ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΪΚΑ ΜΑΘΗΜΑΤΑ

Τίτλος Μαθήματος: Θεωρία Ομάδων

Ενότητα: Επεκτάσεις Ομάδων

Διδάσκων: Καθηγητής Νικόλαος Μαρμαρίδης

Τμήμα: Μαθηματικών

Κεφάλαιο 6

Επεκτάσεις Ομάδων

6.1 Προκαταρκτικές Έννοιες

Σύμφωνα με το Θεώρημα 4.2.4 των Jordan–Hölder αν, μια ομάδα $(G, \star)$ διαθέτει συνθετικές σειρές, τότε αυτές είναι ισόμορφες, δηλαδή το πλήθος και οι τύποι ισομορφισμών των συνθετικών παραγόντων είναι μοναδικά καθορισμένοι. Ιδιαιτέρως, μια πεπερασμένη ομάδα G διαθέτει πάντοτε συνθετικές σειρές, οι οποίες προκύπτουν προδιορίζοντας πρώτα μια μέγιστη ορθόθετη υποομάδα G_1 τής $G = G_0$, ακολούθως μια μέγιστη ορθόθετη υποομάδα G_2 τής G_1 και ούτω καθεξής, μέχρις ότου προκύψει μια μη τετριμμένη υποομάδα G_{r-1}, η οποία να μην διαθέτει καμιά άλλη ορθόθετη υποομάδα εκτός από την $G_r = \{e_G\}$. Προφανώς, η G_{r-1} και τα πηλίκα $G_i/G_{i+1}, i = 0, \ldots, r-1$ είναι απλές ομάδες. Επιπλέον, η σειρά

$$G = G_0 > G_1 > \cdots >> G_{r-1} > G_r = \{e_G\}$$

είναι μια συνθετική σειρά μήκους r.
Συνεπώς, μια πεπερασμένη ομάδα έχει μια «ανάλυση» σε συνθετική σειρά, η οποία όπως προείπαμε είναι «μοναδική». Σημειώνουμε, ότι μη ισόμορφες ομάδες, όπως οι $(\mathbb{Z}_4, +)$ και $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, μπορεί να έχουν τους ίδιους (με ακρίβεια ισομορφισμού) συνθετικούς παράγοντες. Οι προηγούμενες παρατηρήσεις οδηγούν στο λεγόμενο

Πρόγραμμα Hölder

(α΄) Να προσδιοριστούν (με ακρίβεια ισομορφισμού) όλες οι πεπερασμένες απλές ομάδες.

(β΄) Να προσδιοριστούν όλοι οι δυνατοί τρόποι με τους οποίους προκύπτουν οι ομάδες, μέσω συνθετικών σειρών, από τις απλές ομάδες.

Τα ανωτέρω δύο ερωτήματα απετέλεσαν ένα από τα ισχυρά κίνητρα για την ανάπτυξη τής Θεωρίας των Ομάδων. Ανάλογα ερωτήματα υπάρχουν και σε άλλες περιοχές τής

Άλγεβρας:
Μεταξύ ορισμένων δομών με κοινές ιδιότητες, να προσδιοριστούν κάποιες «αναλλοίωτες δομές» με χαρακτηριστικές ιδιότητες και κατόπιν να ευρεθούν οι διαδικασίες με τις οποίες συντίθενται οι υπόλοιπες ομοειδείς δομές από τις αναλλοίωτες.

6.2 Το Πρόβλημα τής Επέκτασης και το ημιευθύ Γινόμενο

Θα αναπτύξουμε τώρα ορισμένες έννοιες που σχετίζονται με το Πρόγραμμα Hölder. Αρχίζουμε με τον

Ορισμός 6.2.1. Έστω ότι $(\mathrm{N}, \star_{\mathrm{N}})$ και $(\mathrm{H}, \star_{\mathrm{H}})$ είναι δύο ομάδες. Μια ομάδα $(\mathrm{G}, \star)$ ονομάζεται *επέκταση* τής N με την H, αν υπάρχει μια ορθόθετη υποομάδα N_1 τής G, όπου η πηλικοομάδα G/N_1 είναι ισόμορφη με την ομάδα H.

Παραδείγματα 6.2.1. (α΄) Αμφότερες οι $(\mathrm{S}_3, \circ)$ και $(\mathbb{Z}_6, +)$ αποτελούν επεκτάσεις τής $(\mathbb{Z}_3, +)$ με την $(\mathbb{Z}_2, +)$. Επιπλέον, η $(\mathbb{Z}_6, +)$ είναι επέκταση τής $(\mathbb{Z}_2, +)$ με την $(\mathbb{Z}_3, +)$, ενώ η $(\mathrm{S}_3, \circ)$ δεν είναι.

(β΄) Αν $(\mathrm{N}, \star_{\mathrm{N}})$ και $(\mathrm{H}, \star_{\mathrm{H}})$ είναι δύο ομάδες, τότε το ευθύ γινόμενό τους $\mathrm{G} = \mathrm{N} \times \mathrm{H}$ είναι επέκταση τής N με την H (καθώς και επέκταση τής H με την N).

6.2.1 Ημιευθύ Γινόμενο

Εδώ θα παρουσιάσουμε μια ειδική περίπτωση επέκτασης ομάδων, η οποία ωστόσο αξίζει να μελετηθεί, αφού, όπως θα δούμε, αρκετές ομάδες εμπίπτουν σε αυτήν την περίπτωση.

Ορισμός 6.2.2. Έστω $(\mathrm{G}, \star)$ μια ομάδα και N, H δύο υποομάδες της. Η ομάδα G ονομάζεται το *εσωτερικό ημιευθύ γινόμενο* τής N με την H, αν

(α΄) $\mathrm{N} \trianglelefteq \mathrm{G}$, δηλαδή η N είναι ορθόθετη υποομάδα τής G,

(β΄) $\mathrm{G} = \mathrm{NH}$ και

(γ΄) $\mathrm{N} \cap \mathrm{H} = \{e_{\mathrm{G}}\}$.

Προσέξτε ότι αν, επιπλέον είναι $\mathrm{H} \trianglelefteq \mathrm{G}$, τότε το εσωτερικό ημιευθύ γινόμενο εκφυλίζεται στο σύνηθες εσωτερικό γινόμενο.

Συμβολισμός. Όταν η G είναι το ημιευθύ εσωτερικό γινόμενο τής ορθόθετης υποομάδας N με την υποομάδα H, τότε γράφουμε $\mathrm{G} = \mathrm{N} \rtimes \mathrm{H}$.

Παρατηρήσεις 6.2.1. (α′) Αν $G = N \rtimes H$, τότε κάθε $g \in G$ εκφράζεται κατά μοναδικό τρόπο ως $g = nh, n \in N, h \in H$. Πράγματι, $\forall g \in G$ υπάρχει μια έκφραση τής προηγούμενης μορφής, επειδή $G = NH$. Αν, $n_1 h_1 = n_2 h_2$, όπου $n_1, n_2 \in N, h_1, h_2 \in H$, τότε $n_2^{-1} n_1 = h_2 h_1^{-1} \in N \cap H = \{e_G\}$. Συνεπώς, $n_2^{-1} n_1 = e_G = h_2 h_1^{-1}$ και γι' αυτό $n_1 = n_2, h_1 = h_2$.

(β′) Επιπλέον αν, $G = N \rtimes H$, τότε επιλέγοντας για κάθε g_1 και $g_2 \in G$ τις μοναδικές εκφράσεις τους $g_1 = n_1 h_1, g_2 = n_2 h_2, n_1, n_2 \in N, h_1, h_2 \in H$, έχουμε

$$g_1 g_2 = n_1 h_1 n_2 h_2 = n_1 (h_1 n_2 h_1^{-1}) h_1 h_2 = n_1 n' h_1 h_2, \quad \text{όπου} \quad h_1 n_2 h_1^{-1} = n' \in N.$$

Ώστε, το «H–τμήμα» τού γινομένου $g_1 g_2$ ισούται με το γινόμενο $h_1 h_2$ των «H–τμημάτων» των g_1 και g_2 αντιστοίχως. Επομένως, η καλά ορισμένη απεικόνιση

$$\phi : G \to H, g = nh, n \in N, h \in H \quad \mapsto \phi(g) := h$$

είναι ένας ομομορφισμός ομάδων, αφού

$$\phi(g_1 g_2) = \phi(n_1 h_1 n_2 h_2) = \phi(n_1 n' h_1 h_2) = h_1 h_2 = \phi(g_1)\phi_(g_2).$$

Επιπλέον, είναι ολοφάνερο ότι ο ϕ είναι ένας επιμορφισμός με $\mathrm{Ker}(\phi) = N$ και επομένως $G/N \cong H$.

Ώστε όταν $G = N \rtimes H$, *τότε η* G *είναι επέκταση τής ορθόθετης υποομάδας* $N \trianglelefteq G$ *με την υποομάδα* $H \cong G/N$.

Η αμέσως επόμενη παρατήρηση αποτελεί το κίνητρο για την γενική περίπτωση, που θα εκθέσουμε στην Πρόταση 6.2.1.

(γ′) Έστω ότι $G = N \rtimes H$. Κάθε $h \in H$ ορίζει μια «1–1» και «επί» απεικόνιση

$$\theta_h : N \to N, n \mapsto \theta_h(n) := hnh^{-1},$$

αφού η N είναι μια ορθόθετη υποομάδα τής G και μάλιστα $\forall h \in H$, η απεικόνιση θ_h είναι ένας αυτομορφισμός τής N, επειδή $\forall n_1, n_2 \in N$ είναι

$$\theta_h(n_1 n_2) = h(n_1 n_2)h^{-1} = (hn_1 h^{-1})(hn_2 h^{-1}) = \theta_h(n_1)\theta_h(n_2).$$

Συνεπώς, η απεικόνιση

$$\theta : H \to \mathrm{Aut}(N), h \mapsto \theta(h) := \theta_h$$

είναι ένας ομομορφισμός ομάδων, αφού

$$\forall h_1, h_2 \in H, n \in N : \theta(h_1 h_2)(n) = \theta_{h_1 h_2}(n) = (h_1 h_2) n (h_1 h_2)^{-1} = h_1 (h_2 n h_2^{-1}) h_1^{-1} = h_1(\theta_{h_2}(n)) h_1^{-1} = \theta_{h_1}(\theta_{h_2}(n)) = \theta_{h_1} \circ \theta_{h_2}(n) = \theta(h_1) \circ \theta(h_2)(n).$$

Επομένως,
$$\forall h_1, h_2 \in H : \theta(h_1 h_2) = \theta(h_1) \circ \theta(h_2).$$

Ώστε, όταν μια ομάδα $(G, \star)$ είναι το εσωτερικό ημιευθύ γινόμενο τής ορθόθετης υποομάδας $N \trianglelefteq G$ με την υποομάδα $H \leq G$, τότε ορίζεται ένας ομομορφισμός ομάδων θ από την υποομάδα H στην ομάδα $\mathrm{Aut}(N)$ των αυτομορφισμών τής N.

