ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΪΚΑ ΜΑΘΗΜΑΤΑ

Τίτλος Μαθήματος: Αλγεβρικές Δομές Ι

Ενότητα: Τάξη στοιχείων και Ομάδων - Κυκλικές (Υπο-)Ομάδες

Διδάσκων: Καθηγητής Νικόλαος Μαρμαρίδης, Καθηγητής Ιωάννης Μπεληγιάννης

Τμήμα: Μαθηματικών

3. **Τάξη στοιχείων και Ομάδων - Κυκλικές (Υπο-)Ομάδες**

3.1. **Δύναμη Στοιχείου.**

Έστω ότι $(G,\star)$ είναι μια ομάδα. Για κάθε ακέραιο αριθμό $m \in \mathbb{Z}$ και κάθε στοιχείο $a \in G$, ορίζουμε την m–**οστή δύναμη** τού στοιχείου a ως ακολούθως:

$$a^m = \begin{cases} \underbrace{a \star a \star \cdots \star a}_{m-\text{φορές}}, & \text{αν} \quad m \in \mathbb{N}, \\ e_G, & \text{αν} \quad m = 0, \\ \underbrace{a^{-1} \star a^{-1} \star \cdots \star a^{-1}}_{|m|-\text{φορές}}, & \text{αν} \quad -m \in \mathbb{N}. \end{cases}$$

Στην περίπτωση που η $(G,\star)$ είναι μια μεταθετική (αβελιανή) ομάδα και χρησιμοποιούμε την προσθετική σημειογραφία αντί τής γενικής πολλαπλασιαστικής, δηλαδή παριστάνουμε την πράξη με «$+$» αντί «$\star$», παριστάνουμε το ουδέτερο τής ομάδας με 0_G αντί e_G και για κάθε $a \in G$, παριστάνουμε με $-a$ αντί a^{-1} το αντίθετο (αντίστροφο) τού a, τότε ορίζουμε:

$$ma = \begin{cases} \underbrace{a + a + \cdots + a}_{m-\text{φορές}}, & \text{αν} \quad m \in \mathbb{N}, \\ 0_G, & \text{αν} \quad m = 0, \\ \underbrace{(-a) + (-a) + \cdots + (-a)}_{|m|-\text{φορές}}, & \text{αν} \quad -m \in \mathbb{N}. \end{cases}$$

Στην περίπτωση αυτή ονομάζουμε το στοιχείο ma το (ακέραιο) m–**πολλαπλάσιο** τού a. Για τις δυνάμεις και αντιστοίχως τα πολλαπλάσια στοιχείων μιας ομάδας ισχύουν κανόνες ανάλογοι των κανόνων που ισχύουν για τις ακέραιες δυνάμεις και τα ακέραια πολλαπλάσια των γνωστών μας αριθμών.

Λήμμα 3.1. *Έστω ότι $(G,\star)$ είναι μια ομάδα ότι a είναι ένα στοιχείο τού G και ότι m,n είναι δύο ακέραιοι αριθμοί. Τότε*

$$a^m \star a^n = a^{m+n}, \tag{α'}$$

όπου $m+n$ παριστά τη συνήθη πρόσθεση των ακεραίων m,n και

$$(a^m)^n = a^{mn}, \tag{β'}$$

όπου mn παριστά τον συνήθη πολλαπλασιασμό των ακεραίων m,n.

Απόδειξη. Εδώ θα εκτελέσουμε την απόδειξη για την ταυτότητα (α') και προτείνουμε ως άσκηση την απόδειξη τής (β').

- Περίπτωση I. Αν $n = 0, m \in \mathbb{Z}$, τότε $a^m \star a^0 = a^m \star e_G = a^m = a^{m+0}$.

- Περίπτωση II. Αν $n \in \mathbb{N}, m \in \mathbb{Z}$, εφαρμόζουμε τη μέθοδο τής πλήρους επαγωγής ως προς n.

Για $n = 1$, η (α') είναι αληθής, αφού

$$\begin{cases} a^m \star a^1 = \underbrace{(a \star a \star \cdots \star a)}_{m-\text{φορές}} \star a = a^{m+1}, & \text{αν} \quad m \in \mathbb{N}, \\ \\ a^m \star a^1 = a^0 \star a = e_G \star a = a^1 = a^{m+1}, & \text{αν} \quad m = 0, \\ \\ a^m \star a^1 = a^{-1} \star a^1 = e_G = a^0 = a^{(-1)+1} = a^{m+1}, & \text{αν} \quad m = -1, \\ \\ a^m \star a^1 = \underbrace{a^{-1} \star a^{-1} \star \cdots \star a^{-1}}_{|m|-\text{φορές}} \star a = \underbrace{a^{-1} \star a^{-1} \star \cdots \star a^{-1}}_{(|m|-1)-\text{φορές}} = a^{m+1}, & \text{αν} \quad m \leq -2. \end{cases}$$

(Προσέξτε ότι στην τελευταία σχέση χρησιμοποιούμε το εξής: Επειδή $m \leq -2$, έπεται $m+1 \leq -1$ και γι' αυτό $|m+1| = -(m+1) = -m-1 = |m|-1$.)
Υποθέτοντας ότι η (α') είναι αληθής για $n = k$ (επαγωγική υπόθεση), δηλαδή ότι $a^m \star a^k = a^{m+k}$, θα αποδείξουμε την αλήθειά της, για $n = k+1$.
Έχουμε $a^m \star a^{k+1} = a^m \star (a^k \star a)$, αφού αυτό το αποδείξαμε μόλις προηγουμένως. Τώρα λόγω τής προσεταιριστικότητας τής «$\star$» έχουμε $a^m \star (a^k \star a) = (a^m \star a^k) \star a$ και λόγω τής επαγωγικής υπόθεσης έχουμε $(a^m \star a^k) \star a = a^{m+k} \star a$. Τέλος, $a^{m+k} \star a = a^{(m+k)+1}$. Ώστε, $a^m \star a^{k+1} = a^{m+(k+1)}$.

Επομένως, η (α') είναι αληθής για κάθε $n \in \mathbb{N}$ και $m \in \mathbb{Z}$.

- Περίπτωση III. Έστω τώρα ότι $n \in \mathbb{Z}, n < 0$ και $m \in \mathbb{Z}$.

Θα δείξουμε και πάλι τη σχέση (α'), δηλαδή ότι $a^m \star a^n = a^{m+n}$. Όμως για να είναι η προηγούμενη σχέση είναι αληθής, αρκεί να είναι αληθής η σχέση $(a^m \star a^n) \star a^{-n} = a^{m+n} \star a^{-n}$.

