ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΪΚΑ ΜΑΘΗΜΑΤΑ

Τίτλος Μαθήματος: Αλγεβρικές Δομές Ι

Ενότητα: Ταξινόμηση Κυκλικών Ομάδων και Ομάδες Αυτομορφισμών

Διδάσκων: Καθηγητής Νικόλαος Μαρμαρίδης, Καθηγητής Ιωάννης Μπεληγιάννης

Τμήμα: Μαθηματικών

---

14. **Ταξινόμηση Κυκλικών Ομάδων και Ομάδες Αυτομορφισμών**

Στην παρούσα ενότητα θα ταξινομήσουμε τις κυκλικές ομάδες ως προς τη σχέση ισομορφίας. Επίσης θα αποδείξουμε ένα σημαντικό κριτήριο ισομορφίας κυκλικών ομάδων. Τέλος θα μελετήσουμε εν συντομία τη δομή του συνόλου των ομομορφισμών και ισομορφισμών μεταξύ κυκλικών ομάδων.

14.1. **Ταξινόμηση Άπειρων Κυκλικών Ομάδων.**

Στην παρούσα ενότητα θα ταξινομήσουμε τις κυκλικές ομάδες άπειρης τάξης και θα περιγράψουμε την κλάση ισομορφίας τους.

Θεώρημα 14.1. *Κάθε άπειρη κυκλική ομάδα G είναι ισόμορφη με την προσθετική ομάδα $(\mathbb{Z},+)$ των ακεραίων.*

Απόδειξη. Έστω $G=\langle a\rangle=\{a^n\in G\mid n\in\mathbb{Z}\}$, όπου $\mathsf{o}(a)=\infty$. Ορίζουμε απεικόνιση

$$f:\mathbb{Z}\longrightarrow G,\quad f(n)=a^n$$

Θα έχουμε:

$$f(n+m)=a^{n+m}=a^na^m=f(n)f(m)$$

Αν $f(n)=f(m)$, τότε $a^n=a^m$ και άρα $a^{n-m}=e$. Επειδή $\mathsf{o}(a)=\infty$, θα έχουμε αναγκαστικά $n-m=0$ και άρα $n=m$. Δηλαδή η f είναι 1-1. Αν $x\in G$, τότε $x=a^k$ για κάποιον ακέραιο $k\in\mathbb{Z}$. Τότε $f(k)=a^k=x$, και επομένως η f είναι επί. Άρα η f είναι ισομορφισμός και επομένως η G είναι ισόμορφη με την $(\mathbb{Z},+)$. □

Θεώρημα 14.2. *Δύο άπειρες κυκλικές ομάδες είναι ισόμορφες.*

Απόδειξη. Έστω

$$G_1=\langle a\rangle=\{a^n\in G_1\mid n\in\mathbb{Z}\}\quad\text{και}\quad G_2=\langle b\rangle=\{b^m\in G_2\mid m\in\mathbb{Z}\}$$

δύο άπειρες κυκλικές ομάδες. Τότε από το Θεώρημα 14.1 οι ομάδες G_1 και G_2 είναι και οι δύο ισόμορφες με την $(\mathbb{Z},+)$ και άρα οι G_1 και G_2 είναι ισόμορφες διότι η σχέση ισομορφίας είναι σχέση ισοδυναμίας στην συλλογή όλων των ομάδων.

Διαφορετικά: Ορίζουμε απεικόνιση

$$f:G_1\longrightarrow G_2,\qquad f(a^n)=b^n$$

Τότε

$$f(a^na^m)=f(a^{n+m})=b^{n+m}=b^nb^m=f(a^n)f(a^m)$$

και άρα η f είναι ομομορφισμός. Επιπλέον η f είναι ισομορφισμός, διότι χρησιμοποιώντας την περιγραφή των συνόλων G_1 και G_2 και το γεγονός ότι οι γεννήτορες a,b έχουν άπειρη τάξη, θα έχουμε:

$$f(a^n)=f(a^m)\implies b^n=b^m\implies n=m\implies a^n=a^m\implies f:\ \text{1-1}$$

$$\forall\, b^m\in G_2:\ \ f(a^m)=b^m\implies f:\ \text{επί}$$

□

Υπενθυμίζουμε ότι η σχέση ισομορφίας " $\cong$ " στο σύνολο $\mathbf{Grp}$ όλων των ομάδων είναι μια σχέση ισοδυναμίας και αν G είναι μια ομάδα, τότε $[G]_{\cong}$ συμβολίζει την κλάση ισομορφίας της G.

Θεώρημα 14.3.

$$[(\mathbb{Z},+)]_{\cong}=\{G\in\mathbf{Grp}\mid G:\ \textit{άπειρη κυκλική}\}$$

Απόδειξη. Αν G είναι μια άπειρη κυκλική ομάδα, τότε από το Θεώρημα 14.1, έπεται ότι $G \cong (\mathbb{Z}, +)$ και άρα $G \in [(\mathbb{Z}, +)]_{\cong}$. Αντίστροφα αν $G \in [(\mathbb{Z}, +)]_{\cong}$, τότε η G είναι ισόμορφη με την $(\mathbb{Z}, +)$ και τότε η G είναι άπειρη κυκλική ομάδα διότι: έστω $f\colon \mathbb{Z} \xrightarrow{\cong} G$ ένας ισομορφισμός με αντίστροφο ισομορφισμό f^{-1}. Θέτουμε $f(1) = a$. Τότε $G = \langle a \rangle$, διότι έστω $x \in G$. Τότε $f^{-1}(x) \in \mathbb{Z}$ και άρα $f^{-1}(x) = n$. Θα έχουμε $x = f(f^{-1}(x)) = f(n) = f(n1) = f(1)^n = a^n \in \langle a \rangle$. Επομένως $G = \langle a \rangle$ και η G είναι κυκλική με γεννήτορα το a η οποία είναι προφανώς άπειρη. □

Κλείνουμε την παρούσα υπο-ενότητα με μια ενδιαφέρουσα ιδιότητα των άπειρων κυκλικών ομάδων.

Πρόταση 14.4. *Έστω $F = \langle a \rangle$ μια άπειρη κυκλική ομάδα. Τότε για κάθε ομάδα G και $x \in G$, υπάρχει μοναδικός ομομορφισμός $f\colon F \longrightarrow G$ έτσι ώστε: $f(a) = x$.*

Απόδειξη. Θεωρούμε την απεικόνιση

$$f:\ F \longrightarrow G, \quad f(a^n) = x^n$$

Τότε η αεπικόνιση f είναι προφανλώς καλά ορισμένη και είναι ομομορφισμός, διότι: $f(a^n a^m) = f(a^{n+m}) = x^{n+m} = x^n x^m = f(a^n) f(a^m)$. Ο ομομορφισμός f είναι μοναδικός, διότι αν $g\colon F \longrightarrow G$ είναι ένας άλλος ομομορφισμός με την ιδιότητα $g(a) = x$, τότε $g(a^n) = g(a)^n = x^n = f(a^n)$, $\forall n' \in \mathbb{Z}$. Επομένως $f = g$. □

14.2. **Ταξινόμηση Πεπερασμένων Κυκλικών Ομάδων.** Στην παρούσα ενότητα θα ταξινομήσουμε τις κυκλικές ομάδες πεπερασμένης τάξης και θα περιγράψουμε την κλάση ισομορφίας κάθε κυκλικής ομάδας τάξης n, $\forall n \geq 1$.