Στην πρόταση που έπεται θα δούμε ότι υπάρχει και η «αντίστροφη» κατασκευή.

Πρόταση 6.2.1. *Έστω ότι $(N, \star_N)$, $(H, \star_H)$ είναι δύο ομάδες και ότι $\theta : H \to \mathrm{Aut}(N)$ είναι ένας ομομορφισμός ομάδων από την H στην ομάδα αυτομορφισμών $(\mathrm{Aut}(N), \circ)$ τής N.*
(Προκειμένου να απλοποιήσουμε τον συμβολισμό, θα γράφουμε θ_h για την εικόνα $\theta(h)$, όπου $h \in H$.)
Θεωρούμε το καρτεσιανό γινόμενο $G = N \times H$ και την απεικόνιση

$$\begin{aligned}&\star : G \times G \to G,\\ &((n_1, h_1), (n_2, h_2)) \mapsto (n_1, h_1) \star (n_2, h_2) := (n_1 \star_N \theta_{h_1}(n_2), h_1 \star_H h_2)\end{aligned}$$

(α′) *Το ζεύγος $(G, \star)$ είναι μια ομάδα με ουδέτερο στοιχείο το (e_N, e_H), όπου e_N (αντιστοίχως e_H) είναι το ουδέτερο στοιχείο τής N (αντιστοίχως τής H).*

(β′) *Τα σύνολα $\overline{N} = N \times \{e_H\}$ και $\overline{H} = \{e_N\} \times H$ είναι υποομάδες τής G. Επιπλέον η υποομάδα $\overline{N}$ είναι ισόμορφη με την N και η υποομάδα $\overline{H}$ είναι ισόμορφη με την H. Τέλος, η $\overline{N}$ είναι μια ορθόθετη υποομάδα τής G.*

(γ′) *Τέλος, η G είναι το εσωτερικό ημιευθύ γινόμενο $\overline{N} \rtimes \overline{H}$.*

Απόδειξη. (α′) Το σύνολο $G = N \times H$ είναι διάφορο τού κενού. Ελέγχουμε τα αξιώματα ομάδας:

Προσεταιριστικότητα

Έστω ότι $(n_1, h_1), (n_2, h_2), (n_3, h_3)$ είναι στοιχεία τού G.
Έχουμε:

$$\begin{aligned}&((n_1, h_1) \star (n_2, h_2)) \star (n_3, h_3) = ((n_1 \star_N \theta_{h_1}(n_2), h_1 \star_H h_2)) \star (n_3, h_3) =\\ &((n_1 \star_N \theta_{h_1}(n_2)) \star_N \theta_{h_1 \star_H h_2}(n_3), (h_1 \star_H h_2) \star_H h_3)\end{aligned}$$

και

$$(n_1, h_1) \star ((n_2, h_2) \star (n_3, h_3)) = (n_1, h_1) \star ((n_2 \star_N \theta_{h_2}(n_3), h_2 \star_H h_3)) =$$
$$(n_1 \star_N \theta_{h_1}(n_2 \star_N \theta_{h_2}(n_3)), h_1 \star_H (h_2 \star_H h_3)).$$

Αλλά

$$n_1 \star_N \theta_{h_1}(n_2 \star_N \theta_{h_2}(n_3)) = n_1 \star_N \theta_{h_1}(n_2) \star_N \theta_{h_1}(\theta_{h_2}(n_3)) =$$
$$n_1 \star_N \theta_{h_1}(n_2) \star_N \theta_{h_1 \star_H h_2}(n_3)$$

και $(h_1 \star_H h_2) \star_H h_3) = h_1 \star_H (h_2 \star_H h_3))$.

Ώστε, $(n_1, h_1) \star ((n_2, h_2) \star (n_3, h_3)) = ((n_1, h_1) \star ((n_2, h_2)) \star (n_3, h_3)$ και η πράξη «$\star$» είναι προσεταιριστική.

Ύπαρξη ουδετέρου

Παρατηρούμε ότι για κάθε $(n, h) \in G$ είναι

$$(e_N, e_H) \star (n, h) = (e_N \star_N \theta_{e_H}(n), e_H \star_H h) = (n, h)$$

και

$$(n, h) \star (e_N, e_H) = (n \star_N \theta_h(e_N), h \star_H e_H) = (n, h).$$

Ύπαρξη αντιστρόφου

Έστω $(n, h) \in G$. Έχουμε:

$$(n, h) \star (\theta_{h^{-1}}(n^{-1}), h^{-1}) = (n \star_N \theta_h(\theta_{h^{-1}}(n^{-1})), h \star_H h^{-1}) =$$
$$(n \star_N \theta_{h \star_H h^{-1}}(n^{-1}), h \star_H h^{-1}) = (e_N, e_H).$$

και

$$(\theta_{h^{-1}}(n^{-1}), h^{-1}) \star (n, h) = (\theta_h(\theta_{h^{-1}}(n^{-1})) \star_N n, h^{-1} \star_H h) =$$
$$(\theta_{h^{-1} \star_H h}(n^{-1}) \star_N n, h \star_H h^{-1}) = (e_N, e_H).$$

Επομένως, το αντίστροφο τού (n, h) είναι το $(\theta_{h^{-1}}(n^{-1}), h^{-1})$.

Το ζεύγος $(G, \star)$ είναι μια ομάδα.

(β′) Προτρέπουμε τον αναγνώστη να ελέγξει μόνος του ότι τα σύνολα $\overline{N} = N \times \{e_H\}$ και $\overline{H} = \{e_N\} \times H$ αποτελούν υποομάδες τής G.

Αποδεικνύουμε ότι η $\overline{N} = N \times \{e_H\}$ είναι μια ορθόθετη υποομάδα τής G. Πράγματι, για κάθε $(m, h) \in G$ και $(n, e_H) \in \overline{N}$ είναι:

$$((m, h) \star (n, e_H)) \star (m, h)^{-1} = (m \star_N \theta_h(n), h) \star (\theta_{h^{-1}}(m^{-1}), h^{-1}) =$$
$$(m \star_N \theta_h(n) \star_N \theta_h(\theta_{h^{-1}}(m^{-1}), h \star_H h^{-1}) = (m \star_N \theta_h(n) \star_N m^{-1}, e_H) \in \overline{N}.$$

Επομένως, $\overline{N} \trianglelefteq G$.

(γ′) Παρατηρούμε ότι $\forall(n,h) \in G$ είναι: $(n,h) = (n,e_H) \star (e_N,h)$. Επομένως, $G = \overline{N}\,\overline{H}$.

Τέλος, η G είναι το εσωτερικό ημιευθύ γινόμενο των $\overline{N}$ και $\overline{H}$, αφού προφανώς $\overline{N} \cap \overline{H} = \{(e_N, e_H)\}$. Ώστε, $G = \overline{N} \rtimes \overline{H}$. □

Ορισμός 6.2.3. Έστω ότι $(N, \star_N)$, $(H, \star_H)$ είναι δύο ομάδες και ότι $\theta : H \to \mathrm{Aut}(N)$ είναι ένας ομομορφισμός ομάδων. Η ομάδα $(G, \star)$ τής Πρότασης 6.2.1 ονομάζεται το *εξωτερικό ημιευθύ γινόμενο* των ομάδων N και H και παριστάνεται ως $N \rtimes_\theta H$.

Παρατηρήσεις 6.2.2. (α′) Λαμβάνοντας υπ' όψιν την Παρατήρηση 6.2.1 (β′), διαπιστώνουμε ότι όταν $G = N \rtimes_\theta H$, τότε η G είναι επέκταση τής ομάδας N με την ομάδα H, αφού η G είναι το εσωτερικό ημιευθύ γινόμενο των $\overline{N}$ και $\overline{H}$. Συνεπώς, $\overline{N} \trianglelefteq G$, $\overline{H} \leq G$, $G/\overline{N} \cong \overline{H}$ και αφού επιπλέον, $\overline{N} \cong N$ και $\overline{H} \cong H$.

Ώστε, το εξωτερικό ημιευθύ γινόμενο $G = N \rtimes_\theta H$ είναι επέκταση τής ομάδας N με την ομάδα H.

(β′) Στην περίπτωση, όπου ο ομομορφισμός $\theta : H \to \mathrm{Aut}(N)$ είναι ο τετριμμένος, δηλαδή $\theta_h = \mathrm{Id}_N, \forall h \in H$, τότε το εξωτερικό ημιευθύ γινόμενο εκφυλίζεται στο σύνηθες εξωτερικό ευθύ γινόμενο $N \times H$.
Πράγματι, για το γινόμενο δύο στοιχείων $(n_1, h_1), (n_2, h_2) \in G$ έχουμε:

$$(n_1, h_1) \star (h_2, n_2) = (n_1 \star_N \theta_{h_1}(n_2), h_1 \star_H h_2) =$$
$$(n_1 \star_N \mathrm{Id}_N(n_2), h_1 \star_H h_2) = (n_1 \star_N n_2, h_1 \star_H h_2).$$

Στη συγκεκριμένη περίπτωση μάλιστα, θεωρώντας το αντίστοιχο εσωτερικό ημιευθύ γινόμενο $G = \overline{N} \rtimes \overline{H}$, όπου $\overline{N} = N \times \{e_H\}$, $\overline{H} = \{e_N\} \times H$ έχουμε ότι και $\overline{N} \trianglelefteq G$ και $\overline{H} \trianglelefteq G$. Συνεπώς, το αντίστοιχο εσωτερικό ημιευθύ γινόμενο εκφυλίζεται στο σύνηθες εσωτερικό ευθύ γινόμενο.

