ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ Ι

Ακαδημαϊκο Ετος 2023-2024

Επιλυση Ασκησεων - Φυλλαδιο 4

Διδασκων: Α. Μπεληγιάννης

ΙΣΤΟΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ

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

Πέμπτη 4 Απριλίου 2024

Άσκηση 1. Να ευρεθεί η τάξη τού στοιχείου a της ομάδας $(G,\star)$, όπου:

(1) $a=[2]_3$, $(G,\star)=(\mathbb{Z}_3,+)$,
(2) $a=-i$, $(G,\star)=(\mathbb{C}^\star,\cdot)$,
(3) $a=-1+i\sqrt{3}$, $(G,\star)=(\mathbb{C}^\star,\cdot)$,
(4) $a=(-1+i\sqrt{3})/2$, $(G,\star)=(\mathbb{C}^\star,\cdot)$,
(5) $\cos(2\pi/7)+i\sin(2\pi/7)$, $(G,\star)=(\mathbb{C}^\star,\cdot)$.
(6) $a=[6]_{10}$, $(G,\star)=(\mathbb{Z}_{10},+)$,
(7) $a=[6]_{15}$, $(G,\star)=(\mathbb{Z}_{15}),+)$,
(8) $a=[10]_{12}$, $(G,\star)=(\mathbb{Z}_{12}),+)$,
(9) $a=[77]_{210}$, $(G,\star)=(\mathbb{Z}_{210}),+)$,
(10) $a=[40]_{210}$, $(G,\star)=(\mathbb{Z}_{210}),+)$,
(11) $a=[70]_{210}$, $(G,\star)=(\mathbb{Z}_{210}),+)$.

Λύση. Στις περισσότερες περιπτώσεις χρησιμοποιούμε ότι αν a είναι ένα στοιχείο πεπερασμένης τάξης σε μια πολλαπλασιαστική, αντίστοιχα προσθετική, ομάδα G, τότε, $\forall k\geq 1$:

$$\mathsf{o}(a^k)=\frac{\mathsf{o}(a)}{(\mathsf{o}(a),k)},\qquad \text{αντίστοιχα:}\quad \mathsf{o}(ka)=\frac{\mathsf{o}(a)}{(\mathsf{o}(a),k)}$$

(1) Έχουμε: $[2]_3=2[1]_3$. Άρα η τάξη τού $[2]_3$ ισούται με:

$$\mathsf{o}([2]_3)=\mathsf{o}(2[1]_3)=\frac{\mathsf{o}([1]_3)}{(\mathsf{o}([1]_3),2)}=\frac{3}{(3,2)}=\frac{3}{1}=3$$

(2) Έχουμε: $(-i)^1=-i$, $(-i)^2=(-i)(-i)=i^2=-1$, $(-i)^3=(-i)(-i)^2=(-i)(-1)=i$, $(-i)^4=(-i)^2(-i)^2=(-1)(-1)=1$. Άρα τάξη τού $(-i)$ είναι 4:

$$\mathsf{o}(-i)=4$$

(3) Παρατηρούμε ότι αν $z\in\mathbb{C}^*$, και $\mathsf{o}(z)<\infty$, τότε θα πρέπει $|z|=1$. Πράγματι, θα έχουμε ότι $z^n=1$, όπου $n=\mathsf{o}(z)$, και τότε $1=|z^n|=|z|^n$. Από την τελευταία σχέση βλέπουμε ότι $|z|=1$.
Για τον μιγαδικό αριθμό $a=-1+i\sqrt{3}$ βλέπουμε εύκολα ότι είναι $|a|=2$, επομένως θα έχουμε

$$\mathsf{o}(a)=\infty$$

(4) Η τριγωνομετρική μορφή τού $a=(-1+i\sqrt{3})/2$ είναι η $a=\cos(2\pi/3)+i\sin(2\pi/3)$. Τότε $a^3=\cos(3\cdot 2\pi/3)+i\sin(3\cdot 2\pi/3)=1$, και επειδή προφανώς $a^2=\cos(4\pi/3)+i\sin(4\pi/3)\neq 1$, έπεται ότι η τάξη τού a ισούται με 3:

$$\mathsf{o}(a)=3$$

(5) Η τάξη του αριθμού $a=\cos(2\pi/7)+i\sin(2\pi/7)$ είναι 7, διότι $a^7=1$ και γι' αυτό[1] ο a έχει ως τάξη έναν διαιρέτη τού 7. Αλλά οι μοναδικοί διαιρέτες τού 7 είναι οι 1 και 7. Αν η τάξη τού a ήταν 1, τότε ο $a=1$. Αλλά $a\neq 1$. Ώστε η τάξη του είναι 7:

$$\mathsf{o}(a)=7$$

[1] Υπενθυμίζουμε ότι αν ένα στοιχείο a σε μια ομάδα G έχει πεπερασμένη τάξη, και $k\in\mathbb{N}$, τότε:

$$a^k=e\quad\Longleftrightarrow\quad \mathsf{o}(a)\mid k$$

(6) Έχουμε: $[6]_{10} = 6[1]_{10}$. Άρα η τάξη τού $[6]_{10}$ ισούται με:

$$\mathsf{o}([6]_{10}) = \mathsf{o}(6[1]_{10}) = \frac{\mathsf{o}([1]_{10})}{(\mathsf{o}([1]_{10}), 6)} = \frac{10}{(10,6)} = \frac{10}{2} = 5$$

(7) Έχουμε: $[6]_{15} = 6[1]_{15}$. Άρα η τάξη τού $[6]_{15}$ ισούται με:

$$\mathsf{o}([6]_{15}) = \mathsf{o}(6[1]_{15}) = \frac{\mathsf{o}([1]_{15})}{(\mathsf{o}([1]_{15}), 6)} = \frac{15}{(15,6)} = \frac{15}{3} = 5$$

(8) Έχουμε: $[6]_{15} = 6[1]_{15}$. Άρα η τάξη τού $[6]_{15}$ ισούται με:

$$\mathsf{o}([10]_{12}) = \mathsf{o}(10[1]_{12}) = \frac{\mathsf{o}([1]_{12})}{(\mathsf{o}([1]_{12}), 10)} = \frac{12}{(12,10)} = \frac{12}{2} = 6$$

(9) Έχουμε: $[77]_{210} = 77[1]_{210}$. Άρα η τάξη τού $[77]_{210}$ ισούται με:

$$\mathsf{o}(77]_{210}) = \mathsf{o}(77[1]_{210}) = \frac{\mathsf{o}([1]_{210})}{(\mathsf{o}([1]_{210}), 77)} = \frac{210}{(210,77)} = \frac{210}{7} = 30$$

(10) Έχουμε: $[40]_{210} = 40[1]_{210}$. Άρα η τάξη τού $[40]_{210}$ ισούται με:

$$\mathsf{o}(40]_{210}) = \mathsf{o}(40[1]_{210}) = \frac{\mathsf{o}([1]_{210})}{(\mathsf{o}([1]_{210}), 40)} = \frac{210}{(210,40)} = \frac{210}{10} = 21$$

(11) Έχουμε: $[70]_{210} = 70[1]_{210}$. Άρα η τάξη τού $[70]_{210}$ ισούται με:

$$\mathsf{o}(70]_{210}) = \mathsf{o}(70[1]_{210}) = \frac{\mathsf{o}([1]_{210})}{(\mathsf{o}([1]_{210}), 70)} = \frac{210}{(210,70)} = \frac{210}{70} = 3$$ ■

Άσκηση 2. Έστω ότι $(G, \cdot)$ είναι μια ομάδα. Να δειχθούν τα ακόλουθα:

1. $\forall x, a \in G$:

$$\mathsf{o}(x^{-1}ax) = \mathsf{o}(a) = \mathsf{o}(xax^{-1})$$

2. $\forall a, b \in G$:

$$\mathsf{o}(ab) = \mathsf{o}(ba)$$

3. Αν H είναι μια υποομάδα της G, τότε $\forall x \in G$, τα σύνολα

$$x^{-1}Hx = \left\{x^{-1}hx \in G \mid h \in H\right\} \quad \text{και} \quad xHx^{-1} = \left\{xhx^{-1} \in G \mid h \in H\right\}$$

είναι υποομάδες της G με τάξη

$$\mathsf{o}(x^{-1}Hx) = \mathsf{o}(H) = \mathsf{o}(xHx^{-1})$$

Λύση. **1.** Για κάθε $x, a \in G$ έχουμε:

$$(x^{-1}ax)^n = (x^{-1}ax) \cdot (x^{-1}ax) \cdots (x^{-1}ax) = x^{-1}a^n x$$

και άρα, για κάθε $n \in \mathbb{N}$, θα έχουμε:

$$(x^{-1}ax)^n = e \iff x^{-1}a^n x = e \iff a^n = xex^{-1} \iff a^n = e \qquad (*)$$

Η παραπάνω σχέση $(*)$ δείχνει ότι

$$\{n \in \mathbb{N} \mid a^n = e\} = \{n \in \mathbb{N} \mid (x^{-1}ax)^n = e\}$$

και επομένως[2]:

$$\mathsf{o}(a) = \min\{m \in \mathbb{N} \mid a^n = e\} = \min\{m \in \mathbb{N} \mid (x^{-1}ax)^m = e\} = \mathsf{o}(x^{-1}ax)$$

[2] ΔΙΑΦΟΡΕΤΙΚΑ: από την $(*)$ έπεται ότι:

$$\mathsf{o}(x^{-1}ax) < \infty \iff \mathsf{o}(a) < \infty$$

Ισοδύναμα $\mathsf{o}(x^{-1}ax) = \infty \iff \mathsf{o}(a) = \infty$, και τότε αν μια από τις δύο τάξεις είναι άπειρη, θα έχουμε: $\mathsf{o}(x^{-1}ax) = \infty = \mathsf{o}(a)$.

Έστω $\mathsf{o}(x^{-1}ax) < \infty$, ή ισοδύναμα $\mathsf{o}(a) < \infty$, και έστω $\mathsf{o}(x^{-1}ax) = n$. Τότε $(x^{-1}ax)^n = e$ και από τη σχέση $(*)$ έχουμε $a^n = e$. Συνεπώς

$$\mathsf{o}(a) \mid n = \mathsf{o}(x^{-1}ax) \qquad (1)$$

Αν $\mathsf{o}(a) = m$, δηλαδή $a^m = e$, τότε από τη σχέση $(*)$ έχουμε $(x^{-1}ax)^m = e$ και άρα

$$\mathsf{o}(x^{-1}ax) \mid m = \mathsf{o}(a) \qquad (2)$$

Από τις σχέσεις (1) και (2) συνεπάγεται ότι $\mathsf{o}(x^{-1}ax) = n = m = \mathsf{o}(a)$.

2. Έστω $a, b \in G$. Επειδή

$$a^{-1} \cdot ab \cdot a = eba = ba$$

από το ερώτημα (1) έχουμε το ζητούμενο: $\mathsf{o}(ab) = \mathsf{o}(a^{-1} \cdot ab \cdot a) = \mathsf{o}(ba)$.

