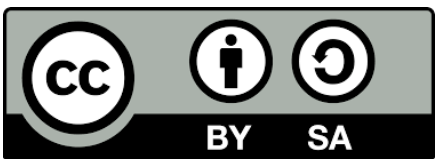
ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΪΚΑ ΜΑΘΗΜΑΤΑ

Τίτλος Μαθήματος: Αλγεβρικές Δομές Ι

Ενότητα: Ταξινόμηση Κυκλικών Ομάδων και των Υποομάδων τους

Διδάσκων: Καθηγητής Νικόλαος Μαρμαρίδης, Καθηγητής Ιωάννης Μπεληγιάννης

Τμήμα: Μαθηματικών



5. **Ταξινόμηση Κυκλικών Ομάδων και των Υποομάδων τους**

Στην παρούσα ενότητα θα ταξινομήσουμε τις κυκλικές ομάδες, τις υποομάδες τους, και τους γεννήτορές τους. Οι ταξινομήσεις αυτές θα βασιστούν στην αριθμητική των θετικών ακεραίων αριθμών.

Απο τώρα και στο εξής σταθεροποιούμε μια κυκλική ομάδα

$$G = \langle a \rangle$$

με γεννήτορα το στοιχείο $a \in G$.

Το ακόλουθο αποτέλεσμα δείχνει ότι οι κυκλικές ομάδες συμπεριφέρονται καλά ως προς τις υποομάδες.

Θεώρημα 5.1. *Κάθε υποομάδα μιας κυκλικής ομάδας είναι κυκλική ομάδα.*

Απόδειξη. Έστω όπως παραπάνω $G = \langle a \rangle$ μια κυκλική ομάδα, και έστω $H \leq G$ μια υποομάδα της G.

Αν $H = \{e\}$, τότε προφανώς $H = \langle e \rangle$ και η H είναι κυκλική.

Έστω $H \neq \{e\}$, και επομένως υπάρχει $g \in H \setminus \{e\}$. Θα έχουμε $g = a^k$ για κάποιο $k \in \mathbb{Z}$. Τότε $k \neq 0$ διότι διαφορετικά $g = a^0 = e$ το οποίο είναι άτοπο. Αν $k < 0$, τότε επειδή η H είναι υποομάδα θα έχουμε ότι $g^{-1} = (a^k)^{-1} = a^{-k} \in H$ και $-k > 0$. Επομένως η G περιέχει *θετικές* δυνάμεις a^k, $k > 0$, του γεννήτορα a.

Έστω n ο μικρότερος θετικός ακέραιος με την ιδιότητα $g^n \in H$. Θα δείξουμε ότι:

$$H = \langle g^n \rangle$$

Επειδή $g^n \in H$ και η H είναι υποομάδα, έπεται ότι $\langle g^n \rangle \subseteq H$. Έστω $h \in H$. Τότε $h = a^m$, για κάποιο $m \in \mathbb{Z}$. Από την Ευκλείδεια Διαίρεση, θα έχουμε τότε:

$$m = nq + r, \qquad 0 \leq r < n$$

και επομένως:

$$a^m = a^{nq+r} = a^{nq}a^r = (a^n)^q a^r \quad \Longrightarrow \quad a^r = (a^n)^{-q}a^m$$

Επειδή $a^n \in H$ εκ' κατασκευής, θα έχουμε $(a^n)^{-q} \in H$. Επιπλέον επειδή $a^m \in H$, θα έχουμε $a^r = (a^n)^{-q}a^m \in H$ διότι η H είναι υποομάδα. Επειδή n είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα $g^n \in H$, και επειδή $a^r \in H$, όπου $0 \leq r < n$, έπεται ότι αναγκαστικά: $r = 0$. Επομένως

$$h = a^m = a^{nq} = (a^n)^q \ \in \ \langle a^n \rangle$$

Συμπεραίνουμε ότι $H \subseteq \langle a^n \rangle$. Άρα $H = \langle a^n \rangle$ και επομένως η H είναι κυκλική. □

5.1. **Υποομάδες και Γεννήτορες Άπειρων Κυκλικών Ομάδων.** Στην παρούσα υπο-ενότητα υποθέτουμε ότι η κυκλική ομάδα $G = \langle a \rangle$ είναι άπειρης τάξης, ή ισοδύναμα ο γεννήτορας a έχει άπειρη τάξη $\mathsf{o}(a) = \infty$. Τότε:

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

Θεώρημα 5.2. *Έστω G μια άπειρη κυκλική ομάδα.*

(1) *Η G έχει μόνον δύο γεννήτορες: αν a είναι ένας γεννήτορας τότε ο μοναδικός διαφορετικός γεννήτορας της G είναι ο a^{-1}.*

(2) *Αν $G = \langle a \rangle$, τότε οι υποομάδες της G είναι οι ακόλουθες και μόνον αυτές:*

$$H \ \leq \ G \quad \Longleftrightarrow \quad H = \langle a^n \rangle, \ \ n \geq 0$$

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

(3) *Αν* $H_n = \langle a^n \rangle$ *και* $H_m = \langle a^m \rangle$ *είναι δύο υποομάδες της* $G = \langle a \rangle$*, τότε:*

$$H_n \subseteq H_m \iff m \mid n$$

Απόδειξη. (1) Έστω a ένας γεννήτορας της G, δηλαδή $G = \langle a \rangle$. Έστω b ένας άλλος γεννήτορας: $G = \langle b \rangle$. Θα έχουμε $b = a^k$ για κάποιο $n \in \mathbb{Z}$. Έτσι θα έχουμε:

$$\langle a \rangle = \langle a^n \rangle$$

Τότε $a \in \langle a^n \rangle$ και επομένως $a = (a^n)^k = a^{nk}$ για κάποιο $k \in \mathbb{Z}$. Τότε όμως θα έχουμε:

$$a = a^{nk} \implies aa^{-nk} = e \implies a^{1-nk} = e \implies 1 - nk = 0$$

διότι το ατοιχείο a έχει πεπερασμένη τάξη. Έτσι $1 = nk$. Επειδή όμως $n, k \in \mathbb{Z}$, θα έχουμε ότι είτε $n = k = 1$, ή $n = k = -1$. Στην πρώτη περίπτωση $b = a^n = a$ και στην δεύτερη περίπτωση $b = a^n = a^{-1}$.