Παρακάτω θα δώσουμε παραδείγματα εσωτερικών και εξωτερικών ημιευθέων γινομένων. Ωστόσο, το πρώτο παράδειγμα κάνει σαφές ότι η έννοια «ημιευθύ γινόμενο» δεν είναι η πλέον γενική περίπτωση τής έννοιας «επέκταση ομάδων»:

Παραδείγματα 6.2.2. (α′) Θεωρούμε την ομάδα τετρανίων:

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}, \text{ με } (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1$$

και όπου το 1 είναι το ταυτοτικό στοιχείο τής Q_8 και το -1 μετατίθεται με οποιοδήποτε άλλο στοιχείο.
Ισχυριζόμαστε ότι

*η Q_8 **δεν είναι** το (εσωτερικό) ημιευθύ γινόμενο δύο μη τετριμμένων υποομάδων της. Θα αποδείξουμε μάλιστα ότι δεν υπάρχουν μη τετριμμένες υποομάδες N, H τής Q_8, τέτοιες ώστε $Q_8 = NH$ και $N \cap H = \{1\}$.*

Πράγματι, παρατηρούμε ότι αν, $Q_8 = NH$ και $N \cap H = \{1\}$, όπου $N \neq \{1\}, Q_8$ και $H \neq \{1\}, Q_8$, τότε η τάξη τής μίας από τις δύο υποομάδες ισούται με 4 και η άλλη ισούται με 2, αφού

$$8 = |Q_8| = |NH| = \frac{|N||H|}{|N \cap H|} = |N||H|.$$

Αλλά η Q_8 διαθέτει μόνο μία υποομάδα τάξης 2, την $\langle -1 \rangle$, αφού υπάρχει ακριβώς ένα στοιχείο τάξης 2. Λόγω αυτής τής παρατήρησης, συμπεραίνουμε τώρα ότι κάθε υποομάδα τής Q_8 τάξης 4 οφείλει να είναι κυκλική, αφού αν δεν ήταν κυκλική, τότε θα είχε δύο διαφορετικές υποομάδες τάξης 2, (επειδή θα ήταν ισόμορφη με την $\mathbb{Z}_2 \times \mathbb{Z}_2$), που δεν μπορεί να συμβαίνει. Αφού όμως κάθε κυκλική υποομάδα τάξης 4 περιέχει πάντοτε μια υποομάδα τάξης 2, συμπεραίνουμε ότι κάθε υποομάδα τής Q_8 τάξης 4, περιέχει την $\langle -1 \rangle$ και γι' αυτό η τομή μιας υποομάδας τάξης 4 με την μοναδική υποομάδα τάξης 2, δηλαδή την $\langle -1 \rangle$, ισούται με $\langle -1 \rangle$. Ώστε, πάντοτε η τομή μιας υποομάδας τάξης 2 με μια υποομάδα τάξης 4 είναι διαφορετική από την $\{1\}$.

Εν τούτοις, η Q_8 είναι επέκταση τής $\mathbb{Z}_4$ με την $\mathbb{Z}_2$, επειδή η Q_8 διαθέτει ορθόθετες κυκλικές υποομάδες τάξης 4, παραδείγματος χάριν την $N = \langle i \rangle \cong \mathbb{Z}_4$ και όπου $Q_8/N \cong \mathbb{Z}_2$.

(β′) Η διεδρική ομάδα $D_{2n} = \{\rho, \sigma \mid \rho^n = e = \sigma^2, \rho\sigma = \sigma\rho^{n-1}\}$ είναι ίση με το εσωτερικό ημιευθύ γινόμενο τής ορθόθετης υποομάδας $\langle \rho \rangle$ με την υποομάδα $\langle \sigma \rangle$, δηλαδή $D_{2n} = \langle \rho \rangle \rtimes \langle \sigma \rangle$.

Πράγματι, η $\langle \rho \rangle$ είναι ορθόθετη υποομάδα τής D_{2n}, αφού $[D_{2n} : \langle \rho \rangle]$=2. Προφανώς, η τομή $\langle \rho \rangle \cap \langle \sigma \rangle$ ισούται με $\{e\}$. Τέλος, η υποομάδα $\langle \rho \rangle \langle \sigma \rangle$ ισούται με την D_{2n}, αφού το πλήθος των στοιχείων τής $\langle \rho \rangle \langle \sigma \rangle$ είναι

$$|\langle \rho \rangle \langle \sigma \rangle| = \frac{|\langle \rho \rangle||\langle \sigma \rangle|}{|\langle \rho \rangle| \cap |\langle \sigma \rangle|} = 2n.$$

Τέλος, ο ομομορφισμός $\theta : \langle \sigma \rangle = \{e, \sigma\} \to \mathrm{Aut}(\langle \rho \rangle)$, που είδαμε στην Παρατήρηση 6.2.1 (γ′), προσδιορίζεται πολύ εύκολα: Η $\langle \sigma \rangle$ είναι κυκλική ομάδα τάξης 2 και γι' αυτό κάθε ομομορφισμός με πεδίο ορισμού την $\langle \sigma \rangle$ προσδιορίζεται πλήρως από την τιμή της στον γεννήτορα σ.

Πράγματι, $\theta_\sigma(\rho) = \sigma\rho\sigma^{-1} = \sigma\rho\sigma = \sigma\sigma\rho^{n-1} = \rho^{n-1} = \rho^{-1}$. Προσέξτε, ότι το ρ^{-1} είναι πάντοτε γεννήτορας τής κυκλικής ομάδας $\langle \rho \rangle$.
Ως εκ τούτου η D_{2n} είναι ισόμορφη με το εξωτερικό ευθύ γινόμενο $\mathbb{Z}_n \rtimes_\theta \mathbb{Z}_2$ των κυκλικών ομάδων $(\mathbb{Z}_n, +)$ και $(\mathbb{Z}_2, +)$, όπου $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n)$ είναι ο ομομορφισμός ομάδων με $\theta_{[1]_2}([1]_n) = [n-1]_n$.

(γ′) Η προηγούμενη κατασκευή μπορεί να εκτελεστεί και με οποιαδήποτε αβελιανή ομάδα $(A, +)$ στη θέση τής $(\mathbb{Z}_n, +)$.
Τώρα, ο ομομορφισμός $\theta : \mathbb{Z}_2 \to A$ είναι ο $\theta_{[1]_2}(a) = -a, \forall a \in A$.

Σημειώστε, ότι ο θ δεν είναι ο τετριμμένος ομομορφισμός αν, και μόνο αν, η A διαθέτει τουλάχιστον ένα στοιχείο τάξης $\neq 2$, δηλαδή ένα στοιχείο $a \in A$ με $a \neq -a$ και τότε το εξωτερικό ημιευθύ γινόμενο $A \rtimes_\theta \mathbb{Z}_2$ δεν είναι ισόμορφο με το εξωτερικό ευθύ γινόμενο $A \times \mathbb{Z}_2$.

Παραδείγματα 6.2.3. (α′) Η συμμετρική ομάδα $(S_4, \circ)$ είναι το εσωτερικό ημιευθύ γινόμενο τής ορθόθετης υποομάδας

$$V = \{\mathrm{Id}, \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}\}$$

με την υποομάδα $H = \{\sigma \in S_4 \mid \sigma(4) = 4\}$, δηλαδή $S_4 = V \rtimes H$.
Πράγματι, η V είναι ορθόθετη υποομάδα τής S_4, επειδή $\forall \tau \in S_4$ είναι

$$\tau \circ \begin{pmatrix}\alpha & \beta\end{pmatrix} \circ \begin{pmatrix}\gamma & \delta\end{pmatrix} \circ \tau^{-1} = \begin{pmatrix}\tau(\alpha) & \tau(\beta)\end{pmatrix} \circ \begin{pmatrix}\tau(\gamma) & \tau(\delta)\end{pmatrix},$$

και επειδή τα $\tau(\alpha), \tau(\beta), \tau(\gamma), \tau(\delta) \in \{1, 2, 3, 4\}$ είναι ανά δύο διαφορετικά, όταν τα $\alpha, \beta, \gamma, \delta \in \{1, 2, 3, 4\}$ είναι ανά δύο διαφορετικά.

Επιπλέον,

$$|VH| = \frac{|V||H|}{|V \cap H|} = 4 \cdot 6 = 24,$$

αφού $V \cap H = \{\mathrm{Id}\}$ και συνεπώς, $S_4 = VH$.

Θα προσπαθήσουμε να προσδιορίσουμε τον ομομορφισμό $\theta : H \to \mathrm{Aut}(V)$, βλ. Παρατήρηση 6.2.1 (γ′).

Η υποομάδα V τής S_4 είναι ισόμορφη με το ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_2$ τής $(\mathbb{Z}_2, +)$ με τον εαυτό της.

Η απεικόνιση

$$\begin{aligned}
\chi :& V \to \mathbb{Z}_2 \times \mathbb{Z}_2, \\
& \mathrm{Id} \mapsto ([0]_2, [0]_2), u = \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix} \mapsto ([1]_2, [0]_2) \\
& v = \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix} \mapsto ([0]_2, [1]_2), u \circ v = \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix} \mapsto ([1]_2, [1]_2),
\end{aligned}$$

είναι ένας ισομορφισμός ομάδων.
Επομένως, $\mathrm{Aut}(V) \cong \mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2)$. Επειδή κάθε ενδομορφισμός τής $\mathbb{Z}_2 \times \mathbb{Z}_2$ είναι και μια $\mathbb{Z}_2$–γραμμική απεικόνιση, οι αυτομορφισμοί τής $\mathbb{Z}_2 \times \mathbb{Z}_2$ μπορούν, επιλέγοντας μια $\mathbb{Z}_2$–βάση τής $\mathbb{Z}_2 \times \mathbb{Z}_2$, να ταυτιστούν με τους 2×2 αντιστρέψιμους πίνακες με συνιστώσες από το σώμα $\mathbb{Z}_2$.