Θεώρημα 14.5. *Κάθε πεπερασμένη κυκλική ομάδα τάξης $n \geq 1$ είναι ισόμορφη με την προσθετική ομάδα $(\mathbb{Z}_n, +)$ των ακεραίων modulo n.*

Απόδειξη. Έστω $G = \langle a \rangle = \{e, a, a^2, \cdots, a^{n-1}\}$, όπου $\mathsf{o}(a) = n$. Ορίζουμε απεικόνιση

$$f:\ \mathbb{Z}_n \longrightarrow G, \quad f([k]_n) = a^k$$

Δείχνουμε ότι η f είναι καλά ορισμένη. Έστω $[k]_n = [k']_n$ και επομένως $n \mid k - k'$. Έτσι $k - k' = nr$, για κάποιο $r \in \mathbb{Z}$. Τότε:

$$a^{k-k'} = a^{nr} = (a^n)^r = e^r = e \implies a^k a^{-k'} = e \implies a^k = a^{k'} \implies f([k]_n) = f([k']_n)$$

Επομένως η f είναι καλά ορισμένη και επιπλέον η f είναι ομομορφισμός, διότι:

$$f([k]_n + [l]_n) = f([k+l]_n) = a^{k+l} = a^k a^l = f([k]_n) f([l]_n)$$

Αν $f([k]_n) = f([l]_n)$, όπου $0 \leq k, l \leq n-1$, τότε $a^k = a^l$ και άρα $a^{k-l} = e$. Επειδή $\mathsf{o}(a) = n$, θα έχουμε αναγκαστικά $n \mid k - l$ και άρα $[k]_n = [l]_n$. Δηλαδή η f είναι 1-1. Επειδή η f είναι προφανώς επί, έπεται ότι η f είναι ισομορφισμός και άρα η G είναι ισόμορφη με την $(\mathbb{Z}_n, +)$. □

Θεώρημα 14.6. *Δύο πεπερασμένες κυκλικές ομάδες ίδιας τάξης είναι ισόμορφες.*

Απόδειξη. Έστω

$$G_1 = \langle a \rangle = \{e,\ a,\ a^2,\ \cdots,\ a^{n-1}\} \quad \text{και} \quad G_2 = \langle b \rangle = \{e,\ b,\ b^2,\ \cdots,\ b^{n-1}\}$$

δύο κυκλικές ομάδες τάξης n. Τότε από το Θεώρημα 14.5 οι ομάδες G_1 και G_2 είναι και οι δύο ισόμορφες με την $(\mathbb{Z}_n, +)$ και άρα οι G_1 και G_2 είναι ισόμορφες διότι η σχέση ισομορφίας είναι σχέση ισοδυναμίας στην συλλογή όλων των ομάδων.

Διαφορετικά: Ορίζουμε απεικόνιση

$$f:\ G_1 \longrightarrow G_2, \qquad f(a^k) = b^k, \qquad 0 \leq k \leq n-1$$

Τότε εύκολα βλέπουμε ότι η f είναι ένας ισομορφισμός ομάδων. □

Θα περιγραψουμε τώρα την κλάση ισομορφίας μιας κυκλικής ομάδας τάξης n.

Θεώρημα 14.7.

$$[(\mathbb{Z}_n, +)]_{\cong} = \big\{G \in \mathbf{Grp} \mid G:\ \textit{κυκλική τάξης}\ n\big\}$$

Απόδειξη. Αν G είναι μια πεπερασμένη κυκλική ομάδα τάξης n, τότε από το Θεώρημα 14.5, έπεται ότι $G \cong (\mathbb{Z}_n, +)$ και άρα $G \in [(\mathbb{Z}_n, +)]_{\cong}$. Αντίστροφα αν $G \in [(\mathbb{Z}_n, +)]_{\cong}$, τότε η G είναι ισόμορφη με την $(\mathbb{Z}_n, +)$ και τότε η G είναι μια πεπερασμένη κυκλική ομάδα τάξης n, διότι: έστω $f\colon \mathbb{Z}_n \xrightarrow{\cong} G$ ένας ισομορφισμός με αντίστροφο ισομορφισμό f^{-1}. Θέτουμε $f([1]_n) = a$. Τότε $G = \langle a\rangle$, διότι έστω $x \in G$. Τότε $f^{-1}(x) \in \mathbb{Z}_n$ και άρα $f^{-1}(x) = [k]_n$. Θα έχουμε $x = f(f^{-1}(x)) = f([k]_n) = f(k[1]_n) = f([1]_n)^k = a^k \in \langle a\rangle$. Επομένως $G = \langle a\rangle$ και η G είναι κυκλική με γεννήτορα το a η οποία είναι προφανώς πεπερασμένη τάξης n. □

14.3. **Κριτήριο Ισομορφίας Κυκλικών Ομάδων.** Το ακόλουθο σημαντικό κριτήριο ισομορφίας κυκλικών ομάδων είναι άμεση συνέπεια των παραπάνω Θεωρημάτων.

Θεώρημα 14.8. *Δύο κυκλικές ομάδες είναι ισόμορφες αν και μόνον αν έχουν την ίδια τάξη:*

$$\textit{Αν}\ G_1,\ G_2\ \textit{είναι κυκλικές ομάδες, τότε:}\ \ G_1 \cong G_2 \iff \mathsf{o}(G_1) = \mathsf{o}(G_2)$$

Απόδειξη. Αν οι ομάδες G_1 και G_2 είναι ισόμορφες, τότε ιδιαίτερα οι G_1 και G_2 έχουν την ίδια τάξη διότι υπάρχει μια 1-1 και επί απεικόνιση μεταξύ αυτών. Αντίστροφα έστω $\mathsf{o}(G_1) = \mathsf{o}(G_2) := n$. Αν $n = \infty$, τότε από το Θεώρημα 14.2, οι ομάδες G_1 και G_2 είναι ισόμορφες με την $(\mathbb{Z}, +)$. Άρα και μεταξύ τους ισόμορφες. Αν $n < \infty$, τότε από το Θεώρημα 14.6, οι ομάδες G_1 και G_2 είναι ισόμορφες με την $(\mathbb{Z}_n, +)$, και άρα οι G_1 και G_2 είναι και μεταξύ τους ισόμορφες. □

Θέτοντας $\mathbb{Z}_1 = \{e\}$ να είναι η τετριμμένη ομάδα η οποία προφανώς είναι κυκλική, τα προηγούμενα αποτελέσματα δείχνουν ότι οι κυκλικές ομάδες, «μέχρι ισομορφισμό», είναι οι εξής:

$$\mathbb{Z}, \quad \text{και} \quad \mathbb{Z}_1,\ \mathbb{Z}_2,\ \mathbb{Z}_3,\ \cdots,\ \mathbb{Z}_n,\ \cdots$$

14.4. **Ομάδες Ομομορφισμών Κυκλικών Ομάδων.** Στην παρούσα υπο-ενότητα θα μελετήσουμε ομομορφισμούς μεταξύ κυκλικών ομάδων.

Πρόταση 14.9. *Έστω $G = \langle a\rangle$ μια κυκλική ομάδα, και έστω $f\colon G \longrightarrow G$ μια απεικόνιση. Τότε τα ακόλουθα είναι ισοδύναμα:*

(1) *Η f είναι ένας ενδομορφισμός της G.*
(2) *Υπάρχει ακέραιος $k \in \mathbb{Z}$:*

$$\forall g \in G: \quad f(g) = g^k$$

Απόδειξη. (2) $\Longrightarrow$ (1) Δείχνουμε ότι η απεικόνιση $f(g) = g^k$ είναι ομομορφισμός. Επειδή η G είναι αβελιανή, θα έχουμε:

$$f(g_1g_2) = (g_1g_2)^k = g_1^k g_2^k = f(g_1)f(g_2)$$

και άρα η f είναι ομομορφισμός ομάδων, δηλαδή η f είναι ένας ενδομορφισμός της G.