(2) Έστω $H \leq G$ μια υποομάδα της G. Από το Θεώρημα 5.1 έπεται ότι η H είναι κυκλική και επομένως $H = \langle a^n \rangle$. Μπορούμε να υποθέσουμε ότι $n \geq 0$, διότι αν $n \leq 0$, τότε από το (1) έπεται ότι $H = \langle (a^n)^{-1} \rangle = \langle a^{-n} \rangle$ και $-n \geq 0$. Επομένως δείξαμε ότι η H είναι υποομάδα της G αν και μόνον αν η H είναι της μορφής $H = \langle a^n \rangle$, $n \geq 0$, και έτσι μένει να δείξουμε ότι:

$$\forall n, m \geq 0, \quad n \neq m \implies \langle a^n \rangle \neq \langle a^m \rangle$$

Υποθέτουμε ότι η παραπάνω συνεπαγωγή δεν είναι αληθής και θα καταλήξουμε σε άτοπο. Θα έχουμε:

$$\langle a^n \rangle = \langle a^m \rangle \implies a^n \in \langle a^m \rangle \text{ και } a^m \in \langle a^n \rangle \implies \exists\, k, l \in \mathbb{Z}: \ a^n = a^{mk} \text{ και}$$

$$a^m = a^{nl} \implies a^{n-mk} = e = a^{m-nl}$$

Επειδή ο γεννήτορας a της G έχει πεπερασμένη τάξη, έπεται ότι:

$$n - mk = 0 = m - nl \implies n = mk \text{ και } m = nl \implies n \mid m \text{ και } m \mid n \implies n = m$$

Άρα οι διακεκριμμένες υποομάδες της G είναι $H_n = \langle a^n \rangle$, $\forall n \geq 0$.

(3) Έστω $H_n = \langle a^n \rangle \subseteq H_m = \langle a^m \rangle$. Τότε όπως είδαμε και στο (2), θα έχουμε: $a^n \in \langle a^m \rangle$ και τότε $m \mid n$. Αντίστροφα αν $m \mid n$, τότε $n = mk$ για κάποιο $k \in \mathbb{Z}$ και τότε $a^n = a^{mk} = (a^m)^k \in \langle a^m \rangle$. Αυτό όμως σημαίνει ότι $H_n = \langle a^n \rangle \subseteq H_m = \langle a^m \rangle$. □

Πόρισμα 5.3. *Έστω* $G = \langle a \rangle$ *μια άπειρη κυκλική ομάδα. Τότε οι απεικόνισεις*

$$\Phi : \mathbb{N} \longrightarrow \{\textit{Υποομάδες της } G\}, \quad \Phi(n) = \langle a^n \rangle$$

$$\Psi : \{1, -1\} \longrightarrow \{\textit{Γεννήτορες της } G\}, \quad \Psi(k) = \langle a^n \rangle$$

είναι 1-1 και επί. Επιπλέον $m \mid n \iff \Phi(n) \subseteq \Phi(m)$.

Υπενθυμίζουμε ότι η τομή $H \cap K$ υποομάδων H, K μιας ομάδας G είναι υποομάδα, και το γινόμενο $H \cdot K$ των H, K είναι υποομάδα, όταν η G είναι αβελιανή ή γενικότερα αν ισχύει: $HK = KH$. Στην περίπτωση κατά την οποία η G είναι (άπειρη) κυκλική, και οι ομάδες $H \cap K$ και $H \cdot K$ θα είναι κυκλικές.

Η επόμενη Πρόταση δίνει ακριβείς πληροφορίες γι' αυτές τις κυκλικές υποομάδες.

Πρόταση 5.4. *Έστω* $G = \langle a \rangle$ *μια άπειρη κυκλική ομάδα.*

(1)

$$\langle a^n \rangle \cdot \langle a^m \rangle = \langle a^{(m,n)} \rangle$$

(2)

$$\langle a^n \rangle \bigcap \langle a^m \rangle = \langle a^{[n,m]} \rangle$$

Απόδειξη. (1) Έστω $d = (m, n)$. Τότε

$$d \mid n \implies n = dk \qquad \text{και} \qquad d \mid m \implies n = dl, \qquad \text{όπου} \qquad k, l \in \mathbb{Z}$$

και επομένως:

$$a^n = a^{dk} = (a^d)^k \in \langle a^d \rangle \qquad \text{και} \qquad a^m = a^{dl} = (a^d)^l \in \langle a^d \rangle$$

Άρα

$$a^n \in \langle a^d \rangle \ni a^m \implies \langle a^n \rangle \subseteq \langle a^d \rangle \supseteq \langle a^m \rangle$$

Επειδή η $\langle a^d \rangle$ είναι υποομάδα, προφανώς θα έχουμε ότι

$$\langle a^n \rangle \cdot \langle a^m \rangle \subseteq \langle a^d \rangle \tag{$*$}$$

Από την άλλη πλευρά, επειδή $d = (m, n)$, έπεται ότι υπάρχουν ακέραιοι $r, s \in \mathbb{Z}$, έτσι ώστε $d = nr + ms$. Τότε:

$$a^d = a^{nr+ms} = a^{nr} a^{ms} = (a^n)^r (a^m)^s \in \langle a^n \rangle \cdot \langle a^m \rangle$$

Αυτό όμως σημαίνει ότι

$$\langle a^d \rangle \subseteq \langle a^n \rangle \cdot \langle a^m \rangle \tag{$**$}$$

Από τις σχέσεις $(*)$ και $(**)$, θα έχουμε: $\langle a^n \rangle \cdot \langle a^m \rangle = \langle a^d \rangle$.