Επιλέγοντας ως $\mathbb{Z}_2$–βάση τής $\mathbb{Z}_2 \times \mathbb{Z}_2$ την $\{([1]_2, [0]_2), ([0]_2, [1]_2)\}$ έχουμε:

$$\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) = \left\{ \begin{pmatrix} [1]_2 & [0]_2 \\ [0]_2 & [1]_2 \end{pmatrix}, \begin{pmatrix} [1]_2 & [0]_2 \\ [1]_2 & [1]_2 \end{pmatrix}, \begin{pmatrix} [0]_2 & [1]_2 \\ [1]_2 & [0]_2 \end{pmatrix}, \begin{pmatrix} [1]_2 & [1]_2 \\ [0]_2 & [1]_2 \end{pmatrix}, \begin{pmatrix} [1]_2 & [1]_2 \\ [1]_2 & [0]_2 \end{pmatrix}, \begin{pmatrix} [0]_2 & [1]_2 \\ [1]_2 & [1]_2 \end{pmatrix} \right\}$$

Σημειώνουμε ότι η $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong \mathrm{Aut}(V)$ είναι ισόμορφη με την $(S_3, \circ)$, αφού πρόκειται για μια μη αβελιανή ομάδα τάξης 6.

Για να προσδιορίσουμε τον ομομορφισμό $\theta : H \to \mathrm{Aut}(V)$ είναι αρκετό να υπολογίσουμε τις εικόνες $\theta_{(1\ 2\ 3)}$ και $\theta_{(1\ 2)}$ των στοιχείων $(1\quad 2\quad 3)$ και $(1\quad 2) \in H$, αφού $H = \langle (1\quad 2\quad 3), (1\quad 2) \rangle = S_3$.

'Εχουμε:

$$\theta_{(1\ 2\ 3)}(u) = (1\quad 2\quad 3) \circ u \circ (1\quad 2\quad 3)^{-1} = (2\quad 3) \circ (1\quad 4) = u \circ v$$
$$\theta_{(1\ 2\ 3)}(v) = (1\quad 2\quad 3) \circ v \circ (1\quad 2\quad 3)^{-1} = (2\quad 1) \circ (3\quad 4) = u.$$

Το στοιχείο $\theta_{(1\ 2\ 3)} \in \mathrm{Aut}(V)$ αντιστοιχεί στον αντιστρέψιμο πίνακα $\begin{pmatrix} [1]_2 & [1]_2 \\ [1]_2 & [0]_2 \end{pmatrix}$ και η τάξη του ισούται με 3.

$$\theta_{(1\ 2)}(u) = (1\quad 2) \circ u \circ (1\quad 2)^{-1} = (2\quad 1) \circ (3\quad 4) = u$$
$$\theta_{(1\ 2)}(v) = (1\quad 2) \circ v \circ (1\quad 2)^{-1} = (2\quad 3) \circ (1\quad 4) = u \circ v.$$

Το στοιχείο $\theta_{(1\ 2)} \in \mathrm{Aut}(V)$ αντιστοιχεί στον αντιστρέψιμο πίνακα $\begin{pmatrix} [1]_2 & [1]_2 \\ [0]_2 & [1]_2 \end{pmatrix}$ και η τάξη του ισούται με 3.

Η υποομάδα $\langle \theta_{(1\ 2\ 3)}, \theta_{(1\ 2)} \rangle$ τής $\mathrm{Im}\theta \leq \mathrm{Aut}(V)$ έχει τάξη 6 και γι' αυτό $\mathrm{Im}\theta = \mathrm{Aut}(V)$. Συνεπώς, ο θ είναι ένας επιμορφισμός μεταξύ δύο ομάδων τάξης 6 και ως εκ τούτου είναι ισομορφισμός.

(β′) Η εναλλάσσουσα ομάδα $(\mathbb{A}_4, \circ)$ είναι το εσωτερικό ημιευθύ γινόμενο τής ορθόθετης υποομάδας

$$V = \{\mathrm{Id}, (1\quad 2) \circ (3\quad 4), (1\quad 3) \circ (2\quad 4), (1\quad 4) \circ (2\quad 3)\}$$

με την κυκλική υποομάδα $K = \langle (1\quad 2\quad 3) \rangle$, δηλαδή $\mathbb{A}_4 = V \rtimes K$.
Πράγματι, η V είναι ορθόθετη υποομάδα τής $\mathbb{A}_4$ ως ορθόθετη υποομάδα τής $(S_4, \circ)$.
Επιπλέον,

$$|VK| = \frac{|V||K|}{|V \cap K|} = 4 \cdot 3 = 12,$$

αφού $V \cap K = \{\mathrm{Id}\}$ και συνεπώς, $\mathbb{A}_4 = VK$.

Θα προσδιορίσουμε και πάλι τον ομομορφισμό $\theta : \mathsf{K} \to \mathrm{Aut}(\mathsf{V})$, βλ. Παρατήρηση 6.2.1 (γ′).

Εδώ, η υποομάδα K είναι κυκλική με γεννήτορα το στοιχείο $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$ και συνεπώς για τον προσδιορισμό τού θ αρκεί ο υπολογισμός τής τιμής $\theta_{(1\ 2\ 3)}$.

Έχουμε:

$$\theta_{(1\ 2\ 3)}(\mathrm{Id}) = \begin{pmatrix}1 & 2 & 3\end{pmatrix} \circ \mathrm{Id} \circ \begin{pmatrix}1 & 2 & 3\end{pmatrix}^{-1} = \mathrm{Id},$$

$$\theta_{(1\ 2\ 3)}\left(\begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}\right) = \begin{pmatrix}1 & 2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\end{pmatrix}^{-1} = \begin{pmatrix}2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 4\end{pmatrix},$$

$$\theta_{(1\ 2\ 3)}\left(\begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}\right) = \begin{pmatrix}1 & 2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\end{pmatrix}^{-1} = \begin{pmatrix}2 & 1\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix},$$

$$\theta_{(1\ 2\ 3)}\left(\begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}\right) = \begin{pmatrix}1 & 2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\end{pmatrix}^{-1} = \begin{pmatrix}2 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 3\end{pmatrix}.$$

(γ′) Θεωρούμε τις κυκλικές ομάδες $\mathsf{C}_3 = \langle a, a^3 = e_{\mathsf{C}_3} \rangle$, $\mathsf{C}_4 = \langle b, b^4 = e_{\mathsf{C}_4} \rangle$ τάξης 3 και 4 αντιστοίχως, και τον μη τετριμμένο ομομορφισμό

$$\begin{aligned} \theta : & \mathsf{C}_4 \to \mathrm{Aut}(\mathsf{C}_3) \\ & b \to \ \theta_b : \mathsf{C}_3 \to \mathsf{C}_3 \\ & \qquad\qquad x \to x^{-1} \end{aligned}$$

Το εξωτερικό ημιευθύ γινόμενο $\mathsf{G} = \mathsf{C}_3 \rtimes_\theta \mathsf{C}_4$ είναι μια ομάδα με 12 στοιχεία, η οποία δεν είναι αβελιανή, αφού

$$\begin{aligned} (a,b) \star (a^2,b) &= (a\theta_b(a^2), b^2) = (aa^{-2}, b^2) = (a^2, b^2) \neq \\ (a^2,b) \star (a,b) &= (a^2\theta_b(a), b^2) = (a^2a^{-1}, b^2) = (a, b^2). \end{aligned}$$

Επιπλέον, η G διαθέτει περισσότερες από μία 2–Sylow υποομάδες, αφού διαφορετικά η 2–Sylow υποομάδα $\{e_{\mathsf{C}_3}\} \times \mathsf{C}_4$ θα ήταν μια ορθόθετη υποομάδα τής G και τότε η G θα ήταν ισόμορφη με το ευθύ γινόμενο $\mathsf{C}_3 \times \mathsf{C}_4$ που είναι μια αβελιανή ομάδα.

Έτσι, συμπεραίνουμε ότι η μη αβελιανή ομάδα $\mathsf{G} = \mathsf{C}_3 \rtimes_\theta \mathsf{C}_4$ ***δεν είναι ισόμορφη*** με την εναλλάσσουσα ομάδα $\mathbb{A}_4$, που είναι μη αβελιανή τάξης 12, αφού η υποομάδα

$$\mathsf{V} = \{\mathrm{Id}, \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}\} \leq \mathbb{A}_4$$

είναι μια ορθόθετη 2–Sylow υποομάδα τής $\mathbb{A}_4$, η οποία είναι βέβαια και η μοναδική 2–Sylow υποομάδα τής $\mathbb{A}_4$.

Πότε είναι δύο εξωτερικά ημιευθέα γινόμενα ισόμορφα; Θα παρουσιάσουμε μια πολύ ειδική περίπτωση, την οποία θα εφαρμόσουμε αμέσως μετά.

