Νίκος Μαρμαρίδης

ΘΕΩΡΙΑ ΟΜΑΔΩΝ

Νίκος Μαρμαρίδης

Ομότιμος Καθηγητής Μαθηματικού Τμήματος
Πανεπιστημίου Ιωαννίνων

Θεωρία Ομάδων

Προχωρημένη Θεωρία Ομάδων

Ελληνικά Ακαδημαϊκά Ηλεκτρονικά
Συγγράμματα και Βοηθήματα
www.kallipos.gr

Θεωρία Ομάδων

Συγγραφή
Μαρμαρίδης Νίκος

Κριτικός αναγνώστης
Μπεληγιάννης Απόστολος

ΣΥΝΔΕΣΜΟΣ ΕΛΛΗΝΙΚΩΝ ΑΚΑΔΗΜΑΪΚΩΝ ΒΙΒΛΙΟΘΗΚΩΝ

Εθνικό Μετσόβιο Πολυτεχνείο
Ηρώων Πολυτεχνείου 9, 15780 Ζωγράφου

http://www.kallipos.gr

ISBN: 978-960-603-240-0

Πρόλογος

Το παρόν κείμενο αποτελεί μια εισαγωγή στη Θεωρία Ομάδων. Στο πρώτο, σχετικά εκτενές, κεφάλαιο παρουσιάζονται οι βασικές γνώσεις τής θεωρίας. Το συγκεκριμένο κεφάλαιο μπορεί να αποτελέσει και τμήμα οποιουδήποτε εισαγωγικού μαθήματος στην Άλγεβρα. Στα επόμενα δύο κεφάλαια μελετάται η Θεωρία Sylow με τη βοήθεια τής δράσης ομάδας επί ενός συνόλου και δίνεται έμφαση στις πεπερασμένες απλές ομάδες. Στο τέταρτο κεφάλαιο ταξινομούνται οι πεπερασμένες αβελιανές ομάδες. Το πέμπτο κεφάλαιο διαπραγματεύεται το Θεώρημα Jordan–Hölder. Στο έκτο κεφάλαιο συζητούνται διεξοδικά οι επιλύσιμες ομάδες και αποδεικνύεται λεπτομερώς ότι κάθε ομάδα τάξης < 60 είναι επιλύσιμη. Το έβδομο κεφάλαιο πραγματεύεται τις επεκτάσεις ομάδων και την ειδική περίπτωση των ημιευθέων γινομένων. Στο τέλος τού κεφαλαίου παρουσιάζεται μια ικανή και αναγκαία συνθήκη ώστε κάθε ομάδα τάξης n να είναι κυκλική, βλ. [21]. Στο Παράρτημα υπάρχει μια σύντομη ιστορία τής ταξινόμησης των πεπερασμένων απλών ομάδων, βλ. [35]. Σε όλο το κείμενο δίνεται ιδιαίτερη έμφαση στις διεδρικές ομάδες, που χρησιμοποιούνται συχνά σε παραδείγματα και εφαρμογές. Οι λυμένες ασκήσεις αποτελούν ουσιαστικά και μέρος τής θεωρίας, χωρίς όμως να είναι απαραίτητες στο υπόλοιπο θεωρητικό τμήμα, τουλάχιστον σε μια πρώτη ανάγνωση. Για παράδειγμα, οι ασκήσεις Α64, Α65, Α94 και Α95 περιέχουν μια πλήρη απόδειξη για το πότε η ομάδα $\mathbb{U}_n$ των αντιστρέψιμων στοιχείων τής $\mathbb{Z}_n$ είναι κυκλική.

Νίκος Μαρμαρίδης

Λειψοί Δωδεκανήσων– Θεσσαλονίκη, Οκτώβριος 2015

Περιεχόμενα

1 Στοιχειώδεις Γνώσεις από τη Θεωρία Ομάδων 1
- 1.1 Πράξεις . . . 1
- 1.2 Ομάδες . . . 10
- 1.3 Υποομάδες . . . 52
- 1.4 Πλευρικές Κλάσεις, Θεώρημα Lagrange . . . 67
- 1.5 Κυκλικές Ομάδες, Τάξη Στοιχείου . . . 81
- 1.6 Ορθόθετες Υποομάδες, Πηλικοομάδες . . . 101
- 1.7 Ομομορφισμοί . . . 112
- 1.8 Ομάδες Μετατάξεων . . . 141

2 Δράση Ομάδας επί ενός Συνόλου 164
- 2.1 Δράσεις και μετατακτικές Αναπαραστάσεις . . . 164
- 2.2 Τροχιές και Σταθεροποιητές . . . 169
  - 2.2.1 Το Θεώρημα Burnside . . . 172
- 2.3 Δράση Ομάδας επί Υποσυνόλων της και Πλευρικών Κλάσεών της . . . 175
  - 2.3.1 Αριστερή Δράση . . . 175
  - 2.3.2 Δράση στις αριστερές πλευρικές Κλάσεις . . . 176
  - 2.3.3 Το Θεώρημα Cauchy . . . 183
- 2.4 Συζυγία . . . 185
  - 2.4.1 Επεκτείνοντας τη Δράση Συζυγίας . . . 187
  - 2.4.2 Η Εξίσωση των Κλάσεων . . . 188
- 2.5 Ποια είναι η Τιμή τής Πιθανότητας δύο Στοιχεία μιας Ομάδας να μετατίθενται; . . . 192

3 Θεωρία Sylow 197
- 3.1 Τα Θεωρήματα Sylow . . . 197
- 3.2 Εφαρμογές τής Θεωρίας Sylow . . . 205
  - 3.2.1 Αυτομορφισμοί Ομάδας και χαρακτηριστικές Υποομάδες . . . 210
  - 3.2.2 Η εναλλάσσουσα ομάδα $\mathbb{A}_5$ είναι απλή . . . 213
  - 3.2.3 Η απλότητα τής $\mathbb{A}_n$, για $n \geq 5$ . . . 214
  - 3.2.4 Κριτήρια για το πότε μια Ομάδα δεν είναι απλή . . . 216

3.2.5 Πεπερασμένες Υποομάδες τής Ομάδας των αντιστρέψιμων Στοιχείων ενός Σώματος . . . 218

4 Ευθέα Γινόμενα Ομάδων **224**
4.1 Εξωτερικό και Εσωτερικό ευθύ Γινόμενο . . . 224
4.1.1 Εξωτερικό ευθύ Γινόμενο . . . 224
4.1.2 Εσωτερικό ευθύ Γινόμενο . . . 226
4.1.3 Σχέση εξωτερικού και εσωτερικού ευθέος Γινομένου . . . 228
4.2 Η Ταξινόμηση των πεπερασμένων αβελιανών Ομάδων . . . 230

5 Το Θεώρημα Jordan–Hölder **243**
5.1 Προκαταρκτικές Έννοιες . . . 243
5.1.1 Υποορθόθετες και ορθόθετες Σειρές για μια Ομάδα . . . 243
5.2 Το Θεώρημα Εκλέπτυνσης Schreier . . . 245
5.2.1 Το Λήμμα τής Πεταλούδας . . . 245
5.3 Συνθετικοί και κυρίαρχοι Παράγοντες . . . 251
5.3.1 Περιγραφή συνθετικών ή κυρίαρχων Παραγόντων . . . 251
5.3.2 Οι χαρακτηριστικώς απλές πεπερασμένες Ομάδες . . . 253

6 Επιλύσιμες Ομάδες **259**
6.1 Προκαταρκτικές Έννοιες . . . 259
6.2 Μεταθέτες και παράγωγες Ομάδες . . . 262
6.2.1 Η παράγωγη Σειρά μιας Ομάδας . . . 263
6.3 Μηδενοδύναμες Ομάδες . . . 266
6.3.1 Τα ανώτερα Κέντρα μιας Ομάδας . . . 266
6.4 Οι Ομάδες τάξης <60 είναι επιλύσιμες . . . 274

7 Επεκτάσεις Ομάδων **287**
7.1 Προκαταρκτικές Έννοιες . . . 287
7.2 Το Πρόβλημα τής Επέκτασης και το ημιευθύ Γινόμενο . . . 288
7.2.1 Ημιευθύ Γινόμενο . . . 288
7.3 Για ποιές Τιμές τού $n \in \mathbb{N}$ είναι κάθε Ομάδα Τάξης n κυκλική; . . . 302

Παράρτημα **311**

Βιβλιογραφία **315**

Κεφάλαιο 1

Στοιχειώδεις Γνώσεις από τη Θεωρία Ομάδων

Στο παρόν κεφάλαιο θα ασχοληθούμε με την έννοια τής ομάδας. Πρόκειται για ένα σύνολο μαζί με έναν «μηχανισμό», που από δύο οποιαδήποτε στοιχεία τού συνόλου δημιουργεί ένα τρίτο. Ο συγκεκριμένος «μηχανισμός» οφείλει να υπακούει σε ορισμένους κανόνες. Το σύνολο μαζί με τον «μηχανισμό» ονομάζεται «ομάδα». Η έννοια τής «ομάδας» πρωτοεμφανίστηκε τον 19ο αιώνα στην προσπάθεια τής επίλυσης των αλγεβρικών εξισώσεων και κατόπιν επεκτάθηκε στη μελέτη τής συμμετρίας γεωμετρικών αλλά και γενικότερων μαθηματικών αντικειμένων. Σήμερα, αποτελεί μια θεμελιώδη έννοια με ισχυρή παρουσία σε πολλούς κλάδους των Σύγχρονων Μαθηματικών.

1.1 Πράξεις

Έστω ότι S είναι ένα μη κενό σύνολο. Μια *διμελής πράξη* ή απλώς *πράξη* επί τού S είναι μια απεικόνιση

$$\varphi : S \times S \to S, \;\; (s,t) \;\mapsto\; \varphi((s,t)).$$

Η εικόνα $\varphi((s,t))$ τού στοιχείου (s,t) ονομάζεται το *αποτέλεσμα τής πράξης* επί των στοιχείων s, t.
Συνήθως, μια πράξη επί τού S δηλώνεται με κάποιο σύμβολο που δεν είναι απαραίτητα αλφαβητικό γράμμα, όπως είναι τα $+$, $!$, $-$, $\star$, $\circ$, $\#$, $\cdot$, $\spadesuit$, $\clubsuit$ κ.ο.κ.. Επιπλέον, όταν η απεικόνιση $\star : S \times S \to S$ είναι μια διμελής πράξη, τότε το αποτέλεσμά της, δηλαδή η εικόνα $\star((s,t))$, δηλώνεται ως $s \star t$. Ορισμένες φορές το αποτέλεσμα μιας πράξης πάνω σε δύο στοιχεία s, t τού S δηλώνεται απλώς με την παράθεση τού ενός στοιχείου δίπλα στο άλλο, δηλαδή ως st.

Ορισμός 1.1.1. Ένα σύνολο $S \neq \emptyset$ μαζί με μια διμελή πράξη $\star : S \times S \to S$, ονομάζεται *αλγεβρική δομή με μια πράξη* και συμβολίζεται ως $(S, \star)$.

Παράδειγμα 1.1.2. (α′) Το ζεύγος $(\mathbb{N}, +)$, όπου $\mathbb{N}$ είναι το σύνολο των φυσικών αριθμών και «+» είναι η γνωστή πρόσθεση φυσικών αποτελεί μια αλγεβρική δομή. Εδώ, η πρόσθεση ορίζει την απεικόνιση

$$+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \;\; (n, m) \;\; \mapsto \;\; +((m, n)) := m + n.$$

(β′) Το ζεύγος $(\mathbb{Z}, -)$, όπου $\mathbb{Z}$ είναι το σύνολο των ακέραιων αριθμών και «−» είναι η γνωστή αφαίρεση των ακέραιων αποτελεί επίσης μια αλγεβρική δομή. Εδώ, η αφαίρεση ορίζει την απεικόνιση

$$- : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, \;\; (n, m) \;\; \mapsto \;\; -((m, n)) := m - n.$$

(γ′) Θεωρούμε και πάλι την αφαίρεση «−» των ακέραιων αριθμών, περιορίζοντάς τη στο σύνολο των φυσικών $\mathbb{N}$. Τώρα, η αφαίρεση «−» δεν ορίζει μια αλγεβρική δομή επί τού συνόλου $\mathbb{N}$ των φυσικών αριθμών, δηλαδή δεν ορίζει μια απεικόνιση από το $\mathbb{N} \times \mathbb{N}$ στο $\mathbb{N}$, αφού η αφαίρεση φυσικών δεν δίνει πάντοτε φυσικό αριθμό. Επί παραδείγματι, η διαφορά $2 - 3 = -1$ δεν είναι φυσικός αριθμός.

(δ′) Έστω T το υποσύνολο $\{-1, 0, 1\}$ των ακέραιων αριθμών και ας θεωρήσουμε την πράξη «+» τής πρόσθεσης των ακέραιων αριθμών. Η «+» δεν ορίζει μια αλγεβρική δομή επί τού T, αφού το άθροισμα δύο στοιχείων τού T, δεν είναι πάντοτε στοιχείο τού T. Για παράδειγμα, το $1 + 1 = 2 \notin T$. Με άλλα λόγια η πρόσθεση «+» δεν χορηγεί απεικόνιση από το $T \times T$ στο T.

(ε′) Ας θεωρήσουμε και πάλι το προηγούμενο υποσύνολο $T = \{-1, 0, 1\}$ των ακέραιων αριθμών και τον πολλαπλασιασμό «·» ακέραιων αριθμών. Εδώ, ο «·» ορίζει μια απεικόνιση $\cdot : T \times T \to T$, αφού το γινόμενο δύο στοιχείων τού T είναι πάντοτε στοιχείο τού T. Συνεπώς, το ζεύγος $(T, \cdot)$ αποτελεί μια αλγεβρική δομή.

(στ′) Έστω X ένα μη κενό σύνολο και S_X το σύνολο των αμφιρριπτικών απεικονίσεων, από το X στον εαυτό του. Υπενθυμίζουμε ότι γενικά μια απεικόνιση $f : X \to Y$ από ένα σύνολο X σε ένα σύνολο Y ονομάζεται αμφιρριπτική, όταν είναι ενριπτική, δηλαδή «ένα προς ένα» $(1 - 1)$ και επιρριπτική, δηλαδή «επί». Επιπλέον, υπενθυμίζουμε ότι η σύνθεση $f \circ g$ δύο αμφιρριπτικών απεικονίσεων $f, g : X \to X$ είναι και πάλι μια αμφιρριπτική απεικόνιση. Συνεπώς, το ζεύγος $(S_X, \circ)$, όπου $\circ : S_X \times S_X \to S_X$ είναι η απεικόνιση, η οποία ορίζεται ως $(f, g) \mapsto f \circ g, \forall (f, g) \in S_X \times S_X$ αποτελεί μια αλγεβρική δομή. Η συγκεκριμένη αλγεβρική δομή έχει ιδιαίτερη σημασία στην Άλγεβρα και μάλιστα θα μελετηθεί σε μια ξεχωριστή ενότητα. Το ζεύγος $(S_X, \circ)$ ονομάζεται η *ομάδα συμμετρίας* ή η *συμμετρική ομάδα* τού συνόλου X και κάθε στοιχείο της λέγεται μια *μετάταξη* ή *μετάθεση* των στοιχείων τού X.

Ιδιότητες πράξεων

Έστω $(S, \star)$ μια αλγεβρική δομή.
Η πράξη «⋆» ονομάζεται *προσεταιριστική*, όταν για κάθε $s, t, r \in S$ ισχύει:

$$s \star (t \star r) = (s \star t) \star r.$$

Στη συγκεκριμένη περίπτωση για το αποτέλεσμα αυτό, θα γράφουμε απλώς $s \star t \star r$, αφού είναι ανεξάρτητο από τον τρόπο με τον οποίο εκτελείται η πράξη, χωρίς όμως να αλλαχθεί η σειρά των παραγόντων.
Η πράξη «$\star$» ονομάζεται *μεταθετική* ή *αβελιανή*, όταν για κάθε $s, t \in S$ ισχύει:

$$s \star t = t \star s.$$

Παράδειγμα 1.1.3.

(α′) Η πράξη τής πρόσθεσης ακέραιων αριθμών (συνεπώς και των φυσικών αριθμών) είναι προσεταιριστική και μεταθετική.

(β′) Η πράξη τού πολλαπλασιασμού ακέραιων αριθμών (συνεπώς και των φυσικών αριθμών) είναι προσεταιριστική και μεταθετική.

(γ′) Η πράξη τής αφαίρεσης ακέραιων αριθμών δεν είναι ούτε προσεταιριστική ούτε μεταθετική. (Να υπολογίσετε τα $(1-2)-3$ και $1-(2-3)$ καθώς και τα $1-2$ και $2-1$.)

(δ′) Η πράξη «$\circ$» τής σύνθεσης αμφιρριπτικών απεικονίσεων από ένα μη κενό σύνολο X στον εαυτό του είναι προσεταιριστική. Πράγματι, αν $f, g, h : X \to X$ είναι αμφιρριπτικές απεικονίσεις, τότε $(f \circ g) \circ h = f \circ (g \circ h)$, αφού για κάθε $x \in X$ είναι:

$$[(f \circ g) \circ h](x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = [f \circ (g \circ h)](x).$$

Όπως θα δούμε παρακάτω, η πράξη «$\circ$» είναι μεταθετική, ακριβώς τότε, όταν το πλήθος των στοιχείων τού X είναι 1 ή 2.

Παρατήρηση 1.1.4. Έστω ότι $(S, \star)$ είναι μια αλγεβρική δομή, όπου η πράξη «$\star$» είναι προσεταιριστική. Η προσεταιριστικότητα τής «$\star$» γενικεύεται σε οποιοδήποτε πεπερασμένο πλήθος στοιχείων τού S.
Για παράδειγμα,

$$\forall s, t, p, q \in S : ((s \star t) \star p) \star q = (s \star (t \star p)) \star q = s \star ((t \star p) \star q) = s \star (t \star p \star q).$$

Ισχυριζόμαστε ότι αν η «$\star$» είναι μια προσεταιριστική πράξη, τότε το γινόμενο n το πλήθος στοιχείων τού S είναι ανεξάρτητο από τον τρόπο που εκτελείται η πράξη, αρκεί να μην αλλάζει η σειρά των παραγόντων.
Θα κάνουμε μια τυπική απόδειξη με τη βοήθεια πλήρους επαγωγής ως προς n.
Για $n = 2$ ή 3 δεν χρειάζεται να αποδείξουμε κάτι. Έστω ότι αυτό αληθεύει για οποιοδήποτε πλήθος στοιχείων k, όπου $2 \leq k \leq n$. Συμβολίζουμε με $s_1 \star \cdots \star s_k$ το αποτέλεσμα τής πράξης, όταν $2 \leq k \leq n$, αφού έχουμε υποθέσει ότι είναι ανεξάρτητο από τον τρόπο που εκτελείται η πράξη, αρκεί να μην έχει αλλάξει η σειρά των παραγόντων. Θα το αποδείξουμε, όταν το πλήθος των στοιχείων ισούται με $n+1$. Ας υποθέσουμε ότι εκτελώντας με δύο διαφορετικούς τρόπους την πράξη «$\star$» στα $s_1, s_2, \ldots, s_{n+1} \in S$ καταλήγουμε στα αποτελέσματα $(s_1 \star \cdots \star s_i) \star (s_{i+1} \star \cdots \star s_{n+1})$ και $(s_1 \star \cdots \star s_j) \star (s_{j+1} \star \cdots \star s_{n+1})$, όπου

$2 \leq i, j \leq n$. Χωρίς περιορισμό τής γενικότητας μπορούμε να υποθέσουμε ότι $i < j$. Τώρα έχουμε:

$$\begin{aligned}
&(s_1 \star \cdots \star s_j) \star (s_{j+1} \star \cdots \star s_{n+1}) = \\
&(s_1 \star \cdots \star s_i \star s_{i+1} \star \cdots \star s_j) \star (s_{j+1} \star \cdots \star s_{n+1}) = \\
&((s_1 \star \cdots \star s_i) \star (s_{i+1} \star \cdots \star s_j)) \star (s_{j+1} \star \cdots \star s_{n+1}) = \\
&(s_1 \star \cdots \star s_i) \star ((s_{i+1} \star \cdots \star s_j) \star (s_{j+1} \star \cdots \star s_{n+1})) = \\
&(s_1 \star \cdots \star s_i) \star (s_{i+1} \star \cdots \star s_{n+1}).
\end{aligned}$$

Άρα, τα δύο αποτελέσματα είναι ίσα.

Ο πίνακας πράξης

Έστω ότι $S = \{s_1, s_2, \ldots, s_n\}$ είναι ένα πεπερασμένο σύνολο και ότι

$$\star : S \times S \to S$$

είναι μια πράξη επί τού S.
Ο πίνακας στοιχείων τού S, που αποτελείται από n γραμμές και n στήλες και ο οποίος έχει το στοιχείο $s_i \star s_j$ στην (i, j)–θέση, για κάθε i και j, $1 \leq i, j \leq n$, ονομάζεται ο *πίνακας τής πράξης* $\star$ *επί* τού συνόλου S, βλ. Σχήμα 1.1.

$\star$	s_1	s_2	$\ldots$	s_i	$\ldots$	s_j	$\ldots$	s_n
s_1	$s_1 \star s_1$	$s_1 \star s_2$	$\ldots$	$s_1 \star s_i$	$\ldots$	$s_1 \star s_j$	$\ldots$	$s_1 \star s_n$
s_2	$s_2 \star s_1$	$s_2 \star s_2$	$\ldots$	$s_2 \star s_i$	$\ldots$	$s_2 \star s_j$	$\ldots$	$s_2 \star s_n$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
s_i	$s_i \star s_1$	$s_i \star s_2$	$\ldots$	$s_i \star s_i$	$\ldots$	$s_i \star s_j$	$\ldots$	$s_i \star s_n$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
s_j	$s_j \star s_1$	$s_j \star s_2$	$\ldots$	$s_j \star s_i$	$\ldots$	$s_j \star s_j$	$\ldots$	$s_j \star s_n$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
s_n	$s_n \star s_1$	$s_n \star s_2$	$\ldots$	$s_n \star s_i$	$\ldots$	$s_n \star s_j$	$\ldots$	$s_n \star s_n$

Σχήμα 1.1: Ο πίνακας πράξης επί τού συνόλου S.

Παρατήρηση 1.1.5. (α′) Όταν είναι γνωστός ο πίνακας πράξης ενός συνόλου, τότε μπορεί να διαπιστωθεί αμέσως, αν η πράξη που περιγράφει ο πίνακας είναι μεταθετική ή όχι. Πράγματι, είναι αρκετό να παρατηρήσει κανείς ότι για κάθε i, j με $1 \leq i, j, \leq n$, τα στοιχεία $s_i \star s_j$ και $s_j \star s_i$, κείνται συμμετρικά ως προς την κύρια διαγώνιο τού πίνακα. Συνεπώς, η πράξη είναι μεταθετική, αν και μόνο αν, τα στοιχεία τού πίνακα, που κείνται συμμετρικά ως προς την κύρια διαγώνιό του, είναι ίσα.

(β′) Αν S είναι ένα σύνολο με n στοιχεία, τότε κάθε πίνακας με n γραμμές και n στήλες, που συνίσταται από στοιχεία τού S, ορίζει μια πράξη επί τού S.

Παράδειγμα 1.1.6. (α′) Θεωρούμε το σύνολο $S = \{s, t, r\}$ και την πράξη

$$\begin{aligned}
&\star : S \times S \to S, \;\; \text{όπου} \\
&\star\,((s,s)) = s \star s = s, \quad \star((s,t)) = s \star t = t, \quad \star((s,r)) = s \star r = r, \\
&\star\,((t,s)) = t \star s = t, \quad \star((t,t)) = t \star t = r, \quad \star((t,r)) = t \star r = s, \\
&\star\,((r,s)) = r \star s = r, \quad \star((r,t)) = r \star t = s, \quad \star((r,r)) = r \star r = t.
\end{aligned}$$

Ο πίνακας τής πράξης «$\star$» παρουσιάζεται στο Σχήμα 1.2.

$\star$	s	t	r
s	s	t	r
t	t	r	s
r	r	s	t

Σχήμα 1.2: Ο πίνακας τής πράξης «$\star$» επί τού συνόλου S.

Παρατηρούμε ότι πρόκειται για μια μεταθετική πράξη.

(β′) Θεωρούμε το σύνολο $S' = \{s', t', r', q'\}$ και τον πίνακα

	s'	t'	r'	q'
s'	q'	r'	r'	q'
t'	t'	r'	t'	t'
r'	s'	s'	q'	q'
q'	r'	r'	r'	r'

Ο πίνακας ορίζει μια μοναδική πράξη $\Diamond : S' \times S' \to S'$ επί τού συνόλου S' κατά τον εξής τρόπο:

$$\begin{aligned}
&s'\Diamond s' = q', \quad && s'\Diamond t' = r', \quad && s'\Diamond r' = r', \quad && s'\Diamond q' = q', \\
&t'\Diamond s' = t', && t'\Diamond t' = r', && t'\Diamond r' = t', && t'\Diamond q' = t', \\
&r'\Diamond s' = s', && r'\Diamond t' = s', && r' \star r' = q', && r'\Diamond q' = q', \\
&q'\Diamond s' = r', && q'\Diamond t' = r', && q'\Diamond r' = r', && q'\Diamond q' = r'.
\end{aligned}$$

Η πράξη «$\Diamond$» δεν είναι μεταθετική, αφού ο πίνακας που την ορίζει δεν είναι συμμετρικός ως προς την κύρια διαγώνιό του. Επί παραδείγματι, $t'\Diamond s' = t' \neq r' = s'\Diamond t'$.

Ασκήσεις στην έννοια τής πράξης

Λυμένες Ασκήσεις

Α 1. Να εξεταστεί αν το σύνολο $S = \{1, 2, 3, 4, 5, 6, 7, 8\} \subseteq \mathbb{N}$ μαζί με τη δοσμένη αντιστοιχία $(s, t) \mapsto s \star t$ απαρτίζει αλγεβρική δομή. Όταν απαρτίζει αλγεβρική δομή, τότε να εξεταστεί αν η πράξη είναι προσεταιριστική ή/και μεταθετική και να σχηματιστεί ο αντίστοιχος πίνακας πράξης.

(α′) $\forall (s, t) \in S \times S, (s, t) \mapsto s \star t := \max\{s, t\}$, όπου $\max\{s, t\}$ είναι ο μεγαλύτερος των s, t.

(β′) $\forall (s, t) \in S \times S, (s, t) \mapsto s \star t := s + t$, όπου «$+$» είναι η πρόσθεση των ακέραιων,

(γ′) $\forall (s, t) \in S \times S, (s, t) \mapsto s \star t := s + t - \max\{s, t\}$, όπου «$+$», αντιστοίχως «$-$» είναι η πρόσθεση, αντιστοίχως αφαίρεση, των ακέραιων,

(δ′) $\forall (s, t) \in S \times S, (s, t) \mapsto s \star t := \frac{s}{t}$, όπου $\frac{s}{t}$ είναι το αντίστοιχο κλάσμα των ρητών αριθμών,

(ε′) $\forall (s, t) \in S \times S, (s, t) \mapsto s \star t := \frac{s}{d(s,t)}$, όπου $d(s, t)$ είναι ο μέγιστος κοινός διαιρέτης των s και t και $\frac{s}{d(s,t)}$ είναι το αντίστοιχο κλάσμα των ρητών αριθμών.

Λύση. (α′) Η αντιστοιχία που δίδεται ορίζει μια απεικόνιση $\star : S \times S \to S$, αφού το $\max\{s, t\}$ δύο οποιωνδήποτε στοιχείων τού S είναι και πάλι στοιχείο τού S. Η συγκεκριμένη απεικόνιση είναι προσεταιριστική, αφού

$$\forall s, t, r \in S : s \star (t \star r) = \max\{s, \max\{t, r\}\} = \max\{s, t, r\} = \max\{\max\{s, t\}, r\}\} = (s \star t) \star r.$$

Η συγκεκριμένη απεικόνιση είναι μεταθετική, αφού

$$\forall s, t \in S : s \star t = \max\{s, t\} = \max\{t, s\} = t \star s.$$

Ο πίνακας τής πράξης είναι ο εξής:

$\star$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	2	3	4	5	6	7	8
3	3	3	3	4	5	6	7	8
4	4	4	4	4	5	6	7	8
5	5	5	5	5	5	6	7	8
6	6	6	6	6	6	6	7	8
7	7	7	7	7	7	7	7	8
8	8	8	8	8	8	8	8	8

(β′) Η αντιστοιχία που δίδεται δεν ορίζει απεικόνιση $\star : S \times S \to S$, αφού το άθροισμα δύο στοιχείων τού S δεν είναι πάντοτε στοιχείο τού S. Για παράδειγμα $8\star 8 = 8+8 = 16 \notin S$.

(γ′) Η αντιστοιχία που δίδεται ορίζει μια απεικόνιση $\star : S \times S \to S$, αφού

$$\forall s,t \in S, \quad s \star t = s + t - \max\{s,t\} = \begin{cases} s, & \text{όταν } \max\{s,t\} = t \in S \\ t, & \text{όταν } \max\{s,t\} = s \in S \end{cases}$$

Παρατηρώντας την ανωτέρω ανάλυση, διαπιστώνουμε ότι $\forall s, t \in S$, το αποτέλεσμα $s \star t$ συμπίπτει με το ελάχιστο των s, t, δηλαδή $s \star t = \min\{s,t\}$. Έτσι συμπεραίνουμε αμέσως ότι η συγκεκριμένη απεικόνιση είναι προσεταιριστική, αφού

$$\begin{aligned}\forall s,t,r \in S : s \star (t \star r) &= \min\{s, \min\{t,r\}\} = \min\{s,t,r\} = \\ &\min\{\min\{s,t\}, r\}\} = (s \star t) \star r.\end{aligned}$$

Η συγκεκριμένη απεικόνιση είναι μεταθετική, αφού

$$\forall s,t \in S : s \star t = \min\{s,t\} = \min\{t,s\} = t \star s.$$

Ο πίνακας τής πράξης είναι ο εξής:

$\star$	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1
2	1	2	2	2	2	2	2	2
3	1	2	3	3	3	3	3	3
4	1	2	3	4	4	4	4	4
5	1	2	3	4	5	5	5	5
6	1	2	3	4	5	6	6	6
7	1	2	3	4	5	6	7	7
8	1	2	3	4	5	6	7	8

(δ′) Η αντιστοιχία που δίδεται δεν ορίζει απεικόνιση $\star : S \times S \to S$, αφού το πηλίκο δύο στοιχείων τού S δεν είναι πάντοτε στοιχείο τού S. Για παράδειγμα $1 \star 2 = \frac{1}{2} \notin S$.

(ε′) Η αντιστοιχία που δίδεται ορίζει μια απεικόνιση $\star : S \times S \to S$, αφού οι θετικοί διαιρέτες των στοιχείων τού S είναι στοιχεία τού S και $\forall s \in S$, το $s \star t := \frac{s}{d(s,t)}$ είναι πάντοτε διαιρέτης τού s.

Η συγκεκριμένη απεικόνιση δεν είναι προσεταιριστική, αφού δεν είναι αληθές ότι $\forall s,t,r \in S$ είναι $s \star (t \star r) = (s \star t) \star r$. Για παράδειγμα:

$$2 \star (5 \star 8) = 2 \star \frac{5}{d(5,8)} = 2 \star \frac{5}{1} = \frac{2}{d(2,5)} = \frac{2}{1} = 2, \text{ ενώ}$$
$$(2 \star 5) \star 8 = \frac{2}{d(2,5)} \star 8 = \frac{2}{1} \star 8 = \frac{2}{d(2,8)} = \frac{2}{2} = 1.$$

Η συγκεκριμένη απεικόνιση δεν είναι ούτε μεταθετική, αφού δεν είναι αληθές ότι $\forall s, t \in S$ είναι $s \star t = t \star s$. Για παράδειγμα:

$$2 \star 8 = \frac{2}{d(2,8)} = \frac{2}{2} = 1 \text{ ενώ } 8 \star 2 = \frac{8}{d(8,2)} = \frac{8}{2} = 4.$$

Ο πίνακας τής πράξης «$\star$» είναι ο εξής:

$\star$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	2	1	2	1	2	1
3	3	3	1	3	3	1	3	3
4	4	2	4	1	4	2	4	1
5	5	5	5	5	1	5	5	5
6	6	3	2	3	6	1	6	3
7	7	7	7	7	7	7	1	7
8	8	4	8	2	8	4	8	1

A 2. Να δοθεί παράδειγμα μιας αλγεβρικής δομής $(S, \star)$, όπου το $S = \{s_1, s_2, s_3, s_4, s_5\}$ είναι ένα σύνολο με πέντε στοιχεία και η «$\star$» είναι μια μεταθετική πράξη.

Λύση. Όπως ήδη γνωρίζουμε, βλ. Παρατήρηση 1.1.5, όταν ένα σύνολο $S = \{s_1, s_2, \ldots, s_n\}$ αποτελείται από n το πλήθος στοιχεία, τότε μια πράξη «$\star$» επί τού S προσδιορίζεται πλήρως από τις τιμές $s_i \star s_j, 1 \leq i, j \leq n$. Έτσι, μια πράξη μπορεί να οριστεί μέσω ενός πίνακα με n γραμμές και n στήλες, όπου κάθε συνιστώσα του είναι ένα οποιοδήποτε στοιχείο τού S. Επομένως, για να απαντήσουμε στο ερώτημα, αρκεί να σχηματίσουμε έναν τέτοιου είδους πίνακα, ο οποίος να είναι συμμετρικός ως προς την κύρια διαγώνιό του, αφού τότε θα έχουμε $\forall i, j, s_i \star s_j = s_j \star s_i$.

Παρακάτω παρουσιάζουμε δύο διαφορετικούς πίνακες, οι οποίοι είναι συμμετρικοί ως προς την κύρια διαγώνιο, δίνοντας έτσι δύο διαφορετικές απαντήσεις στο ερώτημα τής άσκησης.

$\star$	s_1	s_2	s_3	s_4	s_5
s_1	s_2	s_2	s_1	s_1	s_5
s_2	s_2	s_1	s_3	s_4	s_2
s_3	s_1	s_3	s_5	s_4	s_5
s_4	s_1	s_4	s_4	s_5	s_1
s_5	s_5	s_2	s_5	s_1	s_4

,

$\star$	s_1	s_2	s_3	s_4	s_5
s_1	s_3	s_3	s_3	s_3	s_3
s_2	s_3	s_3	s_3	s_3	s_3
s_3	s_3	s_3	s_3	s_3	s_3
s_4	s_3	s_3	s_3	s_3	s_3
s_5	s_3	s_3	s_3	s_3	s_3

Στον πρώτο πίνακα τα στοιχεία (οι συνιστώσες του) είναι τοποθετημένα συμμετρικά ως προς την κύρια διαγώνιο. Στον δεύτερο πίνακα, όλα τα στοιχεία (οι συνιστώσες του) είναι ίσα και έτσι ο πίνακας είναι κατά τετριμμένο τρόπο επίσης συμμετρικός ως προς την κύρια διαγώνιό του.

Α 3. Να δειχθεί ότι η πράξη $\circ : S_X \times S_X \to S_X$ τής συμμετρικής ομάδας ενός συνόλου X, βλ. Παράδειγμα 1.1.2(στ′), είναι μεταθετική (αβελιανή) μόνον όταν το πλήθος των στοιχείων τού X είναι μικρότερο ή ίσο τού 2.

Λύση. Έστω ότι $X = \{x\}$. Τότε υπάρχει μόνο μία αμφιρριπτική απεικόνιση από το X στο X, η οποία είναι η ταυτοτική $\mathrm{Id}_X : X \to X, x \mapsto x$. Άρα το S_X έχει μόνο ένα στοιχείο, δηλαδή $S_X = \{\mathrm{Id}_X\}$ και προφανώς η σύνθεση $\circ : S_X \times S_X \to S_X$ είναι μεταθετική πράξη.

Έστω ότι $X = \{x, y\}$. Τότε υπάρχουν ακριβώς δύο αμφιρριπτικές απεικονίσεις από το X στο X: η ταυτοτική $\mathrm{Id}_X : X \to X, x \mapsto x, y \mapsto y$ και η $\varphi : X \to X, x \mapsto y, y \mapsto x$. Ο πίνακας τής σύνθεσης $\circ : S_X \times S_X \to S_X$ είναι ο

$\circ$	Id_X	φ
Id_X	Id_X	φ
φ	φ	Id_X

και η πράξη «$\circ$» είναι μεταθετική.

Έστω ότι $X = \{x, y, z\}$. Θεωρούμε τις αμφιρριπτικές απεικονίσεις $\sigma : X \to X$ και $\tau : X \to X$ με $\sigma(x) = x, \sigma(y) = z, \sigma(z) = y$ και $\tau(x) = y, \tau(y) = x, \tau(z) = z$. Παρατηρούμε ότι $\sigma \circ \tau(x) = \sigma(y) = z$, ενώ $\tau \circ \sigma(x) = \tau(x) = y$. Επομένως, $\sigma \circ \tau \neq \tau \circ \sigma$ και εδώ η $\circ : S_X \times S_X \to S_X$ δεν είναι πλέον μια μεταθετική πράξη.

Έστω ότι το X έχει τουλάχιστον τρία διαφορετικά στοιχεία, ας πούμε τα x, y, z. Θεωρούμε τις απεικονίσεις

$$\begin{aligned} &\sigma : X \to X, x \mapsto x, y \mapsto z, z \mapsto y \text{ και } a \mapsto a, \forall a \in X, \text{ όταν } a \neq x, y, z \\ &\tau : X \to X, x \mapsto y, y \mapsto x, z \mapsto z \text{ και } a \mapsto a, \forall a \in X, \text{ όταν } a \neq x, y, z. \end{aligned}$$

Οι σ και τ είναι προφανώς αμφιρριπτικές και $\sigma \circ \tau \neq \tau \circ \sigma$, αφού $\sigma \circ \tau(x) = \sigma(y) = z \neq y = \tau(x) = \tau \circ \sigma(x)$. Επομένως, η σύνθεση $\circ : S_X \times S_X \to S_X$ δεν είναι μεταθετική πράξη, όταν το πλήθος των στοιχείων τού X είναι γνησίως μεγαλύτερο από 2.

Προτεινόμενες Ασκήσεις

ΠΑ 1. Να εξεταστεί, αν οι επόμενες αντιστοιχίες ορίζουν μια αλγεβρική δομή επί τού συνόλου των ακέραιων αριθμών $\mathbb{Z}$:

(α′) $\forall (z, w) \in \mathbb{Z} \times \mathbb{Z}, (z, w) \mapsto z \star w := \sqrt{z + w}$,

(β′) $\forall (z, w) \in \mathbb{Z} \times \mathbb{Z}, (z, w) \mapsto z \star w := (z + w)^2$,

(γ′) $\forall (z, w) \in \mathbb{Z} \times \mathbb{Z}, (z, w) \mapsto z \star w := z - w - zw$,

(δ′) $\forall (z, w) \in \mathbb{Z} \times \mathbb{Z}, (z, w) \mapsto z \star w := 0$,

(ε′) $\forall (z, w) \in \mathbb{Z} \times \mathbb{Z}, (z, w) \mapsto z \star w := z$.

Όταν ορίζεται αλγεβρική δομή, τότε να εξεταστεί αν η πράξη είναι προσεταιριστική ή μεταθετική.

ΠΑ 2. Έστω το σύνολο $S = \{0, 1\} \subset \mathbb{Z}$. Να εξεταστεί, αν η αντιστοιχία $\forall \alpha, \beta \in S, (\alpha, \beta) \mapsto \alpha \star \beta := \alpha + \beta$ ορίζει μια αλγεβρική δομή επί τού S.

ΠΑ 3. Έστω το σύνολο $S = \{-1, 1\} \subset \mathbb{Z}$. Να εξεταστεί, αν η αντιστοιχία $\forall \alpha, \beta \in S, (\alpha, \beta) \mapsto \alpha \star \beta := \frac{\alpha}{\beta}$ ορίζει μια αλγεβρική δομή επί τού S.

ΠΑ 4. Θεωρούμε το σύνολο $S = \{\alpha, \beta, \gamma, \delta, \varepsilon\}$. Να συμπληρωθεί κατά τέτοιον τρόπο ο επόμενος πίνακας, ώστε να αποτελεί τον πίνακα μιας μεταθετικής πράξης «$\star$» επί τού S.

$*$	α	β	γ	δ	ε
α					
β					
γ					
δ					
ε					

ΠΑ 5. Θεωρούμε το σύνολο $S = \{1, 2, 3, 4, 5\}$. Να συμπληρωθεί κατά τέτοιον τρόπο ο επόμενος πίνακας, ώστε να αποτελεί τον πίνακα μιας προσεταιριστικής πράξης «$\star$» επί τού S.

$*$	1	2	3	4	5
1					
2					
3					
4					
5					

ΠΑ 6. Έστω ότι S είναι ένα σύνολο και ότι $\mathcal{P}(S) = \{A \mid A \subseteq S\}$ είναι το δυναμοσύνολο τού S.

(α′) Να δειχθεί ότι η αντιστοιχία $\bigcup : \mathcal{P}(S) \times \mathcal{P}(S) \to \mathcal{P}(S), (A, B) \mapsto A \bigcup B$, όπου «$\bigcup$» η συνολοθεωρητική ένωση, ορίζει μια αλγεβρική δομή επί τού συνόλου $\mathcal{P}(S)$ με την «$\bigcup$» να είναι μια προσεταιριστική και μεταθετική πράξη.

(β′) Να δειχθεί ότι η αντιστοιχία $\bigcap : \mathcal{P}(S) \times \mathcal{P}(S) \to \mathcal{P}(S), (A, B) \mapsto A \bigcap B$, όπου «$\bigcap$» η συνολοθεωρητική τομή, ορίζει μια αλγεβρική δομή επί τού συνόλου $\mathcal{P}(S)$ με την «$\bigcap$» να είναι μια προσεταιριστική και μεταθετική πράξη.

1.2 Ομάδες

Αλγεβρικές δομές που ικανοποιούν επιπλέον ιδιότητες αποτελούν ένα από τα κύρια αντικείμενα μελέτης στα Μαθηματικά. Μεταξύ αυτών εξέχουσα θέση κατέχουν οι ομάδες.

Ορισμός 1.2.1. Μια αλγεβρική δομή $(G, \star)$ ονομάζεται *ομάδα*, όταν ικανοποιούνται τα ακόλουθα:

(α′) Η πράξη «$\star$» είναι προσεταιριστική.

(β′) Υπάρχει ένα στοιχείο $e \in G$ με την ιδιότητα $\forall g \in G, e \star g = g = g \star e$.

(γ′) Για κάθε $g \in G$, υπάρχει κάποιο $h \in G$ με $g \star h = e = h \star g$.

Όταν επιπλέον η πράξη «$\star$» είναι μεταθετική, δηλαδή, όταν $\forall g, g' \in G$, είναι $g \star g' = g' \star g$, τότε η ομάδα $(G, \star)$ ονομάζεται *αβελιανή* ή *μεταθετική*.

Συμβολισμός.

(α′) **Η πολλαπλασιαστική σημειογραφία.**
Ορισμένες φορές ονομάζουμε την πράξη μιας ομάδας $(G, \star)$ «*πολλαπλασιασμό*», χωρίς να είναι απαραίτητα κάποιος γνωστός πολλαπλασιασμός. Στην περίπτωση αυτή, το αποτέλεσμα τής πράξης $g \star g'$ το ονομάζουμε «*γινόμενο*» των g και g' και το συμβολίζουμε είτε ως $g \cdot g'$ είτε απλώς ως gg'.

(β′) **Η προσθετική σημειογραφία.**
Συχνά, όταν η $(G, \star)$ είναι μια αβελιανή (μεταθετική) ομάδα, τότε χρησιμοποιούμε ως σύμβολο τής πράξης το «$+$», ονομάζουμε «*άθροισμα*» των g και g' το αποτέλεσμα $g + g'$ και αποκαλούμε «*πρόσθεση*» τη συγκεκριμένη πράξη, χωρίς να είναι απαραίτητα κάποια γνωστή πρόσθεση.

Όπως θα δούμε σύντομα, το πλήθος των στοιχείων μιας ομάδας καθορίζει αρκετές από τις ιδιότητες που αυτή έχει.

Ορισμός 1.2.2. Μια ομάδα $(G, \star)$ καλείται *πεπερασμένη*, όταν το πλήθος των στοιχείων τού συνόλου G είναι πεπερασμένο. Διαφορετικά η ομάδα $(G, \star)$ ονομάζεται *άπειρη*.

Ορισμός 1.2.3. Το πλήθος των στοιχείων μιας ομάδας $(G, \star)$ καλείται η *τάξη* τής G και συμβολίζεται με $\circ(G)$ ή με $|G|$ ή με $[G : 1]$, για λόγους που θα δούμε αργότερα.

Όταν λοιπόν η τάξη μιας ομάδας $(G, \star)$ είναι πεπερασμένη, ας πούμε $n \in \mathbb{N}$, τότε επιλέγουμε τον συμβολισμό $[G : 1] = n$ και όταν είναι άπειρη, τότε επιλέγουμε τον συμβολισμό $[G : 1] = \infty$.

Παράδειγμα 1.2.4 (Ομάδες Αριθμών).

(α′) **Η αβελιανή ομάδα των ακέραιων αριθμών με πράξη την πρόσθεση ακέραιων**

Το ζεύγος $(\mathbb{Z}, +)$, όπου $\mathbb{Z}$ είναι το σύνολο των ακεραίων και «$+$» είναι η γνωστή πρόσθεση ακέραιων αριθμών, αποτελεί μια ομάδα.

Πράγματι, το σύνολο $\mathbb{Z}$ των ακεραίων είναι $\neq \emptyset$, η απεικόνιση

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (z, w) \mapsto z + w$$

χορηγεί μια προσεταιριστική πράξη, το 0 των ακέραιων αριθμών ικανοποιεί το αίτημα (β′) τού Ορισμού 1.2.1 και τέλος, όταν $z \in \mathbb{Z}$, τότε ο αντίθετός του ακέραιος, δηλαδή ο $(-z)$, ικανοποιεί το αίτημα (γ′) τού Ορισμού 1.2.1, αφού $z + (-z) = 0 = (-z) + z$.
Επιπλέον, η $(\mathbb{Z}, +)$ αποτελεί μια αβελιανή (μεταθετική) ομάδα, αφού $\forall m, n \in \mathbb{Z}$ έχουμε $m + n = n + m$. Προφανώς, $[\mathbb{Z} : 1] = \infty$.

(β′) **Οι αβελιανές ομάδες των ρητών, πραγματικών και μιγαδικών με πράξη την αντίστοιχη πρόσθεση ρητών, πραγματικών και μιγαδικών αριθμών**

Εντελώς ανάλογα, αποδεικνύεται ότι τα ζεύγη $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ και αντιστοίχως $(\mathbb{C}, +)$, που συνίστανται από τους ρητούς, πραγματικούς και αντιστοίχως μιγαδικούς αριθμούς και τις γνωστές πράξεις τής πρόσθεσης ρητών, πραγματικών και αντιστοίχως μιγαδικών αριθμών, αποτελεί μια αβελιανή (μεταθετική) ομάδα. Προφανώς, $[\mathbb{Q} : 1] = \infty$, $[\mathbb{R} : 1] = \infty$ και $[\mathbb{C} : 1] = \infty$.

(γ′) **Η αβελιανή ομάδα των κλάσεων ισοτιμίας των ακεραίων $\mathbb{Z}$ mod n ή κατά μόδιο $\mathbf{n} \in \mathbb{N}$ με πράξη την πρόσθεση των κλάσεων mod n ή κατά μόδιο n**

Έστω $n \in \mathbb{N}$ ένας πάγιος φυσικός. Επί τού συνόλου $\mathbb{Z}$ θεωρούμε τη σχέση

$$\sim_n = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid \text{ ο } n \text{ διαιρεί τη διαφορά } a - b\}.$$

Από τη Θεωρία Αριθμών, γνωρίζουμε ότι η σχέση «$\sim_n$» είναι μια σχέση ισοδυναμίας.
Δύο ακέραιοι a, b που ανήκουν στην ίδια κλάση ισοδυναμίας ως προς την «$\sim_n$» ονομάζονται *ισότιμοι κατά μόδιο* n και αυτό δηλώνεται γράφοντας $a \equiv b \bmod n$.
Οι κλάσεις ισοδυναμίας τής «$\sim_n$» ονομάζονται *κλάσεις ισοτιμίας κατά μόδιο* n.
Η κλάση ισοτιμίας τού $a \in \mathbb{Z}$ είναι το σύνολο $\{b \in \mathbb{Z} \mid a \equiv b \bmod n\}$ και παριστάνεται με $[a]_n$.
Το $\{[0], [1], [2], \ldots, [n-1]\}$ είναι σύνολο των κλάσεων ισοτιμίας κατά μόδιο n και (προσωρινά) θα το συμβολίζουμε με $\mathbb{Z}/\sim_n$.
Παρατηρούμε ότι για οποιονδήποτε φυσικό $n \in \mathbb{N}$, το $\mathbb{Z}/\sim_n \neq \emptyset$.
Από τη Θεωρία Αριθμών γνωρίζουμε ότι όταν $a \equiv a' \bmod n$ και $b \equiv b' \bmod n$, τότε $(a + b) \equiv (a' + b') \bmod n$. Με άλλα λόγια, όταν $[a]_n = [a']_n$ και $[b]_n = [b']_n$, τότε $[a + b]_n = [a' + b']_n$. Ως εκ τούτου, η αντιστοιχία

$$+_n : (\mathbb{Z}/\sim_n) \times (\mathbb{Z}/\sim_n) \longrightarrow \mathbb{Z}/\sim_n, ([a]_n, [b]_n) \mapsto [a + b]_n$$

αποτελεί μια καλά ορισμένη απεικόνιση. Συνεπώς, η «$+_n$» αποτελεί μια πράξη επί τού $\mathbb{Z}/\sim_n$, η οποία μάλιστα είναι προσεταιριστική και μεταθετική, αφού η πρόσθεση των ακεραίων έχει αυτές τις δύο ιδιότητες.
Παρατηρούμε ότι η κλάση $[0]_n$ ικανοποιεί το αίτημα (β′) τού Ορισμού 1.2.1 επειδή για κάθε $[z]_n \in \mathbb{Z}/\sim_n$ είναι $[z]_n +_n [0]_n = [z + 0]_n = [z]_n = [0 + z]_n = [0]_n +_n [z]_n$.
Επιπλέον, για κάθε $[z]_n \in \mathbb{Z}/\sim_n$, έχουμε $[z]_n +_n [n - z]_n = [z + (n - z)]_n = [0]_n$.
Επομένως, η κλάση $[n - z]_n$ ικανοποιεί το αίτημα (γ′) τού Ορισμού 1.2.1.
Άρα, η αλγεβρική δομή $(\mathbb{Z}/\sim_n, +n)$ είναι μια ομάδα και μάλιστα αβελιανή (μεταθετική).
Η τάξη $[\mathbb{Z}/\sim_n : 1]$ τής $\mathbb{Z}/\sim_n$ ισούται με n, αφού $\mathbb{Z}/\sim_n = \{[0], [1], [2], \ldots, [n-1]\}$.

Συμβολισμός. Η ομάδα των κλάσεων ισοτιμίας $(\mathbb{Z}/\sim_n, +_n)$ παριστάνεται συνήθως ως $(\mathbb{Z}_n, +_n)$ ή ως $(\mathbb{Z}_n, +)$ ή συντομότερα ως $\mathbb{Z}_n$. Η πράξη «$+_n$» παριστάνεται συχνά απλώς ως «$+$» (ιδιαιτέρως όταν είναι σαφές για ποιο n πρόκειται) και ονομάζεται η *πρόσθεση των ακεραίων κατά μόδιο* n.

(δ′) **Οι αβελιανές ομάδες των μη μηδενικών ρητών, των μη μηδενικών πραγματικών και των μη μηδενικών μιγαδικών αριθμών με πράξη τον αντίστοιχο πολλαπλασιασμό ρητών, πραγματικών και μιγαδικών αριθμών**
Το ζεύγος $(\mathbb{Q}^\star, \cdot)$, όπου $\mathbb{Q}^\star$ είναι το σύνολο των μη μηδενικών ρητών αριθμών, δηλαδή το $\mathbb{Q}\setminus\{0\}$ και «$\cdot$» είναι ο γνωστός πολλαπλασιασμός ρητών αριθμών, αποτελεί μια αβελιανή ομάδα.
Πράγματι, $\mathbb{Q}^\star \neq \emptyset$, η απεικόνιση $\cdot : \mathbb{Q}^\star \times \mathbb{Q}^\star \to \mathbb{Q}^\star, (r,s) \mapsto r \cdot s$ είναι μια προσεταιριστική πράξη, το 1 των ρητών αριθμών ικανοποιεί το αίτημα (β′) τού Ορισμού 1.2.1 και τέλος, αν $r \in \mathbb{Q}^\star$, τότε ο αντίστροφός του ρητός, που είναι ο $1/r$ και ο οποίος υπάρχει, αφού $r \neq 0$, ικανοποιεί το αίτημα (γ′) τού Ορισμού 1.2.1, επειδή $r \cdot (1/r) = 1 = (1/r) \cdot r$.
Τέλος, η $(\mathbb{Q}^\star, \cdot)$ αποτελεί μια αβελιανή (μεταθετική) ομάδα, αφού $\forall r, s \in \mathbb{Q}^\star$ έχουμε $r \cdot s = s \cdot r$. Προφανώς, η τάξη $[\mathbb{Q}^\star : 1] = \infty$.
Εντελώς ανάλογα, αποδεικνύεται ότι τα ζεύγη $(\mathbb{R}^\star, \cdot)$ και αντιστοίχως $(\mathbb{C}^\star, \cdot)$, που συνίστανται από τους μη μηδενικούς πραγματικούς, αντιστοίχως μη μηδενικούς μιγαδικούς αριθμούς και τη γνωστή πράξη τού πολλαπλασιασμού «$\cdot$» πραγματικών, αντιστοίχως μιγαδικών αριθμών, αποτελεί μια αβελιανή (μεταθετική) ομάδα. Προφανώς, $[\mathbb{R}^\star : 1] = \infty$ και $[\mathbb{C}^\star : 1] = \infty$.

Παράδειγμα 1.2.5 (Ομάδες από τη Γραμμική Άλγεβρα).

(α′) **Η ομάδα των m × n πινάκων και πράξη την πρόσθεση πινάκων**
Το ζεύγος $(\mathcal{M}_{m\times n}(\mathbb{K}), +)$, όπου $\mathcal{M}_{m\times n}(\mathbb{K})$ είναι το σύνολο των $m \times n$ πινάκων (m, n είναι δύο πάγιοι φυσικοί αριθμοί) με συνιστώσες από το $\mathbb{K}$, όπου $\mathbb{K}$ είναι ένα από τα σύνολα[1] $\mathbb{Q}, \mathbb{R}$ ή $\mathbb{C}$ και «$+$» είναι η πρόσθεση πινάκων, αποτελεί μια ομάδα.

Πράγματι, το $\mathcal{M}_{m\times n}(\mathbb{K})$ είναι $\neq \emptyset$, αφού για οποιουσδήποτε φυσικούς αριθμούς m και n υπάρχουν πάντοτε $m \times n$ πίνακες με συνιστώσες από το $\mathbb{K}$.

Η πράξη τής πρόσθεσης

$$+ : \mathcal{M}_{m\times n}(\mathbb{K}) \times \mathcal{M}_{m\times n}(\mathbb{K}) \longrightarrow \mathcal{M}_{m\times n}(\mathbb{K}), \quad ((a_{ij}), (b_{ij})) \mapsto (c_{ij}) := (a_{ij} + b_{ij})$$

είναι μια καλά ορισμένη απεικόνιση, αφού όταν οι (a_{ij}) και (b_{ij}) είναι δύο $m \times n$ πίνακες, τότε και το άθροισμά τους, δηλαδή ο πίνακας $(a_{ij} + b_{ij})$ είναι επίσης ένας $m \times n$ πίνακας.

Η πράξη τής πρόσθεσης πινάκων είναι προσεταιριστική, αφού η πρόσθεση τού $\mathbb{K}$ είναι προσεταιριστική και αφού δύο $m \times n$ πίνακες $(a_{ij}), (b_{ij})$ είναι ίσοι, αν και μόνο αν, $a_{ij} = b_{ij}$, για κάθε $i, j, 1 \leq i \leq m$ και $1 \leq j \leq n$.

Ο μηδενικός $m \times n$ πίνακας $0_{\mathcal{M}_{m\times n}(\mathbb{K})}$, δηλαδή ο πίνακας που κάθε συνιστώσα του ισούται με $0_{\mathbb{K}}$ ικανοποιεί το αίτημα (β′) τού Ορισμού 1.2.1.

Τέλος, ικανοποιείται και το αίτημα (γ′) τού Ορισμού 1.2.1, αφού για κάθε $(a_{ij}) \in \mathcal{M}_{m\times n}(\mathbb{K})$, υπάρχει ο πίνακας

$$(-a_{ij}) \in \mathcal{M}_{m\times n}(\mathbb{K}) \text{ με } (a_{ij}) + (-a_{ij}) = (a_{ij} - a_{ij}) = (0_{\mathbb{K}}) = 0_{\mathcal{M}_{m\times n}(\mathbb{K})}.$$

[1]Τα $\mathbb{Q}, \mathbb{R}$ ή $\mathbb{C}$ είναι σώματα. Το $\mathbb{K}$ μπορεί να είναι επίσης και οποιοδήποτε άλλο σώμα, αν στη διάρκεια των μέχρι τώρα σπουδών σας έχετε συναντήσει και άλλα σώματα όπως το $\mathbb{Z}_p$ με p πρώτο αριθμό.

Επιπλέον, το ζεύγος $(\mathcal{M}_{m\times n}(\mathbb{K}), +)$ είναι μια αβελιανή (μεταθετική) ομάδα, αφού για κάθε $(a_{ij}), (b_{ij}) \in \mathcal{M}_{m\times n}(\mathbb{K})$ έχουμε:

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}) = (b_{ij} + a_{ij}) = (b_{ij}) + (a_{ij}).$$

Προφανώς, $[\mathcal{M}_{m\times n}(\mathbb{K}) : 1] = \infty$.