(2) Έστω $\delta = [m, n]$. Τότε:

$$\delta = mk = nl \implies a^\delta = a^{nl} = (a^n)^l \in \langle a^n \rangle \qquad \text{και} \qquad a^\delta = a^{mk} = (a^m)^k \in \langle a^m \rangle$$

Επομένως $a^\delta \in \langle a^n \rangle \cap \langle a^m \rangle$ το οποίο προφανώς σημαίνει ότι:

$$\langle a^\delta \rangle \subseteq \langle a^n \rangle \cap \langle a^m \rangle \tag{$\dagger$}$$

Αντίστροφα έστω $x \in \langle a^n \rangle \cap \langle a^m \rangle$. Τότε $x = (a^n)^p$ και $x = (a^m)^q$, όπου $p, q \in \mathbb{Z}$. Επομένως, χρησιμοποιώντας ότι το στειχείο a έχει άπειρη τάξη, θα έχουμε:

$$x = (a^n)^p = (a^m)^q \implies a^{np} = a^{mq} \implies a^{np-mq} = e \implies np = mq$$

Θέτοντας $t := np = mq$, θα έχουμε ότι: $x \in \langle a^t \rangle$. Επιπλέον $m \mid t$ και $n \mid t$. Τότε όμως $\delta \mid t$, και επομένως από το Θεώρημα 5.2 θα έχουμε:

$$x \in \langle a^t \rangle \subseteq \langle a^\delta \rangle$$

το οποίο σημαίνει ότι:

$$\langle a^n \rangle \cap \langle a^m \rangle \subseteq \langle a^\delta \rangle \tag{$\dagger\dagger$}$$

Από τις σχέσεις $(\dagger)$ και $(\dagger\dagger)$, θα έχουμε: $\langle a^n \rangle \cap \langle a^m \rangle = \langle a^\delta \rangle$. □

Συνοψίζουμε τα παραπάνω αποτελέσματα εφαρμοσμένα στην άπειρη κυκλική (προσθετική) ομάδα $(\mathbb{Z}, +)$.

Παράδειγμα 5.5. *Θεωρούμε την άπειρη κυκλική ομάδα $(\mathbb{Z}, +)$. Όπως θα δούμε αργότερα κάθε άλλη άπειρη κυκλική ομάδα είναι «ισόμορφη», δηλαδή δομικά ίδια, με την ομάδα $(\mathbb{Z}, +)$.*

(1) *Οι μόνοι γεννήτορες της $(\mathbb{Z}, +)$ είναι το 1 και το -1.*

(2) *Οι διακεκριμμένες υποομάδες της $(\mathbb{Z}, +)$ είναι οι εξής*

$$n\mathbb{Z} = \big\{ nz \in \mathbb{Z} \mid z \in \mathbb{Z} \big\}, \qquad \forall n \geq 0$$

(3)

$$n\mathbb{Z} \leq m\mathbb{Z} \iff m \mid n$$

(4)

$$n\mathbb{Z} \bigcap m\mathbb{Z} = [n, m]\mathbb{Z} \qquad \text{και} \qquad n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z}$$

5.2. **Υποομάδες και Γεννήτορες Πεπερασμένων Κυκλικών Ομάδων.** Στην παρούσα υπο-ενότητα υποθέτουμε ότι η κυκλική ομάδα $G = \langle a \rangle$ είναι πεπερασμένης τάξης: $\mathsf{o}(G) = n$, ή ισοδύναμα ο γεννήτορας a έχει πεπερασμένη τάξη $\mathsf{o}(a) = n$. Τότε:

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

Σκοπός μας είναι να αποδείξουμε ένα Θεώρημα για την G το οποίο να είναι ανάλογο με το Θεώρημα 5.2. Για την διατύπωση και απόδειξη αυτού του ανάλογου αποτελέσματος, Θα χρειασθούμε μια σειρά από βοηθητικές προτάσεις.

Λήμμα 5.6. *Έστω $H = \langle a^m \rangle$ μια υποομάδα της $G = \langle a \rangle$, όπου $\mathsf{o}(a) = n$. Τότε:*

$$H = \langle a^d \rangle, \quad \textit{όπου} \quad d = (n, m), \quad \textit{και} \quad \mathsf{o}(H) = \mathsf{o}(a^m) = \frac{n}{d}$$

Απόδειξη. Επειδή $d = (n, m)$, θα έχουμε $m = dk$ και τότε:

$$a^m = a^{dk} = (a^d)^k \in \langle a^d \rangle \quad \Longrightarrow \quad \langle a^m \rangle \subseteq \langle a^d \rangle$$

Επίσης επειδή $d = (n, m)$, θα έχουμε $d = nx + my$ για κάποια $x, y \in \mathbb{Z}$. Τότε επειδή $\mathsf{o}(a) = n$:

$$a^d = a^{nx+my} = a^{nx}a^{my} = (a^n)^x(a^m)^y = e^x(a^m)^y = (a^m)^y \in \langle a^m \rangle \implies a^d \in \langle a^m \rangle \implies \langle a^d \rangle \subseteq \langle a^m \rangle$$

Από τις παραπάνω σχέσεις βλέπουμε ότι $\langle a^m \rangle = \langle a^d \rangle$. Τέλος χρησιμοποιώντας το Θεώρημα 3.11, θα έχουμε:

$$\mathsf{o}(H) = \mathsf{o}(\langle a^m \rangle) = \frac{\mathsf{o}(a)}{(\mathsf{o}(a), m)} = \frac{n}{(n, m)} = \frac{n}{d} \qquad \square$$

Λήμμα 5.7. *Έστω $G = \langle a \rangle$, όπου $\mathsf{o}(a) = n$, και $r, s \geq 1$. Τότε:*

$$\langle a^r \rangle = \langle a^s \rangle \quad \Longleftrightarrow \quad (n, r) = (n, s)$$

Απόδειξη. «$\Longrightarrow$» Θα έχουμε:

$$\langle a^r \rangle = \langle a^s \rangle \implies \mathsf{o}(a^r) = \mathsf{o}(a^s) \iff \frac{\mathsf{o}(a)}{(\mathsf{o}(a), r)} = \frac{\mathsf{o}(a)}{(\mathsf{o}(a), s)} \iff \frac{n}{(n, r)} = \frac{n}{(n, s)} \iff (n, r) = (n, s)$$