Λήμμα 6.2.2. *Έστω ότι* H *και* N *είναι δύο ομάδες, ότι* $\theta : H \to \mathrm{Aut}(N)$ *είναι ένας ομομορφισμός ομάδων και ότι* $\sigma : H \to H$ *είναι ένας αυτομορφισμός τής* H*. Τότε τα εξωτερικά ημιευθέα γινόμενα* $N \rtimes_\theta H$ *και* $N \rtimes_{\theta\circ\sigma} H$ *είναι ισόμορφες ομάδες.*

Απόδειξη. Παρατηρούμε ότι η σύνθεση $\theta \circ \sigma : H \to \mathrm{Aut}(N)$ είναι ένας ομομορφισμός ομάδων και ως εκ τούτου το εξωτερικό ημιευθύ γινόμενο $N \rtimes_{\theta\circ\sigma} H$ μπορεί να σχηματιστεί.
Η απεικόνιση

$$\psi : N \rtimes_\theta H \to N \rtimes_{\theta\circ\sigma} H, (n,h) \mapsto \psi((n,h)) := (n, \sigma^{-1}(h))$$

είναι μια «1–1» και «επί» απεικόνιση. Υπολείπεται η απόδειξη ότι η ψ είναι ένας ομομορφισμός ομάδων.
Για κάθε $(n,h), (\overline{n}, \overline{h}) \in N \rtimes_\theta H$, έχουμε:

$$\psi((n,h)(\overline{n},\overline{h})) = \psi((n\theta_h(\overline{n}), h\overline{h})) = (n\theta_h(\overline{n}), \sigma^{-1}(h\overline{h})) \text{ και}$$
$$\psi((n,h))\psi((\overline{n},\overline{h})) = (n,\sigma^{-1}(h))(\overline{n},\sigma^{-1}(\overline{n})) = (n\theta \circ \sigma_{\sigma^{-1}(h)}(\overline{n}), \sigma^{-1}(h)\sigma^{-1}(\overline{h})).$$

Επειδή, $\sigma^{-1}(h)\sigma^{-1}(\overline{h}) = \sigma^{-1}(h\overline{h})$ και $n(\theta\circ\sigma)_{\sigma^{-1}(h)}(\overline{n}) = n\theta_h(\overline{n})$, αφού $(\theta \circ \sigma)_{\sigma^{-1}(h)} = \theta_h$, συμπεραίνουμε ότι ο ψ είναι ένας ομομορφισμός ομάδων και οι $N \rtimes_\theta H$, $N \rtimes_{\theta\circ\sigma} H$ είναι ισόμορφες ομάδες. □

Η επόμενη πρόταση συμπληρώνει την Πρόταση 2.2.2

Πρόταση 6.2.3. *Έστω ότι* $(G, \star)$ *είναι μια ομάδα τάξης* pq*, όπου οι* p, q *είναι πρώτοι αριθμοί με* $p < q$*.*

(α′) *Αν ο* p *δεν διαιρεί τον* $q-1$*, τότε* $G \cong \mathbb{Z}_q \times \mathbb{Z}_p$*.*

(β′) *Αν ο* p *διαιρεί τον* $q-1$*, τότε ή* $G \cong \mathbb{Z}_q \times \mathbb{Z}_p$ *ή* $G \cong \mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p$*, όπου ο* $\theta : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$ *είναι ένας μη τετριμμένος ομομορφισμός. Όλοι οι μη τετριμμένοι ομομορφισμοί χορηγούν ισόμορφες ομάδες.*

Απόδειξη. Με τη βοήθεια τής Θεωρίας Sylow, βλ. και Πρόταση 2.2.2, γνωρίζουμε ότι η G διαθέτει μια ορθόθετη κυκλική υποομάδα C_q πρώτης τάξης q και μια κυκλική υποομάδα C_p πρώτης τάξης p. Επειδή $C_q \cap C_p = \{e_G\}$ και $C_qC_p = G$, συμπεραίνουμε ότι η G είναι το εσωτερικό ημιευθύ γινόμενο $C_q \rtimes C_p$ καθώς και ότι η G είναι ισόμορφη με το εξωτερικό ημιευθύ γινόμενο $\mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p$, όπου ο $\theta : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$ είναι ένας ομομορφισμός ομάδων, αφού $C_q \cong \mathbb{Z}_q$ και $C_p \cong \mathbb{Z}_p$.

Είναι γνωστό ότι η ομάδα $\mathrm{Aut}(\mathbb{Z}_q)$ των αυτομορφισμών τής $\mathbb{Z}_q$ είναι ισόμορφη με την πολλαπλασιαστική ομάδα $\mathbb{Z}_q^\star$ των αντιστρέψιμων στοιχείων τού πεπερασμένου σώματος $\mathbb{Z}_q$, βλ. Παράδειγμα 2.2.1. Από το Θεώρημα 2.2.22 γνωρίζουμε ότι η $\mathbb{Z}_q^\star$

είναι κυκλική και αφού $\mathbb{Z}_q^\star = \mathbb{Z}_q \setminus \{[0]_q\}$, η τάξη της ισούται με $q-1$. Επομένως, η $\mathrm{Aut}(\mathbb{Z}_q)$ είναι κυκλική ομάδα τάξης $q-1$.
Έστω

$$\theta : \mathbb{Z}_p \longrightarrow \mathrm{Aut}(\mathbb{Z}_q)$$

ένας οποιοσδήποτε ομομορφισμός ομάδων. Η εικόνα $\mathrm{Im}\theta$ τού ομομορφισμού θ είναι ισόμορφη με μια πηλικοομάδα τής $\mathbb{Z}_p$ και επειδή ο p είναι πρώτος αριθμός ή $\mathrm{Im}\theta \cong \mathbb{Z}_p$ ή η $\mathrm{Im}\theta = \{\mathrm{Id}_{\mathbb{Z}_q}\}$ και τότε ο θ είναι ο τετριμμένος ομομορφισμός. Επιπλέον, αφού η $\mathrm{Im}\theta$ είναι υποομάδα τής $\mathrm{Aut}(\mathbb{Z}_q) \cong \mathbb{Z}_{q-1}$, η τάξη της οφείλει να είναι διαιρέτης τού $q-1$.

(α′). Αν $p \nmid q-1$, τότε από τα προηγούμενα συμπεραίνουμε ότι ο μοναδικός ομομορφισμός $\mathbb{Z}_p \longrightarrow \mathrm{Aut}(\mathbb{Z}_q)$ είναι ο τετριμμένος και γι' αυτό στη συγκεκριμμένη περίπτωση το εσωτερικό ημιευθύ γινόμενο $G = C_q \rtimes C_p$ είναι ισόμορφο με το εξωτερικό ευθύ γινόμενο $\mathbb{Z}_q \times \mathbb{Z}_p$.

(β′). Αν $p \mid q-1$, τότε από τα προηγούμενα συμπεραίνουμε ότι εκτός του τετριμμένου ομομορφισμού $\tau : \mathbb{Z}_p \longrightarrow \mathrm{Aut}(\mathbb{Z}_q), \forall [z]_p \in \mathbb{Z}_p, \tau([z]_p) = \mathrm{Id}_{\mathbb{Z}_q}$ υπάρχουν και άλλοι μη τετριμμένοι ομομορφισμοί, επειδή η $\mathrm{Aut}(\mathbb{Z}_q)$ ως κυκλική ομάδα περιέχει για κάθε διαιρέτη τής τάξης της, ιδιαιτέρως για τον διαιρέτη p, και υποομάδα αντίστοιχης τάξης. Μπορούμε λοιπόν να εμφυτέσουμε την $\mathbb{Z}_p$, μέσω ενός μονομορφισμού $\theta : \mathbb{Z}_p \longrightarrow \mathrm{Aut}(\mathbb{Z}_q)$, εντός τής ομάδας αυμορφισμών τής $\mathbb{Z}_q$. Έτσι στη συγκεκριμένη περίπτωση έχουμε ή $G = C_q \rtimes C_p \cong \mathbb{Z}_q \times \mathbb{Z}_p$ ή $G = C_q \rtimes C_p \cong \mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p$, όπου ο $\theta : \mathbb{Z}_p \longrightarrow \mathrm{Aut}(\mathbb{Z}_q)$ είναι ένας μονομορφισμός.

Έστω ότι $\theta : \mathbb{Z}_p \longrightarrow \mathrm{Aut}(\mathbb{Z}_q)$ και $\phi : \mathbb{Z}_p \longrightarrow \mathrm{Aut}(\mathbb{Z}_q)$ είναι δύο μη τετριμμένοι ομομορφισμοί. Προφανώς, οι θ και ϕ είναι αμφότεροι μονομορφισμοί, αφού η $\mathbb{Z}_p$ είναι πρώτης τάξης p. Θα δείξουμε ότι τα εξωτερικά ημιευθέα γινόμενα $\mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p$ και $\mathbb{Z}_q \rtimes_\phi \mathbb{Z}_p$ είναι ισόμορφα. Παρατηρούμε ότι οι μη τετριμμένες υποομάδες $\mathrm{Im}\theta$ και $\mathrm{Im}\phi$ τής $\mathrm{Aut}(\mathbb{Z}_q)$ είναι και οι δύο τάξης p, αφού είναι και οι δύο ισόμορφες με την $\mathbb{Z}_p$. Συνεπώς, $\mathrm{Im}\theta = \mathrm{Im}\phi$, αφού η $\mathrm{Aut}(\mathbb{Z}_q)$ ως κυκλική ομάδα έχει μόνο μία υποομάδα τάξης s για κάθε διαιρέτη s τής τάξης της.

Επομένως, ορίζεται η απεικόνιση

$$\phi^{-1} \circ \theta : \mathbb{Z}_p \xrightarrow{\theta} \mathrm{Im}\theta = \mathrm{Im}\phi \xrightarrow{\phi^{-1}} \mathbb{Z}_p,$$

η οποία είναι ένας αυτομορφισμός τής $\mathbb{Z}_p$.
Από το Λήμμα 6.2.2 γνωρίζουμε ότι τα εξωτερικά ημιευθέα γινόμενα $\mathbb{Z}_p \rtimes_\phi \mathbb{Z}_q$ και $\mathbb{Z}_p \rtimes_{\phi\circ(\phi^{-1}\circ\theta)} \mathbb{Z}_q$ είναι ισόμορφες ομάδες. Έτσι, αφού $\phi\circ(\phi^{-1}\circ\theta) = \theta$, καταλήγουμε ότι $\mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p \cong \mathbb{Z}_q \rtimes_\phi \mathbb{Z}_p$. □

Όπως θα δούμε, η επόμενη πρόταση βεβαιώνει ότι αν, ο ομομορφισμός $\theta : \mathbb{Z}_p \longrightarrow \mathrm{Aut}(\mathbb{Z}_q)$ δεν είναι ο τετριμμένος, τότε το εξωτερικό ημιευθύ γινόμενο $\mathbb{Z}_p \rtimes_\theta \mathbb{Z}_q$ δεν είναι **ποτέ** αβελιανή ομάδα.