(β′) **Η γενική γραμμική ομάδα**
Έστω $\mathrm{GL}_n(\mathbb{K})$ το σύνολο των αντιστρέψιμων $n \times n$ πινάκων, $n \in \mathbb{N}$, με συνιστώσες από το $\mathbb{K}$, όπου το $\mathbb{K}$ είναι ένα από τα σώματα $\mathbb{Q}, \mathbb{R}$ ή $\mathbb{C}$. Προφανώς, $\mathrm{GL}_n(\mathbb{K}) \neq \emptyset$. Υπενθυμίζουμε ότι όταν A, B είναι δύο πίνακες από το $\mathrm{GL}_n(\mathbb{K})$, τότε και το γινόμενό τους $A \cdot B$ ανήκει στο $\mathrm{GL}_n(\mathbb{K})$, αφού ως γνωστόν το γινόμενο δύο αντιστρέψιμων $n \times n$ πινάκων είναι και πάλι ένας αντιστρέψιμος $n \times n$ πίνακας. Έτσι, η απεικόνιση

$$\cdot : \mathrm{GL}_n(\mathbb{K}) \times \mathrm{GL}_n(\mathbb{K}) \to \mathrm{GL}_n(\mathbb{K}), (A, B) \mapsto A \cdot B$$

αποτελεί μια πράξη επί τού $\mathrm{GL}_n(\mathbb{K})$, η οποία όπως γνωρίζουμε από τη Γραμμική Άλγεβρα είναι προσεταιριστική.
Ο μοναδιαίος πίνακας I_n, δηλαδή ο διαγώνιος $n \times n$ πίνακας τού οποίου όλα τα στοιχεία τής κύριας διαγώνιου είναι ίσα με $1_{\mathbb{K}}$, είναι το ουδέτερο στοιχείο ως προς την πράξη «·», αφού για κάθε $A \in \mathrm{GL}_n(\mathbb{K})$ είναι $I_n \cdot A = A = A \cdot I_n$.
Τέλος, για κάθε $A \in \mathrm{GL}_n(\mathbb{K})$ υπάρχει ο αντίστροφος πίνακας A^{-1}, ο οποίος βέβαια ικανοποιεί τις $A \cdot A^{-1} = I_n = A^{-1} \cdot A$. Επομένως, ικανοποιούνται όλα τα αιτήματα τού Ορισμού 1.2.1 και το ζεύγος $(\mathrm{GL}_n(\mathbb{K}), \cdot)$ είναι μια ομάδα, που ονομάζεται η *γενική γραμμική ομάδα βαθμού n υπεράνω τού* $\mathbb{K}$. Η ομάδα αυτή είναι αβελιανή (μεταθετική) μόνο για $n = 1$, αφού όταν $n \geq 2$, τότε υπάρχουν πάντοτε αντιστρέψιμοι πίνακες A, B με $A \cdot B \neq B \cdot A$.

(γ′) **Η ομάδα των πραγματικών ορθογώνιων $n \times n$ πινάκων**
Από τη Γραμμική Άλγεβρα υπενθυμίζουμε ότι ένας $n \times n$ πίνακας A με πραγματικές συνιστώσες ονομάζεται ορθογώνιος, όταν $A \cdot A^t = I_n$, όπου A^t είναι ο ανάστροφος τού A και I_n είναι ο ταυτοτικός $n \times n$ πίνακας, δηλαδή όταν ο A είναι ένας αντιστρέψιμος πίνακας με $A^t = A^{-1}$. Συμβολίζουμε με $\mathcal{O}_n(\mathbb{R})$ το σύνολο των $n \times n$ ορθογώνιων πινάκων. Το ζεύγος $(\mathcal{O}_n(\mathbb{R}), \cdot)$, όπου «·» είναι ο πολλαπλασιασμός πινάκων, αποτελεί μια ομάδα.

Πράγματι, το $\mathcal{O}_n(\mathbb{R})$ είναι $\neq \emptyset$, αφού ο ταυτοτικός $n \times n$ πίνακας I_n είναι ορθογώνιος. Το γινόμενο δύο πινάκων $A, B \in \mathcal{O}_n(\mathbb{R})$, είναι και πάλι ορθογώνιος πίνακας, αφού $(A \cdot B)^t = B^t \cdot A^t = B^{-1} \cdot A^{-1} = (A \cdot B)^{-1}$ και έτσι το $(\mathcal{O}_n(\mathbb{R}), \cdot)$ είναι μια αλγεβρική δομή. Ο μοναδιαίος πίνακας I_n ικανοποιεί το αίτημα (β′) τού Ορισμού 1.2.1.

Τέλος, όταν $A \in \mathcal{O}_n(\mathbb{R})$, τότε $A^t = A^{-1}$ και γι' αυτό ο A^t ικανοποιεί το (γ′) τού Ορισμού 1.2.1 και έτσι το ζεύγος $(\mathcal{O}_n(\mathbb{R}), \cdot)$ είναι μια ομάδα, η οποία για $n \geq 2$, δεν είναι αβελιανή, αφού μπορεί κανείς να βρει εύκολα δύο πίνακες $A, B \in \mathcal{O}_n(\mathbb{R})$ με $A \cdot B \neq B \cdot A$.

Για την τάξη τής ομάδας των ορθογώνιων πινάκων έχουμε $[\mathcal{O}_n(\mathbb{R}) : 1] = \infty$, αφού κάθε πίνακας τής μορφής rI_n, όπου r είναι οποιοσδήποτε μη μηδενικός πραγματικός αριθμός, είναι ορθογώνιος.

Παράδειγμα 1.2.6 (Ομάδες από τη Γεωμετρία).

(α′) **Η ομάδα των ισομετριών τού χώρου $\mathbb{R}^n$**
Αρχίζουμε με κάποιες έννοιες από τη Γραμμική Άλγεβρα.

Στον $\mathbb{R}$–διανυσματικό χώρο $\mathbb{R}^n$ το *εσωτερικό γινόμενο* δύο διανυσμάτων $x = (\xi_1, \xi_2, \ldots, \xi_n)$ και $y = (\eta_1, \eta_2, \ldots, \eta_n)$ ορίζεται ως ο πραγματικός αριθμός:

$$\langle x, y\rangle := \sum_{i=1}^{n} \xi_i \eta_i.$$

Η *απόσταση* μεταξύ δύο διανυσμάτων x και y τού $\mathbb{R}^n$ ορίζεται ως ο μη αρνητικός πραγματικός αριθμός

$$d(x, y) := \sqrt{\langle x - y, x - y\rangle}.$$

Μια απεικόνιση $\sigma : \mathbb{R}^n \to \mathbb{R}^n$ με την ιδιότητα

$$\forall x, y \in \mathbb{R}^n, d(x, y) = d(\sigma(x), \sigma(y)).$$

ονομάζεται *ισομετρία* ή *στερεά κίνηση* τού $\mathbb{R}^n$. Με άλλα λόγια, μια ισομετρία είναι μια απεικόνιση από τον $\mathbb{R}^n$ στον $\mathbb{R}^n$, η οποία διατηρεί τις αποστάσεις.

Ο Euler[2] είναι ο πρώτος που ταξινόμησε τις ισομετρίες τού $\mathbb{R}^n$. Το αντίστοιχο θεώρημα στη σύγχρονη εκδοχή του έχει ως εξής:

Θεώρημα 1.2.7 (Ταξινόμηση Ισομετριών). *Μια απεικόνιση $\sigma : \mathbb{R}^n \to \mathbb{R}^n$ είναι ισομετρία, αν και μόνο αν, υπάρχει ένας $n \times n$ ορθογώνιος πίνακας $A_\sigma \in \mathcal{O}_n(\mathbb{R})$ και ένα διάνυσμα[3] $a_\sigma \in \mathbb{R}^n$, έτσι ώστε*

$$\forall x \in \mathbb{R}^n, \sigma(x) = A_\sigma x + a_\sigma,$$

όπου ο πίνακας A_σ και το διάνυσμα a_σ προσδιορίζονται κατά μοναδικό τρόπο από την ισομετρία σ και αντιστρόφως[4].

Στο εξής το σύνολο των ισομετριών τού $\mathbb{R}^n$ θα συμβολίζεται με $\mathrm{Iso}(\mathbb{R}^n)$.

Θα αποδείξουμε ότι το ζεύγος $(\mathrm{Iso}(\mathbb{R}^n), \circ)$, όπου «$\circ$» είναι η σύνθεση απεικονίσεων, αποτελεί μια ομάδα.

Προφανώς, $\mathrm{Iso}(\mathbb{R}^n) \neq \emptyset$, αφού η ταυτοτική απεικόνιση $\mathrm{Id}_n : \mathbb{R}^n \to \mathbb{R}^n, x \mapsto x$ είναι ισομετρία.

Η σύνθεση δύο ισομετριών είναι επίσης ισομετρία. Πράγματι, όταν οι $\sigma = (A_\sigma, a_\sigma)$ και $\tau = (A_\tau, a_\tau)$ είναι ισομετρίες τού $\mathbb{R}^n$, όπου οι $A_\sigma, A_\tau \in \mathcal{O}_n(\mathbb{R})$ και τα $a_\sigma, a_\tau \in \mathbb{R}^n$, βλ. το παραπάνω Θεώρημα Ταξινόμησης Ισομετριών, τότε για τη σύνθεση $\sigma \circ \tau$ έχουμε:

$$\forall x \in \mathbb{R}^n : \sigma \circ \tau(x) = \sigma(A_\tau x + a_\tau) = A_\sigma(A_\tau x + a_\tau) + a_\sigma = A_\sigma A_\tau x + (A_\sigma a_\tau + a_\sigma).$$

[2]Leonhard Euler (1707–1783), ένας από τους σημαντικότερους μαθηματικούς τής ανθρωπότητας.
[3]Τα διανύσματα τού $\mathbb{R}^n$ θεωρούνται ως στήλες.
[4]με ακρίβεια ομοιότητας

Επομένως, η $\sigma \circ \tau$ είναι ισομετρία, αφού ο πίνακας $A_\sigma A_\tau$ είναι ορθογώνιος και το $A_\sigma a_\tau + a_\sigma$ είναι διάνυσμα τού $\mathbb{R}^n$. Άρα, η σύνθεση

$$\circ : \mathrm{Iso}(\mathbb{R}^n) \times \mathrm{Iso}(\mathbb{R}^n) \to \mathrm{Iso}(\mathbb{R}^n), (\sigma, \tau) \mapsto \sigma \circ \tau$$

αποτελεί μια προσεταιριστική[5] πράξη και το ζεύγος $(\mathrm{Iso}(\mathbb{R}^n), \circ)$ είναι μια αλγεβρική δομή.

Η ταυτοτική απεικόνιση Id_n ικανοποιεί το αίτημα (β′) τού Ορισμού 1.2.1.

Τέλος, όταν

$$\sigma : \mathbb{R}^n \to \mathbb{R}^n, x \mapsto \sigma(x) := A_\sigma x + a_\sigma,$$

είναι ισομετρία, τότε η απεικόνιση

$$\sigma' : \mathbb{R}^n \to \mathbb{R}^n, x \mapsto \sigma'(x) := A_\sigma^{-1} x + (-A_\sigma^{-1} a_\sigma),$$

είναι και αυτή μια ισομετρία, αφού ο $A_\sigma \in \mathcal{O}_n(\mathbb{R})$ και συνεπώς ο $A\sigma^{-1}$ είναι επίσης ορθογώνιος.

Επιπλέον, $\sigma' \circ \sigma = \mathrm{Id}_n$, επειδή

$$\forall x \in \mathbb{R}^n : \ \sigma' \circ \sigma(x) = \sigma'(A_\sigma x + a_\sigma) = A_\sigma^{-1}(A_\sigma x + a_\sigma) + (-A_\sigma^{-1} a_\sigma) = \\ A_\sigma^{-1} A_\sigma x + A_\sigma^{-1} a_\sigma + (-A_\sigma^{-1} a_\sigma) = x.$$

Όμοια αποδεικνύεται ότι $\sigma \circ \sigma' = \mathrm{Id}_n$.

Έτσι ικανοποιείται το αίτημα (γ′) τού Ορισμού 1.2.1 και το ζεύγος $(\mathrm{Iso}(\mathbb{R}^n), \circ)$ είναι μια ομάδα. Παρατηρούμε ότι το σύνολο $\mathcal{O}_n(\mathbb{R})$ περιέχεται στο $\mathrm{Iso}(\mathbb{R}^n)$ και ότι η πράξη τής ομάδας $(\mathcal{O}_n(\mathbb{R}), \cdot)$ «συμπίπτει με τον περιορισμό τής πράξης» τής ομάδας $(\mathrm{Iso}(\mathbb{R}^n), \circ)$ επί τού $\mathcal{O}_n(\mathbb{R})$. Έτσι συμπεραίνουμε αμέσως ότι η $(\mathrm{Iso}(\mathbb{R}^n), \circ)$ δεν είναι αβελιανή. Για τον ίδιο λόγο συμπεραίνουμε επίσης αμέσως ότι $[(\mathrm{Iso}(\mathbb{R}^n)) : 1] = \infty$.

(β′) **Η περιγραφή των στοιχείων τής ομάδας $(\mathrm{Iso}(\mathbb{R}^2), \circ)$ των ισομετριών τού επιπέδου $\mathbb{R}^2$.**

Από το Θεώρημα Ταξινόμησης Ισομετριών τού $\mathbb{R}^n$, βλ. σελ. 15, κάθε ισομετρία τού επιπέδου $\mathbb{R}^2$ είναι τής μορφής

$$\sigma : \mathbb{R}^2 \to \mathbb{R}^2, \quad x \mapsto \sigma(x) := A_\sigma x + a_\sigma,$$

όπου ο $A_\sigma \in \mathcal{O}_2(\mathbb{R})$ και το $a_\sigma \in \mathbb{R}^2$.

Το ακόλουθο λήμμα ταξινομεί τα στοιχεία τού $\mathcal{O}_2(\mathbb{R})$:

Πρόταση 1.2.8. *Όταν $A \in \mathcal{O}_2(\mathbb{R})$, τότε*

(i) *η ορίζουσα τού A ισούται ή με 1 ή με -1,*

[5] Γενικώς η σύνθεση «∘» απεικονίσεων είναι προσεταιριστική.

(ii) *όταν* $\det(A) = 1$, *τότε υπάρχει μια γωνία* $\varphi, 0 < \varphi \leq 2\pi$, *τέτοια ώστε*

$$A = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \text{ και}$$

(ii) *όταν* $\det(A) = -1$, *τότε ο* A *διαθέτει τις ιδιοτιμές* 1 *και* -1. *Αν* v_1 *και* v_{-1} *είναι τα αντίστοιχα ιδιοδιανύσματα, τότε ο πίνακας* A *είναι όμοιος με τον πίνακα*

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Με τη βοήθεια τού προηγούμενου λήμματος προκύπτει η περιγραφή όλων των ισομετριών

$$\sigma : \mathbb{R}^2 \to \mathbb{R}^2, x \mapsto A_\sigma x + a_\sigma \text{ τού } \mathbb{R}^2.$$

Περιπτώσεις:

(i) $(A_\sigma, 0), \det A_\sigma = 1$.
Σύμφωνα με το προηγούμενο Λήμμα, ο πίνακας A_σ ισούται με

$$\begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix},$$

για κάποια γωνία $\varphi, 0 < \varphi \leq 2\pi$ και η ισομετρία $(A_\sigma, 0)$ αποτελεί μια *στροφή* τού επιπέδου κατά γωνία φ (κατά τη φορά των δεικτών τού ρολογιού) γύρω από έναν άξονα κάθετο στο επίπεδο $\mathbb{R}^2$. Αν $\varphi \neq 2\pi$, τότε η συγκεκριμένη ισομετρία διατηρεί σταθερό ακριβώς ένα σημείο τού $\mathbb{R}^2$, το οποίο είναι το σημείο τομής τού άξονα με το επίπεδο $\mathbb{R}^2$. Αν $\varphi = 2\pi$, τότε η ισομετρία συμπίπτει με την ταυτοτική απεικόνιση και κάθε σημείο τού $\mathbb{R}^2$ παραμένει σταθερό.

(ii) $(A_\sigma, 0), \det A_\sigma = -1$.
Σύμφωνα με το Λήμμα, βλ. σελ. 16, υπάρχουν δύο κάθετα μεταξύ τους ιδιοδιανύσματα v_1 και v_{-1} τού $\mathbb{R}^2$ με $A_\sigma v_1 = v_1$ και $A_\sigma v_{-1} = -v_{-1}$. Γι' αυτό η ισομετρία $(A_\sigma, 0)$ αποτελεί *κατοπτρισμό* ως προς την ευθεία $\mathbb{R}v_1$. Το διάνυσμα v_{-1} απεικονίζεται μέσω τού κατοπτρισμού στο $-v_{-1}$. Τα σημεία τού $\mathbb{R}^2$, που διατηρούνται σταθερά από τη συγκεκριμένη ισομετρία, είναι ακριβώς τα σημεία που κείνται πάνω στην ευθεία $\mathbb{R}v_1$.

Σημειώστε, ότι ο κατοπτρισμός ως προς την ευθεία $\mathbb{R}v_1$ μπορεί να θεωρηθεί ως *στροφή τού χώρου* $\mathbb{R}^3$ *κατά γωνία* π γύρω από τον άξονα $\mathbb{R}v_1$.

(iii) $(A_\sigma, a_\sigma), a_\sigma \neq 0, \det A_\sigma = 1$.
Λαμβάνοντας υπ' όψιν την περίπτωση (i), διαπιστώνουμε ότι η συγκεκριμένη ισομετρία εκτελεί μία στροφή γύρω από έναν άξονα κάθετο στο επίπεδο και ακολούθως μία παράλληλη μεταφορά τού επιπέδου κατά το διάνυσμα a_σ. Κανένα σημείο τού επιπέδου δεν παραμένει σταθερό.

(iv) $(A_\sigma, a_\sigma), a_\sigma \neq 0, \det A_\sigma = -1$.
Λαμβάνοντας υπ' όψιν την περίπτωση (ii), διαπιστώνουμε ότι η συγκεκριμένη ισομετρία εκτελεί έναν κατοπτρισμό ως προς μία ευθεία τού επιπέδου και ακολούθως μία παράλληλη μεταφορά τού επιπέδου κατά το διάνυσμα a_σ. Κανένα σημείο τού επιπέδου δεν παραμένει σταθερό.

(γ′) **Η ομάδα ισομετριών $(D_n, \circ)$ ενός κανονικού επίπεδου n-γώνου $\Delta_n, n \geq 3$**
Στο επίπεδο θεωρούμε ένα κανονικό n-γωνο Δ_n, όπου $n \geq 3$ και το υποσύνολο

$$D_n = \{\sigma \in \mathrm{Iso}(\mathbb{R}^2) \mid \sigma(\Delta_n) = \Delta_n\}$$

τού συνόλου $\mathrm{Iso}(\mathbb{R}^2)$ των ισομετριών τού $\mathbb{R}^2$.

Παρατηρούμε ότι όταν οι ισομετρίες σ και τ ανήκουν στο D_n, τότε και η σύνθεσή τους $\sigma \circ \tau$ ανήκει στο D_n, αφού $\sigma \circ \tau(\Delta_n) = \sigma(\tau(\Delta_n)) = \sigma(\Delta_n) = \Delta_n$. Γι' αυτό το ζεύγος $(D_n, \circ)$ αποτελεί μια αλγεβρική δομή, όπου η πράξη τής σύνθεσης «$\circ$» είναι προσεταιριστική. Η ταυτοτική απεικόνιση Id_2 ικανοποιεί το (β′) τού Ορισμού 1.2.1. Επιπλέον, όταν $\sigma \in D_n$, τότε η αντίστροφη ισομετρία σ^{-1} ανήκει επίσης στο D_n, αφού από $\sigma(\Delta_n) = \Delta_n$, έπεται $\Delta_n = \mathrm{Id}_2(\Delta_n) = \sigma^{-1}(\sigma(\Delta_n)) = \sigma^{-1}(\Delta_n)$. Τώρα, επειδή $\sigma \circ \sigma^{-1} = \mathrm{Id}_2 = \sigma^{-1} \circ \sigma$ και αφού το σ^{-1} ανήκει στο D_n, διαπιστώνουμε ότι ικανοποιείται και το (γ′) τού Ορισμού 1.2.1 και συνεπώς το ζεύγος $(D_n, \circ)$ είναι μια ομάδα.

Η ομάδα $(D_n, \circ)$ ονομάζεται η *διεδρική ομάδα* ή *ομάδα συμμετρίας* τού κανονικού n-γώνου και συνήθως συμβολίζεται απλώς ως D_n.
Θα αποδείξουμε ότι

Πρόταση 1.2.9. *Η τάξη $[D_n : 1]$ τής διεδρικής ομάδας $(D_n, \circ), n \geq 3$, ισούται με $2n$.*

Πριν από την απόδειξη τής παραπάνω πρότασης, ας κάνουμε ορισμένες προκαταρκτικές παρατηρήσεις:

(i) Θα αποδείξουμε ότι οι κορυφές και οι πλευρές τού $\sigma(\Delta_n)$ συμπίπτουν με τις κορυφές και τις πλευρές τού Δ_n.
Έστω ότι $A_i, 1 \leq i \leq n$, είναι οι κορυφές τού Δ_n, ότι O_n είναι το κέντρο συμμετρίας τού Δ_n και ότι σ είναι οποιοδήποτε στοιχείο τού D_n. Ισχυριζόμαστε ότι $\sigma(O_n) = O_n$. Πράγματι, η περιφέρεια $\mathcal{C}$ που περιγράφεται γύρω από το D_n έχει ως κέντρο το O_n. Η $\mathcal{C}$ συμπίπτει με την περιφέρεια $\mathcal{C}'$ που περιγράφεται γύρω από το $\sigma(\Delta_n)$, αφού $\sigma(\Delta_n) = \Delta_n$. Το κέντρο τής $\mathcal{C}' = \mathcal{C}$ ισούται με το $\sigma(O_n)$, διότι το σ είναι μια ισομετρία. Επειδή το κέντρο τής περιγεγραμμένης περιφέρειας είναι μοναδικό, έπεται ότι $\sigma(O_n) = O_n$. Έστω A_i οποιαδήποτε κορυφή τού Δ_n. Η ακτίνα τής περιγεγραμμένης περιφέρειας $\mathcal{C}$ συμπίπτει με το ευθύγραμμο τμήμα $\overline{O_n, A_i}$. Επειδή το $\sigma \in D_n$ είναι ισομετρία έχουμε:

$$d(O_n, A_i) = d(\sigma(O_n), \sigma(A_i)) = d(O_n, \sigma(A_i)).$$

Παρατηρώντας ότι τα μοναδικά σημεία τού $\sigma(\Delta_n) = \Delta_n$, που απέχουν από το O_n, απόσταση ίση με $d(O_n, A_i)$, είναι οι κορυφές τού Δ_n καταλήγουμε στο συμπέρασμα ότι το $\sigma(A_i)$ είναι και πάλι μια από τις κορυφές τού Δ_n.

Έστω $\overline{A_i, A_{i+1}}$ το σύνολο των σημείων τού ευθύγραμμου τμήματος με άκρα τις διαδοχικές κορυφές A_i και A_{i+1}. Για κάθε $\sigma \in D_n$, η εικόνα $\sigma(\overline{A_i, A_{i+1}}) = \{\sigma(s) \mid s \in \overline{A_i, A_{i+1}}\}$ οφείλει να είναι και πάλι ένα ευθύγραμμο τμήμα, αφού το σ είναι ισομετρία, με άκρα τις διαδοχικές κορυφές $\sigma(A_i)$ και $\sigma(A_{i+1})$. Επομένως, $\sigma(\overline{A_i, A_{i+1}}) = \overline{\sigma(A_i), \sigma(A_{i+1})}$.

(ii) Επιχειρηματολογώντας με τον ίδιο τρόπο, αποδεικνύουμε ότι για κάθε κορυφή A_i και για κάθε $\sigma \in D_n$ είναι: $\sigma(\overline{O_n, A_i}) = \overline{\sigma(O_n), \sigma(A_i)} = \overline{O_n, \sigma(A_i)}$, αφού $O_n = \sigma(O_n)$.

(iii) Από την ταξινόμηση των στοιχείων τής ομάδας $(\mathrm{Iso}(\mathbb{R}^2), \circ)$, βλ. σελ. 17, και επειδή το κέντρο συμμετρίας O_n τού Δ_n παραμένει σταθερό από οποιοδήποτε στοιχείο $\sigma \in D_n$, διαπιστώνουμε ότι οι ισομετρίες τού $\mathbb{R}^2$ που ανήκουν στην D_n θα είναι τής μορφής $(A_\sigma, 0)$, όπου ο A_σ είναι ένας ορθογώνιος πίνακας με $\det A_\sigma = \pm 1$ και ως εκ τούτου, θα είναι γραμμικές απεικονίσεις. Γι' αυτό, θεωρώντας ένα σύστημα συντεταγμένων τού $\mathbb{R}^2$ με απαρχή το O_n και τα διανύσματα $\overrightarrow{O_n A_i}$ και $\overrightarrow{O_n A_{i+1}}$, που ορίζονται από δύο **διαδοχικές** κορυφές A_i και A_{i+1}, διαπιστώνουμε ότι οποιαδήποτε ισομετρία $\sigma \in D_n$ προσδιορίζεται πλήρως από τις εικόνες $\sigma(A_i)$ και $\sigma(A_{i+1})$, αφού τα $\overrightarrow{O_n A_i}$ και $\overrightarrow{O_n A_{i+1}}$ απαρτίζουν μια βάση τού $\mathbb{R}^2$, ως δύο μη συγγραμμικά, άρα και γραμμικώς ανεξάρτητα, διανύσματα.

Τώρα είμαστε έτοιμοι για την απόδειξη τής πρότασης.

Απόδειξη. Ισχυριζόμαστε ότι $[D_n : 1] \leq 2n$. Πράγματι, όπως προείπαμε, οποιοδήποτε στοιχείο σ τής D_n προσδιορίζεται πλήρως από τις εικόνες $\sigma(A_i)$, $\sigma(A_{i+1})$ δύο διαδοχικών κορυφών A_i, A_{i+1}. Οι κορυφές $\sigma(A_i)$, $\sigma(A_{i+1})$ οφείλουν και πάλι να είναι διαδοχικές. Αν είναι λοιπόν $\sigma(A_i) = A_j$, τότε για την εικόνα $\sigma(A_{i+1})$ έχουμε δύο πιθανές τιμές, οι οποίες αντιστοιχούν ακριβώς στις δύο κορυφές τού Δ_n που κείνται εκατέρωθεν τής $\sigma(A_i) = A_j$. Επομένως, το πλήθος των ισομετριών $\sigma \in \mathrm{Iso}(\mathbb{R}^2)$ με $\sigma \in D_n$ είναι $\leq 2n$.

Ισχυριζόμαστε ότι $[D_n : 1] \geq 2n$. Πράγματι, παρατηρούμε ότι υπάρχουν n το πλήθος στροφές τού $\mathbb{R}^2$, που απεικονίζουν ένα κανονικό n-γωνο Δ_n στον εαυτό του. Πρόκειται για τις στροφές κατά γωνία $\varphi = 2k\pi/n, k = 1, 2, \ldots, n$ (κατά τη φορά των δεικτών τού ρολογιού) γύρω από άξονα κάθετο στο επίπεδο τού Δ_n, ο οποίος διέρχεται από το κέντρο συμμετρίας O_n τού Δ_n. Τέλος, υπάρχουν n το πλήθος κατοπτρισμοί τού επιπέδου, οι οποίοι απεικονίζουν το Δ_n στον εαυτό του. Αυτοί προκύπτουν από τους n το πλήθος άξονες συμμετρίας που διαθέτει πάντοτε ένα κανονικό n-γωνο Δ_n. Υπενθυμίζουμε ότι όταν ο n είναι περιττός, τότε οι n το πλήθος άξονες συμμετρίας διέρχονται από μια κορυφή τού Δ_n και το μέσον τής απέναντι πλευράς του, και όταν ο n είναι άρτιος, τότε από τους άξονες αυτούς $n/2$ το πλήθος διέρχονται από απέναντι κορυφές και $n/2$ το πλήθος διέρχονται από τα μέσα απέναντι πλευρών.

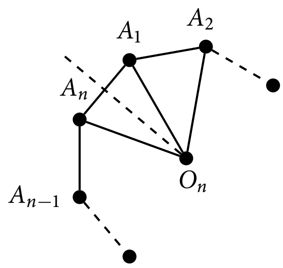
Έτσι τελικά προκύπτει ότι $[D_n : 1] = 2n$. □

Πρόταση 1.2.10. *Για κάθε $n \geq 3$, η ομάδα $(D_n, \circ)$ δεν είναι αβελιανή.*

Απόδειξη. Θα αποδείξουμε κάτι ισχυρότερο. Έστω ότι ρ είναι η στροφή κατά γωνία $2\pi/n$ γύρω από τον άξονα, ο οποίος είναι κάθετος στο επίπεδο τού κανονικού n-γώνου Δ_n με φορά αυτήν που ακολουθούν κατά την κίνησή τους οι δείκτες τού ρολογιού και ότι τ είναι ένας οποιοσδήποτε κατοπτρισμός τού Δ_n, που ορίζεται από τον άξονα συμμετρίας που διέρχεται από μια οποιαδήποτε κορυφή ή από το μέσα δύο απέναντι πλευρών. Σημειώστε ότι η δεύτερη περίπτωση εμφανίζεται μόνο όταν το Δ_n έχει άρτιο πλήθος πλευρών.

Ισχυριζόμαστε ότι
$$\tau \circ \rho = \rho^{-1} \circ \tau.$$

Πρώτη Περίπτωση Ο άξονας κατοπτρισμού τού τ διέρχεται από μια κορυφή.
Χωρίς περιορισμό τής γενικότητας (π.χ. με μια εκ νέου αρίθμηση) μπορούμε να δεχθούμε ότι η κορυφή αυτή είναι η A_1, βλ. το επόμενο σχήμα.



Θεωρούμε τη βάση τού $\mathbb{R}^2$ που αποτελείται από τα διανύσματα $\overrightarrow{O_nA_1}$ και $\overrightarrow{O_nA_n}$. Είναι $\tau(\overrightarrow{O_nA_1}) = \overrightarrow{O_nA_1}$, $\tau(\overrightarrow{O_nA_n}) = \overrightarrow{O_nA_2}$, $\rho(\overrightarrow{O_nA_1}) = \overrightarrow{O_nA_2}$ και $\rho(\overrightarrow{O_nA_n}) = \overrightarrow{O_nA_1}$. Επομένως, $\tau \circ \rho(\overrightarrow{O_nA_1}) = \overrightarrow{O_nA_n}$, $\tau \circ \rho(\overrightarrow{O_nA_n}) = \overrightarrow{O_nA_1}$, $\rho^{-1} \circ \tau(\overrightarrow{O_nA_1}) = \overrightarrow{O_nA_n}$ και $\rho^{-1} \circ \tau(\overrightarrow{O_nA_n}) = \overrightarrow{O_nA_1}$. Άρα, $\tau \circ \rho = \rho^{-1} \circ \tau$ (*), αφού οι ισομετρίες παίρνουν τις ίδιες τιμές στη βάση $\{\overrightarrow{O_nA_1}, \overrightarrow{O_nA_n}\}$, βλ. τη σχετική παρατήρηση (iii), σελ. 19.

Δεύτερη Περίπτωση (μόνο όταν ο n είναι άρτιος) Ο άξονας κατοπτρισμού τού τ διέρχεται από τα μέσα δύο απέναντι πλευρών.
Χωρίς περιορισμό τής γενικότητας (π.χ. με μια εκ νέου αρίθμηση) μπορούμε να δεχθούμε ότι άξονας κατοπτρισμού διέρχεται από το μέσο τής πλευράς $\overline{A_n, A_1}$, βλ. στο παραπάνω σχήμα. Υπολογίζοντας τις τιμές των συνθέσεων $\tau \circ \rho$ και $\rho^{-1} \circ \tau$ στα διανύσματα τής βάσης $\{\overrightarrow{O_nA_1}, \overrightarrow{O_nA_n}\}$. Έχουμε $\tau \circ \rho(\overrightarrow{O_nA_1}) = \tau(\overrightarrow{O_nA_2}) = \overrightarrow{O_nA_{n-1}}$, $\tau \circ \rho(\overrightarrow{O_nA_n}) = \tau(\overrightarrow{O_nA_1}) = \overrightarrow{O_nA_n}$, $\rho^{-1} \circ \tau(\overrightarrow{O_nA_1}) = \rho^{-1}(\overrightarrow{O_nA_n}) = \overrightarrow{O_nA_{n-1}}$ και $\rho^{-1} \circ \tau(\overrightarrow{O_nA_n}) = \rho^{-1}(\overrightarrow{O_nA_1}) = \overrightarrow{O_nA_n}$. Επομένως, $\rho \circ \tau = \tau \circ \rho^{-1}$ (**).

Αν ήταν η ομάδα D_n αβελιανή, τότε θα είχαμε, $\tau \circ \rho = \rho \circ \tau$ και έτσι, λόγω των (*)

και (**), θα ήταν $\rho \circ \tau = \rho^{-1} \circ \tau$. Τότε όμως θα ήταν

$$\begin{aligned} &\rho \circ \tau = \rho^{-1} \circ \tau \Leftrightarrow \rho \circ \tau \circ \tau^{-1} = \rho^{-1} \circ \tau \circ \tau^{-1} \Leftrightarrow \\ &\rho \circ \mathrm{Id}_n = \rho^{-1} \circ \mathrm{Id}_n \Leftrightarrow \rho \circ \rho = \mathrm{Id}_n, \end{aligned}$$

από όπου προκύπτει ότι η ρ είναι στροφή κατά γωνία π. Αυτό αντιφάσκει στο ότι η ρ είναι στροφή κατά γωνία $2\pi/n$ με $n \geq 3$. Άρα, η D_n δεν είναι αβελιανή ομάδα. □

Παρατήρηση 1.2.11. Ας συγκρατήσουμε τον τύπο $\tau \circ \rho = \rho^{-1} \circ \tau$, για τη στροφή ρ κατά γωνία $2\pi/n$ και οποιοδήποτε κατοπτρισμό τ, που όπως θα δούμε αργότερα είναι πολύ σημαντικός για την περιγραφή των στοιχείων τής D_n.

Στα επόμενα δύο λήμματα συγκεντρώνουμε ορισμένες απλές ιδιότητες που απορρέουν από τον ορισμό τής έννοιας τής ομάδας.

Λήμμα 1.2.12. *Έστω $(G, \star)$ μια ομάδα.*

(α′) *Το στοιχείο $e \in G$ με την ιδιότητα: $\forall g \in G, e \star g = g = g \star e$ είναι μοναδικό,* βλ. Ορισμό 1.2.1(β′).

(β′) *Για κάθε $g \in G$, το αντίστοιχο στοιχείο h με την ιδιότητα: $g \star h = e = h \star g$ είναι μοναδικό,* βλ. Ορισμό 1.2.1(γ′).

Απόδειξη. (α′) Έστω ότι υπάρχουν στοιχεία $e, e' \in G$, που και τα δύο ικανοποιούν το αίτημα (β′) τού Ορισμού 1.2.1. Τότε έχουμε

$$e \star e' = e',$$

αφού το e ικανοποιεί την πρώτη ισότητα τής ιδιότητας (β′) τού Ορισμού 1.2.1 και

$$e \star e' = e,$$

αφού το e' ικανοποιεί τη δεύτερη ισότητα τής ιδιότητας (β′) τού Ορισμού 1.2.1. Επομένως, $e = e'$.

(β′) Έστω ότι $g \in G$ και ότι υπάρχουν στοιχεία $h, h' \in G$, που και τα δύο ικανοποιούν το αίτημα (γ′) τού Ορισμού 1.2.1, δηλαδή ικανοποιούν τις

$$g \star h = e = h \star g \text{ και } g \star h' = e = h' \star g.$$

Από την ισότητα $e = h \star g$ και επειδή η πράξη «$\star$» είναι προσεταιριστική παίρνουμε:

$$e \star h' = (h \star g) \star h' = h \star (g \star h') = h \star e = h, \text{ λόγω τής ιδιότητας τού } e.$$

Αλλά $e \star h' = h'$ και πάλι λόγω τής ιδιότητας τού e. Επομένως, $h = h'$. □

Ορισμός 1.2.13. Το μοναδικό στοιχείο τής ομάδας $(G, \star)$ που ικανοποιεί την ιδιότητα (β′) τού Ορισμού 1.2.1 ονομάζεται *το ταυτοτικό* ή το *ουδέτερο στοιχείο* τής ομάδας και συμβολίζεται με e_G ή απλώς με e.

Παρατήρηση 1.2.14. Στην περίπτωση τής πολλαπλασιαστικής σημειογραφίας, ορισμένες φορές το ουδέτερο τής ομάδας συμβολίζεται με 1_G ή απλώς με 1 και στην περίπτωση τής προσθετικής σημειογραφίας, που τη χρησιμοποιούμε μόνο όταν η ομάδα είναι αβελιανή (μεταθετική), το ουδέτερο τής ομάδας συμβολίζεται με 0_G ή απλώς με 0.

Ορισμός 1.2.15. Για κάθε $g \in G$, το μοναδικό, ως προς g, στοιχείο τής ομάδας $(G, \star)$ που ικανοποιεί την ιδιότητα (γ′) τού Ορισμού 1.2.1 ονομάζεται το *αντίστροφο* τού στοιχείου g και συμβολίζεται με g^{-1}.

Παρατήρηση 1.2.16. Στην περίπτωση τής προσθετικής σημειογραφίας, που τη χρησιμοποιούμε μόνο όταν η ομάδα είναι αβελιανή (μεταθετική), το αντίστροφο ενός στοιχείου $g \in G$ συμβολίζεται με $-g$ και ονομάζεται *το αντίθετο* τού g.

Η ύπαρξη και μοναδικότητα τού αντίστροφου οποιουδήποτε στοιχείου μιας ομάδας $(G, \star)$ επιτρέπει τα εξής άμεσα συμπεράσματα:

Λήμμα 1.2.17. *Έστω $(G, \star)$ μια ομάδα.*

(α′) *Για κάθε $a, b \in G$ είναι: $(a \star b)^{-1} = b^{-1} \star a^{-1}$.*

(β′) *Για κάθε $a \in G$ είναι: $(a^{-1})^{-1} = a$.*

Απόδειξη. (α′) Το αντίστροφο $(a \star b)^{-1}$ τού $a \star b$ είναι μοναδικό. Επομένως, αν βρούμε κάποιο $g \in G$ με $g \star (a \star b) = e = (a \star b) \star g$, τότε αμέσως θα έχουμε ότι $g = (a \star b)^{-1}$. Για το στοιχείο $(b^{-1} \star a^{-1})$ ισχύει:

$$(b^{-1} \star a^{-1}) \star (a \star b) = b^{-1} \star (a^{-1} \star a) \star b = b^{-1} \star e \star b = b^{-1} \star b = e.$$

Όμοια αποδεικνύεται ότι $(a \star b) \star (b^{-1} \star a^{-1}) = e$. Συνεπώς, $(a \star b)^{-1} = b^{-1} \star a^{-1}$.
(β′) Η σκέψη είναι πανομοιότυπη. Αν βρούμε κάποιο $g \in G$ με $g \star a^{-1} = e = a^{-1} \star g$, τότε βέβαια θα έχουμε ότι $g = (a^{-1})^{-1}$. Γι' αυτό από τις σχέσεις $a \star a^{-1} = e = a^{-1} \star a$, προκύπτει αμέσως ότι $a = (a^{-1})^{-1}$. □

Λήμμα 1.2.18. *Έστω $(G, \star)$ μια ομάδα.*

(α′) *Για κάθε $a, b \in G$, η εξίσωση $a \star x = b$ διαθέτει ακριβώς μία λύση ως προς x.*

(β′) *Για κάθε $a, b \in G$, η εξίσωση $y \star a = b$ διαθέτει ακριβώς μία λύση ως προς y.*

Απόδειξη. (α′) Το στοιχείο $a^{-1} \star b$ αποτελεί λύση τής $a \star x = b$, αφού

$$a \star (a^{-1} \star b) = (a \star a^{-1}) \star b = e * b = b.$$

Επιπλέον, αν g_1 και g_2 αποτελούν λύσεις τής $a \star x = b$, τότε από $a \star g_1 = b$ και $a \star g_2 = b$ έπεται $a \star g_1 = a \star g_2$ και συνεπώς

$$g_1 = e \star g_1 = (a^{-1} \star a) \star g_1 = a^{-1} \star (a \star g_1) = a^{-1} \star (a \star g_2) = (a^{-1} \star a) \star g_2 = e \star g_2 = g_2.$$

(β′) Η απόδειξη είναι παρόμοια και προτείνεται ως άσκηση. □

$\star$	g_1	g_2	$\dots$	g_i	$\dots$	g_j	$\dots$	$\dots$	g_n
g_1	$g_1 \star g_1$	$g_1 \star g_2$	$\dots$	$g_1 \star g_i$	$\dots$	$g_1 \star g_j$	$\dots$	$\dots$	$g_1 \star g_n$
g_2	$g_2 \star g_1$	$g_2 \star g_2$	$\dots$	$g_2 \star g_i$	$\dots$	$g_2 \star g_j$	$\dots$	$\dots$	$g_2 \star g_n$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
g_i	$g_i \star g_1$	$g_i \star g_2$	$\dots$	$g_i \star g_i$	$\dots$	$g_i \star g_j$	$\dots$	$\dots$	$g_i \star g_n$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
g_j	$g_j \star g_1$	$g_j \star g_2$	$\dots$	$g_j \star g_i$	$\dots$	$g_j \star g_j$	$\dots$	$\dots$	$g_j \star g_n$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
g_n	$g_n \star g_1$	$g_n \star g_2$	$\dots$	$g_n \star g_i$	$\dots$	$g_n \star g_j$	$\dots$	$\dots$	$g_n \star g_n$

Σχήμα 1.3: Ο πίνακας τής πράξης «$\star$», όπου $G = \{g_1, g_2, \dots, g_n\}$.

Με τη βοήθεια τού ανωτέρω λήμματος αποδεικνύεται η εξής σημαντική πρόταση:

Πρόταση 1.2.19. *Έστω $(G, \star)$ μια αλγεβρική δομή, όπου το σύνολο G είναι ένα πεπερασμένο σύνολο και η πράξη «$\star$» είναι προσεταιριστική.*

Το ζεύγος $(G, \star)$ αποτελεί ομάδα, αν και μόνο αν, κάθε στοιχείο τού συνόλου G εμφανίζεται σε κάθε γραμμή και αντίστοιχα σε κάθε στήλη τού πίνακα τής πράξης «$\star$», βλ. Σχήμα 1.3, *ακριβώς μία φορά.*

Απόδειξη. Επειδή το G είναι ένα πεπερασμένο σύνολο μπορούμε να πούμε ότι
$G = \{g_1, g_2, \dots, g_n\}, n \in \mathbb{N}$.
«$\Rightarrow$» Έστω ότι το ζεύγος $(G, \star)$ αποτελεί ομάδα. Η i–οστή γραμμή τού πίνακα τής πράξης «$\star$», αποτελείται από τα γινόμενα $g_i \star g_\lambda$, όπου $\lambda = 1, 2, \dots, n$. Κάθε στοιχείο g τής G εμφανίζεται στην i–οστή γραμμή τουλάχιστον μία φορά, αφού, σύμφωνα με το Λήμμα 1.2.18, η εξίσωση $g_i \star x = g$ έχει πάντοτε λύση ως προς x και επειδή η λύση αυτή είναι μοναδική, δεν μπορεί να υπάρχουν δύο διαφορετικά στοιχεία g_i και g_j τής G με $g_i \star g_j = g = g_i \star g_k$. Άρα, κάθε στοιχείο τής G εμφανίζεται στην i–οστή γραμμή ακριβώς μία φορά.

Η απόδειξη για τις στήλες είναι ανάλογη και προτείνεται ως άσκηση.

«$\Leftarrow$» Ας υποθέσουμε τώρα ότι σε κάθε γραμμή και κάθε στήλη τού πίνακα τής πράξης «$\star$» εμφανίζεται κάθε στοιχείο τής G ακριβώς μία φορά. Θα δείξουμε ότι το ζεύγος $(G, \star)$ αποτελεί ομάδα. Θεωρούμε την i–οστή στήλη. Σε αυτήν, σύμφωνα με την υπόθεση, εμφανίζεται το στοιχείο g_i ακριβώς μία φορά. Δηλαδή, υπάρχει g_k με $g_k \star g_i = g_i$.
Για το συγκεκριμένο $g_k \in G$, θα αποδείξουμε ότι

$$\forall g_j, \ \ 1 \leq j \leq n, \quad g_k \star g_j = g_j. \tag{*}$$

Πράγματι, για κάθε $g_j, 1 \leq j \leq n$ υπάρχει στην i–οστή γραμμή, λόγω τής υπόθεσης, κάποιος δείκτης $\ell, 1 \leq \ell \leq n$ με $g_j = g_i \star g_\ell$. Επομένως,

$$g_k \star g_j = g_k \star (g_i \star g_\ell) = (g_k \star g_i) \star g_\ell = g_i \star g_\ell = g_j.$$

Εργαζόμενοι τώρα με τις στήλες αποδεικνύεται με ανάλογο τρόπο ότι υπάρχει κάποιο συγκεκριμένο $g_m \in G$ με

$$\forall g_j,\ \ 1 \leq j \leq n,\quad g_j \star g_m = g_m. \tag{**}$$

Για τα συγκεκριμένα στοιχεία g_k και g_m έχουμε, $g_k \star g_m = g_m$, λόγω τής ιδιότητας (*) τού g_k και $g_k \star g_m = g_k$ λόγω τής ιδιότητας (**) τού g_m. Άρα, $g_k = g_m$. Ας γράψουμε $e = g_k = g_m$. Για κάθε $g \in G$, λόγω τής (*) έχουμε $e \star g = g$ και λόγω τής (**) έχουμε $g \star e = g$. Συνεπώς, ικανοποιείται το αίτημα (β′) τού Ορισμού 1.2.1, δηλαδή το e είναι το ουδέτερο στοιχείο τής υποψήφιας ομάδας.

Θα αποδείξουμε τώρα ότι κάθε $g_i \in G$ διαθέτει αντίστροφο. Παρατηρούμε ότι στην i–οστή γραμμή υπάρχει κάποιο g_j με $g_i \star g_j = e$ και στην i–οστή στήλη υπάρχει κάποιο g_ℓ με $g_\ell \star g_i = e$. Θα δείξουμε ότι $g_j = g_\ell$.

Πράγματι,

$$g_j = e \star g_j = (g_\ell \star g_i) \star g_j = g_\ell \star (g_i \star g_j) = g_\ell \star e = g_\ell.$$

Επομένως,

$$g_i \star g_j = e = g_j \star g_i.$$

Συνεπώς, ικανοποιείται το αίτημα (γ′) τού Ορισμού 1.2.1 και το ζεύγος $(G, \star)$ αποτελεί ομάδα. □

Παράδειγμα 1.2.20. Έστω το σύνολο $G = \{e, a, b, c\}$ και $\star_1 : G \times G \to G, \star_2 : G \times G \to G$ δύο πράξεις επί τού G, που ορίζονται από τους δύο πίνακες τού Σχήματος 1.4.

$\star_1$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

,

$\star_2$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

Σχήμα 1.4: Οι πίνακες πράξης δύο ομάδων με τέσσερα στοιχεία.

Κάθε ένα από τα ζεύγη $(G, \star_1)$ και $(G, \star_2)$ απαρτίζουν μια ομάδα.

Πράγματι, σύμφωνα με το Λήμμα 1.2.19 αρκεί να ελέγξουμε ότι καθεμία από τις «$\star_1$» και «$\star_2$» είναι προσεταιριστική πράξη, αφού σε κάθε γραμμή και κάθε στήλη των πινάκων, κάθε στοιχείο τού G εμφανίζεται ακριβώς μία φορά.

Για να είναι η «$\star_1$» προσεταιριστική πράξη πρέπει, για κάθε $x_1, x_2, x_3 \in G$ να ισχύει $x_1 \star_1 (x_2 \star_2 x_3) = (x_1 \star_1 x_2) \star_1 x_3$. Αλλά όταν ένα από τα στοιχεία τής προηγούμενης σχέσης είναι το e, τότε η αλήθεια τής σχέσης είναι άμεση, αφού $\forall x \in G, e \star_1 x = x = x \star_1 e$. Επομένως, χωρίς περιορισμό τής γενικότητας, αρκεί να ελέγξουμε την προσεταιριστικότητα, όταν και τα τρία στοιχεία x_1, x_2, x_3 είναι $\neq e$ εξαιρώντας την προφανή περίπτωση $x_1 = x_2 = x_3$. Στις επόμενες γραμμές εξετάζουμε όλες τις σχέσεις με $x_1 = a$ και προτείνουμε ως άσκηση, την εξέταση των περιπτώσεων $x_1 = b$ και $x_1 = c$. Έχουμε:

$$
\begin{aligned}
a \star_1 (a \star_1 b) &= a \star_1 c = b = e \star_1 b = (a \star_1 a) \star_1 b,\\
a \star_1 (a \star_1 c) &= a \star_1 b = c = e \star_1 c = (a \star_1 a) \star_1 c,\\
a \star_1 (b \star_1 a) &= a \star_1 c = b = c \star_1 a = (a \star_1 b) \star_1 a,\\
a \star_1 (b \star_1 b) &= a \star_1 e = a = c \star_1 b = (a \star_1 b) \star_1 b,\\
a \star_1 (b \star_1 c) &= a \star_1 a = e = c \star_1 c = (a \star_1 b) \star_1 c,\\
a \star_1 (c \star_1 a) &= a \star_1 b = c = b \star_1 a = (a \star_1 c) \star_1 a,\\
a \star_1 (c \star_1 b) &= a \star_1 a = e = b \star_1 b = (a \star_1 c) \star_1 b,\\
a \star_1 (c \star_1 c) &= a \star_1 e = a = b \star_1 c = (a \star_1 c) \star_1 c.
\end{aligned}
$$

Συνεπώς, το ζεύγος $(G, \star_1)$ απαρτίζει μια ομάδα. Η συγκεκριμένη ομάδα είναι αβελιανή (μεταθετική), αφού ο πίνακας πράξης για την «$\star_1$» είναι συμμετρικός ως προς την κύρια διαγώνιό του. Επιπλέον, το ουδέτερο στοιχείο είναι το e και για κάθε $x \in G$, είναι $x \star_1 x = e$. Η $(G, \star_1)$ ονομάζεται η *ομάδα των τεσσάρων στοιχείων* ή *ομάδα Klein*.

Με ανάλογο τρόπο αποδεικνύεται ότι και το ζεύγος $(G, \star_2)$ συνιστά μια ομάδα. Πρόκειται και πάλι για μια αβελιανή (μεταθετική) ομάδα με ουδέτερο στοιχείο το e. Εδώ όμως, υπάρχουν $x \in G$ με $x \star_2 x \neq e$. Για παράδειγμα, $a \star_2 a = b$. Συνεπώς, οι δύο αυτές ομάδες δεν διαθέτουν τις ίδιες αλγεβρικές ιδιότητες. Όπως θα δούμε αργότερα, τέτοιου είδους ομάδες ονομάζονται «μη ισόμορφες».

Παράδειγμα 1.2.21. Η αβελιανή ομάδα $(\mathbb{U}_n, \cdot)$ των αντιστρέψιμων κλάσεων ισοτιμίας των ακεραίων κατά μόδιο n $\in\mathbb{N}$ με πράξη τον πολλαπλασιασμό των κλάσεων κατά μόδιο n

Στο Παράδειγμα 1.2.4(γ′) διαπιστώθηκε ότι το ζεύγος $(\mathbb{Z}_n, +)$ αποτελεί μια αβελιανή ομάδα. Στο σύνολο $\mathbb{Z}_n = \mathbb{Z}/\sim_n$ των κλάσεων ισοτιμίας των ακεραίων $\mathbb{Z}$ κατά μόδιο n ορίζεται ακόμη μια πράξη, η οποία προέρχεται από τον συνήθη πολλαπλασιασμό των ακέραιων αριθμών.

Από τη Θεωρία Αριθμών γνωρίζουμε ότι όταν $a \equiv a' \bmod n$ και $b \equiv b' \bmod n$, τότε $(a \cdot b) \equiv (a' \cdot b') \bmod n$. Με άλλα λόγια, όταν $[a]_n = [a']_n$ και $[b]_n = [b']_n$, τότε $[a \cdot b]_n = [a' \cdot b']_n$. Γι' αυτό η αντιστοιχία

$$\cdot_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n, ([a]_n, [b]_n) \mapsto [a \cdot b]_n$$

αποτελεί μια καλά ορισμένη απεικόνιση. Συνεπώς, η «$\cdot_n$» αποτελεί μια πράξη επί τού $\mathbb{Z}_n$, η οποία μάλιστα είναι προσεταιριστική και μεταθετική, αφού η πρόσθεση των ακεραίων έχει αυτές τις δύο ιδιότητες. Έτσι το ζεύγος $(\mathbb{Z}_n, \cdot_n)$ απαρτίζει μια αλγεβρική δομή. Από εδώ και στο εξής θα ονομάζουμε την πράξη «$\cdot_n$» *πολλαπλασιασμό των κλάσεων κατά μόδιο n*.

Ωστόσο, δεν υπάρχει φυσικός αριθμός n ≥ 2 τέτοιος, ώστε το ζεύγος $(\mathbb{Z}_n, \cdot_n)$ να αποτελεί ομάδα. Πράγματι, αν ήταν το $(\mathbb{Z}_n, \cdot_n)$ ομάδα τότε, σύμφωνα με το Λήμμα 1.2.18, η

εξίσωση $[a] \cdot_n x = [b]$ θα είχε ακριβώς μία λύση ως προς x, για οποιεσδήποτε δύο κλάσεις $[a], [b] \in \mathbb{Z}_n$. Στην περίπτωση όμως τής εξίσωσης $[0] \cdot_n x = [0]$ το πλήθος των λύσεων είναι ακριβώς n, επειδή για κάθε κλάση $[z]$ είναι $[0] \cdot_n [z] = [0 \cdot z] = [0]$. Αφού λοιπόν υποθέσαμε ότι $n \geq 2$, το $(\mathbb{Z}_n, \cdot_n)$ δεν είναι ομάδα.
Εντούτοις, υπάρχουν πάντοτε υποσύνολα τού $\mathbb{Z}_n$, τα οποία είναι ομάδες ως προς την πράξη «$\cdot_n$».

Έστω $\mathbb{U}_n$ το ακόλουθο υποσύνολο των κλάσεων ισοτιμίας τού $\mathbb{Z}$ κατά μόδιο n:

$$\mathbb{U}_n = \{[m] \in \mathbb{Z}_n \mid 1 \leq m \leq n, \text{ όπου ο ΜΚΔ}(n, m) = 1\}.$$

Συμβολίζουμε με ΜΚΔ(n, m) τον μέγιστο κοινό διαιρέτη των n και m.
Παρατηρούμε ότι αν ο ΜΚΔ$(n, m) = 1$, τότε για κάθε ακέραιο z που ανήκει στην κλάση $[m]$, ο ΜΚΔ$(n, |z|)$ ισούται επίσης με 1 ($|z|$ συμβολίζει την απόλυτη τιμή τού ακεραίου z). Πράγματι, επειδή $z \in [m]$, έχουμε $z - m = n \cdot \kappa$, $\kappa \in \mathbb{Z}$ (*). Αν ήταν ο ΜΚΔ$(n, |z|) = \delta \neq 1$, τότε θα υπήρχε ένας πρώτος διαιρέτης p τού δ με $z = \alpha \cdot p$, $\alpha \in \mathbb{Z}$ και $m = \beta \cdot p$, $\beta \in \mathbb{Z}$. Τότε όμως θα ήταν ο p, λόγω τής (*), επίσης διαιρέτης τού m. Πράγμα άτοπο.

Θα δείξουμε ότι το ζεύγος $(\mathbb{U}_n, \cdot_n)$, όπου «$\cdot_n$» είναι ο πολλαπλασιασμός των κλάσεων κατά μόδιο n, αποτελεί μια αβελιανή (μεταθετική) ομάδα.

Το $\mathbb{U}_n \neq \emptyset$, αφού το $[1]$ είναι πάντοτε στοιχείο τού $\mathbb{U}_n$.

Ήδη γνωρίζουμε ότι ο «$\cdot_n$» αποτελεί μια προσεταιριστική και μεταθετική πράξη επί τού συνόλου $\mathbb{Z}_n$. Θα δείξουμε ότι ο πολλαπλασιασμός των κλάσεων κατά μόδιο n περιορισμένος στο $\mathbb{U}_n$ ορίζει μια πράξη επί τού $\mathbb{U}_n$, δηλαδή ότι το $\mathbb{U}_n$ είναι κλειστό ως προς τον «$\cdot_n$».

Πράγματι, αν $[z], [w]$ είναι στοιχεία τού $\mathbb{U}_n$, τότε το $[z] \cdot_n [w] = [z \cdot w]$ είναι επίσης στοιχείο τού $\mathbb{U}_n$, αφού στην αντίθετη περίπτωση θα ήταν ο ΜΚΔ$(n, z \cdot w) = \delta \neq 1$ και ως εκ τούτου, θα υπήρχε τότε ένας πρώτος p με p/n και $p/(z \cdot w)$ και έτσι ο p, αφού είναι πρώτος αριθμός, θα διαιρούσε τουλάχιστον έναν από τους z, w. Πράγμα άτοπο, αφού τα $[z]$ και $[w]$ είναι στοιχεία τού $\mathbb{U}_n$. Επομένως, ο πολλαπλασιασμός κατά μόδιο n ορίζει την πράξη

$$\cdot_n : \mathbb{U}_n \times \mathbb{U}_n \to \mathbb{U}_n, ([z], [w]) \mapsto [z] \cdot_n [w] := [z \cdot w],$$

η οποία είναι προσεταιριστική και μεταθετική.

Προφανώς, η κλάση $[1]$ είναι το ουδέτερο στοιχείο τής $\mathbb{U}_n$ ως προς την πράξη «$\cdot_n$».

Υπολείπεται η απόδειξη ότι κάθε $[m] \in \mathbb{U}_n$, διαθέτει αντίστροφο ως προς την «$\cdot_n$».

Αν $[m] \in \mathbb{U}_n$, τότε υπάρχουν $\alpha, \beta \in \mathbb{Z}$ με $1 = \alpha \cdot n + \beta \cdot m$ (**), διότι ο ΜΚΔ$(n, m) = 1$. Παρατηρούμε ότι και ο ΜΚΔ$(n, |\beta|) = 1$, αφού διαφορετικά ένας κοινός πρώτος διαιρέτης των n και $|\beta|$ θα διαιρούσε τον 1, πράγμα άτοπο. Επομένως, η κλάση $[\beta]$ ανήκει επίσης στο $\mathbb{U}_n$.

Θεωρώντας τώρα στο σύνολο $\mathbb{Z}_n$ την ισότητα που προκύπτει από την (**) παίρνουμε:

$$\begin{aligned}[1] =& [\alpha \cdot n + \beta \cdot m] = [\alpha] \cdot_n [n] +_n [\beta] \cdot_n [m] = [\alpha] \cdot_n [0] +_n [\beta] \cdot_n [m] = \\ & [\alpha \cdot 0] +_n [\beta] \cdot_n [m] = [0] +_n [\beta] \cdot_n [m] = [\beta] \cdot_n [m].\end{aligned}$$

Συνεπώς, η κλάση $[\beta] \in \mathbb{U}_n$ είναι το αντίστροφο τής κλάσης $[m] \in \mathbb{U}_n$ ως προς τον πολλαπλασιασμό κατά μόδιο n και το ζεύγος $(\mathbb{U}_n, \cdot_n)$ αποτελεί μια αβελιανή ομάδα.