3. Έστω $a, b \in x^{-1}Hx$. Τότε υπάρχουν στοιχεία $h_1, h_2 \in H$ έτσι ώστε:

$$a = x^{-1}h_1x \quad \text{και} \quad b = x^{-1}h_2x, \quad \text{όπου} \quad h_1, h_2 \in H$$

Επειδή το σύνολο H είναι υποομάδα της G θα έχουμε:

- $e = x^{-1}ex \in x^{-1}Hx$.
- $ab = x^{-1}h_1x \cdot x^{-1}h_2x = x^{-1}h_1h_2x \in x^{-1}Hx$.
- $a^{-1} = (x^{-1}h_1x)^{-1} = x^{-1}h_1^{-1}(x^{-1})^{-1} = x^{-1}h_1^{-1}x \in x^{-1}Hx$.

Άρα για κάθε $x \in G$ το σύνολο $x^{-1}Hx$ είναι υποομάδα της G.

Στη συνέχεια υπολογίζουμε τη τάξη της υποομάδας $x^{-1}Hx$. Θεωρούμε την απεικόνιση:

$$f : H \longrightarrow x^{-1}Hx, \quad h \longmapsto f(h) = x^{-1}hx$$

Ισχυριζόμαστε ότι η συνάρτηση f είναι «1-1» και «επί». Έχουμε:

- **«1-1»**: Έστω ότι για $h_1, h_2 \in H$, ισχύει: $f(h_1) = f(h_2)$. Τότε

$$x^{-1}h_1x = x^{-1}h_2x \implies h_1x = h_2x \implies h_1 = h_2 \implies f\text{: 1-1}$$

- **«Επί»**: Έστω $x^{-1}hx \in x^{-1}Hx$. Τότε για το στοιχείο $h \in H$ ισχύει ότι $f(h) = x^{-1}hx$. Άρα η απεικόνιση f είναι «επί».

Επομένως: $\mathsf{o}(x^{-1}Hx) = \mathsf{o}(H)$.

Παρόμοια αποδεικνύουμε ότι το υποσύνολο xHx^{-1} είναι μνια υποομάδα της G και η απεικόνιση

$$g : H \longrightarrow xHx^{-1}, \quad h \longmapsto g(h) = xhx^{-1}$$

είναι «1-1» και «επί». Επομένως: $\mathsf{o}(xHx^{-1}) = \mathsf{o}(H)$. ■

Άσκηση 3. Βρείτε το πλήθος των γεννητόρων μιας κυκλικής ομάδας με τάξη:

(α΄) 5, **(β΄)** 8, **(γ΄)** 12, **(δ΄)** 60

Λύση. Έστω G μια κυκλική ομάδα τάξης n. Τότε γνωρίζουμε από τη θεωρία ότι το πλήθος των γεννητόρων της G ισούται με $\phi(n)$ όπου ϕ είναι η συνάρτηση του Euler. Υπενθυμίζουμε ότι αν $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$ είναι η πρωτογενής ανάλυση του αριθμού $n \in \mathbb{N}$ τότε:

$$\phi(n) = (p_1^{a_1} - p_1^{a_1-1}) \cdot (p_2^{a_2} - p_2^{a_2-1}) \cdots (p_n^{a_n} - p_n^{a_n-1}) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$$

Έχουμε:

(α΄) $\phi(5) = 5^1 - 5^0 = 4$.

(β΄) $\phi(8) = \phi(2^3) = (2^3 - 2^2) = 4$.

(γ΄) $\phi(12) = \phi(3 \cdot 2^2) = \phi(3) \cdot \phi(2^2) = (3^1 - 3^0) \cdot (2^2 - 2^1) = 2 \cdot 2 = 4$.

(δ΄) $\phi(60) = \phi(2^2 \cdot 3 \cdot 5) = \phi(2^2) \cdot \phi(3) \cdot \phi(5) = (2^2 - 2^1) \cdot (3^1 - 3^0) \cdot (5^1 - 5^0) = 2 \cdot 2 \cdot 4 = 16$. ■

Άσκηση 4. **1.** Οι γεννήτορες της κυκλικής πολλαπλασιαστικής ομάδας U_n όλων των n-στών ριζών της μονάδας στο $\mathbb{C}$ καλούνται **πρωταρχικές n-οστές ρίζες της μονάδας**.

Βρείτε τις πρωταρχικές n-οστές ρίζες της μονάδας για $n = 4$, $n = 17$, $n = 24$, και $n = 31$.

2. Να ευρεθούν όλοι οι γεννήτορες των ομάδων $(\mathbb{Z}_{10}, +)$, $(\mathbb{Z}_{12}, +)$ και $(\mathbb{Z}_{15}, +)$.

Λύση. **1.** Έχουμε

$$\mathsf{U}_n = \left\{ e^{\frac{2\pi k i}{n}} \in \mathbb{C} \mid 0 \leq k \leq n-1 \right\} = \langle e^{\frac{2\pi i}{n}} \rangle$$

Επομένως οι πρωταρχικές ρίζες της μονάδας είναι οι δυνάμεις του γεννήτορα $(e^{\frac{2\pi i}{n}})^k = e^{\frac{2\pi k i}{n}}$, $1 \leq k \leq n$, για τις οποίες $(k, n) = 1$, δηλαδή οι πρωταρχικές n-οστές ρίζες της μονάδας είναι τα στοιχεία του συνόλου

$$\left\{ e^{\frac{2\pi k i}{n}} \in \mathbb{C} \mid 1 \leq k \leq n \ \ \& \ \ (k, n) = 1 \right\}$$

(1) Οι πρωταρχικές ρίζες της U_4 είναι 2 διότι $\phi(4) = \phi(2^2) = 2$. Έχουμε:

$$\mathsf{U}_4 = \{ z \in \mathbb{C} \mid z^4 = 1 \} = \{ i, -1, 1, -i \} = \langle i \rangle = \langle -i \rangle$$

και άρα οι πρωταρχικές ρίζες της U_4 είναι οι εξής: $i, -i$.

(2) Οι πρωταρχικές ρίζες της U_{17} είναι 16 διότι $\phi(17) = 17 - 1 = 16$. Επομένως θα έχουμε ότι οι πρωταρχικές ρίζες είναι οι εξής:

$$\{ e^{\frac{2\pi k i}{n}} \in \mathbb{C} \mid k = 1, 2, \cdots, 16 \}$$

(3) Οι πρωταρχικές ρίζες της U_{24} είναι 8 διότι $\phi(24) = \phi(2^3) = 8$. Επομένως θα έχουμε ότι οι πρωταρχικές ρίζες είναι οι εξής:

$$\{ e^{\frac{2\pi k i}{n}} \in \mathbb{C} \mid k = 1, 5, 7, 11, 13, 17, 19, 23 \}$$

(4) Οι πρωταρχικές ρίζες της U_{31} είναι 30 διότι $\phi(31) = 31 - 1 = 30$. Επομένως θα έχουμε ότι οι πρωταρχικές ρίζες είναι οι εξής:

$$\{ e^{\frac{2\pi k i}{n}} \in \mathbb{C} \mid k = 1, 2, 3, \cdots, 30 \}$$

2. Έχουμε

$$\mathbb{Z}_n = \left\{ [0]_n, [1]_n, \cdots, [n-1]_n = \langle [1]_n \rangle \right\}$$

Επομένως οι γεννήτορες της $\mathbb{Z}_n$ είναι σε πλήθος $\phi(n)$ και είναι τα φυσικά πολλαπλάσια του γεννήτορα $k[1]_n = [k]_n$, $1 \leq k \leq n$, για τις οποίες $(k, n) = 1$, δηλαδή είναι τα στοιχεία του συνόλου

$$\left\{ [k]_n \in \mathbb{Z}_n \mid 1 \leq k \leq n \ \ \& \ \ (k, n) = 1 \right\}$$

(1) Για την $(\mathbb{Z}_{10}, +)$: Το πλήθος των γεννητόρων της είναι $\phi(10) = 4$, και είναι τα εξής:

$$[1]_{10}, \quad [3]_{10}, \quad [7]_{10}, \quad [9]_{10}$$

(2) Για την $(\mathbb{Z}_{12}, +)$: Το πλήθος των γεννητόρων της είναι $\phi(12) = 4$, και είναι τα εξής:

$$[1]_{12}, \quad [5]_{12}, \quad [7]_{12}, \quad [11]_{12}$$

(3) Για την $(\mathbb{Z}_{15}, +)$: Το πλήθος των γεννητόρων της είναι $\phi(15) = 8$, και είναι τα εξής:

$$[1]_{15}, \quad [4]_{15}, \quad [2]_{12}, \quad [7]_{12}, \quad [8]_{12}, \quad [11]_{12}, \quad [13]_{15}, \quad [14]_{15}$$ ■

Άσκηση 5. **1**. Βρείτε το πλήθος των στοιχείων της κυκλικής υποομάδας $\langle [25]_{30} \rangle$ της ομάδας $(\mathbb{Z}_{30}, +)$.
2. Βρείτε το πλήθος των στοιχείων της κυκλικής υποομάδας $\langle [30]_{42} \rangle$ της ομάδας $(\mathbb{Z}_{42}, +)$.
3. Βρείτε το πλήθος των στοιχείων της κυκλικής υποομάδας $\langle i \rangle$ της πολλαπλασιαστικής ομάδας $\mathbb{C}^*$ των μη μηδενικών μιγαδικών αριθμών.
4. Βρείτε το πλήθος των στοιχείων της κυκλικής υποομάδας $\langle 1 + i \rangle$ της πολλαπλασιαστικής ομάδας $\mathbb{C}^*$ των μη μηδενικών μιγαδικών αριθμών.