(1) $\Longrightarrow$ (2) Έστω ότι η f είναι ενδομορφισμός. Τότε $f(a) \in G = \langle a \rangle$ και άρα υπάρχει $k \in \mathbb{Z}$ έτσι ώστε: $f(a) = a^k$. Θα δείξουμε ότι $f(g) = g^k$, $\forall g \in G$. Θα έχουμε $g = a^r$ για κάποιο $r \in \mathbb{Z}$. Χρησιμοποιώντας ότι η f είναι ενδομορφισμός, θα έχουμε:

$$f(g) = f(a^r) = f(a)^r = (a^k)^r) = a^{kr} = (a^r)^k = g^k \qquad \square$$

Σημειώνουμε ότι, η G είναι άπειρη κυκλική, τότε το $k \in \mathbb{Z}$ είναι μοναδικό διότι αν $f(a) = a^l$, τότε $a^k = a^l$ και άρα $a^{k-l} = e$ το οποίο σημαίνει ότι $k = l$ διότι το a έχει άπειρη τάξη. Αν η G είναι πεπερασμένη κυκλική, με τάξη n, τότε θα έχουμε αν $f(a) = a^l = a^k$, τότε $a^{k-l} = e$ και άρα $\mathsf{o}(a) = n \mid k - l$ το οποίο σημαίνει ότι το k είναι μοναδικό modulo n.

Συμβολισμός 14.10. *Αν G και G' είναι δύο ομάδες, τότε συμβολίζουμε με*

$$\mathsf{Hom}(G, G') = \left\{ f \colon G \longrightarrow G' \;\mid\; f : \;\; \textit{ομομορφισμός} \right\}$$

το σύνολο όλων των ομομορφισμών από την G στην G'.

Αν $G = G'$, τότε συμβολιζουμε με:

$$\mathsf{End}(G) = \mathsf{Hom}(G, G)$$

το σύνολο όλων των ενδομορφισμών της G.

Σκοπός μας είναι να υπολογίσουμε την δομή του συνόλου $\mathsf{Hom}(G, H)$ των ομομορφισμών μεταξύ κυκλικών ομάδων G και H. Γενικά το σύνολο $\mathsf{Hom}(G, H)$ των ομομορφισμών μεταξύ ομάδων G και H δεν έχει δομή ομάδας. Η επόμενη Πρόταση δείχνει ότι όταν η ομάδα H είναι αβελιανή, τότε το σύνολο $\mathsf{Hom}(G, H)$ μπορεί να εφοδιασθεί με δομή ομάδας.

Πρόταση 14.11. *Αν $(G, \circ)$ και $(G', \cdot)$ είναι δύο ομάδες, και υποθέτουμε ότι η G' είναι αβελιανή.*

(1) *Το σύνολο $\mathsf{Hom}(G, G')$ αποτελεί αβελιανή ομάδα με πράξη:*

$$\star : \;\; \mathsf{Hom}(G, G') \times \mathsf{Hom}(G, G') \longrightarrow \mathsf{Hom}(G, G'), \quad (f, g) \longmapsto \quad f \star g : G \longrightarrow G', \;\; (f \star g)(x) = f(x) \cdot g(x)$$

(2) *Το ουδέτερο στοιχείο της $\mathsf{Hom}(G, G')$ είναι ο ομομορφισμός*

$$\epsilon : \; G \longrightarrow G', \quad x \longmapsto \epsilon(x) = e_{G'}$$

(3) *Το αντίστροφο στοιχείο του ομομορφισμού $f \in \mathsf{Hom}(G, G')$ είναι ο ομομορφισμός*

$$\widetilde{f} : \; G \longrightarrow G, \quad x \longmapsto \widetilde{f}(x) = f(x)^{-1}$$

Απόδειξη. (1) Η πράξη $\star$ είναι καλά ορισμένη, δηλαδή, $\forall f, g \in \mathsf{Hom}(G, G')$: $f \star g \in \mathsf{Hom}(G, G')$. Πράγματι, έστω $x, y \in G$. Τότε θα έχουμε:

$$(f \star g)(x \circ y) = f(x \circ y) \cdot g(x \circ y) = f(x) \cdot f(y) \cdot g(x) \cdot g(y) = f(x) \cdot g(x) \cdot f(y) \cdot g(y) = (f \star g)(x) \cdot (f \star g)(y)$$

και άρα η απεικόνιση $f \star g$ ανήκει στο σύνολο $\mathsf{Hom}(G, G')$.

(2) Προσεταιριστικότητα: Έστω $f, g, h \colon G \longrightarrow G'$. Τότε $\forall x \in G$:

$$(f \star (g \star h))](x) = f(x) \cdot (g \star h)(x) = f(x) \cdot (g(x) \cdot h(x)) = (f(x) \cdot g(x)) \cdot h(x) = ((f \star g)(x)) \cdot h(x) = [(f \star g) \star h](x)$$

Επομένως $f \star (g \star h) = (f \star g) \star h$ και η πράξη $\star$ είναι προσεταιριστική στο σύνολο $\mathsf{Hom}(G, G')$.

(3) Ύπαρξη Ουδετέρου Στοιχείου: Έστω $f \colon G \longrightarrow G'$. Τότε $\forall x \in G$:

$$(f \star \epsilon)(x) = f(x) \cdot \epsilon(x) = f(x) \cdot e_{G'} = f(x) = e_{G'} \cdot f(x) = \epsilon(x) \cdot f(x) = (\epsilon \star f)(x)$$

και άρα: $f \star \epsilon = f = \epsilon \star f$. Δηλαδή ο τετριμμένος ομομορφισμός $\epsilon \in \mathsf{Hom}(G, G')$ είναι ουδέτερο στοιχείο για την πράξη $\star$.

(4) Ύπαρξη Αντιστρόφου Στοιχείου: Έστω $f: G \longrightarrow G'$. Δείχνουμε πρώτα ότι η απεικόνιση $\widetilde{f}: G \longrightarrow G$, $\widetilde{f}(x) = f(x)^{-1}$, $\forall x \in G$, είναι ομομορφισμός ομάδων. Πραγματικά, χρησιμοποιώντας ότι η f είναι ομομορφισμός και ότι η G' είναι αβελιανή, θα έχουμε:

$$\widetilde{f}(x \circ y) = f(x \circ y)^{-1} = (f(x) \cdot f(y))^{-1} = f(y)^{-1} \cdot f(x)^{-1} = f(x)^{-1} \cdot f(y)^{-1} = \widetilde{f}(x) \cdot \widetilde{f}(y)$$

επομένως η $\widetilde{f}$ είναι ομομορφισμός ομάδων και άρα $\widetilde{f} \in \mathsf{Hom}(G, G')$.

Επιπρόσθετα $\forall x \in G$:

$$(f \star \widetilde{f})(x) = f(x) \cdot \widetilde{f}(x) = f(x) \cdot f(x)^{-1} = e_{G'} = \epsilon(x) = e_{G'} = f(x)^{-1} \cdot f(x) = \widetilde{f}(x) \cdot f(x) = (\widetilde{f} \star f)(x)$$

και επομένως $f \star \widetilde{f} = \epsilon = \widetilde{f} \star f$. Δηλαδή ο ομομορφισμός $\widetilde{f}$ είναι το αντίστροφο στοιχείο του ομομορφισμού f για την πράξη $\star$ στο σύνολο $\mathsf{Hom}(G, G')$.

(5) Μεταθετικότητα: Έστω $f, g \in \mathsf{Hom}(G, G')$. Τότε $\forall x \in G$:

$$(f \star g)(x) = f(x) \cdot g(x) = g(x) \cdot f(x) = (g \star f)(x)$$

και επομένως $f \star g = g \star f$, δηλαδή η πράξη $\star$ στο σύνολο $\mathsf{Hom}(G, G')$ είναι μεταθετική. □

Παράδειγμα 14.12. *Επειδή κάθε κυκλική ομάδα είναι αβελιανή, από την προηγούμενη πρόταση έπεται ότι, αν G, H είναι αβελιανές ομάδες, τότε το σύνολο $\mathsf{Hom}(G, H)$ αποτελεί μια αβελιανή ομάδα. Ιδιαίτερα, $\forall n, m \geq 1$, τα σύνολα:*

$$\mathrm{End}(\mathbb{Z}) = \mathsf{Hom}(\mathbb{Z}, \mathbb{Z}), \quad \mathsf{Hom}(\mathbb{Z}, \mathbb{Z}_n), \quad \mathsf{Hom}(\mathbb{Z}_n, \mathbb{Z}), \quad \mathsf{Hom}(\mathbb{Z}_n, \mathbb{Z}_m)$$

είναι αβελιανές ομάδες. Όλες οι παραπάνω ομάδες είναι προσθετικές. Έτσι η δομή αβελιανής ομάδας σε κάθε ένα από τα παραπάνω σύνολα, όπως προκύπτει από την Πρόταση 14.11*, θα είναι μέσω της ακόλουθης πράξης πρόσθεσης ομομορφισμών, όπου f, g είναι ομομορφισμοί σε κάθε ένα από τα παραπάνω τέσσερα σύνολα, και x ανήκει στο πεδίο ορισμού τους:*

$$(f + g)(x) = f(x) + g(x)$$

Το κεντρικό αποτέλεσμα της παρούσης υπο-ενότητας είναι το ακόλουθο Θεώρημα, το οποίο δείχνει ότι οι ομάδες ομομορφισμών μεταξύ κυκλικών ομάδων είναι κυκλικές και επιπρόσθετα δίνει την ακριβή κλάση ισομορφίας τους.