Συνήθως, η $(\mathbb{U}_n, \cdot_n)$ ονομάζεται η *ομάδα των αντιστρέψιμων στοιχείων* τού $\mathbb{Z}_n$ και ο πολλαπλασιασμός κατά μόδιο n συμβολίζεται απλώς με «$\cdot$».

Η τάξη τής $[\mathbb{U}_n : 1]$, δηλαδή το πλήθος των κλάσεων ισοτιμίας $[m], m \in \mathbb{N}, 1 \leq m \leq n$ με ΜΚΔ$(n, m) = 1$, ισούται με $\varphi(n)$, όπου φ είναι η φ–συνάρτηση Euler.

Από τη Θεωρία Αριθμών γνωρίζουμε ότι όταν $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_\lambda^{\alpha_\lambda}$ είναι η πρωτογενής ανάλυση τού $n \in \mathbb{N}, n > 1$, τότε $\varphi(n) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdot \cdots \cdot \varphi(p_\lambda^{\alpha_\lambda})$. Επίσης γνωρίζουμε ότι $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, όπου ο p είναι πρώτος αριθμός και ο α είναι φυσικός. Τέλος, ορίζεται $\varphi(1) = 1$.

Δυνάμεις Στοιχείων

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

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

Στην περίπτωση που η $(G, \star)$ είναι μια αβελιανή (μεταθετική) ομάδα και χρησιμοποιούμε την προσθετική σημειογραφία αντί τής γενικής πολλαπλασιαστικής, βλ. σελ. 11, δηλαδή παριστάνουμε την πράξη με «$+$» αντί «$\star$», παριστάνουμε το ουδέτερο τής ομάδας με 0_G αντί e_G και για κάθε $a \in G$, παριστάνουμε με $-a$ αντί a^{-1} το αντίθετο (αντίστροφο) τού a, τότε ορίζουμε:

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

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

Λήμμα 1.2.22 (Κανόνες δυνάμεων)**.** *Έστω ότι $(G, \star)$ είναι μια ομάδα ότι a είναι ένα στοιχείο τού G και ότι m, n είναι δύο ακέραιοι αριθμοί. Τότε*

$$a^m \star a^n = a^{m+n}, \tag{α′}$$

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

$$(a^m)^n = a^{mn}, \tag{β′}$$

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

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

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

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

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

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

(Προσέξτε ότι στην τελευταία σχέση χρησιμοποιούμε το εξής: Επειδή $m \leq -2$, έπεται $m + 1 \leq -1$ και γι' αυτό $|m + 1| = -(m + 1) = -m - 1 = |m| - 1$.)

Υποθέτοντας ότι η (α′) είναι αληθής για $n = k$ (επαγωγική υπόθεση), δηλαδή ότι $a^m \star a^k = a^{m+k}$, θα αποδείξουμε την αλήθειά της, για $n = k + 1$.

Έχουμε $a^m \star a^{k+1} = a^m \star (a^k \star a)$, αφού αυτό το αποδείξαμε μόλις προηγουμένως. Τώρα λόγω τής προσεταιριστικότητας τής «$\star$» έχουμε $a^m \star (a^k \star a) = (a^m \star a^k) \star a$ και λόγω τής επαγωγικής υπόθεσης έχουμε $(a^m \star a^k) \star a = a^{m+k} \star a$. Τέλος, $a^{m+k} \star a = a^{(m+k)+1}$. Ώστε, $a^m \star a^{k+1} = a^{m+(k+1)}$.

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

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

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

Για το αριστερό μέλος τής υποψήφιας ισότητας έχουμε:

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

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

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

Για το δεξιό μέλος τής υποψήφιας ισότητας έχουμε:

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

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

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

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

Παρατήρηση 1.2.23 (Κανόνες πολλαπλασίων). (α′) Στην περίπτωση τής προσθετικής σημειογραφίας η πρώτη ταυτότητα τού Λήμματος 1.2.22 εκφράζεται ως

$$(mg) + (ng) = (m + n)g. \tag{α′}$$

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

Η δεύτερη ταυτότητα τού Λήμματος 1.2.22 εκφράζεται ως

$$m(ng) = (mn)g. \tag{β′}$$

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

(β′) Λόγω τού Λήμματος 1.2.22 έχουμε ότι το αντίστροφο μιας δύναμης a^m, $m \in \mathbb{Z}$ ενός στοιχείου $a \in G$ είναι το στοιχείο a^{-m}, αφού

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

(γ′) Αν η $(G, +)$ είναι αβελιανή, τότε χρησιμοποιώντας προσθετική σημειογραφία έχουμε $-(ma) = (-m)a$.
Προσέξτε ότι το στοιχείο $-(ma)$ είναι το αντίθετο τού ma και ότι το $(-m)a$ είναι το $(-m)$–πολλαπλάσιο τού a.

Θα συμπληρώσουμε τον κατάλογο των παραδειγμάτων με ένα ιδιαιτέρως σημαντικό:

Παράδειγμα 1.2.24. (Από τα Σύνολα)

(α′) **Η συμμετρική ομάδα $(S_X, \circ)$ ενός μη κενού συνόλου X**
Έστω ότι X είναι ένα μη κενό σύνολο και ότι S_X είναι το σύνολο όλων των αμφιρριπτικών απεικονίσεων από το X επί τού εαυτού του.
Στο Παράδειγμα 1.1.2(στ′) έχουμε ήδη διαπιστώσει ότι το ζεύγος $(S_X, \circ)$, όπου $\circ : S_X \times S_X \to S_X$ είναι η πράξη τής σύνθεσης των απεικονίσεων, είναι μια αλγεβρική δομή.

Το ζεύγος $(S_X, \circ)$ αποτελεί ομάδα, επειδή η «$\circ$» είναι προσεταιριστική, επειδή η ταυτοτική απεικόνιση $\mathrm{Id}_X : X \to X$ ικανοποιεί το αίτημα (β′) τού Ορισμού 1.2.1 και επειδή όταν $\sigma \in S_X$, τότε η αντίστροφη απεικόνιση σ^{-1}, η οποία υπάρχει αφού η σ είναι αμφιρριπτική, ικανοποιεί το αίτημα (γ′) τού Ορισμού 1.2.1.
Η ομάδα $(S_X, \circ)$ ονομάζεται η *ομάδα συμμετρίας* ή η *συμμετρική ομάδα* τού συνόλου X.
Παρατηρούμε ότι όταν το πλήθος των στοιχείων τού X είναι ≥ 3, τότε ήδη γνωρίζουμε, βλ. Άσκηση Α3, ότι η $(S_X, \circ)$ δεν είναι αβελιανή.

(β′) **Η συμμετρική ομάδα S_n ενός συνόλου X με $n \in \mathbb{N}$ το πλήθος στοιχεία**
Όταν το σύνολο X είναι πεπερασμένο, ας πούμε ότι $|X| = n$, τότε συχνά γράφουμε

S_n αντί S_X και δίνουμε στη συμμετρική ομάδα $(S_n, \circ)$ την ονομασία *ομάδα μετατάξεων* ή *μεταθέσεων επί των n στοιχείων*.
Τα στοιχεία της, δηλαδή οι αμφιρριπτικές απεικονίσεις από το X επί τού X, ονομάζονται οι *μετατάξεις* ή οι *μεταθέσεις των στοιχείων τού X*.
Επειδή μάλιστα η φύση των στοιχείων τού X δεν επηρεάζει καθόλου τη δομή τής ομάδας, θεωρούμε συνήθως ότι το X ισούται με το σύνολο $\{1, 2, \ldots, n\}$.

Τα στοιχεία τής S_n παριστάνονται ως εξής:

Κάθε αμφιρριπτική απεικόνιση $\sigma : X \to X$ προσδιορίζεται πλήρως από τις τιμές της $\sigma(i) = j_i, i = 1, 2, \ldots, n$, όπου τα $j_1, j_2, \ldots, j_n$ διατρέχουν όλα τα στοιχεία τού $\{1, 2, \ldots, n\}$. Αφού λοιπόν

$$1 \mapsto \sigma(1) = j_1, 2 \mapsto \sigma(2) = j_2, \ldots, n \mapsto \sigma(n) = j_n,$$

μπορούμε να παραστήσουμε τη σ στη μορφή ενός πίνακα[6] με δύο οριζόντιες γραμμές και n στήλες, όπου η πρώτη γραμμή αποτελείται από τα στοιχεία $1, 2, \ldots, n$ και η δεύτερη γραμμή αποτελείται από τις εικόνες τους $\sigma(1), \sigma(2), \ldots, \sigma(n)$. Έτσι γράφουμε:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix} \text{ ή } \sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}.$$

Η τάξη τής S_n ισούται με $[S_n : 1] = n! = 1, 2 \ldots n$, βλ. Άσκηση Α11.

Συμβολισμός. Το ταυτοτικό στοιχείο τής $(S_X, \circ)$ θα το συμβολίζουμε με Id_X ή απλώς με Id. Αν το X είναι ένα σύνολο n στοιχείων, τότε για να δηλώσουμε το ταυτοτικό στοιχείο συχνά θα γράφουμε Id_n.

Παράδειγμα 1.2.25. Η συμμετρική ομάδα $(\mathrm{S}_4, \circ)$ τού συνόλου $\mathrm{X} = \{1, 2, 3, 4\}$.
Η S_4 αποτελείται από τις αμφιρριπτικές απεικονίσεις από το σύνολο X επί τού εαυτού του και η τάξη της $\circ(S_4)$ ισούται με $4! = 24$.
Γράφουμε τα στοιχεία της S_4 χρησιμοποιώντας τη σημειογραφία που είδαμε αμέσως παραπάνω.

$$\begin{aligned}
&\mathrm{Id}_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}, \\
&\tau_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \tau_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \tau_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \\
&\tau_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix},
\end{aligned}$$

[6]Προσοχή, δεν πρόκειται για τους πίνακες που συναντάμε στη Γραμμική Άλγεβρα.

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix},$$
$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}, \sigma_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix},$$
$$\sigma_7 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}, \sigma_8 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix},$$

$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}, \rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}, \rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix},$$
$$\rho_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}, \rho_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}, \rho_6 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix},$$

$$\delta_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \delta_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \delta_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Ας εφαρμόσουμε την πράξη τής ομάδας, που εδώ είναι η σύνθεση των απεικονίσεων, πάνω σε κάποια ζεύγη στοιχείων:
Για να υπολογίσουμε τη σύνθεση $\tau_5 \circ \sigma_2$ οφείλουμε να λογαριάσουμε τις τιμές της πάνω στα στοιχεία[7] $1, 2, 3, 4$ τού X. Έχουμε:

$$\tau_5 \circ \sigma_2(1) = \tau_5(1) = 3, \tau_5 \circ \sigma_2(2) = \tau_5(3) = 1,$$
$$\tau_5 \circ \sigma_2(3) = \tau_5(4) = 4, \tau_5 \circ \sigma_2(4) = \tau_5(2) = 2.$$

Δηλαδή, η $\tau_5 \circ \sigma_2$ απεικονίζει το 1 στο 3, το 2 στο 1, το 3 στο 4 και το 4 στο 3. Συνεπώς, η σύνθεση $\tau_5 \circ \sigma_2$ είναι το στοιχείο $\rho_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ τής S_4.
Παρόμοια για τη σύνθεση $\sigma_2 \circ \tau_5$ έχουμε:

$$\sigma_2 \circ \tau_5(1) = \sigma_2(3) = 4, \sigma_2 \circ \tau_5(2) = \sigma_2(2) = 3,$$
$$\sigma_2 \circ \tau_5(3) = \sigma_2(1) = 1, \sigma_2 \circ \tau_5(4) = \sigma_2(4) = 2.$$

Συνεπώς, η σύνθεση $\sigma_2 \circ \tau_5$ είναι το στοιχείο $\rho_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$ τής S_4.

Επειδή $\tau_5 \circ \sigma_2 = \rho_2 \neq \rho_4 = \sigma_2 \circ \tau_5$ διαπιστώνουμε ότι η $(S_4, \circ)$ *δεν αποτελεί μια αβελιανή (μεταθετική) ομάδα.*

Θα υπολογίσουμε τώρα το αντίστροφο στοιχείο τού $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$, δηλαδή το σ_2^{-1} και κατόπιν το αντίστροφο στοιχείο τού $\tau_5 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$, δηλαδή το τ_5^{-1}.

[7] Για να υπολογίσουμε τις τιμές μιας αμφιρριπτικής απεικόνισης από ένα σύνολο με n στοιχεία στον εαυτό του, είναι αρκετό να υπολογίσουμε μόνο τις πρώτες $n-1$ τιμές, αφού η τελευταία τιμή είναι ακριβώς εκείνο το στοιχείο που δεν εμφανίζεται μεταξύ των πρώτων $n-1$ τιμών.

Παρατηρούμε ότι αφού το στοιχείο σ_2^{-1} είναι η αντίστροφη απεικόνιση τής σ_2 και αφού $\sigma_2(1) = 1$, θα πρέπει να ισχύει $\sigma_2^{-1}(1) = 1$. Ανάλογα, αφού $\sigma_2(2) = 3$, θα πρέπει να ισχύει $\sigma_2^{-1}(3) = 2$, αφού $\sigma_2(3) = 4$, θα πρέπει να ισχύει $\sigma_2^{-1}(4) = 3$ και τέλος αφού αφού $\sigma_2(4) = 2$, θα πρέπει να ισχύει $\sigma_2^{-1}(2) = 4$. Επομένως, το στοιχείο σ_2^{-1} ισούται με το στοιχείο $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$, δηλαδή $\sigma_2^{-1} = \sigma_1$.
Εργαζόμενοι με τον ίδιο τρόπο βλέπουμε ότι $\tau_5^{-1}(1) = 3$, $\tau_5^{-1}(2) = 2$, $\tau_5^{-1}(3) = 1$ και $\tau_5^{-1}(4) = 4$. Επομένως, το στοιχείο τ_5^{-1} ισούται με το στοιχείο $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$, δηλαδή με τον εαυτό του τ_5! [8]

Ασκήσεις στην έννοια τής ομάδας

Λυμένες Ασκήσεις

Α 4. Να σχηματισθούν οι πίνακες πράξης των επόμενων ομάδων:
(α′) $(\mathbb{Z}_4, +)$, (β′) $(\mathbb{Z}_5, +)$, (γ′) $(\mathbb{Z}_6, +)$, βλ. Παράδειγμα 1.2.4(γ′)
(δ′) $(\mathbb{U}_9, \cdot)$, βλ. Παράδειγμα 1.2.21, και (ε′) $(S_3, \circ)$, βλ. Παράδειγμα 1.2.24(β′).

Λύση. (α′) Το σύνολο των κλάσεων ισοτιμίας κατά μόδιο 4 είναι το $\mathbb{Z}_4 = \{[0], [1], [2], [3]\}$ κατά μόδιο (μέτρο, mod)4 και η πράξη είναι η πρόσθεση κατά μόδιο 4. Για τον σχηματισμό τού πίνακα τής πράξης, χρειάζεται να σχηματίσουμε το άθροισμα ανά δύο όλων των στοιχείων τής $\mathbb{Z}_4$[9]. Για παράδειγμα, $[2] + [2] = [4] = [0]$, αφού οι αριθμοί 4 και 0 είναι ισότιμοι κατά μόδιο 4. Όμοια είναι $[2] + [3] = [5] = [1]$, αφού οι 5 και 1 είναι ισότιμοι κατά μόδιο 4.

Ο πίνακας πράξης τής $(\mathbb{Z}_4, +)$ είναι ο ακόλουθος:

$+$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

(β′) Παρόμοια έχουμε ότι $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$ και η πράξη τής $\mathbb{Z}_5$ είναι η πρόσθεση των κλάσεων ισοτιμίας κατά μόδιο (μέτρο, mod) 5. Για τον σχηματισμό τού πίνακα τής πράξης, χρειάζεται να σχηματίσουμε το άθροισμα ανά δύο όλων των στοιχείων τής $\mathbb{Z}_5$. Για παράδειγμα έχουμε $[3] + [3] = [6] = [1]$, και $[4] + [3] = [7] = [2]$.

[8] Αυτό δεν πρέπει να μας εκπλήσσει, αφού το έχουμε ήδη συναντήσει στη Γραμμική Άλγεβρα. Ο αντίστροφος τού πίνακα $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, ως προς τον πολλαπλασιασμό πινάκων, είναι ο εαυτός του.

[9] Βέβαια, επειδή η συγκεκριμένη πράξη είναι μεταθετική, χρειάζεται να εκτελέσουμε πολύ λιγότερους υπολογισμούς. Η παρατήρηση αυτή ισχύει και στην περίπτωση των επόμενων δύο ομάδων, δηλαδή των $\mathbb{Z}_5$ και $\mathbb{Z}_6$.

Ο πίνακας πράξης τής $(\mathbb{Z}_5, +)$ είναι ο ακόλουθος:

$+$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

(γ′) Εντελώς ανάλογα προκύπτει ότι ο πίνακας πράξης τής ομάδας $(\mathbb{Z}_6, +)$, όπου $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$, είναι ο εξής:

$+$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

(δ′) Η $\mathbb{U}_9$ απαρτίζεται από τις κλάσεις $[1], [2], [4], [5], [7], [8]$ κατά μόδιο 9 και η πράξη τής $(\mathbb{U}_9, \cdot)$ είναι ο πολλαπλασιασμός των συγκεκριμένων κλάσεων κατά μόδιο 9. Για τον σχηματισμό τού πίνακα τής πράξης, οφείλουμε να πολλαπλασιάσουμε όλα τα στοιχεία τής $\mathbb{U}_9$ ανά δύο[10]. Για παράδειγμα έχουμε $[4] \cdot [5] = [20] = [2]$, αφού οι αριθμοί 20 και 2 είναι ισότιμοι κατά μόδιο 9. Όμοια είναι $[7] \cdot [8] = [56] = [2]$.

Ο πίνακας πράξης τής $(\mathbb{U}_9, \cdot)$ είναι ο ακόλουθος:

$\cdot$	[1]	[2]	[4]	[5]	[7]	[8]
[1]	[[1]	[2]	[4]	[5]	[7]	[8]
[2]	[2]	[4]	[8]	[1]	[5]	[7]
[4]	[4]	[8]	[7]	[2]	[1]	[5]
[5]	[5]	[1]	[2]	[7]	[8]	[4]
[7]	[7]	[5]	[1]	[8]	[4]	[2]
[8]	[8]	[7]	[5]	[4]	[2]	[1]

(ε′) Η ομάδα $(S_3, \circ)$ των μετατάξεων τού συνόλου $X = \{1, 2, 3, \}$ διαθέτει $3! = 6$ στοιχεία, τα οποία είναι τα εξής:

$$\mathrm{Id}_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

[10]Βέβαια, επειδή η συγκεκριμένη πράξη είναι μεταθετική, χρειάζεται να εκτελέσουμε πολύ λιγότερους υπολογισμούς.

Για να σχηματίσουμε τον πίνακα τής πράξης πρέπει να συνθέσουμε ανά δύο όλα τα στοιχεία τής S_3. Ας υπολογίσουμε για παράδειγμα τη σύνθεση $\rho \circ \tau_1$. Έχουμε:

$$\begin{aligned} \rho \circ \tau_1(1) &= \rho(\tau_1(1)) = \rho(1) = 1, \\ \rho \circ \tau_1(2) &= \rho(\tau_1(2)) = \rho(3) = 1, \\ \rho \circ \tau_1(3) &= \rho(\tau_1(3)) = \rho(2) = 3. \end{aligned}$$

Επομένως, $\rho \circ \tau_1 = \tau_3$.
Όμοια για τη σύνθεση $\rho \circ \sigma$, έχουμε:

$$\begin{aligned} \rho \circ \sigma(1) &= \rho(\sigma(1)) = \rho(3) = 1, \\ \rho \circ \sigma(2) &= \rho(\sigma(2)) = \rho(1) = 2, \\ \rho \circ \sigma(3) &= \rho(\sigma(3)) = \rho(2) = 3. \end{aligned}$$

Άρα, $\rho \circ \sigma = \mathrm{Id}_3$. Ο πίνακας πράξης τής $(S_3, \circ)$ είναι ο:

$\circ$	Id_3	τ_1	τ_2	τ_3	ρ	σ
Id_3	Id_3	τ_1	τ_2	τ_3	ρ	σ
τ_1	τ_1	Id_3	ρ	σ	τ_2	τ_3
τ_2	τ_2	σ	Id_3	ρ	τ_3	τ_1
τ_3	τ_3	ρ	σ	Id_3	τ_1	τ_2
ρ	ρ	τ_3	τ_1	τ_2	σ	Id_3
σ	σ	τ_2	τ_3	τ_1	Id_3	ρ

Α 5. Να δειχθεί ότι

(α′) στη συμμετρική ομάδα $(S_3, \cdot)$, η έκτη δύναμη κάθε στοιχείου της ισούται με το ταυτοτικό στοιχείο Id_3.

(β′) στην ομάδα $(\mathbb{Z}_8, +)$, η όγδοη δύναμη κάθε στοιχείου της ισούται με το ταυτοτικό στοιχείο $[0]$.

Λύση. (α′) Για τον υπολογισμό των δυνάμεων θα χρησιμοποιήσουμε τον πίνακα πράξης τής S_3 που μόλις υπολογίσαμε.

Είναι ${\mathrm{Id}_3}^6 = \mathrm{Id}_3$.

Από τον πίνακα πράξης τής S_3 διαπιστώνουμε ότι για κάθε $\tau_i, i = 1, 2, 3$ είναι $(\tau_i)^2 = \tau_i \circ \tau_i = \mathrm{Id}_3$. Από τους κανόνες των δυνάμεων, βλ. Λήμμα 1.2.22, γνωρίζουμε ότι $(\tau_i)^6 = ((\tau_i)^2)^3$ και αφού $(\tau_i)^2 = \mathrm{Id}_3$, συμπεραίνουμε ότι $(\tau_i)^6 = {\mathrm{Id}_3}^3 = \mathrm{Id}_3$.

Όμοια, από τον πίνακα πράξης τής S_3 διαπιστώνουμε ότι για το ρ είναι: $\rho^3 = \rho^2 \circ \rho = \sigma \circ \rho = \mathrm{Id}_3$. Τώρα από τους κανόνες δυνάμεων προκύπτει $\rho^6 = (\rho^3)^2 = {\mathrm{Id}_3}^2 = \mathrm{Id}_3$.

Για το σ μπορούμε να εκτελέσουμε μια απόδειξη όμοια με αυτήν που κάναμε για το στοιχείο ρ. Μπορούμε όμως να επιχειρηματολογήσουμε και ως εξής: Προηγουμένως είδαμε ότι $\sigma = \rho^2$. Επομένως, $\sigma^6 = (\rho^2)^6 = (\rho^6)^2 = {\mathrm{Id}_3}^2 = \mathrm{Id}_3$.

(β′) Εδώ χρησιμοποιούμε την προσθετική σημειογραφία και γι’ αυτό οι δυνάμεις εκφράζονται πολλαπλασιαστικά, βλ. Παρατήρηση 1.2.23. Προφανώς, $8[0] = [0]$. Ας είναι

$[m], 1 \leq m \leq 7$ οποιοδήποτε από τα μη μηδενικά στοιχεία τής $\mathbb{Z}_8$. Έχουμε $8[m] = 8(m[1]) = (8m)[1] = m(8[1]) = m[8] = m[0] = [0]$.

(Πιθανόν να παρατηρήσατε ότι και στα δύο ερωτήματα τής άσκησης, κάθε στοιχείο τής ομάδας υψωμένο στην τάξη τής ομάδας χορηγεί το ουδέτερο στοιχείο της. Σύντομα θα δούμε ότι δεν πρόκειται για απλή σύμπτωση, αλλά ότι ισχύει στην περίπτωση οποιασδήποτε πεπερασμένης ομάδας. Σχετική είναι και η επόμενη άσκηση.)

A 6. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι g είναι ένα στοιχείο της. Να δειχθεί ότι υπάρχει κάποιος $n \in \mathbb{N}$ με $g^n = e_G$.

Λύση. Σχηματίζουμε το σύνολο $M_g = \{g^m \mid m \in \mathbb{N}\}$ των φυσικών δυνάμεων τού g. Το M_g είναι υποσύνολο τής G, αφού η G όντας ομάδα είναι κλειστή ως προς την πράξη «$\star$». Άρα, το M_g είναι ένα πεπερασμένο σύνολο, διότι $[G:1] < \infty$. Γι' αυτό υπάρχουν $i, j \in \mathbb{N}, i \neq j$ με $g^i = g^j$. Χωρίς περιορισμό τής γενικότητας μπορούμε να δεχθούμε ότι $i < j$ και ως εκ τούτου ο αριθμός $n = j - i$ ανήκει στο $\mathbb{N}$. Τώρα είναι:

$$g^i = g^j \Leftrightarrow g^{-i} \star g^i = g^{-i} \star g^j \Leftrightarrow e_G = g^{j-i}.$$

Άρα, $g^n = g^{j-i} = e_G$.

A 7. Να προσδιοριστούν τα στοιχεία τής ομάδας $(\mathbb{U}_{18}, \cdot)$ και κατόπιν να υπολογιστούν τα $[5]^3, [5]^{-1}, [5]^{-15}$.

Λύση. Η $\mathbb{U}_{18}$ αποτελείται από τις κλάσεις $[m]$, όπου $m \in \mathbb{N}, 1 \leq m \leq 18$ με $\text{ΜΚΔ}(m, 18) = 1$. Συνεπώς,

$$\mathbb{U}_{18} = \{[1], [5], [7], [11], [13], [17]\}.$$

Για το $[5]^3$ έχουμε $[5]^3 = [5^3] = [125]$ και αφού $125 - 17 = 108 = 6 \cdot 18$, έπεται $[5]^3 = [125] = [17]$.

Για τον υπολογισμό τού $[5]^{-1}$ ακολουθούμε την εξής διαδικασία: Αφού ο $\text{ΜΚΔ}(18, 5) = 1$, υπάρχουν $\kappa, \lambda \in \mathbb{Z}$ με $1 = \kappa 18 + \lambda 5$. Τότε $[1] = [\kappa] \cdot [18] + [\lambda] \cdot [5]$ και αφού εργαζόμαστε κατά μόδιο 18, έχουμε $[1] = [\kappa] \cdot [0] + [\lambda] \cdot [5]$, δηλαδή $[1] = [\lambda] \cdot [5]$ και το $[\lambda]$ είναι το αντίστροφο τού $[5]$. Εδώ είναι $1 = 2 \cdot 18 + (-7)(5)$. Ώστε $[1] = [-7] \cdot [5]$ και επειδή $[-7] = [11]$, έπεται $[5]^{-1} = [11]$.

Για τον υπολογισμό τού $[5]^{-15}$ εργαζόμαστε ως εξής: Από τους κανόνες δυνάμεων, βλ. Λήμμα 1.2.22, προκύπτει ότι $[5]^{-15} = ([5]^{-1})^{15}$. Ήδη γνωρίζουμε ότι $[5]^{-1} = [11]$. Συνεπώς, $[5]^{-15} = ([5]^{-1})^{15} = [11]^{15}$. Από την προηγούμενη άσκηση γνωρίζουμε ότι υπάρχει φυσικός n με $[11]^n = [1]$. Υπολογίζουμε τις δυνάμεις $[11]^n, n \in \mathbb{N}$ τού $[11]$ μέχρι να προκύψει το ουδέτερο στοιχείο τής $\mathbb{U}_{18}$, δηλαδή το $[1]$.

Έχουμε $[11]^2 = [13], [11]^3 = [17], [11]^4 = [7], [11]^5 = [5], [11]^6 = [1]$.

Τώρα έχουμε ότι $15 = 2 \cdot 6 + 3$. Κάνοντας χρήση των κανόνων που αναφέρονται στις δυνάμεις στοιχείου ομάδας, βλ. Λήμμα 1.2.22, παίρνουμε:

$$[11]^{15} = [11]^{(2 \cdot 6 + 3)} = [11]^{(2 \cdot 6)} \cdot [11]^3 = ([11]^6)^2 \cdot [11]^3 = [1]^2 \cdot [11]^3 = [11]^3 = [17].$$

Άρα,

$$[5]^{-15} = [11]^{15} = [11]^3 = [17].$$

Α 8. (α′) Στην ομάδα $(\mathbb{Z}_{18}, +)$ να επιλυθούν ως προς x οι εξισώσεις
(i) $x + [53] = [24]$ και (ii) $[21] - x = [12]$.

(β′) Στην ομάδα $(S_9, \circ)$ να επιλυθούν ως προς x οι εξισώσεις
(i) $x \circ \rho^{-1} = \tau^{-1}$ και (ii) $\tau \circ x = \sigma$, όπου

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 8 & 6 & 5 & 1 & 7 & 4 & 9 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 6 & 7 & 9 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

και

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 1 & 4 & 8 & 7 & 6 & 5 & 2 \end{pmatrix}.$$

Λύση. (α′) (i) Έχουμε:

$$x+[53] = [24] \Leftrightarrow x+[53]+(-[53]) = [24]+(-[53]) \Leftrightarrow x = [24]+[-53] \Leftrightarrow x = [-29].$$

Ώστε, $x = [-29]$. Επειδή το σύνολο των στοιχείων τής $\mathbb{Z}_{18}$ περιγράφεται συνήθως από τις κλάσεις $[0], [1], \ldots, [17]$, θα προσδιορίσουμε με ποια από αυτές τις κλάσεις ισούται η $[-29]$. Αλλά αφού $-29 = -2 \cdot 18 + 7$, έχουμε $[-29] = [7]$. Επομένως, $[x] = [7]$.
(ii) Έχουμε:

$$[21] - x = [12] \Leftrightarrow ([21] - x) + [21] = [12] + [21] \Leftrightarrow -x = [33] \Leftrightarrow x = -[33] \Leftrightarrow x = [-33].$$

Ώστε, $x = [-33]$. Αλλά αφού $-33 = -2 \cdot 18 + 3$, έχουμε $[-33] = [3]$. Επομένως, $[x] = [3]$.
(β′) (i) Έχουμε:

$$x \circ \rho^{-1} = \tau^{-1} \Leftrightarrow (x \circ \rho^{-1}) \circ \rho = \tau^{-1} \circ \rho \Leftrightarrow x \circ (\rho^{-1} \circ \rho) = \tau^{-1} \circ \rho \Leftrightarrow x \circ \mathrm{Id}_9 = \tau^{-1} \circ \rho.$$

Επομένως, $x = \tau^{-1} \circ \rho$. Για να διαπιστώσουμε τώρα, ποιο είναι ακριβώς το στοιχείο x θα υπολογίσουμε το τ^{-1} και κατόπιν τη σύνθεση $\tau^{-1} \circ \rho$. Το τ^{-1} είναι ίσο με τη μετάταξη $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 2 & 3 & 1 & 4 \end{pmatrix}$. Έτσι έχουμε:

$$x = \tau^{-1} \circ \rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 2 & 3 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 8 & 6 & 5 & 1 & 7 & 4 & 9 \end{pmatrix} =$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 7 & 8 & 1 & 2 & 5 & 9 & 3 & 6 & 4 \end{pmatrix}.$$

(ii) Έχουμε:

$$\tau \circ x = \sigma \Leftrightarrow \tau^{-1} \circ (\tau \circ x) = \tau^{-1} \circ \sigma \Leftrightarrow \mathrm{Id}_9 \circ x = \tau^{-1} \circ \sigma.$$

Επομένως,

$$x = \tau^{-1} \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 2 & 3 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 1 & 4 & 8 & 7 & 6 & 5 & 2 \end{pmatrix} =$$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 7 & 9 & 6 & 1 & 3 & 2 & 5 & 8 \end{pmatrix}.$$

Α 9. Ποιες από τις ακόλουθες πράξεις

$$\star : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, (a, b) \mapsto a \star b$$

ορίζουν επί τού $\mathbb{R}$ τη δομή μιας ομάδας; (Οι πράξεις στη δεξιά πλευρά είναι οι συνήθεις πράξεις των πραγματικών αριθμών.)

(α′) $a \star b := 5a + b$,

(β′) $a \star b := a + b + ab$,

(γ′) $a \star b := a$.

Λύση. (α′) Σύμφωνα με τον ορισμό τής ομάδας, η πράξη «$\star$» οφείλει να είναι προσεταιριστική. Θα πρέπει $\forall a, b, c \in \mathbb{R}$ να ισχύει: $(a \star b) \star c = a \star (b \star c)$. Αλλά, $(a \star b) \star c = (5a + b) \star c = 5(5a + b) + c$ και $a \star (b \star c) = 5a + b \star c = 5a + 5b + c$. Επιλέγοντας, $a = 1, b = c = 0$ διαπιστώνουμε ότι $(a \star b) \star c = 25 \neq 5 = a \star (b \star c)$. Συνεπώς, η συγκεκριμένη πράξη δεν ορίζει τη δομή ομάδας επί τού $\mathbb{R}$.

(β′) Σύμφωνα με τον ορισμό τής ομάδας, η «$\star$» οφείλει να είναι προσεταιριστική. Θα πρέπει $\forall a, b, c \in \mathbb{R}$ να ισχύει: $\forall a, b, c \in \mathbb{R}, (a \star b) \star c = a \star (b \star c)$.
Εδώ έχουμε:

$$(a\star b)\star c = (a+b+ab)\star c = a+b+ab+c+(a+b+ab)c = a+b+ab+c+ac+bc+abc$$

και

$$a\star(b\star c) = a\star(b+c+bc) = a+b+c+bc+a(b+c+bc) = a+b+c+bc+ab+ac+abc.$$

Συνεπώς η «$\star$» είναι προσεταιριστική πράξη.

Σύμφωνα με τον ορισμό τής ομάδας, θα πρέπει να υπάρχει ουδέτερο στοιχείο, δηλαδή κάποιο $e \in \mathbb{R}$ με $a \star e = a = e \star a$ ή ισοδύναμα $a + e + ae = a = e + a + ea$, για κάθε $a \in G$. Παρατηρούμε ότι το μοναδικό στοιχείο τού $\mathbb{R}$, που $\forall a \in G$, ικανοποιεί την προηγούμενη σχέση είναι το στοιχείο $e = 0$. Θα πρέπει τώρα δείξουμε ότι κάθε $a \in G$ διαθέτει αντίστροφο στοιχείο, δηλαδή ότι όταν $a \in G$, τότε υπάρχει $b \in G$ με $a \star b = e = b \star a$ ή ισοδύναμα $a + b + ab = 0 = a + b + ba$. Ιδιαιτέρως, όταν $a = -1$, τότε θα πρέπει να υπάρχει b με $-1 + b + (-1)b = 0$. Αυτό όμως είναι αδύνατο, αφού η τελευταία σχέση είναι ισοδύναμη με την $-1 = 0$. Ώστε το στοιχείο -1 δεν διαθέτει αντίστροφο και η συγκεκριμένη πράξη δεν ορίζει τη δομή ομάδας επί τού $\mathbb{R}$.

(γ′) Αν το $\mathbb{R}$ ήταν ομάδα με τη συγκεκριμένη πράξη, τότε θα έπρεπε, σύμφωνα με το Λήμμα 1.2.18(α′), η εξίσωση $a \star x = b$ να είχε λύση ως προς x, για κάθε $a, b \in \mathbb{R}$. Ας υποθέσουμε ότι το $(\mathbb{R}, \star)$ είναι ομάδα και ότι c είναι μια λύση τής εξίσωσης $2\star c = 1$. Όμως σύμφωνα με τον ορισμό τής «$\star$», το στοιχείο $2\star c$ είναι ίσο με 2 και επομένως $2 = 2\star c = 1$. Το τελευταίο είναι άτοπο και γι’ αυτό το $\mathbb{R}$ με τη συγκεκριμένη πράξη δεν είναι ομάδα.

Α 10. Έστω ότι G είναι το υποσύνολο τού $M_{2\times 2}(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z} \right\}$ που αποτελείται από τους ακόλουθους πίνακες:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, B = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, C = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix},$$
$$D = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, F = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Να δειχθεί ότι το G μαζί με τον συνήθη πολλαπλασιασμό πινάκων «$\cdot$» απαρτίζει μια ομάδα. Να σχηματιστεί ο πίνακας πράξης τής ομάδας και να εξεταστεί, αν πρόκειται για αβελιανή (μεταθετική) ομάδα.

Λύση.

$\cdot$	E	A	B	C	D	F
E	E	A	B	C	D	F
A	A	B	E	D	F	C
B	B	E	A	F	C	D
C	C	F	D	E	B	A
D	D	C	F	A	E	B
F	F	D	C	B	A	E

Σχήμα 1.5: Ο πίνακας τής πράξης «$\cdot$» επί των στοιχείων τού συνόλου G.

Το σύνολο G είναι διάφορο τού κενού. Κατά τον σχηματισμό τού πίνακα πράξης, βλ. Σχήμα 1.5, διαπιστώνουμε ότι το γινόμενο δύο οποιωνδήποτε πινάκων από το G ανήκει και πάλι στο G.
Η πράξη είναι προσεταιριστική, αφού γνωρίζουμε ότι γενικώς ο πολλαπλασιασμός πινάκων είναι προσεταιριστικός. Τέλος παρατηρούμε ότι σε κάθε γραμμή και κάθε στήλη τού πίνακα πράξης τού G, , βλ. Σχήμα 1.5, εμφανίζεται κάθε στοιχείο τού G ακριβώς μία φορά. Σύμφωνα με την Πρόταση 1.2.19, το ζεύγος $(G, \cdot)$ αποτελεί ομάδα. Η συγκεκριμένη ομάδα δεν είναι αβελιανή, αφού $A \cdot C = D \neq F = C \cdot A$.

Α 11. Έστω ότι X είναι ένα σύνολο διάφορο τού κενού και ότι $(S_X, \circ)$ είναι η συμμετρική ομάδα τού X, βλ. Παράδειγμα 1.2.24.
Να δειχθεί ότι

(α′) όταν το X είναι ένα άπειρο σύνολο, τότε η τάξη $[S_X : 1]$ είναι άπειρη και

(β′) όταν το X είναι ένα πεπερασμένο σύνολο, ας πούμε ότι $X = \{1, 2, \ldots, n\}$, τότε η τάξη $[S_X : 1]$ είναι ίση με $n!$.

Λύση. (α′) Θα κατασκευάσουμε ένα υποσύνολο τού S_X με άπειρο το πλήθος στοιχεία. Ας είναι a ένα συγκεκριμένο στοιχείο τού X. Για κάθε $x \in X$, ορίζουμε την απεικόνιση:

$$\sigma_x : X \to X, \text{ όπου } \sigma_x(a) = x, \sigma_x(x) = a \text{ και } \forall y \neq x, a, \sigma_x(y) = y.$$

Η σ_x είναι αμφιρριπτική, αφού $\sigma_X \circ \sigma_X = \mathrm{Id}_X$ και γι' αυτό το σύνολο $\Sigma_X = \{\sigma_x \mid x \in X\}$ είναι υποσύνολο τού S_X.

Η απεικόνιση

$$\mathcal{L} : X \to \Sigma_X, x \mapsto \mathcal{L}(x) := \sigma_x$$

είναι αμφιρριπτική, αφού κατά προφανή τρόπο είναι επιρριπτική και επιπλέον είναι ενριπτική αφού, αν $\sigma_x = \mathcal{L}(x) = \mathcal{L}(y) = \sigma_y$, τότε $x = \sigma_x(a) = \sigma_y(a) = y$. Συνεπώς, τα X και Σ_X είναι ισοπληθή και έτσι το Σ_X έχει άπειρο το πλήθος στοιχεία. Επομένως, το S_X είναι άπειρο σύνολο, αφού περιέχει το άπειρο υποσύνολο Σ_X. Άρα, $[S_X : 1] = \infty$

(β′) Όταν το X είναι ένα πεπερασμένο σύνολο, τότε είναι γνωστό ότι οι αμφιρριπτικές απεικονίσεις από το X επί τού X συμπίπτουν με τις ενριπτικές. Ας δούμε με πόσους διαφορετικούς τρόπους μπορεί να προκύψει μια ενριπτική απεικόνιση σ από το X στο X. Για την εικόνα $\sigma(1)$ υπάρχουν n το πλήθος επιλογές μεταξύ των στοιχείων τού X. Για την εικόνα $\sigma(2)$ μπορεί να επιλεγεί οποιοδήποτε στοιχείο με εξαίρεση το $\sigma(1)$, αφού η σ είναι ενριπτική. Συνεπώς, για την εικόνα $\sigma(2)$ υπάρχουν $(n-1)$ το πλήθος επιλογές. Για την εικόνα $\sigma(3)$ υπάρχουν $(n-2)$ το πλήθος επιλογές, δηλαδή η $\sigma(3)$ μπορεί να είναι οποιοδήποτε στοιχείο τού X εκτός των $\sigma(1), \sigma(2)$. Συνεχίζοντας κατ' αυτόν τον τρόπο, διαπιστώνουμε ότι όταν έχουμε επιλέξει τις τιμές των $\sigma(1), \sigma(2), \ldots, \sigma(i), i < n$, τότε για το $\sigma(i+1)$ απομένουν $(n-i)$ το πλήθος επιλογές.
Συνεπώς, μια ενριπτική απεικόνιση από το X στο X μπορεί να προκύψει με $n \cdot (n-1) \cdot \ldots 2 \cdot 1 = n!$ τρόπους. Επομένως, $[S_X : 1] = n!$

Α 12. Έστω ότι $(G, \star)$ είναι μια ομάδα και a, b δύο στοιχεία της. Αν το στοιχείο a μετατίθεται με το b, τότε να δειχθεί ότι και το αντίστροφο τού a, δηλαδή το a^{-1}, μετατίθεται επίσης με το b.

Λύση. Αφού το a μετατίθεται με το b έχουμε $a \star b = b \star a$. Συνεπώς

$$\begin{aligned}
& a \star b = b \star a \Leftrightarrow a^{-1} \star (a \star b) \star a^{-1} = a^{-1} \star (b \star a) \star a^{-1} \Leftrightarrow \\
& (a^{-1} \star a) \star (b \star a^{-1}) = (a^{-1} \star b) \star (a \star a^{-1}) \Leftrightarrow \\
& e_G \star (b \star a^{-1}) = (a^{-1} \star b) \star e_G \Leftrightarrow b \star a^{-1} = a^{-1} \star b.
\end{aligned}$$

Α 13. Να δειχθεί ότι κάθε ομάδα $(G, \star)$ διαθέτει ακριβώς ένα στοιχείο a με $a \star a = a$.

Λύση. Για οποιαδήποτε δύο στοιχεία $a, b \in G$ μιας ομάδας G, η εξίσωση $a \star x = b$, διαθέτει ακριβώς μία λύση ως προς x. Το ίδιο συμβαίνει και με την εξίσωση $a \star x = a$. Προφανώς, η μοναδική αυτή λύση είναι η $x = e_G$, όπου e_G είναι το ουδέτερο στοιχείο τής G. Όταν λοιπόν είναι $a \star a = a$, τότε το a είναι λύση τής $a \star x = a$ και επομένως $a = e_G$.

Α 14. Έστω $(G, \star)$ μια ομάδα. Όταν η τάξη $\circ(G)$ είναι ένας άρτιος αριθμός, τότε να δείξετε ότι υπάρχει ένα στοιχείο $a \neq e_G$ στην G τέτοιο, ώστε $a \star a = e_G$. (*Το e_G είναι το ταυτοτικό στοιχείο τής G.*)

Λύση. Αφού η G έχει άρτιο πλήθος στοιχείων, το σύνολο $G \setminus \{e\}$, το οποίο αποτελείται από τα στοιχεία που είναι διαφορετικά από το ουδέτερο, διαθέτει περιττό πλήθος στοιχείων. Αν τώρα για κάθε $a \in G \setminus \{e\}$, είχαμε $a \neq a^{-1}$, τότε το πλήθος των στοιχείων τού $G \setminus \{e\}$ μετρώντας το με τη βοήθεια των υποσυνόλων $\{a, a^{-1}\}$ θα ήταν άρτιο. Αυτό όμως είναι αδύνατο. Επομένως, υπάρχει κάποιο $a \neq e$ με $a = a^{-1}$.

Α 15. Έστω $(G, \star)$ μια ομάδα και $a, b \in G$. Να δείξετε ότι

$$(a \star b)^{-1} = a^{-1} \star b^{-1} \Leftrightarrow a \star b = b \star a.$$

Να συμπεράνετε ότι μια ομάδα η $(G, \star)$ είναι αβελιανή (μεταθετική), αν και μόνο αν,

$$\forall a, b \in G, (a \star b)^{-1} = a^{-1} \star b^{-1}.$$

Λύση. Έχουμε:

$$(a \star b)^{-1} = a^{-1} \star b^{-1} \Leftrightarrow ((a \star b)^{-1})^{-1} = (a^{-1} \star b^{-1})^{-1}.$$

Αλλά σύμφωνα με το Λήμμα 1.2.17. είναι $((a \star b)^{-1})^{-1} = a \star b$ και $(a^{-1} \star b^{-1})^{-1} = (b^{-1})^{-1} \star (a^{-1})^{-1} = b \star a$. Επομένως,

$$(a \star b)^{-1} = a^{-1} \star b^{-1} \Leftrightarrow a \star b = b \star a.$$

Αν λοιπόν $\forall a, b \in G$, είναι $(a \star b)^{-1} = a^{-1} \star b^{-1}$, τότε η $(G, \star)$ είναι αβελιανή και αν η $(G, \star)$ είναι αβελιανή τότε $\forall a, b \in G$ είναι $a \star b = b \star a$ και επομένως, $\forall a, b \in G$, είναι $(a \star b)^{-1} = a^{-1} \star b^{-1}$.

Α 16. Έστω $(G, \star)$ μια ομάδα. Όταν

$$\forall a \in G, \text{ είναι: } a \star a = e_G,$$

τότε να δείξτε ότι η G είναι αβελιανή. (*Το e_G είναι το ταυτοτικό στοιχείο τής G.*)

Λύση. Προφανώς, $a \star a = e_G \Leftrightarrow a = a^{-1}$. Αν αυτό συμβαίνει, για όλα τα στοιχεία τής G, τότε συμπεραίνουμε ότι το αντίστροφο κάθε στοιχείου τής G ισούται με τον εαυτό του. Ιδιαιτέρως, αν $a, b \in G$, το αντίστροφο τού στοιχείου $a \star b$ ισούται με $a \star b$, δηλαδή $(a \star b)^{-1} = a \star b$. Αλλά, $a = a^{-1}$ και $b = b^{-1}$. Έτσι τελικώς προκύπτει

$$\forall a, b \in G, \quad (a \star b)^{-1} = a \star b = a^{-1} \star b^{-1}.$$

Τώρα από την Άσκηση Α15, έπεται αμέσως ότι η $(G, \star)$ είναι μια αβελιανή ομάδα.

Α 17. Έστω $(G, \star)$ μια ομάδα. Όταν ισχύει

$$\forall a, b \in G, (a \star b)^2 = a^2 \star b^2.$$

τότε να δείξτε ότι η G είναι αβελιανή (μεταθετική).

Λύση. Σύμφωνα με τον ορισμό δυνάμεων στοιχείων έχουμε: $(a \star b)^2 = (a \star b) \star (a \star b)$ και $a^2 \star b^2 = (a \star a) \star (b \star b)$. Λαμβάνοντας υπ' όψιν την προσεταιριστικότητα τής πράξης «$\star$», η υπόθεση τής άσκησης γράφεται:

$$\forall a, b \in G : a \star (b \star a) \star b = a \star (a \star b) \star b$$

και έχουμε:

$$\begin{aligned}\forall a, b \in G: \quad & a \star (b \star a) \star b = a \star (a \star b) \star b \Leftrightarrow \\ & a^{-1} \star (a \star (b \star a) \star b) \star b^{-1} = a^{-1} \star (a \star (a \star b) \star b) \star b^{-1} \Leftrightarrow \\ & (a^{-1} \star a) \star (b \star a) \star (b \star b^{-1}) = (a^{-1} \star a) \star (a \star b) \star (b \star b^{-1}) \Leftrightarrow \\ & e_G \star (b \star a) \star e_G = e_G \star (a \star b) \star e_G \Leftrightarrow b \star a = a \star b.\end{aligned}$$

Η ομάδα G είναι αβελιανή (μεταθετική).

Α 18. Έστω ότι $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι δύο ομάδες. Να δειχθεί ότι το καρτεσιανό γινόμενο $G_1 \times G_2$ εφοδιασμένο με την πράξη

$$\star : (G_1 \times G_2) \times (G_1 \times G_2) \to G_1 \times G_2, ((a_1, a_2), (b_1, b_2)) \mapsto (a_1 \star_1 b_1, a_2 \star_2 b_2)$$

αποτελεί μια ομάδα.
(Η συγκεκριμένη ομάδα ονομάζεται το (εξωτερικό) *ευθύ γινόμενο* των ομάδων G_1 και G_2.)

Λύση. Για κάθε $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$, έχουμε

$$\begin{aligned}&(a_1, a_2) \star ((b_1, b_2) \star (c_1, c_2)) = (a_1, a_2) \star (b_1 \star_1 c_1, b_2 \star_2 c_2) = \\ &(a_1 \star_1 (b_1 \star_1 c_1), a_2 \star_2 (b_2 \star_2 c_2)).\end{aligned}$$

Επίσης

$$\begin{aligned}&((a_1, a_2) \star (b_1, b_2)) \star (c_1, c_2) = (a_1 \star_1 b_1, a_2 \star_2 b_2) \star (c_1, c_2) = \\ &((a_1 \star_1 b_1) \star_1 c_1, (a_2 \star_2 b_2) \star_2 c_2).\end{aligned}$$

Αλλά $a_1 \star_1 (b_1 \star_1 c_1) = (a_1 \star_1 b_1) \star_1 c_1$ και $a_2 \star_2 (b_2 \star_2 c_2) = (a_2 \star_2 b_2) \star_2 c_2$, αφού οι αντίστοιχες πράξεις «$\star_1$» και «$\star_2$» είναι προσεταιριστικές. Έτσι τελικώς έχουμε

$$(a_1, a_2) \star ((b_1, b_2) \star (c_1, c_2)) = ((a_1, a_2) \star (b_1, b_2)) \star (c_1, c_2)$$

και η «$\star$» είναι μια προσεταιριστική πράξη.

Αν e_i είναι το ουδέτερο στοιχείο τής G_i, $i = 1, 2$, τότε το (e_1, e_2) είναι το ουδέτερο τού $G_1 \times G_2$, αφού για κάθε $(a_1, a_2) \in G_1 \times G_2$ έχουμε:

$$\begin{aligned}&(a_1, a_2) \star (e_1, e_2) = (a_1 \star_1 e_1, a_2 \star_2 e_2) = (a_1, a_2) = \\ &(e_1 \star_1 a_1, e_2 \star_2 a_2) = (e_1, e_2) \star (a_1, a_2).\end{aligned}$$

Αν $(a_1, a_2) \in G_1 \times G_2$ και a_i^{-1} είναι το αντίστροφο τού $a_i \in G_i$, $i = 1, 2$, τότε

$$(a_1, a_2) \star (a_1^{-1}, a_2^{-1}) = (a_1 \star_1 a_1^{-1}, a_2 \star_2 a_2^{-1}) = (e_1, e_2) =$$
$$(a_1^{-1} \star_1 a_1, a_2^{-1} \star_2 a_2) = (a_1^{-1}, a_2^{-1}) \star (a_1, a_2).$$

Επομένως, το αντίστροφο τού $(a_1, a_2) \in G_1 \times G_2$ είναι το (a_1^{-1}, a_2^{-1}) και το ζεύγος $(G_1 \times G_2, \star)$ αποτελεί ομάδα.

Ο ορισμός τού ευθέος γινομένου δύο ομάδων επεκτείνεται στο ευθύ γινόμενο οποιασδήποτε οικογένειας $((G_i, \star_i))_{i\in I}$ ομάδων, όπου το I είναι ένα πεπερασμένο ή άπειρο σύνολο δεικτών. Στην περίπτωση αυτή το υποκείμενο σύνολο τής ομάδας είναι το καρτεσιανό γινόμενο $\Pi_{i\in I}G_i$ και το γινόμενο δύο στοιχείων $(a_i)_{i\in I}$ και $(a_i')_{i\in I}$ τής $\Pi_{i\in I}G_i$ ορίζεται ως το στοιχείο $(a_i \star_i a_i')_{i\in I} \in \Pi_{i\in I}G_i$.

Α 19. Θεωρούμε τις ομάδες των κλάσεων ισοτιμίας $(\mathbb{Z}_2, +)$ και $(\mathbb{Z}_3, +)$. Να σχηματιστεί ο πίνακας πράξης τού ευθέος γινομένου $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Λύση. Το σύνολο των στοιχείων τής ομάδας $\mathbb{Z}_2$ είναι το $\{[0]_2, [1]_2\}$ και τής ομάδας $\mathbb{Z}_3$ είναι το $\{[0]_3, [1]_3, [2]_3\}$, όπου ο δείκτης 2 ή 3 υπονοεί την αντίστοιχη κλάση ισοτιμίας κατά μόδιο 2 ή 3. Έτσι έχουμε:

$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{e = ([0]_2, [0]_3), a = ([0]_2, [1]_3), b = ([0]_2, [2]_3),$$
$$c = ([1]_2, [0]_3), d = ([1]_2, [1]_3), f = ([1]_2, [2]_3)\}$$

$+$	e	a	b	c	d	f
e	e	a	b	c	d	f
a	a	b	e	d	f	c
b	b	e	a	f	c	d
c	c	d	f	e	a	b
d	d	f	c	a	b	e
f	f	c	d	b	e	a

Σχήμα 1.6: Ο πίνακας τής πράξης «+» επί των στοιχείων τής ομάδας $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Ας ονομάσουμε «+» την επαγόμενη πράξη, όπως αυτή ορίζεται στην αμέσως προηγούμενη άσκηση. Ο πίνακας πράξης προκύπτει υπολογίζοντας τις τιμές $x + y$, όπου $x, y \in \mathbb{Z}_2 \times \mathbb{Z}_3$. Για παράδειγμα:

$$b + c = ([0]_2, [2]_3) + ([1]_2, [0]_3) = ([0]_2 +_2 [1]_2, [2]_3 +_3 [0]_3) = ([1]_2, [2]_3) = f,$$
$$f + d = ([1]_2, [2]_3) + ([1]_2, [1]_3) = ([1]_2 +_2 [1]_2, [2]_3 +_3 [1]_3) = ([0]_2, [0]_3) = e.$$

Ο πίνακας πράξης τής ομάδας $\mathbb{Z}_2 \times \mathbb{Z}_3$ αποδίδεται στο Σχήμα 1.6.

Α 20. Ας είναι G το ανοικτό διάστημα $(-1,1)$ των πραγματικών αριθμών $\mathbb{R}$. Να δειχθεί ότι η αντιστοιχία

$$(a,b) \mapsto a \star b := \frac{a+b}{1+ab}$$

ορίζει μια πράξη «$\star$» επί τού G, η οποία καθιστά το ζεύγος $(G,\star)$ μια αβελιανή (μεταθετική) ομάδα.

Λύση. Θα αποδείξουμε πρώτα ότι η ανωτέρω αντιστοιχία χορηγεί μια καλά ορισμένη απεικόνιση $\star : G \times G \to G$, δηλαδή ότι αν $a, b \in G$, τότε και το $a \star b = \frac{a+b}{1+ab}$ ανήκει επίσης στο G. Παρατηρούμε ότι $a \in G \Leftrightarrow |a| < 1$. Επειδή λοιπόν $a, b \in G$ έχουμε $|ab| < 1$, συνεπώς $0 < 1 + ab$ και γι' αυτό έχει νόημα το κλάσμα $a \star b = \frac{a+b}{1+ab}$, αφού ο παρονομαστής του είναι $\neq 0$. Έχουμε:

$$\begin{aligned}
&\forall a, b \in G, \\
&a \star b \in G \Leftrightarrow |a \star b| = \left|\frac{a+b}{1+ab}\right| < 1 \Leftrightarrow |a+b| < |1+ab| \Leftrightarrow \\
&(a+b)^2 < (1+ab)^2 \Leftrightarrow a^2 + b^2 < 1 + a^2b^2 \Leftrightarrow \\
&a^2 - 1 < b^2(a^2-1) \Leftrightarrow 1 > b^2. \qquad (\alpha')
\end{aligned}$$

Προσέξτε ότι όταν $a \in (-1,1)$, τότε $a^2 - 1 < 0$ και γι' αυτό η $a^2 - 1 < b^2(a^2-1)$ δίνει $1 > b^2$. Επίσης, όταν $1 > b^2$ και αφού $a^2 - 1 < 0$, τότε έπεται $a^2 - 1 < b^2(a^2-1)$. Επομένως, η τελευταία ισοδυναμία τής (α') είναι αληθής και γι' αυτό το $a \star b$ ανήκει στο G.

Η προσεταιριστική ιδιότητα τής «$\star$» προκύπτει εύκολα κατόπιν εκτέλεσης των πράξεων $a \star (b \star c)$ και $(a \star b) \star c$.

Για το στοιχείο $0 \in G$, έχουμε $\forall a \in G, 0 \star a = \frac{0+a}{1+0a} = a = a \star 0$.

Τέλος, αν $a \in G$, τότε το $-a$ ανήκει επίσης στο G και $a \star (-a) = \frac{a+(-a)}{1+a(-a)} = 0 = (-a) \star (a)$.

Επομένως, το ζεύγος $(G,\star)$ αποτελεί ομάδα με ουδέτερο στοιχείο το 0 των πραγματικών αριθμών και με αντίστροφο κάθε $a \in G$ το $-a$. Προφανώς πρόκειται για αβελιανή ομάδα, αφού $\forall a, b \in G, a \star b = \frac{a+b}{1+ab} = \frac{b+a}{1+ba} = b \star a$.

Α 21. Στο σύνολο των ακέραιων αριθμών $\mathbb{Z}$ θεωρούμε την πράξη:

$$\star : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (n,m) \mapsto n \star m = \begin{cases} n+m, & \text{αν ο } n \text{ είναι άρτιος αριθμός,} \\ n-m, & \text{αν ο } n \text{ είναι περιττός αριθμός.} \end{cases}$$

Να δειχθεί ότι το ζεύγος $(\mathbb{Z},\star)$ αποτελεί ομάδα.

Λύση. Θα δείξουμε η «$\star$» είναι προσεταιριστική πράξη, δηλαδή ότι $\forall k, \ell, m \in \mathbb{Z}$ ισχύει: $k \star (\ell \star m) = (k \star \ell) \star m$. Διακρίνουμε τις εξής περιπτώσεις:

(α') Αν οι k, ℓ είναι άρτιοι, τότε $k \star (\ell \star m) = k \star (\ell + m) = k + (\ell + m)$ και $(k \star \ell) \star m = (k+\ell) \star m) = (k+\ell) + m$, επειδή το άθροισμα $k + \ell$ των άρτιων αριθμών k, ℓ είναι άρτιος αριθμός. Συνεπώς στην περίπτωση αυτή, ισχύει η προσεταιριστικότητα τής πράξης.