Λύση. **1.** Έχουμε:

$$\langle [25]_{30} \rangle = \left\{ k[25]_{30} \in \mathbb{Z}_{30} \mid k \in \mathbb{Z} \right\} = \left\{ [25]_{30}, [20]_{30}, [15]_{30}, [10]_{30}, [5]_{30}, [0]_{30} \right\}$$

και άρα $\mathsf{o}([25]_{30}) = 6$. Διαφορετικά, επειδή προφανώς $\mathsf{o}(a) < \infty$, χρησιμοποιώντας το γνωστό τύπο:

$$\mathsf{o}(a^k) = \frac{\mathsf{o}(a)}{(\mathsf{o}(a), k)} \qquad (*)$$

Θα έχουμε:

$$\mathsf{o}([25]_{30}) = \mathsf{o}(25 \cdot [1]_{30}) = \frac{\mathsf{o}([1])}{(\mathsf{o}([1]), 25)} = \frac{30}{(30, 25)} = \frac{30}{5} = 6$$

2. Υπολογίζοντας τη κυκλική υποομάδα $\langle [30]_{42} \rangle$ της ομάδας $(\mathbb{Z}_{42}, +)$ έχουμε:

$$\langle [30]_{42} \rangle = \big\{ [30]_{42}, [18]_{42}, [6]_{42}, [36]_{42}, [24]_{42}, [12]_{42}, [0]_{42} \big\} \implies \mathsf{o}([30]_{42}) = 7$$

ή χρησιμοποιώντας τον τύπο $(*)$ βρίσκουμε

$$\mathsf{o}([30]_{42}) = \mathsf{o}(30 \cdot [1]_{42}) = \frac{\mathsf{o}([1])}{(\mathsf{o}([1]), 30)} = \frac{42}{(42, 30)} = \frac{42}{6} = 7$$

3. Έχουμε:

$$\langle i \rangle = \big\{ i, i^2, i^3, i^4, \cdots \big\} = \big\{ i, -1, -i, 1 \big\} \implies \mathsf{o}(\langle i \rangle) = 4$$

4. Έστω ότι $\mathsf{o}(1+i) < \infty$. Τότε υπάρχει $n \geq 1$ έτσι ώστε $(1+i)^n = 1$ και άρα

$$1 + i \in \mathsf{U}_n = \big\{ z \in \mathbb{C} \mid z^n = 1 \big\} \subseteq \big\{ z \in \mathbb{C} \mid |z| = 1 \big\}$$

Δηλαδή το μέτρο του $1+i$ είναι ένα. Αυτό όμως είναι άτοπο αφού $|1+i| = \sqrt{2} \neq 1$. Επομένως η τάξη του $1 + i \in \mathbb{C}^*$ είναι $\mathsf{o}(1+i) = \infty$. ■

Άσκηση 6. Ποιες είναι οι δυνατές τάξεις για τις υποομάδες των επόμενων κυκλικών ομάδων;

(α') $(\mathbb{Z}_6, +)$, **(β')** $(\mathbb{Z}_8, +)$, **(γ')** $(\mathbb{Z}_{12}, +)$, **(δ')** $(\mathbb{Z}_{60}, +)$, **(ε')** $(\mathbb{Z}_{17}, +)$

Λύση. Υπενθυμίζουμε από τη Θεωρία ότι: *«για κάθε διαιρέτη d της τάξης n μιας κυκλικής ομάδας G, υπάρχει μοναδική υποομάδα $H \leq G$ με τάξη του διαιρέτη d: $|H| = d$»*. Άρα έχουμε:

(α') Διαιρέτες του 6: $1, 2, 3, 6$. Άρα η $(\mathbb{Z}_6, +)$ έχει 4 υποομάδες με τάξεις: $1, 2, 3, 6$.
(β') Διαιρέτες του 8: $1, 2, 4, 8$. Άρα η $(\mathbb{Z}_8, +)$ έχει 4 υποομάδες με τάξεις: $1, 2, 4, 6$.
(γ') Διαιρέτες του 12: $1, 2, 3, 4, 6, 12$. Άρα η $(\mathbb{Z}_{12}, +)$ έχει 6 υποομάδες με τάξεις: $1, 2, 3, 4, 6, 12$.
(δ') Διαιρέτες του 60: $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$. Άρα η $(\mathbb{Z}_{60}, +)$ έχει 12 υποομάδες με τάξεις: $1, 2, 3, 5, 6, 10, 12, 15, 20, 30, 60$.
(ε') Διαιρέτες του 17: $1, 17$. Άρα η $(\mathbb{Z}_{17}, +)$ έχει 2 υποομάδες με τάξεις: $1, 17$. ■

Άσκηση 7. Βρείτε όλες τις υποομάδες των παρακάτω ομάδων και σχεδιάστε το διάγραμμα Hasse των υποομάδων της.

(α') $(\mathbb{Z}_{12}, +)$, **(β')** $(\mathbb{Z}_{36}, +)$, **(γ')** $(\mathbb{Z}_8, +)$

Λύση. Έστω $G = \langle a \rangle$ μια κυκλική ομάδα τάξης $|G| = m = \mathsf{o}(a)$. Υπενθυμίζουμε ότι για κάθε διαιρέτη $d \mid m$ υπάρχει μοναδική υποομάδα $H_d \leq G$ με τάξη $|H_d| = d$ και επιπλέον γνωρίζουμε ότι:

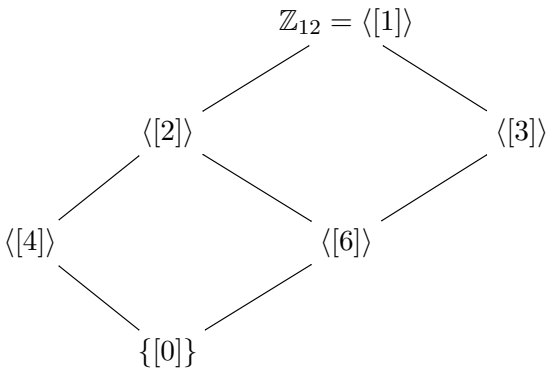
$$H_d = \langle a^{\frac{m}{(d,m)}} \rangle$$

Άρα για να βρούμε όλες τις υποομάδες, βρίσκουμε όλους τους διαιρέτες της τάξης της ομάδας, και με βάση τις παραπάνω πληροφορίες προσδιορίζουμε τις υποομάδες που αντιστοιχούν στους διαιρέτες.

(α') Η τάξη της $\mathbb{Z}_{12}$ είναι 12 και οι διαιρέτες του 12 είναι οι αριθμοί: 1, 2, 3, 4, 6, 12. Συνεπώς θα βρούμε στο σύνολο έξι υποομάδες. Έχουμε (εδώ $[\cdot]$ συμβολίζει $[\cdot]_{12}$):

- $H_1 = \langle [1]^{\frac{12}{(1,12)}} \rangle = \langle [1]^{\frac{12}{1}} \rangle = \langle 12 \cdot [1] \rangle = \langle [12] \rangle = \{ [0] \}$
- $H_2 = \langle [1]^{\frac{12}{(2,12)}} \rangle = \langle [1]^{\frac{12}{2}=6} \rangle = \langle 6 \cdot [1] \rangle = \langle [6] \rangle = \{ [0], [6] \}$
- $H_3 = \langle [1]^{\frac{12}{(3,12)}} \rangle = \langle [1]^{\frac{12}{3}=4} \rangle = \langle 4 \cdot [1] \rangle = \langle [4] \rangle = \{ [0], [4], [8] \}$
- $H_4 = \langle [1]^{\frac{12}{(4,12)}} \rangle = \langle [1]^{\frac{12}{4}=3} \rangle = \langle 3 \cdot [1] \rangle = \langle [3] \rangle = \{ [0], [3], [6], [9] \}$
- $H_6 = \langle [1]^{\frac{12}{(6,12)}} \rangle = \langle [1]^{\frac{12}{6}=2} \rangle = \langle 2 \cdot [1] \rangle = \langle [2] \rangle = \{ [0], [2], [4], [6], [8], [10] \}$
- $H_{12} = \langle [1]^{\frac{12}{(12,12)}} \rangle = \langle [1]^{\frac{12}{12}=1} \rangle = \langle [1] \rangle = \{ [0], [1], [2], [3], [4], [5], [6], [7], [8], [9], [10], [11] \} = \mathbb{Z}_{12}$

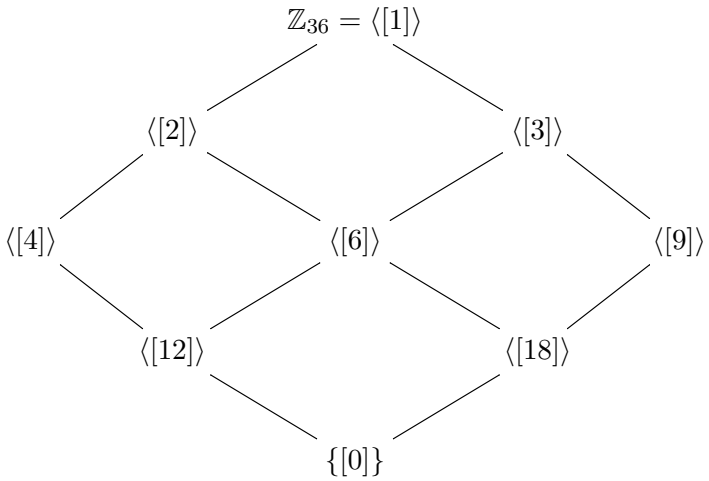
Συνεπώς το διάγραμμα Hasse των υποομάδων της $\mathbb{Z}_{12}$ είναι το εξής:



(β') Η τάξη της $\mathbb{Z}_{36}$ είναι 36 και οι διαιρέτες του 36 είναι οι αριθμοί: 1, 2, 3, 4, 6, 9, 12, 18. Συνεπώς θα βρούμε στο σύνολο 8 υποομάδες. Έχουμε (εδώ $[\cdot]$ συμβολίζει $[\cdot]_{36}$):

- $H_1 = \langle [1]^{\frac{36}{(1,36)}} \rangle = \langle [1]^{\frac{36}{1}} \rangle = \langle 36 \cdot [1] \rangle = \langle [36] \rangle = \{[0]\}$
- $H_2 = \langle [1]^{\frac{36}{(2,36)}} \rangle = \langle [1]^{\frac{36}{2}=18} \rangle = \langle 18 \cdot [1] \rangle = \langle [18] \rangle = \{[0], [18]\}$
- $H_3 = \langle [1]^{\frac{36}{(3,36)}} \rangle = \langle [1]^{\frac{36}{3}=12} \rangle = \langle 12 \cdot [1] \rangle = \langle [12] \rangle = \{[0], [12], [24]\}$
- $H_4 = \langle [1]^{\frac{36}{(4,36)}} \rangle = \langle [1]^{\frac{36}{4}=9} \rangle = \langle 9 \cdot [1] \rangle = \langle [9] \rangle = \{[0], [9], [18], [27]\}$
- $H_6 = \langle [1]^{\frac{36}{(6,36)}} \rangle = \langle [1]^{\frac{36}{6}=6} \rangle = \langle 6 \cdot [1] \rangle = \langle [6] \rangle = \{[0], [6], [12], [18], [24], [30]\}$
- $H_9 = \langle [1]^{\frac{36}{(9,36)}} \rangle = \langle [1]^{\frac{36}{9}=4} \rangle = \langle 4 \cdot [1] \rangle = \langle [4] \rangle = \{[0], [4], [8], [12], [16], [20], [24], [28], [32]\}$
- $H_{12} = \langle [1]^{\frac{36}{(12,36)}} \rangle = \langle [1]^{\frac{36}{12}=3} \rangle = \langle 3 \cdot [1] \rangle = \langle [3] \rangle = \{[0], [3], [6], [9], [12], [15], [18], [21], [24], [27], [30], [33]\}$
- $H_{18} = \langle [1]^{\frac{36}{(18,36)}} \rangle = \langle [1]^{\frac{36}{18}=2} \rangle = \langle 2 \cdot [1] \rangle = \langle [2] \rangle = \{[0], [2], [4], [6], [8], [10], [12], [14], [16], [18], [20], [22], [24], [26], [28], [30] ,[32], [34]\}$