Θεώρημα 14.13. (1)

$$\mathsf{Hom}(\mathbb{Z}, \mathbb{Z}) \xrightarrow{\cong} \mathbb{Z}$$

(2)

$$G \text{ πεπερασμένη αβελιανή ομάδα, π.χ. } G = \mathbb{Z}_n, \implies \mathsf{Hom}(G, \mathbb{Z}) \xrightarrow{\cong} \{e\}$$

(3)

$$\mathsf{Hom}(\mathbb{Z}, \mathbb{Z}_n) \xrightarrow{\cong} \mathbb{Z}_n$$

(4)

$$\mathsf{Hom}(\mathbb{Z}_n, \mathbb{Z}_m) \xrightarrow{\cong} \mathbb{Z}_{(n,m)}$$

Απόδειξη. (1) Ορίζουμε απεικονίσεις

$$\Phi: \mathsf{Hom}(\mathbb{Z}, \mathbb{Z}) \longrightarrow \mathbb{Z}, \quad \Phi(f) = f(1)$$
$$\Psi: \mathbb{Z} \longrightarrow \mathsf{Hom}(\mathbb{Z}, \mathbb{Z}), \quad \Psi(n) = f_n$$

όπου

$$f_n: \mathbb{Z} \longrightarrow \mathbb{Z}, \quad f_n(m) = nm$$

Από την Πρόταση 14.9, έπεται ότι η απεικόνιση f_n είναι ενδομορφισμός της ομάδας $(\mathbb{Z}, +)$, $\forall n \in \mathbb{Z}$. Δείχνουμε ότι οι απεικονίσεις Φ και Ψ είναι ισομορφισμοί και $\Psi = \Phi^{-1}$.

(α) Θα έχουμε:

$$\forall n \in \mathbb{Z}: \quad \Phi\Psi(n) = \Phi(f_n) = f_n(1) = n1 = n \quad \Longrightarrow \quad \Phi\Psi = \mathrm{Id}_{\mathbb{Z}}$$

$$\forall f \in \mathsf{Hom}(\mathbb{Z},\mathbb{Z}): \quad \Psi\Phi(f) = \Psi(f(1)) = f_{f(1)}$$

όμως $\forall m \in \mathbb{Z}: \quad f_{f(1)}(m) = f(1)m = f(1m) = f(m) \quad \Longrightarrow \quad f_{f(1)} = f \quad \Longrightarrow \quad \Psi\Phi(f) = f$

Επομένως:

$$\Psi\Phi = \mathrm{Id}_{\mathsf{Hom}(\mathbb{Z},\mathbb{Z})}$$

Άρα οι απεικονίσεις Φ και Ψ είναι 1-1 και επί και $\Psi = \Phi^{-1}$.

(β) Δείχνουμε ότι η Φ είναι ομομορφισμός ομάδων:

$$\Phi(f+g) = (f+g)(1) = f(1) + g(1) = \Phi(f) + \Phi(g)$$

Άρα η Φ είναι ισομορφισμός αβελιανών ομάδων με αντίστροφο τον ομομορφισμό Ψ.

(2) Έστω G μια πεπερασμένη αβελιανή (πολλαπλασιαστική) ομάδα. Τότε κάθε στοιχείο της G θα έχει πεπερασμένη τάξη:

$$\forall a \in G, \ \ \exists n \geq 1: \quad a^n = e$$

Αν $f \in \mathsf{Hom}(G,\mathbb{Z})$ είναι ένας ομομορφισμός, τότε:

$$\forall a \in G: \ \ 0 = f(e) = f(a^n) = nf(a) \ \ \Longrightarrow \ \ n = 0 \ \ \text{ή} \ \ f(a) = 0 \ \ \Longrightarrow \ \ f(a) = 0$$

Άρα ο μοναδικός ομομορφισμός $f \in \mathsf{Hom}(G,\mathbb{Z})$ είναι ο τετριμμένος $f = \varepsilon\colon G \longrightarrow \mathbb{Z}$, $\varepsilon(a) = 0$, ο οποίος είναι το ταυτοτικό στοιχείο της αβελιανής ομάδας $\mathsf{Hom}(G,\mathbb{Z})$. Επομένως

$$\mathsf{Hom}(G,\mathbb{Z}) = \{\varepsilon\} \ \ \xrightarrow{\cong} \ \ \{e\}$$

(3) Ορίζουμε απεικονίσεις

$$\Phi: \ \mathsf{Hom}(\mathbb{Z},\mathbb{Z}_n) \ \longrightarrow \ \mathbb{Z}_n, \quad \Phi(f) = f(1)$$

Επειδή $\Phi(f+g) = (f+g)(1) = f(1)+g(1) = \Phi(f)+\Phi(g)$, έπεται ότι η Φ είναι ομομορφισμός ομάδων. Επιπλέον η Φ είναι μονομορφισμός διότι:

$$\Phi(f) = [0]_n \ \ \Longrightarrow \ \ f(1) = [0]_n \ \ \text{και τότε:} \ \forall m \in \mathbb{Z} \ \ f(m) = f(m1) = mf(1) = m[0]_n = [0m]_n = [0]_n$$

Επομένως ο ομομορφισμός f είναι ο τετριμμένος $f = \varepsilon\colon G \longrightarrow \mathbb{Z}$, $\varepsilon(a) = 0$, ο οποίος είναι το ταυτοτικό στοιχείο της αβελιανής ομάδας $\mathsf{Hom}(\mathbb{Z},\mathbb{Z}_n)$. Αυτό σημαίνει ότι ο ομομορφσιμός Φ είναι μονομορφισμός.

Μένει να δείξουμε ότι ο μονομορφισμός Φ είναι επιμορφισμός. Έστω $[k]_n \in \mathbb{Z}_n$. Ορίζουμε μια απεικόνιση

$$f_{[k]_n}: \mathbb{Z} \ \longrightarrow \ \mathbb{Z}_n, \quad f_{[k]_n}(m) = [km]_n$$

Τότε η απεικόνιση $f_{[k]_n}$ είναι ομομορφισμός, διότι:

$$f_{[k]_n}(m_1+m_2) = [k(m_1+m_2)]_n = [km_1+km_2]_n = [km_1]_n + [km_2]_n = f_{[k]_n}(m_1) + f_{[k]_n}(m_2)$$

Επιπλέον:

$$\Phi(f_{[k]_n}) = f_{[k]_n}(1) = [k1]_n = [k]_n \ \ \Longrightarrow \ \ \Phi: \ \text{επιμορφισμός}$$

Άρα η απεικόνιση Φ είναι ισομορφισμός ομάδων και επομένως

$$\mathsf{Hom}(\mathbb{Z},\mathbb{Z}_n) \ \ \xrightarrow{\cong} \ \ \mathbb{Z}_n$$

(4) Η απόδειξη χρειάζεται αρκετή προεργασία και θα δοθεί μετά την απόδειξη των τεσσάρων παρακάτω προκαταρκτικών αποτελεσμάτων τα οποία είναι ενδιαφέροντα από μόνα τους. □