Για το αριστερό μέλος τής υποψήφιας ισότητας έχουμε:

$$(a^m \star a^n) \star a^{-n} = a^m \star (a^n \star a^{-n}) = a^m \star (a^{n+(-n)}),$$

όπου η τελευταία ισότητα ισχύει, λαμβάνοντας υπ' όψιν την Περίπτωση II, αφού $(-n) \in \mathbb{N}$. Έτσι προκύπτει

$$(a^m \star a^n) \star a^{-n} = a^m \star (a^{n+(-n)}) = a^m \star a^0 = a^m.$$

Για το δεξιό μέλος τής υποψήφιας ισότητας έχουμε:

$$a^{m+n} \star a^{-n} = a^{m+n+(-n)} = a^m$$

και πάλι λόγω τής Περίπτωσης II, αφού $(-n) \in \mathbb{N}$. Ώστε τελικά,

$$(a^m \star a^n) \star a^{-n} = a^m = a^{m+n} \star a^{-n}$$

και συνεπώς $a^m \star a^n = a^{m+n}$. □

Παρατήρηση 3.2. (1) *Στην περίπτωση τής προσθετικής σημειογραφίας η πρώτη ταυτότητα τού Λήμματος 3.1 εκφράζεται ως*

$$(mg) + (ng) = (m+n)g. \tag{α'}$$

Προσέξτε ότι το «+» στο αριστερό μέλος τής ταυτότητας είναι η πράξη τής ομάδας ενώ το «+» στο δεξιό μέλος τής ταυτότητας είναι η πράξη τής πρόσθεσης των ακέραιων αριθμών.

Η δεύτερη ταυτότητα τού Λήμματος 3.1 εκφράζεται ως

$$m(ng) = (mn)g. \tag{β'}$$

Προσέξτε ότι το mn που εμφανίζεται στο δεξιό μέλος τής ως άνω ταυτότητας είναι το γινόμενο τού ακεραίου m επί τον ακέραιο n.

(2) *Λόγω τού Λήμματος 3.1 έχουμε ότι το αντίστροφο μιας δύναμης $a^m, m \in \mathbb{Z}$ ενός στοιχείου $a \in G$ είναι το στοιχείο a^{-m}, αφού*
$$a^m \star a^{-m} = a^{m+(-m)} = a^0 = e_G = a^{(-m)+m} = a^{-m} \star a^m.$$
(3) *Αν η $(G, +)$ είναι αβελιανή, τότε χρησιμοποιώντας προσθετική σημειογραφία έχουμε $-(ma) = (-m)a$.*
Προσέξτε ότι το στοιχείο $-(ma)$ είναι το αντίθετο τού ma και ότι το $(-m)a$ είναι το $(-m)$-πολλαπλάσιο τού a.

3.2. **Κυκλικές Ομάδες.**

Με τη βοήθεια του Λήμματος 2.5 αποδεικνύουμε την εξής πολύ σημαντική

Πρόταση 3.3. *Αν $(G, \star)$ είναι μια ομάδα και αν a είναι ένα στοιχείο της G, τότε το σύνολο*
$$\langle a \rangle := \{a^z \mid z \in \mathbb{Z}\}$$
αποτελεί μια υποομάδα τής G. Επιπλέον η $\langle a \rangle$ είναι η μικρότερη υποομάδα της G η οποία περιέχει το στοιχείο a.

Απόδειξη. Το σύνολο $\langle a \rangle$ είναι διάφορο του κενού, αφού το $a = a^1$ ανήκει στο $\langle a \rangle$.

Αν $x, y \in \langle a \rangle$, τότε υπάρχουν $z_1, z_2 \in \mathbb{Z}$ με $x = a^{z_1}$ και $y = a^{z_2}$. Συνεπώς το στοιχείο
$$x \star y^{-1} = a^{z_1} \star (a^{z_2})^{-1} = a^{z_1} \star a^{-z_2} = a^{z_1 - z_2}$$
ανήκει επίσης στο σύνολο $\langle a \rangle$, αφού ο $z_1 - z_2$ είναι και αυτός ακέραιος αριθμός. Άρα $\langle a \rangle$ είναι μια υποομάδα της G η οποία περιέχει το στοιχείο a.

Τέλος αν H είναι μια υποομάδα της G και $a \in H$, τότε με διαδοχική εφαρμογή του Λήμματος 2.3 έπεται ότι η H περιέχει όλα τα στοιχεία της μορφής a^z, $z \in \mathbb{Z}$. Επομένως $\langle a \rangle \subseteq H$. $\square$

Παρατήρηση 3.4. *Στην περίπτωση που η ομάδα $(G, \star)$ είναι αβελιανή και αντί της γενικής σημειογραφίας χρησιμοποιείται η προσθετική σημειογραφία $(G, +)$, τότε συμβολίζουμε με $\langle a \rangle$, $a \in G$, το σύνολο*
$$\langle a \rangle = \{za \mid z \in \mathbb{Z}\}$$

Ορισμός 3.5. *Η υποομάδα $\langle a \rangle$ της G ονομάζεται η* ***κυκλική υποομάδα*** *τής G που παράγεται από το στοιχείο a και το στοιχείο a ονομάζεται ένας* ***γεννήτορας*** *της $\langle a \rangle$.*

Ορισμός 3.6. *Η ομάδα $(G, \star)$ ονομάζεται* ***κυκλική****, αν υπάρχει κάποιο $a \in G$ με $G = \langle a \rangle$. Το στοιχείο a ονομάζεται ένας* ***γεννήτορας*** *της G.*

Παράδειγμα 3.7. (1) *Η ομάδα $(\mathbb{Z}, +)$ των ακεραίων αριθμών είναι κυκλική με γεννήτορα τον ακέραιο 1, αφού*
$$\mathbb{Z} = \{z \cdot 1 \mid z \in \mathbb{Z}\} = \langle 1 \rangle .$$
Το -1 είναι επίσης ένας γεννήτορας τής $\mathbb{Z}$, αφού για κάθε $z \in \mathbb{Z}$, έχουμε $z = (-z)(-1)$.