(β′) Αν οι k, ℓ είναι περιττοί, τότε $k \star (\ell \star m) = k \star (\ell - m) = k - (\ell - m)$ και $(k \star \ell) \star m = (k - \ell) \star m = (k - \ell) + m$, επειδή η διαφορά $k - \ell$ των περιττών αριθμών k, ℓ είναι άρτιος αριθμός. Συνεπώς στην περίπτωση αυτή ισχύει η προσεταιριστικότητα τής πράξης.

(γ′) Αν ο k είναι άρτιος και ο ℓ περιττός, τότε $k \star (\ell \star m) = k \star (\ell - m) = k + \ell - m$ και $(k \star \ell) \star m = (k + \ell) \star m = (k + \ell) - m$, επειδή το άθροισμα $k + \ell$ τού άρτιου k με τον περιττό ℓ είναι περιττός αριθμός. Συνεπώς στην περίπτωση αυτή ισχύει η προσεταιριστικότητα τής πράξης.

(δ′) Αν ο k είναι περιττός και ο ℓ είναι άρτιος, τότε $k \star (\ell \star m) = k \star (\ell + m) = k - (\ell + m)$ και $(k \star \ell) \star m = (k - \ell) \star m = (k - \ell) - m$, επειδή το άθροισμα $k - \ell$ τού περιττού k με τον άρτιο ℓ είναι περιττός αριθμός. Συνεπώς και στην περίπτωση αυτή ισχύει η προσεταιριστικότητα τής πράξης

Έτσι συμπεραίνουμε ότι η πράξη είναι προσεταιριστική.

Το στοιχείο $0 \in \mathbb{Z}$ είναι το ουδέτερο στοιχείο τής «$\star$», αφού $\forall m \in \mathbb{Z}$ είναι $0 \star m = 0 + m = m$ και $m \star 0 = m + 0 = m$ (όταν ο m είναι άρτιος) και $m \star 0 = m - 0 = m$ (όταν ο m είναι περιττός).

Όταν ο $m \in \mathbb{Z}$ είναι άρτιος, τότε το αντίστροφό του είναι το $-m$, επειδή $m \star (-m) = m + (-m) = 0 = (-m) + m = (-m) \star m$ ενώ όταν ο $m \in \mathbb{Z}$ είναι περιττός, τότε το αντίστροφό του είναι το m, επειδή $m \star m = m + (-m) = 0 = (-m) + m = m \star m$.

Επομένως το ζεύγος $(\mathbb{Z}, \star)$ είναι ομάδα, η οποία δεν είναι αβελιανή, αφού για $m \neq 0$ άρτιο και n περιττό δεν ισχύει ποτέ η ισότητα $m \star n = n \star m$. Αφού

$$m \star n = n \star m \Leftrightarrow m + n = n - m \Leftrightarrow 2m = 0 \Leftrightarrow m = 0.$$

Α 22. Να δειχθεί το Θεώρημα Wilson: Για κάθε πρώτο αριθμό p είναι:

$$(p-1)! \equiv -1 \bmod p.$$

Λύση. Θεωρούμε την ομάδα $(\mathbb{U}_p, \cdot)$ των αντιστρέψιμων κλάσεων ισοτιμίας τού $\mathbb{Z}$ κατά μόδιο p, βλ. Παράδειγμα 1.2.21.
Το σύνολο των στοιχείων τής ομάδας ισούται με $\{[1], [2], \ldots [p-1]\}$. Παρατηρούμε ότι η προς απόδειξη σχέση εκφράζεται με τη βοήθεια των στοιχείων τής $\mathbb{U}_p$ ως

$$[1] \cdot [2] \cdot \cdots \cdot [p-1] = [-1]. \tag{*}$$

Το αριστερό μέλος τής (*) είναι το γινόμενο όλων των στοιχείων τής $\mathbb{U}_p$. Η $\mathbb{U}_p$ είναι αβελιανή και γι' αυτό στο προηγούμενο γινόμενο κάθε στοιχείο, που δεν έχει ως αντίστροφο τον εαυτό του, πολλαπλασιασμένο με το αντίστροφό του δίνει ως αποτέλεσμα το ουδέτερο στοιχείο [1] τής $\mathbb{U}_p$. Έτσι, το $[1] \cdot [2] \cdot \cdots \cdot [p-1]$ ισούται τελικώς με το γινόμενο των στοιχείων τής $\mathbb{U}_p$, τα οποία έχουν ως αντίστροφο τον εαυτό τους. Ας δούμε ποια στοιχεία τής $\mathbb{U}_p$ έχουν αυτήν την ιδιότητα. Έστω $[\kappa] \in \mathbb{U}_p$ μια κλάση ισοτιμίας με $[\kappa] = [\kappa]^{-1}$, δηλαδή με $[\kappa]^2 = [1]$, όπου $1 \leq \kappa \leq p-1$. Έχουμε $[\kappa]^2 = [1] \Leftrightarrow p \mid (\kappa - 1)(\kappa + 1) \Leftrightarrow$ είτε $p \mid (\kappa - 1)$ είτε $p \mid (\kappa + 1)$. Αφού $1 \leq \kappa \leq p - 1$, η $p \mid (\kappa - 1)$ δίνει $\kappa = 1$ και η $p \mid (\kappa + 1)$ δίνει $\kappa = p - 1$. Επομένως

$$[1] \cdot [2] \cdot \cdots \cdot [p-1] = [1][p-1] = [-1] \Rightarrow (p-1)! \equiv -1 \bmod p.$$

Α 23. Έστω ότι $(G, \star)$ είναι μια ομάδα με τάξη $[G:1] = n \in \mathbb{N}$.

(α′) Αν H, K είναι δύο μη κενά υποσύνολα τής G, όχι απαραίτητα διαφορετικά, τότε να δειχθεί είτε ότι η G ισούται με το σύνολο $H \star K = \{h \star k \mid h \in H, k \in K\}$ είτε ότι $[G:1] \geq |H| + |K|$, όπου $|H|$, αντιστοίχως $|K|$, είναι το πλήθος των στοιχείων τού H, αντιστοίχως τού K.

(β′) Αν H είναι ένα μη κενό υποσύνολο τής G με $|H| > [G:1]/2$, τότε $G = H \star H$.

Λύση. (α′) Θα δείξουμε ότι όταν $[G:1] < |H| + |K|$, τότε $G = H \star K$. Για κάθε $g \in G$, σχηματίζουμε το σύνολο $\overline{K} = \{g \star k^{-1} \mid k \in K\}$. Η απεικόνιση $\varphi_g : K \to \overline{K}, k \mapsto g \star k^{-1}$ είναι αμφιρριπτική («1 − 1» και «επί»), (*γιατί;*). Ως εκ τούτου, $|\overline{K}| = |K|$ και αφού τώρα $[G:1] < |H| + |\overline{K}|$, συμπεραίνουμε ότι $H \bigcap \overline{K} \neq \emptyset$. Επομένως, υπάρχουν $h \in H, k \in K$ με $h = g \star k^{-1}$, δηλαδή $g = h \star k$.
(β′) Από $|H| > [G:1]/2$, έπεται $|H| + |H| > [G:1]$. Συνεπώς, το (α′), δίνει $G = H \star H$.

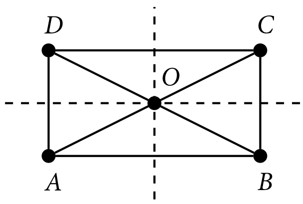
Α 24. Έστω $(\mathrm{Iso}(\mathbb{R}^2), \circ)$ η ομάδα των ισομετριών τού $\mathbb{R}^2$ και ότι Π είναι ένα ορθογώνιο παραλληλόγραμμο που δεν είναι όμως τετράγωνο. Να δειχθεί ότι το υποσύνολο $P_4 = \{\sigma \in \mathrm{Iso}(\mathbb{R}^2) \mid \sigma(\Pi) = \Pi\}$ με πράξη τη σύνθεση ισομετριών «$\circ$» σχηματίζει μια ομάδα. και να υπολογιστεί ο πίνακας τής πράξης «$\circ$».

Λύση. Παρατηρούμε ότι το σύνολο P_4 είναι $\neq \emptyset$, αφού το ταυτοτικό στοιχείο Id_2 τής $\mathrm{Iso}(\mathbb{R}^2)$ ανήκει στο P_4. Το P_4 είναι κλειστό ως προς τη σύνθεση «$\circ$», αφού όταν $\sigma, \tau \in P_4$, τότε $\sigma \circ \tau(\Pi) = \sigma(\tau(\Pi)) = \sigma(\Pi) = \Pi$. Επιπλέον, όταν η ισομετρία $\sigma \in P_4$, τότε και η αντίστροφη ισομετρία $\sigma^{-1} \in \mathrm{Iso}(\mathbb{R}^2)$ ανήκει επίσης στο P_4, διότι από $\sigma(\Pi) = \Pi$, έπεται $\Pi = \mathrm{Id}_2(\Pi) = \sigma^{-1}(\sigma(\Pi)) = \sigma^{-1}(\Pi)$. Άρα, το ζεύγος $(P_4, \circ)$ είναι ομάδα.

Θα προσδιορίσουμε το σύνολο των στοιχείων τού P_4 με τρόπο ανάλογο εκείνου με τον οποίο προσδιορίσαμε τα στοιχεία τής διεδρικής ομάδας D_n, βλ. Παράδειγμα 1.2.6(γ′).

Το ορθογώνιο παραλληλόγραμμο Π εγγράφεται σε μια περιφέρεια $\mathcal{C}$ κέντρου O. Έστω $\sigma \in P_4$. Επειδή το σ είναι ισομετρία, η εικόνα $\sigma(\mathcal{C})$ είναι επίσης μια περιφέρεια με κέντρο $\sigma(O)$. Η $\sigma(\mathcal{C})$ είναι η περιγεγραμμένη περιφέρεια τού $\sigma(\Pi)$. Αφού το $\sigma(\Pi) = \Pi$, συμπεραίνουμε ότι $\mathcal{C} = \sigma(\mathcal{C})$ και έτσι $\sigma(O) = O$. Το σύνολο $\{\sigma(A), \sigma(B), \sigma(C), \sigma(D)\}$ των κορυφών τού $\sigma(\Pi) = \Pi$, το οποίο είναι υποσύνολο τού $\sigma(\Pi) = \Pi$, συμπίπτει με το σύνολο $\{A, B, C, D\}$, αφού τα μόνα σημεία τού $\sigma(\Pi) = \Pi$ τα οποία κείνται πάνω στην περιφέρεια $\mathcal{C}$ είναι ακριβώς τα A, B, C, D, διότι το σ είναι μια ισομετρία με $\sigma(O) = O$. Από την Παρατήρηση (iii), βλ. σελ. 19, συμπεραίνουμε ότι η σ είναι ένας ορθογώνιος γραμμικός μετασχηματισμός. Υπενθυμίζουμε ότι οι ορθογώνιοι μετασχηματισμοί διατηρούν τις γωνίες μεταξύ διανυσμάτων[11].

[11]Γενικότερα, οποιαδήποτε ισομετρία διατηρεί τις γωνίες μεταξύ διανυσμάτων.



Θεωρούμε τη βάση τού $\mathbb{R}^2$ που αποτελείται από τα διανύσματα $\overrightarrow{OA}$ και $\overrightarrow{OD}$. Κάθε $\sigma \in P_4$ περιγράφεται πλήρως από τις τιμές $\sigma(\overrightarrow{OA})$ και $\sigma(\overrightarrow{OD})$. Έχοντας κατά νου ότι η γωνία μεταξύ των $\overrightarrow{OA}$ και $\overrightarrow{OD}$ οφείλει να ισούται με τη γωνία μεταξύ των $\sigma(\overrightarrow{OA})$ και $\sigma(\overrightarrow{OD})$ συμπεραίνουμε τα εξής:

Όταν $\sigma(\overrightarrow{OA}) = \overrightarrow{OA}$, τότε $\sigma(\overrightarrow{OD}) = \overrightarrow{OD}$ και γι' αυτό η ισομετρία σ ισούται με την ταυτοτική απεικόνιση Id_2.
Όταν $\sigma(\overrightarrow{OA}) = \overrightarrow{OD}$, τότε $\sigma(\overrightarrow{OD}) = \overrightarrow{OA}$ και γι' αυτό η ισομετρία σ ισούται με τον κατοπτρισμό, ας τον ονομάσουμε τ_1, ως προς τον άξονα που διέρχεται από τα μέσα των απέναντι πλευρών $\overline{A,D}$ και $\overline{B,C}$.
Όταν $\sigma(\overrightarrow{OA}) = \overrightarrow{OB}$, τότε $\sigma(\overrightarrow{OD}) = \overrightarrow{OC}$ και γι' αυτό η ισομετρία σ ισούται με τον κατοπτρισμό, ας τον ονομάσουμε τ_2, ως προς τον άξονα που διέρχεται από τα μέσα των απέναντι πλευρών $\overline{A,B}$ και $\overline{D,C}$.
Τέλος, όταν $\sigma(\overrightarrow{OA}) = \overrightarrow{OC}$, τότε $\sigma(\overrightarrow{OD}) = \overrightarrow{OB}$ και γι' αυτό η ισομετρία σ ισούται με την περιστροφή, ας την ονομάσουμε ρ, κατά γωνία π, γύρω από τον άξονα που είναι κάθετος στο επίπεδο τού Π και διέρχεται από το O.

Παρατηρούμε ότι $\tau_1^2 = \tau_2^2 = \mathrm{Id}_2$, αφού οι τ_1 και τ_2 είναι κατοπτρισμοί. Επίσης παρατηρούμε ότι $\rho^2 = \mathrm{Id}_2$, επειδή η ρ είναι περιστροφή κατά γωνία π.

Με τη βοήθεια των ανωτέρω μπορεί να σχηματίσει κανείς τον αριστερό από τους δύο επόμενους πίνακες. Τώρα επειδή το $(P_4, \circ)$ είναι ομάδα, ο αριστερός πίνακας συμπληρώνεται κατά μοναδικό τρόπο στον παρακάτω δεξιό πίνακα, αφού σε κάθε γραμμή και κάθε στήλη τού πίνακα πράξης τής $(P_4, \circ)$ πρέπει να εμφανίζεται κάθε στοιχείο τής ομάδας ακριβώς μία φορά, βλ. Πρόταση 1.2.19. Αυτός ακριβώς είναι ο πίνακας πράξης τής $(P_4, \circ)$.

$\circ$	Id_2	τ_1	τ_2	ρ
Id_2	Id_2	τ_1	τ_2	ρ
τ_1	τ_1	Id_2	$\star$	$\star$
τ_2	τ_2	$\star$	Id_2	$\star$
ρ	ρ	$\star$	$\star$	Id_2

,

$\circ$	Id_2	τ_1	τ_2	ρ
Id_2	Id_2	τ_1	τ_2	ρ
τ_1	τ_1	Id_2	ρ	τ_2
τ_2	τ_2	ρ	Id_2	τ_1
ρ	ρ	τ_2	τ_1	Id_2

Φυσικά, μπορεί να υπολογίσει κανείς και άμεσα τον παραπάνω πίνακα. Για παράδειγμα, $\tau_1 \circ \rho(\overrightarrow{OA}) = \tau_1(\overrightarrow{OC}) = \overrightarrow{OB}$. Τώρα επειδή οι γωνίες μεταξύ διανυσμάτων οφείλουν να διατηρούνται από την ισομετρία $\tau_1 \circ \rho$, συμπεραίνουμε ότι $\tau_1 \circ \rho(\overrightarrow{OD}) = \overrightarrow{OC}$. Επομένως, $\tau_1 \circ \rho = \tau_2$.

Α 25. Να περιγραφεί το σύνολο των στοιχείων τής διεδρικής ομάδας $(D_n, \circ)$ των συμμετριών τού κανονικού n-γώνου, $n \geq 3$.

Λύση. Γνωρίζουμε ότι $[D_n : 1]] = 2n$, βλ. την Πρόταση στη σελ. 18. Έστω ότι ρ είναι η στροφή κατά γωνία $2\pi/n$ γύρω από τον άξονα, ο οποίος είναι κάθετος στο επίπεδο τού κανονικού n-γώνου με φορά αυτήν που ακολουθούν κατά την κίνησή τους οι δείκτες τού ρολογιού και ότι τ είναι ένας οποιοσδήποτε κατοπτρισμός τού κανονικού n-γώνου. Υπενθυμίζουμε ότι $\tau^2 = \mathrm{Id}_n$ και ότι $\rho^n = \mathrm{Id}_n$. Τα $\rho^\kappa, 1 \leq \kappa \leq n-1$ είναι ανά δύο διαφορετικά, αφού αντιστοιχούν στις στροφές γύρω από τον κάθετο άξονα κατά γωνία $2\kappa\pi/n$. Ο κατοπτρισμός τ προφανώς δεν ισούται με κανένα από τα $\rho^\kappa, 1 \leq \kappa \leq n-1$. Τα $\tau \circ \rho^\kappa, 1 \leq \kappa \leq n-1$ είναι ανά δύο διαφορετικά, αφού από $\tau \circ \rho^\kappa = \tau \circ \rho^\lambda, 1 \leq \kappa, \lambda \leq n-1, \kappa \neq \lambda$, έπεται $\tau^{-1} \circ \tau \circ \rho^\kappa = \tau^{-1} \circ \tau \circ \rho^\lambda$ και επομένως $\rho^\kappa = \rho^\lambda$, το οποίο είναι άτοπο. Ο κατοπτρισμός τ δεν ισούται με κανένα από τα $\tau \circ \rho^\kappa, 1 \leq \kappa \leq n-1$. Αφού αν ήταν $\tau = \tau \circ \rho^\kappa$, τότε θα ήταν $\mathrm{Id}_n = \rho^\kappa$. Τέλος, επειδή τα $\tau \circ \rho^\kappa, 1 \leq \kappa \leq n-1$ είναι κατοπτρισμοί δεν συμπίπτουν με καμιά από τις περιστροφές $\rho^\kappa, 1 \leq \kappa \leq n-1$.

Το πλήθος τού συνόλου $\{\mathrm{Id}_n, \tau, \rho, \rho^2, \ldots, \rho^{n-1}, \tau \circ \rho, \tau \circ \rho^2, \ldots, \tau \circ \rho^{n-1}\}$ ισούται με $2n = [D_n : 1]$. Άρα τα στοιχεία τής D_n συμπίπτουν με τα στοιχεία τού προηγούμενου συνόλου.

Α 26. Να σχηματιστεί ο πίνακας πράξης τής διεδρικής ομάδας $(D_4, \circ)$.

Λύση. Η D_4 είναι η ομάδα ισομετριών τού τετραγώνου Έστω ότι ρ είναι η στροφή κατά γωνία $2\pi/4$ γύρω από τον άξονα, ο οποίος είναι κάθετος στο επίπεδο τού κανονικού τετραγώνου με φορά αυτήν που ακολουθούν κατά την κίνησή τους οι δείκτες τού ρολογιού και ότι τ είναι ένας οποιοσδήποτε κατοπτρισμός τού κανονικού τετραγώνου. Από την αμέσως προηγούμενη άσκηση γνωρίζουμε ότι

$$D_4 = \{\mathrm{Id}_4, \tau, \rho, \rho^2, \rho^3, \tau \circ \rho, \tau \circ \rho^2, \tau \circ \rho^3\}.$$

Επειδή γνωρίζουμε ότι $\tau^2 = \rho^4 = \mathrm{Id}_4$ μπορούμε να συμπληρώσουμε τον πίνακα πράξης τής $(D_4, \circ)$ ως εξής:

$\circ$	Id_4	τ	ρ	ρ^2	ρ^3	$\tau \circ \rho$	$\tau \circ \rho^2$	$\tau \circ \rho^3$
Id_4	Id_4	τ	ρ	ρ^2	ρ^3	$\tau \circ \rho$	$\tau \circ \rho^2$	$\tau \circ \rho^3$
τ	τ	Id_4	$\tau \circ \rho$	$\tau \circ \rho^2$	$\tau \circ \rho^3$	ρ	ρ^2	ρ^3
ρ	ρ	$\star$	ρ^2	ρ^3	Id_4	$\star$	$\star$	$\star$
ρ^2	ρ^2	$\star$	ρ^3	Id_4	ρ	$\star$	$\star$	$\star$
ρ^3	ρ^3	$\star$	Id_4	ρ	ρ^2	$\star$	$\star$	$\star$
$\tau \circ \rho$	$\tau \circ \rho$	$\star$	$\tau \circ \rho^2$	$\tau \circ \rho^3$	τ	$\star$	$\star$	$\star$
$\tau \circ \rho^2$	$\tau \circ \rho^2$	$\star$	$\tau \circ \rho^3$	τ	$\tau \circ \rho$	$\star$	$\star$	$\star$
$\tau \circ \rho^3$	$\tau \circ \rho^3$	$\star$	τ	$\tau \circ \rho$	$\tau \circ \rho^2$	$\star$	$\star$	$\star$

Επίσης επειδή γνωρίζουμε ότι $\tau \circ \rho = \rho^{-1} \circ \tau$ ή ισοδύναμα ότι $\rho \circ \tau = \tau \circ \rho^{-1} = \tau \circ \rho^3$, μπορούμε να συμπληρώσουμε και τις υπόλοιπες θέσεις τού πίνακα.

Για παράδειγμα, $\rho \circ \tau = \tau \circ \rho^3$, $(\rho \circ \tau) \circ \rho = (\tau \circ \rho^3) \circ \rho = \tau$, $(\rho \circ \tau) \circ \rho^2 = (\tau \circ \rho^3) \circ \rho^2 = \tau \circ \rho$, $(\rho \circ \tau) \circ \rho^3 = (\tau \circ \rho^3) \circ \rho^3 = \tau \circ \rho^2$.
Όμοια, $\rho^2 \circ \tau = \rho \circ (\rho \circ \tau) = \rho \circ (\tau \circ \rho^3) = (\rho \circ \tau) \circ \rho^3 = (\tau \circ \rho^3) \circ \rho^3 = \tau \circ \rho^2$, $\rho^2 \circ (\tau \circ \rho) = (\rho^2 \circ \tau) \circ \rho = (\tau \circ \rho^2) \circ \rho = \tau \circ \rho^3$, $\rho^2 \circ (\tau \circ \rho^2) = (\rho^2 \circ \tau \circ \rho) \circ \rho = (\tau \circ \rho^3) \circ \rho = \tau$, $\rho^2 \circ (\tau \circ \rho^3) = (\rho^2 \circ \tau \circ \rho^2) \circ \rho = \tau \circ \rho$.
Παρόμοια συμπληρώνονται και οι υπόλοιπες θέσεις τού πίνακα. Σημειώστε ότι οι εγγραφές τής τελευταίας στήλης τού πίνακα, αντίστοιχα τής τελευταίας γραμμής, δεν είναι απαραίτητο να υπολογιστούν, αφού σε αυτές τοποθετείται εκείνο το στοιχείο τής στήλης,

αντίστοιχα γραμμής, που δεν έχει εμφανιστεί μέχρι τώρα σε αυτήν τη στήλη, αντίστοιχα γραμμή, αφού γνωρίζουμε ότι η D_4 είναι ομάδα.

Κατ' αυτόν τον τρόπο προκύπτει ότι ο πίνακας τής πράξης τής $(D_4, \circ)$ είναι ο εξής:

$\circ$	Id_4	τ	ρ	ρ^2	ρ^3	$\tau\circ\rho$	$\tau\circ\rho^2$	$\tau\circ\rho^3$
Id_4	Id_4	τ	ρ	ρ^2	ρ^3	$\tau\circ\rho$	$\tau\circ\rho^2$	$\tau\circ\rho^3$
τ	τ	Id_4	$\tau\circ\rho$	$\tau\circ\rho^2$	$\tau\circ\rho^3$	ρ	ρ^2	ρ^3
ρ	ρ	$\tau\circ\rho^3$	ρ^2	ρ^3	Id_4	τ	$\tau\circ\rho$	$\tau\circ\rho^2$
ρ^2	ρ^2	$\tau\circ\rho^2$	ρ^3	Id_4	ρ	$\tau\circ\rho^3$	τ	$\tau\circ\rho$
ρ^3	ρ^3	$\tau\circ\rho$	Id_4	ρ	ρ^2	$\tau\circ\rho^2$	$\tau\circ\rho^3$	τ
$\tau\circ\rho$	$\tau\circ\rho$	ρ^3	$\tau\circ\rho^2$	$\tau\circ\rho^3$	τ	Id_4	ρ	ρ^2
$\tau\circ\rho^2$	$\tau\circ\rho^2$	ρ^2	$\tau\circ\rho^3$	τ	$\tau\circ\rho$	ρ^3	Id_4	ρ
$\tau\circ\rho^3$	$\tau\circ\rho^3$	ρ	τ	$\tau\circ\rho$	$\tau\circ\rho^2$	ρ^2	ρ^3	Id_4

Προτεινόμενες Ασκήσεις

ΠΑ 7. (α′) Έστω το σύνολο $\mathbb{Q}^+$ των θετικών ρητών αριθμών και «$\cdot$» η πράξη τού συνήθους πολλαπλασιασμού ρητών. Να δειχθεί ότι το ζεύγος $(\mathbb{Q}^+, \cdot)$ είναι μια αβελιανή ομάδα.

(β′) Έστω το σύνολο $\mathbb{Z}[x]$ των πολυωνύμων μιας μεταβλητής με ακέραιους συντελεστές και «$+$» η πράξη τής πρόσθεσης πολυωνύμων. Να δειχθεί ότι το ζεύγος $(\mathbb{Z}[x], +)$ είναι μια αβελιανή ομάδα.

(*Στην Άσκηση* Α82 *θα διαπιστώσουμε ότι αυτές οι τόσο διαφορετικές ομάδες είναι ισόμορφες!*)

ΠΑ 8. Να δειχθεί ότι η απεικόνιση (*με πράξεις στη δεξιά πλευρά των ισοτήτων τις συνήθεις πράξεις των πραγματικών αριθμών*)

$$\star : \mathbb{R} \setminus \{-1\} \times \mathbb{R} \setminus \{-1\} \to \mathbb{R} \setminus \{-1\}, (a, b) \mapsto a \star b := a + b + ab$$

ορίζει επί τού συνόλου $\mathbb{R} \setminus \{-1\}$ τη δομή μιας αβελιανής ομάδας και να λυθούν ως προς x οι ακόλουθες εξισώσεις:

(α′) $5 \star x = 2$,

(β′) $x \star 5 = 2$,

(γ′) $x \star 1 = 2$,

(δ′) $\sqrt{2} \star x = \sqrt{3}$,

(ε′) $2 \star x \star 3 = 7$.

ΠΑ 9. Να σχηματιστεί ο πίνακας πράξης τής ομάδας $(\mathbb{Z}_7, +)$.

ΠΑ 10. Στην ομάδα $(\mathbb{Z}_{101}, +)$ να επιλυθούν ως προς x οι ακόλουθες εξισώσεις: (i) $x + [-10] = [-20]$, (ii) $[5] + x = -[4]$, (iii) $[4012] + x + [1200] = [-2011]$.

ΠΑ 11. (α′) Να προσδιοριστούν όλα τα στοιχεία x τής $(\mathbb{Z}_{16}, +)$ με $x = -x$.

(β′) Να δειχθεί ότι η ομάδα $(\mathbb{Z}_{11}, +)$ δεν διαθέτει στοιχείο $x \neq [0]$ με $x = -x$.

ΠΑ 12. Θεωρούμε την ομάδα $(\mathbb{U}_{20}, \cdot)$ των αντιστρέψιμων κλάσεων ισοτιμίας των ακεραίων $\mathbb{Z}$ κατά μόδιο 20 με πράξη τον πολλαπλασιασμό των κλάσεων κατά μόδιο 20, βλ. Παράδειγμα 1.2.21.

(α′) Να δειχθεί ότι το σύνολο $\mathbb{U}_{20}$ ισούται με $\{[1], [3], [7], [9], [11], [13], [17], [19]\}$.

(β′) Να δειχθεί ότι για κάθε στοιχείο $u \in \mathbb{U}_{20}$ ισχύει $u^8 = [1]$.

(γ′) Να λυθεί ως προς x εξίσωση $[17]^{-108} \cdot x \cdot [7]^{333} = [3]^{-1}$.

ΠΑ 13. Να εξεταστεί ποια από τα επόμενα ζεύγη $(G, \star)$, όπου G σύνολο και «$\star$» πράξη επί τού G, αποτελούν ομάδα:

(α′) $G = \mathbb{Z}$, «$\star$» ο συνήθης πολλαπλασιασμός ακέραιων αριθμών,

(β′) $G = \mathbb{Q} \setminus \{0\}$, «$\star$» η συνήθης διαίρεση ρητών αριθμών,

(γ′) $G = \mathbb{R}^+ = \{r \in \mathbb{R} \mid r > 0\}$, «$\star$» ο συνήθης πολλαπλασιασμός πραγματικών αριθμών,

(δ′) $G = \{2^m \mid m \in \mathbb{Z}\}$, «$\star$» ο συνήθης πολλαπλασιασμός ακέραιων αριθμών.

ΠΑ 14. Θεωρούμε την ομάδα $(G, \cdot)$ τής A10.

(α′) Να προσδιοριστούν όλα τα στοιχεία $x \neq E$ με $x^2 = E$.

(β′) Να προσδιοριστούν όλα τα στοιχεία $x \neq E$ με $x^3 = E$.

(γ′) Να αποδείξετε ότι δεν υπάρχει στοιχείο $x \in G$, $x \neq E$ με $x^5 = E$.

(δ′) Να αποδείξετε ότι κάθε στοιχείο $x \in G$ ικανοποιεί την $x^6 = E$.

ΠΑ 15. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι $g \in G$ είναι ένα συγκεκριμένο στοιχείο της. Να δειχθεί ότι η αντιστοιχία

$$\circledast : G \times G \to G, (a, b) \mapsto a \star g \star b$$

ορίζει μια πράξη επί τού G και ότι το ζεύγος $(G, \circledast)$ είναι ομάδα.

ΠΑ 16. Έστω ότι $(G, \star)$ είναι μια ομάδα. Να δειχθεί ότι

$$\forall m \in \mathbb{N}, \forall a_1, a_2, \ldots, a_m \in G, (a_1 \star a_2 \star \cdots \star a_m)^{-1} = a_m^{-1} \star a_{m-1}^{-1} \star \cdots \star a_1^{-1}.$$

ΠΑ 17. Θεωρούμε την ομάδα $(\mathbb{R}^\star, \cdot)$ των μη μηδενικών πραγματικών αριθμών με πράξη τον συνήθη πολλαπλασιασμό και την ομάδα $(\mathbb{Z}, +)$ με πράξη τη συνήθη πρόσθεση. Να δειχθεί ότι το καρτεσιανό γινόμενο $\mathbb{R}^\star \times \mathbb{Z}$ εφοδιασμένο με την αντιστοιχία:

$$\circledast : (\mathbb{R}^\star \times \mathbb{Z}) \times (\mathbb{R}^\star \times \mathbb{Z}) \to \mathbb{R}^\star \times \mathbb{Z}, ((a, m), (b, n)) \mapsto (a \cdot b, m + n)$$

αποτελεί μια ομάδα.

ΠΑ 18. Έστω ότι $(G, \star)$ είναι μια αβελιανή (μεταθετική) ομάδα. Να δειχθεί ότι

$$\forall m, n \in \mathbb{N}, \forall a_1, a_2, \ldots, a_m \in G, (a_1 \star a_2 \star \cdots \star a_m)^n = a_1^n \star a_2^n \star \cdots \star a_m^n.$$

ΠΑ 19. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι a, b είναι δύο στοιχεία της. Αν $a^5 \star b^3 = b \star a$ και $a^4 = e_G$, $b^2 = e_G$, να δειχθεί ότι $a \star b = b \star a$.

ΠΑ 20. Να προσδιοριστεί η ομάδα των ισομετριών τού $\mathbb{R}^2$, οι οποίες απεικονίζουν έναν ρόμβο στον εαυτό του. Να σχηματίσετε τον πίνακα πράξης τής συγκεκριμένης ομάδας.

ΠΑ 21. Έστω ότι G είναι το καρτεσιανό γινόμενο $\mathbb{Z} \times \mathbb{Q}$. Να δειχθεί ότι η αντιστοιχία

$$((a, b), (c, d)) \mapsto (a + c, 2^c b + d)$$

ορίζει μια πράξη «$\star$» επί τού συνόλου G και ακολούθως να δειχθεί ότι το ζεύγος $(G, \star)$ απαρτίζει μια ομάδα. Να εξεταστεί, αν η $(G, \star)$ είναι αβελιανή (μεταθετική) ομάδα.

ΠΑ 22. Έστω $(G, \star)$ μια ομάδα. Να εξετάσετε αν ισχύει ή όχι καθένας από τους επόμενους ισχυρισμούς:

(α′) Αν a είναι ένα στοιχείο τής G με $a \star a = e_G$, τότε $a = e_G$.

(β′) Αν a, b είναι στοιχεία τής G με $a \star a = b \star b$, τότε $a = b$.

(γ′) $\forall a, b \in G$ είναι $(a \star b) \star (a \star b) = (a \star a) \star (b \star b)$.

(δ′) Αν a είναι ένα στοιχείο τής G με $a \star a = a$, τότε $a = e_G$.

(ε′) Για κάθε $a \in G$, υπάρχει κάποιο $b \in G$ με $a = b \star b$.

(στ′) Για οποιαδήποτε δύο στοιχεία $a, b \in G$, υπάρχει $c \in G$ με $b = a \star c$.

(*Υπόδειξη: Η Άσκηση* Α10 *είναι καλή πηγή αντιπαραδειγμάτων.*)

ΠΑ 23. Έστω ότι $\mathcal{A}$ είναι το σύνολο $\mathbb{R} \setminus \{0, 1\}$ και $\mathcal{F}$ το σύνολο των ακόλουθων απεικονίσεων από το $\mathcal{A}$ στο $\mathcal{A}$:

$$f_1 : \mathcal{A} \to \mathcal{A}, r \mapsto r \qquad f_2 : \mathcal{A} \to \mathcal{A}, r \mapsto \frac{1}{r} \qquad f_3 : \mathcal{A} \to \mathcal{A}, r \mapsto 1 - r$$
$$f_4 : \mathcal{A} \to \mathcal{A}, r \mapsto \frac{r}{r-1} \qquad f_5 : \mathcal{A} \to \mathcal{A}, r \mapsto \frac{r-1}{r} \qquad f_6 : \mathcal{A} \to \mathcal{A}, r \mapsto \frac{1}{1-r}.$$

Να δειχθεί ότι το σύνολο $\mathcal{F}$ με την πράξη τής σύνθεσης «$\circ$» των απεικονίσεων αποτελεί ομάδα και να εξεταστεί, αν η συγκεκριμένη ομάδα είναι αβελιανή (μεταθετική).

ΠΑ 24. Έστω ότι $\mathcal{F}(\mathbb{R})$ είναι το σύνολο των συναρτήσεων από το $\mathbb{R}$ στο $\mathbb{R}$.

(α′) Να δειχθεί ότι η αντιστοιχία:

$$(f, g) \mapsto f + g, \text{ όπου } \forall r \in \mathbb{R}, (f + g)(r) := f(r) + g(r)$$

ορίζει μια απεικόνιση

$$+ : \mathcal{F}(\mathbb{R}) \times \mathcal{F}(\mathbb{R}) \to \mathcal{F}(\mathbb{R}), (f, g) \mapsto f + g$$

και κατόπιν να δειχθεί ότι το ζεύγος $(\mathcal{F}(\mathbb{R}), +)$ αποτελεί μια αβελιανή ομάδα.

(β′) Να εξετάσετε, αν μπορείτε να επαναλάβετε τα ανωτέρω χρησιμοποιώντας τώρα την αντιστοιχία
$$(f,g) \mapsto f \cdot g, \text{ όπου } \forall r \in \mathbb{R}, (f \cdot g)(r) := f(r)g(r)$$

ΠΑ 25. Έστω G το σύνολο $\{\frac{1+2m}{1+2n} \mid m, n \in \mathbb{Z}\}$. Να δειχθεί ότι το G εφοδιασμένο με τον πολλαπλασιασμό των ρητών αριθμών αποτελεί μια αβελιανή ομάδα.

ΠΑ 26. Θεωρούμε τους ακόλουθους τέσσερεις 2×2 πίνακες με συνιστώσες από το σύνολο $\mathbb{C}$ των μιγαδικών αριθμών:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \text{ και } K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \text{ όπου } i^2 = -1$$

και κατόπιν το σύνολο

$$\mathcal{Q}_8 = \{E, I, J, K, -E, -I, -J, -K\}$$

που αποτελείται από τους προηγούμενους τέσσερεις πίνακες μαζί με τους αντίθετούς τους.

Να δείξετε

(α′) ότι το σύνολο $\mathcal{Q}_8$ είναι κλειστό ως προς τον συνήθη πολλαπλασιασμό «·» πινάκων σχηματίζοντας τον πίνακα τής πράξης «·» και κατόπιν

(β′) ότι το ζεύγος $(\mathcal{Q}_8, \cdot)$ αποτελεί μια μη αβελιανή (μη μεταθετική) ομάδα.

(γ′) Για κάθε στοιχείο x τής $\mathcal{Q}_8$, να προσδιορίσετε τον μικρότερο φυσικό $n(x)$ με την ιδιότητα $x^{n(x)} = E$ και κατόπιν να επιβεβαιώσετε ότι $\forall x \in \mathcal{Q}_8, x^8 = E$.

Συνήθως, η ομάδα $(\mathcal{Q}_8, \cdot)$ ονομάζεται *τετρανιακή ομάδα* ή *ομάδα των τετρανίων*.

ΠΑ 27. Ας είναι $\mathcal{H}$ το σύνολο των 3×3 πινάκων τής μορφής

$$\begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \gamma \\ 0 & 0 & 1 \end{pmatrix}, \alpha, \beta, \gamma \in \mathbb{R}.$$

Να δειχθεί ότι το ζεύγος $(\mathcal{H}, \cdot)$, όπου «·» είναι ο συνήθης πολλαπλασιασμός πινάκων, αποτελεί μια ομάδα.

Η συγκεκριμένη ομάδα καλείται *ομάδα Heisenberg* και έχει ιδιαίτερη σημασία στην Κβαντομηχανική.

ΠΑ 28. Έστω $(G, \star)$ μια ομάδα άρτιας τάξης. Να δειχθεί ότι υπάρχουν στοιχεία τής G, τα οποία δεν είναι τετράγωνα, δηλαδή ότι υπάρχουν $a \in G$ με $a \neq x^2, \forall x \in G$.

1.3 Υποομάδες

Ορισμός 1.3.1. Έστω ότι $(G, \star)$ είναι μια ομάδα. Ένα μη κενό υποσύνολο H τής G ονομάζεται *υποομάδα* τής G, όταν το ζεύγος $(H, \star)$ απαρτίζει ομάδα.

Παρατήρηση 1.3.2. Με άλλα λόγια, το $H \subseteq G$ είναι μια υποομάδα,

(α′) όταν το $H \neq \emptyset$,

(β′) όταν ο περιορισμός τής πράξης $\star : G \times G \to G$ στο υποσύνολο $H \times H \subseteq G \times G$ ορίζει μια πράξη επί τού H, δηλαδή μια απεικόνιση από το $H \times H$ στο H (συχνά η ιδιότητα αυτή δηλώνεται με την έκφραση «το H είναι κλειστό ως προς την πράξη τής G») και

(γ′) όταν το H μαζί με την πράξη «$\star$» σχηματίζουν μια ομάδα.

Λήμμα 1.3.3. *Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H είναι μια υποομάδα της.*

(α′) *Το ουδέτερο στοιχείο e_H τής H συμπίπτει με το ουδέτερο στοιχείο e_G τής G.*

(β′) *Για κάθε $a \in H$, το αντίστροφό του a_H^{-1} στην H συμπίπτει με το αντίστροφό του a^{-1} στην G.*

Απόδειξη. (α′) Παρατηρούμε ότι $e_H \star e_H = e_H$, επειδή το e_H είναι το ουδέτερο τής H και $e_H \star e_G = e_H$, επειδή το e_G είναι το ουδέτερο τής G. Επομένως, τα e_H και e_G είναι και τα δύο λύσεις τής εξίσωσης $e_H \star x = e_H$, ως προς x, στην ομάδα G. Αφού όμως η G είναι ομάδα, η προηγούμενη εξίσωση έχει, σύμφωνα με το Λήμμα 1.2.18, ακριβώς μία λύση. Επομένως, $e_H = e_G$.

(β′) Παρατηρούμε ότι $a \star a_H^{-1} = e_G$ και $a \star a^{-1} = e_G$. Συνεπώς, στην ομάδα G τα a_H^{-1} και a^{-1} είναι και τα δύο λύσεις τής εξίσωσης $a \star x = e_G$, ως προς x. Αφού όμως η G είναι ομάδα, η προηγούμενη εξίσωση έχει ακριβώς μία λύση, λόγω τού Λήμματος 1.2.18. Επομένως, $a_H^{-1} = a^{-1}$. □

Ορισμός 1.3.4. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H είναι μια υποομάδα της. Η υποομάδα H καλείται μια *γνήσια υποομάδα* τής G, όταν το H είναι γνήσιο υποσύνολο τής G, δηλαδή όταν $H \subseteq G$ και $H \neq G$.

Είναι φανερό ότι κάθε ομάδα $(G, \star)$ διαθέτει δύο υποομάδες, τις G και $\{e_G\}$. Οι υποομάδες αυτές ονομάζονται οι *τετριμμένες υποομάδες* τής G. Η G *δεν είναι ποτέ γνήσια υποομάδα* τού εαυτού της και η $\{e_G\}$ είναι γνήσια υποομάδα τής G, αν και μόνο αν, $\{e_G\} \subsetneq G$.

Παράδειγμα 1.3.5. (α′) Θεωρούμε την ομάδα $(\mathbb{Z}_{12}, +)$ των κλάσεων ισοτιμίας των ακεραίων $\mathbb{Z}$ κατά μόδιο 12, βλ. Παράδειγμα 1.2.4(γ′). Το υποσύνολο $H = \{[0], [4], [8]\}$ τής $\mathbb{Z}_{12}$ αποτελεί μια υποομάδα. Πρώτα παρατηρούμε ότι $H \neq \emptyset$. Ας θεωρήσουμε τώρα, τον πίνακα που προκύπτει από τον πίνακα πράξης τής $(\mathbb{Z}_{12}, +)$ περιορισμένο στα στοιχεία τής H:

$+$	$[0]$	$[4]$	$[8]$
$[0]$	$[0]$	$[4]$	$[8]$
$[4]$	$[4]$	$[8]$	$[0]$
$[8]$	$[8]$	$[0]$	$[4]$

Από τον ανωτέρω πίνακα διαπιστώνουμε ότι η πράξη τής $(\mathbb{Z}_{12},+)$, δηλαδή η πρόσθεση των ακεραίων κατά μόδιο 12, ορίζει μια πράξη επί τού H. Τέλος, σε κάθε γραμμή και κάθε στήλη τού πίνακα εμφανίζεται κάθε στοιχείο τής H ακριβώς μία φορά. Επειδή η πρόσθεση των ακεραίων κατά μόδιο 12 είναι προσεταιριστική πράξη και λόγω τής Πρότασης 1.2.19, έπεται ότι το ζεύγος $(H,+)$ απαρτίζει μια ομάδα και ως εκ τούτου είναι υποομάδα τής $(\mathbb{Z}_{12},+)$.

(β′) Θεωρούμε την ομάδα $(\mathbb{Z}_{18},+)$ των κλάσεων ισοτιμίας των ακεραίων $\mathbb{Z}$ κατά μόδιο 18, βλ. Παράδειγμα 1.2.4(γ′). Το υποσύνολο $H=\{[0],[5],[8]\}$ τής $\mathbb{Z}_{18}$ δεν αποτελεί μια υποομάδα, αφού το H δεν είναι κλειστό ως προς την πρόσθεση των ακεραίων κατά μόδιο 18. Για παράδειγμα, το άθροισμα $[5]+[8]=[13]$ των στοιχείων $[5]$ και $[8]$ τής H δεν είναι στοιχείο τής H.

(γ′) Θεωρούμε την ομάδα $(\mathbb{Z},+)$ των ακέραιων αριθμών, βλ. Παράδειγμα 1.2.4(α′), και ας είναι $k\in\mathbb{Z}$ ένας πάγιος ακέραιος αριθμός. Το σύνολο

$$k\mathbb{Z}=\{k\lambda \mid \lambda\in\mathbb{Z}\}$$

αποτελεί μια υποομάδα τής ομάδας $(\mathbb{Z},+)$.

Πράγματι, ο περιορισμός τής πράξης τής πρόσθεσης στο σύνολο $k\mathbb{Z}\times k\mathbb{Z}$ ορίζει μια απεικόνιση

$$k\mathbb{Z}\times k\mathbb{Z}\to k\mathbb{Z},\ (x,y)\mapsto x+y,$$

αφού, αν $x,y\in k\mathbb{Z}$, τότε $x=k\lambda$, $\lambda\in\mathbb{Z}$, $y=k\mu$, $\mu\in\mathbb{Z}$ και το στοιχείο $x+y$ ανήκει και πάλι στο $k\mathbb{Z}$, επειδή $x+y=k\lambda+k\mu=k(\lambda+\mu)$.

Η πράξη τής πρόσθεσης «$+$» ακέραιων αριθμών είναι προσεταιριστική στα στοιχεία τού $\mathbb{Z}$ και γι' αυτό είναι επίσης προσεταιριστική στα στοιχεία τού $k\mathbb{Z}$. Το ουδέτερο τής $(\mathbb{Z},+)$, δηλαδή το 0, ανήκει στο $k\mathbb{Z}$, αφού $0=k0$.

Τέλος, αν $x\in k\mathbb{Z}$, τότε ο αντίθετός του $-x=k(-\lambda)$ ανήκει επίσης στο $k\mathbb{Z}$.

Συνήθως, η υποομάδα $k\mathbb{Z}$ συμβολίζεται ως $\langle k\rangle$ και ονομάζεται η *κυκλική υποομάδα* τής $(\mathbb{Z},+)$ που *παράγεται* από το στοιχείο $k\in\mathbb{Z}$, βλ. Άσκηση Α30.

(δ′) Θεωρούμε την ομάδα $(\mathbb{R}^\star,\cdot)$ των μη μηδενικών πραγματικών αριθμών με πράξη τον πολλαπλασιασμό, βλ. Παράδειγμα 1.2.4(δ′), και το υποσύνολο $\mathbb{Q}^\star\subseteq\mathbb{R}^\star$ των μη μηδενικών ρητών αριθμών. Ήδη γνωρίζουμε ότι το $\mathbb{Q}^\star$ είναι μια ομάδα με πράξη τον περιορισμό τού πολλαπλασιασμού των πραγματικών $\cdot:\mathbb{R}\times\mathbb{R}\to\mathbb{R}$ στο σύνολο $\mathbb{Q}\times\mathbb{Q}$. Η $\mathbb{Q}^\star$ είναι υποομάδα τής $(\mathbb{R}^\star,\cdot)$.

(ε′) Θεωρούμε την ομάδα $(\mathcal{M}_{m\times n}(\mathbb{R}),+)$ των $m\times n$ πινάκων με συνιστώσες από τους πραγματικούς αριθμούς, βλ. Παράδειγμα 1.2.5(α′). Ας είναι H το ακόλουθο υποσύνολο τού $\mathcal{M}_{m\times n}(\mathbb{R})$:

$$H=\{(h_{ij})\in\mathcal{M}_{m\times n}(\mathbb{R}) \mid \forall i, 1\le i\le m, h_{i1}=0\}.$$

Δηλαδή, το H συνίσταται ακριβώς από εκείνους τους πίνακες των οποίων η πρώτη στήλη είναι μηδενική. Προφανώς, το $H\neq\emptyset$.

Το H αποτελεί μια υποομάδα τής $(\mathcal{M}_{m\times n}(\mathbb{R}), +)$. Πράγματι, το άθροισμα δύο πινάκων, που οι αντίστοιχες πρώτες στήλες τους είναι μηδενικές, ισούται με έναν πίνακα, τού οποίου η πρώτη στήλη είναι η μηδενική. Επομένως, ο περιορισμός τής πρόσθεσης πινάκων στο σύνολο $H \times H$ ορίζει μια απεικόνιση από το $H \times H$ στο H. Η πρόσθεση πινάκων είναι προσεταιριστική πράξη. Το ουδέτερο τής $(\mathcal{M}_{m\times n}(\mathbb{R}), +)$, δηλαδή ο μηδενικός $m \times n$ πίνακας, ανήκει στο H, επειδή κάθε στήλη του ισούται με τη μηδενική στήλη. Τέλος, ο αντίθετος $-(h_{ij}) = (-h_{ij})$ ενός πίνακα $(h_{ij}) \in H$ είναι και πάλι στοιχείο τής H, επειδή τα στοιχεία τής πρώτης στήλης τού $(-h_{ij})$ είναι όλα ίσα με το μηδέν, αφού $\forall i, 1 \leq i \leq m, h_{i1} = 0$.

(στ′) Θεωρούμε την ομάδα $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ των αντιστρέψιμων $n \times n$ πινάκων με συνιστώσες από τους πραγματικούς αριθμούς, όπου «$\cdot$» είναι η πράξη τού πολλαπλασιασμού πινάκων, βλ. Παράδειγμα 1.2.5(β′). Έστω $\mathrm{SL}_n(\mathbb{R})$ το υποσύνολο τού $\mathrm{GL}_n(\mathbb{R})$ που αποτελείται από τους πίνακες A με ορίζουσα $\det A = 1$. Το $\mathrm{SL}_n(\mathbb{R})$ αποτελεί μια υποομάδα τής $(\mathrm{GL}_n(\mathbb{R}), \cdot)$.

Πράγματι, ο ταυτοτικός πίνακας I_n έχει $\det I_n = 1$ και γι' αυτό το σύνολο $\mathrm{SL}_n(\mathbb{R})$ είναι $\neq \emptyset$. Το γινόμενο δύο πινάκων με ορίζουσα 1 είναι και πάλι ένας πίνακας με ορίζουσα 1, αφού γενικώς $\det(A \cdot B) = \det A \det B$. Επομένως, η πράξη τού πολλαπλασιασμού πινάκων περιορισμένη στο $\mathrm{SL}_n(\mathbb{R}) \times \mathrm{SL}_n(\mathbb{R})$ ορίζει μια απεικόνιση $\mathrm{SL}_n(\mathbb{R}) \times \mathrm{SL}_n(\mathbb{R}) \to \mathrm{SL}_n(\mathbb{R})$. Ο πολλαπλασιασμός πινάκων είναι προσεταιριστικός. Τέλος, όταν $A \in \mathrm{SL}_n(\mathbb{R})$, τότε και ο A^{-1} ανήκει στο $\mathrm{SL}_n(\mathbb{R})$, αφού $\det A^{-1} = \frac{1}{\det A} = \frac{1}{1} = 1$.

(ζ′) Έστω $(\mathrm{Iso}(\mathbb{R}^2), \circ)$ η ομάδα των ισομετριών τού επιπέδου, βλ. Παράδειγμα 1.2.6(β′). Η διεδρική ομάδα D_n, βλ. Παράδειγμα 1.2.6(γ′), καθώς επίσης και η ομάδα ισομετρίας ενός ορθογώνιου παραλληλογράμμου, βλ. Άσκηση Α24 αποτελούν υποομάδες τής $(\mathrm{Iso}(\mathbb{R}^2), \circ)$.

Τώρα θα παρουσιάσουμε ένα πολύ σημαντικό λήμμα με το οποίο διαπιστώνουμε πότε ένα μη κενό υποσύνολο μιας ομάδας είναι υποομάδα.

Λήμμα 1.3.6. *Έστω $(G, \star)$ μια ομάδα και H ένα υποσύνολό της. Το H αποτελεί μια υποομάδα τής $(G, \star)$, αν και μόνο αν, το H δεν είναι το κενό σύνολο και αν για κάθε $(a, b) \in H \times H$, το στοιχείο $a \star b^{-1}$ ανήκει επίσης στο H.*

Απόδειξη. «$\Rightarrow$» Έστω ότι το H είναι μια υποομάδα. Τότε, σύμφωνα με τον ορισμό τής υποομάδας, το H δεν είναι κενό. Επιπλέον, όταν το (a, b) είναι στοιχείο τού $H \times H$, τότε το b ανήκει στην H και επομένως το b^{-1} ανήκει επίσης στην H, βλ. Λήμμα 1.3.3(β′) και επειδή η H είναι υποομάδα, το $a \star b^{-1}$ είναι επίσης στοιχείο τής H.
«$\Leftarrow$» Υπάρχει κάποιο $a \in G$ με $a \in H$, αφού το $H \neq \emptyset$. Όμως τότε, το (a, a) είναι στοιχείο τού $H \times H$ και γι' αυτό, από την υπόθεση, το στοιχείο $a \star a^{-1} = e_G$ είναι στοιχείο τού H. Για κάθε $a \in H$, το στοιχείο (e_G, a) είναι στοιχείο τού $H \times H$ και γι' αυτό, σύμφωνα με την υπόθεση, το στοιχείο $e_G \star a^{-1} = a^{-1}$ είναι στοιχείο τού H.
Θα δείξουμε τώρα ότι ο περιορισμός τής «$\star$» στο $H \times H$ ορίζει μια απεικόνιση από το $H \times H$ στο H, δηλαδή ότι όταν το $(a, b) \in H \times H$, τότε και το $a \star b$ ανήκει στο H. Όταν

όμως το $(a,b) \in H \times H$, τότε το $b \in H$ και γι' αυτό όπως είδαμε προηγουμένως και το $b^{-1} \in H$. Συνεπώς, το ζεύγος (a, b^{-1}) ανήκει στο $H \times H$ και γι' αυτό εφαρμόζοντας και πάλι την υπόθεση, το στοιχείο $a \star (b^{-1})^{-1}$ ανήκει στο H. Σύμφωνα με το Λήμμα 1.2.17, το $(b^{-1})^{-1} = b$. Επομένως, το στοιχείο $a \star b$ είναι στοιχείο τού H.
Τέλος, επειδή η «$\star$» είναι μια προσεταιριστική πράξη επί των στοιχείων τής G, είναι φανερό ότι παραμένει προσεταιριστική επί των στοιχείων τού υποσυνόλου H. Επομένως, η H είναι μια υποομάδα τής G. $\square$

Παρατήρηση 1.3.7. Αν η $(G,+)$ είναι μια αβελιανή ομάδα, τότε χρησιμοποιώντας την προσθετική σημειογραφία, βλ. σελ. 11, η συνθήκη στο δεύτερο τμήμα τού προηγούμενου λήμματος γράφεται: «για κάθε ζεύγος $(a,b) \in H \times H$, το στοιχείο $a - b$ ανήκει επίσης στο H».

Συμβολισμός. Συχνά, δηλώνουμε ότι ένα υποσύνολο H μιας ομάδας $(G,\star)$ είναι υποομάδα της, γράφοντας $H \leq G$. Αν μάλιστα πρόκειται για γνήσια υποομάδα και θέλουμε αυτό να το τονίσουμε, τότε γράφουμε $H < G$.

Παρατήρηση 1.3.8. (α′) Είναι προφανές ότι αν $(G,\star)$ είναι μια ομάδα και αν H, K είναι υποσύνολα τού G με $H \leq G$ και $K \leq H$, τότε $K \leq G$.

(β′) Επίσης είναι προφανές ότι αν $(G,\star)$ είναι μια αβελιανή (μεταθετική) ομάδα και αν $H \leq G$, τότε η H είναι επίσης αβελιανή. Πράγματι, αν η H δεν είναι αβελιανή τότε υπάρχουν $a, b \in H \subseteq G$ με $a \star b \neq b \star a$. Πράγμα άτοπο, αφού η $(G,\star)$ είναι αβελιανή.

(γ′) Τονίζουμε για μια ακόμη φορά, ότι ένα μη κενό υποσύνολο $H \subseteq G$ μιας ομάδας $(G,\star)$ αποτελεί υποομάδα τής G, μόνο στην περίπτωση που είναι ομάδα ως προς την πράξη «$\star$» τής G. Ωστόσο, το ίδιο υποσύνολο H μπορεί να είναι ομάδα ως προς μια διαφορετική πράξη. Επί παραδείγματι, το σύνολο $\mathbb{R}^\star$ των μη μηδενικών πραγματικών αριθμών είναι υποσύνολο τού $\mathbb{R}$, δηλαδή $\mathbb{R}^\star \subset \mathbb{R}$. Ωστόσο, το $\mathbb{R}^\star$ δεν είναι υποομάδα τής $(\mathbb{R},+)$, αφού το $\mathbb{R}^\star$ δεν είναι κλειστό ως προς την πρόσθεση τού $\mathbb{R}$. (Για παράδειγμα, $5, -5 \in \mathbb{R}^\star$, αλλά $5 + (-5) = 0 \notin \mathbb{R}^\star$.). Εν τούτοις, το σύνολο $\mathbb{R}^\star$ αποτελεί ομάδα με πράξη τον πολλαπλασιασμό των πραγματικών αριθμών.

Ας δούμε πώς εφαρμόζεται το Λήμμα 1.3.6 σε ορισμένες απλές περιπτώσεις:

Παράδειγμα 1.3.9. (α′) Για τις ομάδες $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ και $(\mathbb{C},+)$, όπου «$+$» είναι η γνωστή μας πρόσθεση είναι, λόγω τού Λήμματος 1.3.6, $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$, αφού $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ και η διαφορά δύο ακεραίων (αντιστοίχως ρητών, αντιστοίχως πραγματικών) αριθμών είναι πάντοτε ένας ακέραιος (αντιστοίχως ρητός, αντιστοίχως πραγματικός) αριθμός.

(β′) Θεωρούμε την ομάδα $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ των αντιστρέψιμων $n \times n$ πινάκων με συνιστώσες από τους πραγματικούς αριθμούς, όπου «$\cdot$» είναι η πράξη τού πολλαπλασιασμού πινάκων, βλ. Παράδειγμα 1.2.5(β′), και έστω ότι

$$\mathcal{T} = \{T \in \mathrm{GL}_n(\mathbb{R}) \mid T \text{ διαγώνιος πίνακας } \}$$

Υπενθυμίζουμε ότι ένας $n \times n$ πίνακας $T = (t_{ij})$ είναι διαγώνιος, αν και μόνο αν, κάθε συνιστώσα του t_{ij} με $i \neq j$ είναι ίση με μηδέν και ότι ένας διαγώνιος πίνακας ανήκει στο $\mathcal{T}$, αν και μόνο αν, η ορίζουσά του $\det T = t_{11}t_{22}\ldots t_{nn}$ είναι διάφορη τού μηδενός.

Θα δείξουμε ότι $\mathcal{T} \leq \mathrm{GL}_n(\mathbb{R})$.