Λήμμα 14.14. *Έστω $n, m \geq 1$, και υποθέτουμε ότι: $(n,m) = 1$. Τότε υπάρχει ένας ισομορφισμός:*

$$\mathbb{Z}_{nm} \ \ \xrightarrow{\cong} \ \ \mathbb{Z}_n \times \mathbb{Z}_m$$

Απόδειξη. Από το Θεώρημα 5.15 προκύπτει ότι επείδδή $(n,m)=1$, η ομάδα ευθύ γινόμενο $\mathbb{Z}_n \times \mathbb{Z}_m$ είναι κυκλική. Επομένως από το Θεώρημα 14.8 η ομάδα $\mathbb{Z}_n \times \mathbb{Z}_m$ θα είναι ισόμορφη με την κυκλική ομάδα $\mathbb{Z}_{nm}$. □

Λήμμα 14.15. *Έστω $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ η ανάλυση του φυσικού αριθμού n σε γινόμενο δυνάμεων διακεκριμμένων πρώτων αριθμών. Τότε υπάρχει ένας ισομορφισμός:*

$$\mathbb{Z}_n \quad \xrightarrow{\cong} \quad \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}}$$

Απόδειξη. Επειδή $(p_i^{a_i}, p_j^{a_j}) = 1$, $1 \leq i \neq j \leq k$, ο ισχυρισμός έπεται εύκολα από το Λήμμα 14.14 με επαγωγή. □

Λήμμα 14.16. *Έστω p, q δύο διαφορετικοί πρώτοι αριθμοί. Τότε για κάθε $k, l \geq 1$:*

$$\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{q^l}) \quad \xrightarrow{\cong} \quad \{e\}$$

Απόδειξη. Έστω $f\colon \mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{q^l}$ ένας ομομορφισμός. Αν $[x]_{p^k} \in \mathbb{Z}_{p^k}$, τότε $p^k[x]_{p^k} = [0]_{p^k}$ και τότε $f(p^k[x]_{p^k}) = p^k f([x]_{p^k}) = [0]_{q^l}$. Αυτό σημαίνει ότι $\mathsf{o}(f([x]_{p^k})) \mid p^k$. Όμως ο αριθμός $\mathsf{o}(f([x]_{p^k}))$ θα διαιρεί την τάξη q^l της ομάδας $\mathbb{Z}_{q^l}$ και άρα θα είναι μια δύναμη του q, έστω $\mathsf{o}(f([x]_{p^k})) = q^a$. Τότε $q^a \mid p^k$, και επειδή p, q είναι διαφορετικοί πρώτοι αριθμοί, θα έχουμε $q^a = 1 = \mathsf{o}(f([x]_{p^k}))$, δηλαδή $f([x]_{p^k}) = [0]_{q^l}$. Έτσι ο τυχόν ομομορφισμός f στέλνει κάθε στοιχείο της ομάδας $\mathbb{Z}_{p^k}$ στο μηδενικό στοιχείο της ομάδας $\mathbb{Z}_{q^l}$. Αυτό σημαίνει ότι ο f είναι ο τετριμμένος ομομορφισμός και άρα $\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{q^l}) = \{e\}$. □

Λήμμα 14.17. *Έστω $G = \langle a \rangle$ και $H = \langle b \rangle$ δύο κυκλικές ομάδες, και υποθέτουμε ότι η G είναι πεπερασμένη. Τότε τα ακόλουθα είναι ισοδύναμα:*

(1) *Υπάρχει ομομορφισμός $f\colon G \longrightarrow H$ έτσι ώστε $f(a) = b$.*
(2) $\mathsf{o}(b) \mid \mathsf{o}(a)$.

Αν $\mathsf{o}(b) \mid \mathsf{o}(a)$, τότε υπάρχει μοναδικός ομομορφισμός $f\colon G \longrightarrow H$ έτσι ώστε $f(a) = b$ και τότε: $f(a^k) = b^k$, $\forall k \in \mathbb{Z}$.

Απόδειξη. Υποθέτουμε ότι $\mathsf{o}(G) = \mathsf{o}(a) = n$, και άρα $G = \left\{e, a, a^2, \cdots a^{n-1}\right\}$.

(1) $\Longrightarrow$ (2) Έστω $f\colon G \longrightarrow H$ ένας ομομορφισμός έτσι ώστε $f(a) = b$. Τότε $a^n = e$ και άρα $b^n = f(a)^n = f(a^n) = f(e) = e$. Επομένως $\mathsf{o}(b) \mid n = \mathsf{o}(a)$.

(2) $\Longrightarrow$ (1) Έστω $\mathsf{o}(b) \mid n = \mathsf{o}(a)$, και $n = mk$, όπου $m = \mathsf{o}(b)$. Ορίζουμε απεικόνιση

$$f\colon \langle a \rangle \longrightarrow \langle b \rangle, \quad f(a^k) = b^k$$

Προφανώς η απεικόνιση f είναι ένας καλά ορισμένος ομομορφισμός και ισχύει $f(a) = b$. Αν $g\colon \langle a \rangle \longrightarrow \langle b \rangle$, είναι ένας άλλος ομομορφισμός έτσι ώστε $g(a) = b$. Τότε: $g(a^k) = g(a)^k = b^k = f(a)^k = f(a^k)$ και επομένως $f = g$. □

Λήμμα 14.18. *Έστω p ένας πρώτος αριθμός. Τότε για κάθε $k, l \geq 1$:*

$$\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l}) \quad \xrightarrow{\cong} \quad \mathbb{Z}_{p^{\min\{k,l\}}}$$

Απόδειξη. Έστω $a = [1]_{p^k}$ και $b = [1]_{p^l}$. Τότε

$$\mathbb{Z}_{p^k} = \langle a \rangle \quad \text{και} \quad \mathbb{Z}_{p^l} = \langle b \rangle$$

Θα δείξουμε ότι το πλήθος των διακεκριμμένων ομομορφισμών $\mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{p^l}$ είναι $p^{\min\{k,l\}}$.

- Αν $k \geq l$, τότε $p^k \geq p^l$ και προφανώς $\mathsf{o}(b) = p^l \mid p^k = \mathsf{o}(a)$. Τότε από το Λήμμα 4.17, έπεται ότι υπάρχει (μοναδικός) ομομορφισμός $f\colon \mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{p^l}$ έτσι ώστε $f(a) = b$. Παρατηρούμε ότι επειδή $k \geq l$, θα έχουμε $\min\{k,l\} = l$ και επομένως υπάρχουν l το πλήθος ομομορφισμοί $\mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{p^l}$ διότι το πλήθος των διαιρετών του p^k οι οποίοι είναι μικρότεροι ή ίσοι από το p^l και διάφοροι τοι 1 είναι ακριβώς l: $p, p^2, \cdots, p^l$.
- Αν $k \leq l$, τότε $\min\{k,l\} = k$ και κάθε ομομορφισμός $\mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{p^l}$ έχει προφανώς εικόνα στην (μοναδική) κυκλική υποομάδα τάξης p^k της $\mathbb{Z}_{p^l}$. Άρα το ζητούμενο πλήθος συμπίπτει με το πλήθος των ομομορφισμών $\mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{p^k}$. Από την πρώτη περίπτωση τότε θα έχουμε ότι το πλήθος αυτών των ομομορφισμών είναι ακριβώς $p^k = p^{\min\{k,l\}}$.

Άρα θα έχουμε: $\mathsf{o}(\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l})) = p^{\min\{k,l\}}$.