Συνεπώς το διάγραμμα Hasse των υποομάδων της $\mathbb{Z}_{36}$ είναι το εξής:



(γ') Η τάξη της $\mathbb{Z}_8$ είναι 8 και οι διαιρέτες του 8 είναι οι αριθμοί: 1, 2, 4, 8. Συνεπώς θα βρούμε στο σύνολο 4 υποομάδες. Έχουμε (εδώ $[\cdot]$ συμβολίζει $[\cdot]_8$):

- $H_1 = \langle [1]^{\frac{8}{(1,8)}} \rangle = \langle [1]^{\frac{8}{1}=8} \rangle = \langle 8 \cdot [1] \rangle = \langle [8] \rangle = \{[0]\}$
- $H_2 = \langle [1]^{\frac{8}{(2,8)}} \rangle = \langle [1]^{\frac{8}{2}=4} \rangle = \langle 4 \cdot [1] \rangle = \langle [4] \rangle = \{[0], [4]\}$

- $H_4 = \langle [1]^{\frac{8}{(4,8)}} \rangle = \langle [1]^{\frac{8}{4}=2} \rangle = \langle 2 \cdot [1] \rangle = \langle [2] \rangle = \{[0],[2],[4],[6]\}$
- $H_8 = \langle [1]^{\frac{8}{(8,8)}} \rangle = \langle [1]^{\frac{8}{8}=1} \rangle = \langle 1 \cdot [1] \rangle = \langle [1] \rangle = \{[0],[1],[2],[3],[4],[5],[6],[7]\} = \mathbb{Z}_8$

Άρα το διάγραμμα Hasse των υποομάδων της $\mathbb{Z}_8$ είναι το ακόλουθο:

$$\begin{array}{c} \langle [1] \rangle = \mathbb{Z}_8 \\ | \\ \langle [2] \rangle \\ | \\ \langle [4] \rangle \\ | \\ \{0\} \end{array}$$

■

Άσκηση 8. Έστω $(G, \cdot)$ μια ομάδα και θεωρούμε το ακόλουθο σποσύνολο της G:

$$F(G) = \big\{ x \in G \mid \mathsf{o}(x) < \infty \big\}$$

(1) Αν η ομάδα G είναι αβελιανή, να δειχθεί ότι το υποσύνολο $F(G)$ είναι μια υποομάδα της G.
(2) Αν η ομάδα G δεν είναι αβελοανή, να δειχθεί με ένα αντιπαράδειγμα ότι το υποσύνο $F(G)$ δεν είναι υποομάδα της G.
(3) Να βρεθεί η υποομάδα $F(\mathbb{C}^*)$.
(4) Αν η ομάδα G είναι πεπερασμένη, τότε $F(G) = G$. Αν $F(G) = G$, να δειχθεί με ένα αντιπαράδειγμα ότι η ομάδα G δεν είναι απαραίτητα πεπερασμένη.

Λύση. (1) Προφανώς $F(G) \neq \emptyset$ διότι $\mathsf{o}(e) = 1$ και άρα $e \in F(G)$. Έστω $x, y \in F(G)$. Τότε υπάρχουν θετικοί ακέραιοι n και m έτσι ώστε $\mathsf{o}(x) = n$ και $\mathsf{o}(y) = m$. Ιδιαίτερα θα έχουμε $x^n = e = y^m$. Επειδή η ομάδα G είναι αβελιανή, θα έχουμε

$$(xy)^{nm} = x^{nm} y^{nm} = (x^n)^m (y^m)^n = e^m e^n = e$$

και επομένως $\mathsf{o}(xy) < \infty$, δηλαδή $xy \in F(G)$. Τέλος, επειδή σε μια ομάδα $\mathsf{o}(x) = \mathsf{o}(x^{-1})$, $llx \in F(G)$, έπεται ότι $x^{-1} \in F(G)$, $\forall x \in F(G)$.

Επομένως το υποσύνολο $F(G)$ είναι μια υπομάδα της G.

(2) Θεωρούμε την μη-αβελιανή ομάδα $(\mathsf{GL}_2(\mathbb{R}), \cdot)$ των 2×2 αντιστρέψιμων πινάκων υπεράνω του $\mathbb{R}$, και έστω οι πίνακες

$$A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{και} \quad A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Τότε

$$A^2 = I_2 = B^2 \quad \text{και} \quad AB = A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

Άρα $\mathsf{o}(A) = 2 = \mathsf{o}(B)$, επομένως $A, B \in F(\mathsf{GL}_2(\mathbb{R}))$. Όμως επειδή, όπως μπορούμε να δούμε εύκολα

$$(AB)^n = A = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$$

έπεται ότι $AB \notin F(\mathsf{GL}_2(\mathbb{R}))$ και επομένως το υποσύνολο $F(\mathsf{GL}_2(\mathbb{R}))$ δεν είναι κλειστό στην πράξη της ομάδας και άρα δεν είναι υποομάδα της $\mathsf{GL}_2(\mathbb{R})$.

(3) Θεωρούμνε την αβελιανή ομάδα $(\mathsf{C}^*, \cdot)$ των μη-μηδενικών μιγαδικών αριθμών. Αν $z \in \mathbb{C}^*$, τότε υπάρχει θετικός ακέραιος n έτσι ώστε $z^n = 1$, και επομένως $z \in \mathsf{U}_n$, δηλαδή ο μιγαδικός αριθμός z είναι μια n-οστή ρίζα της μονάδας. Έτσι $z \in \bigcup_{n=1}^{\infty} \mathsf{U}_n$ και επομένως

$$F(\mathbb{C}^*) = \bigcup_{n=1}^{\infty} \mathsf{U}_n = \mathsf{U}$$

δηλαδή η υποομάδα $F(\mathbb{C}^*)$ συμπίπτει με την υποομάδα των ριζών της μονάδας, βλέπε Ασκήσεις **1**, **2** του Φυλλαδίου Ασκήσεων **3**.

(4) Προφανώς $F(G) = G$ αν η G είναι πεπερασμένη, διότι τότε κάθε στοιχείο της G έχει πεπερασμένη τάξη: αν το στοιχείο $x \in G$ είχε άπειρη τάξη, τότε εξ' ορισμού η κυκλική υποομάδα $\langle x \rangle$ της G η οποία παράγεται από το x θα ήταν μια άπειρη κυκλική υποομάδα της πεπερασμένης ομάδας G και αυτό είναι άτοπο διότι ένα πεπερασμένο σύνολο δεν μπορεί να περιέχει ένα άπειρο υποσύνολο.

Θεωρούμε την υποομάδα $\mathsf{U} \leq \mathbb{C}^*$ των ριζών της μονάδας. Τότε από την Άσκηση **3** του Φυλλαδίου **3** έπεται ότι η U είναι μια άπειρη ομάδα, κάθε στοιχείο της οποίας έχει πεπερασμένη τάξη. Άρα $F(\mathsf{U}) = \mathsf{U}$ και η U είναι μια άπειρη ομάδα. ■

Άσκηση 9. Έστω ότι $G = \{g_1, g_2, \cdots, g_n\}$ είναι μια πεπερασμένη αβελιανή ομάδα, και έστω $g_1 = e$.

1. Να δειχθεί ότι: **(α)** $(g_1 g_2 \cdots g_n)^2 = e$ και **(β)** $\forall g \in G$: $g^n = e$.[3]

2. Τι συμβαίνει αν η τάξη της G είναι περιττός αριθμός;

Λύση. **1. (α)** Γνωρίζουμε ότι για κάθε $g \in G$ υπάρχει το αντίστροφο στοιχείο $g^{-1} \in G$. Επειδή η G είναι αβελιανή και $g_1, g_2, \cdots, g_n$ είναι όλα τα στοιχεία της G έπεται ότι στο γινόμενο $g_1 g_2 \cdots g_n$ θα μείνουν μόνα εκείνα τα στοιχεία $g \in G$ έτσι ώστε $g = g^{-1}$, καθώς τα υπόλοιπα εμφανίζονται ως γινόμενα ζευγών $gg^{-1} = e$ τα οποία δεν συνεισφέρουν τίποτα στο γινόμενο $g_1 g_2 \cdots g_n$. Άρα $g_1 g_2 \cdots g_n = h_1 h_2 \cdots h_k$ όπου $h_i \in G$ και $h_i = h_i^{-1}$, δηλαδή ισοδύναμα $h_i^2 = e$. Τότε όμως αφού η G είναι αβελιανή έχουμε

$$(g_1 g_2 \cdots g_n)^2 = (h_1 h_2 \cdots h_k)^2 = h_1^2 h_2^2 \cdots h_k^2 = ee \cdots e = e$$

και άρα δείξαμε πράγματι ότι $(g_1 g_2 \cdots g_n)^2 = e$.

(β) Έστω τυχόν στοιχείο $g \in G$. Τότε τα στοιχεία $gg_1, gg_2, \cdots, gg_n$ είναι διακεκριμένα διότι αν $gg_i = gg_j$, όπου $i \neq j$, τότε θα έχουμε $g^{-1}gg_i = g^{-1}gg_j$ και άρα $g_i = g_j$. Αυτό είναι άτοπο διότι $g_i \neq g_j$ αν $i \neq j$. Επειδή το σύνολο G είναι πεπερασμένο, έπεται ότι:

$$G = \{g_1, g_2, \cdots, g_n\} = \{gg_1, gg_2, \cdots, gg_n\}$$

Δηλαδή τα στοιχεία $gg_1, gg_2, \cdots, gg_n$ είναι τα στοιχεία $g_1, g_2, \cdots, g_n$ ενδεχομένως με διαφορετική σειρά. Χρησιμοποιώντας ότι η ομάδα G είναι αβελιανή και θέτοντας $x = g_1 g_2 \cdots g_n$. θα έχουμε:

$$x = g_1 \cdot g_2 \cdot \cdots \cdot g_n = gg_1 \cdot gg_2 \cdot \cdots \cdot gg_n = g \cdot g \cdot \cdots \cdot g \cdot g_1 \cdot g_2 \cdot \cdots \cdot g_n = g^n \cdot x$$

απ' όπου ο Νόμος Διαγραφής δίνει ότι:

$$g^n = e$$

2. Έστω ότι η τάξη της G είναι περιττός αριθμός. Αν το στοιχείο $g_1 g_2 \cdots g_n$ δεν είναι το ουδέτερο, δηλαδή $g_1 g_2 \cdots g_n \neq e$, τότε από το ερώτημα (1) έπεται ότι $\mathsf{o}(g_1 g_2 \cdots g_n) = 2$. Επειδή όμως $2 \mid \mathsf{o}(G)$ έχουμε καταλήξει σε άτοπο. Συνεπώς αν η τάξη $\mathsf{o}(G)$ είναι περιττός αριθμός τότε $g_1 g_2 \cdots g_n = e$:

$$\mathsf{o}(G): \text{ περιττός} \quad \Longrightarrow \quad g_1 g_2 \cdots g_n = e$$ ■

[3] Θα δούμε αργότερα, με χρήση του Θεωρήματος Lagrange, ότι $g^n = e$ για κάθε στοιχείο g σε μια πεπερασμένη ομάδα G, όχι απαραίτητα αβελιανή.