Πρόταση 6.2.4. *Έστω ότι* $(N, \star_N)$, $(H, \star_H)$ *είναι δύο ομάδες και ότι* $\theta : H \to \mathrm{Aut}(N)$ *είναι ένας ομομορφισμός ομάδων. Τα ακόλουθα είναι ισοδύναμα:*

(α') *Η ταυτοτική απεικόνιση* $\mathrm{Id} : N \rtimes_\theta H \to N \times H, (n, h) \to (n, h)$ *από το εξωτερικό ημιευθύ γινόμενο* $N \rtimes_\theta H$ *στο εξωτερικό ευθύ γινόμενο* $N \times H$ *είναι ένας ομομορφισμός ομάδων.*

(β') *Ο ομομορφισμός* $\theta : H \to \mathrm{Aut}(N)$ *είναι τετριμμένος.*

(γ') *Η υποομάδα* $\{e_N\} \times H$ *τού εξωτερικού ημιευθέος γινομένου* $N \rtimes_\theta H$ *είναι ορθόθετη.*

Απόδειξη. «(α') $\Rightarrow$ (β')» Λόγω τής υπόθεσης, το γινόμενο δύο οποιωνδήποτε στοιχείων τής ομάδας $N \rtimes_\theta H$ συμπίπτει με το αντίστοιχο γινόμενο στην ομάδα $N \times H$. Έτσι έχουμε:

$$\forall (n, h), (\bar{n}, \bar{h}) \in N \rtimes_\theta H : (n, h) \star (\bar{n}, \bar{h}) = (n \star_N \theta_h(\bar{n}), h \star_H \bar{h}) =$$
$$(n \star_N \bar{n}, h \star_H \bar{h}).$$

Επομένως, $\forall n, \bar{n} \in N, \forall h \in H$ είναι: $n \star_N \theta_h(\bar{n}) = n \star_N \bar{n} \Leftrightarrow \theta_h(\bar{n}) = \bar{n}$. Ώστε, $\forall h \in H, \theta_h = \mathrm{Id}_N$ και συνεπώς ο θ είναι τετριμμένος.

«(β') $\Rightarrow$ (γ')» Αφού ο θ είναι ο τετριμμένος ομομορφισμός, η πράξη τής $N \rtimes_\theta H$, συμπίπτει με την πράξη τής $N \times H$, δηλαδή οι ομάδες $N \rtimes_\theta H$ και $N \times H$ ταυτίζονται. Αλλά στο εξωτερικό ευθύ γινόμενο $N \times H$ αμφότεροι οι παράγοντες $\{e_N\} \times H$ και $N \times \{e_H\}$ είναι ορθόθετες υποομάδες.

«(γ') $\Rightarrow$ (α')» Επειδή $\{e_N\} \times H \trianglelefteq N \rtimes_\theta H$, έχουμε $\forall (n, h) \in N \rtimes_\theta H$ και $\forall (e_N, \bar{h}) \in \{e_N\} \times H$ ότι το στοιχείο $(n, h) \star (e_N, \bar{h}) \star (n, h)^{-1}$ ανήκει στην $\{e_N\} \times H$. Έχουμε:

$$(n, h) \star (e_N, \bar{h}) \star (n, h)^{-1} = (n \star_N \theta_h(e_N), h \star_H \bar{h}) \star (\theta_{h^{-1}}(n^{-1}), h^{-1}) =$$
$$\left(n \star_N \theta_{h \star_H \bar{h}}\left(\theta_{h^{-1}}(n^{-1})\right), h \star_H \bar{h} \star_H h^{-1}\right) =$$
$$(n \star_N \theta_{h \star_H \bar{h} \star_H h^{-1}}(n^{-1}), h \star_H \bar{h} \star_H h^{-1}) \in \{e_N\} \times H.$$

Γι΄αυτό

$$\forall n \in N, h, \bar{h} \in H : \; n \star_N \theta_{h \star_H \bar{h} \star_H h^{-1}}(n^{-1}) = e_N \Leftrightarrow \theta_{h \star_H \bar{h} \star_H h^{-1}}(n^{-1}) = n^{-1} \Leftrightarrow$$
$$\theta_{\bar{h}}(n^{-1}) = \theta_h \circ \theta_{h^{-1}}(n^{-1}) = n^{-1}.$$

Ώστε $\forall \bar{h} \in H, n \in N$, $\theta_{\bar{h}}(n) = n$, δηλαδή $\forall \bar{h} \in H$, $\theta_{\bar{h}} = \mathrm{Id}_N$. Επομένως, ο ομομορφισμός $\theta : H \to \mathrm{Aut}(N)$ είναι ο τετριμμένος και γι' αυτό το εξωτερικό ημιευθύ γινόμενο $N \rtimes_\theta H$ ταυτίζεται με το εξωτερικό ευθύ γινόμενο $N \times H$ και η ταυτοτική απεικόνιση $\mathrm{Id} : N \rtimes_\theta H \to N \times H, (n, h) \to (n, h)$ είναι ένας ομομορφισμός ομάδων. □

Πόρισμα 6.2.5. *Έστω ότι* $(N, \star_N)$, $(H, \star_H)$ *είναι δύο ομάδες, ότι* $\theta : H \to \mathrm{Aut}(N)$ *είναι ένας ομομορφισμός ομάδων και ότι* $N \rtimes_\theta H$ *είναι το αντίστοιχο εξωτερικό ημιευθύ γινόμενο.*

Η ομάδα $N \rtimes_\theta H$ *είναι αβελιανή αν, και μόνο αν, οι* N, H *είναι αβελιανές ομάδες και ο ομομορφισμός* θ *είναι τετριμμένος.*

Απόδειξη. «$\Leftarrow$» Προφανές, αφού η $N \rtimes_\theta H$ συμπίπτει με το εξωτερικό ευθύ γινόμενο $N \times H$, οι παράγοντες τού οποίου είναι αβελιανές ομάδες και ως εκ τούτου το $N \times H$ είναι επίσης αβελιανή ομάδα.
«$\Rightarrow$» Αν η ομάδα $N \rtimes_\theta H$ είναι αβελιανή, τότε προφανώς η υποομάδα $\{e_N\} \times H$ είναι μια ορθόθετη υποομάδα τής $N \rtimes_\theta H$. Από την προηγούμενη πρόταση συμπεραίνουμε ότι ο ομομορφισμός θ είναι τετριμμένος και ότι η $N \rtimes_\theta H$ συμπίπτει με το εξωτερικό ευθύ γινόμενο $N \times H$. Επειδή τώρα το εξωτερικό ευθύ γινόμενο $N \times H$ είναι μια αβελιανή ομάδα, έχουμε ότι και οι παράγοντές του N και H είναι επίσης αβελιανές ομάδες. □

Έτσι για το ημιευθύ γινόμενο δύο κυκλικών ομάδων με τάξεις δύο διαφορετικούς πρώτους αριθμούς έχουμε το εξής:

Πόρισμα 6.2.6. *Έστω ότι* p *και* q *είναι δύο πρώτοι αριθμοί με* $p < q$. *Το εξωτερικό ημιευθύ γινόμενο* $\mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p$ *είναι μια αβελιανή ομαδα αν, και μόνο αν, ο ομομορφισμός* $\theta : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$ *είναι τετριμμένος. Στην περίπτωση αυτή* $\mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p = \mathbb{Z}_q \times \mathbb{Z}_p$.

6.3 Για ποιές Τιμές τού $n \in \mathbb{N}$ είναι κάθε Ομάδα Τάξης n κυκλική;

Ολοκληρώνουμε τη σύντομη διαδρομή στη Θεωρία Ομάδων δίνοντας απάντηση στο ανωτέρω ερώτημα. Πρόκειται για ένα πολύ φυσιολογικό ερώτημα, που μια μερική του απάντηση είναι γνωστή σε όποιονδήποτε έχει παρακολουθησει ένα εισαγωγικό μάθημα στην Άλγεβρα:

Αν ο $n \in \mathbb{N}$ *είναι ένας πρώτος αριθμός, τότε κάθε ομάδα τάξης* n *είναι κυκλική.*
Στο παρόν κείμενο διαπιστώσαμε επίσης ότι *κάθε ομάδα τάξης* pq *είναι κυκλική, όταν* p *και* q *είναι δύο πρώτοι αριθμοί με* $p < q$ *και* $p \nmid q - 1$, βλ. Προτάσεις 2.2.2 και 6.2.3.

Ας δούμε το γενικό αποτέλεσμα που θα αποδείξουμε:

Θεώρημα 6.3.1. *Έστω* n *ένας πάγιος φυσικός. Κάθε ομάδα τάξης* n *είναι κυκλική αν, και μόνο αν, οι αριθμοί* n *και* $\phi(n)$ *είναι σχετικώς πρώτοι, όπου* ϕ *είναι η συνάρτηση Euler-*ϕ.

Παρατηρήσεις 6.3.1. Υπενθυμίζουμε τα εξής:

(α') Η τιμή $\phi(n)$ τής συνάρτησης Euler-ϕ επί τού φυσικού n ισούται με το πλήθος των στοιχείων τού συνόλου $\mathcal{M} = \{m \in \mathbb{N} \mid 1 \leq m \leq n,\ \text{Μ.Κ.Δ}\ (m, n) = 1\}$.

(β') Αν $n = n'n''$ με Μ.Κ.Δ.$(n', n'') = 1$, τότε $\phi(n) = \phi(n')\phi(n'')$.

