3\rangle = 3\mathbb{Z}$ της $(\mathbb{Z}, +)$.

(3) Να ευρεθούν οι πλευρικές κλάσεις (τα σύμπλοκα):
   (α΄) της υποομάδας $\langle [6]_{12}\rangle$ στην ομάδα $(\mathbb{Z}_{12}, +)$,
   (β΄) της υποομάδας $\langle [6]_{12}\rangle$ στην (υπο)ομάδα $\langle [2]_{12}\rangle$ της $(\mathbb{Z}_{12}, +)$.

Λύση. (1) Η πρώτη πλευρική κλάση (σύμπλοκο) είναι η $0 + \langle 5\rangle = \langle 5\rangle = \{5z \mid z \in \mathbb{Z}\}$. Παρατηρούμε ότι $1 \in \mathbb{Z} \setminus \langle 5\rangle$, γι' αυτό η πλευρική κλάση (σύμπλοκο) $1 + \langle 5\rangle \neq \langle 5\rangle$. Τώρα, το $2 \in \mathbb{Z} \setminus (\langle 5\rangle \cup (1 + \langle 5\rangle))$ και η πλευρική κλάση $2 + \langle 5\rangle$ είναι μια πλευρική κλάση διαφορετική από τις προηγούμενες. Παρόμοια, το $3 \in \mathbb{Z} \setminus (\langle 5\rangle \cup (1 + \langle 5\rangle) \cup (2 + \langle 5\rangle))$ και η πλευρική κλάση $3 + \langle 5\rangle$ είναι μια πλευρική κλάση διαφορετική από τις προηγούμενες. Τέλος, το $4 \in \mathbb{Z} \setminus (\langle 5\rangle \cup (1 + \langle 5\rangle) \cup (2 + \langle 5\rangle) \cup (3 + \langle 5\rangle))$ και η πλευρική κλάση $4 + \langle 5\rangle$ είναι μια πλευρική κλάση διαφορετική από τις προηγούμενες.

Ισχυριζόμαστε ότι

$$\mathbb{Z} = (\langle 5\rangle \bigcup (1+\langle 5\rangle) \bigcup (2+\langle 5\rangle) \bigcup (3+\langle 5\rangle) \bigcup (4+\langle 5\rangle)$$

Πράγματι, αν $z \in \mathbb{Z}$, τότε εκτελώντας την Ευκλείδεια διαίρεση με υπόλοιπο του z δια 5, παίρνουμε:

$$z = 5q + r, \quad \text{όπου} \quad r = 0, 1, 2, 3, 4.$$

Επειδή λοιπόν $z - 5q = r$, το z ανήκει σε ακριβώς σε μια από τις κλάσεις $\langle 5\rangle$, $(1+\langle 5\rangle)$, $(2+\langle 5\rangle)$, $(3+\langle 5\rangle)$, $(4+\langle 5\rangle$, και άρα αυτές είναι όλες οι πλευρικές κλάσεις.

(2) (α′) Ο προσδιορισμός είναι εντελώς ίδιος. Εδώ οι πλευρικές κλάσεις είναι οι εξής:

$$\langle 9\rangle, \quad (1+\langle 9\rangle), \quad (2+\langle 9\rangle), \quad (3+\langle 9\rangle), \quad (4+\langle 9\rangle), \quad (5+\langle 9\rangle), \quad (6+\langle 9\rangle), \quad (7+\langle 9\rangle), \quad (8+\langle 9\rangle)$$

(β′) Ο προσδιορισμός είναι και πάλι ο ίδιος, μόνο που τώρα εργαζόμαστε στην ομάδα $\langle 3\rangle = 3\mathbb{Z}$ εντός της οποίας θεωρούμε την υποομάδα $\langle 9\rangle = 9\mathbb{Z}$. Τα στοιχεία της $\langle 3\rangle$ είναι της μορφής $3z$, όπου $z \in \mathbb{Z}$. Τώρα οι πλευρικές κλάσεις

$$(3\cdot 0 + \langle 9\rangle), \qquad (3\cdot 1 + \langle 9\rangle), \qquad (3\cdot 2 + \langle 9\rangle),$$

είναι ανά δύο διαφορετικές. Επιπλέον, εκτελώντας Ευκλείδεια διαίρεση με υπόλοιπο του $3z$ δια 9, παίρνουμε:

$$3\rho = 9q + r, \qquad \text{όπου} \quad r = 0, 1, 2, \cdots, 8$$

Επειδή το 3 διαιρεί τη διαφορά $3z - 9q$, διαιρεί και το r. Γι′ αυτό $r = 0 = 3\cdot 0$, $3 = 3\cdot 1$, $6 = 3\cdot 2$. Έτσι το τυχόν στοιχείο $3z$ της $\langle 3\rangle$ ανήκει σε ακριβώς μία από τις κλάσεις $(3\cdot 0 + \langle 9\rangle)$, $(3\cdot 1 + \langle 9\rangle)$, $(3\cdot 2 + \langle 9\rangle)$, και άρα αυτές είναι όλες οι πλευρικές κλάσεις της $\langle 9\rangle$ στην $\langle 3\rangle$.

(3) (α′) Εδώ γνωρίζουμε εκ των προτέρων το πλήθος των αριστερών πλευρικών κλάσεων, αφού από το Θεώρημα Lagrange το πλήθος τους ισούται με τον δείκτη $\frac{\mathsf{o}(\mathbb{Z}_{12})}{\mathsf{o}(\langle [6]\rangle)} = \frac{12}{2} = 6$. Παρατηρούμε ότι $\langle [6]\rangle = \{[0], [6]\}$.

Εδώ οι κλάσεις είναι οι εξής (όλες οι παρακάτω κλάσεις είναι mod 12):

$$([0] + \langle [6]\rangle) = \{[0], [6]\}, \quad ([1] + \langle [6]\rangle) = \{[1]+[0], [1]+[6]\} = \{[1], [7]\},$$
$$([2] + \langle [6]\rangle) = \{[2]+[0], [2]+[6]\} = \{[2], [8]\}, \quad ([3] + \langle [6]\rangle) = \{[3]+[0], [3]+[6]\} = \{[3], [9]\}$$
$$([4] + \langle [6]\rangle) = \{[4]+[0], [4]+[6]\} = \{[4], [10]\}, \quad ([5] + \langle [6]\rangle) = \{[5]+[0], [5]+[6]\} = \{[5], [11]\}$$

(β′) Εδώ θεωρούμε την υποομάδα $\langle [2]\rangle$ της $\mathbb{Z}_{12}$ και την $\langle [6]\rangle$ ως υποομάδα της $\langle [2]\rangle$. Γι′ αυτό το πλήθος των κλάσεων είναι $\frac{\mathsf{o}(\langle [2]\rangle)}{\mathsf{o}(\langle [6]\rangle)} = \frac{6}{2} = 3$ και οι κλάσεις είναι οι

$$([0] + \langle [6]\rangle) = \{[0], [6]\}, \qquad ([2] + \langle [6]\rangle) = \{[2]+[0], [2]+[6]\} = \{[2], [8]\},$$
$$([4] + \langle [6]\rangle) = \{[4]+[0], [4]+[6]\} = \{[4], [10]\}$$ □

Άσκηση 3. Έστω η ομάδα $(\mathbb{Z}_{12}, +)$. Θεωρούμε την ομάδα ευθύ γινόμενο $(\mathbb{Z}_{12}\times\mathbb{Z}_{12}, +)$[2], και έστω $\mathcal{V}$ το ακόλουθο υποσύνολο τής $\mathbb{Z}_{12}\times\mathbb{Z}_{12}$:

$$\mathcal{V} = \big\{([a]_{12}, [b]_{12}) \in \mathbb{Z}_{12}\times\mathbb{Z}_{12} \mid \text{όπου: } 3 \mid a \ \ \& \ \ 3 \mid b\big\}$$

Δείξτε ότι το σύνολο $\mathcal{V}$ είναι μια υποομάδα της $\mathbb{Z}_{12}\times\mathbb{Z}_{12}$ και υπολογίστε τον δείκτη $[\mathbb{Z}_{12}\times\mathbb{Z}_{12} : \mathcal{V}]$.

Λύση. Επειδή το $\mathcal{V}$ είναι ένα πεπερασμένο σύνολο, αφού είναι υποσύνολο τής $\mathbb{Z}_{12}\times\mathbb{Z}_{12}$, η οποία είναι μια ομάδα με τάξη[3]

$$|\mathbb{Z}_{12}\times\mathbb{Z}_{12}| = \mathsf{o}(\mathbb{Z}_{12}\times\mathbb{Z}_{12}) = \mathsf{o}(\mathbb{Z}_{12})\cdot\mathsf{o}(\mathbb{Z}_{12}) = 12^2 = 144$$

είναι αρκετό να αποδείξουμε ότι το σύνολο $\mathcal{V}$ είναι μη-κενό και είναι κλειστό ως προς την πράξη «+» τής $\mathbb{Z}_{12}\times\mathbb{Z}_{12}$.

[2] Υπενθυμίζουμε ότι η πράξη «+» τής $\mathbb{Z}_{12}\times\mathbb{Z}_{12}$ ορίζεται ως $([a]_{12}, [b]_{12}) + ([a']_{12}, [b']_{12}) = ([a+a']_{12}, [b+b']_{12})$.

[3] Υπενθυμίζουμε ότι για την τάξη μιας ομάδας G χρησιμοποιούμε έναν εκ των συμβολισμών: $|G|$, $\mathsf{o}(G)$.

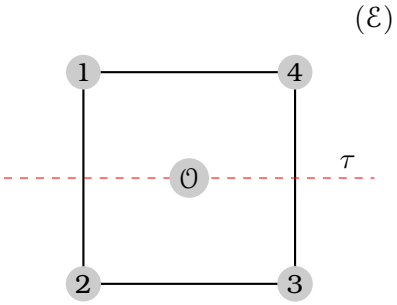
Προφανώς $\mathcal{V} \neq \emptyset$, διότι $([3]_{12}, [3]_{12}) \in \mathcal{V}$. Αν $([a]_{12}, [b]_{12})$ και $([a']_{12}, [b']_{12})$ είναι στοιχεία τού $\mathcal{V}$, τότε και το $([a]_{12}, [b]_{12}) + ([a']_{12}, [b']_{12}) = ([a+a']_{12}, [b+b']_{12})$ είναι στοιχείο τού $\mathcal{V}$, επειδή από $3 \mid a$ και $3 \mid a'$ (αντίστοιχα $3 \mid b$ και $3 \mid b'$) έπεται $3 \mid a + a'$ (αντίστοιχα $3 \mid b + b'$). Επομένως, $\mathcal{V} \leq \mathbb{Z}_{12} \times \mathbb{Z}_{12}$.

Θα υπολογίσουμε το πλήθος των στοιχείων τής $\mathcal{V}$. Παρατηρούμε ότι τα στοιχεία $[a]_{12} \in \mathbb{Z}_{12}$ με $3 \mid a$ είναι τα $[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}$. Γι' αυτό η τάξη τής $\mathcal{V}$ είναι $|\mathcal{V}| = 4^2 = 16$ και ο δείκτης $[\mathbb{Z}_{12} \times \mathbb{Z}_{12} : \mathcal{V}]$ ισούται με

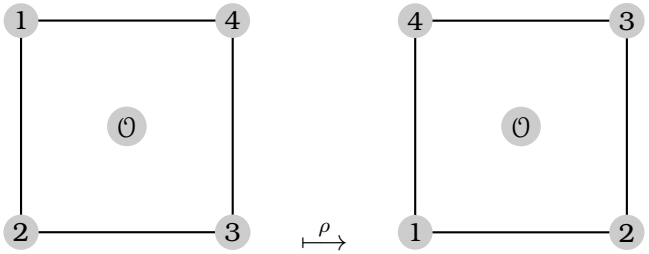
$$[\mathbb{Z}_{12} \times \mathbb{Z}_{12} : \mathcal{V}] = \frac{|\mathbb{Z}_{12} \times \mathbb{Z}_{12}|}{|\mathcal{V}|} = \frac{144}{16} = 9 \qquad \square$$

Άσκηση 4. Θεωρούμε ένα τετράγωνο T στο επίπεδο $(\mathcal{E})$, και έστω $\mathcal{O}$ το σημείο τομής των διαγωνίων του. Έστω $\rho, \tau \colon \mathcal{E} \longrightarrow \mathcal{E}$ οι απεικονίσεις του επιπέδου, όπου (βλέπε το παρακάτω σχήμα):

(1) ρ είναι η στροφή κατά $\pi/2$ (με φορά αντίθετη της φοράς που ακολουθούν οι δείκτες του ρολογιού) του επιπέδου $(\mathcal{E})$ γύρω από τον άξονα που είναι κάθετος στο επίπεδο του τετραγώνου και διέρχεται από το κέντρο συμμετρίας του $\mathcal{O}$, βλέπε το παρακάτω Σχημα 2.