Προφανώς $\mathcal{T} \neq \emptyset$. Επιπλέον, αν $R = (r_{ij}) \in \mathcal{T}$, τότε και ο R^{-1} ανήκει στο $\mathcal{T}$, αφού είναι διαγώνιος με ορίζουσα $\det R^{-1}$ ίση με $r_{11}^{-1}r_{22}^{-1}\ldots r_{nn}^{-1} \neq 0$. Αν τώρα δύο πίνακες $T = (t_{ij})$ και $R = (r_{ij})$ ανήκουν στο $\mathcal{T}$, τότε και το γινόμενο $T \cdot R^{-1}$ ανήκει επίσης στο $\mathcal{T}$, αφού είναι διαγώνιος πίνακας με ορίζουσα $\det(T \cdot R^{-1})$ ίση με $t_{11}r_{11}^{-1}t_{22}r_{22}^{-1}\ldots t_{nn}r_{nn}^{-1} \neq 0$. Σύμφωνα με το Λήμμα 1.3.6, έχουμε $\mathcal{T} \leq \mathrm{GL}_n(\mathbb{R})$.

(γ′) Θεωρούμε τις ομάδες $(\mathrm{GL}_n(\mathbb{Q}), \cdot)$, $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ και $(\mathrm{GL}_n(\mathbb{C}), \cdot)$, βλ. Παράδειγμα 1.2.5. Επειδή $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, έχουμε $\mathrm{GL}_n(\mathbb{Q}) \subset \mathrm{GL}_n(\mathbb{R}) \subset \mathrm{GL}_n(\mathbb{C})$. Επιπλέον, αν $A, B \in \mathrm{GL}_n(\mathbb{Q})$ (αντιστοίχως $A, B \in \mathrm{GL}_n(\mathbb{R})$), τότε και $A \cdot B^{-1} \in \mathrm{GL}_n(\mathbb{Q})$ (αντιστοίχως $A \cdot B^{-1} \in \mathrm{GL}_n(\mathbb{R})$), αφού όταν $B \in \mathrm{GL}_n(\mathbb{Q})$ (αντιστοίχως $B \in \mathrm{GL}_n(\mathbb{R})$), τότε $B^{-1} \in \mathrm{GL}_n(\mathbb{Q})$ (αντιστοίχως $B^{-1} \in \mathrm{GL}_n(\mathbb{R})$). Επομένως,

$$\mathrm{GL}_n(\mathbb{Q}) < \mathrm{GL}_n(\mathbb{R}) < \mathrm{GL}_n(\mathbb{C}).$$

Θα δούμε τώρα ένα κριτήριο για το πότε ένα πεπερασμένο υποσύνολο μιας ομάδας είναι υποομάδα. Στις επόμενες ενότητες θα διαπραγματευθούμε σημαντικές ιδιότητες ομάδων που εξαρτώνται από το πλήθος των στοιχείων τους.

Λήμμα 1.3.10. *Έστω $(G, \star)$ μια ομάδα και H ένα μη κενό υποσύνολό της με πεπερασμένο το πλήθος στοιχεία. Αν το H είναι κλειστό ως προς την πράξη «$\star$» τής G, τότε είναι μια υποομάδα τής G.*

Απόδειξη. Επειδή το H είναι κλειστό ως προς την πράξη «$\star$» τής G, για να είναι το H υποομάδα τής G, αρκεί (σύμφωνα με την Παρατήρηση 1.3.2 και το Λήμμα 1.3.3) να ανήκει το e_G στο H και για κάθε $a \in H$, το a^{-1} να ανήκει επίσης στο H.

Αφού το H είναι πεπερασμένο σύνολο, μπορούμε να υποθέσουμε ότι $H = \{a_1, a_2, \ldots, a_n\}$ με $n \in \mathbb{N}$. Ας είναι $a \in H$. Θεωρούμε την απεικόνιση

$$\ell_a : H \to H, \;\; a_i \mapsto \ell_a(a_i) := a \star a_i.$$

Η ℓ_a είναι μια ενριπτική απεικόνιση, αφού αν a_i, a_j είναι στοιχεία τής H με $\ell_a(a_i) = \ell_a(a_j)$, τότε $a \star a_i = a \star a_j$ και επομένως[12] $a^{-1} \star (a \star a_i) = a^{-1} * (a \star a_j)$, δηλαδή $a_i = a_j$. Αλλά, όπως γνωρίζουμε, μια ενριπτική απεικόνιση από το πεπερασμένο σύνολο H στον εαυτό του είναι επίσης και επιρριπτική. Συνεπώς, υπάρχει κάποιο $a_j \in H$ με $a = \ell_a(a_j)$, δηλαδή $a = a \star a_j$. Συνεπώς, $a^{-1} \star a = a^{-1} \star a \star a_j$. Άρα, το ουδέτερο $e_G = a_j \in H$.

Επιπλέον, αφού η ℓ_a είναι επιρριπτική και επειδή τώρα γνωρίζουμε ότι $e_G \in H$, συμπεραίνουμε ότι υπάρχει $a_j \in H$ με $\ell_a(a_j) = e_G$, δηλαδή $a \star a_j = e_G$. Συνεπώς, $a_j = a^{-1}$ και έτσι το $a_j \in H$ είναι το αντίστροφο τού a. □

[12] Το αντίστροφο a^{-1} τού a υπάρχει στην G, αφού η G είναι ομάδα.

Παρατήρηση 1.3.11. Προσέξτε ότι είναι πολύ ουσιαστική η υπόθεση τού προηγούμενου λήμματος, που απαιτεί να είναι πεπερασμένο το υποσύνολο $H \subseteq G$.

Για παράδειγμα, θεωρούμε την ομάδα των ακέραιων αριθμών $(\mathbb{Z}, +)$ και το υποσύνολο $\mathbb{N} \subset \mathbb{Z}$ των φυσικών αριθμών. Το $\mathbb{N}$ είναι κλειστό ως προς την πρόσθεση των ακεραίων, αλλά δεν είναι υποομάδα τού $\mathbb{Z}$. Το προηγούμενο λήμμα δεν μπορεί να εφαρμοστεί, διότι το $\mathbb{N}$ είναι ένα άπειρο σύνολο.

Αντίθετα, αν θεωρήσουμε τη γενική γραμμική ομάδα $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ και το υποσύνολό της $G = \{E, A, B, D, E, F\}$ που απαρτίζεται από τους έξι 2×2 πίνακες τής Άσκησης A10, τότε παρατηρώντας τον πίνακα τής πράξης «·», βλ. Σχήμα 1.5, σελ. 38, διαπιστώνουμε ότι το G είναι κλειστό ως προς την πράξη «·» και γι' αυτό, σύμφωνα με το Λήμμα 1.3.10, το G απαρτίζει μια υποομάδα τής $\mathrm{GL}_2(\mathbb{R})$.

Ασκήσεις στις υποομάδες

Λυμένες Ασκήσεις

A 27. (α′) Έστω $\mathcal{E}$ το υποσύνολο των μιγαδικών αριθμών με μέτρο 1, δηλαδή $\mathcal{E} = \{z \in \mathbb{C} \mid |z| = 1\}$. Να δειχθεί ότι το $\mathcal{E}$ είναι υποομάδα τής ομάδας $(\mathbb{C}^\star, \cdot)$, βλ. Παράδειγμα 1.2.4(δ′).

(β′) Έστω $\mathcal{E}_\mathbb{N}$ το υποσύνολο των μιγαδικών αριθμών z με $z^n = 1$ για κάποιο $n \in \mathbb{N}$, δηλαδή $\mathcal{E}_\mathbb{N} = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N},\ \text{τέτοιο ώστε } z^n = 1\}$. Να δειχθεί ότι το $\mathcal{E}_\mathbb{N}$ είναι υποομάδα τής $(\mathcal{E}, \cdot)$.

(γ′) Έστω $\mathcal{E}_n$ το σύνολο των μιγαδικών αριθμών z με $z^n = 1$, για κάποιο πάγιο φυσικό αριθμό $n \in \mathbb{N}$, δηλαδή

$$\mathcal{E}_n = \{z \in \mathbb{C} \mid \text{ όπου } n \in \mathbb{N},\ \text{είναι ένας πάγιος αριθμός με } z^n = 1\}.$$

Να δειχθεί ότι το $\mathcal{E}_n$ είναι υποομάδα τής $(\mathcal{E}_\mathbb{N}, \cdot)$.
Η $(\mathcal{E}_n, \cdot)$ ονομάζεται η *ομάδα των n-οστών ριζών τής μονάδας*.

Λύση. Σε όλες τις περιπτώσεις μπορούμε να εφαρμόσουμε το Λήμμα 1.3.6.
(α′) Το $\mathcal{E}$ είναι διάφορο τού κενού, αφού το $1 \in \mathcal{E}$. Επιπλέον, αν $z, w \in \mathcal{E}$, τότε υπάρχει ο αντίστροφος $w^{-1} = \frac{1}{w}$ τού w, αφού $w \neq 0$ και μάλιστα $|w^{-1}| = \frac{1}{|w|} = 1$. Συνεπώς, το zw^{-1} ανήκει στο $\mathcal{E}$, αφού $|zw^{-1}| = |z||w^{-1}| = 1$ και επομένως $\mathcal{E} \leq \mathbb{C}$.
(β′) Το σύνολο $\mathcal{E}_\mathbb{N}$ είναι διάφορο τού κενού, αφού το $1 \in \mathcal{E}_\mathbb{N}$. Επιπλέον, $\mathcal{E}_\mathbb{N} \subseteq \mathcal{E}$, αφού αν $z \in \mathcal{E}_\mathbb{N}$, τότε $z^n = 1$, για κάποιο $n \in \mathbb{N}$ και γι' αυτό $|z^n| = |z|^n = 1$, που δίνει $|z| = 1$, επειδή $|z| \in \mathbb{R}$ και $|z| > 0$. Αν $w \in \mathcal{E}_\mathbb{N}$, τότε $w^n = 1$ για κάποιο $n \in \mathbb{N}$. Τώρα για τον αντίστροφο $w^{-1} = \frac{1}{w}$ τού w, ο οποίος υπάρχει αφού $w \neq 0$, είναι επίσης αληθές ότι $(w^{-1})^n = \frac{1}{w^n} = 1$. Αν λοιπόν $z, w \in \mathcal{E}_\mathbb{N}$, τότε υπάρχουν $m, n \in \mathbb{N}$ με $z^m = 1$, $(w^{-1})^n = 1$ και συνεπώς για το γινόμενο zw^{-1} είναι

$$\left(zw^{-1}\right)^{mn} = (z^m)^n((w^{-1})^n)^m = 1^n 1^m = 1.$$

Έτσι έπεται ότι το zw^{-1} ανήκει στο $\mathcal{E}_\mathbb{N}$ και ότι $\mathcal{E}_\mathbb{N} \leq \mathcal{E}$.

Το πλήθος των στοιχείων τής ομάδας $(\mathcal{E}_{\mathbb{N}}, \cdot)$ είναι άπειρο, αφού για οποιοδήποτε φυσικό αριθμό m, το σύνολο $\mathcal{E}_{\mathbb{N}}$ περιέχει τουλάχιστον $m+1$ στοιχεία. Πρόκειται για ακριβώς εκείνους τους $m+1$ το πλήθος μιγαδικούς αριθμούς, οι οποίοι είναι λύσεις τής εξίσωσης $x^{m+1} = 1$ στο $\mathbb{C}$.
(γ′) Προφανώς, $\mathcal{E}_n \subseteq \mathcal{E}_{\mathbb{N}}$. Μπορεί να εκτελεστεί μία απόδειξη η οποία να διαφέρει ελάχιστα από τις δύο προηγούμενες. Ωστόσο, επειδή το σύνολο $\mathcal{E}_n$ έχει n το πλήθος στοιχεία, αφού συμπίπτει με το σύνολο των λύσεων τής εξίσωσης $x^n = 1$ στο $\mathbb{C}$, ο ισχυρισμός μπορεί να προκύψει και με τη βοήθεια τού Λήμματος 1.3.10. Έτσι, για να είναι το σύνολο $\mathcal{E}_n \neq \emptyset$ υποομάδα τής $(\mathbb{C}^\star), \cdot$, αρκεί να είναι κλειστό ως προς τον πολλαπλασιασμό των μιγαδικών. Πράγματι, όταν $z, w \in \mathcal{E}_n$, τότε είναι:

$$(zw)^n = z^n w^n = 1.$$

Η $(\mathcal{E}_n, \cdot)$ ονομάζεται η *ομάδα των n–οστών ριζών τής μονάδας.*

Α 28. Έστω $(S_X, \circ)$ η συμμετρική ομάδα ενός συνόλου X, βλ. Παράδειγμα 1.2.24(α′), με πλήθος στοιχείων ≥ 2 και ω ένα στοιχείο τού X. Να δειχθεί ότι το υποσύνολο

$$S_X^\omega = \{\sigma \in S_X \mid \sigma(\omega) = \omega\}$$

αποτελεί μια υποομάδα τής S_X.

Λύση. Το S_X^ω είναι $\neq \emptyset$, αφού η ταυτοτική απεικόνιση Id_X ανήκει στο S_X^ω. Το S_X^ω είναι κλειστό ως προς την πράξη «$\circ$», αφού $\forall \sigma, \tau \in S_X^\omega$ είναι $\sigma \circ \tau(\omega) = \sigma(\tau(\omega)) = \sigma(\omega) = \omega$. Τέλος, όταν ένα στοιχείο σ ανήκει στο S_X^ω, τότε και η αντίστροφη απεικόνιση σ^{-1} ανήκει στο S_X^ω, αφού από $\sigma(\omega) = \omega$, έπεται $\omega = \mathrm{Id}_X(\omega) = \sigma^{-1}(\sigma(\omega)) = \sigma^{-1}(\omega)$.

Α 29. Έστω ότι $(G_1, \star_1), (G_2, \star_2)$ είναι δύο ομάδες και $(G_1 \times G_2, \star)$ το ευθύ γινόμενό τους, βλ. Άσκηση Α18. Αν η H_1 (αντιστοίχως η H_2) είναι υποομάδα τής $(G_1, \star_1)$ (αντιστοίχως τής $(G_2, \star_2)$), τότε να δειχθεί ότι το καρτεσιανό γινόμενο $H_1 \times H_2$ είναι υποομάδα τής $(G_1 \times G_2, \star)$.

Λύση. Το υποσύνολο $H_1 \times H_2$ είναι $\neq \emptyset$, αφού $H_1 \neq \emptyset$ και $H_2 \neq \emptyset$.
Για κάθε $(h_1, h_2), (k_1, k_2) \in H_1 \times H_2$, το $h_1 \star_1 k_1^{-1}$ ανήκει στην H_1, αφού η H_1 είναι υποομάδα τής G_1 και όμοια το $h_2 \star_2 k_2^{-1}$ ανήκει στην H_2. Επομένως, το στοιχείο

$$(h_1, h_2) \star (k_1, k_2)^{-1} = (h_1, h_2) \star (k_1^{-1}, k_2^{-1}) = (h_1 \star_1 k_1^{-1}, h_2 \star_2 k_2^{-1})$$

ανήκει στο $H_1 \times H_2$. Σύμφωνα με Λήμμα 1.3.6, το $H_1 \times H_2$ είναι μια υποομάδα τού ευθέως γινομένου $G_1 \times G_2$.

Α 30. Έστω ότι $(G, \star)$ είναι μια ομάδα.

(α′) Αν $\{H_i \mid i \in I\}$ είναι ένα μη κενό υποσύνολο υποομάδων τής G, τότε να δειχθεί ότι η τομή $\bigcap_{i \in I} H_i$ είναι μια υποομάδα τής $(G, \star)$.

(β′) Αν M είναι ένα υποσύνολο τής G, τότε να δειχθεί ότι η τομή όλων των υποομάδων H τής G που περιέχουν το M, δηλαδή το σύνολο

$$\bigcap \{H \mid H \leq G \text{ και } M \subseteq H\}, \tag{*}$$

είναι επίσης μια υποομάδα τής G. Να δειχθεί κατόπιν ότι πρόκειται για τη μικρότερη υποομάδα, ως προς τη σχέση τού υποσυνόλου «$\subseteq$», που περιέχει το σύνολο M.

(Η συγκεκριμένη υποομάδα ονομάζεται η *υποομάδα τής* $(G, \star)$ *που παράγεται από το σύνολο* M και συμβολίζεται με $\langle M \rangle$. Το σύνολο M καλείται ένα *σύνολο γεννητόρων* τής $\langle M \rangle$. Όταν το M είναι ένα μονοσύνολο τής G, ας πούμε $M = \{a\}$, τότε η $\langle M \rangle$ ονομάζεται η *κυκλική υποομάδα* που παράγεται από το στοιχείο a και συνήθως συμβολίζεται με $\langle a \rangle$. Όταν το M είναι ένα πεπερασμένο σύνολο, τότε η υποομάδα $\langle M \rangle$ ονομάζεται *πεπερασμένως παραγόμενη*. Η $(G, \star)$ ονομάζεται *πεπερασμένως παραγόμενη*, όταν υπάρχει ένα πεπερασμένο υποσύνολο $M \subseteq G$ με $\langle M \rangle = G$.)

(γ′) Αν M είναι ένα μη κενό υποσύνολο τής G, τότε να δειχθεί ότι

(i) το υποσύνολο

$$\mathcal{H} = \left\{ m_{i_1}^{\varepsilon_1} \star m_{i_2}^{\varepsilon_2} \star \cdots \star m_{i_s}^{\varepsilon_s} \mid m_{i_j} \in M, \varepsilon_j \in \{1, -1\}, \forall j, 1 \leq j \leq s \right\}$$

τής G, (όπου τα m_{i_j} δεν είναι απαραιτήτως διαφορετικά μεταξύ τους) αποτελεί μια υποομάδα τής G και ότι

(ii) η $\mathcal{H}$ συμπίπτει με την υποομάδα $\langle M \rangle$ που παράγεται από το σύνολο M. (Συνεπώς, όταν το σύνολο γεννητόρων M είναι ίσο με ένα μονοσύνολο $\{a\}$, τότε η κυκλική υποομάδα $\langle a \rangle$ είναι η μικρότερη υποομάδα τής G που περιέχει το a και από το (i) προκύπτει αμέσως ότι $\langle a \rangle = \{a^z \mid z \in \mathbb{Z}\}$.)

Λύση. (α′) Για την απόδειξη θα χρησιμοποιήσουμε το Λήμμα 1.3.6. Παρατηρούμε ότι $\bigcap_{i \in I} H_i \neq \emptyset$, αφού $\forall i \in I, e_G \in H_i$. Αν $a, b \in \bigcap_{i \in I} H_i$, τότε $\forall i \in I, a, b \in H_i$ και επειδή $\forall i \in I$, η H_i είναι υποομάδα τής $(G, \star)$, έπεται ότι $\forall i \in I$, το $a \star b^{-1}$ ανήκει στην H_i και γι’ αυτό $a \star b^{-1} \in \bigcap_{i \in I} H_i$. Επομένως, $\bigcap_{i \in I} H_i \leq G$.

(β′) Έστω $\mathcal{L} = \{H \mid H \leq G \text{ και } M \subseteq H\}$ το σύνολο των υποομάδων τής $(G, \star)$ που περιέχουν το M. Η ομάδα G ανήκει στο $\mathcal{L}$, αφού η G είναι υποομάδα τού εαυτού της και περιέχει το M. Συνεπώς, το $\mathcal{L}$ δεν είναι το κενό σύνολο και σύμφωνα με το μέρος (α′) τής άσκησης, η τομή $\bigcap_{H \in \mathcal{L}} H$ είναι μια υποομάδα τής $(G, \star)$. Προφανώς, $M \subseteq \bigcap_{H \in \mathcal{L}} H$, αφού για κάθε $H \in \mathcal{L}$, είναι $M \subseteq H$. Αν τώρα H είναι μια υποομάδα με $M \subseteq H$, τότε η H ανήκει στο $\mathcal{L}$, και επειδή η H συμμετέχει στην τομή, έπεται $\bigcap_{H \in \mathcal{L}} H \subseteq H$. Έτσι συμπεραίνουμε ότι η $\bigcap_{H \in \mathcal{L}} H$ είναι η μικρότερη υποομάδα τής $(G, \star)$ που περιέχει το M.

(γ′)(i) Για την απόδειξη θα χρησιμοποιήσουμε και πάλι το Λήμμα 1.3.6. Επειδή $M \subseteq \mathcal{H}$, είναι φανερό ότι $\mathcal{H} \neq \emptyset$.

Όταν τα $\alpha, \beta \in \mathcal{H}$, τότε υπάρχουν στοιχεία $m_{i_1}, m_{i_2}, \ldots, m_{i_s}, r_{\ell_1}, r_{\ell_2}, \ldots, r_{\ell_t} \in M$ με $\alpha = m_{i_1}^{\varepsilon_1} \star m_{i_2}^{\varepsilon_2} \star \cdots \star m_{i_s}^{\varepsilon_s}$ και $\beta = r_{\ell_1}^{\zeta_1} \star r_{\ell_2}^{\zeta_2} \star \cdots \star r_{\ell_t}^{\zeta_t}$, όπου τα $\varepsilon_j, \zeta_k \in \{1, -1\}, \forall j, k, 1 \leq j \leq s, 1 \leq k \leq t$. Τότε όμως και το στοιχείο $\alpha \star \beta^{-1}$ ανήκει επίσης στο $\mathcal{H}$, αφού έχει τη μορφή

$$a \star \beta^{-1} = m_{i_1}^{\varepsilon_1} \star m_{i_2}^{\varepsilon_2} \star \cdots \star m_{i_s}^{\varepsilon_s} \star r_{\ell_t}^{-\zeta_t} \star r_{\ell_{t-1}}^{-\zeta_{t-1}} \star \cdots \star r_{\ell_1}^{-\zeta_1}$$

και αφού τα $-\zeta_t, -\zeta_{t-1}, \ldots, -\zeta_1$ ανήκουν επίσης στο σύνολο $\{1, -1\}$. Συνεπώς, το $\mathcal{H}$ αποτελεί μια υποομάδα τής G.
(γ′)(ii) Τέλος, η $\mathcal{H}$ είναι η μικρότερη υποομάδα τής G που περιέχει το σύνολο M, αφού κάθε υποομάδα που περιέχει τα $m \in M$, οφείλει να περιέχει και τα αντίστροφά τους m^{-1}, καθώς και όλα τα πεπερασμένα γινόμενα που έχουν ως παράγοντες είτε τα στοιχεία τού M είτε τα αντίστροφά τους. Αλλά το σύνολο αυτών των πεπερασμένων γινομένων είναι ακριβώς το $\mathcal{H}$. Όμως στο (β′) τής παρούσας άσκησης είδαμε ότι η μικρότερη υποομάδα που περιέχει το M είναι η $\langle M \rangle$. Επομένως, $\mathcal{H} = \langle M \rangle$.

Α 31. Έστω ότι η $(G, \star)$ είναι μια πεπερασμένως παραγόμενη ομάδα και ότι M είναι ένα σύνολο γεννητόρων της. Να δειχθεί ότι υπάρχει ένα πεπερασμένο υποσύνολο $N \subseteq M$ με $\langle N \rangle = G$.

Λύση. Αφού η G είναι πεπερασμένως παραγόμενη, υπάρχει ένα πεπερασμένο υποσύνολο $L = \{\ell_1, \ell_2, \ldots, \ell_t\} \subseteq G$ με $\langle L \rangle = G$. Επειδή το $\langle M \rangle = G$, συμπεραίνουμε ότι για κάθε $j, 1 \leq j \leq t$ το $\ell_j = m_{j,i_1}^{\varepsilon_{j,1}} \star m_{j,i_2}^{\varepsilon_{j,2}} \star \cdots \star m_{j,i_{s_j}}^{\varepsilon_{j,s_j}}$, όπου τα $s_j, i_{s_j} \in \mathbb{N}$, τα m_{j,i_1}, m_{j,i_2}, $\ldots, m_{j,i_{s_j}} \in M$ και τα $\varepsilon_{j,1}, \varepsilon_{j,2}, \ldots, \varepsilon_{j,s_j} \in \{1, -1\}$. Θεωρούμε το πεπερασμένο υποσύνολο $N = \{m_{j,i_1}, m_{j,i_2}, \ldots, m_{j,i_{s_j}} \mid 1 \leq j \leq t\}$. Αφού το $L \subseteq \langle N \rangle$, συμπεραίνουμε ότι και η $\langle L \rangle \leq \langle N \rangle$. Αλλά, $\langle L \rangle = G$ και $\langle N \rangle \leq G$ και έτσι $G = \langle N \rangle$.

Α 32. Έστω η ομάδα των ακεραίων $(\mathbb{Z}, +)$ και $\mathcal{P}$ το σύνολο των πρώτων αριθμών. Για κάθε $p \in \mathcal{P}$, θεωρούμε την κυκλική υποομάδα $\langle p \rangle = p\mathbb{Z} = \{kp \mid k \in \mathbb{Z}\}$ τής $\mathbb{Z}$, βλ. Παράδειγμα 1.3.5(γ′), Να δειχθεί ότι $\bigcap\limits_{p \in \mathcal{P}} p\mathbb{Z} = \{0\}$.

Λύση. Αφού η $\bigcap\limits_{p \in \mathcal{P}} p\mathbb{Z}$ είναι υποομάδα τής $\mathbb{Z}$, έχουμε $\{0\} \leq \bigcap\limits_{p \in \mathcal{P}} p\mathbb{Z}$. Θα δείξουμε ότι δεν υπάρχει μη μηδενικός ακέραιος z με $z \in \bigcap\limits_{p \in \mathcal{P}} p\mathbb{Z}$, από όπου θα προκύψει ότι $\bigcap\limits_{p \in \mathcal{P}} p\mathbb{Z} \leq \{0\}$ και συνεπώς η επιθυμητή ισότητα $\bigcap\limits_{p \in \mathcal{P}} p\mathbb{Z} = \{0\}$.

Πράγματι, αν υπήρχε κάποιος $z \in \mathbb{Z}, z \neq 0$ με $z \in \bigcap\limits_{p \in \mathcal{P}} p\mathbb{Z}$, τότε και ο θετικός ακέραιος $|z|$ θα ανήκε επίσης στην $\bigcap\limits_{p \in \mathcal{P}} p\mathbb{Z}$, αφού, σύμφωνα με την προηγούμενη άσκηση, η $\bigcap\limits_{p \in \mathcal{P}} p\mathbb{Z}$ είναι υποομάδα τής $\mathbb{Z}$. Τότε όμως ο $|z|$ ανήκει σε κάθε υποομάδα $p\mathbb{Z}$, όπου p πρώτος αριθμός. Συνεπώς, κάθε πρώτος p διαιρεί τον θετικό ακέραιο $|z|$. Αυτό όμως είναι άτοπο, αφού το πλήθος των πρώτων διαιρετών ενός θετικού ακέραιου είναι πάντοτε πεπερασμένο.

Α 33. Έστω $(G, \star)$ μια ομάδα. Να δειχθεί ότι η υποομάδα τής G που παράγεται από το κενό υποσύνολο $\emptyset$ τής G ισούται με την τετριμμένη υποομάδα $\{e_G\}$ τής G.

Λύση. Για οποιαδήποτε υποομάδα H τής G, έχουμε $\emptyset \subset H$. Γι' αυτό κάθε υποομάδα H τής G συμμετέχει στην τομή που χορηγεί την $\langle \emptyset \rangle$. Επομένως,

$$\langle \emptyset \rangle = \bigcap_{\forall H, H \leq G} H\ .$$

Μεταξύ των υποομάδων τής G που συμμετέχουν στην τομή είναι και η τετριμμένη υποομάδα $\{e_G\}$. Γι' αυτό $\langle\emptyset\rangle \subseteq \{e_G\}$ (*). Αλλά η $\{e_G\}$ περιέχεται σε κάθε υποομάδα τής G, αφού το ουδέτερο στοιχείο e_G ανήκει σε κάθε υποομάδα τής G. Επειδή η $\langle\emptyset\rangle$ είναι υποομάδα τής G, έπεται $\{e_G\} \leq \langle\emptyset\rangle$ (**). Τα (*) και (**) χορηγούν $\{e_G\} = \langle\emptyset\rangle$.

Α 34. Έστω $(\mathbb{Z}, +)$ η ομάδα των ακέραιων αριθμών και $m, n \in \mathbb{N}$ δύο σχετικώς πρώτοι αριθμοί. Να δειχθεί ότι η υποομάδα των ακεραίων που παράγεται από το σύνολο $M = \{m, n\}$ ισούται με $\mathbb{Z}$.

Λύση. Σύμφωνα με τον ορισμό:

$$\langle\{m, n\}\rangle = \bigcap_{\{m,n\}\subseteq H, H\leq G} H.$$

Στη συγκεκριμένη άσκηση θα δείξουμε ότι κάθε υποομάδα $H \leq \mathbb{Z}$ που περιέχει τους σχετικώς πρώτους αριθμούς m, n ισούται με την ομάδα $\mathbb{Z}$ και γι' αυτό $\langle\{m, n\}\rangle = \mathbb{Z}$. (Σύντομα θα δούμε ότι για δύο οποιουσδήποτε φυσικούς αριθμούς m, n, η υποομάδα $\langle\{m, n\}\rangle$ ισούται με την κυκλική υποομάδα $\langle\delta\rangle$ τής $\mathbb{Z}$, όπου δ είναι ο μέγιστος κοινός διαιρέτης των m και n.)

Ας υποθέσουμε λοιπόν, ότι η H είναι μια υποομάδα τής $\mathbb{Z}$ με $\{m, n\} \subseteq H$. Τότε όμως και κάθε ακέραιο πολλαπλάσιο λm, $\lambda \in \mathbb{Z}$ τού m καθώς και κάθε ακέραιο πολλαπλάσιο κn, $\kappa \in \mathbb{Z}$ τού n είναι επίσης στοιχείο τής H, αφού η H είναι μια υποομάδα. Για τον ίδιο ακριβώς λόγο και κάθε ακέραιος τής μορφής $\lambda m + \kappa n$, $\lambda, \kappa \in \mathbb{Z}$ ανήκει και αυτός στην υποομάδα H.
Γενικώς είναι γνωστό, ότι αν δ είναι ο μέγιστος κοινός διαιρέτης δύο οποιωνδήποτε φυσικών αριθμών s, t, τότε υπάρχουν ακέραιοι α, β με $\delta = \alpha s + \beta t$. Στην περίπτωσή μας οι m, n είναι σχετικώς πρώτοι, επομένως $1 = \alpha m + \beta n$, για κάποιους ακέραιους αριθμούς α, β και γι' αυτό ο αριθμός 1 ανήκει στην H. Όμως τότε και κάθε $z \in \mathbb{Z}$ ανήκει στην H, αφού ο $z = z \cdot 1$ είναι ακέραιο πολλαπλάσιο τού 1 και η H είναι υποομάδα. Επομένως, $H = \mathbb{Z}$ και $\langle\{m, n\}\rangle = \mathbb{Z}$.

Α 35. Να δειχθεί με τη βοήθεια ενός παραδείγματος ότι η ένωση $H \bigcup K$ δύο υποομάδων H και K μιας ομάδας $(G, \star)$ δεν αποτελεί πάντοτε υποομάδα τής G.

Λύση. Έστω $(\mathbb{Z}, +)$ η ομάδα των ακέραιων αριθμών με πράξη τη συνήθη πρόσθεση και $H = 2\mathbb{Z}$, αντιστοίχως $K = 3\mathbb{Z}$, οι κυκλικές υποομάδες τής $(\mathbb{Z}, +)$. Αν η ένωση $H \bigcup K = 2\mathbb{Z} \bigcup 3\mathbb{Z}$ ήταν μια υποομάδα, τότε σύμφωνα με το Λήμμα 1.3.6, το στοιχείο $3 - 2 = 1$ θα έπρεπε να ανήκει στην ένωση $H \bigcup K$, αφού τα 3 και 2 είναι στοιχεία τού συνόλου $H \bigcup K$. Με άλλα λόγια, θα έπρεπε το 1 να ανήκει στην $H \bigcup K$. Αυτό όμως είναι άτοπο, επειδή το 1 δεν είναι ούτε πολλαπλάσιο τού 2, άρα $1 \notin H$, ούτε πολλαπλάσιο τού 3, άρα $1 \notin K$. Επομένως, η $H \bigcup K$ δεν είναι υποομάδα τής $(\mathbb{Z}, +)$.

Α 36. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H, K είναι δύο υποομάδες της. Να δειχθεί ότι η ένωση $H \bigcup K$ είναι μια υποομάδα τής $(G, \star)$, αν και μόνο αν, είτε $H \subseteq K$ είτε $K \subseteq H$.

Λύση. «$\Leftarrow$» Αν $H \subseteq K$, τότε $H \bigcup K = K$ και επομένως η $H \bigcup K$ είναι υποομάδα τής $(G, \star)$. Η επιχειρηματολογία είναι πανομοιότυπη, όταν $K \subseteq H$.

«$\Rightarrow$» Έστω ότι η ένωση $H\bigcup K$ είναι υποομάδα τής $(G,\star)$ και ότι $H \nsubseteq K$. Θα δείξουμε ότι $K \subseteq H$. Επειδή $H \nsubseteq K$, υπάρχει κάποιο συγκεκριμένο $h \in H$ με $h \notin K$. Ας είναι k ένα οποιοδήποτε στοιχείο τής K. Επειδή η $H\bigcup K$ είναι υποομάδα τής $(G,\star)$, το στοιχείο $h\star k$ ανήκει στην $H\bigcup K$. Αλλά το $h\star k$ δεν μπορεί να ανήκει στο K, αφού αν $h\star k = k' \in K$, τότε $h = k'\star k^{-1} \in K$, που είναι αδύνατο, αφού $h \notin K$. Επομένως, το $h\star k$ είναι στοιχείο τής H, δηλαδή $h\star k = h' \in H$ και έτσι το $k = h'\star h^{-1}$ είναι στοιχείο τής H. Συνεπώς, $K \subseteq H$.

Α 37. Έστω ότι $(G,\star)$ είναι μια ομάδα και ότι H, K είναι δύο υποομάδες της. Να δειχθεί ότι το σύνολο

$$H\star K = \{h\star k \mid h \in H, k \in K\}$$

είναι μια υποομάδα τής $(G,\star)$, αν και μόνο αν, $H\star K = K\star H$.

Λύση. «$\Rightarrow$» Έστω ότι $H\star K \leq G$.

Θα αποδείξουμε πρώτα ότι $K\star H \subseteq H\star K$. Για κάθε $k\in K$ και $h\in H$, έχουμε $k\star h = (e_G\star k)\star(h\star e_G)$. Τα στοιχεία $e_G\star k$ και $h\star e_G$ ανήκουν στην υποομάδα $H\star K$, αφού το ουδέτερο στοιχείο e_G τής G ανήκει και στην H και στην K. Γι' αυτό το γινόμενό τους $(e_G\star k)\star(h\star e_G)$, ανήκει επίσης στην $H\star K$, δηλαδή υπάρχουν $h' \in H$ και $k' \in K$ με $(e_G\star k)\star(h\star e_G) = h'\star k'$. Επομένως, $k\star h = h'\star k' \in H\star K$. Συνεπώς, $K\star H \subseteq H\star K$.

Θα αποδείξουμε τώρα ότι $H\star K \subseteq K\star H$. Για κάθε $h \in H$ και κάθε $k \in K$, έχουμε $h\star k = [(h\star k)^{-1}]^{-1} = (k^{-1}\star h^{-1})^{-1}$ (*). Το στοιχείο $k^{-1}\star h^{-1}$ ανήκει στο σύνολο $K\star H \subseteq H\star K$ και γι' αυτό υπάρχουν $\bar{h} \in H$ και $\bar{k} \in K$ με $k^{-1}\star h^{-1} = \bar{h}\star\bar{k}$ (**). Από τις (*) και (**) προκύπτει ότι $h\star k = (\bar{h}\star\bar{k})^{-1} = \bar{k}^{-1}\star\bar{h}^{-1}$. Το γινόμενο $\bar{k}^{-1}\star\bar{h}^{-1}$ ανήκει στο $K\star H$, επειδή το $\bar{k}^{-1}$ ανήκει στο K (αφού το K είναι υποομάδα) και το $\bar{h}^{-1}$ ανήκει στο H (αφού το H είναι υποομάδα). Επομένως, το στοιχείο $h\star k$ ανήκει στο $K\star H$. Συνεπώς, $H\star K \subseteq K\star H$. Ώστε, $H\star K = K\star H$.

«$\Leftarrow$» Έστω ότι $H\star K = K\star H$. Θα δείξουμε ότι $H\star K \leq G$ εφαρμόζοντας το Λήμμα 1.3.6. Παρατηρούμε ότι $H\star K \neq \emptyset$, αφού το ουδέτερο $e_G = e_G\star e_G$ ανήκει στο $H\star K$, διότι το e_G ανήκει στις υποομάδες H και K. Τώρα θα δείξουμε ότι όταν $x_1, x_2 \in H\star K$, τότε το $x_1\star x_2^{-1}$ είναι στοιχείο τού $H\star K$. Πράγματι, $x_1 = h_1\star k_1$ με $h_1 \in H$ και $k_1 \in K$, αφού $x_1 \in H\star K$. Όμοια, $x_2 = h_2\star k_2$ με $h_2 \in H$ και $k_2 \in K$. Τώρα έχουμε:

$$x_1\star x_2^{-1} = (h_1\star k_1)\star(h_2\star k_2)^{-1} = h_1\star k_1\star k_2^{-1}\star h_2^{-1}. \qquad (***)$$

Το $k_1\star k_2^{-1}$ είναι κάποιο στοιχείο τής K, αφού τα k_1, k_2 ανήκουν στην υποομάδα K. Επομένως, το $k_1\star k_2^{-1}\star h_2^{-1}$, το οποίο είναι στοιχείο τού $K\star H$, ισούται, λόγω τής υπόθεσης, με κάποιο $h_3\star k_3 \in H\star K$, όπου $h_3 \in H$ και $k_3 \in K$. Έτσι, από την (***) έπεται $x_1\star x_2^{-1} = h_1\star h_3\star k_3$. Το γινόμενο $h_1\star h_3$ ανήκει στην H, αφού τα $h_1, h_3 \in H$ και η H είναι υποομάδα. Ώστε, το $x_1\star x_2^{-1}$ ανήκει στο $H\star K$ και γι' αυτό το συγκεκριμένο σύνολο είναι υποομάδα τής $(G,\star)$.

Α 38. Έστω ότι $(G,\star)$ είναι μια ομάδα και H μια υποομάδα της. Να δειχθεί ότι το υποσύνολο

$$\mathcal{N}_G(H) = \{a\in G \mid a\star H\star a^{-1} \subseteq H\}$$

αποτελεί υποομάδα τής $(G, \star)$ και μάλιστα $H \le \mathcal{N}_G(H)$.
(Η υποομάδα $\mathcal{N}_G(H)$ ονομάζεται, για λόγους που θα δούμε αργότερα, βλ. Παρατήρηση 2.4.7, ο *ορθοθετοποιητής τής* H ή η *ορθοθετοποιούσα την* H υποομάδα τής G.)

Λύση. Είναι φανερό ότι $H \subseteq \mathcal{N}_G(H)$, αφού για κάθε $a \in H$, είναι $a \star h \star a^{-1} \in H, \forall h \in H$, επειδή η H είναι υποομάδα τής $(G, \star)$. Ιδιαιτέρως, $\mathcal{N}_G(H) \neq \emptyset$. Αν $a, b \in \mathcal{N}_G(H)$, τότε για κάθε $h \in H$ έχουμε:

$$(a \star b) \star h \star (a \star b)^{-1} = a \star (b \star h \star b^{-1}) \star a^{-1}.$$

Το στοιχείο $h' = b \star h \star b^{-1}$ ανήκει στο H επειδή $b \in \mathcal{N}_G(H)$ και $h \in H$. Συνεπώς, το $a \star h' \star a^{-1} = a \star (b \star h \star b^{-1}) \star a^{-1}$ ανήκει στο H, αφού το $h' \in H$ και $a \in \mathcal{N}_G(H)$. Ώστε, $\mathcal{N}_G(H) \le G$ και επειδή $H \subseteq \mathcal{N}_G(H)$, έπεται $H \le \mathcal{N}_G(H)$.

Α 39. Έστω ότι $(G, \star)$ είναι μια ομάδα. Να δειχθεί ότι το σύνολο:

$$\mathcal{Z}(G) := \{a \in G \mid a \star g = g \star a, \forall g \in G\}$$

είναι μια υποομάδα τής G.

Η υποομάδα $\mathcal{Z}(G)$ ονομάζεται το *κέντρο* τής G.

Λύση. Το σύνολο $\mathcal{Z}(G) \neq \emptyset$, διότι το ουδέτερο στοιχείο e_G τής G μετατίθεται με οποιοδήποτε στοιχείο τής G. Όταν τα $a, b \in \mathcal{Z}(G)$, τότε το $a \star b^{-1}$ είναι στοιχείο τού $\mathcal{Z}(G)$, αφού από $\forall g \in G, g \star b = b \star g$ έπεται $\forall g \in G, b^{-1} \star g = g \star b^{-1}$ και αφού

$$\begin{aligned}\forall g \in G :&(a \star b^{-1}) \star g = a \star (b^{-1} \star g) = a \star (g \star b^{-1}) = \\ &(a \star g) \star b^{-1} = (g \star a) \star b^{-1} = g \star (a \star b^{-1}).\end{aligned}$$

Σύμφωνα με το Λήμμα 1.3.6, το $\mathcal{Z}(G)$ είναι υποομάδα τής $(G, \star)$.

Α 40. Να ευρεθεί το κέντρο $\mathcal{Z}(D_n)$ τής διεδρικής ομάδας $(D_n, \circ)$, $n \ge 3$.

Λύση. Από την Άσκηση Α25 γνωρίζουμε ότι

$$D_n = \{\mathrm{Id}_n, \tau, \rho, \rho^2, \ldots, \rho^{n-1}, \tau \circ \rho, \tau \circ \rho^2, \ldots, \tau \circ \rho^{n-1}\}.$$

Επίσης γνωρίζουμε ότι $\tau^2 = \mathrm{Id}_n$, $\rho^n = \mathrm{Id}_n$ και ότι $\rho \circ \tau = \tau \circ \rho^{-1} = \tau \circ \rho^{n-1}$ (*), βλ. σελ. 20.

Ισχυριζόμαστε ότι κανένα από τα στοιχεία τής μορφής $\tau \circ \rho^i, 1 \le i \le n$, δεν ανήκει στο $\mathcal{Z}(D_n)$. Πράγματι, αν κάποιο $\tau \circ \rho^i$ με $1 \le i \le n$ ανήκε στο $\mathcal{Z}(D_n)$, τότε θα ήταν $(\tau \circ \rho^i) \circ \rho = \rho \circ (\tau \circ \rho^i) = (\rho \circ \tau) \circ \rho^i$ από όπου, λόγω τής (*), θα προέκυπτε ότι $(\tau \circ \rho^i) \circ \rho = (\tau \circ \rho^{n-1}) \circ \rho^i$. Έτσι θα είχαμε ότι $\rho^{i+1} = \rho^{n+i-1}$ και κατόπιν ότι $\rho^{n-2} = \mathrm{Id}_n$, το οποίο είναι άτοπο.

Ας υποθέσουμε τώρα ότι κάποια δύναμη $\rho^i, 1 \le i \le n-1$ ανήκει στο $\mathcal{Z}(D_n)$. Τότε βέβαια θα πρέπει να ισχύει ότι $\rho^i \circ \tau = \tau \circ \rho^i$ (**). Όμως η (*) δίνει ότι $\rho^i \circ \tau = \tau \circ \rho^{n-i}$ και γι' αυτό από την (**) προκύπτει ότι $\tau \circ \rho^i = \tau \circ \rho^{n-i}$ και τελικά ότι $\rho^i = \rho^{n-i}$. Αφού όμως $1 \leq i, n-i \leq n-1$, έπεται ότι $i = n-i$ και γι' αυτό ο n οφείλει να είναι άρτιος και το $i = n/2$.

Επομένως, όταν ο n είναι περιττός, τότε $\mathcal{Z}(D_n) = \{\mathrm{Id}_n\}$.
Τώρα θα δείξουμε ότι όταν ο n είναι άρτιος, η αναγκαία συνθήκη $i = n/2$ που απαιτείται ώστε να ανήκει το ρ^i στο $\mathcal{Z}(D_n)$ είναι και ικανή.

Πράγματι, για κάθε $\tau \circ \rho^j, 0 \leq j \leq n-1$ είναι:

$$\rho^{n/2} \circ (\tau \circ \rho^j) = (\rho^{n/2} \circ \tau) \circ \rho^j = (\tau \circ \rho^{n/2}) \circ \rho^j = \tau \circ (\rho^{n/2} \circ \rho^j) = (\tau \circ \rho^j) \circ \rho^{n/2}.$$

Επομένως, όταν ο n είναι άρτιος, τότε $\mathcal{Z}(D_n) = \{\mathrm{Id}_n, \rho^{n/2}\}$.

Α 41. Να δειχθεί ότι το κέντρο $\mathcal{Z}(S_n)$ τής συμμετρικής ομάδας $(S_n, \circ), n \geq 3$ είναι τετριμμένο.

Λύση. Θα χρησιμοποιήσουμε την έννοια τού κεντροποιητή $\mathcal{C}_G(a)$ στοιχείου a ομάδας G που ο ορισμός και οι ιδιότητές του δίνονται στην Άσκηση ΠΑ35. Ιδιαίτερα, την ιδιότητα ότι το κέντρο $\mathcal{Z}(G)$ περιέχεται στην τομή $\bigcap_{y \in Y} \mathcal{C}_G(y)$, όπου Y είναι οποιοδήποτε μη κενό υποσύνολο τής G.

Για κάθε $j \in X = \{1, 2, \ldots, n\}, j \neq 1$, θεωρούμε την απεικόνιση $\varphi_{1j} : X \to X$, που ορίζεται ως $\varphi_{1j}(1) := j$, $\varphi_{1j}(j) := 1$ και $\varphi_{1j}(x) := x, \forall x \in X, x \neq 1, j$. Προφανώς, η φ_{1j} ανήκει στη συμμετρική ομάδα S_n. Σύμφωνα με όσα είπαμε πιο πάνω, το $\mathcal{Z}(S_n)$ περιέχεται στην τομή $\bigcap_{\ell=2}^{n} \mathcal{C}_G(\varphi_{1\ell})$.
Θα δείξουμε ότι η $\bigcap_{\ell=2}^{n} \mathcal{C}_G(\varphi_{1\ell})$ ισούται με την τετριμμένη υποομάδα $\{\mathrm{Id}_n\}$ τής S_n, από όπου θα προκύψει αμέσως ότι $\mathcal{Z}(S_n) = \{\mathrm{Id}_n\}$.

Όταν $\sigma \in S_n$ με $\sigma \in \mathcal{C}_G(\varphi_{1j})$, τότε $\varphi_{1j} \circ \sigma = \sigma \circ \varphi_{1j}$. Ιδιαιτέρως,

$$\varphi_{1j} \circ \sigma(1) = \sigma \circ \varphi_{1j}(1) = \sigma(j), (*) \text{ και } \varphi_{1j} \circ \sigma(j) = \sigma \circ \varphi_{1j}(j) = \sigma(1), (**).$$

Παρατηρούμε ότι $\{\sigma(1), \sigma(j)\} = \{1, j\}$. Πράγματι, αν $\sigma(1) \notin \{1, j\}$, τότε $\varphi_{1j} \circ \sigma(1) = \sigma(1)$ και η $(*)$ δίνει $\sigma(1) = \sigma(j)$. Αυτό όμως είναι άτοπο αφού η σ είναι αμφιρριπτική και $1 \neq j$. Παρόμοια, αν $\sigma(j) \notin \{1, j\}$, τότε $\varphi_{1j} \circ \sigma(j) = \sigma(j)$ και η $(**)$ δίνει $\sigma(j) = \sigma(1)$, το οποίο όπως είδαμε είναι άτοπο.

Έστω $k \in \mathbb{N}, 2 \leq k \leq n$ με $k \neq j$, το οποίο υπάρχει διότι $n \geq 3$ και φ_{1k} το αντίστοιχο στοιχείο τής S_n. Όταν $\sigma \in S_n$ με $\sigma \in \mathcal{C}_G(\varphi_{1j}) \bigcap \mathcal{C}_G(\varphi_{1j})$, τότε συμπεραίνουμε όπως προηγουμένως ότι $\{\sigma(1), \sigma(j)\} = \{1, j\}$ και $\{\sigma(1), \sigma(k)\} = \{1, k\}$. Επομένως, $\sigma(1) \in \{1, j\} \bigcap \{1, k\}$ και επειδή τα $j, k \geq 2$ και $j \neq k$, συμπεραίνουμε ότι $\sigma(1) = 1$ και ως εκ τούτου, $\sigma(j) = j$ και $\sigma(k) = k$. Επομένως, $\sigma \in \bigcap_{\ell=2}^{n} \mathcal{C}_G(\varphi_{1\ell}) \Leftrightarrow \sigma = \mathrm{Id}_n$. Άρα, $\mathcal{Z}(S_n) = \{\mathrm{Id}_n\}$.

Προτεινόμενες Ασκήσεις

ΠΑ 29. Να δειχθεί ότι η πολλαπλασιαστική ομάδα των μη μηδενικών μιγαδικών αριθμών $(\mathbb{C}^\star, \cdot)$, διαθέτει για κάθε φυσικό αριθμό $n \in \mathbb{N}$, υποομάδες H με τάξη $[H : 1] = n$. Να συμπεράνετε ότι υπάρχουν ομάδες άπειρης τάξης που διαθέτουν μη τετριμμένες υποομάδες (οποιασδήποτε) πεπερασμένης τάξης.

ΠΑ 30. Έστω η ομάδα $(\mathbb{Z}_{20}, +)$ των ακέραιων αριθμών κατά μόδιο 20 και τα ακόλουθα υποσύνολά της

$$H_1 = \{[2], [18], [4], [12], [0]\}, H_2 = \{[18], [16], [14], [12], [10], [8], [6], [4], [2], [0]\}$$
$$H_3 = \{[0], [-2], [2]\}, \quad H_4 = \{[0], [-10]\}, \quad H_5 = \{[0], [3], [6], [9], [18]\}.$$

Ποια από τα υποσύνολα αυτά είναι υποομάδες τής $(\mathbb{Z}_{20}, +)$;

ΠΑ 31. Έστω η συμμετρική ομάδα $(S_3, \circ)$, βλ. Άσκηση Α4(ε′). Να δειχθεί ότι καθένα από τα σύνολα $M_1 = \{\tau_1, \rho\}$, $M_2 = \{\tau_3, \sigma\}$ και $M_3 = \{\tau_1, \tau_2\}$ είναι σύνολο γεννητόρων τής S_3. Να εξεταστεί, αν υπάρχει υποσύνολο P τής S_3 με $|P| = 1$, το οποίο να αποτελεί σύνολο γεννητόρων της.

ΠΑ 32. Έστω $(S_X, \circ)$ η συμμετρική ομάδα ενός συνόλου X με πλήθος στοιχείων $|X| \geq 3$. Έστω ω ένα πάγιο στοιχείο τού X.

Να δειχθεί ότι το σύνολο $\mathcal{S} = \{(\sigma, \tau) \in S_X \times S_X \mid \sigma(\omega) = \tau(\omega)\}$ δεν είναι υποομάδα τού ευθέως γινομένου $S_X \times S_X$ τής S_X με τον εαυτό της.

ΠΑ 33. Έστω ότι $(G, \star)$ είναι μια ομάδα. Να δειχθεί ότι το υποσύνολο

$$\overline{G} := \{a \in G \mid (a \star x)^2 = (x \star a)^2, \forall x \in G\}.$$

αποτελεί υποομάδα τής $(G, \star)$.

ΠΑ 34. Έστω ότι $(G, \star)$ είναι μια ομάδα, ότι H είναι μια υποομάδα τής G και ότι a είναι ένα στοιχείο τής G.

(α′) Να δειχθεί ότι το υποσύνολο

$$a \star H \star a^{-1} := \{a \star h \star a^{-1} \mid h \in H\}.$$

αποτελεί υποομάδα τής $(G, \star)$.

(β′) Να δειχθεί ότι $[a \star H \star a^{-1} : 1] = [H : 1]$.
(Κάθε υποομάδα τής μορφής aHa^{-1}, $a \in G$ ονομάζεται *συζυγής* τής H.)

ΠΑ 35. Έστω ότι $(G, \star)$ είναι μια ομάδα, ότι $H \leq G$ και ότι $a \in G$. Να δειχθούν τα εξής:

(α′) Το σύνολο $\mathcal{C}_G(H) := \{g \in G \mid \forall h \in H, g \star h = h \star g\}$ είναι μια υποομάδα τής G.
(Η $\mathcal{C}_G(H)$ ονομάζεται ο *κεντροποιητής τής H* ή η *κεντροποιούσα την H υποομάδα τής G*.)

(β′) Το σύνολο $\mathcal{C}_G(a) := \{g \in G \mid g \star a = a \star g\}$ είναι μια υποομάδα τής G.
(Η $\mathcal{C}_G(a)$ ονομάζεται ο *κεντροποιητής τού a* ή η *κεντροποιούσα το a υποομάδα τής G*.)

(γ′) $\mathcal{C}_G(H) = \bigcap_{a \in H} \mathcal{C}_G(a)$.

(δ′) $\mathcal{Z}(G) = \bigcap_{a \in G} \mathcal{C}_G(a)$.

(ε′) Για κάθε υποομάδα $H \leq G$, το κέντρο $\mathcal{Z}(G)$ τής G είναι υποομάδα τής $\mathcal{C}_G(H)$.

(στ′) Για κάθε $a \in G$, το κέντρο $\mathcal{Z}(G)$ τής G είναι υποομάδα τής $\mathcal{C}_G(a)$.

ΠΑ 36. Έστω ότι $(G, \star)$ είναι μια ομάδα. Να δειχθεί ότι ο κεντροποιητής $\mathcal{C}_G(G)$ τής G ισούται με το κέντρο τής G.

ΠΑ 37. Έστω ότι G είναι η συμμετρική ομάδα $(S_3, \circ)$, βλ. Α4(ε′) και ότι H είναι μία από τις επόμενες υποομάδες τής S_3: $\{\mathrm{Id}_3\}$, S_3, $\langle\tau_1\rangle, \langle\tau_2\rangle, \langle\tau_3\rangle$ και $\langle\rho\rangle$. (Σημειώστε ότι στην Άσκηση Α42, θα αποδείξουμε ότι οι προηγούμενες υποομάδες είναι όλες οι υποομάδες τής S_3.) Για κάθε H, να υπολογιστούν οι υποομάδες:

(α′) Ο ορθοθετοποιητής $\mathcal{N}_G(H)$ τής H.

(β′) Ο κεντροποιητής $\mathcal{C}_G(H)$ τής H.

ΠΑ 38. Έστω ότι η $(G, \star)$ είναι μια αβελιανή ομάδα. Να δειχθεί ότι το σύνολο

$$H := \{a \in G \mid a = a^{-1}\}$$

αποτελεί μια υποομάδα τής $(G, \star)$.

ΠΑ 39. Έστω ότι η $(G, \star)$ είναι μια αβελιανή ομάδα και ότι $n \in \mathbb{N}$ είναι ένας πάγιος φυσικός αριθμός. Να δειχθούν τα εξής:

(α′) Το σύνολο

$$G_n := \{a \in G \mid a^n = e_G\}$$

αποτελεί μια υποομάδα τής $(G, \star)$.

(β′) Το σύνολο

$$G^n := \{a^n \mid a \in G\}$$

αποτελεί μια υποομάδα τής $(G, \star)$.

ΠΑ 40.

Έστω $G_1 \times G_2$ το (εξωτερικό) ευθύ γινόμενο των ομάδων $(G_1, \star_1)$ και $(G_2, \star_2)$.

(α′) Να δειχθεί ότι το $G_1 \times G_2$ είναι αβελιανή ομάδα, αν και μόνο αν, οι G_1 και G_2 είναι αβελιανές ομάδες.

(β′) Όταν οι G_1 και G_2 είναι αβελιανές ομάδες, τότε να δειχθεί ότι $(G_1 \times G_2)^n = G_1^n \times G_2^n$.

ΠΑ 41. Έστω ότι η $(G, \star)$ είναι μια αβελιανή ομάδα, ότι K είναι μια υποομάδα τής $(G, \star)$ και ότι $n \in \mathbb{N}$ είναι ένας πάγιος φυσικός αριθμός. Να δειχθεί ότι το σύνολο

$$H(K, n) := \{a \in G \mid a^n \in K\}$$

αποτελεί μια υποομάδα τής $(G, \star)$.

ΠΑ 42. Έστω ότι η $(G, \star)$ είναι μια αβελιανή ομάδα και ότι K μια υποομάδα τής $(G, \star)$. Να δειχθεί ότι το σύνολο

$$H(K) := \{a \in G \mid a^n \in K, \text{ για κάποιο } n \in \mathbb{N}\}$$

αποτελεί μια υποομάδα τής $(G, \star)$.

ΠΑ 43. Έστω ότι $(G, \star)$ είναι μια ομάδα. Να δειχθούν τα εξής:

(α′) Ένα υποσύνολο $L \subseteq G$ είναι υποομάδα τής G, αν και μόνο αν, η υποομάδα $\langle L \rangle$ που παράγεται από το L ισούται με το σύνολο L.

(β′) Έστω ότι H και K είναι υποομάδες τής G. Να δειχθεί ότι τα σύνολα $H \star K$ και $K \star H$ είναι ίσα, αν και μόνο αν, η υποομάδα $\langle H \bigcup K \rangle$ που παράγεται από την ένωση $H \bigcup K$ ισούται με $H \star K$.

1.4 Πλευρικές Κλάσεις, Θεώρημα Lagrange

Στην παρούσα ενότητα θα ασχοληθούμε κυρίως με ομάδες πεπερασμένης τάξης. Απαριθμώντας τα στοιχεία μιας ομάδας με δύο διαφορετικούς τρόπους θα καταλήξουμε σε ένα πολύ σημαντικό θεώρημα που η αρχική του μορφή οφείλεται στον Lagrange.[13]

Διαμερίσεις και Σχέσεις Ισοδυναμίας

Κατά την ανάπτυξη τής θεωρίας, θα χρειαστούμε την έννοια τής διαμέρισης από τη Θεωρία Συνόλων. Υπενθυμίζουμε τα εξής:

Έστω ότι $X \neq \emptyset$ είναι ένα σύνολο και ότι $\mathcal{X} = (X_i)_{i \in I}$ είναι μια οικογένεια υποσυνόλων του. Η οικογένεια $\mathcal{X}$ ονομάζεται μια *διαμέριση* τού συνόλου X όταν ικανοποιούνται τα ακόλουθα:

(α′) Για κάθε $i \in I$, το σύνολο X_i είναι $\neq \emptyset$.

(β′) Η ένωση $\bigcup_{i \in I} X_i$ ισούται με το σύνολο X.

(γ′) Όταν $X_i \bigcap X_j \neq \emptyset$, $i, j \in I$, τότε $X_i = X_j$.