Άσκηση 10. Έστω ότι $(G,\cdot)$ είναι μια πεπερασμένη ομάδα η οποία ικανοποιεί την ακόλουθη συνθήκη:[4]

$$\textit{Αν } H,K \textit{ είναι οποιεσδήποτε υποομάδες της } G, \textit{ τότε: } \quad \textit{είτε } H\subseteq K \text{ είτε } K\subseteq H$$

Να δειχθεί ότι η G είναι κυκλική ομάδα της οποίας η τάξη της ισούται με τη δύναμη ενός πρώτου αριθμού.

Λύση. Αν $G=\{e\}$, τότε η G ικανοποιεί την δοσμένη συνθήκη και η G είναι προφανώς κυκλική τάξης $2^0=1$.

Έστω $\mathsf{o}(G)>1$, δηλαδή $G\neq\{e\}$, και υποθέτουμε ότι η ομάδα G δεν είναι κυκλική. Έστω $a_1\in G$ με $a_1\neq e$. Τότε αφού η G δεν είναι κυκλική έπεται ότι

$$\langle a_1\rangle \subsetneqq G$$

όπου $\langle a_1\rangle$ είναι η κυκλική υποομάδα της G που παράγεται από το a_1. Άρα υπάρχει στοιχείο $a_2\in G\backslash\langle a_1\rangle$ και θεωρούμε την κυκλική υποομάδα $\langle a_2\rangle$ της G. Από την υπόθεση έχουμε

$$\langle a_1\rangle\subseteq\langle a_2\rangle \quad \text{ή} \quad \langle a_2\rangle\subseteq\langle a_1\rangle$$

Όμως αφού $a_2\notin\langle a_1\rangle$ έπεται ότι

$$\langle a_2\rangle\not\subseteq\langle a_1\rangle \implies \langle a_1\rangle\subseteq\langle a_2\rangle$$

Επειδή η G δεν είναι κυκλική έχουμε ότι $G\neq\langle a_2\rangle$ και άρα υπάρχει στοιχείο $a_3\in G\backslash\langle a_2\rangle$. Τότε όπως παραπάνω έχουμε

$$\langle a_2\rangle\subseteq\langle a_3\rangle \quad \text{και} \quad \langle a_3\rangle\neq G$$

Συνεχίζοντας αυτή τη διαδικασία θα έχουμε μια αλυσίδα υποομάδων της G η οποία δεν σταματά:

$$\{e\}\subsetneqq\langle a_1\rangle\subsetneqq\langle a_2\rangle\subsetneqq\langle a_3\rangle\subsetneqq\cdots\cdots\subsetneqq G$$

και άρα θα έχουμε άπειρο πλήθος διακεκριμμένων στοιχείων $e,a_1,a_2,a_3,\cdots$ στην G. Έτσι όμως έχουμε καταλήξει σε άτοπο δίοτι η ομάδα G είναι πεπερασμένη. Άρα η ομάδα G είναι κυκλική.

Έστω $\mathsf{o}(G)=n=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$, όπου $p_1,p_2,\cdots,p_r$ πρώτοι αριθμοί με $p_i\neq p_j$ για $i\neq j$. Έστω $r\geq 2$. Τότε υπάρχουν i,j με $i\neq j$ έτσι ώστε $p_i\mid n$ και $p_j\mid n$. Επειδή η ομάδα G είναι κυκλική έπεται ότι υπάρχει υποομάδα H της G με τάξη $|H|=p_i$ και υποομάδα K της G με τάξη $|K|=p_j$. Από την υπόθεση όμως έχουμε

$$H\subseteq K \quad \text{ή} \quad K\subseteq H \implies p_i\mid p_j \quad \text{ή} \quad p_j\mid p_i$$

το οποίο είναι άτοπο διότι $p_i\neq p_j$. Επομένως $r=1$, δηλαδή στην πρωτογενή ανάλυση του n εμφανίζεται μόνο ένας πρώτος αριθμός, έστω ο πρώτος p, και άρα

$$\mathsf{o}(G)=n=p^k$$

για κάποιον θετικό ακέραιο $k\geq 1$. Συνεπώς δείξαμε ότι μια πεπερασμένη *μονοσειριακή* ομάδα είναι κυκλική που η τάξη της ισούται με τη δύναμη ενός πρώτου αριθμού. ■

Άσκηση 11. Θεωρούμε την ομάδα $(\mathsf{U}(\mathbb{Z}_{20}),\cdot)$ των αντιστρέψιμων κλάσεων ισοδυναμίας των ακεραίων $\bmod 20$ με πράξη τον πολλαπλασιασμό κλάσεων ισοτιμίας $\bmod 20$. Στην παρούσα Άσκηση $[\cdot]$ συμβολίζει $[\cdot]_{20}$.

1. Να δειχθεί ότι
$$\mathsf{U}(\mathbb{Z}_{20})=\big\{[1],[3],[7],[9],[11],[13],[17],[19]\big\}$$
2. Να δειχθεί ότι για κάθε στοιχείο $u\in\mathsf{U}(\mathbb{Z}_{20})$ ισχύει $u^8=[1]$.
3. Είναι η ομάδα $(\mathsf{U}(\mathbb{Z}_{20}),\cdot)$ κυκλική;
4. Να λυθεί ως προς x η εξίσωση $[17]^{(-108)}\cdot x\cdot[7]^{333}=[3]^{-1}$ στην ομάδα $\mathsf{U}(\mathbb{Z}_{20})$.

Λύση. **1.** Έχουμε:

$$\mathsf{o}\big(\mathsf{U}(\mathbb{Z}_{20})\big)=\phi(20)=\phi(2^2\cdot 5)=\phi(2^2)\cdot\phi(5)=(2^2-2^1)\cdot(5^1-5^0)=2\cdot 4=8$$

και

$$\mathsf{U}(\mathbb{Z}_{20})=\{1\leq k\leq 20\mid (k,20)=1\}=\{[1],[3],[7],[9],[11],[13],[17],[19]\}$$

[4] μια τέτοια ομάδα καλείται **μονοσειριακή** (uniserial)

2. Επειδή $\mathsf{o}\big(\mathsf{U}(\mathbb{Z}_{20})\big) = 8$ και η ομάδα $\mathsf{U}(\mathbb{Z}_{20})$ είναι αβελιανή, από τη Άσκηση 9, έπεται ότι $u^8 = [1]$ για κάθε στοιχείο $u \in \mathsf{U}(\mathbb{Z}_{20})$.

3. Αν η ομάδα $(\mathsf{U}(\mathbb{Z}_{20}), \cdot)$ ήταν κυκλική, τότε θα υπήρχε ένα στοιχείο της, έστω $u \in \mathsf{U}(\mathbb{Z}_{20})$, με τάξη $\mathsf{o}(u) = 8 = \mathsf{o}(\mathsf{U}(\mathbb{Z}_{20}))$. Όμως, όπως βλέπουμε εύκολα:

$$\mathsf{o}([3]) = \mathsf{o}([7]) = \mathsf{o}([13]) = \mathsf{o}([17]) = 4 \quad \text{και} \quad \mathsf{o}([9]) = \mathsf{o}([11]) = \mathsf{o}([19]) = 2$$

Επομένως η ομάδα $(\mathsf{U}(\mathbb{Z}_{20}), \cdot)$ δεν διαθέτει στοιχείο τάξης 8 και άρα δεν είναι κυκλική.

4. Επειδή $u^8 = [1]$ για κάθε στοιχείο $u \in \mathsf{U}(\mathbb{Z}_{20})$ έχουμε ότι $u^{-1} = u^7$. Τότε έχουμε

$$\begin{aligned}
[17]^{(-108)} \cdot x \cdot [7]^{333} = [3]^{(-1)} \quad &\Longrightarrow \quad x = [17]^{108} \cdot [3]^{-1} \cdot [7]^{-333} \\
&\Longrightarrow \quad x = [17]^{108} \cdot [3]^{7} \cdot ([7]^{-1})^{333} \\
&\Longrightarrow \quad x = [17]^{108} \cdot [3]^{7} \cdot ([7]^{7})^{333} \\
&\Longrightarrow \quad x = [17]^{108} \cdot [3]^{7} \cdot ([7])^{2331} \\
&\Longrightarrow \quad x = [17]^{13\cdot 8+4} \cdot [3]^{7} \cdot ([7])^{291\cdot 8+3} \\
&\Longrightarrow \quad x = [17]^{4} \cdot [3]^{7} \cdot ([7])^{3} \\
&\Longrightarrow \quad x = [17]^{2} \cdot [17]^{2} \cdot [3]^{2} \cdot [3]^{2} \cdot [3]^{3} \cdot [7]^{3} \\
&\Longrightarrow \quad x = [9] \cdot [9] \cdot [9] \cdot [9] \cdot [27] \cdot [49] \cdot [7] \\
&\Longrightarrow \quad x = [81] \cdot [81] \cdot [27] \cdot [49] \cdot [7] \\
&\overset{\mathsf{mod}\,20}{\Longrightarrow} \quad x = [1] \cdot [1] \cdot [7] \cdot [9] \cdot [7] = [63] \cdot [7] = [3] \cdot [7] = [1] \quad \blacksquare
\end{aligned}$$

Άσκηση 12. Να δειχθεί ότι μια ομάδα η οποία διαθέτει ακριβώς δύο υποομάδες είναι κυκλική τάξης p, όπου p είναι ένας πρώτος αριθμός.

Λύση. Επειδή η τετριμμένη υποομάδα $\{e\}$ και η ίδια η ομάδα G είναι υποομάδες της G, έπεται ότι οι μόνες υποομάδες της G είναι οι εξής: $\{e\}$ και G. Αν $G = \{e\}$, τότε $G = \langle e \rangle = \{e\}$ και άρα η G έχει ακριβώς μια υποομάδα κάτι το οποίο είναι άτοπο από την υπόθεση.

Άρα $G \neq \{e\}$, και επομένως υπάρχει στοιχείο $a \in G \backslash \{e\}$. Θεωρούμε την κυκλική υποομάδα $\langle a \rangle \leq G$ η οποία παράγεται από το a. Επειδή $a \neq e$ έπεται ότι $\langle a \rangle \neq \langle e \rangle$ και άρα $G = \langle a \rangle$, δηλαδή η ομάδα G είναι κυκλική. Επιπλέον η τάξη της G είναι πεπερασμένη διότι αν $\mathsf{o}(G) = \infty$ τότε η G θα ήταν άπειρη κυκλική και όπως γνωρίζουμε σ' αυτήν την περίπτωση η G θα είχε άπειρες υποομάδες:

$$\langle e \rangle,\ \langle a \rangle,\ \langle a^2 \rangle, \cdots,\ \langle a^n \rangle, \cdots$$

το οποίο είναι άτοπο. Άρα $\mathsf{o}(G) = \mathsf{o}(a) = p < \infty$, για κάποιον θετικό ακέραιο p.