(2) *Η ομάδα $(\mathbb{Z}_4, +)$ των ακεραίων αριθμών κατά μόδιο 4, είναι κυκλική με γεννήτορα την κλάση $[1]$, αφού*
$$1[1] = 1, \;\; 2[1] = [2], \;\; 3[1] = [3], \;\; 4[1] = [0].$$
Επομένως,
$$\mathbb{Z}_4 = \langle [1] \rangle .$$

(3) *Γενικότερα, αν n είναι ένας πάγιος φυσικός αριθμός, τότε η ομάδα $(\mathbb{Z}_n, +)$ των ακεραίων αριθμών κατά μόδιο n είναι κυκλική με γεννήτορα την κλάση $[1]$, αφού*

$$1[1] = 1, 2[1] = [2], \ldots, i[1] = [i], \ldots (n-1)[1] = [n-1], n[1] = [0].$$

Υπενθυμίζουμε ότι $i[1]$ με $i = 1, 2, \ldots, n$, σημαίνει $[1] + [1] + \cdots + [1]$, i-φορές.

(4) *΄Οπως είδαμε η αβελιανή ομάδα $(\mathbb{Z}_4, +)$ έχει τέσσερα στοιχεία και είναι κυκλική. Ωστόσο, υπάρχει μια αβελιανή ομάδα που έχει επίσης τέσσερα στοιχεία, αλλά δεν είναι κυκλική.*
Πράγματι, θεωρούμε το σύνολο $\mathcal{V}_4 = \{e, a, b, c\}$ και την πράξη $\star : \mathcal{V}_4 \times \mathcal{V}_4 \to \mathcal{V}_4$, η οποία ορίζεται από τον πίνακα:

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Αφήνουμε στον αναγνώστη τον έλεγχο ότι η «$\star$» είναι μια προσεταιριστική πράξη και κατόπιν ότι το ζεύγος $(\mathcal{V}_4, \star)$ είναι μια αβελιανή ομάδα. Ωστόσο η $\mathcal{V}_4$ δεν είναι κυκλική, επειδή

$$\langle e \rangle = \{e\}, \quad \langle a \rangle = \{e, a\}, \quad \langle b \rangle = \{e, b\}, \quad \langle c \rangle = \{e, c\}.$$

Προσέξτε ότι $a^2 = b^2 = c^2 = e$ και γι΄ αυτό οποιαδήποτε ακέραια δύναμη του a (αντίστοιχα του b ή c) είναι ή το e ή το a (αντίστοιχα ή το e ή το b ή το c).

Η συγκεκριμένη ομάδα ονομάζεται η ομάδα των τεσσάρων στοιχείων του Klein.

Οι επόμενες δύο παρατηρήσεις είναι απλές συνέπειες των ορισμών.

Παρατήρηση 3.8. (1) *Κάθε κυκλική ομάδα $(G, \star)$ είναι αβελιανή.*

Πράγματι, αν a είναι ένας γεννήτορας τής G, τότε $G = \langle a \rangle$. Ας είναι x_1, x_2 δύο στοιχεία τού G, τότε υπάρχουν ακέραιοι m_1, m_2 με $x_1 = a^{m_1}$ και $x_2 = a^{m_2}$ και έχουμε:

$$x_1 \star x_2 = a^{m_1} \star a^{m_2} = a^{m_1+m_2} = a^{m_2+m_1} = a^{m_2} \star a^{m_1} = x_2 \star x_1.$$

Ωστόσο, κάθε αβελιανή ομάδα δεν είναι κυκλική. Για παράδειγμα, όπως είδαμε προηγουμένως η ομάδα τού Klein είναι αβελιανή αλλά δεν είναι κυκλική.

(2) *Αν $(G, \star)$ είναι μια κυκλική ομάδα με γεννήτορα κάποιο στοιχείο $a \in G$, δηλαδή $G = \langle a \rangle$, τότε και το στοιχείο a^{-1} είναι επίσης γεννήτορας τής G:*

$$G = \langle a \rangle \qquad \Longleftrightarrow \qquad G = \langle a^{-1} \rangle$$

Πράγματι, για κάθε $x \in G$ υπάρχει κάποιος ακέραιος m με $x = a^m$ και γι΄ αυτό έχουμε επίσης $x = (a^{-1})^{-m}$. Επομένως $G = \left\langle a^{-1} \right\rangle$ και ο a^{-1} είναι επίσης γεννήτορας τής $(G, \star)$.

3.3. **Τάξη στοιχείου.** Έστω $(G, \star)$ μια ομάδα και $a \in G$. Θεωρούμε την κυκλική υποομάδα

$$\langle a \rangle := \left\{ a^m \in G \mid m \in \mathbb{Z} \right\}$$

της G, που παράγεται από το στοιχείο $a \in G$.

Ορισμός 3.9. **Τάξη** *τού στοιχείου $a \in G$ καλείται η τάξη $\mathsf{o}(\langle a \rangle)$ της κυκλικής υποομάδας $\langle a \rangle$ της G η οποία παράγεται από το a και συμβολίζεται με $\mathsf{o}(a)$:*

$$\mathsf{o}(a) = \mathsf{o}(\langle a \rangle)$$

Συνεπώς, η τάξη τού $a \in G$ μπορεί να είναι ή άπειρη ή κάποιος φυσικός $n \in \mathbb{N}$, ανάλογα με το αν η τάξη τής $\langle a \rangle$ είναι άπειρη ή $n \in \mathbb{N}$. Γι' αυτό παριστάνοντας την τάξη τού $a \in G$ με $\mathsf{o}(a)$ έχουμε:

$$\mathsf{o}(a) := \begin{cases} \infty, & \text{αν} \quad \mathsf{o}(\langle a \rangle) = \infty, \\ n \in \mathbb{N}, & \text{αν} \quad \mathsf{o}(\langle a \rangle) = n. \end{cases}$$

Πρόταση 3.10. *Έστω $(G, \star)$ μια ομάδα και a ένα στοιχείο της.*

(α') *Η τάξη $\mathsf{o}(a)$ τού στοιχείου a είναι πεπερασμένη, αν και μόνο αν, υπάρχουν ακέραιοι αριθμοί i, j με $i \neq j$ και $a^i = a^j$.*

(β') *Αν η τάξη $\mathsf{o}(a)$ τού a είναι πεπερασμένη, τότε:*

(i) *το υποσύνολο $M = \{m \in \mathbb{N} \mid a^m = e_G\}$ τού $\mathbb{N}$ είναι διάφορο τού κενού συνόλου,*

(ii) *η κυκλική υποομάδα $\langle a \rangle$ ισούται με $\{a^1, a^2, \ldots, a^n\}$, όπου $n = \min M$ είναι το ελάχιστο στοιχείο τού M και η τάξη $\mathsf{o}(a)$ τού a ισούται με $n = \min M$.*

(iii) *επιπλέον, $a^z = e_G$ για κάποιο $z \in \mathbb{Z}$, αν και μόνο αν, ο αριθμός $z \in \mathbb{Z}$ είναι πολλαπλάσιο τής τάξης $\mathsf{o}(a)$.*

Απόδειξη. • (α') Θεωρούμε την κυκλική υποομάδα $\langle a \rangle = \{a^z \mid z \in \mathbb{Z}\}$ και την απεικόνιση

$$\phi : \mathbb{Z} \longrightarrow \langle a \rangle, \qquad i \longmapsto \phi(i) := a^i,$$

η οποία είναι προφανώς «Επί».