Σχήμα 1. Ανάκλαση τ τετραγώνου ως προς άξονα συμμετρίας ο οποίος διέρχεται από τα μέσα δύο παράλληλων πλευρών του τετραγώνου



Σχήμα 2. Στροφή (με φορά αντίθετη της φορά τοων δεικτών του ρολογιού) ρ του τετραγώνου κατά γωνία $\pi/2$.

(2) τ είναι η στερεά κίνηση (συμμετρία) που προκύπτει από ανάκλαση του επιπέδου ως προς άξονα συμμετρίας ο οποίος διέρχεται από τα μέσα δύο παράλληλων πλευρών του τετραγώνου, βλέπε το παρακάτω Σχημα 1.

Εφοδιάζουμε το σύνολο D_4 με τη σύνθεση $\circ$ απεικονίσεων και γράφουμε απλούστερα $\rho\tau$ αντί $\rho \circ \tau$, ρ^2 αντί $\rho \circ \rho$, κλπ. Να δειχθεί ότι ισχύουν οι σχέσεις $\tau^2 = \iota$, $\rho^4 = \iota$, $\rho\tau = \tau\rho^3$, όπου ι είναι η ταυτοτική απεικόνιση του επιπέδου $\mathcal{E}$, και το σύνολο

$$\mathsf{D}_4 = \left\{\iota,\ \rho,\ \rho^2,\ \rho^3,\ \tau,\ \tau\rho,\ \tau\rho^2,\ \tau\rho^3\right\}$$

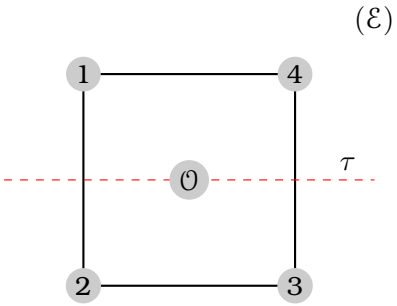
αποτελεί μια μη-αβελιανή ομάδα τάξης 8, η οποία καλείται η **διεδρική ομάδα** D_4 των συμμετριών του τετραγώνου.

Να υπολογιστούν οι αριστερές πλευρικές κλάσεις (τα αριστερά σύμπλοκα) της $\langle\tau\rangle$ στην D_4.

Λύση. Παρατηρώντας ότι ισχύουν οι σχέσεις $\tau^2 = \iota$, $\rho^4 = \iota$, και $\rho\tau = \tau\rho^3$, εύκολα βλέπουμε ότι το σύνολο D_4, θεωρούμενο ως υποσύνολο της ομάδας G όλων των αντιστρέψιμων απεικονίσεων $\mathcal{E} \longrightarrow \mathcal{E}$ με πράξη τη σύνθεση απεικονίσεων, είναι κλειστό στην πράξη της σύνθεσης απεικονίσεων και επομένως, σύμφωνα με γνωστό κριτήριο, αποτελεί ομάδα (υποομάδα της G).

Προφανώς μπορούμε να θεωρήσουμε την διεδρική ομάδα D_4 ως ομάδα (1-1 και επί απεικονίσεων (μεταθέσεων) επί του συνόλου $\{1, 2, 3, 4\}$ των κορυφών του τετραγώνου, και τότε θα έχουμε:

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \quad \& \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$



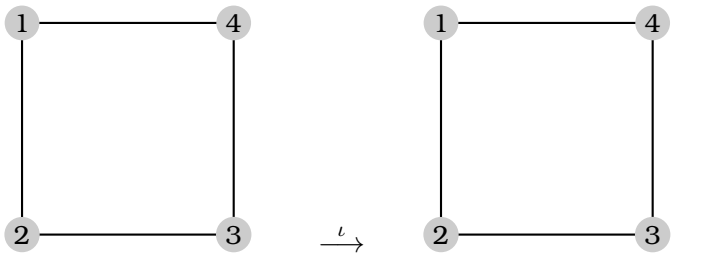
Σχήμα 3. Το τετράγωνο με τον άξονα συμμετρίας τ

Εύκολα βλέπουμε ότι ισχύουν οι σχέσεις $\tau^2 = \iota$, $\rho^4 = \iota$, $\rho\tau = \tau\rho^3$. και η ομάδα D_4 περιγράφεται ως

$$\mathsf{D}_4 = \left\{\iota,\ \rho,\ \rho^2,\ \rho^3,\ \tau,\ \tau\rho,\ \tau\rho^2,\ \tau\rho^3\right\}$$

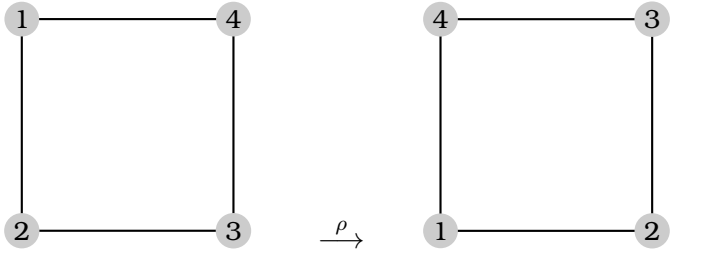
Τα στοιχεία της ομάδας D_4 ως συμμετρίες του τετραγώνου περιγράφονται ως ακολούθως:

(1)



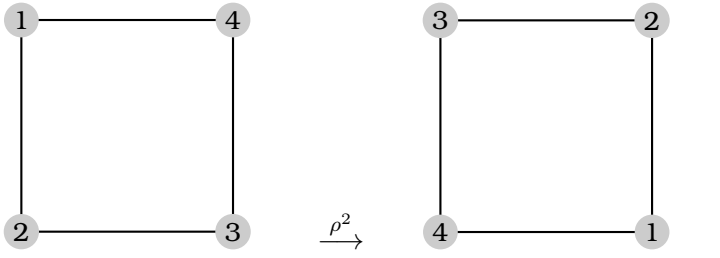
$$\iota = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

(2)



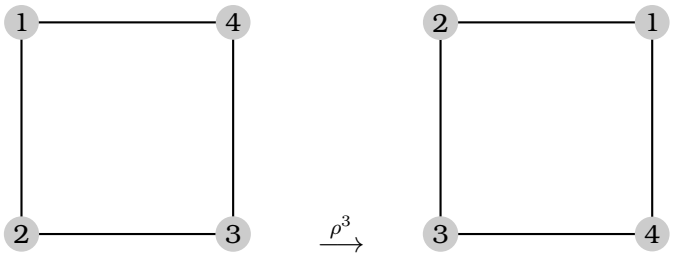
$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

(3)



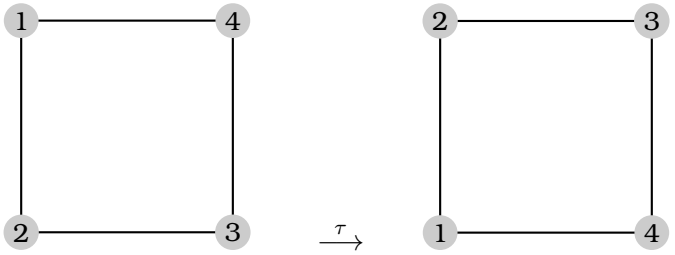
$$\rho^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

(4)



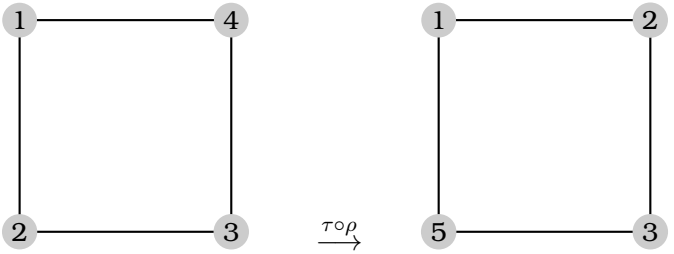
$$\rho^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

(5)



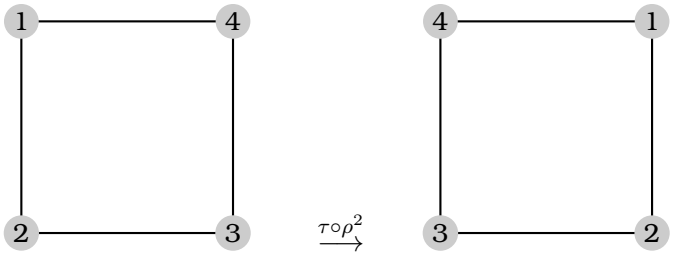
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

(6)



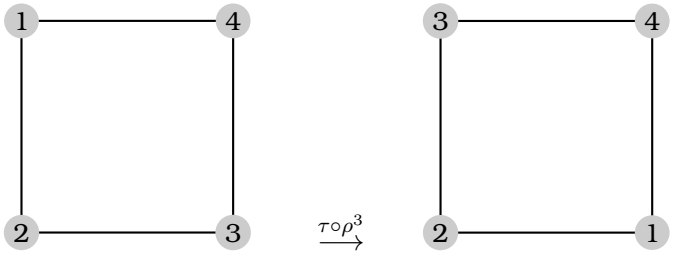
$$\tau\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

(7)



$$\tau\rho^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

(8)



$$\tau\rho^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$$

Η υποομάδα $\langle\tau\rangle = \{\iota, \tau\}$ έχει τάξη 2 και άρα ο δείκτης της στην D_4 είναι

$$[\mathsf{D}_4 : \langle\tau\rangle] = \frac{|\mathsf{D}_4|}{|\langle\tau\rangle|} = \frac{8}{2} = 4$$

Συνεπώς, υπάρχουν ακριβως τέσσερεις αριστερές πλευρικές κλάσεις της $\langle\tau\rangle$ στην D_4. Αυτές είναι οι:

$$\begin{aligned}
\iota\langle\tau\rangle &= \langle\tau\rangle = \{\iota\iota, \iota\tau\} = \{\iota, \tau\} \\
\rho\langle\tau\rangle &= \{\rho\iota, \rho\tau\} = \{\rho, \tau\rho^3\} \\
\rho^2\langle\tau\rangle &= \{\rho^2\iota, \rho^2\tau\} = \{\rho^2, \tau\rho^2\} \\
\rho^3\langle\tau\rangle &= \{\rho^3\iota, \rho^3\tau\} = \{\rho^3, \tau\rho\}
\end{aligned}$$

□

Άσκηση 5. Έστω ότι $(G, \cdot)$ είναι μια ομάδα και ότι $H \leq G$ είναι μια υποομάδα της.

(1) Να δειχθεί ότι το πλήθος των αριστερών πλευρικών κλάσεων της H στην G ισούται με το πλήθος των δεξιών πλευρικών κλάσεων της H στην G.
(2) Να δοθεί παράδειγμα ομάδας $(G, \cdot)$ και υποομάδας H της G, έτσι ώστε $a \in G$ και $aH \neq Ha$.
(3) Να δειχθεί ότι αν μια ομάδα $(G, \cdot)$ είναι αβελιανή, τότε για κάθε $a \in G$ ισχύει[4]: $aH = Ha$.