Αν ο p είναι σύνθετος, θα έχουμε $p = \kappa \cdot \lambda$, όπου $1 < \kappa, \lambda < p$. Επειδή η G είναι κυκλική, έπεται ότι[5] η G θα έχει γνήσια μη-τετριμμένη υποομάδα τάξης κ, το οποίο είναι άτοπο από την υπόθεση. Άρα ο αριθμός p είναι πρώτος και επομένως η ομάδα G είναι κυκλική με τάξη p, όπου ο p είναι πρώτος αριθμός. $\blacksquare$

[5] Υπενθυμίζουμε ότι για κάθε διαιρέτη της τάξης μιας πεπερασμένης κυκλικής ομάδας, υπάρχει μοναδική υποομάδα με τάξη τον διαιρέτη.

Άσκηση 13. Έστω $(G,\cdot)$ μια ομάδα και a,b είναι δύο στοιχεία της με $ab=ba$. Αν οι τάξεις $\mathsf{o}(a),\mathsf{o}(b)$ είναι πεπερασμένες και $(\mathsf{o}(a),\mathsf{o}(b))=1$, να δειχθεί ότι η τάξη του στοιχείου ab ισούται με $\mathsf{o}(a)\cdot\mathsf{o}(b)$:

$$\mathsf{max}\{\mathsf{o}(a),\mathsf{o}(b)\}<\infty \quad \& \quad (\mathsf{o}(a),\mathsf{o}(b))=1 \quad \& \quad ab=ba \qquad \Longrightarrow \qquad \mathsf{o}(ab)=\mathsf{o}(a)\cdot\mathsf{o}(b)$$

Λύση. Έστω $\mathsf{o}(a)=n$, $\mathsf{o}(b)=m$ και $\mathsf{o}(ab)=k$. Άρα $a^n=e$, $b^m=e$ και επειδή $ab=ba$ έπεται ότι

$$(ab)^{nm}=ab\cdot ab\cdots ab=a^{nm}b^{nm}=(a^n)^m(b^m)^n=e^me^n=e \implies \mathsf{o}(ab)=k\mid nm=\mathsf{o}(a)\mathsf{o}(b) \tag{1}$$

Αφού $\mathsf{o}(ab)=k$ και $ab=ba$ έχουμε

$$(ab)^k=e \implies a^kb^k=e \implies a^k=b^{-k} \implies \mathsf{o}(a^k)=\mathsf{o}(b^{-k})=\mathsf{o}(b^k) \tag{$*$}$$

Τότε από τη σχέση $(*)$ έχουμε

$$\begin{cases} \mathsf{o}(a^k)=\frac{\mathsf{o}(a)}{\mathsf{o}(a),k}=\frac{n}{(n,k)} \\ \\ \mathsf{o}(b^k)=\frac{\mathsf{o}(b)}{\mathsf{o}(b),k}=\frac{m}{(m,k)} \end{cases} \implies \frac{n}{(n,k)}=\frac{m}{(m,k)} \implies n\cdot(m,k)=m\cdot(n,k)$$

$$\implies \begin{cases} n\mid m\cdot(n,k) \\ \\ m\mid n\cdot(m,k) \end{cases} \overset{(n,m)=1}{\Longrightarrow} \begin{cases} n\mid (n,k) \\ \\ m\mid (m,k) \end{cases}$$

$$\implies \begin{cases} n=(n,k) \\ \\ m=(m,k) \end{cases} \implies \begin{cases} n\mid k \\ \\ m\mid k \end{cases}$$

και άρα επειδή $(n,m)=1$ έπεται ότι

$$\mathsf{o}(a)\mathsf{o}(b)=nm\mid k=\mathsf{o}(ab) \tag{2}$$

Από τις σχέσεις (1) και (2) συμπεραίνουμε ότι $\mathsf{o}(a)\mathsf{o}(b)=\mathsf{o}(ab)$[6]. ■

Άσκηση 14. Έστω ότι $(G,\cdot)$ είναι μια ομάδα και ότι H, K είναι δύο κυκλικές υποομάδες της G.

1. Αν η G είναι αβελιανή και $|H|=10$ και $|K|=14$, να δειχθεί ότι η G διαθέτει μια υποομάδα L τάξης $|L|=70$.
2. Αν $|H|=14$ και $|K|=15$, να περιγραφεί η υποομάδα $H\cap K$.

Λύση. **1.** Παρατηρούμε ότι αφού η H είναι κυκλική τάξης 10, για κάθε διαιρέτη d τού 10 θα διαθέτει ένα στοιχείο με τάξη d. Έτσι επειδή $5\mid 10$, υπάρχει στοιχείο $a\in H$ με τάξη 5, δηλαδή $\mathsf{o}(a)=5$. Η K είναι κυκλική τάξης 14 και γι' αυτό οποιοσδήποτε γεννήτοράς της έχει τάξη 14. Ας είναι $b\in K$ ένας γεννήτορας τής K, τότε $\mathsf{o}(b)=14$. Τα συγκεκριμένα στοιχεία a,b είναι και στοιχεία της G, αφού $H\leq G$ και $K\leq G$. Αλλά η G είναι αβελιανή ομάδα και γι' αυτό $ab=ba$. Επιπλέον, για τον μέγιστο κοινό διαιρέτη των τάξεών τους είναι $(\mathsf{o}(a),\mathsf{o}(b))=(5,14)=1$. Γι' αυτό σύμφωνα με την Άσκηση 13 έπεται $\mathsf{o}(ab)=\mathsf{o}(a)\mathsf{o}(b)=5\cdot 14=70$. Τότε η κυκλική υποομάδα

$$L=\langle ab\rangle \ \leq \ G \qquad \text{έχει τάξη} \qquad |L|=\mathsf{o}(ab)=70$$

[6] ΔΙΑΦΟΡΕΤΙΚΑ: Όπως και πριν έχουμε ότι $(ab)^{nm}=e$. Θα δείξουμε ότι ο αριθμός nm είναι η τάξη του ab δείχνοντας ότι είναι ο μικρότερος φυσικός k με την ιδιότητα $(ab)^k=e$.

Αν λοιπόν υπάρχει τέτοιο k θα έχουμε όπως και πριν ότι $a^k=b^{-k}$. Τότε $\langle b\rangle\ni b^{-k}=a^k\in\langle a\rangle$, και άρα $a^k=b^{-k}\in\langle a\rangle\cap\langle b\rangle$. Όμως η ομάδα $\langle a\rangle\cap\langle b\rangle$ ως υποομάδα της $\langle a\rangle$ και υποομάδα της $\langle b\rangle$ θα είναι κυκλική με τάξη έναν διαιρέτη της $\mathsf{o}(a)=|\langle a\rangle|$ και έναν διαιρέτη της $\mathsf{o}(b)=|\langle b\rangle|$. Επειδή $(\mathsf{o}(a),\mathsf{o}(b))=1$, έπεται ότι η τάξη της $\langle a\rangle\cap\langle b\rangle$ θα είναι 1 και άρα $a^k=e=b^{-k}$. Τότε $n=\mathsf{o}(a)\mid k$ και $m=\mathsf{o}(b^{-1})=\mathsf{o}(b)\mid k$, και επομένως επειδή $(n,m)=1$, θα έχουμε $nm\mid k$, δηλαδή $nm\leq k$.

Επομένως $\mathsf{o}(ab)=nm=\mathsf{o}(a)\mathsf{o}(b)$.

2. Η $H \cap K$ είναι υποομάδα τής κυκλικής υποομάδας H, η οποία έχει τάξη 14, άρα η τάξη τής $H \cap K$ είναι ένας διαιρέτης τού 14. Η $H \cap K$ είναι υποομάδα τής κυκλικής υποομάδας K, η οποία έχει τάξη 15, άρα η τάξη τής $H \cap K$ είναι ένας διαιρέτης τού 15. Ώστε η τάξη τής $H \cap K$ κοινός διαιρέτης των αριθμών 14 και 15. Όμως ο Μ.Κ.Δ. $(14, 15) = 1$. Επομένως, $\mathsf{o}(H \cap K) = 1$. Αυτό σημαίνει ότι

$$H \cap K = \{e\}$$ ■

Άσκηση 15. **1.** Έστω ότι G είναι 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 $\mathsf{o}(H) = m$. Τα στοιχεία της H τα οποία την παράγουν έχουν τάξη m, δηλαδή αν $H = \langle x \rangle$ και $\mathsf{o}(x) = m$ τότε για κάθε $y \in H$ έχουμε:

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

Γνωρίζουμε όμως από τη Θεωρία ότι τέτοια στοιχεία είναι ακριβώς $\phi(m)$ σε πλήθος. Επίσης αν $z \in G$ είναι ένα άλλο στοιχείο με $\mathsf{o}(z) = m$ τότε λόγω μοναδικότητας των υποομάδαν τάξης m στην G, έχουμε ότι $\langle z \rangle = H$. Επομένως για κάθε διαιρέτη $m \mid n$ το πλήθος των στοιχείων της G τάξης m ισούται με $\phi(m)$.

2. Έστω G μια κυκλική ομάδα. Άν 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[7]. ■

Άσκηση 16. **1.** Έστω ότι p και q είναι πρώτοι αριθμοί. Βρείτε το πλήθος των γεννητόρων της κυκλικής ομάδας $\mathbb{Z}_{\mathrm{pq}}$ καθώς και το διάγραμμα Hasse των υποομάδων της.

2. Έστω p ένας πρώτος αριθμός. Βρείτε το πλήθος των γεννητόρων της κυκλικής ομάδας $\mathbb{Z}_{\mathrm{p}^r}$, όπου $r \geq 1$, καθώς και το διάγραμμα Hasse των υποομάδων της.

Λύση. (1) Διακρίνουμε δύο περιπτώσεις.

1. Υποθέτουμε ότι $p \neq q$.