«$\Longrightarrow$» Αν $\forall i, j \in \mathbb{Z}$ με $i \neq j$ είναι $a^i \neq a^j$, τότε η ϕ είναι «1-1» απεικόνιση, αφού από $a^i = \phi(i) = \phi(j) = a^j$, έπεται $i = j$. Συνεπώς, η ϕ είναι «1-1» και «Επί» και το $\mathbb{Z}$ είναι ισοπληθές τού $\langle a \rangle$. Πράγμα άτοπο, αφού τότε η τάξη τής $\langle a \rangle$ δεν είναι πεπερασμένη.

«$\Longleftarrow$» Έστω ότι:

$$\exists\, i, j \in \mathbb{Z}, \ \text{ όπου } \ i \neq j, \quad \text{ και: } \quad a^i = a^j \tag{$*$}$$

Χωρίς περιορισμό τής γενικότητος μπορούμε να υποθέσουμε ότι $j > i$ και ως εκ τούτου να δεχθούμε ότι η διαφορά $j - i > 0$ είναι κάποιος φυσικός αριθμός, ας πούμε ότι $j - i = m \in \mathbb{N}$. Έτσι από την (*) λαμβάνουμε $a^{j-i} = e_G$, δηλαδή

$$a^m = e_G \tag{$**$}$$

Θα αποδείξουμε τώρα ότι κάθε στοιχείο τής $\langle a \rangle$ συμπίπτει με κάποιο από τα στοιχεία $a^0, a^1, a^2, \ldots, a^{m-1}$, το πλήθος[22] των οποίων είναι το πολύ m και συνεπώς η τάξη τής $\langle a \rangle$ είναι πεπερασμένη.

Πράγματι, ας είναι $a^z, z \in \mathbb{Z}$ ένα στοιχείο τής $\langle a \rangle$. Εκτελώντας την διαίρεση με υπόλοιπο τού z δια τού m παίρνουμε $z = \lambda m + \upsilon$, όπου $\lambda \in \mathbb{Z}$ και $0 \leq \upsilon \leq m - 1$. Συνεπώς,

$$a^z = a^{\lambda m + \upsilon} = (a^m)^\lambda \star a^\upsilon = (e_G)^\lambda \star a^\upsilon = a^\upsilon,$$

όπου $0 \leq \upsilon \leq m - 1$.

• (β')(i) Σύμφωνα με το (α') υπάρχουν ακέραιοι i, j, όπου $i \neq j$ με $a^i = a^j$, αφού η $\circ(a)$ είναι πεπερασμένη. Έτσι συμπεραίνουμε, όπως προηγουμένως, ότι υπάρχουν φυσικοί $m \in \mathbb{N}$ με $a^m = e_G$. Συνεπώς, το υποσύνολο $M = \{m \in \mathbb{N} \mid a^m = e_G\}$ είναι ένα μη κενό υποσύνολο τού $\mathbb{N}$.

(β')(ii) Το M διαθέτει ένα ελάχιστο στοιχείο $n = \min M$, αφού πρόκειται για ένα μη κενό υποσύνολο τού $\mathbb{N}$. Ισχυριζόμαστε ότι τα στοιχεία $a^1, a^2, \ldots, a^{n-1}, a^n = e_G$ είναι όλα ανά δύο διαφορετικά μέταξύ τους. Πράγματι, αν $a^i = a^j$ με $1 \leq i, j \leq n$ και $i \neq j$, τότε υποθέτοντας χωρίς περιορισμό τής γενικότητας ότι $j > i$, παίρνουμε $a^{j-i} = e_G$, όπου $n > j - i > 0$. Αλλά τότε ο φυσικός $j - i$ αφενός

[22] Δεν ισχυριζόμαστε ότι οι δυνάμεις $a^0, a^1, a^2, \ldots, a^{m-1}$ είναι ανά δύο διαφορετικές. Για την απόδειξη μάς αρκεί να είναι πεπερασμένες το πλήθος.

ανήκει στο M και αφετέρου είναι μικρότερος απο το ελάχιστο στοιχείο n τού M, πράγμα άτοπο. Ώστε τα $a^1, a^2, \ldots, a^{n-1}, a^n = e_G$ είναι διαφορετικά και απαρτίζουν ένα σύνολο με πλήθος στοιχείων ίσο με n.

Θα δείξουμε ότι $\langle a \rangle = \{a^1, a^2, \ldots, a^{n-1}, a^n = e_G\}$.

Προφανώς, $\{a^1, a^2, \ldots, a^{n-1}, a^n = e_G\} \subseteq \langle a \rangle$. Ας είναι $a^z, z \in \mathbb{Z}$ ένα στοιχείο τής $\langle a \rangle$. Εκτελώντας διαίρεση με υπόλοιπο τού z δια τού n παίρνουμε $z = n\lambda + \rho$, όπου $\lambda \in \mathbb{Z}$ και $0 \leq \rho \leq n-1$. Έχουμε:

$$a^z = a^{n\lambda+\rho} = (a^n)^\lambda \star a^\rho = e_G^\lambda \star a^\rho = a^\rho.$$

Αν $0 < \rho \leq n-1$, τότε το a^z ανήκει στο $\{a^1, a^2, \ldots, a^{n-1}, a^n = e_G\}$ και, αν $\rho = 0$, τότε $a^z = a^0 = e_G = a^n$ που είναι επίσης στοιχείο τού $\{a^1, a^2, \ldots, a^{n-1}, a^n = e_G\}$. Ώστε,

$$\langle a \rangle = \{a^1, a^2, \ldots, a^{n-1}, a^n = e_G\} \quad \text{και} \quad \min M = n = \mathsf{o}(\langle a \rangle) = \mathsf{o}(a).$$

(β')(iii) «$\Longrightarrow$» Ας υποθέσουμε ότι για κάποιο $z \in \mathbb{Z}$ είναι $a^z = e_G$. Εκτελώντας τη διαίρεση με υπόλοιπο τού z δια τού $\circ(a)$, παίρνουμε:

$$z = \circ(a)\lambda + \upsilon, \quad \text{όπου} \quad \lambda \in \mathbb{Z} \quad \text{και} \quad 0 \leq \upsilon \leq \circ(a) - 1 \tag{***}$$