Τέλος από το Λήμμα 4.17, έπεται άμεσα ότι η απεικόνιση

$$\psi : \mathbb{Z}_{p^k} \longrightarrow \mathbb{Z}_{p^l}, \qquad \psi([r]_{p^k}) = p^{l-\min\{k,l\}}[r]_{p^l}$$

είναι ομομορφισμός ομάδων και μάλιστα επειδή η τάξη της ομάδας $\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l})$ είναι $p^{\min k,l}$, ισχύει:

$$p^{\min\{k,l\}}\psi = \varepsilon \quad \text{όπου} \quad \varepsilon([x]_{p^k}) = [0]_{p^l}$$

δηλαδή ο ομομορφισμός ε είναι το ταυτοτικό στοιχείο της ομάδας $\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l})$. Αν $n\psi = \varepsilon$, τότε θα έχουμε:

$$n\psi = \varepsilon \implies n\psi([1]_{p^k}) = \varepsilon([1]_{p^k}) \implies np^{l-\min\{k,l\}}[1]_{p^l} = [0]_{p^l} \implies [np^{l-\min\{k,l\}}]_{p^l} = [0]_{p^l} \implies$$
$$\implies p^l \mid np^{l-\min\{k,l\}} \implies np^{l-\min\{k,l\}} = p^l m \implies np^l = p^l p^{\min\{k,l\}} m \implies n = p^{\min\{k,l\}} m \implies$$
$$p^{\min\{k,l\}} \leq n$$

Επομένως

$$\mathsf{o}(\psi) = p^{\min\{k,l\}} = \mathsf{o}(\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l}))$$

και άρα η ομάδα $\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l})$ τάξης $p^{\min\{k,l\}}$ έχει ένα στοιχείο τάξης $p^{\min\{k,l\}}$. Επομένως η ομάδα $\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l})$ είναι κυκλική τάξης $p^{\min\{k,l\}}$. Τότε από το Θεώρημα 14.8, η ομάδα $\mathsf{Hom}(\mathbb{Z}_{p^k}, \mathbb{Z}_{p^l})$ είναι ισόμορφη με την κυκλική ομάδα $\mathbb{Z}_{p^{\min\{k,l\}}}$. □

Λήμμα 14.19. (1) *Έστω G_1, G_2 και H αβελιανές ομάδες. Τότε υπάρχει ένας ισομορφισμός ομάδων*

$$\mathsf{Hom}(G_1 \times G_2, H) \xrightarrow{\cong} \mathsf{Hom}(G_1, H) \times \mathsf{Hom}(G_2, H)$$

(2) *Έστω G και H_1, H_2 αβελιανές ομάδες. Τότε υπάρχει ένας ισομορφισμός ομάδων*

$$\mathsf{Hom}(G, H_1 \times H_2) \xrightarrow{\cong} \mathsf{Hom}(G, H_1) \times \mathsf{Hom}(G, H_2)$$

(3) *Γενικότερα έστω $\{G_i\}_{i=1}^n$ και $\{H_j\}_{j=1}^m$ αβελιανές ομάδες, και έστω*

$$G = G_1 \times G_2 \times \cdots \times G_n \quad \text{και} \quad H = H_1 \times H_2 \times \cdots \times H_m$$

οι αντίστοιχες ομάδες ευθύ γινόμενο. Τότε:

$$\mathsf{Hom}(G, H) \xrightarrow{\cong} \times_{i=1}^n \times_{j=1}^m \mathsf{Hom}(G_i, H_j)$$

δηλαδή:

$$\mathsf{Hom}(G, H) \xrightarrow{\cong} \mathsf{Hom}(G_1, H_1) \times \cdots \times \mathsf{Hom}(G_1, H_m) \times \cdots \times \mathsf{Hom}(G_n, H_1) \times \cdots \times \mathsf{Hom}(G_n, H_m)$$

Απόδειξη. (1) Ορίζουμε απεικόνιση

$$\Phi:\ \mathsf{Hom}(G_1\times G_2,H)\ \longrightarrow\ \mathsf{Hom}(G_1,H)\times\mathsf{Hom}(G_2,H),\qquad \Phi(f)=(f_1,f_2)$$

όπου

$$f_1:\ G_1\ \longrightarrow\ H,\quad f_1(x_1)=f(x_1,e_{G_2})\qquad\text{και}\qquad f_2:\ G_2\ \longrightarrow\ H,\quad f_2(x_2)=f(e_{G_1},x_2)$$

Επίσης ορίζουμε απεικόνιση

$$\Psi:\ \mathsf{Hom}(G_1,H)\times\mathsf{Hom}(G_2,H)\ \longrightarrow\ \mathsf{Hom}(G_1\times G_2,H),\qquad \Psi(g_1,g_2)=g$$

όπου

$$g:\ G_1\times G_2\ \longrightarrow\ H,\quad g(x_1,x_2)=g_1(x_1)+g_2(x_2)$$

Εύκολα βλέπουμε ότι οι απεικονίσεις Ψ και Φ είναι ομομορφισμοί ομάδων και ισχύει $\Psi=\Phi^{-1}$.

(2) Ορίζουμε απεικόνιση

$$\Phi:\ \mathsf{Hom}(G,H_1\times H_2)\ \longrightarrow\ \mathsf{Hom}(G,H_1)\times\mathsf{Hom}(G,H_2),\qquad \Phi(f)=(f_1,f_2)$$

όπου

$$f_i:\ G\ \longrightarrow\ H_i,\quad f_i=\pi_i\circ f$$

όπου

$$\pi_1:\ H_1\times H_2\ \longrightarrow\ H_1,\quad \pi(h_1,h_2)=h_1\qquad\text{και}\qquad \pi_2:\ H_1\times H_2\ \longrightarrow\ H_2,\quad \pi(h_1,h_2)=h_2$$

είναι οι ομομορφισμοί προβολές από την ομάδα ευθύ γινόμενο στις ομάδες παράγοντες.

Επίσης ορίζουμε απεικόνιση

$$\Psi:\ \mathsf{Hom}(G,H_1)\times\mathsf{Hom}(G,H_2)\ \longrightarrow\ \mathsf{Hom}(G,H_1\times H_2),\qquad \Psi(g_1,g_2)=g$$

όπου

$$g:\ G\ \longrightarrow\ H_1\times H_2,\quad g(x)=(g_1(x),g_2(x))$$

Εύκολα βλέπουμε ότι οι απεικονίσεις Ψ και Φ είναι ομομορφισμοί ομάδων και ισχύει $\Psi=\Phi^{-1}$.

(3) Υποθέτουμε πρώτα ότι $n=1$. Θα κατασκευάσουμε έναν ισομορφισμό

$$\Phi:\ \mathsf{Hom}(G_1,H_1\times\cdots\times H_m)\ \stackrel{\cong}{\longrightarrow}\ \mathsf{Hom}(G_1,H_1)\times\cdots\times\mathsf{Hom}(G_1,H_m)$$

ως εξής:

$$\Phi(f)=(f_1,\cdots,f_m)\quad\text{όπου}\quad f_i=\pi_i\circ f$$

και όπου

$$\pi_i:\ H_1\times\cdots\times H_m\ \longrightarrow\ H_i,\quad \pi_i(h_1,\cdots,h_m)=h_i$$

είναι οι ομομορφισμοί προβολές από την ομάδα ευθύ γινόμενο στις ομάδες παράγοντες.

Αν $(f_1,\cdots,f_m)\in\mathsf{Hom}(G_1,H_1)\times\cdots\times\mathsf{Hom}(G_1,H_m)$, τότε ορίζουμε μια απεικόνιση

$$f:\ G_1\ \longrightarrow\ H_1\times\cdots\times H_m,\qquad f(x)=(f_1(x),\cdots,f_m(x))$$

η οποία με τη σειρά της ορίζει μια απεικόνιση

$$\Psi:\ \mathsf{Hom}(G_1,H_1)\times\cdots\times\mathsf{Hom}(G_1,H_m)\ \longrightarrow\ \mathsf{Hom}(G_1,H_1)\times\cdots\times\mathsf{Hom}(G_1,H_m),\quad \Psi(f_1,\cdots,f_m)=f$$

Εύκολα βλέπουμε ότι οι απεικονίσεις Ψ και Φ είναι ομομορφισμοί ομάδων και ισχύειο $\Psi=\Phi^{-1}$.