Τότε $(p, q) = 1$, Το πλήθος $\phi(pq)$ των γεννητόρων της $\mathbb{Z}_{\mathrm{pq}}$ θα είναι

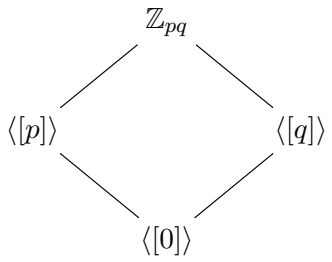
$$\phi(pq) = \phi(p) \cdot \phi(q) = (p^1 - p^0) \cdot (q^1 - q^0) = (p-1) \cdot (q-1)$$

Η τάξη της $\mathbb{Z}_{pq}$ είναι pq και οι διαιρέτες του pq είναι οι αριθμοί: 1, p, q, pq. Συνεπώς θα βρούμε στο σύνολο 4 υποομάδες. Έχουμε (εδώ $[\cdot]$ συμβολίζει $[\cdot]_{pq}$):

- $H_1 = \langle [1]^{\frac{pq}{(1,pq)}} \rangle = \langle [1]^{\frac{pq}{1}} \rangle = \langle pq \cdot [1] \rangle = \langle [pq] \rangle = \langle [0] \rangle$ τάξης 1.
- $H_p = \langle [1]^{\frac{pq}{(p,pq)}} \rangle = \langle [1]^{\frac{pq}{p}=q} \rangle = \langle q \cdot [1] \rangle = \langle [q] \rangle$ τάξης p.
- $H_q = \langle [1]^{\frac{pq}{(q,pq)}} \rangle = \langle [1]^{\frac{pq}{q}=p} \rangle = \langle p \cdot [1] \rangle = \langle [p] \rangle$ τάξης q.
- $H_{pq} = \langle [1]^{\frac{pq}{(pq,pq)}} \rangle = \langle [1]^{\frac{pq}{pq}=1} \rangle = \langle [1] \rangle = \{[0], [1], [2], \cdots, [pq-1]\} = \mathbb{Z}_{pq}$ τάξης pq.

[7] Είναι γνωστό από την Θεωρία Αριθμών ότι ο αριθμός $\phi(n)$ είναι άρτιος αν $n \geq 3$. Η παραπάνω απόδειξη δίνει μια ομαδοθεωρητική απόδειξη αυτού του ισχυρισμού: Έστω $n \geq 3$. Θεωρούμε την κυκλική ομάδα $(\mathbb{Z}_n, +)$ της οποίας το πλήθος των γεννητόρων είναι, όπως γνωρίζουμε, $\phi(n)$. Άρα σύμφωνα με τη Άσκηση 15 ο αριθμός $\phi(n)$ είναι άρτιος.

Συνεπώς το διάγραμμα Hasse των υποομάδων της $\mathbb{Z}_{pq}$ είναι το εξής:



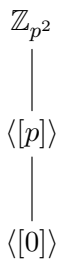
2. Υποθέτουμε ότι $p = q$.
Τότε το πλήθος $\phi(p^2)$ των γεννητόρων της $\mathbb{Z}_{p^2}$ θα είναι

$$\phi(p^2) = (p^2 - p^1) = p \cdot (p-1)$$

Η τάξη της $\mathbb{Z}_{p^2}$ είναι p^2 και οι διαιρέτες του p^2 είναι οι αριθμοί: 1, p, p^2. Συνεπώς θα βρούμε στο σύνολο 3 υποομάδες. Έχουμε (εδώ $[\cdot]$ συμβολίζει $[\cdot]_{p^2}$):

- $H_1 = \langle [1]^{\frac{p^2}{(1,p^2)}} \rangle = \langle [1]^{\frac{p^2}{1}} \rangle = \langle p^2 \cdot [1] \rangle = \langle [p^2] \rangle = \langle [0] \rangle$ τάξης 1.
- $H_p = \langle [1]^{\frac{p^2}{(p,p^2)}} \rangle = \langle [1]^{\frac{p^2}{p}=p} \rangle = \langle p \cdot [1] \rangle = \langle [p] \rangle$ τάξης p.
- $H_{p^2} = \langle [1]^{\frac{p^2}{(p^2,p^2)}} \rangle = \langle [1]^{\frac{p^2}{p^2}=1} \rangle = \langle [1] \rangle = \{[0], [1], [2], \cdots, [p^2-1]\} = \mathbb{Z}_{p^2}$ τάξης p^2.

Συνεπώς το διάγραμμα Hasse των υποομάδων της $\mathbb{Z}_{p^2}$ είναι το εξής:



(2) Το πλήθος των γεννητόρων της $\mathbb{Z}_{p^r}$ είναι

$$\phi(p^r) = (p^r - p^{r-1}) = p^{r-1} \cdot (p-1)$$

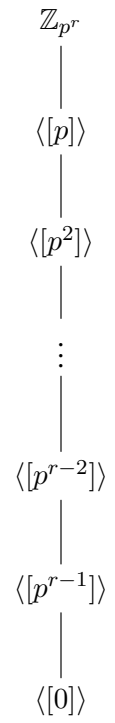
Η τάξη της $\mathbb{Z}_{p^r}$ είναι p^r και οι διαιρέτες του p^r είναι οι αριθμοί: 1, p, p^2, $\cdots$, p^r. Συνεπώς θα βρούμε στο σύνολο $r+1$ υποομάδες. Έχουμε (εδώ $[\cdot]$ συμβολίζει $[\cdot]_{p^r}$):

- $H_1 = \langle [1]^{\frac{p^r}{(1,p^r)}} \rangle = \langle [1]^{\frac{p^r}{1}} \rangle = \langle p^r \cdot [1] \rangle = \langle [p^r] \rangle = \langle [0] \rangle$.
- $H_p = \langle [1]^{\frac{p^r}{(p,p^r)}} \rangle = \langle [1]^{\frac{p^r}{p}=p^{r-1}} \rangle = \langle p^{r-1} \cdot [1] \rangle = \langle [p^{r-1}] \rangle$.
- $H_{p^2} = \langle [1]^{\frac{p^r}{(p^2,p^r)}} \rangle = \langle [1]^{\frac{p^r}{p^2}=p^{r-2}} \rangle = \langle p^{r-2} \cdot [1] \rangle = \langle [p^{r-2}] \rangle$.

$\vdots$

- $H_{p^{r-1}} = \langle [1]^{\frac{p^r}{(p^{r-1},p^r)}} \rangle = \langle [1]^{\frac{p^r}{p^{r-1}}=p} \rangle = \langle p \cdot [1] \rangle = \langle [p] \rangle$.
- $H_{p^r} = \langle [1]^{\frac{p^r}{(p^r,p^r)}} \rangle = \langle [1]^{\frac{p^r}{p^r}=1} \rangle = \langle [1] \rangle = \mathbb{Z}_{p^r}$.

Τότε το διάγραμμα Hasse των υποομάδων της $\mathbb{Z}_{pq}$ είναι το εξής:



■

Άσκηση 17. **1.** Να δειχθεί ότι η ομάδα $(\mathbb{Q}, +)$ των ρητών αριθμών με πράξη την συνήθη πρόσθεση δεν είναι κυκλική ομάδα.

2. Να δειχθεί ότι η ομάδα των πραγματικών αριθμών $(\mathbb{R}, +)$ με πράξη την συνήθη πρόσθεση δεν είναι κυκλική ομάδα.

Λύση. **1.** Έστω ότι η ομάδα $(\mathbb{Q}, +)$ είναι κυκλική. Τότε υπάρχει ρητός $\frac{p}{q} \in \mathbb{Q}$ έτσι ώστε

$$\mathbb{Q} = \langle \frac{p}{q} \rangle$$

Όμως τότε

$$\frac{p}{2q} \in \mathbb{Q} \quad \Longrightarrow \quad \frac{p}{2q} \in \langle \frac{p}{q} \rangle$$

και άρα υπάρχει $n \in \mathbb{Z}$ έτσι ώστε

$$\frac{p}{2q} = n \cdot \frac{p}{q} \implies \frac{p}{2} = np \implies p(\frac{1}{2} - n) = 0 \implies p = 0 \quad \text{ή} \quad n = \frac{1}{2}$$

Σε κάθε περίπτωση όμως έχουμε καταλήξει σε άτοπο διότι $n \in \mathbb{Z}$ και αν $p = 0$ τότε προφανώς $\mathbb{Q} = \{0\}$. Επομένως η ομάδα $(\mathbb{Q}, +)$ δεν είναι κυκλική.

2. Από τη Θεωρία γνωρίζουμε ότι κάθε υποομάδα μιας κυκλικής ομάδας είναι κυκλική. Επειδή $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$, αν η ομάδα $(\mathbb{R}, +)$ είναι κυκλική τότε θα είχαμε ότι και η ομάδα $(\mathbb{Q}, +)$ είναι κυκλική, το οποίο είναι άτοπο από το (1). Επομένως η ομάδα $(\mathbb{R}, +)$ δεν είναι κυκλική. ■

Άσκηση 18. Σημειώστε αν είναι σωστό (Σ) ή λάθος (Λ).

(1) Κάθε κυκλική ομάδα είναι αβελιανή.
(2) Κάθε αβελιανή ομάδα είναι κυκλική
(3) Κάθε στοιχείο μιας κυκλικής ομάδας παράγει την ομάδα.
(4) Για κάθε $n \in \mathbb{N}$, υπάρχει τουλάχιστον μια αβελιανή ομάδα με τάξη n.
(5) Κάθε ομάδα τάξης ≤ 4 είναι κυκλική.

(6) Για κάθε στοιχείο $[a]_{20}$ της $\mathbb{Z}_{20}$ που είναι γεννήτορας, υπάρχει ένα στοιχείο $b \in [a]_{20}$, το οποίο είναι πρώτος αριθμός.
(7) Η S_3 είναι κυκλική ομάδα.
(8) Όλες οι υποομάδες της S_3 είναι κυκλικές.
(9) Κάθε κυκλική ομάδα τάξης > 2 έχει τουλάχιστον δυο διαφορετικούς γεννήτορες.

Λύση. (1) Σ, το γνωρίζουμε από την Θεωρία.
(2) Λ, για παράδειγμα η ομάδα $\mathcal{V}_4$ του Klein είναι αβελιανή αλλά όχι κυκλική.
(3) Λ, για παράδειγμα στην $\mathbb{Z}_4$ έχουμε ότι $\mathbb{Z}_4 = \langle [1] \rangle = \langle [3] \rangle$.
(4) Σ, διότι η $\mathbb{Z}_n$ με $n > 0$ είναι πεπερασμένη αβελιανή τάξης n.
(5) Λ, η ομάδα $\mathcal{V}_4$ του Klein έχει τάξη 4 και δεν είναι κυκλική.
(6) Σ. Οι γεννήτορες της $\mathbb{Z}_{20}$ είναι σε πλήθος $\phi(20) = 8$ και είναι οι εξής:

$$\mathbb{Z}_{20} = \langle [1] \rangle = \langle [3] \rangle = \langle [7] \rangle = \langle [9] \rangle = \langle [11] \rangle = \langle [13] \rangle = \langle [17] \rangle = \langle [19] \rangle$$

Όλοι οι αντιπρόσωποι είναι πρώτοι αριθμοί εκτός από τους $[1]$, $[9]$. Τότε έχουμε ότι $29 \in [9]_{20}$ και $41 \in [1]_{20}$, όπου οι αριθμοί 29 και 41 είναι πρώτοι αριθμοί.
(7) Λ, διότι κανένα από τα στοιχεία της S_3 δεν παράγει ολόκληρη την ομάδα.
(8) Σ, διότι όπως μπορούμε να υπολογίσουμε εύκολα όλες οι υποομάδες της S_3 έχουν τάξη ≤ 3 και άρα είναι κυκλικές.
(9) Σ. Έστω $G = \langle a \rangle$ κυκλική τάξης $n > 2$ και ας υποθέσουμε ότι η G έχει μόνο έναν γεννήτορα, το στοιχείο a. Τότε και το a^{-1} είναι γεννήτορας και $G = \langle a \rangle = \langle a^{-1} \rangle$. Άρα από την υπόθεση που κάναμε έχουμε:

$$a = a^{-1} \implies a^2 = e$$

και άρα $G = \{e, a\}$, δηλαδή η ομάδα G έχει τάξη 2. Αυτό όμως είναι άτοπο από την υπόθεση μας. Άρα κάθε κυκλική ομάδα τάξης > 2 έχει τουλάχιστον δυο διαφορετικούς γεννήτορες. ■

Άσκηση 19. Στις παρακάτω προτάσεις, δώστε παράδειγμα ομάδας με την ιδιότητα που περιγράφεται ή εξηγήστε γιατί δεν υπάρχει τέτοιο παράδειγμα.