Συνεπώς,

$$e_G = a^z = a^{\lambda z+\upsilon} = (a^z)^\lambda \star a^\upsilon = (e_G)^\lambda \star a^\upsilon = a^\upsilon,$$

Αν για το υπόλοιπο υ τής προηγούμενης διαίρεσης είχαμε $\upsilon \neq 0$, τότε η ισότητα $e_G = a^\upsilon$, δίνει το άτοπο, να ανήκει ο υ στο σύνολο $M = \{m \in \mathbb{N} \mid a^m = e_G\}$ και να είναι συγχρόνως μικρότερος από το $\min M = \mathsf{o}(a)$. Γι'αυτό από την (***) έπεται $z = \mathsf{o}(a)\lambda$ και η τάξη $\mathsf{o}(a)$ είναι διαιρέτης τού z.

«$\Longleftarrow$» Αν $z = \mathsf{o}(a)\lambda$ με $\lambda \in \mathbb{Z}$, τότε

$$a^z = a^{\mathsf{o}(a)\lambda} = (a^{\mathsf{o}(a)})^\lambda = e_G^\lambda = e_G$$

□

Το ακόλουθο Θεώρημα συνοψίζει τα κυριότερα αποτελέσματα γύρω από την τάξη ενός στοιχείου μιας ομάδας.

Θεώρημα 3.11. *Έστω $(G, \star)$ μια ομάδα και $g \in G$ ένα στοιχείο πεπερασμένης τάξης: $\mathsf{o}(g) = n$. Τότε $\forall k \in \mathbb{Z}$:*

(**1**)

$$\mathsf{o}(g^k) = \frac{n}{(n,k)}$$

(**2**)

$$k/n \quad \Longleftrightarrow \quad \mathsf{o}(g^k) = \frac{n}{|k|}$$

(**3**)

$$(k,n) = 1 \quad \Longleftrightarrow \quad \mathsf{o}(g^k) = n$$

Απόδειξη. (**1**) Προφανώς το g^k έχει πεπερασμένη τάξη. Έστω $r = \mathsf{o}(g^k)$. Θα δείξουμε ότι $r = \frac{n}{(n,k)}$. Θα έχουμε:

$$(g^k)^r = e \implies g^{kr} = e \implies n/kr$$

όπου η τελευταία συνεπαγωγή προέκυψε από την Πρόταση 3.10(β')(iii). Επομένως υπάρχει $m \in \mathbb{Z}$ έτσι ώστε:

$$kr = nm$$

Μπορούμε να γράψουμε:

$$n = (n,k)n' \quad \text{και} \quad k = (n,k)k', \quad \text{και} \quad (k', n') = 1$$

Τότε: $n' = \frac{n}{(n,k)}$ και άρα αρκεί να δείξουμε ότι: $r = n'$. Θα έχουμε:

$$kr = nm \implies (n,k)k'r = (n,k)n'm \implies k'r = n'm \implies n'/k'r \implies n'/r \implies n' \leq r$$

όπου η προτελευταία συνεπαγωγή προέκυψε διότι $(k', n') = 1$.

Από την άλλη πλευρά, παρατηρώντας ότι:

$$kn' = (n,k)k'n' = nk'$$

θα έχουμε:

$$(g^k)^{n'} = g^{kn'} = g^{nk'} = (g^n)^{k'} = e^{k'} = e \implies r/n' \implies r \leq n'$$

Επομένως: $\mathsf{o}(g^k) = r = n' = \frac{n}{(k,n)}$.

(2), **(3)** Προκύπτουν άμεσα από το **(1)**. $\square$

3.4. **Τάξη Γινομένου Στοιχείων μιας Ομάδας.** Αν x, y είναι δύο στοιχεία πεπερασμένης τάξης μιας ομάδας, τότε πώς σχετίζονται οι τάξεις των στοιχείων x, y, xy;

Γενικά δεν υπάρχει κάποια σχέση μεταξύ των τάξεων $\mathsf{o}(x), \mathsf{o}(y), \mathsf{o}(xy)$:

Παράδειγμα 3.12. *Στην συμμετρική ομάδα S_4 θεωρούμε τους 3-κύκλους:*

$$\sigma = (123) \qquad \textit{και} \qquad \tau = (241)$$

Τότε

$$\mathsf{o}(\sigma) = 3 = \mathsf{o}(\tau) \qquad \textit{αλλά} \qquad \mathsf{o}(\sigma \circ \tau) = \mathsf{o}((13) \circ (24)) = 2$$

Παρατηρούμε ότι: $\sigma \circ \tau = (13)(24) \neq (14)(23) = \tau \circ \sigma$.

Παράδειγμα 3.13. *Στην συμμετρική ομάδα S_5 θεωρούμε τους κύκλους:*

$$\sigma = (123) \qquad \textit{και} \qquad \tau = (15342)$$

Τότε

$$\mathsf{o}(\sigma) = 3, \qquad \mathsf{o}(\tau) = 5 \qquad \textit{αλλά} \qquad \mathsf{o}(\sigma \circ \tau) = \mathsf{o}((15) \circ (34)) = 2$$

Παρατηρούμε ότι: $\sigma \circ \tau = (15)(34) \neq (34)(35) = \tau \circ \sigma$.

Παράδειγμα 3.14. *Θεωρούμε την (άπειρη μη-αβελιανή) ομάδα*

$$\mathsf{GL}_2(\mathbb{R}) = \big\{A \in \mathsf{M}_{2\times 2}(\mathbb{R}) \mid \mathsf{det}(A) \neq 0\big\}$$

και έστω

$$A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

Τότε προφανώς $A, B, AB \in \mathsf{GL}_2(\mathbb{R})$. Παρατηρούμε ότι:

$$A^2 = I_2 = B^2$$

Επομένως τα στοιχεία A, B έχουν τάξη 2. Όμως

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \qquad \textit{και} \qquad BA = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = (AB)^{-1}$$

και άρα $\forall n \geq 1$:

$$(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \qquad \textit{και} \qquad (BA)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix},$$

Επομένως τα στοιχεία A, B έχουν τάξη 2 αλλά το γινόμενό τους AB και BA έχει άπειρη τάξη.

Παρατηρούμε ότι: $AB \neq BA$.