«$\Longleftarrow$» Θα έχουμε όπως και παραπάνω: $(n, r) = (n, s) \implies \mathsf{o}(a^r) = \mathsf{o}(a^s)$. Όμως χρησιμοποιώντας το Λήμμα 5.6, και την υπόθεση $(n, r) = (n, s)$, θα έχουμε:

$$\langle a^r \rangle = \langle a^{(n,r)} \rangle \quad \text{και} \quad \langle a^s \rangle = \langle a^{(n,s)} \rangle \quad \Longrightarrow \quad \langle a^r \rangle = \langle a^s \rangle \qquad \square$$

Λήμμα 5.8. *Έστω $G = \langle a \rangle$, όπου $\mathsf{o}(a) = n$. Το στοιχείο a^m είναι γεννήτορας της G αν και μόνον αν $(m, n) = 1$:*

$$\langle a \rangle = \langle a^m \rangle \iff (n, m) = 1$$

Απόδειξη. Χρησιμοποιώντας το Λήμμα 5.7, Θα έχουμε:

$$a^m \text{ είναι γεννήτορας της } G \iff \langle a^m \rangle = \langle a \rangle \iff (n, m) = (n, 1) \iff (n, m) = 1 \qquad \square$$

Μπορούμε τώρα να αποδείξουμε το ακόλουθο αποτέλεσμα το οποίο είναι ανάλογο του Θεωρήματος 5.2.

Θεώρημα 5.9. *Έστω $G = \langle a \rangle$ μια κυκλική ομάδα τάξης $\mathsf{o}(G) = \mathsf{o}(a) = n$.*

(1)

$$\textit{Σύνολο γεννητόρων της} \quad G \;=\; \big\{a^m \in G \mid (n,m)=1\big\}$$

$$\textit{Πλήθος γεννητόρων της } G \;=\; \varphi(n) = \big|\big\{1 \le m \le n \mid (n,m)=1\big\}\big|$$

(2) *Τα ακόλουθα είναι ισοδύναμα:*

(α') $m \mid n$.

(β') *Υπάρχει υοομάδα* $H \le G$ *έτσι ώστε:* $\mathsf{o}(H) = m$.

Αν $m \mid n$*, τότε υπάρχει μοναδική υποομάδα της* G *με τάξη* m *η οποία είναι η εξής:*

$$H_m = \langle a^{\frac{n}{m}} \rangle$$

(3) *Έστω* m, k *δύο διαιρέτες της τάξης* n *της* G*, και έστω* H_m *και* H_k *οι μοναδικές υποομάδες της* G *με τάξεις* m *και* k *αντίστοιχα. Τότε:*

$$H_m \subseteq H_k \quad\Longleftrightarrow\quad m \mid k$$

Απόδειξη. (1) Προκύπτει άμεσα από το Λήμμα 5.8.

(2) Αν υπάρχει υποομάδα H της G με τάξη $\mathsf{o}(H) = m$, τότε από το Θεώρημα του Lagrange έπεται ότι $m \mid \mathsf{o}(G)$ και άρα $m \mid n$.

Αντίστροφα αν $m \mid n$, τότε θεωρούμε την υποομάδα $H = \langle a^{\frac{n}{m}} \rangle$ της G. Τότε επειδή

$$\mathsf{o}(a^{\frac{n}{m}}) = \frac{n}{(n, \frac{n}{m})} = \frac{n}{\frac{n}{m}} = m$$

έπεται ότι $\mathsf{o}(H) = m$.

Έστω ότι $m \mid n$ και έστω H_1 και H_2 υποομάδες της G έτσι ώστε: $\mathsf{o}(H_1) = m = \mathsf{o}(H_2)$. Από το Θεώρημα 5.1 θα έχουμε

$$H_1 = \langle a^{k_1} \rangle \quad \text{και} \quad H_2 = \langle a^{k_2} \rangle \quad \text{όπου} \quad 1 \le k_1, k_2 \le n$$

Επομένως

$$\frac{n}{(n,k_1)} = \mathsf{o}(a^{k_1}) = \mathsf{o}(H_1) = m = \mathsf{o}(H_2) = \mathsf{o}(a^{k_2}) = \frac{n}{(n,k_2)} \quad\Longrightarrow\quad (n,k_1) = (n,k_2)$$

Τότε από το Λήμμα 5.7 έπεται ότι θα έχουμε $H_1 = \langle a^{k_1} \rangle = \langle a^{k_2} \rangle = H_2$. Άρα για κάθε διαιρέτη $m \mid n$, υπάρχει μοναδική υποομάδα της G με τάξη m. Από το Λήμμα 5.6, μοναδική υποομάδα είναι η $H_m = \langle a^{\frac{n}{m}} \rangle$.

(3) Έστω m, k δύο διαιρέτες της τάξης n της G, και έστω H_m και H_k οι μοναδικές υποομάδες της G με τάξεις m και k αντίστοιχα. Τότε από το (2) θα έχουμε:

$$H_m \subseteq H_k \iff \langle a^{\frac{n}{m}} \rangle \le \langle a^{\frac{n}{k}} \rangle \iff \mathsf{o}(a^{\frac{n}{m}}) \mid \mathsf{o}(a^{\frac{n}{k}}) \iff m \mid k \qquad \square$$

Το ακόλουθο αποτέλεσμα είναι άμεση συνέπεια του Θεωρήματος 5.9.

Πόρισμα 5.10. *Έστω* $G = \langle a \rangle$ *μια κυκλική ομάδα τάξης* $\mathsf{o}(G) = \mathsf{o}(a) = n$*. Οι απεικονίσεις*

$$\Phi : \mathcal{D}(n) = \big\{d \ge 1 \mid d \mid n\big\} \longrightarrow \big\{\textit{Υποομάδες της } G\big\}, \quad \Phi(n) = \langle a^{\frac{n}{d}} \rangle$$

$$\Psi : \big\{1 \le k \le n \mid (n,k)=1\big\} \longrightarrow \big\{\textit{Γεννήτορες της } G\big\}, \quad \Psi(k) = \langle a^k \rangle$$

είναι 1-1 και επί. Επιπλέον: $\mathsf{o}(\Phi(d)) = d$ *και* $d_1 \mid d_2 \iff \Phi(d_1) \subseteq \Phi(d_2)$.