Λύση. (1) Υπενθυμίζουμε ότι οι αριστερές πλευρικές κλάσεις της υποομάδας H στην G είναι οι διακεκριμένες κλάσεις ισοδυναμίας ως προς την ακόλουθη σχέση ισοδυναμίας $\mathcal{R}_H$ επί της G:

$$\forall x, y \in G: \quad x \sim_{\mathcal{R}_H} y \quad \Longleftrightarrow \quad x^{-1} \cdot y \in H$$

Τότε η κλάση ισοδυναμίας $[x]_H := [x]_{\mathcal{R}_H}$ του $x \in G$ ως προς την $\mathcal{R}_H$ είναι η αριστερή πλευρική κλάση $xH = \{xh \in G \mid h \in H\}$.

Παρόμοια οι δεξιές πλευρικές κλάσεις της υποομάδας H στην G είναι οι διακεκριμένες κλάσεσι ισοδυναμίας ως προς την ακόλουθη σχέση ισοδυναμίας ${}_H\mathcal{R}$ επί της G:

$$\forall x, y \in G: \quad x \sim_{{}_H\mathcal{R}} y \quad \Longleftrightarrow \quad x \cdot y^{-1} \in H$$

και η κλάση ισοδυναμίας ${}_H[x] := [x]_{{}_H\mathcal{R}}$ του $x \in G$ ως προς την ${}_H\mathcal{R}$ είναι η δεξιά πλευρική κλάση $Hx = \{hx \in G \mid h \in H\}$.

Θεωρούμε τα σύνολα πηλίκα

$$G/\mathcal{R}_H = \{[x]_H = xH \subseteq G \mid x \in G\} \quad \& \quad G/{}_H\mathcal{R} = \{{}_H[x] = Hx \subseteq G \mid x \in G\}$$

και ορίζουμε:

$$\psi: G/\mathcal{R}_H \longrightarrow G/{}_H\mathcal{R}, \quad \psi(xH) = Hx^{-1}$$

θα δείξουμε ότι η ψ είναι μια 1-1 και επί απεοκόνιση.

• Κατ' αρχήν η ψ είναι καλά ορισμένη: έστω $xH = yH$ και άρα $x \sim_{\mathcal{R}_H} y$. Τότε $x^{-1} \cdot y \in H$. Έστω $x^{-1} \cdot y = h \in H$. Τότε $x^{-1} = h \cdot y^{-1} \in H \cdot y^{-1} = {}_H[y^{-1}]$. Όπως γνωρίζουμε τότε τα στοιχεία x^{-1} και y^{-1} ορίζουν την ίδια κλάση ισοδυναμίας ως προς την σχέση ισοδυναμίας ${}_H\mathcal{R}$ και επομένως θα έχουμε ${}_H[x^{-1}] = {}_H[y^{-1}]$. Αυτό όμως σημαίνει ότι $Hx^{-1} = Hy^{-1}$ και άρα $\psi(xH) = \psi(yH)$, δηλαδή η ψ είναι καλά ορισμένη.

• Έστω $\psi(xH) = \psi(yH)$, δηλαδή $Hx^{-1} = Hy^{-1}$ ή ισοδύναμα ${}_H[x^{-1}] = {}_H[y^{-1}]$. Τότε όμως $x^{-1} \sim_{{}_H\mathcal{R}} y^{-1}$ και άρα $x^{-1} \cdot (y^{-1})^{-1} \in H$. Δηλαδή $x^{-1} \cdot y \in H$ και επομένως $x^{-1} \cdot y = h \in H$. Τότε $y = x \cdot h \in xH = [x]_H$ και άρα $[y]_H = [x]_H \implies yH = xH$. Επομένως η ψ είναι 1-1.

• Έστω ${}_H[z] = Hz \in G/{}_H\mathcal{R}$. Τότε προφανώς $\psi([z^{-1}]_H) = \psi(z^{-1}H) = H(z^{-1})^{-1} = Hz = {}_H[z]$ και άρα η ψ είναι επί.

Επομένως το πλήθος των αριστερών πλευρικών κλάσεων της H στην G ισούται με το πλήθος των δεξιών πλευρικών κλάσεων της H στην G, και, όπως γνωρίζουμε, αυτή η κοινή τιμή ορίζεται να είναι ο δείκτης $[G : H]$ της H στην G.

---

[4] Το αντίστροφο δεν ισχύει: υπάρχουν μη-αβελιανές ομάδες οι οποίες περιέχουν μια υποομάδα H έτσι ώστε: $aH = Ha$, $\forall a \in G$. Για παράδειγμα μπορούμε να θεωρήσουμε την συμμετρική ομάδα S_3 και την υποομάδα $K = \langle\rho_1\rangle$, βλέπε την Άσκηση 1.

(2) Θεωρούμε τη συμμετρική ομάδα $\mathsf{S}_3 := G$ και την υποομάδα της $\langle \mu_1 \rangle := H$, βλέπε την Άσκηση 1. Τότε όπως είδαμε $\rho_1 H \neq H\rho_1$.

(3) Αν η G είναι αβελιανή, θα έχουμε:

$$aH = \{ah \in G \mid h \in H\} = \{ha \in G \mid h \in H\} = Ha$$ □

Άσκηση 6. Έστω $(G, \cdot)$ μια ομάδα και H, K δύο υποομάδες της G. Αν a, b είναι δύο στοιχεία τής G, να δείξετε ότι:

(1) $aH = bK \implies H = K$.
(2) Δεν είναι πάντοτε αληθής η συνεπαγωγή[5]: $aH = Kb \implies H = K$.

Λύση. (1) Αν $aH = bK$, όπου $a, b \in G$, τότε προφανώς θα έχουμε $H = a^{-1}bK$ και επομένως $a^{-1}b \in H$. Αλλά από τη σχέση $a^{-1}b \in H$ έπεται ότι $b \in aH$ και συνεπώς $bH = aH$. Αφού από την υπόθεση είναι $aH = bK$, συμπεραίνουμε ότι $bH = bK$ και συνεπώς $H = b^{-1}(bH) = b^{-1}(bK) = K$.

(2) Επιλέγουμε τις κυκλικές υποομάδες

$$H = \left\langle \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\rangle \quad \& \quad K = \left\langle \mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\rangle$$

τής S_3. Έχουμε:

$$\mu_2 H = \left\{ \mu_2, \ \mu_2 \circ \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \rho_1 \right\} \quad \& \quad K\mu_2 = \left\{ \mu_2, \ \mu_1 \circ \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \rho_1 \right\}$$

Ώστε, $\mu_2 H = K\mu_2$, ενώ $H \neq K$. □

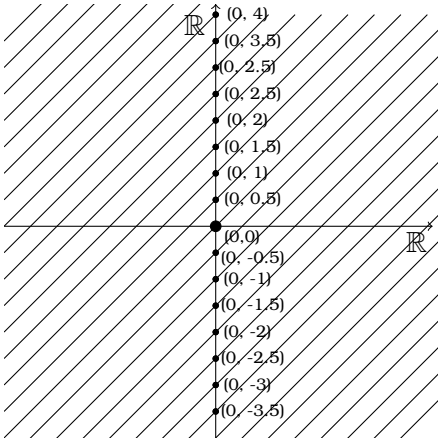
Άσκηση 7. (1) Βρείτε τον δείκτη $[G : H]$ της υποομάδας $H \leq G$ στις ακόλουθες περιπτώσεις:
(α') $H = n\mathbb{Z}$ και $G = \mathbb{Z}$.
(β') $H = \{(x, y) \in \mathbb{R} \times \mathbb{R} \mid x = y\}$ και $G = \mathbb{R} \times \mathbb{R}$ είναι η ομάδα ευθύ γινόμενο της προσθετικής ομάδας $(\mathbb{R}, +)$ με τον εαυτό της.
(2) Βρείτε μια υποομάδα H της πολλαπλασιαστικής ομάδας $(\mathbb{R}^*, \cdot)$ έτσι ώστε: $[\mathbb{R}^* : H] = 2$.

Λύση. (1) (α') Επειδή οι ομάδες $\mathbb{Z}$ και $n\mathbb{Z}$ είναι άπειρες, για να υπολογίσουμε τον δείκτη ης $n\mathbb{Z}$ στην $\mathbb{Z}$, θα πρέπει να υπολογίσουμε το πλήθος των διακεκριμένων πλευρικών κλάσεων της $n\mathbb{Z}$ στην $\mathbb{Z}$. Επειδή η ομάδα $\mathbb{Z}$ είναι αβελιανή δεν χρειάζεται να γίνει διάκριση μεταξύ αριστερών και δεξιών πλευρικών κλάσεων. Όπως αναφέρθηκε και στην προηγούμενη Άσκηση 5, οι πλευρικές κλάσεις της $n\mathbb{Z}$ στην $\mathbb{Z}$ είναι οι κλάσεις ισοδυναμίας των στοιχείων της $\mathbb{Z}$ ως προς τη σχέση ισοδυναμίας: $\forall x, y \in \mathbb{Z}$: $x \sim_{\mathcal{R}_{\mathbb{Z}_n}} y$ αν και μόνον αν $-x + y \in n\mathbb{Z}$. Αυτό είναι ισοδύναμο με: $n \mid x - y$, και επομένως οι διακεκριμένες πλευρικές κλάσεις της $n\mathbb{Z}$ στην $\mathbb{Z}$ είναι οι κλάσεις υπολοίπων mod n, δηλαδή τα στοιχεία του συνόλου: $\{[0]_n, [1]_n, \cdots, [n-1]_n\}$. Επομένως θα έχουμε:

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

(1) (β') Εύκολα βλέπουμε ότι το υποσύνολο H είναι υποομάδα της ομάδας ευθύ γινόμενο $\mathbb{R} \times \mathbb{R}$. Πράγματι, έχουμε προφανώς $(0, 0) \in H$, ιδιαίτερα $H \neq \emptyset$. Αν $(x, x), (y, y) \in H$, τότε $-(x, x) + (y, y) = (-x, -x) + (y, y) = (-x + y, -x + y) \in H$. Άρα $H \leq \mathbb{R} \times \mathbb{R}$. Επειδή η ομάδα ευθύ γινόμενο $\mathbb{R} \times \mathbb{R}$ είναι αβελιανή δεν χρειάζεται να κάνουμε διάκριση μεταξύ αριστερών και δεξιών πλευρικών κλάσεων.

[5] Χρησιμοποιείστε, ως αντιπαράδειγμα, υποομάδες και στοιχεία τής συμμετρικής ομάδας $(\mathsf{S}_3, \circ)$.



Παρατηρούμε ότι η πλευρική κλάση τού στοιχείου $(r_1, r_2) \in \mathbb{R} \times \mathbb{R}$ ισούται με

$$(r_1, r_2) + H = \{(r_1, r_2) + (x, x) \in \mathbb{R} \times \mathbb{R} \mid x \in \mathbb{R}\}.$$

Θεωρούμε την απεικόνιση

$$\Phi : (\mathbb{R} \times \mathbb{R})/\mathcal{R}_H \longrightarrow \mathbb{R}, \quad (r_1, r_2) + H \longmapsto r_2 - r_1$$

Πρόκειται για μια καλά ορισμένη απεικόνιση, αφού αν, $(r_1, r_2) + H = (r_1', r_2') + H$, τότε

$$(r_1, r_2) - (r_1', r_2') \in H \implies r_1 - r_1' = r_2 - r_2' \implies r_2 - r_1 = r_2' - r_1' \implies \Phi\big((r_1, r_2) + H\big) = \Phi\big((r_1', r_2') + H\big)$$

Προφανώς πρόκειται για «επί» απεικόνιση, αφού αν $r \in \mathbb{R}$, τότε η εικόνα μέσω της Φ της πλευρικής κλάσης $(0, r) + H$ είναι το στοιχείο r. Τέλος, η Φ είναι και «1-1», αφού αν $\Phi((r_1, r_2) + H) = \Phi((r_1', r_2') + H)$, τότε θα έχουμε $r_2 - r_1 = r_2' - r_1' \implies r_1 - r_2 = r_1' - r_2'$, και τότε $(r_1, r_2) + H = (r_1', r_2') + H$.