Παράδειγμα 3.15. *Για κάθε $n \geq 3$, υπάρχει μια πεπερασμένη αβελιανή ομάδα G η οποία περιέχει δύο στοιχεία τάξης 2 των οποίων το γινόμενο έχει τάξη n:*

Πράγματι θεωρούμε την ομάδα

$$\mathsf{GL}_2(\mathbb{Z}_n) = \big\{A \in \mathsf{M}_{2\times 2}(\mathbb{Z}_n) \mid \mathsf{det}(A) \neq 0\big\}$$

των αντιστρεψίμων πινάκων με στοιχεία από το $\mathbb{Z}_n$. Οι πίνακες

$$A = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

όπως στο παράδειγμα 3.12 έχουν τάξη 2 και ο πίνακας

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

έχει τάξη n διότι $\forall n \geq 1$:

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

ως πίνακες με στοιχεία από το $\mathbb{Z}_n$. Επομένως τα στοιχεία A, B έχουν τάξη 2 αλλά το γινόμενό τους AB έχει τάξη n.

Παρατηρούμε ότι: $AB \neq BA$ διότι $BA = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$ και $-1 \neq 1$ στο $\mathbb{Z}_n$ διότι $n \geq 3$.

Σε όλα τα παραπάνω παραδείγματα τα στοιχεία της ομάδας δεν μετατίθενται και για στοιχεία x, y πεπερασμένης τάξης, δεν μπορουμε να πούμε τίποτα για την τάξη του $x \star y$ η οποία μπορεί να είναι άπειρη ή οποιοσδήποτε αριθμός.

Όταν όμως σε μια ομάδα G έχουμε δύο στοιχεία x, y πεπερασμένης τάξης και $x \star y = y \star x$, τότε υπάρχει στενή σχέση μεταξύ των τάξεων $\mathsf{o}(x), \mathsf{o}(y), \mathsf{o}(xy)$:

Πρόταση 3.16. *Έστω $(G, \star)$ μια ομάδα και $g, h \in G$ δύο στοιχεία πεπερασμένης τάξης: $\mathsf{o}(g) = m$ και $\mathsf{o}(h) = n$. Τότε:*

$$(m, n) = 1 \qquad \Longrightarrow \qquad \mathsf{o}(g \star h) = mn$$

Απόδειξη. Βλέπε την απόδειξη του Λήμματος 4.3 παρακάτω. □

Όταν δύο a, b στοιχεία πεπερασμένης τάξης μιας ομάδας δεν μετατίθενται, τότε η επόμενη Πρόταση δείχνει ότι τα στοιχεία ab και ba έχουν την ίδια τάξη:

Πρόταση 3.17. *Έστω G μια ομάδα κα $a, b \in G$ δύο στοιχεία της G τα οποία έχουν πεπερασμένη τάξη.*

(1) $\forall x \in G, \ \ \forall a \in G$: $\mathsf{o}(x^{-1}ax) = \mathsf{o}(a) = \mathsf{o}(xax^{-1})$.
(2) $\forall a, b \in G$: $\mathsf{o}(ab) = \mathsf{o}(ba)$.

Απόδειξη. (1) Έστω $x, a \in G$. Τότε:

$$\forall n \in \mathbb{Z}^+ : \ \ (x^{-1}ax)^n = (x^{-1}ax)(x^{-1}ax)\cdots(x^{-1}ax) = x^{-1}aa\cdots ax = x^{-1}a^n x$$

και παρόμοια

$$\forall n \in \mathbb{Z}^+ : \ \ (xax^{-1})^n = \ xa^n x^{-1}$$

Επομένως:

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

και

$$(xax^{-1})^m = e \iff xa^m x^{-1} = e \iff a^m = x^{-1}ex = e \tag{$**$}$$

Οι παραπάνω σχέσεις δείχνουν ότι: $\mathsf{o}(a) < \infty$ αν και μόνον αν $\mathsf{o}(x^{-1}ax) < \infty$ αν και μόνον αν $\mathsf{o}(xax^{-1}) < \infty$.

Επιπλέον έστω ότι $\mathsf{o}(a) = n$ και $\mathsf{o}(x^{-1}ax) = m$. Τότε η σχέση $(*)$ δείχνει ότι n/m. Θέτοντας $b = x^{-1}ax$ θα έχουμε $a = xax^{-1}$ και τότε η σχέση $(**)$ δείχνει ότι m/n. Επομένως καταλήγουμε ότι: $\mathsf{o}(a) = n = m = \mathsf{o}(x^{-1}ax)$. Παρόμοια θα έχουμε και ότι: $\mathsf{o}(a) = \mathsf{o}(xax^{-1})$.

(2) Επειδή $ba = eba = a^{-1}aba = a^{-1}(ab)a$, από το (1) έπεται ότι:

$$\mathsf{o}(ba) = \mathsf{o}(a^{-1}(ab)a) = \mathsf{o}(ab) \qquad \square$$

3.5. **Εφαρμογές του Θεωρήματος Lagrange (II).** Στην παρούσα ενότητα θα δούμε μια άλλη κατηγορία εφαρμογών του Θεωρήματος του Lagrange.

Το επόμενο σημαντικό αποτέλεσμα αποτελεί μια απλή εφαρμογή του Θεωρήματος Lagrange.

Πρόταση 3.18. *Έστω $(G, \star)$ μια πεπερασμενη ομάδα. Τότε $\forall x \in G$:*
(1) $x^{\mathsf{o}(G)} = e$.
(2) $\mathsf{o}(x)/\mathsf{o}(G)$.

Απόδειξη. (1) Η τάξη $\mathsf{o}(x)$ του x, είναι εξ' ορισμού η τάξη της κυκλικής υποομάδας που παράγεται από το x. Απο το Θεώρημα του Lagrange έπεται ότι $\mathsf{o}(x)/\mathsf{o}(G)$, και άρα:

$$\mathsf{o}(G) = k_x \cdot \mathsf{o}(x), \quad \text{όπου} \quad k_x \geq 1$$

Έτσι θα έχουμε:

$$x^{\mathsf{o}(G)} = x^{k_x \cdot \mathsf{o}(x)} = (x^{\mathsf{o}(x)})^{k_x} = e^{k_x} = e \qquad \square$$

(2) Επειδή $\mathsf{o}(x) = \mathsf{o}(\langle x \rangle)$, το ζητούμενο προκύπτει απο το Θεώρημα του Lagrange.