Άρα ο ισχυρισμός αληθεύει για $n=1$. Η γενική περίπτωση αποδεικνύεται εύκολα με επαγωγή στο n, χρησιμοποιώντας το (1), και αφήνεται ως Άσκηση. □

Μπορούμε τώρα να ολοκληρώσουμε την απόδειξη του τελευταίου μέρους (4) του Θεωρήματος 14.13:

Απόδειξη του Θεωρήματος 14.13(4)**:** Έστω

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{και} \quad m = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

οι αναλύσεις των φυσικών αριθμών n και m σε γινόμενο δυνάμεων διακεκριμμένων πρώτων αριθμών. Γνωρίζουμε ότι ο μέγιστος κοινός διαιρέτης των m και n είναι:

$$(m,n) = p_1^{\min\{a_1,b_1\}} \cdots p_k^{\min\{a_k,b_k\}}$$

Από το Λήμμα 14.15 υπάρχουν ισομορφισμοί:

$$\mathbb{Z}_n \xrightarrow{\cong} \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_k^{a_k}} \quad \text{και} \quad \mathbb{Z}_m \xrightarrow{\cong} \mathbb{Z}_{q_1^{b_1}} \times \mathbb{Z}_{p_2^{n_2}} \times \cdots \times \mathbb{Z}_{p_k^{b_k}}$$

Αοπό το Λήμμα 14.18, θα έχουμε έναν ισομορφισμό

$$\mathsf{Hom}(\mathbb{Z}_n, \mathbb{Z}_m) \xrightarrow{\cong} \times_{i=1}^{k} \times_{j=1}^{l} \mathsf{Hom}(\mathbb{Z}_{p_i^{a_i}}, \mathbb{Z}_{q_j^{b_j}})$$

Από το Λήμμα 14.16 θα έχουμε ότι

$$\mathsf{Hom}(\mathbb{Z}_{p_i^{a_i}}, \mathbb{Z}_{p_j^{b_j}}) = \{e\}, \quad \forall i \neq j$$

Επομένως επειδή από το Λήμμα 14.17 έχουμε

$$\mathsf{Hom}(\mathbb{Z}_{p_i^{a_i}}, \mathbb{Z}_{p_j^{b_j}}) \xrightarrow{\cong} \mathbb{Z}_{p^{\min\{a_i,b_j\}}}$$

θα έχουμε τελικά:

$$\mathsf{Hom}(\mathbb{Z}_n, \mathbb{Z}_m) \xrightarrow{\cong} \mathsf{Hom}(\mathbb{Z}_{p_1^{a_1}}, \mathbb{Z}_{p_1^{b_1}}) \times \cdots \times \mathsf{Hom}(\mathbb{Z}_{p_k^{a_k}}, \mathbb{Z}_{p_k^{b_k}}) \xrightarrow{\cong} \mathbb{Z}_{p_1^{\min\{a_1,b_1\}}} \times \cdots \times \mathbb{Z}_{p_k^{\min\{a_k,b_k\}}}$$

και άρα μια τελευταία εφαρμογή του Λήμματος 14.15 δίνει:

$$\mathsf{Hom}(\mathbb{Z}_n, \mathbb{Z}_m) \xrightarrow{\cong} \mathbb{Z}_{p_1^{\min\{a_1,b_1\}}} \times \cdots \times \mathbb{Z}_{p_k^{\min\{a_k,b_k\}}} \xrightarrow{\cong} \mathbb{Z}_{p_1^{\min\{a_1,b_1\}} \cdots p_k^{\min\{a_k,b_k\}}} \xrightarrow{\cong} \mathbb{Z}_{(m,n)} \qquad \square$$

Υπενθυμίζουμε ότι μια ομάδα G καλείται **ελεύθερης στρέψης** αν το μόνο στοιχείο πεπερασμένης τάξης της G είναι το ταυτοτικό.

Άσκηση 293. *Έστω G μια προσθετική αβελιανή ομάδα, και $n \geq 1$.*

(1) *Το σύνολο*

$$G_n = \{x \in G \mid nx = 0\}$$

είναι μια υποομάδα της G.

(2) *Υπάρχει ένας ισομορφισμός αβελιανών ομάδων:*

$$\mathsf{Hom}(\mathbb{Z}_n, G) \xrightarrow{\cong} G_n$$

(3) *Η ομάδα G είναι ελεύθερης στρέψης αν και μόνον αν, $\forall n \geq 1$: $\mathsf{Hom}(\mathbb{Z}_n, G) = \{e\}$.*

14.5. **Ομάδες Αυτομορφισμών Κυκλικών Ομάδων.** Στην παρούσα υπο-ενότητα θα προσδιορίσουμε την ομάδα αυτομορφισμών μιας κυκλικής ομάδας.

Υπενθυμίζουμε ότι

$$\mathsf{Aut}(G) = \big\{ f : G \longrightarrow G \ \mid \ f : \ \text{ισομορφισμός} \big\}$$

και το σύνολο $\mathsf{Aut}(G)$ αποτελεί ομάδα με πράξη τη σύνθεση αυτομορφισμών.

Θα χρειασθούμε το ακόλουθο απλό

Λήμμα 14.20. *Έστω G μια ομάδα και $a \in G$. Έστω $f : G \longrightarrow G$ ένας αυτομορφισμός της G.*

(1) *a είναι γεννήτορας της G αν και μόνον αν $f(a)$ είναι γεννήτορας της G:*

$$G = \langle a \rangle \quad \Longleftrightarrow \quad G = \langle f(a) \rangle$$

(2) $\mathsf{o}(a) = \mathsf{o}(f(a))$.

Απόδειξη. Άσκηση. □

Το ακόλουθο θεώρημα δείχνει ότι η ομάδα αυτομορφισμών μιας άπειρης κυκλικής ομάδας είναι κυκλική και πολύ μικρή.

Θεώρημα 14.21. *Έστω $G = \langle a \rangle$ μια άπειρη κυκλική ομάδα. Τότε υπάρχει ένας ισομορφισμός*

$$\phi : \ \mathsf{Aut}(G) \ \xrightarrow{\ \cong\ } \ \mathbb{Z}_2$$

Απόδειξη. Έστω $G = \langle a \rangle$ ένας γεννήτορας της G. Τότε για κάθε αυτομορφισμό $f : G \longrightarrow G$ της G, το στοιχείο $f(a)$ είναι επίσης γεννήτορας της G. Επειδή η G είναι άπειρη κυκλική, γνωρίζουμε ότι η G έχει ακριβώς δύο γεννήτορες: το στοιχείο a και το στοιχείο a^{-1}. Έτσι $f(a) = a$ ή $f(a) = a^{-1}$. Επειδή $G = \langle a \rangle$, αν $f(a) = a$, έπεται ότι $f = \mathrm{Id}_G$, και αν $f(a) = a^{-1}$, τότε $f(x) = x^{-1}$, $\forall x \in G$. Αντίστροφα οι απεικονίσεις Id_G και $\varphi : G \longrightarrow G, \varphi(x) = x^{-1}$ είναι αυτομορφισμοί της G. Άρα $\mathsf{Aut}(G) = \{\mathrm{Id}_G, \varphi\}$, όπου προφανώς $\varphi^2 = \mathrm{Id}_G$. Επομένως η $\mathsf{Aut}(G)$ είναι ισόμορφη με την κυκλική ομάδα $\mathbb{Z}_2$, μέσω του ισομορφισμού $\mathrm{Id}_G \longmapsto [0]_2$ και $\varphi \longmapsto [1]_2$. □

Πόρισμα 14.22. *Υπάρχει ένας ισομορφισμός ομάδων*

$$\phi : \ \mathsf{Aut}(\mathbb{Z}) \ \xrightarrow{\ \cong\ } \ \mathbb{Z}_2$$

Το ακόλουθο θεώρημα δείχνει ότι το πλήθος των αυτομορφισμών μιας πεπερασμένης κυκλικής ομάδας τάξης n δίνεται από την τιμή της συνάρτησης $\varphi(n)$ του Euler.