Πόρισμα 5.11. *(Διαδικασία εύρεσης Υποομάδων Πεπερασμένης Κυκλικής Ομάδας) Έστω $G = \langle a \rangle$ μια κυκλική ομάδα τάξης $\mathsf{o}(G) = \mathsf{o}(a) = n$.*

- *Υπολογίζουμε τους θετικούς διαιρέτες του n, έστω ότι αυτοί είναι: $d_1, d_2, \cdots, d_{\tau(n)}$.*
- *Για κάθε θετικό διαιρέτη $d_i \mid n$ του n, θεωρούμε την κυκλική υποομάδα $H_{d_i} = \langle a^{\frac{n}{d_i}} \rangle$ η οποία παράγεται από το στοιχείο $a^{\frac{n}{d_i}}$. Τότε η H_{d_i} είναι η μοναδική υποομάδα τάξης d_i της G.*
- *Οι υποομάδες $H_{d_1}, H_{d_2}, \cdots, H_{d_{\tau(n)}}$ είναι όλες οι διακεκριμμένες υποομάδες της G.*

Διαιρέτης του n	**Υποομάδα της G**	**Τάξη Υποομάδας**
d_1	$H_{d_1} = \langle a^{\frac{n}{d_1}} \rangle$	d_1
d_2	$H_{d_1} = \langle a^{\frac{n}{d_2}} \rangle$	d_2
$\vdots$	$\vdots$	$\vdots$
$d_{\tau(n)}$	$H_{d_{\tau(n)}} = \langle a^{\frac{n}{d_{\tau(n)}}} \rangle$	$d_{\tau(n)}$

- *Ισχύει:*

$$\forall i, j = 1, 2, \cdots, \tau(n): \quad H_{d_i} \leq H_{d_j} \iff d_i \mid d_j$$

Παράδειγμα 5.12. *Η κυκλική ομάδα $(\mathbb{Z}_{18}, +) = \langle [1] \rangle = \big\{[0], [1], [2], \cdots, [17]\big\}$, όπου $[k] = [k]_{18}$, $0 \leq k \leq 17$.*

- *Οι διαιρέτες του 18 είναι: $1, 2, 3, 6, 9, 18$ και άρα $\tau(18) = 6$. Επομένως θα έχουμε ακριβώς 6 υποομάδες $H_1, H_2, H_3, H_6, H_9, H_{18}$ στην $\mathbb{Z}_{18}$, ακριβώς μια για κάθε διαιρέτη του 18, με τάξη αντίστοιχα: $1, 2, 3, 6, 9, 18$. Αυτές οι υποομάδες περιγράφονται στον ακόλουθο πίνακα:*

Διαιρέτης του 18	**Υποομάδα της G**	**Τάξη Υποομάδας**
1	$H_1 = \langle \frac{18}{1}[1] \rangle = \langle 18[1] \rangle = \langle [18] \rangle = \langle [0] \rangle = \{[0]\}$	1
2	$H_2 = \langle \frac{18}{2}[1] \rangle = \langle 9[1] \rangle = \langle [9] \rangle$	2
3	$H_3 = \langle \frac{18}{3}[1] \rangle = \langle 6[1] \rangle = \langle [6] \rangle$	3
6	$H_6 = \langle \frac{18}{6} \rangle = \langle 3[1] \rangle = \langle [3] \rangle$	6
9	$H_9 = \langle \frac{18}{9}[1] \rangle = \langle 2[1] \rangle = \langle [2] \rangle$	9
18	$H_{18} = \langle \frac{18}{18}[1] \rangle = \langle [1] \rangle = \mathbb{Z}_{18}$	18

Για παράδειγμα:

$$H_6 = \langle [3] \rangle = \big\{[3], [6], [9], [12], [15], [0]\big\}$$

- *Οι αριθμοί k με $1 \leq k \leq 18$ και $(18, k) = 1$ είναι*

$$\varphi(18) = \varphi(23^2) = 18(1 - \frac{1}{2})(1 - \frac{1}{3}) = 18\frac{1}{2}\frac{2}{3} = 6$$

Πραγματικά:

$$\big\{1 \leq k \leq 18 \quad \text{και} \quad (18, k) = 1\big\} = \big\{1, 5, 7, 11, 13, 17\big\}$$

Επομένως οι γεννήτορες της $\mathbb{Z}_{18}$ είναι οι ακόλουθοι:

$$1[1] = [1], \quad 5[1] = [5], \quad 7[1] = [7], \quad 11[1] = [11], \quad 13[1] = [13], \quad 17[1] = [17]$$

• *Επειδή μεταξύ των διαιρετών* $d = 1, 2, 3, 6, 9, 18$ *του* 18 *έχουμε τις ακόλουθες, εκτός από τις προφανείς* $d \mid 18$*, σχέσεις διαιρετότητας:*

$$2 \mid 6, \qquad 3 \mid 6, \qquad 3 \mid 9$$

μεταξύ των υποομάδων $H_1, H_2, H_3, H_6, H_9, H_{18}$ *θα έχουμε τις ακόλουθες εγκλείσεις (εκτός από τις προφανείς* $H_d \leq \mathbb{Z}_{18} = H_{18}$ *και* $H_1 = \{[0]\} \leq H_d$*):*

$$H_2 \leq H_6, \qquad H_3 \leq H_6, \qquad H_3 \leq H_9$$

δηλαδή:

$$\langle [9] \rangle \ \leq \ \langle [3] \rangle, \qquad \langle [6] \rangle \ \leq \ \langle [3] \rangle, \qquad \langle [6] \rangle \ \leq \ \langle [2] \rangle$$

Άσκηση 280. *Διατυπώστε και αποδείξτε την ανάλογη εκδοχή της Πρότασης* 5.4 *για πεπερασμένες κυκλικές ομάδες.*

5.3. **Η Ομάδα των n-οστών ριζών της μονάδας.** Υπενθυμίζουμε ότι η ομάδα του κύκλου είναι η υποομάδα

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

της πολλαπλασιαστικής ομάδας $\mathbb{C}^*$ των μη-μηδενικών μιγαδικών αριθμών. Θα δούμε ότι η ομάδα $\mathbb{T}$ περιέχει κυκλικές ομάδες τάξης n, για κάθε $n \geq 1$.