Θα δούμε τώρα κάποιες εφαρμογές της παραπάνω Πρότασης στην Θεωρία Αριθμών. Πρώτα υπενθυμίζουμε ότι η **συνάρτηση ϕ του Euler** ορίζεται ως εξής:

$$\varphi : \mathbb{N} \longrightarrow \mathbb{N}, \quad \varphi(n) = \left| \left\{ k \in \mathbb{N} \mid 1 \leq k \leq n \ \ \& \ \ (n,k) = 1 \right\} \right|$$

Πρόταση 3.19. *(**Θεώρημα Euler**) Έστω $n \geq 1$ και $a \in \mathbb{Z}$ με $(a, n) = 1$. Τότε:*

$$a^{\varphi(n)} \equiv 1 \operatorname{mod}(n)$$

Απόδειξη. Η ζητούμενη σχέση γράφεται ισοδύναμα στο $\mathbb{Z}_n$:

$$[a^{\varphi(n)}]_n = ([a]_n)^{\varphi(n)} \equiv [1]_n$$

Επειδή $(a, n) = 1$, έπεται οτι $[a]_n \in \mathsf{U}(\mathbb{Z}_n)$. Επειδή η ομάδα $\mathsf{U}(\mathbb{Z}_n)$ έχει τάξη $\varphi(n)$, από την Πρόταση 3.18 έπεται ότι το ζητούμενο: $([a]_n)^{\varphi(n)} = [1]_n$. $\square$

Πόρισμα 3.20. *(**Μικρό Θεώρημα Fermat**) Έστω p ένας πρώτος αριθμός και $a \in \mathbb{Z}$ με $p \nmid a$. Τότε:*

$$a^{p-1} \equiv 1 \operatorname{mod}(p)$$

Απόδειξη. Επειδή p είναι πρώτος, έπεται ότι$\varphi(p) = p - 1$ και $(a, p) = 1$. Τότε το αποτέλεσμα προκύπτει από το Θεώρημα του Euler. $\square$

Παρατήρηση 3.21. *Το αντίστροφο της Πρότασης* 3.17 *δεν ισχύει: υπάρχουν άπειρες ομάδες* G *με την ιδιότητα* $x^m = e, \forall x \in G$, *όπου* $m \in \mathbb{Z}^+$.

Πραγματικά, θεωρούμε την ομάδα $(\mathbb{Z}_2, +) = \big(\{[0]_2, [1]_2\}, +\big)$ *των ακεραίων modulo 2, και έστω η* **ομάδα-ευθύ γινόμενο**

$$\prod_{n=1}^{\infty} \mathbb{Z}_2 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots \ = \ \big\{(x_n)_{n\geq 1} \mid x_n \in \mathbb{Z}_2, \ \forall n \geq 1\big\}$$

με στοιχεία τις ακολουθίες στοιχείων του $\mathbb{Z}_2$, *και με πράξη*

$$(x_n)_{n\geq 1} + (y_n)_{n\geq 1} = (x_n + y_n)_{n\geq 1}$$

Το ουδέτερο στοιχείο της ομάδας $\prod_{n=1}^{\infty} \mathbb{Z}_2$ *είναι η ακολουθία* $(x_n)_{n\geq 1}$, *όπου* $x_n = [0]_2, \forall n \geq 1$. *Προφανώς η ομάδα* $\prod_{n=1}^{\infty} \mathbb{Z}_2$ *είναι άπειρη. Παρατηρούμε ότι, επειδή* $[x]_2 + [x]_2 = [x+x]_2 = [0]_2, \forall [x]_2 \in \mathbb{Z}_2$, *θα έχουμε* $\forall (x_n)_{n\geq 1} \in \prod_{n=1}^{\infty} \mathbb{Z}_2$:

$$2(x_n)_{n\geq 1} = (x_n)_{n\geq 1} + (x_n)_{n\geq 1} = (x_n + x_n)_{n\geq 1} = ([0]_2)_{n\geq 1}$$

και άρα κάθε μη-ταυτοτικό στοιχείο της ομάδας $\prod_{n=1}^{\infty} \mathbb{Z}_2$ *έχει τάξη* 2.

Ορισμός 3.22. *Έστω* $(G, \star)$ *μια ομάδα.*

(1) *Η ομάδα* G *καλείται* **ομάδα στρέψης** *ή* **περιοδική ομάδα**, *αν κάθε στοιχείο της* G *έχει πεπερασμένη τάξη.*
(2) *Η ομάδα* G *καλείται* **ομάδα ελεύθερης στρέψης**, *αν κάθε στοιχείο της* G, *εκτός του ταυτοτικού, έχει άπειρη τάξη.*

Παράδειγμα 3.23. (1) *Όπως προκύπτει από την Πρόταση* 3.11, *κάθε πεπερασμένη ομάδα είναι ομάδα στρέψης. Σύμφωνα με την Παρατήρηση* 3.13, *υπάρχουν ομάδες στρέψης οι οποίες είναι άπειρες ομάδες.*

(2) *Κάθε ομάδα ελεύθερης στρέψης είναι προφανώς άπειρη ομάδα, και κάθε άπειρη κυκλική ομάδα, π.χ.* $(\mathbb{Z}, +)$, *είναι ομάδα ελεύθερης στρέψης.*
(3) *Υπάρχουν ομάδες οι οποίες είναι* **μεικτές** *δηλαδή περιέχουν στοιχεία πεπερασμένης τάξης και στοιχεία άπειρης τάξης. Ένα τέτοιο παράδειγμα είναι η ομάδα ευθύ γινόμενο:*

$$\mathbb{Z}_2 \times \mathbb{Z} = \big\{([x]_2, m) \mid x, m \in \mathbb{Z}\big\}$$

με πράξη:

$$([x]_2, m) + ([y]_2, n) = ([x+y]_2, m+n)$$

και της οποίας το ουδέτερο στοιχείο είναι το ζεύγος $([0]_2, 0)$.