(γ') Αν $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ είναι η ανάλυση ενός φυσικού $n \geq 2$ σε γινόμενο θετικών δυνάμεων πρώτων αριθμών $p_i, 1 \leq i \leq s$, διαφορετικών ανά δύο, τότε

$$\phi(n) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \ldots \phi(p_s^{\alpha_s}).$$

(δ') Αν p^α είναι μια θετική δύναμη ενός πρώτου αριθμού, τότε $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Επιπλέον, παρατηρούμε τα εξής:

(ε') Έστω ότι $n > 1$ είναι ένας φυσικός με Μ.Κ.Δ.$(n, \phi(n)) = 1$, τότε ο n δεν διαιρείται από το τετράγωνο κανενός πρώτου αριθμού, δηλαδή η ανάλυση τού n σε γινόμενο πρώτων αριθμών είναι

$n = p_1 p_2 \ldots p_s$, όπου οι $p_i, 1 \leq i \leq s$ είναι πρώτοι αριθμοί διαφορετικοί ανά δύο. (*)

Πράγματι, αν υπήρχε κάποιος πρώτος p με $p^2 \mid n$, τότε ο n θα διέθετε την ανάλυση $n = p^\alpha n'$, όπου Μ.Κ.Δ.$(p, n') = 1$ και $\alpha \geq 2$. Αλλά τότε $\phi(n) = (p^\alpha - p^{\alpha-1})\phi(n')$ και συνεπώς ο p θα διαιρούσε και τον n και τον $\phi(n)$, άρα και τον Μ.Κ.Δ.$(n, \phi(n)) = 1$, που είναι άτοπο.

Στην περίπτωση αυτή όπου ο φυσικός n έχει μια ανάλυση σε γινόμενο πρώτων όπως στην (*), τότε λέμε ότι ο n είναι *ελεύθερος τετραγώνων*.

(στ') Αν για κάποιο $n \in \mathbb{N}$, είναι κάθε ομάδα τάξης n κυκλική, τότε ο n είναι ελεύθερος τετραγώνων.

Αν ο n δεν ήταν ελεύθερος τετραγώνων, τότε θα υπήρχε κάποιος πρώτος p με $p^2 \mid n$ και τότε ο n θα διέθετε μια ανάλυση τής μορφής $n = p^\alpha n'$, $\alpha \geq 2$, όπου Μ.Κ.Δ.$(p, n') = 1$.
Θεωρούμε το εξωτερικό ευθύ γινόμενο $G = (C_p \times C_p \cdots \times C_p) \times C_{n'}$, όπου C_p και $C_{n'}$ είναι οι κυκλικές ομάδες με αντίστοιχες τάξεις p και n' και όπου το πλήθος των κυκλικών παραγόντων C_p στο εξωτερικό ευθύ γινόμενο G ισούται με $\alpha \geq 2$. Η G είναι μια ομάδα τάξης $p^\alpha n' = n$, η οποία δεν είναι κυκλική, αφού δεν διαθέτει στοιχείο τάξης $n = p^\alpha n'$. (Η μέγιστη τάξη των στοιχείων τής G ισούται με pn' (*γιατί;*).) Αυτό όμως αντίκειται στην υπόθεση που κάναμε ότι για τον συγκεκριμένο n, κάθε ομάδα ταξης n είναι κυκλική. Συνεπώς, ο n είναι ελεύθερος τετραγώνων.

(ζ') Αν ο φυσικός n είναι ελεύθερος τετραγώνων, τότε και κάθε διαιρέτης n' τού n είναι ελεύθερος τετραγώνων. Επιπλέον ο $\phi(n')$ είναι διαιρέτης τού $\phi(n)$.

(η') Αν $(G, \star)$ είναι μια ομάδα με τάξη n, όπου ο Μ.Κ.Δ.$(n, \phi(n)) = 1$ και $H = \langle a \rangle$ είναι μια κυκλική υποομάδα της, τότε ο ορθοθέτης $N_G(H) = \{g \in G \mid gHg^{-1} =$

$H\}$ τής H συμπίπτει με τον κεντροποιητή $C_G(a) = \{g \in G \mid ga = ag\}$ τού γεννήτορα a τής H.

Έχουμε $C_G(a) \leq N_G(H)$, διότι αν $g \in C_G(a)$ και $h \in H$, τότε υπάρχει $s \in \mathbb{N} \cup \{0\}$ με $h = a^s$ και

$$ghg^{-1} = ga^s g^{-1} = (gag^{-1})^s = h \in H.$$

Θα δείξουμε τώρα ότι $N_G(H) \leq C_G(a)$. Πράγματι αν $g \in N_G(H)$, τότε η συζυγία $\sigma_g : H \to H, h \to ghg^{-1}$, είναι στοιχείο τής ομάδας $\mathrm{Aut}(H)$ των αυτομορφισμών τής H. Από το Παράδειγμα 2.2.1 γνωρίζουμε ότι η τάξη τής ομάδας $\mathrm{Aut}(H)$ ισούται με $\phi(n')$, όπου n' είναι η τάξη τής κυκλικής ομάδας H. Επομένως, η τάξη $\circ(\sigma_g)$ τού σ_g είναι ένας διαιρέτης τής τάξης $\phi(n')$ τής H. Επειδή, λόγω τού (ε'), ο n είναι ελεύθερος τετραγώνων γνωρίζουμε, από το (ζ'), ότι $\phi(n') \mid \phi(n)$ και γι' αυτό έχουμε ότι $\circ(\sigma_g) \mid \phi(n)$.

Αφού για κάθε $s \in \mathbb{N}$, η συζυγία $\sigma_{g^s} : H \to H, h \to g^s hg^{-s}$ ισούται με τη συζυγία $(\sigma_g)^s$ (*γιατί;*), διαπιστώνουμε ότι $(\sigma_g)^{\circ(g)} = \sigma_{g^{\circ(g)}} = \sigma_{e_G} = \mathrm{Id}_H$, όπου $\circ(g)$ είναι η τάξη τού g και Id_H ο ταυτοτικός αυτομορφισμός τής H. Επομένως, $\circ(\sigma_g) \mid \circ(g)$ και αφού η τάξη $\circ(g)$ τού $g \in N_G(H) \leq G$ διαιρεί την τάξη n τής G, συμπεραίνουμε ότι $\circ(\sigma_g) \mid n$.

Αφού όμως Μ.Κ.Δ.$(n, \phi(n)) = 1$ και επειδή όπως διαπιστώσαμε $\circ(\sigma_g) \mid \phi(n)$ και $\circ(\sigma_g) \mid n$, συμπεραίνουμε ότι $\circ(\sigma_g) = 1$, δηλαδή $\sigma_g = \mathrm{Id}_H$. Ιδιαιτέρως, $\sigma_g(a) = a$ και γι' αυτό $gag^{-1} = a$. Ώστε, όταν $g \in N_G(H)$, τότε $g \in C_G(a)$ και συνεπώς $N_G(H) \leq C_G(a)$.

Έτσι αποδείξαμε ότι $N_G(H) = C_G(a)$, για κάθε κυκλική υποομάδα $H = \langle a \rangle$ τής G.

Απόδειξη. **(Η απόδειξη τού Θεωρήματος 6.3.1)**
«$\Rightarrow$» Έστω ότι για κάποιον φυσικό n, κάθε ομάδα τάξης n είναι κυκλική. Θα δείξουμε ότι ο Μ.Κ.Δ.$(n, \phi(n)) = 1$. Σύμφωνα με το $(\sigma\tau')$ των Παρατηρήσεων 6.3.1, ο n είναι ελεύθερος τετραγώνων, δηλαδή ισούται με $p_1 p_2 \dots p_s$, όπου οι $p_i, 1 \leq i \leq s$ είναι πρώτοι αριθμοί διαφορετικοί ανά δύο και ως εκ τούτου ο $\phi(n)$ ισούται με $(p_1 - 1)(p_2 - 1) \dots (p_s - 1)$.

Αν ήταν ο Μ.Κ.Δ.$(n, \phi(n)) \neq 1$, τότε θα υπήρχαν κάποιοι δείκτες $i, j, 1 \leq i, j \leq s$, έτσι ώστε $p_i \mid (p_j - 1), 1 \leq j \leq s$. Προφανώς, $j \neq i$ και $p_i < p_j$. Τότε, από το δεύτερο τμήμα τής απόδειξης τής Πρότασης 6.2.3, γνωρίζουμε ότι θα υπήρχε ένας μονομορφισμός $\theta : \mathbb{Z}_{p_i} \to \mathrm{Aut}(\mathbb{Z}_{p_j})$ και ως εκ τούτου το ημιευθύ γινόμενο $\mathbb{Z}_{p_j} \rtimes_\theta \mathbb{Z}_{p_i}$ θα ήταν μια μη αβελιανή ομάδα τάξης $p_i p_j$. Θεωρούμε την κυκλική ομάδα $\mathbb{Z}_{n'}$, όπου $n = p_i p_j n'$ και το εξωτερικό ευθύ γινόμενο $G = (\mathbb{Z}_{p_j} \rtimes_\theta \mathbb{Z}_{p_i}) \times \mathbb{Z}_{n'}$. Η ομάδα G είναι τάξης n και δεν είναι αβελιανή, αφού ο παράγοντας $\mathbb{Z}_{p_j} \rtimes_\theta \mathbb{Z}_{p_i}$ δεν είναι αβελιανός. Συνεπώς, η G δεν είναι κυκλική. Αυτό όμως είναι άτοπο. Ώστε, ο Μ.Κ.Δ.$(n, \phi(n)) = 1$.

«$\Leftarrow$» Θα δείξουμε ότι, για κάθε φυσικό n με Μ.Κ.Δ.$(n, \phi(n)) = 1$, κάθε ομάδα τάξης n είναι κυκλική.

Έστω ότι υπάρχουν φυσικοί n με Μ.Κ.Δ.$(n, \phi(n)) = 1$, όπου όμως δεν είναι κάθε ομάδα τάξης n κυκλική. Μεταξύ αυτών των φυσικών n επιλέγουμε τον μικρότερο, ας τον ονομάσουμε m. Προφανώς, ο συγκεκριμένος m είναι ένας σύνθετος αριθμός και αφού ο Μ.Κ.Δ.$(m, \phi(m)) = 1$, συμπεραίνουμε από το (ε') των Παρατηρήσεων 6.3.1, ότι ο m είναι ελεύθερος τετραγώνων,

Έστω $(G, \star)$ μια ομάδα τάξης m, η οποία δεν είναι κυκλική. Θα δείξουμε ότι δεν μπορεί να υπάρχει τέτοια ομάδα. Παρατηρούμε ότι η G δεν είναι ούτε αβελιανή, αφού αν ήταν, τότε θα ήταν και κυκλική, επειδή ο m είναι ελεύθερος τετραγώνων, βλ. Πόρισμα 3.2.7.