Ώστε υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ τού συνόλου πηλίκο $(\mathbb{R} \times \mathbb{R})/\mathcal{R}_H$ των κλάσεων ισοδυναμίας που ορίζεται από την υποομάδα H και της ευθείας $\mathbb{R}$ των πραγματικών αριθμών.

Στο παραπάνω σχήμα οι κλάσεις ισοδυναμίας, δηλαδή οι πλευρικές κλάσεις της H στην $\mathbb{R} \times \mathbb{R}$, είναι οι ευθείες που είναι παράλληλες ως προς την ευθεία που διέρχεται από την αρχή των συντεταγμένων και σχηματίζει γωνία $\pi/4$ με τον άξονα των x. Η τομή κάθε ευθείας με τον άξονα των y χορηγεί την απεικόνιση Φ που περιγράψαμε προηγουμένως.

(2) Θεωρούμε το υποσύνολο

$$\mathbb{R}^{>0} = \{x \in \mathbb{R} \mid x > 0\} \subseteq \mathbb{R}^*$$

το οποίο είναι μια υποομάδα της πολλαπλασιαστικής αβελιανής ομάδας $\mathbb{R}^*$, διότι $1 \in \mathbb{R}^{>0}$, και αν $x, y \in \mathbb{R}^{>0}$, τότε $xy \in \mathbb{R}^{>0}$ και $x^{-1} \in \mathbb{R}^{>0}$.

Οι πλευρικές κλάσεις των στοιχείων 1 και -1 είναι:

$$1\mathbb{R}^{>0} = \{1 \cdot x = x \in \mathbb{R}^* \mid x \in \mathbb{R}^{>0}\} = \mathbb{R}^{>0}$$

$$(-1)\mathbb{R}^{>0} = \{(-1) \cdot x = -x \in \mathbb{R}^* \mid x \in \mathbb{R}^{>0}\} = \{x \in \mathbb{R}^* \mid x \in \mathbb{R}^{<0}\} = \mathbb{R}^{<0}$$

και προφανώς αποτελούν μια διαμέριση της $\mathbb{R}^*$. Επομένως αυτά είναι όλα τα διακεκριμένα (αριστερά) σύμπλοκα της $\mathbb{R}^{>0}$ στην $\mathbb{R}^*$. Αυτό σημαίνει ότι[6]

$$[\mathbb{R}^* : \mathbb{R}^{>0}] = 2 \qquad \square$$

Άσκηση 8. Έστω ότι $(G, \cdot)$ είναι μια ομάδα και $H, K \leq G$ είναι δύο υποομάδες τής G οι οποίες έχουν ως τάξη τον ίδιο πρώτο αριθμό p. Αν $H \neq K$, τότε δείξτε ότι $H \cap K = \{e\}$.

[6] Ένας διαφορετικός τρόπος: εύκολα βλέπουμε ότι δύο στοιχεία x, y της $\mathbb{R}^*$ είναι ισοδύναμα ως προς την σχέση ισοδυναμίας $\mathcal{R}_{\mathbb{R}^{>0}}$ την οποία ορίζει η υποομάδα $\mathbb{R}^{>0}$ επί της $\mathbb{R}^*$ αν και μόνον αν $xy > 0$, δηλαδή αν και μόνον αν τα x, y είναι ομόσημα. Συμβολίζοντας με $\mathbb{R}^*/\mathbb{R}^{>0}$ το σύνολο των αριστερών συμπλόκων της $\mathbb{R}^{>0}$ στην $\mathbb{R}^*$, ορίζουμε τότε απεικόνιση

$$\Phi : \mathbb{R}/\mathbb{R}^{>0} \longrightarrow \{-1, 1\}, \quad \Phi(x\mathbb{R}^{>0}) = 1, \ \text{ αν } \ x > 0 \ \text{ και } \ \Phi(x\mathbb{R}^{>0}) = -1, \ \text{ αν } \ x < 0$$

η οποία βλέπουμε ότι είναι καλά ορισμένη, «1-1» και «επί». Επομένως $[\mathbb{R}^* : \mathbb{R}^{>0}] = |\mathbb{R}/\mathbb{R}^{>0}| = 2$.

Λύση. Παρατηρούμε ότι η $H \cap K$ είναι υποομάδα και τής H και τής K. Από το Θεώρημα Lagrange συμπεραίνουμε ότι η τάξη $|H \cap K|$ είναι ένας διαιρέτης και τής τάξης p τής H και τής τάξης p τής K. Συνεπώς, θα είναι ή $|H \cap K| = 1$ ή $|H \cap K| = p$, αφού ο p είναι πρώτος αριθμός. Όμως αν ήταν $|H \cap K| = p$, τότε θα ήταν $H \cap K = H$ και $H \cap K = K$ (αφού $H \cap K \leq H$ και $H \cap K \leq K$) και γι' αυτό $H = H \cap K = K$. Αλλά από την υπόθεση γνωρίζουμε ότι $H \neq K$. Επομένως, $|H \cap K| = 1$ και έτσι $H \cap K = \{e\}$. □

Άσκηση 9. Έστω G μια ομάδα τάξης pq, όπου p και q είναι πρώτοι αριθμοί και $p \neq q$. Να δειχθεί ότι κάθε γνήσια υποομάδα της G είναι κυκλική.

Είναι αληθές ότι μια τέτοια ομάδα είναι κυκλική;

Λύση. Έστω H μια γνήσια υποομάδα της G. Αοό το Θεώρημα του Lagrange έπεται ότι $|H| \mid |G| = pq$ και επομένως θα έχουμε: $|H| = 1$ ή p ή q. Αν $|H| = 1$, τότε $H = \{e\} = \langle e \rangle$ είναι κυκλική. Επειδή κάθε ομάδα με τάξη έναν πρώτο αριθμό είναι κυκλική, αν $|H| = p$ ή $|H| = q$, έπεται ότι η G είναι κυκλική.

Η συμμετρική ομάδα S_3 τάξης $|\mathsf{S}_3| = 6 = 2 \cdot 3$ δεν είναι κυκλική, και άρα, γενικά, μια ομάδα τάξης pq, όπου p και q είναι διαφορετικοί πρώτοι, δεν είναι απαραίτητα κυκλική. □

Άσκηση 10. Αν $(G, \cdot)$ είναι μια ομάδα με τάξη $\mathsf{o}(G) = |G| < 300$, η οποία έχει δύο υποομάδες H και K με τάξεις αντιστοίχως $\mathsf{o}(H) = |H| = 24$ και $\mathsf{o}(K) = |K| = 54$, τότε ποια είναι η τάξη $\mathsf{o}(G) = |G|$ της G;

Λύση. Από το Θεώρημα του Lagrange, θα έχουμε:

$$24 = \mathsf{o}(H) \mid \mathsf{o}(G) \quad \& \quad 54 = \mathsf{o}(K) \mid \mathsf{o}(G)$$

Τότε όμως θα έχουμε ότι και το ελάχιστο κοινό πολλαπλάσιο των 24 και 54 θα διαιρεί την τάξη της G:

$$216 = [24, 54] \mid \mathsf{o}(G) \quad \text{και άρα} \quad \mathsf{o}(G) = 216 \cdot k, \quad \text{για κάποιο} \ \ k \geq 1$$

Επειδή $\mathsf{o}(G) < 300$, αναγκαστικά θα έχουμε: $\mathsf{o}(G) = 216$. □

Άσκηση 11. Έστω ότι p, q είναι πρώτοι αριθμοί, και $(G, \cdot)$ μια ομάδα. Να δειχθεί ότι:

(α) Αν η G είναι *αβελιανή* με τάξη pq και $p \neq q$, τότε η G είναι κυκλική.

(β) Υπάρχουν αβελιανές ομάδες τάξης p^2 οποίες δεν είναι κυκλικές.

Λύση. (α) Επειδή $\mathsf{o}(G) = pq$ και οι p, q ως πρώτοι αριθμοί είναι ≥ 2 με $p \neq q$, συμπεραίνουμε ότι $\mathsf{o}(G) = p \cdot q \geq 2 \cdot 3 = 6$. Επομένως υπάρχει $a \in G$ με $a \neq e$, δηλαδή $G \setminus \{e\} \neq \emptyset$.

Έστω $a \in G \setminus \{e_G\}$. Θεωρούμε την κυκλική υποομάδα $\langle a \rangle$. Προφανώς, $\langle a \rangle \neq \{e\}$.

(1) Αν η τάξη τής κυκλικής υποομάδας $\langle a \rangle$ ισούται με pq (ισοδύναμα $\mathsf{o}(a) = pq$), τότε $\langle a \rangle = G$ και η G είναι κυκλική.

(2) Αν η τάξη τής κυκλικής υποομάδας $\langle a \rangle$ ισούται με έναν από τους πρώτους p ή q, ας πούμε τον p (η απόδειξη είναι ανάλογη όταν ισούται με q), τότε το σύνολο $G \setminus \langle a \rangle$ έχει $pq - p = (q-1)p > 1$ στοιχεία. Έστω $b \in G \setminus \langle a \rangle$. Θεωρούμε την κυκλική υποομάδα $\langle b \rangle$. Προφανώς, $\langle b \rangle \neq \{e\}$, αφού $b \neq e$. Η τάξη τής κυκλικής υποομάδας $\langle b \rangle$ (δηλαδή η τάξη τού b) θα είναι (και πάλι λόγω τού Θεωρήματος Lagrange) ή pq ή p ή q. Προφανώς, $\langle b \rangle \neq \langle a \rangle$, αφού $b \notin \langle a \rangle$.

(3) Αν η τάξη τής κυκλικής υποομάδας $\langle b \rangle$ ισούται με pq (ισοδύναμα $\mathsf{o}(b) = pq$), τότε $\langle b \rangle = G$ και η G είναι κυκλική.

(4) Υπολείπονται οι περιπτώσεις όπου $\mathsf{o}(\langle b \rangle) = p$ ή $\mathsf{o}(\langle b \rangle) = q$. Θα αποκλείσουμε την πρώτη περίπτωση.

Πρώτα παρατηρούμε ότι, επειδή η ομάδα G είναι αβελιανή, το σύνολο

$$H = \langle a \rangle \cdot \langle b \rangle := \big\{ xy \in G \mid x \in \langle a \rangle, \ y \in \langle b \rangle \big\}$$

είναι μια υποομάδα τής G. Πράγματι το υποσύνολο H είναι προφανώς μη-κενό, είναι πεπερασμένο αφού περιέχεται στην πεπερασμένη ομάδα G, και είναι κλειστό ως προς την πράξη τής

G. Πράγματι, αν $x, y \in H$, τότε θα έχουμε $x = a^{i_1}b^{j_1}$ και $y = a^{i_2}b^{j_2}$ για κάποιους ακέραιους i_1, j_i, i_2, j_2. Τότε, χρησιμοποιώντας ότι η ομάδα η G είναι αβελιανή, θα έχουμε:

$$xy = (a^{i_1}b^{j_1})(a^{i_2}b^{j_2}) = a^{i_1}a^{i_2}b^{j_1}b^{j_2} = a^{i_1+i_2}b^{j_1+j_2} \ \in \ H$$

Άρα $H \leq G$.

Τώρα θα αποδείξουμε ότι αν η τάξη της κυκλικής υποομάδας $\langle b\rangle$ ήταν ίση με p, τότε η τάξη $\mathsf{o}(H)$ της H θα ήταν ίση με p^2, πράγμα άτοπο, αφού τότε θα είχαμε, λόγω τού Θεωρήματος Lagrange, ότι το p^2 διαιρεί το pq, ή ισοδύναμα ότι το p διαιρεί το q.

Πράγματι, αν $\mathsf{o}(\langle b\rangle) = p$, τότε λόγω τής Άσκησης 8, είναι $\langle a\rangle \cap \langle b\rangle = \{e\}$, επειδή $\mathsf{o}(\langle a\rangle) = \mathsf{o}(\langle b\rangle) = p$ και αφού όπως είδαμε $\langle a\rangle \neq \langle b\rangle$.