Παρατήρηση 1.4.1. Όταν $\mathcal{X} = (X_i)_{i \in I}$ είναι μια διαμέριση ενός συνόλου X, τότε είναι γνωστό ότι η σχέση

$$\rho_{\mathcal{X}} = \{(x, x') \in X \times X \mid \exists i \in I \text{ με } x, x' \in X_i\}$$

αποτελεί μια σχέση ισοδυναμίας επί τού X, όπου οι κλάσεις ισοδυναμίας τής $\rho_{\mathcal{X}}$ συμπίπτουν με τα σύνολα X_i, $i \in I$ τής διαμέρισης $\mathcal{X}$.

[13] Joseph Louis Lagrange, 1736–1813, Ιταλός Μαθηματικός που έζησε το μεγαλύτερο μέρος τής ζωής του στη Γαλλία.

Ισχύει και το αντίστροφο. Όταν $\rho \subseteq X \times X$ είναι μια σχέση ισοδυναμίας επί ενός συνόλου $X \neq \emptyset$, τότε η οικογένεια $\mathcal{R} = ([x]_\rho)_{x \in X}$ των κλάσεων ισοδυναμίας $[x]_\rho$, αποτελεί μια διαμέριση τού X.

Παραδοχή Από εδώ και στο εξής δεχόμαστε ότι **η παράθεση δύο στοιχείων** a, b μιας ομάδας G **το ένα δίπλα στο άλλο**, δηλαδή το ab **σημαίνει την εκτέλεση τής πράξης** $a \star b$.

Έστω ότι $(G, \star)$ είναι οποιαδήποτε ομάδα (όχι απαραίτητα πεπερασμένη) και ότι $H \leq G$ είναι μια υποομάδα της.

Για κάθε $a \in G$, θεωρούμε το σύνολο:

$$aH := \{ah \mid h \in H\}.$$

Λήμμα 1.4.2. *Η οικογένεια $(aH)_{a \in G}$ με στοιχεία τα υποσύνολα aH τής G αποτελεί μια διαμέριση τής G.*

Απόδειξη. Ελέγχουμε τα τρία αιτήματα τού ορισμού τής σχέσης ισοδυναμίας που δώσαμε προηγουμένως, βλ. σελ. 67. Για κάθε $a \in G$, το aH είναι $\neq \emptyset$, αφού $a = ae_G \in aH$, διότι το e_G είναι και το ουδέτερο τής H. Η ένωση $\bigcup_{a \in G} aH$ ισούται με G, αφού κάθε στοιχείο $a \in G$ ανήκει στο αντίστοιχο σύνολο aH. Τέλος, αν $(aH) \bigcap (bH) \neq \emptyset$, τότε υπάρχει $x \in G$ με $x = ah = bh'$, όπου $h, h' \in H$ και έτσι έχουμε ότι $a = bh'h^{-1}$. Γι΄αυτό, αν $y = aw, w \in H$ είναι οποιοδήποτε στοιχείο τού aH, τότε $y = (bh'h^{-1})w$ και επειδή η H είναι υποομάδα και τα h', h^{-1}, w είναι στοιχεία της, έπεται ότι το y ανήκει στο bH. Συνεπώς, $aH \subseteq bH$. Με ανάλογο τρόπο αποδεικνύεται ότι $bH \subseteq aH$ και ως εκ τούτου $aH = bH$. Ώστε η οικογένεια $(aH)_{a \in G}$ αποτελεί μια διαμέριση τής G. □

Από την Παρατήρηση 1.4.1, συμπεραίνουμε ότι η διαμέριση $(aH)_{a \in G}$ χορηγεί μια σχέση ισοδυναμίας $\rho_{\ell,H} \subseteq G \times G$, όπου η κλάση ισοδυναμίας $[a]$ τού στοιχείου $a \in G$ είναι ακριβώς το σύνολο aH. Δηλαδή, $(a, b) \in \rho_{\ell,H}$, αν και μόνο αν, $a \in bH$ (ή ισοδύναμα $b \in aH$).

Παρατήρηση 1.4.3. Το ζεύγος $(a, b) \in G \times G$ ανήκει στο σύνολο $\rho_{\ell,H}$, δηλαδή το στοιχείο $a \in G$ είναι $\rho_{\ell,H}$–ισοδύναμο με το $b \in G$, αν και μόνο αν, το στοιχείο $b^{-1}a$ (ή ισοδύναμα το στοιχείο $a^{-1}b$) ανήκει στην υποομάδα H.

Πράγματι,

$$a \sim_{\rho_{\ell,H}} b \Leftrightarrow a \in bH \Leftrightarrow a = bh, h \in H \Leftrightarrow b^{-1}a \in H \Leftrightarrow (b^{-1}a)^{-1} = a^{-1}b \in H.$$

Συχνά, όταν δίδεται μια ομάδα G και μια υποομάδα της H, μπορεί πρώτα να οριστεί η σχέση ισοδυναμίας $\rho_{\ell,H} \subseteq G \times G$ μέσω τού

$$(a, b) \in \rho_{\ell,H} \Leftrightarrow b^{-1}a \in H$$

και μετά να προκύψει η διαμέριση $(aH)_{a \in H}$ τής G από τις κλάσεις ισοδυναμίας $aH, a \in H$ τής $\rho_{\ell,H}$. Η σχέση ισοδυναμίας $\rho_{\ell,H}$ χορηγεί επίσης το σύνολο $G/\rho_{\ell,H}$ των κλάσεων ισοδυναμίας aH τής $\rho_{\ell,H}$.

Προσέξτε ότι το $G/\rho_{\ell,H}$ έχει ως στοιχεία **όλες ακριβώς τις διαφορετικές κλάσεις ισοδυναμίας** τής $\rho_{\ell,H}$.

Όπως θα δούμε πολύ σύντομα, οι συγκεκριμένες κλάσεις είναι πολύ σημαντικές στην ανάπτυξη τής Θεωρίας των Ομάδων.

Ορισμός 1.4.4. Έστω ότι $(G, \star)$ είναι μια ομάδα, ότι $H \leq G$ είναι μια υποομάδα της και ότι a είναι ένα στοιχείο τής G. Το σύνολο

$$aH = \{ah \mid h \in H\}$$

καλείται η *αριστερή πλευρική κλάση* τής H στην G με αντιπρόσωπο το $a \in G$ και αντίστοιχα το σύνολο

$$Ha = \{ha \mid h \in H\}$$

καλείται η η *δεξιά πλευρική κλάση* τής H στην G με αντιπρόσωπο το $a \in G$.

Παρατήρηση 1.4.5. Προηγουμένως, διαπιστώσαμε ότι οι αριστερές πλευρικές κλάσεις τής H στην G αποτελούν μια διαμέριση τής G και γι' αυτό ορίζουν τη σχέση ισοδυναμίας $\rho_{\ell,H}$ επί τής G. Εντελώς ανάλογα αποδεικνύεται ότι οι δεξιές πλευρικές κλάσεις τής H στην G διαμερίζουν την G και ως εκ τούτου ορίζουν επίσης μια σχέση ισοδυναμίας $\rho_{r,H} \subseteq G \times G$ επί τής G. Τώρα, δύο στοιχεία $a, b \in G$ είναι $\rho_{r,H}$–ισοδύναμα, δηλαδή $a \sim_{\rho_{r,H}} b$, αν και μόνο αν, $ba^{-1} \in H$, αν και μόνο αν, $ab^{-1} \in H$. Όπως προηγουμένως, η σχέση ισοδυναμίας $\rho_{r,H}$ χορηγεί το σύνολο $G/\rho_{r,H}$ των κλάσεων ισοδυναμίας τής $\rho_{h,H}$. Προσέξτε ότι το $G/\rho_{r,H}$ έχει ως στοιχεία **όλες ακριβώς τις διαφορετικές κλάσεις ισοδυναμίας** τής $\rho_{r,H}$, δηλαδή όλες τις διαφορετικές δεξιές πλευρικές κλάσεις τής H στην G.

Παράδειγμα 1.4.6. Θεωρούμε τη συμμετρική ομάδα $(S_3, \circ)$, τής οποίας τον πίνακα πράξης τον υπολογίσαμε στην Α4.(δ'), βλ. σελ. 32. Έστω T_1 η κυκλική υποομάδα $\langle \tau_1 \rangle = \{\mathrm{Id}_3, \tau_1\}$. Θα προσδιορίσουμε όλες τις αριστερές και όλες τις δεξιές πλευρικές κλάσεις τής T_1 στην S_3.

Οι αριστερές πλευρικές κλάσεις

Η αριστερή πλευρική κλάση $Id_3 \circ T_1$ ισούται με $\{Id_3 \circ Id_3, Id_3 \circ \tau_1\} = \{Id_3, \tau_1\} = T_1$. Για να προσδιορίσουμε μια διαφορετική αριστερή πλευρική κλάση πρέπει να διαλέξουμε ένα στοιχείο τής S_3 που δεν ανήκει στην $\mathrm{Id}_3 \circ T_1 = T_1$, αφού αν διαλέγαμε κάποιο από τα στοιχεία τής $\mathrm{Id}_3 \circ T_1$ και σχηματίζαμε κατόπιν την αντίστοιχη αριστερή πλευρική κλάση, τότε αυτή θα είχε τουλάχιστον ένα κοινό στοιχείο με την $\mathrm{Id}_3 \circ T_1$ και τότε θα συνέπιπτε με την $\mathrm{Id}_3 \circ T_1$, αφού πάντοτε δύο αριστερές πλευρικές κλάσεις ή δεν έχουν κανένα κοινό στοιχείο ή ταυτίζονται.

Η αριστερή πλευρική κλάση τού $\tau_2 \notin Id_3 \circ T_1$ είναι η $\tau_2 \circ T_1 = \{\tau_2 \circ \mathrm{Id}_3, \tau_2 \circ \tau_1\} = \{\tau_2, \sigma\}$.

Για να προσδιορίσουμε τώρα μια αριστερή πλευρική κλάση διαφορετική από τις προηγούμενες, θα διαλέξουμε ένα στοιχείο από το σύνολο $S_3 \setminus (\mathrm{Id}_3 \circ T_1) \bigcup (\tau_2 \circ T_1) = \{\tau_3, \rho\}$. Επιλέγουμε το τ_3 και θεωρούμε την αριστερή πλευρική κλάση $\tau_3 \circ T_1 = \{\tau_3 \circ \mathrm{Id}_3, \tau_3 \circ \tau_1\} = \{\tau_3, \rho\}$. Είναι σαφές ότι δεν υπάρχει άλλη αριστερή πλευρική κλάση, αφού όλα τα στοιχεία τής S_3 έχουν εξαντληθεί. Έτσι προκύπτει η ακόλουθη διαμέριση τής S_3 σε αριστερές πλευρικές κλάσεις:

$$S_3 = T_1 \bigcup (\tau_2 \circ T_1) \bigcup (\tau_3 \circ T_1) = \{\mathrm{Id}_3, \tau_1\} \bigcup \{\tau_2, \sigma\} \bigcup \{\tau_3, \rho\}.$$

Οι δεξιές πλευρικές κλάσεις

Η δεξιά πλευρική κλάση στην οποία ανήκει το ουδέτερο στοιχείο Id_3 τής S_3 είναι η $T_1 \circ \mathrm{Id}_3 = \{\mathrm{Id}_3 \circ \mathrm{Id}_3, \tau_1 \circ \mathrm{Id}_3\} = \{\mathrm{Id}_3, \tau_1\} = T_1$.

Διαλέγουμε τώρα το στοιχείο $\tau_2 \in S_3$, το οποίο δεν ανήκει στην $T_1 \circ \mathrm{Id}_3 = T_1$ και σχηματίζουμε τη δεξιά πλευρική κλάση $T_1 \circ \tau_2 = \{\mathrm{Id}_3 \circ \tau_2, \tau_1 \circ \tau_2\} = \{\tau_2, \rho\}$. Χωρίς να εκτελέσουμε κανέναν υπολογισμό γνωρίζουμε ότι $(T_1 \circ \mathrm{Id}_3) \bigcap (T_1 \circ \tau_2) = \emptyset$, αφού αν η συγκεκριμένη τομή δεν ήταν κενή, τότε αυτά τα δύο σύνολο θα συνέπιπταν αφού είναι κλάσεις ισοδυναμίας τής σχέσης ισοδυναμίας ρ_{r,T_1}

Για να σχηματίσουμε μια δεξιά πλευρική κλάση διαφορετική από τις προηγούμενες πρέπει να διαλέξουμε ένα στοιχείο από το σύνολο $S_3 \setminus (T_1 \circ \mathrm{Id}_3) \bigcup (T_1 \circ \tau_2) = \{\mathrm{Id}_3, \tau_1, \tau_2, \rho\} = \{\tau_3, \sigma\}$. Επιλέγουμε το τ_3 και σχηματίζουμε τη δεξιά πλευρική κλάση $T_1 \circ \tau_3 = \{\mathrm{Id}_3 \circ \tau_3, \tau_1 \circ \tau_3\} = \{\tau_3, \sigma\}$. Είναι σαφές ότι δεν υπάρχει άλλη δεξιά πλευρική κλάση, αφού όλα τα στοιχεία τής S_3 έχουν εξαντληθεί. Έτσι προκύπτει η ακόλουθη διαμέριση τής S_3 σε δεξιές πλευρικές κλάσεις:

$$S_3 = T_1 \bigcup (T_1 \circ \tau_2) \bigcup (T_1 \circ \tau_3) = \{\mathrm{Id}_3, \tau_1\} \bigcup \{\tau_2, \rho\} \bigcup \{\tau_3, \sigma\}.$$

Παρατήρηση 1.4.7. Από το προηγούμενο παράδειγμα διαπιστώνουμε τα εξής:

(α′) Το πλήθος των στοιχείων που έχει κάθε αριστερή ή δεξιά πλευρική κλάση τής T_1 στην S_3 είναι ίσο με δύο, συμπίπτει δηλαδή με το πλήθος των στοιχείων τής υποομάδας T_1 και είναι διαιρέτης τής τάξης τής ομάδας S_3, η οποία είναι έξι.

(β′) Το πλήθος των αριστερών πλευρικών κλάσεων είναι ίσο με τρία, συμπίπτει δηλαδή με το πλήθος των δεξιών πλευρικών κλάσεων και είναι διαιρέτης τής τάξης τής ομάδας S_3 που είναι έξι.

(γ′) Η αριστερή πλευρική κλάση ενός στοιχείου δεν είναι πάντοτε ίση με τη δεξιά πλευρική κλάση τού ίδιου στοιχείου, π.χ. $\tau_2 \circ T_1 = \{\tau_2, \sigma\} \neq T_1 \circ \tau_2 = \{\tau_2, \rho\}$.

Θα αποδείξουμε αμέσως παρακάτω ότι οι παρατηρήσεις (α′) και (β′) ισχύουν γενικώς.

Λήμμα 1.4.8. *Έστω ότι $(G, \star)$ είναι μια ομάδα, ότι $H \leq G$ είναι μια υποομάδα της και ότι τα $a, b \in G$ είναι στοιχεία τής G. Τα σύνολα H, aH και Hb είναι ισοπληθή.*

Απόδειξη. Ως γνωστόν, για να είναι ισοπληθή τα σύνολα H, aH και Hb, είναι αρκετό να υπάρχουν αμφιρριπτικές απεικονίσεις ανάμεσά τους. Θεωρούμε την απεικόνιση

$$\ell_a : H \to aH, h \mapsto ah.$$

Η ℓ_a είναι ενριπτική απεικόνιση, αφού αν $ah = \ell_a(h) = \ell_a(h') = ah', h, h' \in H$, τότε $a^{-1}(ah) = a^{-1}(ah')$ και συνεπώς $h = h'$.

Η ℓ_a είναι επιρριπτική απεικόνιση, αφού αν $y \in aH$, τότε από τον ορισμό τού συνόλου aH, έπεται ότι υπάρχει $h \in H$ με $y = ah$ και επομένως $\ell_a(h) = ah = y$.

Η απόδειξη ότι το H είναι ισοπληθές τού Hb είναι παρόμοια. Αφού το H είναι ισοπληθές και με το aH και με το Hb, έπεται ότι και τα aH, Hb είναι επίσης ισοπληθή. □

Θεώρημα Lagrange

Ερχόμαστε τώρα στο πολύ σημαντικό Θεώρημα Lagrange που αφορά τις πεπερασμένες ομάδες. Σημειώνουμε το προφανές ότι όταν μια ομάδα $(G, \star)$ είναι πεπερασμένη, τότε και κάθε υποομάδα της $H \leq G$ είναι πεπερασμένη. Επιπλέον, το πλήθος των διαφορετικών αριστερών (αντιστοίχως δεξιών) πλευρικών κλάσεων $aH, a \in G$ $(Ha, a \in G)$, δηλαδή το πλήθος των στοιχείων τού συνόλου $G/\rho_{\ell,H}$ (αντιστοίχως τού συνόλου $G/\rho_{r,H}$), είναι πεπερασμένο και μάλιστα μικρότερο ή ίσο από την τάξη $[G:1]$ τής G, αφού οι διαφορετικές αριστερές (αντιστοίχως δεξιές) πλευρικές κλάσεις διαμερίζουν την G.

Ας συμβολίσουμε προσωρινά με $[G : H]_\ell$ (αντιστοίχως $[G : H]_r$), το πλήθος τού $G/\rho_{\ell,H}$ (αντιστοίχως τού $G/\rho_{r,H}$), δηλαδή το πλήθος των διαφορετικών αριστερών (αντιστοίχως δεξιών) πλευρικών κλάσεων τής H στην G.

Θεώρημα 1.4.9 (Θεώρημα Lagrange). *Έστω $(G, \star)$ μια πεπερασμένη ομάδα και $H \leq G$ μια υποομάδα της.*

Η τάξη $[H : 1]$ τής υποομάδας H διαιρεί την τάξη $[G : 1]$ τής ομάδας G και μάλιστα

$$\frac{[G:1]}{[H:1]} = [G:H]_\ell = [G:H]_r$$

Απόδειξη. Έστω ότι $G/\rho_{\ell,H} = \{a_1H, a_2H, \ldots, a_{[G:H]_\ell}H\}$ είναι το σύνολο όλων των διαφορετικών αριστερών πλευρικών κλάσεων τής H στην G, δηλαδή το σύνολο των διαφορετικών κλάσεων ισοδυναμίας τής $\rho_{\ell,H}$. Επειδή η οικογένεια $(aH)_{a\in G}$ αποτελεί μια διαμέριση τής G και επειδή για κάθε aH υπάρχει $a_iH \in G/\rho_{\ell,H}$ με $aH = a_iH$ έχουμε:

$$G = \bigcup_{a\in G} aH = \bigcup_{i=1}^{[G:H]_\ell} a_iH, i = 1, 2, \ldots, [G:H]_\ell.$$

Επομένως,

$$[G:1] = \sum_{i=1}^{[G:H]_\ell} |a_iH|, i = 1, 2, \ldots, [G:H]_\ell. \tag{*}$$

αφού $a_iH \bigcap a_jH = \emptyset$, όταν $i \neq j$. Από το Λήμμα 1.4.8, γνωρίζουμε ότι το πλήθος $|a_iH|$ των στοιχείων οποιασδήποτε αριστερής πλευρικής κλάσης a_iH ισούται με την τάξη $[H:1]$ τής H και γι' αυτό η ανωτέρω σχέση (*) παίρνει τη μορφή:

$$[G:1] = [G:H]_\ell \cdot [H:1]$$

ή ισοδύναμα

$$\frac{[G:1]}{[H:1]} = [G:H]_\ell.$$

Μια επανάληψη τής απόδειξης, χρησιμοποιώντας τις δεξιές πλευρικές κλάσεις τής H στην G, τη σχέση $\rho_{\ell,H}$ και το σύνολο $G/\rho_{\ell,H}$ δίνει την ισότητα:

$$\frac{[G:1]}{[H:1]} = [G:H]_r.$$

Συνεπώς, $[G:H]_\ell = \frac{[G:1]}{[H:1]} = [G:H]_r$. □

Από το Θεώρημα Lagrange, έπεται ότι το πλήθος των διαφορετικών αριστερών πλευρικών κλάσεων μιας υποομάδας H σε μια πεπερασμένη ομάδα $(G,\star)$ συμπίπτει με το πλήθος των διαφορετικών δεξιών πλευρικών κλάσεων τής H στην G. Αυτό ακριβώς διαπιστώσαμε και στο Παράδειγμα 1.4.6. Μάλιστα, ισχύει και το εξής γενικότερο:

Πρόταση 1.4.10. *Έστω ότι $(G,\star)$ είναι μια ομάδα και $H \leq G$ μια υποομάδα της. Έστω $G/\rho_{\ell,H}$ το σύνολο των διαφορετικών αριστερών πλευρικών κλάσεων τής H στην G και $G/\rho_{r,H}$ το αντίστοιχο σύνολο των διαφορετικών δεξιών πλευρικών κλάσεων. Τα $G/\rho_{\ell,H}$ και $G/\rho_{r,H}$ είναι ισοπληθή σύνολα.*

Απόδειξη. Θεωρούμε την αντιστοιχία

$$\theta : G/\rho_{\ell,H} \to G/\rho_{r,H}, aH \mapsto Ha^{-1}.$$

Η συγκεκριμένη αντιστοιχία είναι μια καλά ορισμένη απεικόνιση, αφού αν $aH = bH$, τότε το $b^{-1}a$ ανήκει στην υποομάδα H και γι' αυτό και το αντίστροφό του στοιχείο $(b^{-1}a)^{-1} = a^{-1}b$ ανήκει επίσης στην H, δηλαδή $a^{-1}b = h$, για κάποιο $h \in H$. Συνεπώς, το στοιχείο a^{-1} ανήκει στη δεξιά πλευρική κλάση Hb^{-1} και έτσι $Ha^{-1} = Hb^{-1}$, αφού $a^{-1} \in Ha^{-1} \bigcap Hb^{-1} \neq \emptyset$.

Η απεικόνιση θ είναι ενριπτική, αφού όταν $Ha^{-1} = \theta(aH) = \theta(bH) = Hb^{-1}$, τότε το στοιχείο $b^{-1}a$ ανήκει στην H. Επομένως, το $(b^{-1}a)^{-1} = a^{-1}b$ ανήκει στην H και γι' αυτό $aH = bH$.

Τέλος, η απεικόνιση θ είναι επιρριπτική, αφού για κάθε δεξιά κλάση Ha είναι $\theta(a^{-1}H) = H(a^{-1})^{-1} = Ha$. □

Ώστε πάντοτε το πλήθος τού $G/\rho_{\ell,H}$, δηλαδή το πλήθος των διαφορετικών αριστερών πλευρικών κλάσεων μιας υποομάδας $H \leq G$ στην G είναι ίσο με το πλήθος τού $G/\rho_{r,H}$, δηλαδή με το πλήθος των διαφορετικών δεξιών πλευρικών κλάσεων τής H στην G. Γι' αυτό μπορούμε να ορίσουμε γενικώς:

Ορισμός 1.4.11. Έστω ότι $(G,\star)$ είναι μια ομάδα και $H \leq G$ μια υποομάδα τής G. Καλούμε *δείκτη* τής H στην G το πλήθος των διαφορετικών αριστερών (δεξιών) πλευρικών κλάσεων τής H στην G.

Συμβολισμός. Ο δείκτης τής H στην G συμβολίζεται με $[G:H]$. Έχουμε λοιπόν $|G/\rho_{\ell,H}| = |G/\rho_{r,H}| = [G:H]$.

Παρατήρηση 1.4.12. (α′) Στην περίπτωση τής τετριμμένης υποομάδας $\{e_G\}$, κάθε αριστερή πλευρική κλάση $a\{e_G\}$ ισούται με $\{a\}$. Έτσι έχουμε αμέσως ότι ο δείκτης $[G:\{e_G\}]$ ισούται με το πλήθος των στοιχείων τής G. Αυτός ακριβώς είναι και ο λόγος για τον οποίο χρησιμοποιούμε το σύμβολο $[G:1]$ προκειμένου να δηλώσουμε την τάξη τής ομάδας G.

(β′) Όταν η $(G,+)$ είναι μια αβελιανή (μεταθετική) ομάδα και η H είναι μια υποομάδα της, τότε κάθε αριστερή πλευρική κλάση $a+H$ ισούται με την αντίστοιχη δεξιά

πλευρική κλάση $H + a$, αφού $\forall a \in G, h \in H$ είναι $a + h = h + a$.
Όπως θα δούμε αργότερα, οι υποομάδες H μιας ομάδας $(G, \star)$ που έχουν την ιδιότητα $\forall a \in G, aH = Ha$, χωρίς να ισχύει απαραίτητα ότι $\forall a \in G, h \in H$ είναι $ah = ha$, έχουν πολύ μεγάλη σημασία στη Θεωρία Ομάδων.

Συχνά, το Θεώρημα Lagrange εκφράζεται και στην εξής μορφή:

Πόρισμα 1.4.13 (Θεώρημα Lagrange). *Όταν $(G, \star)$ είναι μια πεπερασμένη ομάδα και H είναι μια υποομάδα της, τότε*

$$[G : 1] = [G : H][H : 1].$$

Πράγματι, στο Παράδειγμα 1.4.6 είδαμε ότι η τάξη $[\langle \tau_1 \rangle : 1] = 2$ είναι διαιρέτης τής τάξης $[S_3 : 1] = 6$.
Ισχύει μάλιστα και κάτι πιο γενικό:

Πόρισμα 1.4.14. *Όταν $(G, \star)$ είναι μια πεπερασμένη ομάδα και H, K είναι υποομάδες της με $K \leq H$, τότε*

$$[G : K] = [G : H][H : K].$$

Απόδειξη. Πράγματι, έχουμε: $[G : 1] = [G : H][H : 1]$ και $[H : 1] = [H : K][K : 1]$. Επομένως, $[G : 1] = [G : H][H : K][K : 1]$ και αφού $[G : 1] = [G : K][K : 1]$, συμπεραίνουμε ότι $[G : K] = [G : H][H : K]$. □

Στην Άσκηση A45, παρουσιάζουμε μια περαιτέρω γενίκευση τού ανωτέρω πορίσματος.

Παράδειγμα 1.4.15. (α′) Θεωρούμε τη συμμετρική ομάδα $(S_X, \circ)$ ενός συνόλου X με πεπερασμένο πλήθος στοιχείων $|X| = n \geq 2$ και την υποομάδα S_X^{ω}, όπου ω είναι ένα πάγιο στοιχείο τού X, η οποία αποτελείται από τα $\sigma \in S_X$ με $\sigma(\omega) = \omega$, βλ. Άσκηση A28. Η τάξη $[S_X^{\omega} : 1]$ ισούται με $(n-1)!$, αφού η υποομάδα S_X^{ω} αποτελείται από τις αμφιρριπτικές (αμφιμονοσήμαντες) απεικονίσεις τού συνόλου $X \setminus \{\omega\}$ στον εαυτό του. Ο δείκτης $[S_X : S_X^{\omega}]$ ισούται με n, αφού $[S_X : S_X^{\omega}] = [S_X : 1]/[S_X^{\omega} : 1] = n!/(n-1)!$.

(β′) Θεωρούμε τη διεδρική ομάδα $(D_n, \circ)$. Υπενθυμίζουμε ότι η D_n είναι η ομάδα ισομετριών ενός κανονικού n-γώνου τού επιπέδου. Ήδη γνωρίζουμε ότι

$$D_n = \{\mathrm{Id}_n, \tau, \rho, \rho^2, \ldots, \rho^{n-1}, \tau \circ \rho, \tau \circ \rho^2, \ldots, \tau \circ \rho^{n-1}\},$$

βλ. Άσκηση A25. Επιπλέον, έχουμε επίσης διαπιστώσει ότι $\tau^2 = \mathrm{Id}_n$, $\rho^n = \mathrm{Id}_n$ και $\rho \circ \tau = \tau \circ \rho^{-1}$.

Θα υπολογίσουμε τους δείκτες $[D_n : \langle \rho \rangle]$ και $[D_n : \langle \tau \rangle]$.

(i) Για τον δείκτη $[D_n : \langle \rho \rangle]$.

Ισχυριζόμαστε ότι η τάξη $[\langle \rho \rangle : 1]$ τής κυκλικής υποομάδας $\langle \rho \rangle = \{\rho^z \mid z \in \mathbb{Z}\}$ τής D_n ισούται με n.
Προς τούτο αρκεί να δείξουμε ότι το υποσύνολο $\mathcal{R} = \{\mathrm{Id}_2, \rho, \rho^2, \ldots, \rho^{n-1}\}$ με

πλήθος στοιχείων $|\mathcal{R}| = n$, είναι μια υποομάδα τής D_n, αφού τότε γνωρίζοντας ότι η $\langle\rho\rangle$ είναι η μικρότερη υποομάδα τής D_n η οποία περιέχει το ρ και αφού $\mathcal{R} \subseteq \langle\rho\rangle$, συμπεραίνουμε ότι $\mathcal{R} = \langle\rho\rangle$ και ως εκ τούτου $[\langle\rho\rangle : 1] = n$. Για να αποδείξουμε ότι το $\mathcal{R}$ είναι μια υποομάδα τής D_n, είναι αρκετό να δείξουμε ότι είναι κλειστό ως προς την πράξη «$\circ$» τής D_n, λόγω τού Λήμματος 1.3.10. Έστω ότι τα $\rho^i, \rho^j \in \mathcal{R}$. Εκτελώντας ευκλείδεια διαίρεση με υπόλοιπο τού $i + j$ διά τού n, έχουμε $i + j = \lambda n + v, 0 \leq v \leq n - 1$. Επομένως,

$$\rho^i \circ \rho^j = \rho^{i+j} = \rho^{\lambda n + v} = (\rho^n)^\lambda \circ \rho^v = \mathrm{Id}_2^\lambda \circ \rho^v = \rho^v$$

και έτσι το $\rho^{i+j} = \rho^v$ ανήκει στο $\mathcal{R}$. Επομένως, το $\mathcal{R}$ είναι υποομάδα τής D_n και $\mathcal{R} = \langle\rho\rangle$.

Άρα, $[D_n : \langle\rho\rangle] = [D_n : 1]/[\langle\rho\rangle : 1] = 2n/n = 2$.

Αφού ο δείκτης $[D_n : \langle\rho\rangle]$ ισούται με 2, υπάρχουν ακριβώς δύο αριστερές κλάσεις, οι οποίες είναι οι

$$\mathrm{Id}_n \circ \langle\rho\rangle = \langle\rho\rangle = \{\mathrm{Id}_n, \rho, \rho^2, \ldots, \rho^{n-1}\}, \quad \tau \circ \langle\rho\rangle = \{\tau, \tau\circ\rho, \tau\circ\rho^2, \ldots, \tau\circ\rho^{n-1}\}$$

και ακριβώς δύο δεξιές πλευρικές κλάσεις, οι οποίες είναι οι

$$\langle\rho\rangle \circ \mathrm{Id}_n = \langle\rho\rangle = \{\mathrm{Id}_n, \rho, \rho^2, \ldots, \rho^{n-1}\}, \quad \langle\rho\rangle \circ \tau = \{\tau, \rho\circ\tau, \rho^2\circ\tau, \ldots, \rho^{n-1}\circ\tau\}.$$

Προσέξτε ότι $\forall i \in \mathbb{N}, 1 \leq i \leq n-1$, είναι $\rho^i \circ \tau = \tau \circ \rho^{-i} = \tau \circ \rho^{n-i}$. Ώστε, η δεξιά πλευρική κλάση $\langle\rho\rangle \circ \tau$ ισούται με την αριστερή πλευρική κλάση $\tau \circ \langle\rho\rangle$.

(ii) Για τον δείκτη $[D_n : \langle\tau\rangle]$.

Αφού $\tau = \tau^{-1}$, η κυκλική υποομάδα $\langle\tau\rangle = \{\tau^z \mid z \in \mathbb{Z}\}$ ισούται με $\{\mathrm{Id}_n, \tau\}$ και $[\langle\tau\rangle : 1] = 2$. Επομένως, $[D_n : \langle\tau\rangle] = [D_n : 1]/[\langle\tau\rangle : 1] = 2n/2 = n$.

Οι n το πλήθος αριστερές πλευρικές κλάσεις είναι οι:

$$\mathrm{Id}_n \circ \langle\tau\rangle = \{\mathrm{Id}_n, \tau\}, \quad \rho \circ \langle\tau\rangle = \{\rho, \rho\circ\tau\}, \ldots, \quad \rho^{n-1} \circ \langle\tau\rangle = \{\rho^{n-1}, \rho^{n-1}\circ\tau\}$$

και οι n το πλήθος δεξιές πλευρικές κλάσεις είναι οι:

$$\langle\tau\rangle \circ \mathrm{Id}_n = \{\mathrm{Id}_n, \tau\}, \quad \langle\tau\rangle \circ \rho = \{\rho, \tau\circ\rho\}, \ldots, \quad \langle\tau\rangle \circ \rho^{n-1} = \{\rho^{n-1}, \tau\circ\rho^{n-1}\}.$$

Εδώ, $\rho \circ \langle\tau\rangle = \{\rho, \rho\circ\tau\} \neq \{\rho, \tau\circ\rho\} = \langle\tau\rangle \circ \rho$, αφού, όπως ήδη γνωρίζουμε, $\rho \circ \tau \neq \tau \circ \rho$.

Παρατήρηση 1.4.16. Το Θεώρημα Lagrange προλέγει την τάξη των υποομάδων μιας πεπερασμένης ομάδας. Όταν μια ομάδα έχει τάξη $n \in \mathbb{N}$, τότε η τάξη κάθε υποομάδας της οφείλει να είναι ένας διαιρέτης d τού n. Έτσι μια ομάδα τάξης 56 είναι αδύνατο να έχει μια υποομάδα τάξης 6, αφού $6 \nmid 56$.

Ωστόσο, το Θεώρημα Lagrange δεν επιτρέπει το συμπέρασμα ότι σε κάθε διαιρέτη d τής τάξης n μιας ομάδας, υπάρχει οπωσδήποτε μια υποομάδα τάξης d. Αργότερα θα δούμε ότι η εναλλάσσουσα ομάδα $\mathbb{A}_4$, η οποία είναι τάξης 12, δεν διαθέτει υποομάδα τάξης 6, βλ. Πρόταση 1.8.40. Μια μερική αντιστροφή τού Θεωρήματος Lagrange, αποτελεί το Θεώρημα Cauchy, βλ. Θεώρημα 2.3.11.

Ολοκληρώνουμε την παρούσα ενότητα με δύο πολύ χρήσιμα θεωρήματα.

Θεώρημα 1.4.17. *Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H, K είναι δύο πεπερασμένες υποομάδες της.*
Για το πλήθος $|HK|$ των στοιχείων τού συνόλου $HK = \{hk \mid h \in H, k \in K\}$ ισχύει το εξής:

$$|HK| = \frac{[H:1][K:1]}{[H \bigcap K:1]}.$$

Απόδειξη. Σχηματίζουμε το σύνολο $H \times K = \{(h,k) \mid h \in H, k \in K\}$ και ορίζουμε τη σχέση

$$\rho = \{((h,k),(\overline{h},\overline{k})) \mid h, \overline{h} \in H, k, \overline{k} \in k, hk = \overline{h}\overline{k}\} \subseteq (H \times K) \times (H \times K).$$

Ισχυριζόμαστε ότι η ρ είναι μια σχέση ισοδυναμίας επί τού $H \times K$.

Πράγματι, $\forall (h,k) \in H \times K$, το $((h,k),(h,k))$ ανήκει προφανώς στη ρ, αφού $hk = hk$, και γι' αυτό η ρ είναι ανακλαστική. Όταν $((h,k),(\overline{h},\overline{k})) \in \rho$, τότε είναι επίσης προφανές ότι $((\overline{h},\overline{k}),(h,k)) \in \rho$, αφού $\overline{h}\overline{k} = hk$, και γι' αυτό η ρ είναι συμμετρική. Τέλος, όταν $((h,k),(\overline{h},\overline{k})) \in \rho$ και $((\overline{h},\overline{k}),(\overline{\overline{h}},\overline{\overline{k}})) \in \rho$, τότε και $((h,k),(\overline{\overline{h}},\overline{\overline{k}})) \in \rho$, αφού από $hk = \overline{h}\overline{k}$ και $\overline{h}\overline{k} = \overline{\overline{h}}\overline{\overline{k}}$, έπεται $hk = \overline{\overline{h}}\overline{\overline{k}}$, και γι' αυτό η ρ είναι συμμετρική.

Για κάθε $(h,k) \in H \times K$ θεωρούμε την αντίστοιχη, ως προς ρ, κλάση ισοδυναμίας $[(h,k)] = \{(\overline{h},\overline{k}) \mid (\overline{h},\overline{k}) \in H \times K, hk = \overline{h}\overline{k}\}$. Επειδή το $H \times K$ είναι πεπερασμένο, συμπεραίνουμε ότι το σύνολο $(H \times K)/\rho$ των κλάσεων ισοδυναμίας είναι επίσης πεπερασμένο. Ας πούμε ότι $(H \times K)/\rho = \{[(h_1,k_1),(h_2,k_2),\ldots(h_n,k_n)]\}$. Το $(H \times K)/\rho$ είναι μια διαμέριση τού $H \times K$ και επομένως

$$|H \times K| = \sum_{i=1}^{n} |[(h_i,k_i)]|, \qquad (*)$$

όπου $|H \times K|$, αντίστοιχα $|[(h_i,k_i)]|$, είναι το πλήθος των στοιχείων τού $H \times K$, αντίστοιχα τής κλάσης $[(h_i,k_i)]$.

Για κάθε $[(h,k)] \in H \times K$, η αντιστοιχία $H \bigcap K \to [(h,k)], \alpha \mapsto (h\alpha, \alpha^{-1}k)$ είναι μια απεικόνιση, αφού το $h\alpha \in H$, το $\alpha^{-1}k \in K$ και το $h\alpha\alpha^{-1}k = hk$. Η απεικόνιση είναι προφανώς ενριπτική, αφού όταν $(h\alpha, \alpha^{-1}k) = (h\beta, \beta^{-1}k), \alpha, \beta \in H \bigcap K$, τότε $\alpha = \beta$. Ισχυριζόμαστε ότι η απεικόνιση είναι και επιρριπτική. Πράγματι, όταν $(\overline{h},\overline{k}) \in [(h,k)]$, τότε $hk = \overline{h}\overline{k}$. Επομένως, το στοιχείο $\alpha := h^{-1}\overline{h} = k\overline{k}^{-1}$ ανήκει στην τομή $H \bigcap K$ και ισχύει ότι $(\overline{h},\overline{k}) = (h\alpha, \alpha^{-1}k)$. Άρα, η απεικόνιση είναι μια αμφίρριψη. Συνεπώς, $\forall (h,k) \in H \times K$, το πλήθος $|[(h,k)]|$ τής κλάσης $[(h,k)]$ ισούται με την τάξη $[H \bigcap K:1]$.

Παρατηρούμε ότι η απεικόνιση $(H \times K)/\rho \to HK, [(h,k)] \mapsto hk$ είναι ανεξάρτητη από τον αντιπρόσωπο (h,k) τής κλάσης $[(h,k)]$, (με άλλα λόγια είναι καλά ορισμένη) και ενριπτική («$1-1$»), αφού $[(h,k)] = [(\overline{h},\overline{k})] \Leftrightarrow hk = \overline{h}\overline{k}$. Επιπλέον, επειδή η συγκεκριμένη απεικόνιση είναι προφανώς επιρριπτική, συμπεραίνουμε ότι είναι μια αμφίρριψη και γι' αυτό το πλήθος n τού $(H \times K)/\rho$ συμπίπτει με το $|HK|$.

Έτσι, ο τύπος (*) που δίνει το πλήθος των στοιχείων τού $H \times K$ παίρνει τη μορφή:

$$|H \times K| = n[(h,k)] = |HK|[H \bigcap K:1],$$

όπου $[(h,k)]$ είναι οποιαδήποτε κλάση.

Συνεπώς, $|HK| = |H \times K|/[H \bigcap K : 1]$ και αφού $|H \times K| = |H||K| = [H:1][K:1]$, καταλήγουμε στον ισχυρισμό τού θεωρήματος. □

Για μια άλλη απόδειξη τού ανωτέρω θεωρήματος, η οποία προκύπτει ως εφαρμογή τής δράσης μιας ομάδας επί ενός συνόλου, βλ. Πρόταση 2.3.9.

Πόρισμα 1.4.18. *Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι $K \leq G$ είναι μια υποομάδα της με τάξη $[K:1] = [G:1]/2$. Τότε για κάθε υποομάδα H τής G θα ισχύει ή ότι $H \leq K$ ή ότι $[H \bigcap K : 1] = [H:1]/2$.*

Μάλιστα, στη δεύτερη περίπτωση ισχύει το εξής: Αν $g \in H \backslash K$, τότε $H = (K \bigcap H) \bigcup g(K \bigcap H)$ με $(K \bigcap H) \bigcap g(K \bigcap H)) = \emptyset$.

Απόδειξη. Όταν η H δεν είναι υποομάδα τής K, τότε για κάθε $g \in H \setminus K$, έχουμε ότι $g \notin K \bigcap H$ και ως εκ τούτου $(K \bigcap H) \bigcap g(K \bigcap H)) = \emptyset$, αφού οι αριστερές πλευρικές κλάσεις $g(K \bigcap H)$ και $e_G(K \bigcap H) = K \bigcap H$ τής υποομάδας $K \bigcap H$ στην G είναι διαφορετικές. Το πλήθος $|gK \bigcup K|$ των στοιχείων τού συνόλου $gK \bigcup K$ ισούται με $2[K:1] = [G:1]$ και επειδή $gK \bigcup K \subseteq HK$, συμπεραίνουμε ότι $HK = G$. Τώρα από τον τύπο τού Θεωρήματος 1.4.17, προκύπτει:

$$[G:1][H \bigcap K : 1] = [H:1][K:1] = \frac{[H:1][G:1]}{2} \Rightarrow [H \bigcap K : 1] = \frac{[H:1]}{2}.$$

Επομένως, ο δείκτης τής $H \bigcap K$ στην H ισούται με 2 και η H είναι η ένωση των αριστερών πλευρικών κλάσεων $H \bigcap K$ και $g(H \bigcap K)$, για κάθε $g \in H \setminus H \bigcap K = H \setminus K$. □

Θεώρημα 1.4.19. *Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H, K είναι δύο υποομάδες της.*

(α′) *Αν οι δείκτες $[G:H]$ και $[G:K]$ των H και K είναι πεπερασμένοι, τότε και ο δείκτης τής τομής $H \bigcap K$ είναι πεπερασμένος και μάλιστα $[G : H \bigcap K] \leq [G:H][G:K]$.*

(β′) *Αν επιπλέον, οι $[G:H]$ και $[G:K]$ είναι σχετικώς πρώτοι αριθμοί, τότε $[G : H \bigcap K] = [G:H][G:K]$.*

Απόδειξη. (α′) Έστω ότι $G/\rho_{\ell,H}$, $G/\rho_{\ell,K}$ και αντιστοίχως $G/\rho_{\ell,H\bigcap K}$ είναι τα σύνολα των αριστερών πλευρικών κλάσεων στην G των υποομάδων H, K και αντιστοίχως $H \bigcap K$.
Η αντιστοιχία $G/\rho_{\ell,H\bigcap K} \to (G/\rho_{\ell,H}) \times (G/\rho_{\ell,K}), g(H \bigcap K) \to (gH, gK)$ είναι μια καλά ορισμένη ενριπτική απεικόνιση, αφού

$$\begin{aligned}\forall \alpha, \beta \in G :\ \alpha(H \bigcap K) = \beta(H \bigcap K) \Leftrightarrow \beta^{-1}\alpha \in H \bigcap K \Leftrightarrow \beta^{-1}\alpha \in H \text{ και } \beta^{-1}\alpha \in K \Leftrightarrow \\ \alpha H = \beta H \text{ και } \alpha K = \beta K \Leftrightarrow (\alpha H, \alpha K) = (\beta H, \beta K).\end{aligned}$$

Επειδή το πλήθος των στοιχείων τού συνόλου $(G/\rho_{\ell,H}) \times (G/\rho_{\ell,K})$ είναι πεπερασμένο, αφού ισούται με $[G:H][G:K]$, συμπεραίνουμε ότι και το $G/\rho_{\ell,H\bigcap K}$ είναι ένα πεπερασμένο σύνολο. Άρα, ο δείκτης $[G : H \bigcap K]$ είναι πεπερασμένος και είναι $\leq [G:H][G:K]$.

(β′) Επειδή η $H \bigcap K$ είναι υποομάδα των H, K και αφού ο δείκτης $[G : H \bigcap K]$ είναι πεπερασμένος, συμπεραίνουμε ότι οι $[G:H]$ και $[G:K]$ είναι διαιρέτες τού $[G : H \bigcap K]$, διότι $[G : H\bigcap K] = [G : H][H : H\bigcap K]$ και $[G : H\bigcap K] = [G : K][K : H\bigcap K]$, βλ. Άσκηση Α45. Τότε όμως και το ελάχιστο κοινό πολλαπλάσιο των σχετικώς πρώτων αριθμών $[G : H]$ και $[G : K]$, το οποίο ισούται με $[G : H][G : K]$, είναι επίσης διαιρέτης τού $[G : H\bigcap K]$. Όμως από το (α′) γνωρίζουμε ότι $[G : H\bigcap K] \leq [G : H][G : K]$. Άρα, $[G : H\bigcap K] = [G : H][G : K]$. □

Ασκήσεις στις πλευρικές Κλάσεις και το Θεώρημα Lagrange

Λυμένες Ασκήσεις

Α 42. Να ευρεθούν όλες οι υποομάδες τής συμμετρικής ομάδας $(S_3, \circ)$.

Λύση. Υπενθυμίζουμε ότι ο πίνακας πράξης τής $(S_3, \circ)$, βλ. Παράδειγμα 4(ε′), είναι ο εξής:

$\circ$	Id_3	τ_1	τ_2	τ_3	ρ	σ
Id_3	Id_3	τ_1	τ_2	τ_3	ρ	σ
τ_1	τ_1	Id_3	ρ	σ	τ_2	τ_3
τ_2	τ_2	σ	Id_3	ρ	τ_3	τ_1
τ_3	τ_3	ρ	σ	Id_3	τ_1	τ_2
ρ	ρ	τ_3	τ_1	τ_2	σ	Id_3
σ	σ	τ_2	τ_3	τ_1	Id_3	ρ

Το Θεώρημα Lagrange προλέγει ότι οποιαδήποτε υποομάδα τής S_3 οφείλει να έχει τάξη έναν διαιρέτη τής τάξης $[S_3 : 1] = 6$. Συνεπώς, αν $H \leq S_3$, τότε η τάξη $[H : 1] \in \{1, 2, 3, 6\}$. Η S_3 έχει τάξη 6 και η $\{\mathrm{Id}_3\}$ έχει τάξη 1. Προφανώς, δεν υπάρχουν άλλες υποομάδες τάξης 6 ή 1.

Θα δείξουμε ότι για $i = 1, 2, 3$, κάθε κυκλική υποομάδα $\langle\tau_i\rangle = \{\tau_i^z \mid z \in \mathbb{Z}\}$ έχει τάξη 2. Παρατηρούμε ότι για κάθε $i = 1, 2, 3$ το σύνολο $\{\mathrm{Id}_3, \tau_i\}$ είναι μια υποομάδα τής S_3, επειδή είναι πεπερασμένο και κλειστό ως προς την πράξη τής S_3. Το $\{\mathrm{Id}_3, \tau_i\}$ περιέχεται στην $\langle\tau_i\rangle$, η οποία είναι η μικρότερη υποομάδα που περιέχει το τ_i. Επομένως, $\{\mathrm{Id}_3, \tau_i\} = \langle\tau_i\rangle$.

Η κυκλική υποομάδα $\langle\rho\rangle = \{\rho^z \mid z \in \mathbb{Z}\}$ έχει τάξη 3. Επιχειρηματολογούμε όπως προηγούμενα. Το σύνολο $\{\mathrm{Id}_3, \rho, \sigma\}$ είναι μια υποομάδα τής S_3, η οποία περιέχεται στην $\langle\rho\rangle$. Επομένως, $\{\mathrm{Id}_3, \rho, \sigma\} = \langle\rho\rangle$. Τέλος εντελώς ανάλογα αποδεικνύουμε ότι $\langle\sigma\rangle = \langle\rho\rangle$, αφού $\rho^2 = \sigma$.

Θα δείξουμε τώρα ότι δεν υπάρχουν άλλες υποομάδες τής S_3 εκτός από τις S_3, $\{\mathrm{Id}_3\}$, $\langle\tau_i\rangle, i = 1, 2, 3$ και $\langle\rho\rangle = \langle\sigma\rangle$.

Κάθε υποομάδα H τής S_3 με $H \neq \{\mathrm{Id}_3\}, S_3$ πρέπει να είναι τάξης ή 2 ή 3. Αν περιέχει το ρ ή το $\rho^2 = \sigma$, τότε οφείλει να περιέχει και την κυκλική υποομάδα $\langle\rho\rangle = \langle\sigma\rangle$, η οποία είναι τάξης 3. Άρα, $H = \langle\rho\rangle$. Αν περιέχει δύο στοιχεία $\tau_i, \tau_j, 1 \leq i, j \leq 3$ με $i \neq j$, τότε περιέχει και το γινόμενο $\tau_i \circ \tau_j$, το οποίο είναι διαφορετικό από τα τ_i, τ_j και Id_3. Επιπλέον, επειδή η H είναι υποομάδα τής S_3, πρέπει να περιέχει και το ταυτοτικό στοιχείο Id_3. Όμως έτσι περιέχει τουλάχιστον τέσσερα στοιχεία, αυτό είναι αδύνατο, αφού $[H : 1] \leq 3$. Η μοναδική περίπτωση που απομένει είναι να περιέχει η H ακριβώς ένα από τα τ_i, $i = 1, 2, 3$, τότε βέβαια $H = \langle\tau_i\rangle$, $i = 1, 2, 3$.

Α 43. Έστω ότι $(\mathbb{Z}, +)$ είναι η ομάδα των ακέραιων αριθμών και ότι $n\mathbb{Z} = \langle n \rangle$ είναι η κυκλική υποομάδα που παράγεται από τον φυσικό $n > 1$. Να δειχθεί ότι

$$\forall a, b \in \mathbb{Z} : a + \langle n \rangle = b + \langle n \rangle \Leftrightarrow a \equiv b \bmod (n).$$

Να συμπεράνετε ότι η σχέση ισοδυναμίας $\rho_{\ell,\langle n \rangle}$, η οποία επάγεται επί τού $\mathbb{Z}$ από την υποομάδα $\langle n \rangle$, ισούται με τη σχέση ισοτιμίας κατά μόδιο n επί τού $\mathbb{Z}$.

Λύση. Έχουμε:

$$\forall a, b \in \mathbb{Z} : a + \langle n \rangle = b + \langle n \rangle \Leftrightarrow a - b \in \langle n \rangle \Leftrightarrow \exists k \in \mathbb{Z} : a - b = nk \Leftrightarrow a \equiv b \bmod (n).$$

Επομένως, το $(a, b) \in \mathbb{Z}$ ανήκει στη $\rho_{\ell,\langle n \rangle}$, αν και μόνο αν, ο n διαιρεί τη διαφορά $a - b$, αν και μόνο αν, οι a, b είναι ισότιμοι mod n.

Α 44. Έστω ότι $(G, \star)$ είναι μια ομάδα, ότι H και K είναι υποομάδες τής G και ότι a είναι ένα στοιχείο τής G. Το σύνολο

$$HaK = \{hak \mid h \in H, k \in K\}$$

ονομάζεται μια *διπλή πλευρική κλάση*.
Να δειχθούν τα εξής:

(α′) Η G είναι ένωση διπλών πλευρικών κλάσεων.

(β′) Δύο διπλές πλευρικές κλάσεις ή έχουν κενή τομή ή συμπίπτουν.

(γ′) Οποιαδήποτε διπλή πλευρική κλάση HaK είναι μια ένωση αριστερών πλευρικών κλάσεων τής K και μια ένωση δεξιών πλευρικών κλάσεων τής H.

(δ′) Αν οι τάξεις των υποομάδων H και K είναι πεπερασμένες, τότε να δειχθεί ότι το πλήθος των στοιχείων τής διπλής πλευρικής κλάσης HaK ισούται με

$$|HaK| = \frac{[H : 1[K : 1]}{[H \bigcap aKa^{-1} : 1]}$$

Λύση. (α′) και (β′) Θεωρούμε τη σχέση $\rho_{H\times K} = \{(a, b) \in G \times G \mid \exists h \in H, k \in K$ με $b = hak\}$. Προτείνουμε να αποδείξει μόνος του ο αναγνώστης ότι η $\rho_{H\times K}$ είναι μια σχέση ισοδυναμίας. Για κάθε $a \in G$, η αντίστοιχη κλάση ισοδυναμίας ως προς $\rho_{H\times K}$, είναι προφανώς η $[a] = \{hak \mid h \in H, k \in K\}$. Το σύνολο $G/\rho_{H\times K}$ των κλάσεων διαμερίζει την G και από αυτό προκύπτει η αλήθεια των ισχυρισμών (α′) και (β′).

(γ′) Έχουμε: $\forall a \in G : HaK = \bigcup_{h\in H}(ha)K$ και $HaK = \bigcup_{k\in K} H(ak)$.

(δ′) Είναι εύκολη η διαπίστωση ότι η αντιστοιχία $HaK \to HaKa^{-1}, hak \mapsto haka^{-1}$ είναι μια καλά ορισμένη αμφιρριπτική, δηλαδή «1 − 1» και «επί», απεικόνιση. Το σύνολο aKa^{-1} είναι μια υποομάδα τής G, συζυγής προς την K και $|HaK| = |H(aKa^{-1})|$. Τώρα, από το Θεώρημα 1.4.17 προκύπτει:

$$|HaK| = |H(aKa^{-1})| = \frac{[H : 1][aKa^{-1} : 1]}{[H \bigcap aKa^{-1} : 1]}.$$

Α 45. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H, K είναι υποομάδες τής G με $K \leq H$. Αν ο δείκτης $[G : K]$ είναι πεπερασμένος, τότε να δειχθεί ότι και οι δείκτες $[G : H]$, $[H : K]$ είναι πεπερασμένοι και μάλιστα ότι ισχύει $[G : K] = [G : H][H : K]$.

Λύση. Θεωρούμε τις σχέσεις ισοδυναμίας ρ_K και ρ_H επί τής G, που προκύπτουν από τις υποομάδες K και H τής G, καθώς και τη σχέση ισοδυναμίας ρ'_K επί τής H, που προκύπτει από το ότι η K είναι και υποομάδα τής H. Έστω G/ρ_K, G/ρ_H και αντίστοιχα H/ρ'_K τα σύνολα των αριστερών πλευρικών κλάσεων τής K στην G, τής H στην G και αντίστοιχα τής K στην H.

Από την υπόθεση γνωρίζουμε ότι ο δείκτης $[G : K]$ ισούται με κάποιον $r \in \mathbb{N}$. Επομένως, το σύνολο G/ρ_K είναι πεπερασμένο και έχει r το πλήθος στοιχεία. Έστω $hK, h \in H$ οποιαδήποτε αριστερή πλευρική κλάση τής K στην H, δηλαδή οποιοδήποτε στοιχείο τού συνόλου H/ρ'_K. Αφού η hK είναι επίσης και αριστερή πλευρική κλάση τής K στην G, διότι $H \leq G$, συμπεραίνουμε ότι $hK \in G/\rho_K$ και επομένως $H/\rho'_K \subseteq G/\rho_K$. Άρα, το H/ρ'_K είναι ένα πεπερασμένο σύνολο, ο $[H : K] = t \in \mathbb{N}$ και το $H/\rho'_K = \{h_1K, h_2K, \ldots, h_tK\}$, όπου $\forall j, 1 \leq j \leq t, h_j \in H$.

Τώρα θα δείξουμε ότι το G/ρ_H είναι επίσης ένα πεπερασμένο σύνολο. Πράγματι, η αντιστοιχία $G/\rho_K \to G/\rho_H, gK \mapsto gH$ είναι μια καλά ορισμένη απεικόνιση, αφού όταν $g_1K = g_2K, g_1, g_2 \in K$, τότε $g_2^{-1}g_1 \in K \leq H$ και συνεπώς $g_1H = g_2H$. Προφανώς, αυτή η απεικόνιση είναι επιρριπτική, διότι κάθε gH έχει ως προεικόνα το gK. Επειδή το G/ρ_K είναι πεπερασμένο, έπεται ότι και το G/ρ_H είναι επίσης πεπερασμένο. Επομένως, ο $[G : H] = p \in \mathbb{N}$ και το $G/\rho_H = \{g_1H, g_2H, \ldots, g_pH\}$, όπου $\forall i, 1 \leq i \leq p, g_i \in G$.

Έστω ότι $g_{i_1}H, g_{i_2}H, 1 \leq i_1, i_2 \leq p, i_1 \neq i_2$ είναι δύο αριστερές πλευρικές κλάσεις από το G/ρ_H και ότι $h_{j_1}K, h_{j_2}K, 1 \leq j_1, j_2 \leq t, j_1 \neq j_2$ είναι δύο αριστερές πλευρικές κλάσεις από το H/ρ_K. Ισχυριζόμαστε, ότι

$$g_{i_1}h_{j_1}K = g_{i_2}h_{j_2}K \Leftrightarrow g_{i_1}H = g_{i_2}H \text{ και } h_{j_1}K = h_{j_2}K$$

Πράγματι, όταν $g_{i_1}H = g_{i_2}H$, τότε τα g_{i_1} και g_{i_2} είναι στοιχεία τής ίδιας αριστερής πλευρικής κλάσης τής H στην G. Επομένως, $g_{i_1} = g_{i_2}$, αφού τα στοιχεία τού συνόλου $G/\rho_H = \{g_1H, g_2H, \ldots, g_pH\}$ είναι σαφώς διακεκριμένα. Παρόμοια, από $h_{j_1}K = h_{j_2}K$, συμπεραίνουμε ότι $h_{j_1} = h_{j_2}$. Άρα, $g_{i_1}h_{j_1}K = g_{i_2}h_{j_2}K$.
Αντίστροφα, όταν $g_{i_1}h_{j_1}K = g_{i_2}h_{j_2}K$ (*), τότε $g_{i_1}h_{j_1}H = g_{i_2}h_{j_2}H$, αφού $K \leq H$. Ακόμα επειδή τα $h_{j_1}, h_{j_2} \in H$, προκύπτει ότι $h_{j_1}H = H = h_{j_2}H$ και ως εκ τούτου, $g_{i_1}H = g_{i_2}H$. Όπως προηγούμενα, συμπεραίνουμε ότι $g_{i_1} = g_{i_2}$. Τώρα, η (*) δίνει $g_{i_1}^{-1}g_{i_1}h_{j_1}K = g_{i_1}^{-1}g_{i_1}h_{j_2}K$, δηλαδή $h_{j_1}K = h_{j_2}K$.

Άρα, το σύνολο $\mathcal{T} = \{g_ih_jK \mid i = 1, 2, \ldots, p, j = 1, 2, \ldots, t\}$ αποτελείται από $p \cdot t$ διαφορετικές αριστερές πλευρικές κλάσεις τής K στην G. Προφανώς, το $\mathcal{T} \subseteq G/\rho_K$.