Αν m' είναι ένας διαιρέτης τού m, τότε Μ.Κ.Δ.$(m', \phi(m')) = 1$. Αφού αν, δ είναι ένας κοινός διαιρέτης των m' και $\phi(m')$, τότε ο δ είναι επίσης κοινός διαιρέτης των m και $\phi(m)$, επειδή $m' \mid m$ και επειδή $\phi(m') \mid \phi(m)$, βλ. (ζ') των Παρατηρήσεων 6.3.1.

Λόγω αυτής τής παρατήρησης, συμπεραίνουμε ότι

οι γνήσιες υποομάδες τής G ***και οι πηλικοομάδες τής*** G ***με ορθόθετες μη τετριμμένες υποομάδες της είναι κυκλικές***, **(*)**

αφού οι τάξεις τους είναι πάντοτε γνήσιοι διαιρέτες τού m.

Το κέντρο $Z(G)$ τής G είναι γνήσια υποομάδα της G επειδή, όπως είδαμε, η G δεν είναι αβελιανή. Τώρα λόγω τού (*), το κέντρο $Z(G)$, ως γνήσια υποομάδα τής G, οφείλει να είναι κυκλική. Επιπλέον, $Z(G) = \{e_G\}$. Πράγματι, αν ήταν $Z(G) \neq \{e_G\}$, τότε επειδή και πάλι λόγω τού (*), η πηλικοομάδα $G/Z(G)$ είναι κυκλική , συμπεραίνουμε ότι η G είναι κυκλική. Πράγμα άτοπο. Ώστε, $Z(G) = \{e_G\}$.

Αφού όμως $Z(G) = \{e_G\}$, τότε $\forall g \in G, g \neq e_G$ συμπεραίνουμε ότι ο κεντροποιητής $C_G(g)$ τού g είναι μια γνήσια υποομάδα τής G, αφού αν $C_G(g) = G$, τότε το $g \in Z(G)$.

Έστω $\mathcal{M}$ μια οποιαδήποτε μεγιστοτική υποομάδα τής G. Η τάξη $[\mathcal{M} : 1]$ τής $\mathcal{M}$ είναι ≥ 2, αφού ο m είναι σύνθετος αριθμός και για κάθε πρώτο διαιρέτη p τού m υπάρχει στοιχείο αντίστοιχης τάξης, βλ. Θεώρημα Cauchy (Θεώρημα 1.3.8). Λόγω τού (*), η $\mathcal{M}$ είναι μια κυκλική υποομάδα τής G και γι'αυτό $\mathcal{M} \leq C_G(g)$, όπου g είναι οποιοδήποτε στοιχείο τής $\mathcal{M}$. Αλλά για κάθε $g \in \mathcal{M}, g \neq e_G$, επειδή η $\mathcal{M}$ είναι μεγιστοτική και η $C_G(g)$ είναι γνήσια υποομάδα τής G, συμπεραίνουμε ότι $\mathcal{M} = C_G(g)$.

Ισχυριζόμαστε ότι

αν, $\mathcal{M}$ ***και*** $\mathcal{N}$ ***είναι δύο διαφορετικές μεγιστοτικές υποομάδες τής*** G, ***τότε*** $\mathcal{M} \cap \mathcal{N} = \{e_G\}$. **(**)**

Πράγματι, αν ήταν $g \in \mathcal{M} \cap \mathcal{N}$ με $g \neq e_G$, τότε $\mathcal{M} = C_G(g) = \mathcal{N}$, που είναι άτοπο.

Ερχόμαστε τώρα στο κύριο επιχείρημα τής απόδειξης:

Έστω $\mathcal{M}$ μια μεγιστοτική υποομάδα τής G. Κάθε υποομάδα τής G, η οποία είναι συζυγής προς την $\mathcal{M}$, είναι επίσης μεγιστοτική. Πράγματι αν, η $g\mathcal{M}g^{-1}$ περιεχότανε γνησίως σε μια υποομάδα $A < G$, τότε η $\mathcal{M}$ θα περιεχότανε γνησίως στην $g^{-1}Ag$ και γι' αυτό $g^{-1}Ag = G$. Αλλά η $g^{-1}Ag$ έχει το ίδιο πλήθος στοιχείων με την A. Αυτό είναι άτοπο. Ώστε κάθε συζυγής προς την $\mathcal{M}$, είναι επίσης μεγιστοτική υποομάδα τής G. Γι' αυτό, λόγω τού (**), δύο οποιεσδήποτε διαφορετικές συζυγείς προς την $\mathcal{M}$, υποομάδες τής G τέμνονται μόνο στο σύνολο $\{e_G\}$.

Το πλήθος των διαφορετικών συζυγών προς την $\mathcal{M}$, υποομάδων τής G ισούται με τον δείκτη $[\mathsf{G} : \mathsf{N}_{\mathsf{G}}(\mathcal{M})] = [\mathsf{G} : 1]/[\mathcal{M} : 1]$, όπου $\mathsf{N}_{\mathsf{G}}(\mathcal{M})$ είναι ο ορθοθέτης τής $\mathcal{M}$, βλ. το (γ') των Παρατηρήσεων 1.4.2.

Η $\mathcal{M}$, ως γνήσια υποομάδα τής G, είναι κυκλική, ας πούμε ότι $\mathcal{M} = \langle a \rangle$. Γι' αυτό, λόγω τού ($\zeta'$) των Παρατηρήσεων 6.3.1, $\mathsf{N}_{\mathsf{G}}(\mathcal{M}) = \mathsf{C}_{\mathsf{G}}(a)$. Αλλά όπως είδαμε προηγουμένως, $\mathcal{M} = \mathsf{C}_{\mathsf{G}}(g)$, για κάθε $g \in \mathcal{M}, g \neq e_{\mathsf{G}}$. Ιδιαιτέρως, $\mathcal{M} = \mathsf{C}_{\mathsf{G}}(a)$ και συνεπώς $\mathsf{N}_{\mathsf{G}}(\mathcal{M}) = \mathcal{M}$.

Έτσι συμπεραίνουμε ότι το πλήθος των διαφορετικών συζυγών προς την $\mathcal{M}$, υποομάδων τής G ισούται με $[\mathsf{G} : 1]/[\mathcal{M} : 1]$.

Τώρα, το πλήθος των στοιχείων $\neq e_{\mathsf{G}}$ που περιέχει η ένωση των διαφορετικών συζυγών προς την $\mathcal{M}$, υποομάδων τής G ισούται με

$$([\mathcal{M} : 1] - 1)\,\frac{[\mathsf{G} : 1]}{[\mathcal{M} : 1]} = [\mathsf{G} : 1] - \frac{[\mathsf{G} : 1]}{[\mathcal{M} : 1]}.$$

Ο αριθμός $[\mathsf{G} : 1] - [\mathsf{G} : 1]/[\mathcal{M} : 1]$ είναι γνήσια μικρότερος από $[\mathsf{G} : 1] - 1$, αφού ο $[\mathcal{M} : 1] \neq 1$ είναι ένας γνήσιος διαιρέτης τού $[\mathsf{G} : 1]$. Γι'αυτό υπάρχει ένα στοιχείο $x \in \mathsf{G}, x \neq e_{\mathsf{G}}$, το οποίο δεν περιέχεται σε καμία από τις συζυγείς ως προς την $\mathcal{M}$, υποομάδες τής G. Αλλά το συγκεκριμένο στοιχείο x οφείλει να περιέχεται σε κάποια μεγιστοτική υποομάδα $\mathcal{N}$, η οποία προφανώς δεν είναι συζυγής ως προς την $\mathcal{M}$.

Όπως και προηγουμένως, διαπιστώνουμε ότι το πλήθος των στοιχείων $\neq e_{\mathsf{G}}$ που περιέχει η ένωση των διαφορετικών συζυγών προς την $\mathcal{N}$, υποομάδων τής G ισούται με

$$([\mathcal{N} : 1] - 1)\,\frac{[\mathsf{G} : 1]}{[\mathcal{N} : 1]} = [\mathsf{G} : 1] - \frac{[\mathsf{G} : 1]}{[\mathcal{N} : 1]}.$$

Το μόνο κοινό στοιχείο όλων αυτών των μεγιστοτικών υποομάδων που είναι ή συζυγείς προς την $\mathcal{M}$ ή συζυγείς προς την $\mathcal{N}$ είναι το e_{G}. Επομένως, η G περιέχει τουλάχιστον τόσα πολλά στοιχεία, διαφορετικά από το e_{G}, όσο είναι το άθροισμα των στοιχείων $\neq e_{\mathsf{G}}$, που περιέχει η ένωση των διαφορετικών συζυγών προς την $\mathcal{M}$ υποομάδων τής G και η ένωση των διαφορετικών συζυγών προς την $\mathcal{N}$ υποομάδων τής G.

Συνεπώς,

$$\left([\mathsf{G} : 1] - \frac{[\mathsf{G} : 1]}{[\mathcal{M} : 1]}\right) + \left([\mathsf{G} : 1] - \frac{[\mathsf{G} : 1]}{[\mathcal{N} : 1]}\right) \lneqq [\mathsf{G} : 1] \Leftrightarrow$$
$$\left(1 - \frac{1}{[\mathcal{M} : 1]}\right) + \left(1 - \frac{1}{[\mathcal{N} : 1]}\right) \lneqq 1.$$

Επειδή $[\mathcal{M} : 1] \geq 2$ και $[\mathcal{N} : 1] \geq 2$, η τελευταία γνήσια! ανισότητα δεν είναι αληθής και έτσι οδηγούμεθα σε άτοπο. Ώστε, δεν υπάρχει μη κυκλική ομάδα G τάξης m με Μ.Κ.Δ.$(m, \phi(m)) = 1$ και η απόδειξη τού θεωρήματος έχει πλέον ολοκληρωθεί. □

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