Ας υπολογίσουμε την τάξη τής H. Επειδή $H = \{a^ib^j | 1 \leq i, j \leq p\}$, έπεται ότι $\mathsf{o}(H) \leq p^2$. Αλλά καθώς τα i και j διατρέχουν το σύνολο $I_p = \{1, 2, \ldots, p\}$, τα στοιχεία a^ib^j είναι ανά δύο διακεκριμμένα. Πράγματι, αν

$$a^{i_1}b^{j_1} = a^{i_2}b^{j_2}, \quad \text{όπου} \quad i_1, i_2, j_1, j_2 \in I_p \tag{$*$}$$

τότε το στοιχείο $a^{i_1-i_2} = b^{j_2-j_1}$ ανήκει στην τομή $\langle a\rangle \cap \langle b\rangle = \{e\}$ και γι' αυτό

$$a^{i_1-i_2} = b^{j_2-j_1} = e \tag{$**$}$$

Αφού είναι $1 \leq i_1 \neq i_2 \leq p$ θα είναι ή $i_1 > i_2$ ή $i_1 < i_2$. Στην πρώτη περίπτωση η $(**)$ δίνει ότι η τάξη τού a είναι μικρότερη από p και στη δεύτερη περίπτωση από την $(**)$ παίρνουμε ότι $a^{i_2-i_1} = e$ από όπου και πάλι έπεται ότι η τάξη τού a είναι μικρότερη από p. Αλλά αυτό είναι και στις δύο περιπτώσεις άτοπο. Όμοια αποδεικνύεται ότι είναι αδύνατο να ισχύει $b^{j_1} = b^{j_2}$ με $j_1, j_2 \in I_p$ και $j_1 \neq j_2$. Ώστε $\circ(H) = p^2$.

Επομένως, η τάξη τού στοιχείου b δεν μπορεί να είναι ούτε p. Επομένως, η τάξη τού b είναι q.

(5) Τώρα θεωρούμε το στοιχείο ab. Επειδή $\mathsf{o}(a) = p$ και $\mathsf{o}(b) = q$, όπου $p \neq q$ πρώτοι αριθμοί και επειδή $ab = ba$, διότι η G είναι αβελιανή, συμπεραίνουμε ότι η τάξη τού ab είναι pq. Ώστε η G έχει σε κάθε περίπτωση ένα στοιχείο τάξης $pq = |G|$ και γι' αυτό είναι πάντοτε κυκλική.

(β) Η ομάδα του Klein $V_4 = \{e, a, b, c\}$, για παράδειγμα το ισοδύναμο μοντέλο της $\mathbb{Z}_2 \times \mathbb{Z}_2$, είναι μια μη-κυκλική ομάδα τάξης $4 = 2^2$. □

Άσκηση 12. Έστω ότι $(G, \cdot)$ είναι μια πεπερασμένη αβελιανή ομάδα και m είναι το μέγιστο τού συνόλου $\mathcal{M} = \{\mathsf{o}(a) \in \mathbb{N} \mid a \in G\}$ των τάξεων των στοιχείων τής G:

$$m = \mathsf{max}\big\{\mathsf{o}(a) \in \mathbb{N} \mid a \in G\big\}$$

Να δειχθεί ότι $\forall a \in G$: $a^m = e$.

Λύση. Έστω ότι $g \in G$ είναι ένα στοιχείο τής G με τάξη $\mathsf{o}(g) = m$ το μέγιστο τού συνόλου $\mathcal{M}$ και ότι $a \in G$ είναι οποιοδήποτε στοιχείο τής G.

Ισχυρισμός: Θα δείξουμε ότι αν, $p^\sigma, \sigma \in \mathbb{N}$ είναι η μέγιστη δύναμη ενός οποιουδήποτε πρώτου p που διαιρεί την τάξη του a, τότε η δύναμη p^σ είναι επίσης διαιρέτης της τάξης $\mathsf{o}(g) = m$.

Απόδειξη του Ισχυρισμού: Θεωρούμε την τάξη $\mathsf{o}(a)$ και την γράφουμε ως $\mathsf{o}(a) = p^\sigma\kappa$, όπου ο p δεν διαιρεί τον $\kappa \in \mathbb{N}$, δηλαδή $(p, \kappa) = 1$. Θεωρούμε επίσης την τάξη $\mathsf{o}(g)$ και την γράφουμε ως $\mathsf{o}(g) = p^\tau\mu$, όπου $\tau \in \mathbb{N} \cup \{0\}$ και όπου ο p δεν διαιρεί τον $\mu \in \mathbb{N}$, δηλαδή $(p, \mu) = 1$. Τώρα σχηματίζουμε τα στοιχεία a^κ και g^{p^τ}. Η τάξη τού a^κ είναι p^σ και του g^{p^τ} είναι μ. Παρατηρώντας ότι $(p^\sigma, \mu) = 1$ και επειδή τα στοιχεία a^κ και g^{p^τ} μετατίθενται μεταξύ τους, αφού η G είναι αβελιανή, συμπεραίνουμε ότι η τάξη τού $a^\kappa g^{p^\tau}$ ισούται με $p^\sigma\mu$. Όμως, επειδή το g έχει τη μέγιστη τάξη $p^\tau\mu$ μεταξύ των τάξεων όλων των στοιχείων τής G, συμπεραίνουμε ότι $p^\sigma\mu \leq p^\tau\mu$ και συνεπώς $p^\sigma \leq p^\tau$. Ώστε η δύναμη p^σ διαιρεί την τάξη $\mathsf{o}(g) = m$ του g. Αυτό ακριβώς που θέλαμε να αποδείξουμε στον ισχυρισμό.

Έστω τώρα $\mathsf{o}(a) = k$. Αν $k = 1$, τότε προφανώς $a = e$ και δεν έχουμε τίποτα να αποδείξουμε, καθώς $e^m = e$. Έστω $k = p_1^{r_1} \cdot p_2^{r_2} \cdots p_t^{r_t}$ η πρωτογενής ανάλυση του a. Σύμφωνα με τον Ισχυρισμό, θα έχουμε:

$$p_i^{r_i} \ \mid \ m = \mathsf{o}(g), \quad 1 \leq i \leq t$$

Τότε όμως προφανώς θα έχουμε και $\mathsf{o}(a) = k = p_1^{r_1} \cdot p_2^{r_2} \cdots p_t^{r_t} \mid m = \mathsf{o}(g)$. Επομένως $m = \mathsf{o}(g) = \lambda \cdot \mathsf{o}(a)$, για κάποιο $\lambda \in \mathbb{N}$ από όπου έπεται ότι

$$a^m = a^{\lambda \mathsf{o}(a)} = (a^{\mathsf{o}(a)})^\lambda = e^\lambda = e \qquad \square$$

Άσκηση 13. Ο **εκθέτης** μιας ομάδας G, αν υπάρχει, ορίζεται να είναι ο ελάχιστος φυσικός αριθμός m έτσι ώστε: $g^m = e$, $\forall g \in G$, και συμβολίζεται[7] με $\mathsf{exp}(G)$. Αν δεν υπάρχει τέτοιος αριθμός, ορίζουμε $\mathsf{exp}(G) = \infty$.

(1) Δείξτε ότι ο εκθέτης υπάρχει για κάθε πεπερασμένη ομάδα G.
(2) Υπάρχουν ομάδες άπειρης τάξης με πεπερασμένο εκθέτη.
(3) Αν η $G = \{g_1, g_2, \cdots, g_n\}$ είναι πεπερασμένη αβελιανή ομάδα, δείξτε ότι:
   (a)
   $$\mathsf{exp}(G) = \big[\mathsf{o}(g_1), \mathsf{o}(g_2), \cdots, \mathsf{o}(g_n)\big]$$
   (b) Δείξτε ότι υπάρχει στοιχείο $g \in G$: $\mathsf{o}(g) = \mathsf{exp}(G)$.

Λύση. (1) Αν η ομάδα G είναι πεπερασμένη, τότε όπως έχουμε δείξει θα έχουμε $a^{|G|} = e$, $\forall a \in G$. Άρα το σύνολο $\{m \in \mathbb{N} \mid a^m = e,\ \forall a \in G\} \neq \emptyset$, και επομένως θα έχει ελάχιστο στοιχείο m. Τότε εξ' ορισμού $m = \mathsf{exp}(G) < \infty$.

(2) Θεωρούμε την προσθετική ομάδα $\mathbb{Z}_2$ των κλάσεων υπολοίπων mod 2. Τότε προφανώς $2x = 0$, $\forall x \in \mathbb{Z}_2$. Έστω G η ομάδα ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$, τα στοιχεία της οποίας είναι ακολουθίες $(x_i)_{i\geq 1}$ στοιχείων της $\mathbb{Z}_2$. Λαμβάνοντας υπ' όψιν τον ορισμό της πράξης στην G, θα έχουμε ότι $2(x_i)_{i\geq 1} = (2x_i)_{i\geq 1} = (0)_{i\geq 1}$ είναι η μηδενική ακολουθία, η οποία είναι το ουδέτερο στοιχείο της G. Επομένως βλέπουμε ότι $\mathsf{exp}(G) = 2$, και προφανώς η ομάδα G είναι άπειρης τάξης.

(3)(α) Επειδή $\forall i = 1, 2, \cdots, n$: $g_i^{\mathsf{exp}(G)} = e$, έπεται ότι θα έχουμε $\mathsf{o}(g_i) \mid \mathsf{exp}(G)$, $1 \leq i \leq n$, και επομένως $m := [\mathsf{o}(g_1), \mathsf{o}(g_2), \cdots, \mathsf{o}(g_n)] \mid \mathsf{exp}(G)$. Ιδιαίτερα $m \leq \mathsf{exp}(G)$.

Από την άλλη πλευρά, $m = \mathsf{o}(g_i)k_i$, για κάποιους θετικούς ακέραιους $1 \leq i \leq n$. Τότε:

$$\forall i = 1, 2, \cdots, n: \quad g_i^m = g_i^{\mathsf{o}(g_i)k_i} = (g_i^{\mathsf{o}(g_i)})^{k_i} = e$$

Άρα $x^m = e$, $\forall x \in G$, και επομένως $\mathsf{exp}(G) \leq m$. Συνοψίζοντας θα έχουμε:

$$\mathsf{exp}(G) = m = [\mathsf{o}(g_1), \mathsf{o}(G_2, \cdots, \mathsf{o}(g_n)]$$

(3)(β) <u>Ισχυρισμός</u>: η G περιέχει ένα στοιχείο g του οποίου η τάξη είναι το ελάχιστο κοινό πολλαπλάσιο των τάξεων όλων των στοιχείων της G:

$$\exists g \in G: \quad \mathsf{o}(g) = [\mathsf{o}(g_1), \mathsf{o}(g_2), \cdots, \mathsf{o}(g_n)]$$

Αν αποδείξουμε τον παραπάνω ισχυρισμό, τότε από το (3)(α) θα έχουμε ότι υπάρχει ένα στοιχείο g στην G με τάξη τον εκθέτη της G.

Η απόδειξη του ισχυρισμού, θα γίνει σε τρία βήματα:

- <u>Βημα 1</u>: Δείχνουμε πρώτα ότι:

«αν $x, y \in G$ και $\mathsf{o}(x) = m,\ \mathsf{o}(y) = n,$ τότε υπάρχει ένα στοιχείο $z \in G$ έτσι ώστε: $\mathsf{o}(z) = [m, n]$»

Για τους θετικούς ακεραίους m, n από την Θεωρία Αριθμών, μπορούμε να γράψουμε:

$$m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} \qquad \text{και} \qquad n = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$$

όπου οι $p_1, p_2, \cdots, p_k$ είναι διακεκριμμένοι πρώτοι αριθμοί, και $e_i, f_i \geq 0$, $1 \leq i \leq k$. Χωρίς βλάβη της γενικότητας, (εν ανάγκη αναδιατάσσοντας τους πρώτους αριθμούς $p_1, p_2, \cdots, p_k$), μπορούμε να υποθέσουμε ότι:

$$e_1 \leq f_i,\ \cdots,\ e_j \leq f_j \qquad \text{και} \qquad e_{j+1} \geq f_{j+1},\ \cdots,\ e_k \geq f_k, \qquad \text{για κάποιο} \quad 1 \leq j \leq k$$

[7] Αν η ομάδα είναι προσθετική, τότε ο εκθέτης της G είναι ο ελάχιστος φυσικός αριθμός m έτσι ώστε: $mg = 0$, $\forall g \in G$, ή ∞ αν δεν υπάρχει τέτοιος φυσικός αριθμός m.