Θεώρημα 14.23. *Έστω $G = \langle a \rangle$ μια πεπερασμένη κυκλική ομάδα τάξης n. Τότε υπάρχει ένας ισομορφισμός*

$$\phi : \ \mathsf{Aut}(G) \ \xrightarrow{\ \cong\ } \ \mathsf{U}(\mathbb{Z}_n)$$

Ιδιαίτερα: $\mathsf{o}\big(\mathsf{Aut}(G)\big) = \varphi(n)$.

Απόδειξη. Θα έχουμε

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

Αν $n = 1$, τότε $G = \{e\}$ και $\mathbb{Z}_1 = [0]_1$ και τότε προφανώς $\mathsf{Aut}(G) = \{\mathrm{Id}_G\} \cong \{\mathrm{Id}_{\mathbb{Z}_1}\} \cong \mathsf{U}(\mathbb{Z}_1)$.

Υποθέτουμε ότι $n > 1$. Έστω $f : G \longrightarrow G$ ένας αυτομορφισμός της G. Τότε το στοιχείο $f(a) \in G$ είναι γεννήτορας της G και άρα $f(a) = a^k$, για ένα μοναδικό στοιχείο k, όπου $1 \leq k \leq n-1$ και $(k, n) = 1$

(αν $k=0$, τότε $f(a)=e$ και άρα $a=e$ διότι η f αυτομορφισμός, δηλαδή $G=\{e\}$ το οποίο είναι άτοπο). Έτσι θα έχουμε $[k]_n \in \mathsf{U}(\mathbb{Z}_n)$, και επομένως μπορούμε να ορίσουμε μια απεικόνιση

$$\Phi:\ \mathsf{Aut}(G) \longrightarrow \mathsf{U}(\mathbb{Z}_n), \quad \Phi(f)=[k]_n, \qquad \text{όπου} \qquad f(a)=a^k$$

- Έστω $f,g \in \mathsf{Aut}(G)$ και έστω ότι $\Phi(f)=\Phi(g)$, δηλαδή: $[k]_n=[l]_n$, όπου $f(a)=a^k$ και $g(a)=a^l$. Τότε $n \mid k-l$ και επειδή $1 \leq k,l \leq n$ και $(k,n)=1=(l,n)$, έπεται ότι $k=l$. Επομένως $f(a)=g(a)$ και τότε προφανώς $f=g$, διότι επειδή οι f,g είναι ομομορφισμοί και $\forall x \in G$, $x=a^m$, θα έχουμε: $f(x)=f(a^m)=f(a)^m=g(a)^m=g(a^m)=g(x)$. Επομένως η απεικόνιση Φ είναι 1-1.
- Έστω $[k]_n \in \mathsf{U}(\mathbb{Z}_n)$, δηλαδή $1 \leq k \leq n-1$ και $(k,n)=1$. Ορίζουμε μια απεικόνιση

$$f_k:\ G \longrightarrow G, \quad f(a^m)=a^{km}$$

Η απεικόνιση f_k είναι ομομορφισμός, διότι:

$$f_k(a^{m_1}a^{m_2})=f_k(a^{m_1+m_2})=a^{(m_1+m_2)k}=a^{m_1k+m_2k}=a^{m_1k}a^{m_2k}=f_k(a^{m_1})f(a^{m_2})$$

Αν $f_k(a^m)=e$, τότε $a^{mk}=e$, και άρα $n \mid mk$. Επειδή $(k,n)=1$, έπεται ότι $n \mid m$. Τότε όμως αναγκαστικά $m=0$, διότι $0 \leq m \leq n-1$. Άρα $a^m=a^0=e$ και ο ομομορφισμός f_k είναι μονομορφισμός. Τότε όμως ο ομομορφισμός f_k είναι αυτομορφισμός διότι $\mathsf{o}(G)=n<\infty$. Τότε εξ' ορισμού θα έχουμε $\Phi(f_k)=[k]_n$, διότι $f_k(a)=a^k$. Άρα η απεικόνιση Φ είναι επί.

- Μένει να δείξουμε ότι η Φ είναι ομομορφισμός ομάδων. Έστω $f,g \in \mathsf{Aut}(G)$. Τότε θα έχουμε $\Phi(f)=a^k$, $g(a)=a^l$, όπου $f(a)=a^k$, $g(a)=a^l$, και $1 \leq k,l \leq n-1$ και $(k,n)=1=(l,n)$. Υποθέτουμε ότι $\Phi(f \circ g)=a^m$, όπου $1 \leq m \leq n-1$, $(n,m)=1$, και $(f \circ g)(a)=a^m$. Όμως $(f \circ g)(a)=f(g(a))=f(a^l)=f(a)^l=(a^k)^l=a^{kl}$. Τότε: $a^{kl}=a^m$ και επομένως $a^{kl-m}=e$. Επειδή $\mathsf{o}(a)=n$, θα έχουμε $n \mid kl-m$ και επομένως $[kl]_n=[m]_n$, δηλαδή: $[k]_k[l]_n=[m]_n$. Τότε:

$$\Phi(f \circ g)=[m]_n=[kl]_n=[k]_n[l]_n=\Phi(f)\Phi(g)$$

και άρα η απεικόνιση Φ είναι ομομορφισμός. Επομένως η Φ είναι ισομορφισμός. □

Πόρισμα 14.24. *Για κάθε $n \geq 1$, υπάρχει ένας ισομορφισμός ομάδων*

$$\phi:\ \mathsf{Aut}(\mathbb{Z}_n) \xrightarrow{\ \cong\ } \mathsf{U}(\mathbb{Z}_n)$$

Σε αντίθεση με την ομάδα αυτομορφισμών μιας άπειρης κυκλικής ομάδας, η οποία είναι κυκλική, η ομάδα αυτομορφισμών μιας πεπερασμένης κυκλικής ομάδας δεν είναι πάντα κυκλική.

Παράδειγμα 14.25. *Θεωρούμε την κυκλική ομάδα $\mathbb{Z}_{12}$ τάξης 12. Από το παράδειγμα 13.10, έχουμε έναν ισομορφισμό*

$$\mathsf{U}(\mathbb{Z}_{12}) \xrightarrow{\ \cong\ } \mathbb{Z}_2 \times \mathbb{Z}_2$$

Επομένως με βάση το Θεώρημα 14.24 θα έχουμε έναν ισομορφισμό

$$\mathsf{Aut}(\mathbb{Z}_{12}) \xrightarrow{\ \cong\ } \mathbb{Z}_2 \times \mathbb{Z}_2$$

και άρα η ομάδα αυτομορφισμών $\mathsf{Aut}(\mathbb{Z}_{12})$ δεν είναι κυκλική.

Υπάρχει το ακόλουθο βασικό αποτέλεσμα το οποίο περιγράφει την ομάδα αυτομορφισμών μιας πεπερασμένης κυκλικής ομάδας ως ευθύ γινόμενο κυκλικών ομάδων:

Θεώρημα 14.26. *Έστω G μια κυκλική ομάδα τάξης*

$$n = 2^i p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r}$$

όπου $p_1, p_2, \cdots, p_r$ είναι διακεκριμμένοι περιττοί πρώτοι αριθμοί, και $i, j_1, j_2, \cdots, j_r \geq 0$.

Τότε:

$$\mathsf{Aut}(G) \quad \xrightarrow{\cong} \quad \begin{cases} \mathbb{Z}_1, & i = 0 \\ \mathbb{Z}_{2^{i-1}}, & i = 1 \text{ ή } 2 \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{i-2}}, & i \geq 3 \end{cases} \quad \times \ \mathbb{Z}_{p_1^{j_1-1}(p_1-1)} \ \times \ \mathbb{Z}_{p_2^{j_2-1}(p_2-1)} \ \times \ \cdots \ \times \ \mathbb{Z}_{p_r^{j_r-1}(p_r-1)}$$

Ιδιαίτερα η τάξη της ομάδας αυτομορφισμών μιας πεπερασμένης κυκλικής ομάδας είναι άρτιος αριθμός.

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