Θα δείξουμε ότι το G/ρ_K είναι υποσύνολο τού $\mathcal{T}$. Έστω ότι $g \in G$ και ότι $gK \in G/\rho_K$ είναι η αντίστοιχη αριστερή πλευρική κλάση τής K στην G. Θεωρούμε την αντίστοιχη πλευρική κλάση $gH \in G/\rho_H$ τής H στην G. Προφανώς, υπάρχει κάποιος δείκτης $i, 1 \leq i \leq p$ με $gH = g_iH$. Τώρα το $g_i^{-1}g$ ανήκει στην H και η αριστερή πλευρική κλάση $g_i^{-1}gK$ τής K στην H ισούται με κάποιο από τα στοιχεία τού συνόλου H/ρ'_K. Επομένως, υπάρχει κάποιος δείκτης $j, 1 \leq j \leq t$ με $g_i^{-1}gK = h_jK$ και γι' αυτό $gK = g_ih_jK$. Αφού $g_ih_jK \in \mathcal{T}$, συμπεραίνουμε ότι $G/\rho_K \subseteq \mathcal{T}$. Έτσι τελικά προκύπτει ότι $G/\rho_K = \mathcal{T}$ και γι' αυτό $r = p \cdot t$. Με άλλα λόγια, $[G:K] = [G:H][H:K]$.

Α 46. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι H και K είναι δύο υποομάδες της. Αν $[H:1] > \sqrt{[G:1]}$ και $[K:1] > \sqrt{[G:1]}$, τότε να δειχθεί ότι $H \bigcap K \neq \{e_g\}$.

Λύση. Είναι

$$[G:1] \geq |HK| = \frac{[H:1][K:1]}{[H \bigcap K:1]} > \frac{\sqrt{[G:1]}\sqrt{[G:1]}}{[H \bigcap K:1]} = \frac{[G:1]}{[H \bigcap K:1]}.$$

Επομένως, $[H \bigcap K:1] > 1$.

Α 47. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης pq, όπου οι p, q είναι πρώτοι αριθμοί με $p > q$. Να δειχθεί ότι η G διαθέτει το πολύ μια υποομάδα τάξης p.
(Αργότερα θα δούμε ότι η G έχει πάντοτε και μια υποομάδα τάξης p και μια υποομάδα τάξης q, βλ. Θεώρημα 2.3.11.)

Λύση. Έστω ότι οι H και H' είναι δύο υποομάδες τής G τάξης p. Από την προηγούμενη άσκηση έχουμε $H \bigcap H' \neq \{e_G\}$, διότι $p > \sqrt{pq} = \sqrt{[G:1]}$. Το Θεώρημα Lagrange πληροφορεί ότι η τάξη $[H \bigcap H':1] \neq 1$ είναι διαιρέτης τής τάξης $[H:1] = p$, αφού $H \bigcap H' \leq H$. Επομένως, $[H \bigcap H' : 1] = p$ και $H \bigcap H' = H$. Εντελώς ανάλογα συμπεραίνουμε ότι $H \bigcap H' = H'$.

Προτεινόμενες Ασκήσεις

ΠΑ 44. Να ευρεθούν όλες οι υποομάδες τής διεδρικής ομάδας $(D_5, \circ)$ και για καθεμιά από αυτές, να προσδιοριστούν οι αντίστοιχες αριστερές και δεξιές πλευρικές κλάσεις στην D_5. Να επαναλάβετε το ερώτημα στην περίπτωση τής διεδρικής ομάδας $(D_7, \circ)$.

ΠΑ 45. Έστω ότι $(G, \star)$ είναι μια ομάδα, ότι H είναι μια υποομάδα της και ότι a είναι ένα στοιχείο τής G. Να δειχθεί ότι $a^{-1}H = (Ha)^{-1}$.

ΠΑ 46. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H είναι μια υποομάδα της με την ιδιότητα: $\forall a, b \in G$ με $Ha \neq Hb \Rightarrow aH \neq bH$. Να δειχθεί ότι $\forall g \in G : gHg^{-1} \subseteq H$.

ΠΑ 47. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H είναι μια υποομάδα της. Αν η H είναι πεπερασμένως παραγόμενη και ο δείκτης $[G:H]$ είναι πεπερασμένος, τότε να δειχθεί ότι και η G είναι πεπερασμένως παραγόμενη.

ΠΑ 48. Να δειχθεί ότι οι μοναδικές υποομάδες μιας ομάδας $(G, \star)$ τάξης p, όπου ο p είναι πρώτος αριθμός, είναι οι G και $\{e_G\}$.

ΠΑ 49. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H είναι μια υποομάδα τής G με $[G:H] = 2$. Να δειχθεί ότι για κάθε $a \in G$, το a^2 είναι στοιχείο τής H.

ΠΑ 50. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H είναι μια υποομάδα της. Να δειχθεί ότι η διαφορά $G \setminus H$ είναι ένα πεπερασμένο σύνολο, αν και μόνο αν, είτε $[G:1] < \infty$ είτε $H = G$.

ΠΑ 51. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι H, K είναι δύο υποομάδες της, όπου οι δείκτες $[G:H]$ και $[G:K]$ είναι σχετικώς πρώτοι αριθμοί. Να δειχθεί ότι $G = HK$.

1.5 Κυκλικές Ομάδες, Τάξη Στοιχείου

Οι ομάδες με την απλούστερη δομή είναι αυτές που αποτελούνται ακριβώς από τις ακέραιες δυνάμεις ενός στοιχείου τους. Έτσι οδηγούμαστε στη έννοια τής κυκλικής ομάδας που συναντήσαμε στην Άσκηση Α30(β′). Επαναλαμβάνουμε τον ορισμό:

Ορισμός 1.5.1. Μια ομάδα $(G, \star)$ ονομάζεται *κυκλική*, όταν υπάρχει κάποιο $a \in G$ με $\langle a \rangle = G$.

Το στοιχείο a ονομάζεται ένας *γεννήτορας* τής κυκλικής ομάδας $\langle a \rangle = G$.

Παράδειγμα 1.5.2. (α′) Η ομάδα των ακεραίων $(\mathbb{Z}, +)$ είναι κυκλική με γεννήτορα τον ακέραιο 1. Πράγματι, κάθε $z \in \mathbb{Z}$ ισούται με $z \cdot 1$ και γι' αυτό $\langle 1 \rangle = \mathbb{Z}$. (Προσέξτε ότι εδώ η πράξη είναι η συνήθης πρόσθεση και ότι χρησιμοποιούμε την προσθετική γραφή.) Επιπλέον, παρατηρούμε ότι και ο $-1 \in \mathbb{Z}$ είναι επίσης γεννήτορας, αφού $\forall z \in \mathbb{Z}$ είναι $z = (-z) \cdot (-1)$. Η τάξη $[\mathbb{Z} : 1]$ ισούται με ∞.

(β′) Η ομάδα $(\mathbb{Z}_n, +)$ των κλάσεων ισοτιμίας mod $n, n \in \mathbb{N}$, βλ. Παράδειγμα 1.2.4(δ′), είναι κυκλική. Η κλάση $[1]_n$ είναι γεννήτορας τής $\mathbb{Z}_n$, αφού $[z]_n = z \cdot [1]_n$. Επομένως $\langle [1]_n \rangle = \mathbb{Z}_n$. Η κλάση $[n-1]_n = [-1]_n$ είναι επίσης ένας γεννήτορας τής $\mathbb{Z}_n$. Η τάξη $[\mathbb{Z}_n : 1]$ ισούται με n.

(γ′) Η ομάδα $(\mathcal{E}_n, \cdot)$ των n-οστών ριζών τής μονάδας, βλ. Άσκηση Α27, είναι κυκλική. Πράγματι, κάθε $z \in \mathcal{E}_n$, δηλαδή κάθε $z \in \mathbb{C}^\star$ με $z^n = 1$, εκφράζεται ως $z = \cos(2\kappa\pi/n) + i\sin(2\kappa\pi/n), 1 \leq \kappa \leq n$. Ο μιγαδικός $\varepsilon_n = (\cos 2\pi/n) + i(\sin 2\pi/n)$ είναι ένας γεννήτορας τής $\mathcal{E}_n$, αφού για κάθε $\kappa \in \mathbb{N}$ είναι $(\varepsilon_n)^\kappa = (\cos 2\kappa\pi/n) + i(\sin 2\kappa\pi/n)$. Η τάξη $[\mathcal{E}_n : 1]$ ισούται με n, αφού το πλήθος των λύσεων τής εξίσωσης $x^n = 1$ στο $\mathbb{C}$ είναι ακριβώς n. Κάθε γεννήτορας τής $\mathcal{E}_n$ ονομάζεται μια *πρωταρχική n-οστή ρίζα τής μονάδας*.

Συνεπώς, υπάρχουν κυκλικές ομάδες άπειρης τάξης και επίσης για κάθε $n \in \mathbb{N}$, υπάρχουν κυκλικές ομάδες τάξης n.

Παρατήρηση 1.5.3. Κάθε κυκλική ομάδα $(G, \star)$ είναι αβελιανή (μεταθετική). Πράγματι, αφού η G είναι κυκλική, υπάρχει $a \in G$ με $\langle a \rangle = G$. Όταν $g, h \in G$, τότε $\exists i, j \in \mathbb{Z}$ με $g = a^i, h = a^j$ και είναι

$$gh = a^i a^j = a^{i+j} = a^{j+i} = a^j a^i = hg.$$

Επομένως, η G είναι αβελιανή ομάδα.

Παράδειγμα 1.5.4. (α′) Έστω $(S_X, \circ)$ η συμμετρική ομάδα ενός συνόλου $X \neq \emptyset$. Η S_X είναι κυκλική, αν και μόνο αν, $|X| = 1$ ή 2. Από την Άσκηση Α3 γνωρίζουμε ότι όταν $|X| \geq 3$, τότε η S_X δεν είναι αβελιανή και επομένως δεν είναι ούτε κυκλική. Όταν $|X| = 1$ ή 2, τότε η τάξη $[S_X : 1]$ είναι αντίστοιχα 1 ή 2. Προφανώς, κάθε ομάδα τάξης ≤ 2 είναι κυκλική.

(β′) Η ομάδα $(\mathbb{Q}, +)$ των ρητών δεν είναι κυκλική. Μάλιστα, θα δείξουμε το εξής ισχυρότερο: Η $(\mathbb{Q}, +)$ δεν είναι πεπερασμένως παραγόμενη. Ας υποθέσουμε ότι υπάρχει κάποιο πεπερασμένο σύνολο $M = \{q_1, q_2, \dots, q_t \mid q_i \in \mathbb{Q}, 1 \le i \le t\}$ με $\langle M \rangle = \mathbb{Q}$ και έστω ότι $n \in \mathbb{N}$ είναι κάποιος φυσικός[14] με $nq_i = z_i \in \mathbb{Z}, \forall i, 1 \le i \le t$. Θεωρούμε την κυκλική υποομάδα $\langle 1/n \rangle \le \mathbb{Q}$. Για κάθε $i, 1 \le i \le t$, ο ρητός $q_i = z_i(1/n)$ ανήκει στην $\langle 1/n \rangle$. Επομένως, το M είναι υποσύνολο τής $\langle 1/n \rangle$ και ως εκ τούτου, $\mathbb{Q} = \langle M \rangle \le \langle 1/n \rangle$. Συνεπώς, $\mathbb{Q} = \langle 1/n \rangle$. Αυτό όμως είναι άτοπο, διότι ο ρητός $1/2n \notin \langle 1/n \rangle$.

Από το προηγούμενο παράδειγμα συμπεραίνουμε ότι κάθε αβελιανή ομάδα δεν είναι απαραιτήτως κυκλική. Ωστόσο, υπάρχουν ακόμα και μη αβελιανές ομάδες, που κάθε γνήσια υποομάδα τους είναι κυκλική. Επί παραδείγματι, κάθε γνήσια υποομάδα τής $(S_3, \circ)$ είναι κυκλική, βλ. Άσκηση Α42. Αυτό μάλιστα δικαιολογείται και από το ότι οποιαδήποτε γνήσια και μη τετριμμένη υποομάδα τής S_3 οφείλει να έχει ως τάξη έναν από τους διαιρέτες 2 ή 3 τού $6 = [S_3 : 1]$. Οι αριθμοί 2 και 3 είναι πρώτοι και η επόμενη πρόταση επιτρέπει να συμπεράνουμε ότι οι γνήσιες μη τετριμμένες υποομάδες τής S_3 είναι κυκλικές.

Πρόταση 1.5.5. *Κάθε ομάδα $(G, \star)$ με τάξη έναν πρώτο αριθμό p είναι κυκλική και κάθε στοιχείο της $a \neq e_G$ είναι ένας γεννήτοράς της.*

Απόδειξη. Αφού $p \ge 2$, υπάρχει κάποιο $a \in G$ με $a \neq e_G$. Θεωρούμε την κυκλική υποομάδα $\langle a \rangle \le G$. Η τάξη $[\langle a \rangle : 1]$ είναι ≥ 2, διότι $a \neq e_G$. Από το Θεώρημα Lagrange γνωρίζουμε ότι η τάξη $[\langle a \rangle : 1]$ είναι διαιρέτης τού πρώτου p. Επομένως, $[\langle a \rangle : 1] = p = [G : 1]$ και $\langle a \rangle = G$. □

Προσέξτε ότι το πλήθος των γεννητόρων μιας κυκλικής ομάδας πρώτης τάξης p ισούται με $p - 1 = \varphi(p)$, όπου φ είναι η φ–συνάρτηση Euler. Σύντομα θα δούμε, βλ. Πρόταση 1.5.12, ότι το πλήθος των γεννητόρων οποιασδήποτε κυκλικής ομάδας τάξης n ισούται με $\varphi(n)$.

Ορισμός 1.5.6. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι $a \in G$. Ονομάζουμε *τάξη* τού στοιχείου a, την τάξη $[\langle a \rangle : 1]$ τής κυκλικής υποομάδας $\langle a \rangle$ τής G.

Θα συμβολίζουμε την τάξη τού $a \in G$ με $\circ(a)$. Συνεπώς, ή θα είναι $\circ(a) = n \in \mathbb{N}$ ή θα είναι $\circ(a) = \infty$.

Από το Θεώρημα Lagrange έπεται αμέσως ότι

Πρόταση 1.5.7. *Όταν $(G, \star)$ είναι μια ομάδα με τάξη $[G : 1] < \infty$ και a είναι ένα στοιχείο τής G, τότε η τάξη $\circ(a)$ είναι διαιρέτης τής τάξης $[G : 1]$.*

Πόρισμα 1.5.8. *Όταν $(G, \star)$ είναι μια ομάδα με τάξη $[G : 1] < \infty$, τότε για κάθε $a \in G$, είναι $a^{[G:1]} = e_G$.*

Απόδειξη. Από την Πρόταση 1.5.7 προκύπτει ότι για κάθε $a \in G$, είναι $[G : 1] = \circ(a)\lambda$, όπου $\lambda \in \mathbb{N}$. Συνεπώς, έχουμε $a^{[G:1]} = (a^{\circ(a)})^{\lambda} = e_G^{\lambda} = e_G$. □

[14] Υπάρχει πάντοτε ένας τέτοιος φυσικός, (*γιατί;*).

Πόρισμα 1.5.9 (Θεώρημα Fermat). *Για κάθε πρώτο αριθμό p και κάθε ακέραιο αριθμό a, είναι $a^p \equiv a \bmod p$.*

Απόδειξη. Θεωρούμε την ομάδα $(\mathbb{U}_p, \cdot)$ των αντιστρέψιμων κλάσεων ισοτιμίας των ακεραίων mod$p$, βλ. Παράδειγμα 1.2.21. Η τάξη της $[\mathbb{U}_p : 1]$ ισούται με $\varphi(p) = p - 1$. Έστω $a \in \mathbb{Z}$ και $[a]_p \in \mathbb{Z}_p$ η αντίστοιχη κλάση ισοτιμίας mod$p$.

Αν $[a]_p \notin \mathbb{U}_p$, τότε επειδή ο μέγιστος κοινός διαιρέτης των a και p είναι $\neq 1$ και επειδή ο p είναι πρώτος συμπεραίνουμε ότι $a \equiv 0 \bmod p$ και κατόπιν ότι $a^p \equiv 0 \bmod p$. Συνεπώς, $a^p \equiv a \bmod p$.

Αν $[a]_p \in \mathbb{U}_p$, τότε $([a]_p)^{[\mathbb{U}_p:1]} = ([a]_p)^{p-1} = [1]_p$, λόγω τού Πορίσματος 1.5.8. Επομένως, $[a]_p \cdot ([a]_p)^{p-1} = ([a]_p)^p = [a]_p$, δηλαδή $a^p \equiv a \bmod p$. □

Θεώρημα 1.5.10. *Έστω ότι $(G, \star)$ είναι μια ομάδα, ότι $a \in G$ και ότι $M_a = \{m \in \mathbb{N} \mid a^m = e_G\} \subseteq \mathbb{N}$.*

(α′) *Όταν η τάξη $\circ(a)$ είναι ένας φυσικός αριθμός, τότε το M_a είναι $\neq \emptyset$, το $\min M_a$ ισούται με την $\circ(a)$ και το σύνολο των στοιχείων τής $\langle a \rangle$ συμπίπτει με το*

$$\{a^0 = e_G, a, a^2, \ldots, a^{n-1}\}.$$

(β′) *Όταν η τάξη $\circ(a)$ είναι άπειρη, τότε το M_a είναι ίσο με το $\emptyset$ και το σύνολο των στοιχείων τής $\langle a \rangle$ συμπίπτει με το*

$$\{\ldots, a^{-(i+1)}, a^{-i}, \ldots, a^{-2}, a^{-1}, a^0 = e_G, a, a^2, \ldots, a^j, a^{j+1}, \ldots\}.$$

Απόδειξη. (α′) Έστω ότι $[\langle a \rangle : 1] = \circ(a) = n \in \mathbb{N}$. Είναι αδύνατο να είναι όλες οι φυσικές δυνάμεις $a^i, i \in \mathbb{N}$ ανά δύο διαφορετικές, αφού τότε το άπειρου πλήθους σύνολο $\{a^i \mid i \in \mathbb{N}\}$ θα ήταν υποσύνολο τής πεπερασμένης υποομάδας $\langle a \rangle = \{a^z \mid z \in \mathbb{Z}\}$. Επομένως, υπάρχουν $i, j \in \mathbb{N}$ με $i \neq j$ και $a^i = a^j$ ή ισοδύναμα $a^{i-j} = e_G$. Τότε, είναι επίσης $a^{|i-j|} = e_G$ και ο φυσικός $|i - j|$ ανήκει στο M_a. Άρα, το $M_a \neq \emptyset$.

Για να αποδείξουμε ότι το ελάχιστο $\min M_a = n$ τού M_a ισούται με την τάξη $\circ(a) = [\langle a \rangle : 1]$, είναι αρκετό να δείξουμε ότι τα στοιχεία $a^0 = e_G, a, a^2, \ldots, a^{n-1}$ είναι ανά δύο διαφορετικά και ότι το σύνολο των στοιχείων τής $\langle a \rangle$ συμπίπτει με το $\{a^0 = e_G, a, a^2, \ldots, a^{n-1}\}$.

Αν ήταν $a^\ell = a^k$ ή ισοδύναμα $a^{\ell-k} = e_G$, για κάποια ℓ, k με $0 \leq \ell, k \leq n - 1$, τότε εκτελώντας διαίρεση με υπόλοιπο τού $\ell - k$ διά τού n θα προέκυπτε ότι $\ell - k = \lambda n + v$, όπου $0 \leq v \leq n - 1$. Συνεπώς, θα είχαμε

$$e_G = a^{\ell-k} = (a^n)^\lambda a^v = (e_G)^\lambda a^v = a^v.$$

Ο αριθμός v οφείλει να ισούται με 0, αφού διαφορετικά όντας φυσικός θα ανήκε στο M_a και αφού θα ήταν και $\leq n - 1 < n$ θα καταλήγαμε στο άτοπο ότι $v \in M_a$ και $v < n = \min M_a$. Άρα, το $\{a^0 = e_G, a, a^2, \ldots, a^{n-1}\}$ είναι ένα σύνολο από n το πλήθος στοιχεία.

Έστω ότι $x \in \langle a \rangle$, τότε $\exists z \in \mathbb{Z}$ με $x = a^z$. Εκτελώντας διαίρεση με υπόλοιπο τού z διά τού n προκύπτει $z = sn + i$, όπου $0 \leq i \leq n - 1$. Επομένως,

$$x = a^z = (a^n)^s a^i = (e_G)^s a^i = a^i, 0 \leq i \leq n - 1.$$

Άρα, $\langle a\rangle = \{a^0 = e_G, a, a^2, \ldots, a^{n-1}\}$.

(β′) Αν ήταν το $M_a \neq \emptyset$, τότε θεωρώντας το $n = \min M_a$ θα διαπιστώναμε, ακριβώς όπως στις αμέσως προηγούμενες γραμμές, ότι οποιοδήποτε $x \in \langle a\rangle$ θα ήταν ίσο με κάποια από τις δυνάμεις $a^0 = e_G, a, a^2, \ldots, a^{n-1}$ και τότε θα ήταν η $\circ(a) = [\langle a\rangle : 1] < \emptyset$. Αυτό όμως αντίκειται στην υπόθεση. Άρα, $M_a = \emptyset$.

Υπολείπεται η απόδειξη, ότι όταν $i, j \in \mathbb{Z}$ με $i \neq j$, τότε και $a^i \neq a^j$. Πράγματι, αν ήταν $a^i = a^j$, τότε ισοδύναμα θα ήταν $a^{i-j} = e_G$ και έτσι θα ήταν $a^{|i-j|} = e_G$. Τότε όμως θα ήταν το $M_a \neq \emptyset$, αφού το $|i-j|$ θα ανήκε στο M_a. Αυτό όμως είναι άτοπο, αφού μόλις είδαμε ότι $M_a = \emptyset$. Επομένως, όλες οι δυνάμεις a^i καθώς το i διατρέχει το $\mathbb{Z}$ είναι ανά δύο διαφορετικές. □

Το παραπάνω θεώρημα μας πληροφορεί ότι η τάξη ενός στοιχείου a μιας ομάδας $(G, \star)$ ή θα είναι ίση με το ελάχιστο τού συνόλου M_a, όταν $M_a \neq \emptyset$ ή θα είναι ίση με ∞, όταν $M_a = \emptyset$. Συχνά, η συγκεκριμένη ιδιότητα χρησιμοποιείται ως ορισμός για την τάξη τού a.

Πόρισμα 1.5.11. *Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι το στοιχείο $a \in G$ έχει τάξη $\circ(a) = n \in \mathbb{N}$.*

(α′) *Για κάθε $z \in \mathbb{Z}$, είναι*
$$a^z = e_G \Leftrightarrow n \mid z.$$

(β′) *Για κάθε θετικό διαιρέτη d τού n, η τάξη τού $a^{n/d}$ ισούται με d.*

Απόδειξη. (α′)«$\Rightarrow$» Εκτελώντας διαίρεση με υπόλοιπο τού z διά τού n, έχουμε:
$z = \lambda n + v, 0 \le v \le n-1$. Συνεπώς, $e_G = a^z = a^{\lambda n + v} = (a^n)^\lambda + a^v = a^v$. Αφού, η τάξη $\circ(a) = n = \min M_a$, βλ. Θεώρημα 1.5.10, συμπεραίνουμε ότι $v = 0$.
«$\Leftarrow$» Προφανές.
(β′) Παρατηρούμε ότι $(a^{n/d})^d = a^n = e_G$. Έστω $\ell \in \mathbb{N}$ με $(a^{n/d})^\ell = e_G$. Από το αμέσως προηγούμενο πόρισμα προκύπτει ότι ο n είναι διαιρέτης τού $(n/d)\ell$. Έστω ότι $(n/d)\ell = \rho n, \rho \in \mathbb{N}$. Τότε $\ell = \rho d$ και ως εκ τούτου, ο d είναι ο μικρότερος φυσικός με $a^d = e_G$. Αφού, η τάξη $\circ(a^{n/d}) = \min M_{(a^{n/d})}$, βλ. Θεώρημα 1.5.10, έχουμε $\circ(a^{n/d}) = d$. □

Πρόταση 1.5.12. *Έστω ότι $(G, \star)$ είναι μια κυκλική ομάδα τάξης n, ότι a είναι ένας γεννήτοράς της, ότι k είναι ένας φυσικός αριθμός και ότι $\delta = \text{ΜΚΔ}(k, n)$. Τότε*

(α′) $\langle a^k\rangle = \langle a^\delta\rangle$ *και*

(β′) $\circ(a^k) = \circ(a^{n/\delta})$.

(γ′) *Το πλήθος των γεννητόρων τής G, δηλαδή των στοιχείων τάξης n, ισούται με $\varphi(n)$, όπου φ είναι η φ–συνάρτηση Euler.*

Απόδειξη. (α′) Αφού ο δ είναι διαιρέτης τού k, έπεται ότι το a^k ανήκει στην υποομάδα $\langle a^\delta\rangle$ και γι' αυτό $\langle a^k\rangle \subseteq \langle a^\delta\rangle$. Επειδή το δ είναι ο μέγιστος κοινός διαιρέτης των k και n, υπάρχουν $\lambda, \mu \in \mathbb{Z}$ με $\delta = k\lambda + n\mu$. Τώρα, $a^\delta = a^{k\lambda + n\mu} = (a^k)^\lambda (a^n)^\mu = (a^k)^\lambda e_G^\mu = (a^k)^\lambda$. Επομένως, το a^δ ανήκει στην υποομάδα $\langle a^k\rangle$ και συνεπώς $\langle a^\delta\rangle \subseteq \langle a^k\rangle$. Άρα, $\langle a^\delta\rangle = \langle a^k\rangle$.
(β′) Η τάξη τού στοιχείου a^k ισούται με $[\langle a^k\rangle : 1]$. Από το πρώτο μέρος τής πρότασης,

έχουμε ότι $\langle a^k \rangle = \langle a^\delta \rangle$. Επομένως, $\circ(a^k) = \circ(a^\delta)$. Ο δ είναι διαιρέτης τού n. Από το Πόρισμα 1.5.11 προκύπτει ότι $\circ(a^\delta) = n/\delta$.
(γ′) Κάθε στοιχείο g τής $G = \langle a \rangle$ είναι κάποιο από τα ανά δύο διαφορετικά στοιχεία $a^k, 1 \leq k \leq n$, διότι $G = \{a^0 = e_G, a, a^2, \ldots, a^{n-1}\}$ και $a^n = e_G = a^0$. Από το (β′) έχουμε ότι η τάξη τού $g = a^k$ ισούται με n, αν και μόνο αν, $n = n/\delta$, όπου δ είναι ο μέγιστος κοινός διαιρέτης των k και n. Επομένως, $\circ(a^k) = n \Leftrightarrow \delta = 1$. Ως γνωστόν, το πλήθος των $k \in \mathbb{N}, 1 \leq k \leq n$, που είναι σχετικώς πρώτοι προς τον φυσικό n, ισούται με $\varphi(n)$. □

Πρόταση 1.5.13. *Έστω ότι $(G, \star)$ είναι μια κυκλική ομάδα και ότι a είναι ένας γεννήτοράς της.*

(α′) *Όταν $[G : 1] = \infty$, τότε οι μοναδικοί γεννήτορες τής $(G, \star)$ είναι οι a και a^{-1}.*

(β′) *Όταν $[G : 1] = n$, τότε ένα στοιχείο $a^z, z \in \mathbb{Z}$ είναι γεννήτορας τής G, αν και μόνο αν, ο ΜΚΔ$(|z|, n)$ ισούται με 1.*

Απόδειξη. (α′) Προφανώς, ο a^{-1} είναι επίσης γεννήτορας τής G, αφού $\forall z \in \mathbb{Z}$, είναι $a^z = (a^{-1})^{(-z)}$. Έστω b ένας γεννήτορας τής G. Τότε $b = a^z$ και $a = b^w$, για κάποιους $z, w \in \mathbb{Z}$. Συνεπώς, $a = (a^z)^w = a^{zw}$ και ως εκ τούτου, $e_G = a^{zw-1}$. Άρα, $e_G = a^{|zw-1|}$, όπου η απόλυτη τιμή $|zw-1| \in \mathbb{N} \bigcup \{0\}$. Αφού όμως $\circ(a) = [\langle a \rangle : 1] = [G : 1] = \infty$, το σύνολο M_a είναι κενό, βλ. Θεώρημα 1.5.10. Επομένως $zw - 1 = 0$ και επειδή οι z, w είναι ακέραιοι αριθμοί, συμπεραίνουμε ότι το $z = \pm 1$. Άρα, $b = a$ ή $b = a^{-1}$.
(β′) Προφανώς το a^z είναι γεννήτορας τής G, αν και μόνο αν, το $a^{|z|}$ είναι γεννήτορας τής G. Σύμφωνα με την προηγούμενη πρόταση, η τάξη $\circ(a^{|z|})$ ισούται με την τάξη $\circ(a^{n/\delta})$, όπου $\delta =$ ΜΚΔ$(|z|, n)$. Η τάξη τού $a^{n/\delta}$ ισούται με n, αν και μόνο αν, $\delta = 1$. □

Οι υποομάδες μιας κυκλικής ομάδας

Θεώρημα 1.5.14. *Έστω $(G, \star)$ μια κυκλική ομάδα. Κάθε υποομάδα H τής G είναι επίσης κυκλική.*

Απόδειξη. Λόγω τής υπόθεσης, υπάρχει $a \in G$ με $\langle a \rangle = G$. Έστω $H \leq G$.
Αν $H = \{e_G\}$, τότε $H = \langle e_G \rangle$.
Αν $H \neq \{e_G\}$, τότε υπάρχει $h \in H$ με $h \neq e_G$ και αφού $H \leq G$, το h θα ισούται με κάποια δύναμη a^z, όπου $z \in \mathbb{Z}, z \neq 0$. Επειδή $a^z \in H$ και η H είναι υποομάδα τής G, έπεται ότι και το $a^{|z|}$ είναι επίσης στοιχείο τής H.

Ως εκ τούτου, το σύνολο

$$M_H = \{m \in \mathbb{N} \mid a^m \neq e_G \ \text{ και } \ a^m \in H\}$$

είναι $\neq \emptyset$. Ισχυριζόμαστε ότι $\langle a^n \rangle = H$, όπου $n = \min M_H$. Προφανώς, $\langle a^n \rangle \subseteq H$ διότι το a^n ανήκει στην H. Θα δείξουμε ότι $H \subseteq \langle a^n \rangle$. Όταν $h \in H$, τότε το $h = a^z$, όπου $z \in \mathbb{Z}$, αφού $H \leq G$. Εκτελώντας διαίρεση με υπόλοιπο τού z διά τού n, έχουμε $z = n\lambda + v$, όπου $0 \leq v \leq n-1$. Τότε το $a^z = (a^n)^\lambda a^v$ (*) και επομένως το στοιχείο $(a^n)^{-\lambda} a^z = a^v$ ανήκει στην H, διότι η H είναι υποομάδα τής G και τα $(a^n)^{-\lambda}$ και a^z είναι στοιχεία τής H. Παρατηρούμε ότι το $v = 0$, αφού διαφορετικά θα προέκυπτε η αντίφαση $a^v \in H$ και

$\upsilon < n = \min M_H$. Τώρα, η (*) παίρνει τη μορφή $a^z = (a^n)^\lambda e_G$ και το a^z ανήκει στην κυκλική υποομάδα $\langle a^n \rangle$. Επομένως, $H \subseteq \langle a^n \rangle$. □

Παράδειγμα 1.5.15. Η ομάδα των ακεραίων $(\mathbb{Z}, +)$ είναι κυκλική και γι' αυτό και κάθε υποομάδα της H είναι επίσης κυκλική. Η απόδειξη τού προηγούμενου θεωρήματος υποδεικνύει το πώς βρίσκουμε έναν γεννήτορα τής H. Όταν $H \neq \{0\}$, τότε[15] $H = \langle n \rangle = n\mathbb{Z} = \{\lambda n \mid \lambda \in \mathbb{Z}\}$, όπου n είναι ο μικρότερος θετικός ακέραιος που περιέχεται στην H. Προφανώς, όταν $H = \{0\}$, τότε $H = \langle 0 \rangle = 0\mathbb{Z}$. Επομένως, κάθε υποομάδα τής $\mathbb{Z}$ είναι τής μορφής $n\mathbb{Z}$, όπου $n \in \mathbb{N} \bigcup \{0\}$.

Πρόταση 1.5.16. *Έστω $(G, \star)$ μια κυκλική ομάδα τάξης n.*

(α′) *Για κάθε διαιρέτη d τού n, υπάρχει ακριβώς μία υποομάδα H τής G τάξης d.*

(β′) *Για κάθε διαιρέτη d τού n, το πλήθος των στοιχείων τής G τάξης d ισούται με $\varphi(d)$, όπου φ είναι η φ–συνάρτηση Euler.*

Απόδειξη. Αφού η G είναι κυκλική τάξης n, υπάρχει $a \in G$ με $G = \langle a \rangle$ και $\circ(a) = n$.
(α′) Έστω d ένας διαιρέτης τού n. Από το Πόρισμα 1.5.11 γνωρίζουμε ότι η κυκλική υποομάδα $\langle a^{n/d} \rangle$ έχει τάξη d. Αν H_1 και H_2 είναι δύο υποομάδες τής G με τάξη d, τότε από το Θεώρημα 1.5.14 γνωρίζουμε ότι αυτές είναι κυκλικές, ας πούμε $H_1 = \langle a^{k_1} \rangle$ και $H_2 = \langle a^{k_2} \rangle$, όπου $k_1, k_2 \in \mathbb{N}, 1 \leq k_1, k_2 \leq n$, διότι $G = \{a^0 = e_G, a, a^2, \ldots, a^{n-1}\}$ και $a^n = e_G = a^0$. Από την Πρόταση 1.5.12, γνωρίζουμε ότι $H_1 = \langle a^{k_1} \rangle = \langle a^{\delta_1} \rangle$ και $H_2 = \langle a^{k_2} \rangle = \langle a^{\delta_2} \rangle$, όπου δ_1, αντίστοιχα δ_2, είναι ο μέγιστος κοινός διαιρέτης των n και k_1, αντίστοιχα των n και k_2. Ακόμα από την ίδια πρόταση γνωρίζουμε ότι για την κοινή τάξη d των H_1 και H_2 ισχύει $\circ(a^{k_1}) = n/\delta_1 = d = \circ(a^{k_2}) = n/\delta_2$. Επομένως, $\delta_1 = \delta_2$ και έτσι $H_1 = H_2$.
(β′) Κάθε στοιχείο τάξης d παράγει μια κυκλική υποομάδα τής G τάξης d. Από το (α′) γνωρίζουμε ότι υπάρχει μία μοναδική υποομάδα $H \leq G$ τάξης d. Άρα, κάθε στοιχείο τάξης d περιέχεται στην H, η οποία είναι κυκλική τάξης d. Από την Πρόταση 1.5.12, γνωρίζουμε ότι το πλήθος των στοιχείων τής (κυκλικής ομάδας) H τάξης d ισούται με $\varphi(d)$. □

Από τη Θεωρία Αριθμών υπενθυμίζουμε τις αριθμητικές συναρτήσεις[16] σ_i, $i \in \mathbb{N} \bigcup \{0\}$:

$$\sigma_i : \mathbb{N} \to \mathbb{N}, n \mapsto \sigma_i(n) := \sum_{d \mid n} d^i,$$

όπου ο d διατρέχει όλους τους φυσικούς διαιρέτες τού n.

Προφανώς, η τιμή τής $\sigma_0(n)$ ισούται με το πλήθος όλων των φυσικών διαιρετών τού n και η τιμή $\sigma_1(n)$ ισούται με άθροισμα όλων των φυσικών διαιρετών τού n.

Πόρισμα 1.5.17. *Έστω $(G, \star)$ μια κυκλική ομάδα τάξης n. Το πλήθος των υποομάδων τής G ισούται με $\sigma_0(n)$.*

[15] Προσθετική σημειογραφία.

[16] Οι συναρτήσεις σ_i είναι πολλαπλασιαστικές και γι' αυτό όταν ο n είναι ένας φυσικός > 1 με πρωτογενή ανάλυση $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, τότε $\sigma_i(n) = \prod_{k=1}^{s} \sigma_i(p_k^{\alpha_k}) = \prod_{k=1}^{s}(1 + p_k^i + \cdots + p_k^{i\alpha_k})$.

Με τη βοήθεια τής θεωρίας που αναπτύξαμε μέχρι τώρα, θα αποδείξουμε ορισμένα σημαντικά αποτελέσματα σχετικά με τις κυκλικές ομάδες και τις τάξεις στοιχείων.

Αρχίζουμε με την εξής γενική παρατήρηση:

Παρατήρηση 1.5.18. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι χ είναι η σχέση $\chi := \{(g, h) \in G \times G \mid \langle g \rangle = \langle h \rangle\}$ επί τής G. Με άλλα λόγια το ζεύγος (g, h) ανήκει στη χ, αν και μόνο αν, τα g και h παράγουν την ίδια κυκλική υποομάδα. Εύκολα διαπιστώνεται ότι η χ είναι μια σχέση ισοδυναμίας και ότι η κλάση ισοδυναμίας $[g]_\chi$ τού $g \in G$, ως προς χ, ισούται με το σύνολο $\mathcal{G}\{\langle g \rangle\}$ των γεννητόρων τής κυκλικής υποομάδας $\langle g \rangle$. Συνεπώς, η οικογένεια $(\mathcal{G}\{\langle g \rangle\})_{g\in G}$ των κλάσεων ισοδυναμίας τής χ αποτελεί μια διαμέριση τής G. Επιπλέον, για $g, h \in G$ είναι:

$$[g]_\chi \neq [h]_\chi \Leftrightarrow \langle g \rangle \neq \langle h \rangle \Leftrightarrow \mathcal{G}\{\langle g \rangle\} \bigcap \mathcal{G}\{\langle h \rangle\} = \emptyset$$

Έτσι συμπεραίνουμε ότι το σύνολο G/χ των κλάσεων ισοδυναμίας ως προς χ ισούται με $\{\mathcal{G}\{\ C\} \mid C \in \mathcal{C}\}$, όπου $\mathcal{C}$ είναι το σύνολο των κυκλικών υποομάδων[17] τής G. Επομένως,

$$G = \bigcup_{C\in\mathcal{C}} \mathcal{G}\{C\} \tag{*}$$

Όταν η G είναι μια πεπερασμένη ομάδα, τότε το σύνολο $\mathcal{C}$ των κυκλικών υποομάδων της είναι πεπερασμένο, ας πούμε ότι $\mathcal{C} = \{C_1, C_2, \ldots, C_s\}$, και από την (*) προκύπτει:

$$[G : 1] = \sum_{i=1}^{s} \mid \mathcal{G}\{C_i\} \mid . \tag{**}$$

Τώρα είμαστε έτοιμοι για το:

Πόρισμα 1.5.19. *Για κάθε φυσικό αριθμό $n \in \mathbb{N}$, είναι*

$$n = \sum_{d|n} \varphi(d),$$

όπου ο d διατρέχει τους φυσικούς διαιρέτες τού n.

Απόδειξη. Έστω $(G, \star)$ οποιαδήποτε κυκλική[18] ομάδα τάξης n. Από την Πρόταση 1.5.16, γνωρίζουμε ότι για κάθε φυσικό διαιρέτη d τού n, υπάρχει ακριβώς μία κυκλική υποομάδα $C_d \leq G$ τάξης d. Ως εκ τούτου, το σύνολο των κυκλικών υποομάδων τής G είναι το $\mathcal{C} = \{C_d \mid d \text{ διατρέχει τους φυσικούς διαιρέτης τού } n\}$. Υπενθυμίζουμε, βλ. Πρόταση 1.5.12, ότι το πλήθος των γεννητόρων τής C_d ισούται με $\varphi(d)$. Από την (**), προκύπτει:

$$n = [G : 1] = \sum_{d|n} \mid \mathcal{G}\{C_d\} \mid = \sum_{d|n} \varphi(d),$$

όπου ο d διατρέχει τους φυσικούς διαιρέτες τού n. □

[17]και προφανώς ανά δύο διαφορετικών, αφού το $\mathcal{C}$ είναι σύνολο!

[18]Γνωρίζουμε ότι για κάθε $n \in \mathbb{N}$, υπάρχει μια κυκλική ομάδα G τάξης n, βλ. Παράδειγμα 1.5.2.

Το προηγούμενο πόρισμα είναι γνωστό και ως Θεώρημα Gauss.

Θεώρημα 1.5.20. *Έστω $(G, \star)$ μια πεπερασμένη ομάδα τάξης n. Η ομάδα G είναι κυκλική, αν και μόνο αν, σε κάθε φυσικό διαιρέτη d τού n υπάρχει το πολύ μια υποομάδα C τής G τάξης d.*

Απόδειξη. «$\Rightarrow$» Όταν η G είναι κυκλική τάξης n, τότε το συμπέρασμα προκύπτει από την Πρόταση 1.5.16.
«$\Leftarrow$» Έστω $d_1, d_2, \ldots, d_s$ οι φυσικοί διαιρέτες τού n για τους οποίους υπάρχει αντίστοιχη κυκλική υποομάδα C_{d_i} τάξης d_i. Επομένως, το σύνολο των κυκλικών υποομάδων τής G είναι το $\mathcal{C} = \{C_{d_1}, C_{d_2}, \ldots, C_{d_s}\}$. Από την (**) προκύπτει:

$$n = [G:1] = \sum_{i=1}^{s} \varphi(d_i) \leq \sum_{d|n} \varphi(d) = n,$$

όπου ο d διατρέχει τους φυσικούς διαιρέτες τού n.
Επομένως, $\sum_{i=1}^{s} \varphi(d_i) = \sum_{d|n} \varphi(d)$ και γι' αυτό πρέπει να υπάρχει σε κάθε διαιρέτη d τού n και μια αντίστοιχη κυκλική υποομάδα τής G τάξης d. Ιδιαιτέρως, υπάρχει κυκλική υποομάδα C τάξης n. Άρα, $C = G$. □

Το επόμενο πολύ σημαντικό αποτέλεσμα αποτελεί εφαρμογή τού θεωρήματος που μόλις είδαμε. Στην Ενότητα 3.2.5 θα δούμε μια επιπλέον απόδειξή του βασισμένη στη Θεωρία Sylow.

Θεώρημα 1.5.21. *Έστω K ένα σώμα και $(K^\star, \cdot)$ η πολλαπλασιαστική ομάδα των αντιστρέψιμων στοιχείων του. Κάθε πεπερασμένη υποομάδα G τής $K^\star$ είναι κυκλική.*

Απόδειξη. Έστω ότι η τάξη τής G ισούται με n. Αν για κάποιο διαιρέτη d τού n υπάρχουν τουλάχιστον δύο υποομάδες $H, H', H \neq H'$ τής G τάξης d, τότε το πλήθος $|H \bigcup H'|$ τής ένωσής τους είναι $\geq d+1$. Κάθε $g \in H \bigcup H'$ αποτελεί λύση τής εξίσωσης $x^d - 1 = 0$ στο σώμα K. Πράγματι, έχουμε[19] $g^d = 1$, διότι το g ανήκει σε μια ομάδα τάξης d. Επομένως η $x^d - 1 = 0$ έχει τουλάχιστον $d+1$ λύσεις. Αυτό είναι άτοπο, αφού σε ένα σώμα οποιαδήποτε εξίσωση m-οστού βαθμού έχει το πολύ m λύσεις. Άρα, σε κάθε διαιρέτη d τού n υπάρχει το πολύ μια υποομάδα τάξης d και ως εκ τούτου, η G είναι κυκλική. □

Πόρισμα 1.5.22. *Η ομάδα $(\mathbb{U}_p, \cdot)$ των αντιστρέψιμων κλάσεων ισοτιμίας των ακεραίων* mod$p$*, όπου p πρώτος αριθμός, είναι κυκλική, (*βλ. Παράδειγμα 1.2.21*).*

Απόδειξη. Γνωρίζουμε ότι για κάθε πρώτο αριθμό p, το σύνολο $\mathbb{Z}_p$ των κλάσεων ισοτιμίας των ακεραίων mod$p$ είναι σώμα ως προς τις πράξεις τής πρόσθεσης και πολλαπλασιασμού mod$p$. Η πολλαπλασιαστική ομάδα των αντιστρέψιμων στοιχείων τού σώματος $\mathbb{Z}_p$ είναι η $\mathbb{U}_p$ με $[\mathbb{U}_p : 1] = \varphi(p) = p - 1$. Από το προηγούμενο θεώρημα έπεται ότι η $\mathbb{U}_p$ είναι κυκλική. □

Τώρα παρουσιάζουμε μια γενίκευση τής Πρότασης 1.5.16:

[19] Το ουδέτερο στοιχείο τής G είναι το μοναδιαίο στοιχείο 1 τού σώματος.

Πρόταση 1.5.23. *Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι d είναι ένας φυσικός. Το πλήθος των στοιχείων τής G τάξης d ισούται με ένα πολλαπλάσιο τού $\varphi(d)$.*

Απόδειξη. Έστω $\mathcal{A}_d = \{g \in G \mid \circ(g) = d\}$ το σύνολο των στοιχείων τής G τάξης d.
Αν $\mathcal{A}_d = \emptyset$, τότε το $|\mathcal{A}_d| = 0$, τότε προφανώς $|\mathcal{A}_d| = 0 \cdot \varphi(d)$.

Έστω ότι $\mathcal{A}_d \neq \emptyset$. Θα εκτελέσουμε μια απόδειξη, η οποία βασίζεται στη σχέση ισοδυναμίας που εισαγάγαμε στην Παρατήρηση 1.5.18.
Θεωρούμε τη σχέση $\chi(d) = \{(g,h) \in \mathcal{A}_d \times \mathcal{A}_d \mid \langle g \rangle = \langle h \rangle\}$. Η $\chi(d)$ είναι μια σχέση ισοδυναμίας επί τού $\mathcal{A}_d$.

Για κάθε κυκλική υποομάδα C τής G συμβολίζουμε με $\mathcal{G}\{C\}$ το σύνολο των γεννητόρων της. Η κλάση ισοδυναμίας $[g]_{\chi(d)}$ τού $g \in \mathcal{A}_d$, αποτελείται από τα $h \in \mathcal{A}_d$ με $\langle g \rangle = \langle h \rangle$. Επομένως, $[g]_{\chi(d)} = \{h \in \mathcal{A}_d \mid h \text{ γεννήτορας τής } \langle g \rangle\} = \mathcal{G}\{\langle g \rangle\}$.

Όπως και προηγουμένως διαπιστώνουμε ότι για $g, h \in \mathcal{A}_d$ είναι:

$$[g]_{\chi(d)} \neq [h]_{\chi(d)} \Leftrightarrow \langle g \rangle \neq \langle h \rangle \Leftrightarrow \mathcal{G}\{\langle g \rangle\} \bigcap \mathcal{G}\{\langle h \rangle\} = \emptyset$$

και ως εκ τούτου συμπεραίνουμε ότι το σύνολο $\mathcal{A}_d/\chi(d)$ των κλάσεων ισοδυναμίας είναι το

$$\{\mathcal{G}\{C\} \mid C \in \mathcal{C}(d)\}, \text{ όπου } \mathcal{C}(d) = \{C \leq G \mid C \text{ κυκλική υποομάδα τάξης } d\}.$$

Έτσι, είναι

$$\mathcal{A}_d = \bigcup_{C \in \mathcal{C}(d)} \mathcal{G}\{C\}$$

και

$$|\mathcal{A}_d| = \sum_{C \in \mathcal{C}(d)} |\mathcal{G}\{C\}|, \qquad (*)$$

Για κάθε $C \in \mathcal{C}(d)$, είναι $|\mathcal{G}\{C\}| = \varphi(d)$. Επιπλέον, το πλήθος των στοιχείων τού συνόλου $\mathcal{C}(d)$ είναι κάποιος $s \in \mathbb{N}$, διότι η G είναι μια πεπερασμένη ομάδα. Έτσι, από την (*) προκύπτει ότι το πλήθος των στοιχείων τής G τάξης d είναι:

$$|\mathcal{A}_d| = s\varphi(d).$$

□

Οι υποομάδες τής διεδρικής ομάδας $(D_n, \circ)$

Υπενθυμίζουμε ότι

$$D_n = \{\mathrm{Id}_n, \tau, \rho, \rho^2, \ldots, \rho^{n-1}, \tau \circ \rho, \tau \circ \rho^2, \ldots, \tau \circ \rho^{n-1}\},$$

όπου $\tau^2 = \mathrm{Id}_n$, $\rho^n = \mathrm{Id}_n$ και $\rho \circ \tau = \tau \circ \rho^{-1}$. Από το Παράδειγμα 1.4.15, γνωρίζουμε ότι η κυκλική υποομάδα $\langle \rho \rangle$ είναι τάξης $n = [D_n : 1]/2$. Ως εκ τούτου, η D_n και η υποομάδα της $\langle \rho \rangle$ ικανοποιούν τις υποθέσεις τού Πορίσματος 1.4.18 με τη βοήθεια τού οποίου θα προσδιορίσουμε όλες τις υποομάδες τής D_n.

Έστω H οποιαδήποτε υποομάδα τής D_n. Σύμφωνα με το πόρισμα που προαναφέραμε υπάρχουν δύο περιπτώσεις:

Πρώτη Περίπτωση Η υποομάδα $H \leq D_n$ περιέχεται στην $\langle\rho\rangle$. Επειδή η $\langle\rho\rangle$ είναι κυκλική τάξης n, γνωρίζουμε ότι η H πρέπει να ισούται με κάποια από τις υποομάδες $\langle\rho^{n/d}\rangle$, όπου ο d είναι ένας φυσικός διαιρέτης τού n, βλ. απόδειξη τής Πρότασης 1.5.16. Επομένως, υπάρχουν $\sigma_0(n)$ το πλήθος υποομάδες τής D_n, οι οποίες περιέχονται στην $\langle\rho\rangle$, βλ. Πόρισμα 1.5.17.

Δεύτερη Περίπτωση Η υποομάδα $H \leq D_n$ δεν περιέχεται στην $\langle\rho\rangle$. Θεωρούμε την τομή $H\bigcap\langle\rho\rangle$, η οποία ως υποομάδα τής $\langle\rho\rangle$ πρέπει να ισούται με κάποια από τις υποομάδες $\langle\rho^{n/d}\rangle$, όπου ο d είναι ένας φυσικός διαιρέτης τού n. Τώρα από το Πόρισμα 1.4.18, προκύπτει ότι η H πρέπει να ισούται με την ένωση των αριστερών πλευρικών κλάσεων $H\bigcap\langle\rho\rangle$ και $\xi \circ (H\bigcap\langle\rho\rangle)$, δηλαδή $H = (H\bigcap\langle\rho\rangle)\bigcup \xi \circ (H\bigcap\langle\rho\rangle) = \langle\rho^{n/d}\rangle \bigcup \xi \circ \langle\rho^{n/d}\rangle$, όπου το ξ ανήκει στη συνολοθεωρητική διαφορά $H \setminus \langle\rho\rangle$. Συνεπώς, το ξ οφείλει να ισούται με κάποιο $\tau \circ \rho^i, 0 \leq i \leq n-1$. Εκτελώντας διαίρεση με υπόλοιπο τού i διά n/d, έχουμε: $i = \lambda(n/d) + \upsilon, 0 \leq \upsilon \leq (n/d) - 1$. Παρατηρούμε ότι

$$\xi \circ \langle\rho^{n/d}\rangle = \tau \circ \rho^i \circ \langle\rho^{n/d}\rangle = \tau \circ \rho^\upsilon \circ \rho^{\lambda(n/d)} \circ \langle\rho^{n/d}\rangle = \tau \circ \rho^\upsilon \circ \langle\rho^{n/d}\rangle.$$

Επομένως, η $H = \langle\rho^{n/d}\rangle \bigcup(\tau \circ \rho^\upsilon \circ \langle\rho^{n/d}\rangle)$ και έτσι το στοιχείο $\tau \circ \rho^\upsilon$ ανήκει στην H και είναι μάλιστα το μικρότερης μη αρνητικής δύναμης, ως προς ρ, στοιχείο τής μορφής $\tau \circ \rho^i$ που ανήκει στην H.

Συνεπώς, όταν $H\bigcap\langle\rho\rangle = \langle\rho^{n/d}\rangle$, τότε $H = \langle\rho^{n/d}\rangle \bigcup(\tau \circ \rho^\upsilon \circ \langle\rho^{n/d}\rangle)$, όπου $0 \leq \upsilon \leq (n/d) - 1$. Άρα, για κάθε διαιρέτη d τού n υπάρχουν n/d το πλήθος υποομάδες τής D_n οι οποίες δεν περιέχονται στην υποομάδα $\langle\rho\rangle$. Γι' αυτό το πλήθος των υποομάδων τής D_n που δεν περιέχονται στη $\langle\rho\rangle$ ισούται με $\sum_{d|n}(n/d) = \sum_{d|n} d$, όπου το d διατρέχει όλους τους φυσικούς διαιρέτες τού n. Όπως έχουμε ήδη συζητήσει, ο αριθμός $\sum_{d|n} d$ ισούται με την τιμή $\sigma_1(n)$ τής αριθμητικής συνάρτησης σ_1 επί τού n, βλ. σελ. 86.

Τέλος, παρατηρούμε ότι η υποομάδα $H = \langle\rho^{n/d}\rangle \bigcup(\tau \circ \rho^\upsilon \circ \langle\rho^{n/d}\rangle)$ περιέχεται στην υποομάδα $\langle\{\rho^{n/d}, \tau \circ \rho^\upsilon\}\rangle$ τής D_n που παράγεται από τα στοιχεία $\rho^{n/d}$ και $\tau \circ \rho^\upsilon$ και επειδή η τελευταία είναι η μικρότερη υποομάδα τής D_n, η οποία περιέχει τα στοιχεία αυτά, συμπεραίνουμε ότι $H = \langle\{\rho^{n/d}, \tau \circ \rho^\upsilon\}\rangle$. Προφανώς, $[H : 1] = 2d$.

Κατ' αυτόν τον τρόπο αποδείξαμε το εξής:

Θεώρημα 1.5.24. *Έστω ότι $(D_n, \circ), n \geq 3$ είναι η διεδρική ομάδα τάξης $2n$ και ότι H είναι οποιαδήποτε υποομάδα της.*

Τότε ή $H = \langle\rho^{n/d}\rangle$ με $[H : 1] = d$, ή $H = \langle\{\rho^{n/d}, \tau \circ \rho^\upsilon\}\rangle$ με $[H : 1] = 2d$, όπου ο d διατρέχει όλους τους φυσικούς διαιρέτες τού n και όπου για κάθε d, ο αριθμός υ διατρέχει τα στοιχεία τού συνόλου $\{0, 1, \ldots, (n/d) - 1\}$.

Το πλήθος των υποομάδων τής D_n ισούται με $\sigma_0(n) + \sigma_1(n)$.

Ασκήσεις στις Κυκλικές Ομάδες και την Τάξη Στοιχείου

Λυμένες Ασκήσεις

Α 48. Έστω ότι $(G, \star)$ είναι μια κυκλική ομάδα και ότι a είναι ένα στοιχείο τής G. Να δειχθεί ότι το $a \in G$ είναι ένας γεννήτορας τής G, αν και μόνο αν, το αντίστροφό του a^{-1} είναι ένας γεννήτορας τής G.

Λύση. Όταν το $a \in G$ είναι ένας γεννήτορας, τότε για κάθε $g \in G$, υπάρχει κάποιος $z \in \mathbb{Z}$ με $g = a^z = (a^{-1})^{(-z)}$. Ως εκ τούτου, το a^{-1} είναι επίσης γεννήτορας τής G.

Α 49. Έστω ότι $(G, \star)$ είναι μια κυκλική ομάδα με ακριβώς έναν γεννήτορα. Να δειχθεί ότι η τάξη $[G : 1]$ τής G ισούται ή με 1 ή με 2.

Λύση. Έστω ότι $a \in G$ είναι ένας γεννήτορας τής G, δηλαδή ότι $G = \langle a \rangle$. Ως γνωστόν, όταν το a είναι γεννήτορας, τότε και το a^{-1} είναι επίσης γεννήτορας. Από την υπόθεση έπεται ότι $a = a^{-1}$, αυτό είναι ισοδύναμο με $a^2 = e_G$. Άρα, $\circ(a) = 1$ ή 2 και ως εκ τούτου, $[G : 1] = 1$ ή 2.

Α 50. Να δειχθεί ότι η ομάδα $(G, \star)$ είναι ένωση των γνήσιων υποομάδων της, αν και μόνο αν, δεν είναι κυκλική.

Λύση. «$\Rightarrow$» Έστω ότι $G = \bigcup_{H_i \lneqq G} H_i$, $(*)$, όπου οι H_i διατρέχουν το σύνολο[20] όλων των γνήσιων υποομάδων τής G. Αν η G ήταν κυκλική, τότε θα είχε κάποιο γεννήτορα a, δηλαδή θα ήταν $\langle a \rangle = G$. Όμως τότε από την $(*)$, θα υπήρχε κάποια υποομάδα H_i με $a \in H_i$ και ως εκ τούτου, θα ήταν $G = \langle a \rangle \leq H_i$ και κατόπιν θα ήταν $G = H_i$, το οποίο είναι άτοπο.
«$\Leftarrow$» Παρατηρούμε ότι για κάθε $a \in G$, η $\langle a \rangle$ είναι γνήσια υποομάδα τής G, διότι η G δεν είναι κυκλική. Προφανώς, $G = \bigcup_{a \in G} \langle a \rangle$. Είναι φανερό ότι $\bigcup_{a \in G} \langle a \rangle \subseteq \bigcup_{H_i \lneqq G} H_i$, όπου οι H_i διατρέχουν το σύνολο όλων των γνήσιων υποομάδων τής G. Αφού $\bigcup_{H_i \lneqq G} H_i \subseteq G$, συμπεραίνουμε ότι $G = \bigcup_{H_i \lneqq G} H_i$.

Α 51. Να δειχθεί ότι για κάθε φυσικό $n \geq 3$, η τιμή $\varphi(n)$ τής φ–συνάρτησης Euler είναι πάντοτε άρτιος αριθμός.

Λύση. Η τιμή $\varphi(n)$ μετρά το πλήθος των γεννητόρων μιας κυκλικής ομάδας G τάξης n, βλ. Πρόταση 1.5.16. Όταν το a είναι ένας γεννήτορας τής G, τότε το a^{-1} είναι επίσης ένας γεννήτοράς της και πάντοτε είναι $a \neq a^{-1}$, διότι διαφορετικά θα ήταν $[G : 1] \leq 2$, λόγω τής αμέσως προηγούμενης άσκησης. Μετρώντας τους γεννήτορες ανά ζεύγη ως a και a^{-1}, διαπιστώνουμε ότι το πλήθος τους είναι άρτιο. Άρα, η $\varphi(n)$ με $n \geq 3$ είναι ένας άρτιος αριθμός.