Θέτοντας

$$r = p_1^{e_1} p_2^{e_2} \cdots p_j^{e_j} \qquad \text{και} \qquad s = p_{j+1}^{f_{j+1}} p_{j+2}^{f_{j+2}} \cdots p_k^{f_k}$$

βλέπουμε εύκολα ότι:

$$[m,n] = \frac{n}{s} \cdot \frac{m}{r} = p_1^{f_1} p_2^{f_2} \cdots p_j^{f_j} p_1^{e_{j+1}} p_2^{e_{j+2}} \cdots p_k^{e_k} \qquad \text{και} \qquad (\frac{m}{r}, \frac{n}{s}) = 1$$

Επιπλέον:

$$\mathsf{o}(x^r) = \frac{m}{r} \qquad \text{και} \qquad \mathsf{o}(y^s) = \frac{n}{s}$$

και επομένως, επειδή η ομάδα G είναι αβελιανή και οι τάξεις των στοιχείων x^r και y^s είναι αριθμοί πρώτοι μεταξύ τους θα έχουμε ότι:

$$\text{το στοιχείο} \quad z = x^r z^s \quad \text{έχει τάξη} \quad \mathsf{o}(z) = [m,n] = \frac{n}{s} \cdot \frac{m}{r}$$

- Βημα 2: Χρησιμοποιώντας την ταυτότητα:

$$\forall m,n,t \in \mathbb{Z}^+ : \qquad [[m,n],t] = [m,n,t]$$

και επαναλαμβάνοντας την παραπάνω διαδικασία θα έχουμε ότι:

$$\text{αν } x,y,z \in G \text{ και } \mathsf{o}(x) = m,\ \mathsf{o}(y) = n,\ \mathsf{o}(z) = t, \text{ τότε υπάρχει ένα στοιχείο } w \in G \text{ έτσι ώστε :}$$

$$\mathsf{o}(w) = [m,n,t]$$

- Βημα 3: Συνεχίζοντας την παραπάνω διαδικασία, και λαμβάνοντας υπ' όψιν ότι η αβελιανή ομάδα είναι πεπερασμένη, μπορούμε επαγωγικά να κατασκευάσουμε ένα στοιχείο g με την επιθυμητή ιδιότητα, δηλαδή η τάξη του g να είναι το ελάχιστο κοινό πολλαπλάσιο των τάξεων των στοιχείων της G. □

Άσκηση 14. Έστω ότι $(G,\cdot)$ είναι μια ομάδα. Να δειχθεί ότι κάθε υποομάδα με δείκτη 2 στην G περιέχει όλα τα στοιχεία της G της μορφής x^2, $x \in G$:

$$H \leq G \quad \text{και} \quad [G:H] = 2 \quad \Longrightarrow \quad \left\{x^2 \in G \mid x \in G\right\} \subseteq H$$

Ιδιαίτερα, αν $|G| = 2n$, $n \geq 1$, και $H \leq G$ είναι μια υποομάδα της G με τάξη n, τότε, $\forall x \in G$: $x^2 \in H$.

Λύση. Έστω ότι $H \leq G$ είναι μια υποομάδα της G με δείκτη $[G:H] = 2$. Επειδή $[G:H] = 2$, έπεται ότι υπάρχουν ακριβώς 2 αριστερές πλευρικές κλάσεις της H στην G. Έστω $x \in G$. Αν $x \in H$, τότε προφανώς $x^2 \in H$ διότι η H είναι υποομάδα της G. Αν $x \in G \setminus H$, τότε επειδή οι αριστερές πλευρικές κλάσεις H και xH είναι διακεκριμένες (αν $xH = H$, τότε $x \in H$ το οποίο είναι άτοπο) θα έχουμε ότι οι αριστερές πλευρικές κλάσεις της H στην G είναι οι $\left\{H,\ xH\right\}$. Επομένως θα έχουμε:

$$G = H \cup xH \qquad \text{και} \qquad H \cap xH = \emptyset$$

και τότε $x^2 \in H$ ή $x^2 \in xH$. Στην τελευταία περίπτωση θα έχουμε $x^2 = xh$, όπου $h \in H$, και άρα $x = h \in H$ το οποίο είναι άτοπο διότι $x \notin H$. Άρα σε κάθε περίπτωση $x^2 \in H$.

Αν $|G| = 2n$, όπου $n \geq 1$, και $H \leq G$ είναι μια υποομάδα της G με τάξη $|H| = n$, τότε από το Θεώρημα του Lagrange είναι $[G:H] = 2$ και το συμπέρασμα προκύπτει από το πρώτο μέρος της Άσκησης. □

Άσκηση 15. Έστω $(G_i,\cdot)$, $1 \leq i \leq 3$, τρείς κυκλικές ομάδες τάξης 2. Να βρεθούν όλες οι υποομάδες της ομάδας ευθύ γινόμενο $G = G_1 \times G_2 \times G_3$.

Λύση. Έστω $G_1 = \langle x \rangle = \{e_1, x\}$, $G_2 = \langle y \rangle = \{e_2, y\}$ και $G_3 = \langle z \rangle = \{e_3, z\}$. Τότε:

$$G = \left\{(e_1,e_2,e_3),\ (x,e_2,e_3),\ (e_1,y,e_3),\ (e_1,e_2,z),\ (x,y,e_3),\ (x,e_2,z),\ (e_1,y,z),\ (x,y,z)\right\}$$

Η ομάδα G είναι μια αβελιανή ομάδα τάξης 8 και προφανώς κάθε στοιχείο της G, εκτός του ουδετέρου, έχει τάξη 2. Έτσι η G περιέχει ακριβώς 7 στοιχεία τάξης 2.

(1) Η τετριμμένη υποομάδα
$$H_1 = \langle e_1\rangle \times \langle e_2\rangle \times \langle e_3\rangle = \langle (e_1, e_2, e_3)\rangle = \{(e_1, e_2, e_3\}$$
είναι η μόνη υποομάδα τάξης 1.

(2) Αν H είναι μια υποομάδα τάξης 2, τότε η H είναι κυκλική και παράγεται από ένα στοιχείο τάξης 2. Επειδή κάθε στοιχείο της G εκτός του ταυτοτικού έχει τάξη 2, έπεται ότι η G περιέχει ακριβώς 7 υποομάδες τάξης 2:
$$H_2 = \langle x\rangle \times \langle e_2\rangle \times \langle e_3\rangle = \langle (x, e_2, e_3)\rangle$$
$$H_3 = \langle e_1\rangle \times \langle y\rangle \times \langle e_3\rangle = \langle (e_1, y, e_3)\rangle, \qquad H_4 = \langle e_1\rangle \times \langle e_2\rangle \times \langle z\rangle = \langle (e_1, e_2, z)\rangle$$
$$H_5 = \langle (x, y, e_3)\rangle, \qquad H_6 = \langle (x, e_2, z)\rangle, \qquad H_7 = \langle (e_1, y, z)\rangle, \qquad H_8 = \langle (x, y, z)\rangle$$

(3) Αν H είναι μια υποομάδα τάξης 4 της G, τότε η G δεν είναι κυκλική διότι η G δεν περιέχει συτοιχεία τάξης 4. Επειδή, όπως προκύπτει από την Άσκηση **;;**, κάθε μη-κυκλική ομάδα τάξης 4 είναι της μορφής $\{e, a, b, ab\}$, όπου a και b είναι διακεκριμμένα στοιχεία ταξης 2 έτσι ώστε $ab = ba$. Επομένως οι υποομάδες τάξης 4 της G είναι της μορφής $\{e, a, b, ab\}$, όπου τα a, b είναι δύο από τα 7 στοιχεία τάξης 2 της G. Έτσι θα έχουμε τις εξής υποομάδες τάξης 4:
$$H_9 = H_2 \times H_3 = \big\{(e_1, e_2, e_3),\ (x, e_2, e_3),\ (e_1, y, e_3),\ (x, y, e_3)\big\}$$
$$H_{10} = H_2 \times H_4 = \big\{(e_1, e_2, e_3),\ (x, e_2, e_3),\ (e_1, e_2, z),\ (x, e_2, z)\big\}$$
$$H_{11} = H_3 \times H_4 = \big\{(e_1, e_2, e_3),\ (e_1, y, e_3),\ (e_1, e_2, z),\ (e_1, y, z)\big\}$$
$$H_{12} = H_2 \times H_7 = \big\{(e_1, e_2, e_3),\ (x, e_2, e_3),\ (e_1, y, z),\ (x, y, z)\big\}$$
$$H_{13} = H_3 \times H_6 = \big\{(e_1, e_2, e_3),\ (e_1, y, e_3),\ (x, e_2, z),\ (x, y, z)\big\}$$
$$H_{14} = H_4 \times H_5 = \big\{(e_1, e_2, e_3),\ (e_1, e_2, z),\ (x, y, e_3),\ (x, y, z)\big\}$$
$$H_{15} = H_6 \times H_7 = \big\{(e_1, e_2, e_3),\ (x, e_2, z),\ (e_1, y, z),\ (x, y, e_3)\big\}$$

(4) Η ομάδα
$$G = G_1 \times G_2 \times G_3 = \langle x\rangle \times \langle y\rangle \times \langle z\rangle$$
είναι η μόνη υποομάδα τάξης 8.

Έτσι συνολικά η G περιέχει ακριβώς 16 υποομάδες, μια τάξης 1, επτά τάξης 2, επτά τάξης 4, και μια τάξης 8. □

Άσκηση 16. Έστω H μια υποομάδα μιας ομάδας G. Να βρεθεί η τάξη της H στις ακόλουθες περιπτώσεις:

(1) $|G| = 68$, $|H| < 32$ και η H δεν είναι κυκλική.
(2) $|G| = 100$, η H δεν είναι κυκλική, και η H δεν διαθέτει στοιχείο τάξης 2.
(3) $|G| = 52$, $H \neq G$, και η H δεν είναι αβελιανή.

Λύση. (1) Επειδή $|G| = 68$, από το Θεώρημα του Lagrange θα έχουμε $|H| \mid 68$, και άρα $|H| = 1$ ή 2 ή 4 ή 17 ή 34 ή 68. Επειδή $|H| < 32$ θα έχουμε $|H| = 1$ ή 2 ή 4 ή 17. Αν $|H| = 1$ ή 2 ή 17, τότε η H είναι προφανώς κυκλική διότι η τετριμμένη ομάδα και κάθε ομάδα με τάξη έναν πρώτο αριθμό είναι κυκλική. Επειδή η H δεν είναι κυκλική, έπεται ότι $|H| = 4$.

Επειδή υπάρχουν δύο μη-ισόμορφες ομάδας με τάξη ίση με 4, η κυκλική τάξης 4 και η ομάδα του Klein, έπεται ότι η H, ως μη-κυκλική ομάδα τάξης 4, είναι ισόμορφη με την ομάδα του Klein.

(2) Επειδή $|G| = 100$, από το Θεώρημα του Lagrange θα έχουμε $|H| \mid 100$, και άρα $|H| = 1$ ή 2 ή 4 ή 5 ή 10 ή 20 ή 25 ή 50 ή 100. Επειδή η H δεν περιέχει στοιχεία τάξης 2, έπεται ότι η τάξη της H είναι περιττός αριθμός, βλέπε την Άσκηση **2** του Φυλλαδίου **2** όπου δείξαμε ότι κάθε ομάδα άρτιας τάξης έχει τουλάχιστον ένα στοιχείο τάξης 2. Άρα $|H| = 1$ ή 5 ή 25. Αν $|H| = 1$ ή 5, τότε η H είναι προφανώς κυκλική διότι η τετριμμένη ομάδα και κάθε ομάδα με τάξη έναν πρώτο αριθμό είναι κυκλική. Επειδή η H δεν είναι κυκλική, έπεται ότι[8] $|H| = 25$.