Υπενθυμίζουμε ότι, $\forall n \geq 1$, ο μιγαδικός αριθμός $z \in \mathbb{C}$ καλείται μια n-**οστή ρίζα της μονάδας** αν: $z^n = 1$. Τότε:

$$z^n = 1 \implies |z|^n = 1 \implies |z| = 1 \ \text{ και } \ \exists\, \theta \in [0, 2\pi] : \ z = e^{i\theta}$$

και επομένως:

$$z^n = 1 \implies e^{in\theta} = 1 \implies \exists\, k \in \mathbb{Z} : \ n\theta = k2\pi \implies \theta = \frac{2\pi k}{n}$$

Άρα:

$$z^n = 1 \implies z = e^{\frac{2\pi i k}{n}}, \qquad \text{όπου} \qquad k \in \mathbb{Z}$$

Παρατηρούμε ότι η τιμή $e^{\frac{2\pi i k}{n}}$ εξαρτάται μόνο από την κλάση ισοδυναμίας του k modulo n:

$$[k]_n = [k']_n \implies n \mid k - k' \implies k - k' = nr, \quad \text{όπου} \quad r \in \mathbb{Z}$$

και άρα θα έχουμε:

$$e^{\frac{2\pi i k}{n}} = e^{\frac{2\pi i (k' + nr)}{n}} = e^{\frac{2\pi i k' + 2\pi i n r}{n}} = e^{\frac{2\pi i k'}{n}} e^{\frac{2\pi i n r}{n}} = e^{\frac{2\pi i k'}{n}} e^{2\pi i r} = e^{\frac{2\pi i k'}{n}}$$

Επομένως θέτοντας:

$$\zeta := e^{\frac{2\pi i}{n}}$$

θα έχουμε

$$\zeta^{qn+r} = \zeta^{qn} \zeta^r = (\zeta^n)^q \zeta^r = 1 \zeta^r = \zeta^r$$

και άρα το σύνολο των διακεκριμμένων n-οστών ριζών της μονάδας είναι:

$$\mathbb{U}_n = \big\{ \zeta^k = e^{\frac{2\pi i k}{n}} \ \in \mathbb{C} \mid 0 \leq k \leq n-1 \big\} = \big\{ 1, \zeta, \zeta^2, \cdots, \zeta^{n-1} \big\}$$

Επειδή προφανώς το σύνολο $\mathbb{U}_n$ είναι κλειστό στον πολλαπλασιασμό μηιγαδικών αριθμών, έπεται ότι το σύνολο $\mathbb{U}_n$ είναι μια υποομάδα της ομάδας $\mathbb{T}$ του κύκλου, και ιδιαίτερα η $\mathbb{U}_n$ είναι κυκλική διότι προφανώς:

$$\mathbb{U}_n = \langle \zeta \rangle = \big\{ 1, \zeta, \zeta^2, \cdots, \zeta^{n-1} \big\}$$

Μια n-οστή ρίζα της μονάδας καλείται **πρωταρχική n-οστή ρίζα της μονάδας** αν είναι γεννήτορας της $\mathbb{U}_n$.

Συνδυάζοντας τις παραπάνω παρατηρήσεις με τα αποτελέσματα της υπο-ενότητας 5.2, θα έχουμε το ακόλουθο αποτέλεσμα.

Πρόταση 5.13. *Το σύνολο $\mathbb{U}_n$ των n-οστών ριζών της μονάδας είναι μια κυκλική υποομάδα τάξης n της ομάδας του κύκλου $\mathbb{T}$:*

$$\mathbb{U}_n = \langle \zeta \rangle = \left\{1, \zeta, \zeta^2, \cdots, \zeta^{n-1}\right\}, \quad \text{όπου} \quad \zeta = e^{\frac{2\pi i}{n}}$$

Υπάρχουν ακριβώς $\varphi(n)$ πρωταρχικές n-οστές ρίζες της ομάδας, οι ακόλουθες:

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

5.4. **Κυκλικές Ομάδες - Ευθέα Γινόμενα.** Υπενθυμίζουμε ότι αν G και H είναι δύο ομάδες, τότε το **ευθύ γινόμενο** $G \times H$ των G και H είναι το σύνολο

$$G \times H = \left\{(g,h) \in G \times H \mid g \in G \ \ \& \ \ h \in H\right\}$$

το οποίο αποτελεί ομάδα όταν εφοδιασθεί με την πράξη:

$$(g_1, h_1)(g_2, h_2) := (g_1 g_2, h_1 h_2)$$

Σημειώνουμε ότι γράφοντας $g_1 g_2$ υπονοούμε την πράξη της G και γράφοντας $h_1 h_2$ υπονοούμε την πραξη της H. Το ουδέτερο στοιχείο της ομάδας $G \times H$ είναι το ζεύγος $(e_G, e_H$, όπου e_G είναι το ουδέτερο στοιχείο της G και e_H είναι το ουδέτερο στοιχείο της H. Τέλος το αντίστροφο του στοιχείου $(g,h) \in G \times H$ είναι το στοιχείο (g^{-1}, h^{-1}), όπου g^{-1} είναι το αντίστροφο του στοιχείου g στην G και h^{-1} είναι το αντίστροφο του στοιχείου h στην H.