Τότε το στοιχείο $([1]_2, 0)$ *έχει τάξη* 2, *και το στοιχείο* $([0]_2, 1)$ *έχει άπειρη τάξη.*

Παράδειγμα 3.24. *Έστω*

$$\mathbb{T} = \big\{z \in \mathbb{C} \mid |z| = 1\big\}$$

εύκολα βλέπουμε ότι η $\mathbb{T}$ *είναι μια υποομάδα της πολλαπλασιαστικής ομάδας* $(\mathbb{C}^*, \cdot)$ *των μη-μηδενικών μιγαδικών αριθμών. Η ομάδα* $\mathbb{T}$ *καλείται, για προφανείς λόγους, η ομάδα του κύκλου.*

Έστω p *ένας πρώτος αριθμός και έστω*

$$\mathbb{Z}(p^\infty) = \big\{z \in \mathbb{C} \mid z^{p^n} = 1, \ \text{για κάποιο} \ n \in \mathbb{Z}^+\big\} \ \subseteq \ \mathbb{T}$$

Εύκολα βλέπουμε ότι η $\mathbb{Z}(p^\infty)$ *είναι μια υποομάδα της* $\mathbb{T}$ *και κάθε στοιχείο της* $\mathbb{Z}(p^\infty)$ *έχει πεπερασμένη τάξη. Έτσι η ομάδα* $\mathbb{Z}(p^\infty)$ *είναι μια άπειρη ομάδα στρέψης.*

Η ομάδα $\mathbb{Z}(p^\infty)$ *καλείται η* p**-οστή ομάδα Prüfer** *και έχει, μεταξύ άλλων, την ενδιαφέρουσα ιδιότητα: όλες οι γνήσιες υποομάδες της είναι πεπερασμένες κυκλικές και υπάρχει ακριβώς μια τέτοια υποομάδα τάξης* p^n, *για κάθε* $n \in \mathbb{Z}^+$.

Οι παραπάνω παρατηρήσεις και παραδείγματα σχετίζονται με ένα περίφημο πρόβλημα στην Θεωρία Ομάδων:

Παρατήρηση 3.25. *(**Το Πρόβλημα του Burnside**) Μια ομάδα $(G, \star)$ καλείται **πεπερασμένα παραγόμενη**, αν υπάρχει πεπερασμένο πλήθος στοιχείων $z_1, z_2, \cdots, z_m \in G$, έτσι ώστε κάθε στοιχείο $x \in G$ να γράφεται ως:*

$$x = z_1^{n_1} \star z_2^{n_2} \star \cdots \star z_m^{n_m}, \qquad \text{για κατάλληλα} \qquad n_1, n_2, \cdots, n_m \in \mathbb{Z}$$

Το γενικό Πρόβλημα του Burnside διατυπώνεται ως εξής:

«Είναι κάθε πεπερασμένα παραγόμενη ομάδα στρέψης, πεπερασμένη;»

Το Πρόβλημα του Burnside απαντήθηκε αρνητικά το 1964 από τους E.Golod και I. Shafarevich, οι οποίοι κατασκεύασαν μια πεπερασμένα παραγόμενη άπειρη ομάδα, κάθε στοιχείο της οποίας έχει πεπερασμένη τάξη η οποία είναι δύναμη ενός πρώτου αριθμού p.

Όπως όμως θα αποδείξουμε αργότερα, το Πρόβλημα του Burnside έχει θετική απάντηση όταν περιορισθούμε στην κλάση των αβελιανών ομάδων:

Κάθε πεπερασμένα παραγόμενη αβελιανή ομάδα στρέψης είναι πεπερασμένη

*Σ'αυτή την περίπτωση η (προσθετική) αβελιανή ομάδα $(G, +)$ καλείται **πεπερασμένα παραγόμενη** αν και μόνον αν υπάρχει πεπεραμένο πλήθος στοιχείων $z_1, z_2, \cdots, z_m \in G$, έτσι ώστε κάθε στοιχείο $x \in G$ να γράφεται ως:*

$$x = n_1 z_1 + n_2 z_2 + \cdots + n_m z_m, \qquad \text{για κατάλληλα} \qquad n_1, n_2, \cdots, n_m \in \mathbb{Z}$$

Η ομάδα Prüfer $\mathbb{Z}(p^\infty)$ είναι μια άπειρη αβελιανή ομάδα στρέψης. Επομένως σύμφωνα με τα παραπάνω δεν μπορεί να είναι πεπερασμένα παραγόμενη.

Πρόταση 3.26. *Έστω $(G, \star)$ μια πεπερασμενη ομάδα. Αν $\mathsf{o}(G) = p$ ένας πρώτος αριθμός, τότε η G είναι κυκλική.*

Απόδειξη. Επειδή $\mathsf{o}(G) = p \geq 2$, έπεται ότι $G \neq \{e\}$ και άρα η G περιέχει ένα στοιχείο $x \neq e$. Σύμφωνα με την Πρόταση 3.11, θα έχουμε: $\mathsf{o}(x)/p$ και επομένως, επειδή ο p είναι πρώτος, θα έχουμε $\mathsf{o}(x) = 1$ ή $\mathsf{o}(x) = p$. Όμως $\mathsf{o}(x) \neq 1$ διότι $x \neq e$, και επομένως $\mathsf{o}(x) = p$. Τότε επειδή $\langle x \rangle \subseteq G$ και $\mathsf{o}(x) = \mathsf{o}(\langle x \rangle) = |G| = \mathsf{o}(G) = p$, έπεται ότι $\langle x \rangle = G$ και η G είναι κυκλική. □

Πρόταση 3.27. *Έστω $(G, \star)$ μια ομάδα τάξης $\mathsf{o}(G) = pq$, όπου p, q είναι πρώτοι αριθμοί. Τότε κάθε γνήσια υποομάδα της G είναι κυκλική.*

Απόδειξη. Έστω H μια γνήσια υποομάδα της G. Απο το Θεωρήματος Lagrange θα έχουμε $\mathsf{o}(H)/pq$. Επειδή οι διαιρέτες του pq είναι $1, p, q, pq$, έπεται ότι: $\mathsf{o}(H) = 1$ ή p ή q ή pq. Επειδή η H είναι γνήσια , έπεται ότι $\mathsf{o}(H) \neq pq$. Αν $\mathsf{o}(H) = 1$, τότε $H = \{e\} = \langle e \rangle$. Τέλος αν $\mathsf{o}(H) = p$ ή q, το συμπέρασμα προκύπτει από την Πρόταση 3.17. □

Γενικότερα, όπως θα αποδείξουμε αργότερα, ισχύει το ακόλουθο Θεώρημα:

Θεώρημα 3.28. *(**Cauchy**) Αν p είναι ένας πρώτος αριθμός ο οποίος διαιρεί την τάξη μιας πεπερασμένης ομάδας G, τότε η G έχει μια υποομάδα τάξης p, (η οποία είναι κυκλική και και επομένως G έχει ένα στοιχείο τάξης p).*

Ανοικτά Ακαδημαϊκά Μαθήματα

Πανεπιστήμιο Ιωαννίνων

Τέλος Ενότητας

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Ιωαννίνων**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ ΚΑΙ ΘΡΗΣΚΕΥΜΑΤΩΝ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Σημειώματα

Σημείωμα Αναφοράς

Σημείωμα Αδειοδότησης