[8] Αποδεικνύεται ότι κάθε ομάδα τάξης p^2, όπου p είναι πρώτος είναι αβελιανή και ισόμορφη είτε με την κυκλική ομάδα τάξης p^2 είτε με την ομάδα ευθύ γινόμενο δύο κυκλικών ομάδων τάξης p. Επειδή η H δεν είναι κυκλική, έπεται ότι η H είναι ισόμορφη με την ομάδα $\mathbb{Z}_5 \times \mathbb{Z}_5$.

(3) Επειδή $|G| = 52$, από το Θεώρημα του Lagrange θα έχουμε $|H| \mid 100$, και άρα $|H| = 1$ ή 2 ή 4 ή 13 ή 26 ή 52. Επειδή $H \neq G$, θα έχουμε $|H| = 1$ ή 2 ή 4 ή 13 ή 26. Αν $|H| = 1$ ή 2 ή 4 ή 13, τότε η H είναι αβελιανή, διότι κάθε ομάδα με τάξη ≤ 4 και κάθε ομάδα με τάξη έναν πρώτο αριθμό είναι κυκλική. Επειδή η H δεν είναι αβελιανή, έπεται ότι[9] $|H| = 26$. □

Άσκηση 17. Έστω $(G, \cdot)$ μια ομάδα τάξης < 45 η οποία περιέχει μια υποομάδα H με τάξη > 10 και δείκτη > 3. Να βρεθούν οι τάξεις των G και H καθώς και ο δείκτης της H στην G.

Λύση. Από το Θεώρημα του Lagrange έπεται ότι $[G : H] = \frac{\mathsf{o}(G)}{\mathsf{o}(H)}$. Τότε:

$$\mathsf{o}(G) < 45 \quad \text{και} \quad \mathsf{o}(H) > 10 \quad \Longrightarrow \quad \mathsf{o}(G) < 45 \quad \text{και}$$

$$\frac{1}{\mathsf{o}(H)} < 10 \quad \Longrightarrow \quad \mathsf{o}(G) \cdot \frac{1}{\mathsf{o}(H)} = [G : H] < \frac{45}{10} = 4.5 \quad \Longrightarrow \quad 3 < [G : H] < 4.5 \quad \Longrightarrow \quad [G : H] = 4$$

Τότε $\mathsf{o}(G) = \mathsf{o}(H) \cdot [G : H] = 4\mathsf{o}(H)$ και επειδή $\mathsf{o}(H) > 10$ και $\mathsf{o}(G) < 45$ θα έχουμε $40 < \mathsf{o}(G) < 45$, δηλαδή η τάξη $\mathsf{o}(G)$ της G είναι ένας εκ των αριθμών $41, 42, 43, 44$ ο οποίος θα πρέπει επιπλέον να διαιρείται από τον δείκτη $[G : H] = 4$. Ο μόνος αριθμός από τις παραπάνω πιθανές τάξεις της G ο οποίος ικανοποιεί αυτή τη σχέση είναι ο 44. Επομένως $\mathsf{o}(G) = 44$ και τότε $\mathsf{o}(H) = \frac{\mathsf{o}(G)}{\mathsf{o}(H)} = \frac{44}{4} = 11$. □

Άσκηση 18. **1.** Έστω G μια κυκλική ομάδα τάξης n. Για κάθε διαιρέτη $m \mid n$, να προσδιορισθεί το πλήθος των στοιχείων της G με τάξη m.

2. Δείξτε ότι, με εξαίρεση δύο, όλες οι κυκλικές ομάδες έχουν άρτιο πλήθος γεννητόρων.

Λύση. **1.** Έστω $m \mid n$. Τότε επειδή η ομάδα G είναι κυκλική έπεται ότι υπάρχει μοναδική υποομάδα $H \leq G$ με $\mathsf{o}(H) = m$. Η υποομάδα H, ως υποομάδα κυκλικής ομάδας είναι κυκλική, έστω με γεννήτορα το στοιχείο x: $H = \langle x \rangle$. Οι γεννήτορες της H έχουν τάξη m, δηλαδή:

$$\langle y \rangle = \langle x \rangle = H \iff \mathsf{o}(y) = m$$

Γνωρίζουμε όμως ότι το πλήθος των γεννητόρων κάθε κυκλικής ομάδας τάξης m, όπως η H, είναι ακριβώς $\phi(m)$. Αν $z \in G$ είναι ένα άλλο στοιχείο με τάξη $\mathsf{o}(z) = m$ τότε λόγω μοναδικότητας έχουμε ότι $\langle z \rangle = H$. Επομένως για κάθε διαιρέτη $m \mid n$ το πλήθος των στοιχείων της G τάξης m συμπίπτει με το πλήθος των γεννητόρων της μοναδικής υποομάδας H της G με τάξη m, και ισούται με $\phi(m)$.

2. Έστω G μια κυκλική ομάδα. Αν η G είναι άπειρη κυκλική, τότε γνωρίζουμε ότι η G έχει ακριβώς δύο γεννήτορες. Έστω ότι η G είναι πεπερασμένη κυκλική.

Αν $|G| = 1$, δηλαδή $G = \{e\} = \langle e \rangle$, τότε η G έχει ακριβώς έναν γεννήτορα. Αν $|G| = 2$, τότε $G = \{e, a\} = \langle a \rangle = \langle a^{-1} \rangle$ και επειδή $a = a^{-1}$, έπεται ότι η G έχει ακριβώς έναν γεννήτορα.

Αν η G είναι πεπερασμένη κυκλική με τάξη $|G| = n \geq 3$, τότε προφανώς κανένας γεννήτορας a της G δεν ικανοποιεί την σχέση $a = a^{-1}$ (διότι διαφορετικά $a^2 = e$ και τότε $G = \{e, a\}$ και $|G| \leq 2$ το οποίο είναι άτοπο). Επειδή a είναι γεννήτορας της G αν και μόνον αν a^{-1} είναι γεννήτορας της G, οι γεννήτορες της G εμφανίζονται ως ζεύγη $\{a, a^{-1}\}$ και $a \neq a^{-1}$. Αυτό όμως σημαίνει ότι το πλήθος τους είναι άρτιος αριθμός.

Συνοψίζουμε: όλες οι κυκλικές ομάδες έχουν άρτιο πλήθος γεννητόρων με εξαίρεση την τετριμμένη κυκλική ομάδα τάξης 1 και την κυκλική ομάδα τάξης 2. □

Άσκηση 19. Να αποδειχθεί, με χρήση Θεωρίας Ομάδων, το Θεώρημα του Gauss:

$$\forall n \geq 1 : \qquad \sum_{d \mid n} \varphi(d) = n$$

[9] Αποδεικνύεται ότι υπάρχουν, με ακρίβεια ισομορφίας, μόνο δύο ομάδας τάξης $2p$, όπου p είναι πρώτος: η κυκλική ομάδα τάξης $2p$ και η διεδρική ομάδα D_p τάξης $2p$. Έτσι επιλέγοντας $p = 13$, επειδή η H είναι μη-κυκλική τάξης $26 = 2 \cdot 13$, θα έχουμε ότι η H είναι ισόμορφη με τη διεδρική ομάδα D_{13}.

Λύση. Έστω G μια κυκλική ομάδα τάξης n. Για κάθε διαιρέτη d της τάξης της ομάδας G, θέτουμε:

$$\mathcal{O}(d) = \big\{g \in G \mid \mathsf{o}(g) = d\big\}$$

Σύμφωνα με την Άσκηση 18 θα έχουμε:

$$|\mathcal{O}(d)| = \varphi(d)$$

Προφανώς τότε μπορούμε να γράψουμε το σύνολο G ως ξένη ένωση

$$G = \bigcup_{d\,|\,n} \mathcal{O}(d)$$

και επομένως

$$n = |G| = |\bigcup_{d\,|\,n} \mathcal{O}(d)| = \sum_{d\,|\,n} |\mathcal{O}(d)| = \sum_{d\,|\,n} \varphi(d) \qquad \square$$

Άσκηση 20. Έστω $\mathsf{GL}(2,\mathbb{R})$ η ομάδα των αντιστρέψιμων 2×2 πινάκων με στοιχεία πραγματικούς αριθμούς, και θεωρούμε τα ακόλουθα υποσύνολά της:

$$G = \big\{X_{a,b} \in \mathsf{M}_{2\times 2}(\mathbb{R}) \mid a,b \in \mathbb{R}\ \&\ a \neq 0\big\} \quad \& \quad H = \big\{X_{1,b} \in \mathsf{M}_{2\times 2}(\mathbb{R}) \mid b \in \mathbb{R}\big\}, \quad \text{όπου} \quad X_{a,b} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$$

(1) Δείξτε ότι[10]: $H \leq G \leq \mathsf{GL}(2,\mathbb{R})$.
(2) Δείξτε ότι, $\forall A \in G$: $A \cdot H = H \cdot A$.
(3) Περιγράψτε το σύνολα πηλίκο $G/H = G/\!\sim_H$.

Λύση. (1) Προφανώς κάθε πίνακας $X_{a,b} \in G$ είναι αντιστρέψιμος διότι $|X_{a,b}| = a \neq 0$, και άρα $G \subseteq \mathsf{GL}(2,\mathbb{R})$.

Προφανώς $I_2 = X_{1,0} \in G$. Θεωρούμε δύο πίνακες-στοιχεία του συνόλους G:

$$X_{a,b} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \qquad \& \qquad X_{a',b'} = \begin{pmatrix} a' & b' \\ 0 & 1 \end{pmatrix}, \quad \text{όπου} \quad a, a' \neq 0$$

Εύκολα υπολογίζουμε ότι:

$$X_{a,b} \cdot X_{a',b'} = X_{aa',ab'+b} = \begin{pmatrix} aa' & ab'+b \\ 0 & 1 \end{pmatrix} \in G \qquad \& \qquad X_{a,b}^{-1} = X_{\frac{1}{a},-\frac{b}{a}} = \begin{pmatrix} \frac{1}{a} & -\frac{b}{a} \\ 0 & 1 \end{pmatrix} \in G$$

Επομένως το υποσύνολο G είναι μια υποομάδα της $\mathsf{GL}(2,\mathbb{R})$.

Επειδή $I_2 = X_{1,0} \in H$, και όπως βλέπουμε από τις παραπάνω σχέσεις για $a = 1 = a'$, έχουμε:

$$X_{1,b} \cdot X_{1,b'} = X_{1,b'+b} = \begin{pmatrix} 1 & ab'+b \\ 0 & 1 \end{pmatrix} \in H \qquad \& \qquad X_{1,b}^{-1} = X_{1,-b} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \in H$$

έπεται ότι το υποσύνολο H είναι μια υποομάδα της G, άρα και της $\mathsf{GL}(2,\mathbb{R})$.

(2) Θεωρούμε πίνακες

$$X_{a,b} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G \qquad \& \qquad X_{1,r} = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} \in H \quad \& \quad X_{1,s} = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \in H$$

Τότε:

$$X_{a,b} \cdot X_{1,r} = \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & ar+b \\ 0 & 1 \end{pmatrix} = X_{a,ar+b}$$

Άρα:

$$X_{a,b}H = \Big\{X_{a,b} \cdot X_{1,r} \in G \mid a \neq 0\ \&\ b,r \in \mathbb{R}\Big\} = \Big\{X_{a,ar+b} \in G \mid a \neq 0\ \&\ b,r \in \mathbb{R}\Big\} \qquad (*)$$

Παρόμοια

$$X_{1,s} \cdot X_{a,b} = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b+s \\ 0 & 1 \end{pmatrix} = X_{a,b+s}$$

[10] Η ομάδα G καλείται η *ομοπαραλληλική ομάδα* των 2×2 αντιστρεψίμων πινάκων.