Θεώρημα 5.14. *Έστω G και H δύο κυκλικές ομάδες.*

(1) *Αν μια από τις G και H είναι άπειρη κυκλική, τότε η ομάδα ευθύ γινόμενο $G \times H$ δεν είναι ποτέ κυκλική.*
(2) *Αν G και H είναι πεπερασμένες κυκλικές, τότε η ομάδα ευθύ γινόμενο $G \times H$ είναι κυκλική αν και μόνον αν:*

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

Απόδειξη. Υποθέτουμε ότι:

$$G = \langle a \rangle = \left\{a^k \in G \mid k \in \mathbb{Z}\right\} \qquad \text{και} \qquad H = \langle b \rangle = \left\{b^l \in H \mid l \in \mathbb{Z}\right\}$$

(1) Έστω ότι η ομάδα $G \times H$ είναι κυκλική και έστω $(x,y) \in G \times H$ ένας γεννήτορας της: $G \times H = \langle (x,y) \rangle$. Τότε:

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

Έστω $(a^k, b^l) \in G \times H$ ένα τυχσίο στοιχείο της $G \times H$, δηλαδή τα k, l είναι τυχαίοι ακέραιοι αριθμοί. Τότε θα έχουμε:

$$(a^k, b^l) = (x,y)^r = (a^i, b^j)^r = ((a^i)^r, (b^j)^r) = (a^{ir}, b^{jr}) \implies$$

$$a^k = a^{ir} \quad \text{και} \quad b^l = b^{jr} \implies a^{k-ir} = e_G \ \text{ και } \ b^{l-jr} = e_H$$

Αν μια από τις G και H είναι άπειρη ομάδα, για παράδειγμα η G, τότε επειδή ο γεννήτορας a της G έχει άπειρη τάξη θα έχουμε $k - ir = 0$ και άρα $k = ir$, δηλαδή $i \mid k$. Επειδή ο ακέραιος i είναι σταθερός και ο ακέραιος k είναι τυχαίος, έπεται ότι το i διαιρεί κάθε ακέραιο. Τότε προφανώς $i = 1$ και άρα θα έχουμε: $k = r$. Έτσι:

$$(a^k, b^l) = (a^k, b^{jk}) \implies b^{l-jk} = e_H$$

Αν η H είναι άπειρη, τότε το b έχει άπειρη τάξη και άρα $l = kj$, δηλαδή το j διαιρεί κάθε ακέραιο l και επομένως $j = 1$. Τότε $l = k$. Διαλέγοντας $k \neq l$, καταλήγουμε σε άτοπο. Αν η H είναι πεπερασμένη, έστω $\mathsf{o}(H) = \mathsf{o}(b) = m$. Τότε

$$b^{l-jk} = e_H \implies m \mid l - kj \implies \exists\, s \in \mathbb{Z}: \ l - kj = ms \implies l = kj + ms \implies l = (k, m)$$

Διαλέγοντας το l έτσι ώστε: $l \neq (k, m)$, καταλήγουμε σε άτοπο. Επομένως η ομάδα ευθύ γινόμενο $G \times H$ δεν μπορεί να είναι κυκλική.

(2) Υποθέτουμε ότι οι κυκλικές ομάδες G και H είναι πεπερασμένες, και έστω:

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

Υποθέτουμε πρώτα ότι $(n, m) = 1$. Θα δείξουμε ότι το στοιχείο (a, b) είναι γεννήτορας της $G \times H$. Επειδή η $G \times H$ έχει τάξη $mn < \infty$, έπεται ότι το στοιχείο (a, b) θα έχουε πεπερασμένη τάξη, έστω $\mathsf{o}((a, b)) = r$. Τότε $r \mid nm$, $(a, b)^r = (e_G, e_H)$ και επομένως $(a^r, b^r) = (e_G, e_H)$. Τότε $a^r = e_G$ και $b^r = e_H$. Τότε όμως θα έχουμε $\mathsf{o}(a) \mid r$ και $\mathsf{o}(b) \mid r$, δηλαδή: $n \mid r$ και $m \mid r$. Τότε όμως $[n, m] \mid r$ και επειδή $(n, m) = 1$, έπεται ότι $[n, m] = nm$ και άρα Θα έχουμε $nm \mid r$. Έτσι $\mathsf{o}((a, b)) = r = nm = \mathsf{o}(G \times H)$ και επομένως η κυκλική υποομάδα της $G \times H$ η οποία παράγεται από το στοιχείο (a, b) συμπίπτει με την $G \times H$, δηλαδή: $G \times H = \langle (a, b) \rangle$ και η $G \times H$ είναι κυκλική.

Αντίστροφα υποθέτουμε ότι η $G \times H$ είναι κυκλική και έστω $G \times H = \langle (x, y) \rangle$. Τότε $\mathsf{o}((x, y)) = nm$. Υποθέτουμε ότι $(n, m) = d \neq 1$. Τότε $d \mid n$ και $d \mid m$ και άρα: $\frac{n}{d}, \frac{m}{d} \in \mathbb{N}$. Τότε επειδή $x \in G$ και $\mathsf{o}(G) = n$, θα έχουμε $x^n = e_G$, και επειδή $x \in G$ και $\mathsf{o}(H) = m$, θα έχουμε $y^m = e_H$. Επομένως θα έχουμε:

$$(x, y)^{\frac{mn}{d}} = (x^{\frac{mn}{d}}, y^{\frac{mn}{d}}) = \left((x^n)^{\frac{m}{d}}, (y^m)^{\frac{n}{d}}\right) = \left((e_G)^{\frac{m}{d}}, (e_H)^{\frac{n}{d}}\right) = (e_G, e_H)$$

και άρα $mn \mid \frac{mn}{d}$, δηλαδή $mn \leq \frac{mn}{d}$ και επειδή $d \neq 1$ καταλήγουμε στο άτοπο $mn < \frac{mn}{d}$. Άρα $d = (m, n) = 1$. □

Παράδειγμα 5.15. *Η κυκλική ομάδα $\mathbb{Z}_{p^r} \times \mathbb{Z}_{q^s}$, $p \neq q$ πρώτοι αριθμοί, $r, s \geq 1$. Επειδή οι p, q είναι πρώτοι αριθμοί και $p \neq q$, έπεται ότι $(p^r, q^s) = 1$. Επομένως η ομάδα ευθύ γινόμενο $\mathbb{Z}_{p^r} \times \mathbb{Z}_{q^s}$ είναι κυκλική με τάξη $p^r q^s$:*

$$\mathbb{Z}_{p^r} \times \mathbb{Z}_{q^s} = \left\langle ([1]_{p^r}, [1]_{q^s}) \right\rangle$$