(1) Μια πεπερασμένη ομάδα η οποία δεν είναι κυκλική.
(2) Μια άπειρη ομάδα η οποία δεν είναι κυκλική.
(3) Μια κυκλική ομάδα η οποία έχει μόνο έναν γεννήτορα.
(4) Μια άπειρη κυκλική ομάδα η οποία έχει τέσσερις γεννήτορες.
(5) Μια πεπερασμένη κυκλική ομάδα η οποία έχει τέσσερις γεννήτορες.

Λύση. (1) Η ομάδα $\mathcal{V}_4$ του Klein είναι μια πεπερασμένη ομάδα η οποία δεν είναι κυκλική.
(2) Από την Άσκηση 17 έχουμε ότι η προσθετική ομάδα $(\mathbb{Q}, +)$ των ρητών είναι μια άπειρη ομάδα η οποία δεν είναι κυκλική.
(3) Η ομάδα $\mathbb{Z}_2 = \{[0]_2, [1]_2\} = \langle [1]_2 \rangle$ είναι μια κυκλική ομάδα η οποία έχει μόνο έναν γεννήτορα.
(4) Δεν υπάρχει παράδειγμα άπειρης κυκλικής ομάδας με τέσσερις γεννήτορες διότι κάθε άπειρη κυκλική έχει ακριβώς 2 γεννήτορες.
(5) Ψάχνουμε παραδείγματα πεπερασμένων κυκλικών ομάδων που έχουν τέσσερις γεννήτορες. Δηλαδή θέλουμε ομάδες της μορφής $\mathbb{Z}_n$ με $\phi(n) = 4$. Για παράδειγμα:
(α΄) Η ομάδα $\mathbb{Z}_5$ έχει τέσσερις γεννήτορες αφού $\phi(5) = 4$.
(β΄) Η ομάδα $\mathbb{Z}_8$ έχει τέσσερις γεννήτορες αφού $\phi(8) = 4$.
(γ΄) Η ομάδα $\mathbb{Z}_{90}$ έχει τέσσερις γεννήτορες αφού $\phi(90) = 4$.
Όμοια μπορείτε να βρείτε και άλλα παραδείγματα. ■

Άσκηση 20. Δείξτε ότι μια ομάδα η οποία έχει πεπερασμένο πλήθος υποομάδων είναι πεπερασμένη ομάδα.

Λύση. Έστω G μια ομάδα η οποία έχει πεπερασμένο πλήθος υποομάδων. Τότε για κάθε $a \in G$ θεωρούμε την κυκλική υποομάδα $\langle a \rangle$ η οποία παράγεται από το a. Ισχυριζόμαστε ότι η υποομάδα $\langle a \rangle$ είναι πεπερασμένη. Πράγματι αν η $\langle a \rangle$ είναι άπειρη τότε η $\langle a \rangle$ άρα και η G έχουν άπειρο πλήθος υποομάδων, τις

$\langle a^i\rangle$, $\forall i \geq 0$. Αυτό όμως είναι άτοπο από την υπόθεση μας και άρα $\mathsf{o}(\langle a\rangle) < \infty$. Όμως

$$G = \bigcup_{a\in G} \{a\} = \bigcup_{a\in G} \langle a\rangle$$

δηλαδή η G είναι ένωση των κυκλικών υποομάδων της. Από την υπόθεση μας γνωρίζουμε ότι η G έχει πεπερασμένο πλήθος υποομάδων και άρα η G έχει πεπερασμένο πλήθος κυκλικών υποομάδων. Επειδή κάθε κυκλική υποομάδα $\langle a\rangle$ της G είναι πεπερασμένη έπεται από τη παραπάνω σχέση ότι η ομάδα G είναι πεπερασμένη. ■

Άσκηση 21. Για κάθε $a, b, c \in \mathbb{R}$ θεωρούμε το σύνολο

$$H = \big\{D(a,b,c) \in \mathsf{M}_{3\times 3} \mid a,b,c \in \mathbb{R}\big\}, \qquad \text{όπου} \qquad D(a,b,c) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

Να δείξετε ότι το υποσύνολο H είναι μια υποομάδα της ειδικής γραμμικής ομάδας $\mathsf{SL}(3,\mathbb{R})$ και ακολούθως να βρεθούν όλα τα στοιχεία πεπερασμένης τάξης στην H.

Λύση. **1.** Παρατηρούμε ότι το σύνολο H δεν είναι κενό αφού περιέχει τον μοναδιαίο 3×3 πίνακα:

$$D(0,0,0) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I_3 \ \in \ H$$

Επίσης επειδή $\mathsf{Det}D(a,b,c) = 1$, έπεται ότι $H \subseteq \mathsf{SL}(3,\mathbb{R})$.

Θεωρούμε τους πίνακες

$$D(a,b,c) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad \& \quad D(e,f,g) = \begin{pmatrix} 1 & e & f \\ 0 & 1 & g \\ 0 & 0 & 1 \end{pmatrix}$$

στο H. Ο αντίστροφος τού $D(e,f,g)$ είναι ο πίνακας

$$D(e,f,g)^{-1} = \begin{pmatrix} 1 & -e & -f+eg \\ 0 & 1 & -g \\ 0 & 0 & 1 \end{pmatrix} = D(e,-f+eg,-g) \ \in H$$

και το γινόμενο πινάκων $D(a,b,c)\cdot D(e,f,g)^{-1}$ είναι ο πίνακας

$$D(a,b,c)\cdot D(e,f,g)^{-1} = D(a,b,c)\cdot D(e,-f+eg,-g) = \begin{pmatrix} 1 & a-e & b-f-ag+eg \\ 0 & 1 & c-g \\ 0 & 0 & 1 \end{pmatrix} =$$

$$= D(a-e, b-f-ag+eg, c-g) \ \in \ H$$

Επομένως, η H είναι υποομάδα τής $\mathsf{SL}_3(\mathbb{R})$, επειδή $H \neq \emptyset$ και επειδή $D(a,b,c)$, $D(e,f,g) \in H$ δίνει ότι $D(a,b,c)\cdot D(e,f,g)^{-1} = D(a-e, b-f-ag+eg, c-g) \in H$.

2. Τώρα θα δείξουμε με επαγωγή ως προς $n \in \mathbb{N}$ ότι η n-οστή φυσική δύναμη τού $D(a,b,c)$ ισούται με τον πίνακα

$$\textbf{(*)} \qquad D(a,b,c)^n = \begin{pmatrix} 1 & na & nb+\rho(n)ac \\ 0 & 1 & nc \\ 0 & 0 & 1 \end{pmatrix}$$

όπου ο συντελεστής $\rho(n)$ τού ac είναι μια συνάρτηση του n η οποία ικανοποιεί τον αναδρομικό τύπο $\rho(1) = 0$ και για $n \geq 2$, $\rho(n) = \rho(n-1) + n - 1$.

Ο ισχυρισμός είναι αληθής για $k = 1$, αφού $D(a,b,c) = \begin{pmatrix} 1 & 1a & 1b+0ac \\ 0 & 1 & 1c \\ 0 & 0 & 1 \end{pmatrix}$.

Έστω ότι είναι αληθής για $k=n$ θα τον δείξουμε για $k=n+1$. Αφού είναι αληθής για $k=n$ έχουμε:

$$D(a,b,c)^n=\begin{pmatrix}1 & na & nb+\rho(n)ac\\ 0 & 1 & nc\\ 0 & 0 & 1\end{pmatrix},\qquad \rho(n)=\rho(n-1)+n-1$$

Τώρα είναι

$$D(a,b,c)^{n+1}=D(a,b,c)^n\cdot D(a,b,c)=\begin{pmatrix}1 & na & nb+\rho(n)ac\\ 0 & 1 & nc\\ 0 & 0 & 1\end{pmatrix}\cdot\begin{pmatrix}1 & a & b\\ 0 & 1 & c\\ 0 & 0 & 1\end{pmatrix}=$$

$$=\begin{pmatrix}1 & a+na & b+nac+nb\rho(n)ac\\ 0 & 1 & c+nc\\ 0 & 0 & 1\end{pmatrix}=\begin{pmatrix}1 & (n+1)a & (n+1)b+(\rho(n)+n)ac\\ 0 & 1 & (n+1)c\\ 0 & 0 & 1\end{pmatrix}$$

όπου τώρα ο συντελεστής $\rho(n+1)$ τού ac τής $(n+1)$ δύναμης τού $D(a,b,c)$ ισούται με $\rho(n)+n$.

3. Αν λοιπόν κάποιο $D(a,b,c)$ είναι πεπερασμένης τάξης, τότε υπάρχει φυσικός n με $D(a,b,c)^n$ ίσο με το ταυτοτικό στοιχείο τής H, δηλαδή ίσο με τον μοναδιαίο 3×3 πίνακα $D(0,0,0)=I_n$. Όμως από τον τύπο για την n-οστή δύναμη τού $D(a,b,c)$ διαπιστώνουμε ότι για να είναι ο $D(a,b,c)^n$ ίσος με τον $D(0,0,0)$, πρέπει $na=0$ και $nc=0$, δηλαδή $a=c=0$. Επίσης πρέπει το στοιχείο τής συνιστώσας $(1,3)$ τού $D(a,b,c)^n$, δηλαδή το $nb+\rho(n)ac$ να ισούται με μηδέν. Αλλά $a=c=0$ και γι' αυτό από $nb+\rho(n)ac=nb=0$, έπεται ότι $b=0$. Ώστε, $D(a,b,c)=D(0,0,0)=I_n$. Συνοψίζουμε: το μοναδικό στοιχείο της H το οποίο έχει πεπερασμένη τάξη είναι το ουδέτερο. ■