Άρα:

$$HX_{a,b} = \Big\{X_{1,s}\cdot X_{a,b}\in G \mid a\neq 0 \;\&\; b,s\in\mathbb{R}\Big\} = \Big\{X_{a,b+s}\in G \mid a\neq 0 \;\&\; b,s\in\mathbb{R}\Big\} \qquad (**)$$

Έστω $X_{a,ar+b}\in X_{a,b}H$. Επειδή $X_{a,ar+b}=X_{a,b+s}\in HX_{a,b+s}$, όπου $s=ar$, έπεται ότι $X_{a,b}H\subseteq HX_{a,b}$. Αντίστροφα, έστω $X_{a,b+s}\in HX_{a,b}$. Επειδή $X_{a,b+s}=X_{a,ar+b}\in X_{a,b}H$, όπου $r=\frac{s}{a}$, έπεται ότι $HX_{a,b}\subseteq X_{a,b}H$. Επομένως:

$$\forall X_{a,b}\in G: \quad X_{a,b}H = HX_{a,b}$$

(3) Συμβολίζουμε με G/H το σύνολο όλων των αριστερών πλευρικών κλάσεων της H στην G:

$$G/H = \big\{X_{a,b}H\subseteq G \mid X_{a,b}\in G\big\}$$

και ορίζουμε την ακόλουθη αντιστοιχία

$$\Phi:\ G/H \longrightarrow \mathbb{R}^*, \quad \Phi(X_{a,b}H)=a$$

Θα δείξουμε ότι η αντιστοιχία Φ είναι μια καλά ορισμένη «1-1» και «επί» απεικόνιση.

Πρώτα προσδιορίζουμε πότε δύο αριστερές πλευρικές κλάσεις $X_{a,b}H$ και $X_{a',b'}$ συμπίπτουν. Θα έχουμε:

$$X_{a,b}H = X_{a',b'}H \iff X_{a,b}^{-1}\cdot X_{a',b'}\in H \iff X_{a^{-1}a',a^{-1}(b'-b)}\in H \iff$$
$$\iff X_{a^{-1}a',a^{-1}(b'-b)} = X_{1,r}, \text{ για κάποιο } r\in\mathbb{R} \iff a^{-1}a'=1 \iff a=a'$$

Επομένως:

$$X_{a,b}H = X_{a',b'}H \iff a=a' \qquad (\dagger)$$

- Η Φ είναι καλά ορισμένη:

Έστω $X_{a,b}H=X_{a',b'}H$. Τότε από την σχέση $(\dagger)$ θα έχουμε $a=a'$ και επομένως από τον ορισμό της Φ, θα έχουμε $\Phi(X_{a,b}H)=\Phi(X_{a',b'}H)$. Άρα η Φ είναι μια καλά ορισμένη απεικόνιση.

- Η Φ είναι «1-1»: Θα έχουμε

$$\Phi(X_{a,b}H)=\Phi(X_{a',b'}H) \implies a=a' \overset{(\dagger)}{\implies} X_{a,b}H=X_{a',b'}H$$

Επομένως η Φ είναι «1-1».

- Η Φ είναι «επί»: Θα έχουμε

$$\forall r\in\mathbb{R}^*: \quad \Phi(X_{r,0}H)=r$$

Επομένως η Φ είναι «επί». □

Άσκηση 21. Έστω ότι $(G,\cdot)$ είναι μια ομάδα και ότι H,K είναι υποομάδες της με $K\leq H$. Αν ο δείκτης $[G:K]$ είναι πεπερασμένος, τότε να δειχθεί ότι οι δείκτες $[G:H]$ και $[H:K]$ είναι πεπερασμένοι και ισχύει[11]

$$[G:K]=[G:H]\cdot[H:K]$$

Λύση. Ο δείκτης $[H:K]$ είναι το πλήθος των στοιχείων τού συνόλου $H/K=\{hK|h\in H\}$, το οποίο είναι υποσύνολο τού $G/K=\{gK|g\in G\}$. Αφού το G/K είναι ένα πεπερασμένο σύνολο, έπεται ότι και το H/K είναι επίσης πεπερασμένο. Ώστε, $[H:K]<\infty$.

Θεωρούμε τα σύνολα $G/K=\{gK|g\in G\}$ και $G/H=\{gH|g\in G\}$ και την αντιστοιχία

$$\Phi\colon G/K \longrightarrow G/H, \quad gK \longmapsto \Phi(gK):=gH$$

Η συγκεκριμένη αντιστοιχία Φ είναι μια «καλά ορισμένη» απεικόνιση, αφού αν, $g_1K=g_2K$, τότε το $g_2^{-1}g_1$ είναι στοιχείο τού $K\leq H$ και γι' αυτό $g_1H=g_2H$. Επιπλέον, η Φ είναι μια «επί» απεικόνιση (*γιατί;*) και

[11] Η ομάδα G δεν είναι απαραίτητα πεπερασμένη. Όταν η ομάδα G είναι πεπερασμένη η απόδειξη προκύπτει άμεσα από το Θεώρημα του Lagrange και έχει αναλυθεί στην τάξη.

επειδή το σύνολο G/K είναι πεπερασμένο, έπεται ότι και το G/H είναι ένα πεπερασμένο σύνολο. Ώστε, $[G:H] < \infty$.

Τώρα θα δείξουμε ότι $[G:K] = [G:H] \cdot [H:K]$.

Έστω ότι $G/H = \{a_1H, a_2H, \ldots, a_nH\}, a_i \in G, 1 \leq i \leq n$ είναι το σύνολο των αριστερών πλευρικών κλάσεων (συμπλόκων) τής H στην G και ότι $H/K = \{b_1K, b_2H, \ldots, b_mK\}, b_j \in H, 1 \leq j \leq m$ είναι το σύνολο των αριστερών πλευρικών κλάσεων (συμπλόκων) τής K στην H.

Ισχυρισμός 1: Τα σύνολα a_ib_jK, $1 \leq i \leq n$, $1 \leq j \leq m$ είναι ανά δύο διαφορετικές αριστερές πλευρικές κλάσεις (σύμπλοκα) της K στην G.

Απόδειξη του Ισχυρισμού 1: Πράγματι, αν για κάποια a_pH, a_qH, b_rK, b_sK με $1 \leq p, q \leq n$, $p \neq q$ και με $1 \leq r, s \leq m$, $r \neq s$ ήταν $a_pb_rK = a_qb_sK$, τότε θα ήταν $(a_qb_s)^{-1}a_pb_r = b_s^{-1}a_q^{-1}a_pb_r \in K$ και αφού $K \leq H$ και τα $b_j \in H$, συμπεραίνουμε ότι $a_q^{-1}a_p \in H$, δηλαδή $a_pH = a_qH$. Αυτό όμως είναι άτοπο. Άρα ο ισχυρισμός 1 είναι αληθής.

Ισχυρισμός 2: Κάθε αριστερή πλευρική κλάση gK είναι μια από τις αριστερές πλευρικές κλάσεις a_ib_jK, $1 \leq i \leq n$, $1 \leq j \leq m$.

Απόδειξη του Ισχυρισμού 2: Το στοιχείο g ανήκει στην a_iH, για κάποιο $i, 1 \leq i \leq n$. Ώστε $g = a_ih, h \in H$. Το $h \in H$ ανήκει στην b_jK για κάποιο $j, 1 \leq j \leq m$. Ώστε $h = b_jk$, $k \in K$. Επομένως, $g = a_ib_jk \in a_ib_jK$ και γι' αυτό $gK = a_ib_jK$.

Επομένως, το σύνολο $\{a_ib_jK \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}$ συμπίπτει με το σύνολο των αριστερών πλευρικών κλάσεων (συμπλόκων) τής K στην G και αφού το πλήθος τού $\{a_ib_jK \mid 1 \leq i \leq n,\ 1 \leq j \leq m\}$ είναι $[G:H] \cdot [H:K]$, συμπεραίνουμε ότι $[G:K] = [G:H] \cdot [H:K]$. □

Άσκηση 22. (Η Πρόταση Poincaré) Αν H, K είναι δύο υποομάδες μιας ομάδας[12] G, των οποίων ο δείκτης στην G είναι πεπερασμένος, τότε και ο δείκτης της $H \cap K$ στην G είναι επίσης πεπερασμένος. Επιπλέον:

$$\big([G:H], [G:K]\big) = 1 \quad \Longrightarrow \quad [G:H\cap K] = \big[[G:H], [G:K]\big]$$

Λύση. Συμβολίζουμε με $G/H \cap K$ το σύνολο $\{a(H\cap K) \mid a \in G\}$ των αριστερών πλευρικών κλάσεων τής $H \cap K$ στην G και με G/H (αντίστοιχα G/K) το σύνολο $\{aH \mid a \in G\}$ (αντίστοιχα $\{aK \mid a \in G\}$) των αριστερών πλευρικών κλάσεων της H στην G (αντίστοιχα της K στην G).

Θεωρούμε την αντιστοιχία

$$\Phi:\ G/H\cap K \ \longrightarrow\ G/H \times G/K, \quad a(H\cap K) \ \longmapsto\ (aH, aK)$$

Παρατηρούμε ότι η συγκεκριμένη αντιστοιχία είναι μια «καλά ορισμένη» απεικόνιση, αφού αν για κάποια $a, b \in G$ είναι $a(H\cap K) = b(H\cap K)$, τότε το $b^{-1}a$ ανήκει στην $H \cap K$. Έτσι έχουμε ότι $b^{-1}a \in H$ και $b^{-1}a \in K$. Επομένως, $aH = bH$ και $aK = bK$, δηλαδή $(aH, aK) = (bH, bK)$.

Ισχυριζόμαστε ότι η Φ είναι μια «1-1» απεικόνιση. Πράγματι, αν είναι $\Phi(a(H\cap K)) = \Phi(b(H\cap K))$, τότε $(aH, aK) = (bH, bK)$. Επομένως, $aH = bH$ και $aK = bK$ και γι' αυτό $b^{-1}a \in H$, $b^{-1}a \in K$. Ώστε, $b^{-1}a \in H \cap K$ και επομένως $a \in b(H\cap K$. Τότε θα έχουμε $a(H\cap K) = b(H\cap K)$.

Αφού οι δείκτες $[G:H]$ και $[G:K]$ είναι πεπερασμένοι, δηλαδή το σύνολο πηλίκο G/H (αντιστοίχως G/K) των αριστερών πλευρικών κλάσεων τής H (αντιστοίχως τής K) στην G έχει πεπερασμένο το πλήθος στοιχεία, συμπεραίνουμε ότι και το καρτεσιανό γινόμενο $G/H \times G/K$ έχει πεπερασμένο το πλήθος στοιχεία. Επειδή τώρα η Φ είναι μια «1-1» απεικόνιση, καταλήγουμε στο ότι και το πλήθος $[G:H\cap K]$ των στοιχείων τού $G/H\cap K$ είναι πεπερασμένο και μάλιστα είναι $\leq$ από το $[G:H]\cdot[G:K]$, το οποίο είναι το πλήθος των στοιχείων τού συνόλου $G/H \times G/K$:

$$G/H\cap K \ \leq\ |G/H \times G/K| \ =\ [G:H]\cdot[G:K] \qquad (*)$$

Σύμφωνα με την προηγούμενη Άσκηση 21 γνωρίζουμε ότι $[G:H\cap K] = [G:H]\cdot[H:H\cap K]$ και $[G:H\cap K] = [G:K]\cdot[K:H\cap K]$. Ώστε ο $[G:H\cap K]$ είναι κοινό πολλαπλάσιο των $[G:H]$ και $[G:K]$. Επομένως ο $[G:H\cap K]$ είναι πολλαπλάσιο και τού $\big[[G:H], [G:K]\big]$, το οποίο ισούται με $[G:H]\cdot[G:K]$, αφού οι $[G:H]$ και $[G:K]$ δεν έχουν κοινούς διαιρέτες. Όμως μόλις παρατηρήσαμε,

[12] Η G δεν είναι απαραίτητα πεπερασμένη ομάδα.

βλέπε τη σχέση (*), ότι $[G : H \cap K] \leq [G : H] \cdot [G : K]$ και αφού είναι και πολλαπλάσιο τού $[G : H] \cdot [G : K]$, συμπεραίνουμε ότι $[G : H \cap K] = [G : H] \cdot [G : K] = \big[[G : H], [G : K]\big]$. $\square$