Επειδή οι διαιρέτες του $p^r q^s$ είναι σε πλήθος $\tau(p^r q^s) = (1 + r)(1 + s)$, δηλαδή οι αριθμοί

$$1, p, p^2, \cdots, p^r, q, q^2, \cdots, q^s, pq, pq^2, \cdots, pq^s, \ \cdots, \ p^r q, p^r q^2, \cdots, p^r q^s$$

έπεται ότι η κυκλική ομάδα $\mathbb{Z}_{p^r} \times \mathbb{Z}_{q^s}$ έχει $(1 + r)(1 + s)$ υποομάδες, μια και μόνου μια υποομάδα τάξης $p^i q^j$, οπου $0 \leq i \leq r$ και $0 \leq j \leq s$.

Από την άλλη πλευρά, επειδή

$$\varphi(p^r q^s) = p^r q^s (1 - \frac{1}{p})(1 - \frac{1}{q}) = p^{r-1}(p - 1) q^{s-1}(q - 1)$$

έπεται ότι η κυκλική ομάδα $\mathbb{Z}_{p^r} \times \mathbb{Z}_{q^s}$ θα έχει $p^{r-1}(p - 1)q^{s-1}(q - 1)$ το πλήθος γεννήτορες.

5.5. **Ταξινόμηση Κυκλικών Ομάδων.** Στην παρούσα υπο-ενότητα θα δούμε την ταξινόμηση των κυκλικών ομάδων, μέσω οικείων μοντέλων.

Υπενθυμίζουμε ότι:

(1) Η ομάδα $(\mathbb{Z}, +)$ είναι μια άπειρη κυκλική ομάδα.
(2) $\forall n \geq 2$, η ομάδα $(\mathbb{Z}_n, +)$ είναι κυκλική τάξης n.

Ιδιαίτερα θα δούμε ότι κάθε άπειρη κυκλική ομάδα είναι «ισόμορφη» με την $(\mathbb{Z}, +)$, και κάθε πεπερασμένη κυκλική ομάδα τάξης n είναι «ισόμορφη» με την $(\mathbb{Z}_n, +)$.

Ορισμός 5.16. *Μια απεικόνιση $f : G \longrightarrow G'$ μεταξύ δύο ομάδων G και G' καλείται* **ισομορφισμός** *αν:*

(1) *Η f είναι 1-1 και επί.*

(2) $\forall x, y \in G$: $f(xy) = f(x)f(y)$.

Η δεύτερη συνθήκη του παραπάνω ορισμού δείχνει ότι ένας ισομορφισμός $f : G \longrightarrow G'$ στέλνει γινόμενα xy στοιχείων x, y της G σε γινόμενα $f(x)f(y)$ των εικόνων $f(x), f(y)$ των στοιχείων x, y μέσω της f στην G'.

Σημειώνουμε ότι, χάριν ευκολίας του συμβολισμού, συμβολίζουμε με το ίδιο σύμβολο την πράξη στις ομάδες G και G'. Γενικά αν $\star$ είναι η πράξη της G και $\circ$ η πράξη της G', τότε η συνθήκη (2) του Ορισμού 5.16 γράφεται: $f(x \star y) = f(x) \circ f(y)$.

Άσκηση 281. *Έστω $f : G \longrightarrow H$ ένας ισομορφισμός μεταξύ δύο ομάδων G και H. Τότε να δείξετε ότι η απεικόνιση $f^{-1} : H \longrightarrow G$ είναι ισομορφισμός.*

Συμβολίζουμε με $\mathbf{Grp}$ τη συλλογή όλων των ομάδων.

Άσκηση 282. *Να δείξετε ότι η ακόλουθη σχέση στη συλλογή $\mathbf{Grp}$:*

$$\forall G_1, G_2 \in \mathbf{Grp}: \quad G_1 \cong G_2 \quad \Longleftrightarrow \quad \text{υπάρχει ισομορφισμός} \quad f : G_1 \longrightarrow G_2$$

είναι μια σχέση ισοδυναμίας επί της συλλογής $\mathbf{Grp}$.

Δύο ομάδες G_1 και G_2 καλούνται **ισόμορφες** *αν $G_1 \cong G_2$.*

Όπως θα δούμε αργότερα ισόμορφες ομάδες έχουν τις ίδιες δομικές ιδιότητες και το μόνο που τις διαφοροποιεί είναι η ενδεχόμενη διαφορετική φύση, όνομα, συμβολισμός, των στοιχείων τους ή της πράξης με την οποία είναι εφοδιασμένη η κάθε μια.

Θεώρημα 5.17. *Έστω G μια κυκλική ομάδα.*

(1) *Αν η G είναι άπειρη, τότε η G είναι ισόμορφη με την προσθετική ομάδα των ακεραίων:*

$$G \ \cong \ (\mathbb{Z}, +)$$

(2) *Αν η G είναι πεπερασμένη τάξης n, τότε η G είναι ισόμορφη με την προσθετική ομάδα των ακεραίων modulo n:*

$$G \ \cong \ (\mathbb{Z}_n, +)$$

(3) *Δύο κυκλικές ομάδες είναι ισόμορφες αν και μόνιν αν έχουν την ίδια τάξη:*

$$G_1 \cong G_2 \ \Longleftrightarrow \ \mathsf{o}(G_1) = \mathsf{o}(G_2)$$

Απόδειξη. Βλέπε Θεωρήματα 14.1, 14.4, και 14.7. □

Για περισσότερες λεπτομέρειες αναφορικά με τις βασικές ιδιότητες ομομορφισμών και ισομορφισμών ομάδων, παραπέμπουμε στις ενότητες 13, 14, και 15.

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.

Σημειώματα

Σημείωμα Αναφοράς

Σημείωμα Αδειοδότησης