Α 52. Έστω ότι $(G, \star)$ είναι μια ομάδα που διαθέτει περισσότερα από $p - 1$ στοιχεία τάξης p, όπου ο p είναι ένας πρώτος αριθμός. Να δειχθεί ότι η G δεν είναι κυκλική.

Λύση. Έστω a ένα στοιχείο τής G τάξης p. Τότε η κυκλική υποομάδα $\langle a \rangle$ τής G, η οποία είναι πρώτης τάξης p, διαθέτει ακριβώς $p - 1$ στοιχεία τάξης p. Λόγω τής υπόθεσης, συμπεραίνουμε ότι υπάρχει κάποιο $b \in G$ με $\circ(b) = p$ και $b \notin \langle a \rangle$. Τότε βέβαια $\langle b \rangle \neq \langle a \rangle$. Άρα, η G διαθέτει τουλάχιστον δύο υποομάδες τάξης p και γι' αυτό δεν είναι κυκλική, βλ. Θεώρημα 1.5.20.

[20]Γενικά όλες οι υποομάδες μιας ομάδας απαρτίζουν ένα σύνολο, διότι κάθε υποομάδα ανήκει στο δυναμοσύνολο $\mathcal{P}(G)$ τής G, δηλαδή στο σύνολο όλων των υποσυνόλων τής G.

Α 53. Να ευρεθούν όλες οι υποομάδες τής $(\mathbb{Z}_{45}, +)$, προσδιορίζοντας σε κάθε περίπτωση έναν γεννήτορά τους.

Λύση. Η $\mathbb{Z}_{45}$ είναι κυκλική. Από την Πρόταση 1.5.16, γνωρίζουμε ότι για κάθε διαιρέτη d τού 45 υπάρχει ακριβώς μια υποομάδα τάξης d. Το σύνολο των διαιρετών τού 45 είναι το $\{1, 3, 3^2, 5, 3 \cdot 5, 3^2 \cdot 5\}$. Επομένως, οι υποομάδες τής $\mathbb{Z}_{45}$ είναι οι εξής:
$\langle [45]_{45} \rangle = \langle [0]_{45} \rangle$, όπου η τάξη τού $3^2 \cdot 5[1]_{45} = [45]_{45}$ ισούται με 1,
$\langle [15]_{45} \rangle$, όπου η τάξη τού $3 \cdot 5[1]_{45} = [15]_{45}$ ισούται με 3,
$\langle [5]_{45} \rangle$, όπου η τάξη τού $5[1]_{45} = [5]_{45}$ ισούται με 9,
$\langle [9]_{45} \rangle$, όπου η τάξη τού $3^2[1]_{45} = [9]_{45}$ ισούται με 5,
$\langle [3]_{45} \rangle$, όπου η τάξη τού $3[1]_{45} = [3]_{45}$ ισούται με 15 και η
$\langle [1]_{45} \rangle$, όπου η τάξη τού $[1]_{45}$ ισούται με 45.

Α 54. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης $[G : 1] = n \in \mathbb{N}$ και ότι a είναι ένα στοιχείο τής G με $\circ(a) = n$.

(α′) Να δειχθεί ότι $\langle a \rangle = G$.

(β′) Να δειχθεί ότι αυτό δεν είναι πάντοτε αληθές, όταν $[G : 1] = \infty$ και $\circ(a) = \infty$.

Λύση. (α′) Η $\langle a \rangle$ είναι μια υποομάδα τής G τάξης n, διότι $\circ(a) = n$. Αφού το πλήθος τού $\langle a \rangle \subseteq G$ είναι πεπερασμένο και ίσο με το πλήθος τού G, συμπεραίνουμε ότι $\langle a \rangle = G$.
(β′) Θεωρούμε τη $(\mathbb{Z}, +)$ και την κυκλική υποομάδα $\langle 5 \rangle$ που παράγεται από το 5. Η τάξη $[\langle 5 \rangle : 1] = \infty = [\mathbb{Z} : 1]$, αφού η $\circ(5) = \infty$. Ωστόσο, η $\langle 5 \rangle$ είναι μια γνήσια υποομάδα τής $\mathbb{Z}$, αφού $3 \notin \langle 5 \rangle$. (*Το* 3 *δεν είναι ακέραιο πολλαπλάσιο τού* 5.)

Α 55. Να ευρεθεί το πλήθος των γεννητόρων μιας κυκλικής ομάδας τάξης 88000.

Λύση. Το πλήθος των γεννητόρων ισούται με την τιμή $\varphi(88000)$ τής φ-συνάρτησης Euler. Αφού η πρωτογενής ανάλυση τού 88000 είναι η $88000 = 2^6 5^3 11$, έχουμε $\varphi(88000) = \varphi(2^6)\varphi(5^3)\varphi(11) = (2^6 - 2^5)(5^3 - 5^2)(11 - 10) = 32000$. Συνεπώς, μια κυκλική ομάδα τάξης 88000 διαθέτει 32000 γεννήτορες.

Α 56. Να ευρεθεί η τάξη τού στοιχείου $[30]_{54}$ τής $(\mathbb{Z}_{54}, +)$.

Λύση. Αφού $[30]_{54} = 30 \cdot [1]_{54}$, συμπεραίνουμε ότι $\circ([30]_{54}) = \frac{54}{\text{ΜΚΔ}(30,54)} \frac{54}{6} = 9$, βλ. Πρόταση 1.5.12.

Α 57. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι a, b είναι στοιχεία τής G. Να δειχθούν τα εξής:

(α′) $\circ(ab) = \circ(ba)$.

(β′) $\circ(a) = \circ(bab^{-1})$.

Λύση. (α′) Θα δείξουμε ότι είναι $(ab)^n = e_G \Leftrightarrow (ba)^n = e_G$, όπου $n \in \mathbb{N}$.
Έστω ότι $(ab)^n = e_G$, τότε $b((ab)^n)a = ba$, δηλαδή $(ba)(ba)\ldots(ba) = ba$, όπου το πλήθος των παραγόντων (ba) στο αριστερό τμήμα τής ισότητας ισούται με $(n + 1)$.
Επομένως, $(ba)^n = e_G$. Με ακριβώς τον ίδιο τρόπο συμπεραίνουμε ότι όταν $(ba)^n = e_G$,

τότε $(ab)^n = e_G$. Άρα, τα σύνολα $M_{ab} = \{n \in \mathbb{N} \mid (ab)^n = e_G\}$ και $M_{ba} = \{n \in \mathbb{N} \mid (ba)^n = e_G\}$, βλ. Θεώρημα 1.5.10, είναι πάντοτε ίσα. Ως εκ τούτου, $\circ(ab) = \circ(ba)$.
(β′) Παρατηρούμε ότι για κάθε $a, b \in G$, είναι $a = (ab^{-1})b$. Από το πρώτο μέρος τής άσκησης, έχουμε $\circ(a) = \circ((ab^{-1})b) = \circ(b(ab^{-1})) = \circ(bab^{-1})$.

Α 58. Να ευρεθούν όλες οι υποομάδες τής τετρανιακής ομάδας $(\mathcal{Q}_8, \circ)$, βλ. Άσκηση ΠΑ26, και για καθεμιά από αυτές, να προσδιοριστεί ο αντίστοιχος δείκτης.

Λύση. Υπενθυμίζουμε ότι το σύνολο των στοιχείων της τετρανιακής ομάδας $(\mathcal{Q}_8, \circ)$ ισούται με τους 2×2 μιγαδικούς πίνακες $\{\pm E,\ \pm I,\ \pm J,\ \pm K\}$, όπου $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ και $K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ με $i^2 = -1$.

Η πράξη «$\circ$» της $(\mathcal{Q}_8, \circ)$ είναι ο πολλαπλασιασμός των 2×2 μιγαδικών πινάκων και ο πίνακας τής «$\circ$» είναι ο:

$\circ$	E	$-E$	I	$-I$	J	$-J$	K	$-K$
E	E	$-E$	I	$-I$	J	$-J$	K	$-K$
$-E$	$-E$	E	$-I$	I	$-J$	J	$-K$	K
I	I	$-I$	$-E$	E	K	$-K$	$-J$	J
$-I$	$-I$	I	E	$-E$	$-K$	K	J	$-J$
J	J	$-J$	$-K$	K	$-E$	E	I	$-I$
$-J$	$-J$	J	K	$-K$	E	$-E$	$-I$	I
K	K	$-K$	J	$-J$	$-I$	I	$-E$	E
$-K$	$-K$	K	$-J$	J	I	$-I$	E	$-E$

Τα στοιχεία $I, -I, J, -J, K, -K$ είναι τάξης 4, το $-E$ είναι τάξης 2 και το E είναι το ουδέτερο στοιχείο. Έτσι υπάρχουν οι υποομάδες $\langle I \rangle = \langle -I \rangle$, $\langle J \rangle = \langle -J \rangle$ και $\langle K \rangle = \langle -K \rangle$ οι οποίες είναι τάξης 4 και η $\langle -E \rangle$, η οποία είναι τάξης 2. Επιπλέον, υπάρχουν οι τετριμμένες υποομάδες $\mathcal{Q}_8$ και $\{E\}$. Ισχυριζόμαστε ότι αυτές είναι όλες οι υποομάδες τής $\mathcal{Q}_8$. Πράγματι, αν H είναι μια μη τετριμμένη υποομάδα τής $\mathcal{Q}_8$, τότε από το Θεώρημα Lagrange, γνωρίζουμε ότι η τάξη $[H : 1]$ είναι ή 2 ή 4, αφού η $[H : 1]$ είναι ένας διαιρέτης τού 8 με $[H : 1] \neq 1, 8$.

Αν $[H : 1] = 2$, τότε η H είναι κυκλική τάξης 2 και ως εκ τούτου, παράγεται από ένα στοιχείο τάξης 2. Το μοναδικό στοιχείο τάξης 2 τής $\mathcal{Q}_8$ είναι το $-E$. Άρα, $H = \langle -E \rangle$.

Αν $[H : 1] = 4$, τότε ή κάθε στοιχείο της $\neq E$ θα είναι τάξης 2 ή η H θα είναι κυκλική τάξης 4. Η πρώτη περίπτωση είναι αδύνατη, διότι τότε η H έχει τρία στοιχεία τάξης 2, ενώ η $\mathcal{Q}_8$ έχει μόνο ένα, το $-E$.

Επομένως, όταν $[H : 1] = 4$, τότε η H είναι κυκλική και παράγεται από κάποιο στοιχείο τάξης 4. Συνεπώς, οφείλει να είναι κάποια από τις τρεις υποομάδες $\langle I \rangle = \langle -I \rangle$, $\langle J \rangle = \langle -J \rangle$ και $\langle K \rangle = \langle -K \rangle$.

Οι δείκτες είναι οι εξής: $[\mathcal{Q}_8 : \mathcal{Q}_8] = \frac{[\mathcal{Q}_8:1]}{[\mathcal{Q}_8:1]} = 8/8 = 1$, $[\mathcal{Q}_8 : \langle E \rangle] = \frac{[\mathcal{Q}_8:1]}{[\langle E \rangle:1]} = 8/1 = 8$, $[\mathcal{Q}_8 : \langle -E \rangle] = \frac{[\mathcal{Q}_8:1]}{[\langle -E \rangle:1]} = 8/2 = 4$, $[\mathcal{Q}_8 : \langle I \rangle] = \frac{[\mathcal{Q}_8:1]}{[\langle I \rangle:1]} = 8/4 = 2$, $[\mathcal{Q}_8 : \langle J \rangle] = \frac{[\mathcal{Q}_8:1]}{[\langle J \rangle:1]} = 8/4 = 2$ και $[\mathcal{Q}_8 : \langle K \rangle] = \frac{[\mathcal{Q}_8:1]}{[\langle K \rangle:1]} = 8/4 = 2$.

Α 59. Έστω ότι οι $(G_1, \star_1)$, $(G_2, \star_2)$ είναι ομάδες, ότι $(G_1 \times G_2, \star)$ είναι το ευθύ γινόμενό τους, ότι $g_1 \in G_1$ και ότι $g_2 \in G$. Να δειχθούν τα εξής:

(α′) Αν είτε $\circ(g_1) = \infty$ είτε $\circ(g_2) = \infty$, τότε η τάξη τού $(g_1, g_2) \in G_1 \times G_2$ είναι άπειρη.

(β′) Αν $\circ(g_1) = m_1$ και $\circ(g_2) = m_2$, τότε η τάξη τού $(g_1, g_2) \in G_1 \times G_2$ είναι ίση με το ελάχιστο κοινό πολλαπλάσιο (ΕΚΠ) των m_1 και m_2.

Λύση. (α′) Αν η τάξη $\circ(g_1, g_2)$ ήταν πεπερασμένη, τότε για κάποιο $n \in \mathbb{N}$ θα ήταν το $(g_1, g_2)^n$ ίσο με το ουδέτερο στοιχείο $e_{G_1 \times G_2}$ τής $G_1 \times G_2$. Ως γνωστόν, $e_{G_1 \times G_2} = (e_{G_1}, e_{G_2})$. Συνεπώς, θα είχαμε $(g_1, g_2)^n = (g_1^n, g_2^n) = (e_{G_1}, e_{G_2})$. Άρα, $g_1^n = e_{G_1}$ και $g_2^n = e_{G_2}$ και συνεπώς $\circ(g_1) < \infty$ και $\circ(g_2) < \infty$. Άτοπο!
(β′) Έστω $\varepsilon := \text{ΕΚΠ}(m_1, m_2)$. Είναι $(g_1, g_2)^\varepsilon = (g_1^\varepsilon, g_2^\varepsilon) = (e_{G_1}, e_{G_2})$, αφού το ε είναι πολλαπλάσιο τής τάξης m_1 τού g_1 και τής τάξης m_2 τού g_2. Αν για κάποιο $n \in \mathbb{N}$, είναι $(g_1, g_2)^n = (e_{G_1}, e_{G_2})$, τότε $g_1^n = e_{G_1}$ και $g_2^n = e_{G_2}$. Άρα, $m_1 \mid n$ και $m_2 \mid n$. Τότε το ε διαιρεί το n και ως εκ τούτου, $\varepsilon \leq n$. Επομένως, $\varepsilon = \circ((g_1, g_2))$.

Α 60. Έστω ότι οι $(G_1, \star_1)$, $(G_2, \star_2)$ είναι δύο κυκλικές ομάδες με τάξεις m και n αντιστοίχως. Να δειχθεί ότι το το ευθύ γινόμενό τους $G_1 \times G_2$ είναι κυκλική ομάδα, αν και μόνο αν, ο $\text{ΜΚΔ}(m, n) = 1$.

Λύση. «$\Rightarrow$» Όταν η $G_1 \times G_2$ είναι κυκλική, τότε διαθέτει ένα στοιχείο (g_1, g_2) τάξης mn, διότι $[G_1 \times G_2] = [G_1 : 1][G_2 : 2] = mn$. Έστω $d = \text{ΜΚΔ}(m, n)$. Παρατηρούμε ότι

$$(g_1, g_2)^{(mn)/d} = (g_1^{(mn)/d}, g_2^{(mn)/d}) = ((g_1^m)^{n/d}, (g_2^n)^{m/d}) = (e_{G_1}, e_{G_2}).$$

Επομένως, $mn \leq \frac{mn}{d}$ και ως εκ τούτου $d = 1$.
«$\Leftarrow$» Έστω ότι $G_1 = \langle g_1 \rangle$ και $G_2 = \langle g_2 \rangle$. Από την προηγούμενη άσκηση γνωρίζουμε ότι η τάξη τού (g_1, g_2) ισούται με το $\text{ΕΚΠ}(\circ(g_1), \circ(g_2)) = \text{ΕΚΠ}(m, n)$. Αφού όμως ο $\text{ΜΚΔ}(m, n) = 1$, συμπεραίνουμε ότι $\circ((g_1, g_2)) = mn$ και ως εκ τούτου, το (g_1, g_2) είναι γεννήτορας τής $G_1 \times G_2$, δηλαδή $G_1 \times G_2 = \langle (g_1, g_2) \rangle$.

Α 61. Έστω η ομάδα $(\mathbb{Q}, +)$ και το ευθύ γινόμενο $(\mathbb{Q} \times \mathbb{Q}, \star)$ τής $\mathbb{Q}$ με τον εαυτό της. Να δειχθεί ότι η $\mathbb{Q} \times \mathbb{Q}$ δεν είναι κυκλική.

Λύση. Αν ήταν η $\mathbb{Q} \times \mathbb{Q}$ κυκλική, τότε θα ήταν και κάθε υποομάδα της κυκλική, βλ. Θεώρημα 1.5.14. Ιδιαιτέρως, η υποομάδα $\mathbb{Q} \times \{0\}$ θα ήταν κυκλική και τότε θα είχε έναν γεννήτορα $(q, 0)$. Αλλά τότε και η $\mathbb{Q}$ θα ήταν κυκλική[21]. Πράγματι, αν το $w \in \mathbb{Q}$, τότε το $(w, 0) \in \mathbb{Q} \times \{0\}$ και γι' αυτό υπάρχει $z \in \mathbb{Z}$ με $z(q, 0) = (zq, 0) = (w, 0)$. Επομένως, $zq = w$ και ως εκ τούτου, η $\mathbb{Q}$ είναι κυκλική. Αυτό είναι άτοπο, διότι από το Παράδειγμα 1.5.4 γνωρίζουμε ότι η $\mathbb{Q}$ δεν είναι κυκλική.

Α 62. Έστω ότι g, h είναι στοιχεία μιας ομάδας $(G, \star)$ με $\circ(g) = m \in \mathbb{N}$, $\circ(h) = n \in \mathbb{N}$. Να δειχθεί ότι η τάξη τής τομής $T := \langle g \rangle \bigcap \langle h \rangle$ είναι ένας κοινός διαιρέτης των m και n.

[21] Το ότι από $\mathbb{Q} \times \{0\}$ κυκλική, έπεται $\mathbb{Q}$ κυκλική είναι άμεσο, αν γνωρίζαμε ότι οι δύο αυτές ομάδες είναι ισόμορφες. Αλλά αυτήν την έννοια θα τη συναντήσουμε αργότερα.

Λύση. Η $T = \langle g\rangle \bigcap \langle h\rangle$ είναι μια πεπερασμένη υποομάδα των $\langle g\rangle$ και $\langle h\rangle$. Από το Θεώρημα Lagrange, βλ. Θεώρημα 1.4.9, γνωρίζουμε ότι η τάξη $[T : 1]$ διαιρεί τις τάξεις των $[\langle g\rangle : 1]$ και $[\langle h\rangle : 1]$ των υποομάδων $\langle g\rangle$ και $\langle h\rangle$ αντιστοίχως.

Α 63. Έστω ότι g, h είναι στοιχεία μιας ομάδας $(G, \star)$ με $gh = hg$ και $\circ(g) \in \mathbb{N}$, $\circ(h) \in \mathbb{N}$. Να δειχθεί ότι

(α′) η τάξη $\circ(gh)$ είναι ένας διαιρέτης τού ελάχιστου κοινού πολλαπλάσιου ε των τάξεων $\circ(g)$ και $\circ(h)$,

(β′) αν οι $\circ(g)$ και $\circ(h)$ είναι σχετικώς πρώτοι αριθμοί, τότε η τάξη $\circ(gh)$ ισούται με το γινόμενο $\circ(g) \cdot \circ(h)$,

(γ′) υπάρχει κάποιο στοιχείο τής G με τάξη ίση με το ΕΚΠ$(\circ(g), \circ(h))$ των τάξεων $\circ(g)$, $\circ(h)$.

Τέλος, να δοθεί παράδειγμα ομάδας $(G, \star)$ και δύο στοιχείων $g, h \in G$ πεπερασμένης τάξης με $gh = hg$, όπου όμως $\circ(gh) \neq \circ(g) \cdot \circ(h)$.

Λύση. (α′) Παρατηρούμε ότι $\forall n \in \mathbb{N}$, είναι $(gh)^n = g^n h^n$, διότι $gh = hg$. Έστω ε το ΕΚΠ$(\circ(g), \circ(h))$ των τάξεων $\circ(g)$ και $\circ(h)$. Τότε $(gh)^\varepsilon = g^\varepsilon h^\varepsilon = e_G$. Ως εκ τούτου, η τάξη $\circ(gh)$ είναι διαιρέτης τού ε.
(β′) Από το (α′) γνωρίζουμε ότι $(gh)^\varepsilon = e_G$. Έστω $n \in \mathbb{N}$ με $(gh)^n = e_G$. Αφού $e_G = (gh)^n = g^n h^n$, συμπεραίνουμε ότι $g^n = h^{-n} \in \langle g\rangle \bigcap \langle h\rangle$. Όμως η τομή $\langle g\rangle \bigcap \langle h\rangle$ ισούται με την τετριμμένη υποομάδα $\{e_G\}$, διότι ο ΜΚΔ$(\circ(g), \circ(h)) = 1$, βλ. την αμέσως προηγούμενη Άσκηση Α62. Γι' αυτό, $g^n = e_G = h^{-n}$ και ως εκ τούτου, ο n είναι κοινό πολλαπλάσιο των $\circ(g)$ και $\circ(h)$. Συνεπώς, το ελάχιστο κοινό πολλαπλάσιο ε είναι διαιρέτης τού n και έτσι το ε είναι ο πιο μικρός φυσικός n με $(gh)^n = e_G$. Άρα, $\circ(gh) = \varepsilon$. Αφού ο ΜΚΔ$(\circ(g), \circ(h)) = 1$, συμπεραίνουμε ότι $\varepsilon = \circ(g) \cdot \circ(h)$.
(γ′) Έστω ότι $\circ(g) = n$ και ότι $\circ(h) = m$.

Αν ο ΜΚΔ$(n, m) = 1$, τότε από το μέρος (β′), γνωρίζουμε ότι το στοιχείο gh έχει τάξη $\circ(gh) = \circ(g) \circ (h) = \varepsilon =$ ΕΚΠ(n, m).

Αν ο ΜΚΔ$(n, m) \neq 1$, τότε υπάρχουν κοινοί πρώτοι διαιρέτες των n και m. Θεωρούμε την πρωτογενή ανάλυση τού $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s} q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t}$ και την πρωτογενή ανάλυση τού $m = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_s^{\gamma_s} r_1^{\delta_1} r_2^{\delta_2} \dots r_w^{\delta_w}$, όπου όλοι οι πρώτοι p_i, q_j, r_j είναι ανά δύο διαφορετικοί και όπου πιθανόν το σύνολο $\{q_1, q_2, \dots, q_t\}$ ή/και το σύνολο $\{r_1, r_2, \dots, r_w\}$ να ισούται με το κενό σύνολο. Έστω το σύνολο $S := \{1, 2, \dots, s\}$ και τα υποσύνολά του $S_1 := \{i \in S \mid \alpha_i \geqq \gamma_i\}$ και $S_2 := S \setminus S_1$.
Το ΕΚΠ$(n, m) = \varepsilon$ των αριθμών n και m ισούται με

$$\prod_{i \in S_1} p_i^{\alpha_i} \prod_{j \in S_2} p_j^{\gamma_j} (q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t})(r_1^{\delta_1} r_2^{\delta_2} \dots r_w^{\delta_w}).$$

Θεωρούμε τα στοιχεία $g' = g^{\prod_{j \in S_2} p_j^{\alpha_j}}$ και $h' = h^{\prod_{i \in S_1} p_i^{\gamma_i}}$. Προφανώς, $g'h' = h'g'$.
Η τάξη $\circ(g')$ τού στοιχείου g' ισούται με $\frac{n}{\prod_{j \in S_2} p_j^{\alpha_j}} = \prod_{i \in S_1} p_i^{\alpha_i} (q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t})$ και η τάξη

$\circ(h')$ τού h' ισούται με $\frac{m}{\prod_{i\in S_1} p_i^{\gamma_i}} = \prod_{j\in S_2} p_j^{\gamma_j}(r_1^{\delta_1} r_2^{\delta_2}\dots r_w^{\delta_w})$. Επειδή ο ΜΚΔ$(\circ(g'),\circ(h')) = 1$, συμπεραίνουμε ότι η τάξη $\circ(g'h')$ ισούται με $\circ(g')\circ(h')$. Παρατηρώντας ότι το γινόμενο $\circ(g')\circ(h')$ είναι ακριβώς το ΕΚΠ$(\circ(g),\circ(h))$, συμπεραίνουμε ότι το στοιχείο $g'h'$ είναι ένα στοιχείο που διαθέτει την επιθυμητή τάξη.

Για την επιπλέον ερώτηση: Θεωρούμε την ομάδα $V = \{e, a, b, c\}$ των τεσσάρων στοιχείων. Η V είναι μια αβελιανή ομάδα και $\circ(a) = \circ(b) = \circ(c) = 2$. Η τάξη τού $a\cdot b = c$ είναι $\circ(c) = 2 \neq 4 = \circ(a)\cdot\circ(b)$.

Α 64. Έστω $(\mathbb{U}_{2^k},\cdot)$ η ομάδα των αντιστρέψιμων κλάσεων ισοτιμίας των ακεραίων mod 2^k, βλ. Παράδειγμα 1.2.21. Να δειχθεί ότι για κάθε $k\geq 3$, η $\mathbb{U}_{2^k}$ δεν είναι κυκλική.

Λύση. Στην $\mathbb{U}_{2^k}, k\geq 3$ θα εξασφαλίσουμε την ύπαρξη δύο στοιχείων τάξης 2. Στην περίπτωση αυτή, η $\mathbb{U}_{2^k}$ δεν μπορεί να είναι κυκλική, αφού αν ήταν τότε θα είχε ακριβώς ένα στοιχείο τάξης 2, διότι $\varphi(2) = 2-2^0 = 1$, βλ. και Άσκηση Α52. Οι κλάσεις $[2^k-1]_{2^k}$ και $[2^{k-1}+1]_{2^k}$ ανήκουν στην $\mathbb{U}_{2^k}$, αφού οι ΜΚΔ$(2^k-1,2^k)$ (το $k>0$) και ΜΚΔ$(2^{k-1}+1,2^k)$ (το $k>1$) ισούνται με 1. Επίσης είναι $[2^k-1]_{2^k}\neq[1]_{2^k}$, διότι $k\geq 2$ και προφανώς $[2^{k-1}+1]_{2^k}\neq[1]_{2^k}$. Συνεπώς, και τα δύο αυτά στοιχεία είναι $\neq[1]_{2^k}$.

Θα δείξουμε ότι η τάξη τους είναι 2. Πράγματι, $[2^k-1]^2_{2^k} = [1]_{2k}$, διότι $2^{2k}-2^{k+1}+1\equiv 1 \bmod 2^k$ και $[2^{k-1}+1]^2_{2^k} = [1]_{2k}$, διότι $2^{2k-2}+2^k+1\equiv 1 \bmod 2^k$, αφού $k\geq 2$.

Υπολείπεται η απόδειξη ότι $[2^k-1]_{2^k}\neq[2^{k-1}+1]_{2^k}$, όταν $k\geq 3$. Αν ήταν $[2^k-1]_{2^k} = [2^{k-1}+1]_{2^k}$, για κάποιο $k\geq 3$, τότε $2^k/2^k-2^{k-1}-2$. Επομένως, θα υπήρχε $\rho\in\mathbb{Z}$ με $2^k-2^{k-1}-2 = 2^k\rho$. Συνεπώς, θα ήταν $2^{k-1}-2^{k-2}-1 = 2^{k-1}\rho$ και επειδή $k-2\geq 1$, τότε το 2 θα ήταν διαιρέτης τού 1. Άτοπο!

Α 65. Έστω $(\mathbb{U}_{p^k},\cdot)$ η ομάδα των αντιστρέψιμων κλάσεων ισοτιμίας των ακεραίων mod p^k, βλ. Παράδειγμα 1.2.21, όπου ο p είναι ένας περιττός πρώτος αριθμός. Να δειχθεί ότι για κάθε $k\in\mathbb{N}$, η $\mathbb{U}_{p^k}$ είναι κυκλική.

Λύση. Κατ' αρχάς παρατηρούμε το εξής: (Π) Έστω ότι $[x]_{p^k}$ είναι ένα στοιχείο τής $\mathbb{U}_{p^k}$ με $k\geq 2$. Όταν για κάποιο $n\in\mathbb{N}$ είναι $[x]^n_{p^k} = [1]_{p^k}$, τότε για κάθε $k', 1\leq k'\leq k$, επίσης είναι $[x]^n_{p^{k'}} = [1]_{p^{k'}}$, αφού από $x^n\equiv 1 \bmod p^k$ έπεται $x^n\equiv 1 \bmod p^{k'}$, αφού ο p είναι πρώτος αριθμός.

Πρώτα θα δείξουμε ότι η $\mathbb{U}_{p^2}$ είναι κυκλική. Υπενθυμίζουμε ότι ήδη γνωρίζουμε ότι η $\mathbb{U}_p$ είναι κυκλική, βλ. Πόρισμα 1.5.22. Έστω ότι $\langle[a]_p\rangle = \mathbb{U}_p$. Ισχυριζόμαστε ότι είτε το $[a]_{p^2}$ είτε το $[a+p]_{p^2}$ είναι γεννήτορας τής $\mathbb{U}_{p^2}$. (Προσέξτε ότι στην $\mathbb{U}_p$ είναι $[a]_p = [a+p]_p$.)

Έστω μ η τάξη τού $[a]_{p^2}$ και ν η τάξη τού $[a+p]_{p^2}$. Από την προηγούμενη παρατήρηση (Π) έχουμε: $[a]^\mu_p = [1]_p$ και $[a+p]^\nu_p = [1]_p$. Ως εκ τούτου, η τάξη $p-1$ τού $[a]_p = [a+p]_p$ διαιρεί και την τάξη μ και την τάξη ν. Επιπλέον από το Θεώρημα Lagrange, γνωρίζουμε ότι οι τάξεις μ και ν είναι διαιρέτες τής τάξης $[\mathbb{U}_{p^2}:1] = p^2-p = p(p-1)$ τής ομάδας $\mathbb{U}_{p^2}$. Γι' αυτό οι δυνατές τιμές των τάξεων μ και ν είναι $p(p-1)$ και $p-1$. Αν αποκλείσουμε την περίπτωση $\mu = p-1$ και $\nu = p-1$, τότε ένα από τα στοιχεία $[a]_{p^2}$ και $[a+p]_{p^2}$ θα είναι γεννήτορας τής $\mathbb{U}_{p^2}$.

Αν ήταν $\mu = p-1$ και $\nu = p-1$, τότε θα ήταν $[a]^{p-1}_{p^2} = [1]_{p^2}$ και $[a+p]^{p-1}_{p^2} = [1]_{p^2}$.

Ισοδύναμα, θα είχαμε:

$$a^{p-1} \equiv 1 \bmod p^2 \text{ και}$$
$$(a+p)^{p-1} = a^{p-1} + \binom{p-1}{1}a^{p-2}p + \binom{p-1}{2}a^{p-3}p^2 + \cdots + p^{p-1} \equiv 1 \bmod p^2 \Leftrightarrow$$
$$(a+p)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}p \equiv 1 \bmod p^2 \Leftrightarrow 1 + (p-1)a^{p-2}p \equiv 1 \bmod p^2 \Leftrightarrow$$
$$(p-1)a^{p-2}p \equiv 0 \bmod p^2.$$

Όμως, $(p-1)a^{p-2}p \equiv 0 \bmod p^2 \Rightarrow (p-1)a^{p-2} \equiv 0 \bmod p$, το οποίο είναι άτοπο. Άρα, ένα από τα $[a]_{p^2}$ και $[a+p]_{p^2}$ έχει τάξη $p(p-1)$ και ως εκ τούτου, η $\mathbb{U}_{p^2}$ είναι κυκλική.

Θα δείξουμε τώρα με επαγωγή ως προς $k \geq 2$ την πρόταση:
Έστω $[b]_{p^2}$ ο γεννήτορας τής $\mathbb{U}_{p^2}$, ο οποίος ισούται ή με τον $[a]_{p^2}$ ή με τον$[a+p]_{p^2}$, όπου $[a]_p$ είναι ο γεννήτορας τής $\mathbb{U}_p$, όπως προηγουμένως. Ισχυριζόμαστε ότι για κάθε $k \geq 2$, το $[b]_{p^k}$ είναι γεννήτορας τής $\mathbb{U}_{p^k}$.

Για $k = 2$ δεν χρειάζεται να αποδείξουμε κάτι. Έστω ότι ο ισχυρισμός τής πρότασής μας είναι αληθής $\forall i, 2 \leq i \leq k$. Θα δείξουμε ότι είναι αληθής και για $k+1$. Με άλλα λόγια θα δείξουμε ότι το στοιχείο $[b]_{p^{k+1}}$ είναι γεννήτορας τής $\mathbb{U}_{p^{k+1}}$, δηλαδή ότι η τάξη του $\mu := \circ([b]_{p^{k+1}})$ ισούται με $p^k(p-1)$.
Κατ' αρχάς λόγω τής επαγωγικής υπόθεσης, όταν $k \geq 3$, τότε η τάξη τού $[b]_{p^k}$ είναι $p^{k-1}(p-1)$ και η τάξη τού $[b]_{p^{k-1}}$ είναι $p^{k-2}(p-1)$, (*). Προσέξτε όμως ότι αυτό αληθεύει και όταν $k=2$, χάρις στην επιλογή τού γεννήτορα $[b]_{p^2} = [a]_{p^2}$ ή $[b]_{p^2} = [a+p]_{p^2}$. Αφού $[b]^{\mu}_{p^{k+1}} = [1]_{p^{k+1}}$, συμπεραίνουμε, λόγω τής παρατήρησης (Π), ότι $[b]^{\mu}_{p^k} = [1]_{p^k}$. Γι' αυτό η τάξη $p^{k-1}(p-1)$ τού $[b]_{p^k}$ είναι διαιρέτης τής τάξης μ. Τώρα επειδή η τάξη μ τού $[b]_{p^{k+1}}$ είναι διαιρέτης τής τάξης $p^k(p-1)$, συμπεραίνουμε ότι ή $\mu = p^k(p-1)$ ή $\mu = p^{k-1}(p-1)$.

Θα αποδείξουμε ότι $[b]^{p^{k-1}(p-1)}_{p^{k+1}} \neq [1]_{p^{k+1}}$ και ότι ως εκ τούτου, $\mu = p^k(p-1)$ και $\mathbb{U}_{p^{k+1}} = \langle [b]_{p^{k+1}} \rangle$.
Πράγματι, από την (*) γνωρίζουμε ότι $[b]^{p^{k-2}(p-1)}_{p^{k-1}} = [1]_{p^{k-1}}$ (η τάξη τού $[b]_{p^{k-1}}$ είναι $p^{k-2}(p-1)$). Επομένως, $b^{p^{k-2}(p-1)} = 1 + \lambda p^{k-1}$. Επιπλέον, ο p δεν διαιρεί τον λ, διότι $[b]^{p^{k-2}(p-1)}_{p^k} \neq [1]_{p^k}$ (λόγω τής (*), η τάξη τού $[b]_{p^k}$ είναι $p^{k-1}(p-1)$), (**).
Έχουμε:

$$b^{p^{k-1}(p-1)} = (b^{p^{k-2}(p-1)})^p = (1+\lambda p^{k-1})^p = 1 + \binom{p}{1}\lambda p^{k-1} + \binom{p}{2}\lambda^2 p^{2(k-1)} + \cdots +$$
$$\binom{p}{p-1}\lambda^{p-1}p^{(p-1)(k-1)} + \lambda^p p^{p(k-1)} = 1 + \binom{p}{1}\lambda p^{k-1} + \sum_{i=2}^{p-1}\binom{p}{i}\lambda^i p^{i(k-1)} +$$
$$\lambda^p p^{p(k-1)}, (\dagger).$$

Η δύναμη p^{k+1} διαιρεί τον τελευταίο όρο του αθροίσματος, αφού $p(k-1) \geq k+1$ (διότι $(p-1)(k-1) \geq 1$, επειδή ο p είναι περιττός πρώτος και ο $k \geq 2$). Ακόμα, επειδή $k \geq 2$

είναι $2(k-1) \geq k$ και γι' αυτό $p^{2(k-1)} \geq p^k$. Συνεπώς, $p^{i(k-1)} \geq p^k, \forall i, 2 \leq i \leq p-1$. Ως εκ τούτου $\forall i, 2 \leq i \leq p-1$, ο p^{k+1} διαιρεί τον $\binom{p}{i}p^{i(k-1)}$, αφού ο πρώτος p είναι πάντοτε παράγοντας τού διωνυμικού συντελεστή $\binom{p}{i}, 1 \leq i \leq p-1$. Έτσι, από τη σχέση (†) έχουμε:

$$[b]_{p^{k+1}}^{p^{k-1}(p-1)} = [1]_{p^{k+1}} + [\lambda p^k]_{p^{k+1}}.$$

Αν ήταν $[b]_{p^{k+1}}^{p^{k-1}(p-1)} = [1]_{p^{k+1}}$, τότε θα ήταν $[\lambda p^k]_{p^{k+1}} = [0]_{p^{k+1}}$ και τότε ο p θα διαιρούσε το λ. Όμως αυτό αντιβαίνει στη (**). Επομένως, $[b]_{p^{k+1}}^{p^{k-1}(p-1)} \neq [1]_{p^{k+1}}$ και γι' αυτό $\mu = \circ([b]_{p^{k+1}}) = p^k(p-1)$, όπως ακριβώς θέλαμε.

A 66. Έστω η γενική γραμμική ομάδα $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ και τα στοιχεία της $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ και $B = \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$. Να δειχθεί ότι $\circ(A) = 2$, $\circ(B) = 2$ και ότι $\circ(AB) = \infty$.

Λύση. Ένα απλός υπολογισμός δείχνει ότι $A^2 = I_2$ και $B^2 = I_2$, όπου I_2 είναι ο ταυτοτικός 2×2 πίνακας. Επομένως, η τάξη των A, B είναι διαιρέτης τού 2 και αφού οι A, B δεν είναι οι ταυτοτικοί πίνακες συμπεραίνουμε ότι $\circ(A) = \circ(B) = 2$.

Με τη βοήθεια μιας πολύ απλής επαγωγικής απόδειξης διαπιστώνεται ότι $\forall n \in \mathbb{N}, (AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. Ως εκ τούτου, $\circ(AB) = \infty$.

Παρατηρούμε ότι γενικά το γινόμενο δύο στοιχείων πεπερασμένης τάξης μπορεί να είναι ένα στοιχείο άπειρης τάξης.

A 67. Έστω ότι $(G, \star)$ είναι μια κυκλική ομάδα άπειρης τάξης. Να δειχθεί ότι για κάθε φυσικό n, υπάρχει ακριβώς μία υποομάδα H τής G με δείκτη $[G : H] = n$.

Λύση. Έστω ότι $G = \langle a \rangle$ και H μια υποομάδα της. Από το Θεώρημα 1.5.14, γνωρίζουμε ότι η H είναι επίσης κυκλική και ότι παράγεται από κάποιο στοιχείο $g = a^n$. Μπορούμε χωρίς περιορισμό τής γενικότητας να δεχθούμε ότι $n \in \mathbb{N} \cup \{0\}$, αφού $\langle a^n \rangle = \langle a^{-n} \rangle$.

Θα δείξουμε ότι για δοσμένο $n \in \mathbb{N}$, ο δείκτης $[G : \langle a^n \rangle]$ ισούται με n. Θεωρούμε τις (αριστερές) πλευρικές κλάσεις $a^0H, a^1H, \ldots, a^{n-1}H$. Ισχυριζόμαστε ότι για $i \neq j, 0 \leq i, j \leq n-1$ είναι $a^iH \neq a^jH$. Πράγματι, αν ήταν $a^iH = a^jH$, τότε το $a^{|i-j|}$ θα ανήκε στην $H = \langle a^n \rangle$ και γι' αυτό θα ήταν $a^{|i-j|} = (a^n)^\lambda, \lambda \in \mathbb{Z}$. Όμως τότε $a^{|i-j|-n\lambda} = e_G$ και τότε $|i-j| - n\lambda = 0$, επειδή η τάξη τού a είναι άπειρη. Άρα, $|i-j| = n\lambda$, το οποίο είναι άτοπο αφού τώρα το λ οφείλει να είναι > 0 (διότι $|i-j| > 0$) και αφού $n \gneqq |i-j|$.
Τώρα ισχυριζόμαστε ότι οι $a^iH, 0 \leq i \leq n-1$ είναι όλες οι πλευρικές κλάσεις τής H στη G. Πράγματι, όταν $a^\rho \in G, \rho \in \mathbb{Z}$, τότε διαιρώντας με υπόλοιπο το ρ δια τού n έχουμε $\rho = \kappa n + \upsilon$ με $0 \leq \upsilon \leq n-1$. Επομένως $a^\rho = a^\upsilon(a^n)^\kappa$ και το a^ρ ανήκει στην πλευρική κλάση $a^\upsilon H$.

Άρα, όταν $H = \langle a^n \rangle, n \in \mathbb{N}$, τότε $[G : H] = n$. Αν τώρα, L είναι μια ακόμα υποομάδα τής G με $[G : L] = n$, τότε επειδή η $L = \langle a^s \rangle, s \in \mathbb{N} \cup \{0\}$ και αφού $s \neq 0$ (διότι διαφορετικά θα ήταν $[G : L] = \infty$) θα πρέπει $[G : L] = s$. Άρα, $s = n$ και $L = H$.

Α 68. Έστω $(G, \star)$ μια κυκλική ομάδα τάξης n και m οποιοσδήποτε φυσικός αριθμός. Έστω $\mathcal{C}(m)$ το σύνολο των υποομάδων τής G, η τάξη των οποίων είναι κάποιος διαιρέτης τού m. Για κάθε υποομάδα C τής G, συμβολίζουμε με $\mathcal{G}\{C\}$ το σύνολο των γεννητόρων της. Να δειχθεί ότι το πλήθος των στοιχείων τού συνόλου $\bigcup_{C \in \mathcal{C}(m)} \mathcal{G}\{C\}$ ισούται με τον ΜΚΔ(n, m).

Λύση. Ως γνωστόν, σε κάθε διαιρέτη d τής τάξης n τής G, υπάρχει ακριβώς μία υποομάδα C_d τάξης d, βλ. Πρόταση 1.5.16. Γι'αυτό το σύνολο $\mathcal{C}(m)$ ισούται με $\{C_{d_s} \mid 1 \leq s \leq \rho\}$, όπου $\Delta = \{d_1, d_2, \ldots, d_\rho\}$ είναι το σύνολο[22] των κοινών διαιρετών των n και m. Όταν οι C και C' είναι δύο διαφορετικές υποομάδες τής G, τότε τα αντίστοιχα σύνολα $\mathcal{G}\{C\}$ και $\mathcal{G}\{C'\}$ των γεννητόρων των C και C' είναι αποσυνδετά. Επομένως,

$$\left| \bigcup_{C \in \mathcal{C}(m)} \mathcal{G}\{C\} \right| = \sum_{C \in \mathcal{C}(m)} |\mathcal{G}\{C\}| = \sum_{i=1}^{\rho} |\mathcal{G}\{C_{d_i}\}| = \sum_{d \in \Delta} \varphi(d),$$

αφού το πλήθος των γεννητόρων μιας κυκλικής ομάδας τάξης d είναι $\varphi(d)$, βλ. Πρόταση 1.5.16. Παρατηρώντας ότι το σύνολο Δ των κοινών διαιρετών των n και m είναι ακριβώς το σύνολο των διαιρετών τού ΜΚΔ(n, m), συμπεραίνουμε ότι το $\sum_{d \in \Delta} \varphi(d)$, που είναι το τελευταίο μέλος των ανωτέρω ισοτήτων, ισούται με $\sum_{d | \text{ΜΚΔ}(n,m)} \varphi(d)$.
Αλλά $\sum_{d |\ \text{ΜΚΔ}(n,m)} \varphi(d) =$ ΜΚΔ(n, m), βλ. Πόρισμα 1.5.19.

Προτεινόμενες Ασκήσεις

ΠΑ 52. Να ευρεθεί η τάξη τού στοιχείου α^{30} τής κυκλικής ομάδας $G = \langle \alpha \rangle$, όπου $\circ(a) =$ 54.

ΠΑ 53. Να ευρεθούν όλες οι υποομάδες τής $(\mathbb{Z}_{64}, +)$, προσδιορίζοντας σε κάθε περίπτωση έναν γεννήτορά τους.

ΠΑ 54. Έστω ότι g, h είναι στοιχεία μιας ομάδας $(G, \star)$ με τάξεις $\circ(g) = 12$ και $\circ(b) = 22$. Αν $\langle g \rangle \bigcap \langle h \rangle \neq \{e_G\}$, τότε να δειχθεί ότι $g^6 = h^{11}$.

ΠΑ 55. Έστω ότι $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι δύο κυκλικές ομάδες, όπου $G_1 = \langle \alpha \rangle$ και $G_2 = \langle \beta \rangle$ με $\circ(\alpha) = 12$ και $\circ(\beta) = 18$. Να βρεθεί το σύνολο των στοιχείων (g, g') τού ευθέος γινομένου $G_1 \times G_2$, που έχουν τάξη 3, αντιστοίχως 4, αντιστοίχως 6.

ΠΑ 56. Έστω το ευθύ γινόμενο $G = \mathbb{Z}_4 \times \mathbb{Z}_{12}$ των $(\mathbb{Z}_4, +)$ και $(\mathbb{Z}_{12}, +)$.

(α′) Να βρεθεί η τάξη των στοιχείων $([3]_4, [10]_{12})$ $([2]_4, [6]_{12})$ και $([3]_4, [0]_{12})$.

(β′) Να εξεταστεί αν η G είναι μια κυκλική ομάδα, χωρίς να υπολογίσετε την τάξη και των 48 στοιχείων της.

ΠΑ 57. Στο ευθύ γινόμενο $D_3 \times \mathbb{Z}_2$ τής διεδρικής ομάδας $(D_3, \circ)$ με την κυκλική ομάδα $(\mathbb{Z}_2, +)$ να προσδιοριστεί ένα στοιχείο τάξης 6.

[22] Το σύνολο Δ είναι πάντοτε $\neq \emptyset$, διότι το $1 \in \Delta$.

ΠΑ 58. Έστω ότι $(\mathbb{Z}, +)$ είναι η ομάδα των ακέραιων αριθμών και ότι m, n είναι δύο φυσικοί αριθμοί. Να δειχθεί ότι

(α′) η τομή $\langle m \rangle \bigcap \langle n \rangle$ των υποομάδων $\langle m \rangle$ και $\langle n \rangle$ ισούται με $\langle \varepsilon \rangle$, όπου ε είναι το ελάχιστο κοινό πολλαπλάσιο των m και n.

(β′) η υποομάδα $\langle m \rangle + \langle n \rangle$ τής $\mathbb{Z}$, ισούται με $\langle \delta \rangle$, όπου δ είναι ο μέγιστος κοινός διαιρέτης ΜΚΔ(m, n) των m και n.

ΠΑ 59. Να δειχθεί ότι μια μη αβελιανή ομάδα $(G, \star)$ τάξης $[G : 1] = 8$ έχει πάντοτε ένα στοιχείο a τάξης $\circ(a) = 4$.

ΠΑ 60. Έστω η γενική γραμμική ομάδα $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ και το υποσύνολό της

$$\mathcal{C} = \left\{ \begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix} \mid z \in \mathbb{Z} \right\}.$$

Να δειχθεί ότι το $\mathcal{C}$ είναι μια κυκλική υποομάδα τής $\mathrm{GL}_2(\mathbb{R})$ άπειρης τάξης.

ΠΑ 61. Έστω η γενική γραμμική ομάδα $(\mathrm{GL}_2(\mathbb{R}), \cdot)$ και το υποσύνολό της

$$G = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mid a^2 + b^2 \neq 0 \right\}.$$

Να δειχθεί ότι το σύνολο G είναι μια υποομάδα τής $\mathrm{GL}_2(\mathbb{R})$ και ότι για κάθε $n \in \mathbb{N}$, υπάρχει $A \in G$ με $\circ(A) = n$.

ΠΑ 62. Έστω η ομάδα $(\mathbb{R}, +)$ και το ευθύ γινόμενο $(\mathbb{R} \times \mathbb{R}, \star)$ τής $\mathbb{R}$ με τον εαυτό της. Να δειχθεί ότι η $\mathbb{R} \times \mathbb{R}$ δεν είναι κυκλική.

ΠΑ 63. Έστω $(\mathbb{U}_n, \cdot)$ η ομάδα των αντιστρέψιμων κλάσεων ισοτιμίας των ακεραίων mod$n$, βλ. Παράδειγμα 1.2.21. Να δειχθεί ότι για κάθε $n \in \{2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14, 17, 18, 19\}$, η αντίστοιχη ομάδα $\mathbb{U}_n$ είναι κυκλική και σε καθεμιά από τις περιπτώσεις να βρεθούν όλοι οι γεννήτορες.

ΠΑ 64. Να βρεθούν οι κυκλικές υποομάδες τής $(\mathbb{U}_{30}, \cdot)$.

ΠΑ 65. Έστω $(G, \star)$ μια ομάδα άπειρης τάξης. Να δειχθεί ότι το πλήθος των υποομάδων της είναι άπειρο.

ΠΑ 66. Έστω ότι μια ομάδα $(G, \star)$ έχει ακριβώς m το πλήθος υποομάδες τάξης p, όπου ο p είναι ένας πρώτος αριθμός. Να δειχθεί ότι η G έχει ακριβώς $m(p-1)$ το πλήθος στοιχεία τάξης p.

ΠΑ 67. Έστω ότι $(G_i, \star_i), 2 \leq i \leq n$, είναι n το πλήθος ομάδες. Να δειχθεί ότι το καρτεσιανό γινόμενο $G_1 \times G_2 \times \cdots \times G_n$ εφοδιασμένο με την πράξη

$$\begin{aligned} \star : &(G_1 \times G_2 \times \cdots \times G_n) \times (G_1 \times G_2 \times \cdots \times G_n) \to G_1 \times G_2 \times \cdots \times G_n, \\ &((a_1, a_2, \ldots, a_n), (b_1, b_2, \ldots, _n b)) \mapsto (a_1 \star_1 b_1, a_2 \star_2 b_2, \ldots, a_n \star_n b_n) \end{aligned}$$

αποτελεί μια ομάδα, βλ. Άσκηση Α18.
(Η συγκεκριμένη ομάδα ονομάζεται το (εξωτερικό) *ευθύ γινόμενο* των ομάδων $G_1, G_2, \ldots, G_n$.).

ΠΑ 68. Έστω ότι $(G_i, \star_i), 2 \leq i \leq n$, είναι n το πλήθος κυκλικές ομάδες με τάξεις $[G_i : 1] = m_i, 1 \leq i \leq n$ αντιστοίχως. Να δειχθεί ότι το εξωτερικό ευθύ γινόμενο $(G_1 \times G_2 \times \cdots \times G_n, \star)$ είναι κυκλική ομάδα, αν και μόνο αν, ο ΜΚΔ$(m_1, m_2, \ldots, m_n) = 1$. (Υπόδειξη: Άσκηση Α60.)

1.6 Ορθόθετες Υποομάδες, Πηλικοομάδες

Ορθόθετες Υποομάδες

Ανάμεσα στις υποομάδες μιας ομάδας ιδιαίτερη θέση κατέχουν οι υποομάδες που κάθε αριστερή πλευρική τους κλάση ισούται με μια δεξιά, αφού στην περίπτωση αυτή η διαμέριση τής ομάδας στις αριστερές πλευρικές κλάσεις είναι ταυτόσημη με την αντίστοιχη διαμέρισή της στις δεξιές πλευρικές κλάσεις.

Ορισμός 1.6.1. Έστω $(G, \star)$ μια ομάδα και K μια υποομάδα τής G. Η K ονομάζεται μια *ορθόθετη* ή *κανονική* υποομάδα τής G, όταν $\forall g \in G$ είναι $gH = Hg$.

Συμβολισμός. Συχνά, δηλώνουμε ότι μια υποομάδα $K \leq G$ μιας ομάδας $(G, \star)$ είναι ορθόθετη, γράφοντας $K \trianglelefteq G$. Αν μάλιστα πρόκειται για γνήσια υποομάδα και θέλουμε αυτό να το τονίσουμε, τότε γράφουμε $K \triangleleft G$.

Παρατήρηση 1.6.2. Για $K \leq G$, υπάρχει και μια ασθενέστερη εκδοχή τού προηγούμενου ορισμού:

$$\forall g \in G, \exists h \in G : \quad gK = Kh. \tag{*}$$

Πράγματι, όταν $gK = Kh$, τότε το $g \in Kh$, επομένως $Kg = Kh$ και συνεπώς $gK = Kg$. Αντίστροφα, μια υποομάδα K, που ικανοποιεί τον Ορισμό 1.6.1, ικανοποιεί και την (*).

Προφανώς, οι τετριμμένες υποομάδες $\{e_G\}$ και G μιας ομάδας $(G, \star)$, είναι πάντοτε ορθόθετες. Όταν η $(G, \star)$ είναι μια αβελιανή ομάδα, τότε κάθε υποομάδα της K είναι ορθόθετη, αφού $\forall g \in G$ και $\forall k \in K$ είναι $gk = kg$. Άρα, $gK = Kg$. Επαναλαμβάνοντας το επιχείρημα βλέπουμε αμέσως ότι το κέντρο $\mathcal{Z}(G)$ μιας ομάδας $(G, \star)$ είναι πάντοτε ορθόθετη υποομάδα τής G.

Ωστόσο, κάθε υποομάδα μιας ομάδας δεν είναι απαραίτητα ορθόθετη. Στο Παράδειγμα 1.4.6, είχαμε θεωρήσει την ομάδα $(S_3, \circ)$ και την κυκλική υποομάδα της $T_1 = \langle \tau_1 \rangle$ και είχαμε διαπιστώσαμε ότι η αριστερή πλευρική κλάση $\tau_2 \circ T_1$ είναι διαφορετική από τη δεξιά πλευρική κλάση $T_1 \circ \tau_2$. Επομένως η T_1 δεν είναι ορθόθετη υποομάδα τής S_3.

Θεώρημα 1.6.3. *Έστω $(G, \star)$ μια ομάδα και K μια υποομάδα τής G. Τα επόμενα είναι ισοδύναμα:*

(α′) $K \trianglelefteq G$.

(β′) $\forall g \in G, \;\; gKg^{-1} \subseteq K$.

(γ′) $\forall g \in G, \;\; gKg^{-1} = K$.

Απόδειξη. «(α′)⇒(β′)» Όταν $x \in gKg^{-1}$, τότε $\exists k \in K$ με $x = gkg^{-1}$. Το gk ανήκει στην αριστερή πλευρική κλάση gK, η οποία ισούται με τη δεξιά πλευρική κλάση Kg, αφού $K \trianglelefteq G$. Επομένως, $\exists k' \in K$ με $gk = k'g$ και έτσι το $x = gkg^{-1} = k'gg^{-1} = k'$ είναι στοιχείο τής K. Άρα, $gKg^{-1} \subseteq K$.
«(β′)⇒(γ′)» Όταν $\forall g \in G$, είναι $gKg^{-1} \subseteq K$, τότε επίσης $\forall g \in G$, είναι $g^{-1}K(g^{-1})^{-1} \subseteq K$, δηλαδή $g^{-1}Kg \subseteq K$. Τώρα η $g^{-1}Kg \subseteq K$ δίνει $g(g^{-1}Kg)g^{-1} = K \subseteq gKg^{-1}$. Άρα, $\forall g \in G$, είναι $K \subseteq gKg^{-1}$. Συνεπώς, $\forall g \in G$, είναι $gKg^{-1} = K$.
«(γ′)⇒(α′)» Προφανώς,

$$\forall g \in G, gKg^{-1} = K \Leftrightarrow \forall g \in G, (gKg^{-1})g = Kg \Leftrightarrow \forall g \in G, gK = Kg.$$

Επομένως, $K \trianglelefteq G$. □

Στα επόμενα παραδείγματα παρουσιάζουμε παραδείγματα ορθόθετων υποομάδων από μη μεταθετικές (μη αβελιανές) ομάδες, αφού όπως είδαμε λίγο παραπάνω οι υποομάδες μιας αβελιανής ομάδας είναι πάντοτε ορθόθετες.

Παράδειγμα 1.6.4. Θεωρούμε την ομάδα ισομετριών τού τετραγώνου, δηλαδή τη διεδρική ομάδα $D_4 = \{\mathrm{Id}_4, \tau, \rho, \rho^2, \rho^3, \tau \circ \rho, \tau \circ \rho^2, \tau \circ \rho^3\}$, βλ. Άσκηση Α25. Υπενθυμίζουμε ότι $\tau^2 = \mathrm{Id}_4$, $\rho^4 = \mathrm{Id}_4$ και ότι $\rho \circ \tau = \tau \circ \rho^{-1}$.

Το σύνολο $K = \{\mathrm{Id}_4, \tau, \rho^2, \tau\circ\rho^2\}$ είναι μια υποομάδα τής D_4, αφού είναι πεπερασμένο και κλειστό ως προς την πράξη τής σύνθεσης «$\circ$» τής D_4. Ο δείκτης $[D_4 : K]$ ισούται με $[D_4 : 1]/[K : 1] = 8/4 = 2$. Οι διαφορετικές αριστερές πλευρικές κλάσεις τής K στη D_4 είναι οι $\mathrm{Id}_4K = K$ και ρK. Αντίστοιχα οι διαφορετικές δεξιές πλευρικές κλάσεις είναι οι $K\mathrm{Id}_4 = K$ και $K\rho$. Έστω ξ οποιοδήποτε στοιχείο τής D_4. Επειδή το σύνολο των αριστερών πλευρικών κλάσεων $\{K, \rho K\}$ αποτελεί μια διαμέριση τής D_4, το ξ θα ανήκει ή στο K ή στο ρK. Αν το $\xi \in K$, τότε $\xi K = K = K\xi$. Αν το $\xi \in \rho K$, τότε το $\xi \notin K$ και γι' αυτό $\xi K = \rho K$. Αφού το σύνολο των δεξιών πλευρικών κλάσεων $\{K, K\rho\}$ αποτελεί επίσης μια διαμέριση τής D_4, συμπεραίνουμε ότι το $\xi \in K\rho$ και ως εκ τούτου $K\xi = K\rho$. Ένας απλός υπολογισμός δίνει ότι $\rho K = K\rho$. Άρα $\forall \xi \in D_4$, $\xi K = K\xi$, δηλαδή $K \trianglelefteq D_4$.

Σύντομα θα αποδείξουμε, βλ. Άσκηση 70, ακολουθώντας μια σχεδόν πανομοιότυπη διαδικασία ότι κάθε υποομάδα με δείκτη ίσο με 2 είναι ορθόθετη.

Ας θεωρήσουμε τώρα την υποομάδα $H = \{\mathrm{Id}_4, \tau\}$ τής D_4, η οποία βέβαια είναι και υποομάδα τής K. Παρατηρούμε[23] ότι η H ως υποομάδα τής K είναι ορθόθετη. Ωστόσο, η H δεν είναι ορθόθετη ως υποομάδα τής D_4, αφού $H\rho = \{\mathrm{Id}_4, \tau \circ \rho\} \neq \rho H = \{\mathrm{Id}_4, \rho \circ \tau\}$, διότι $\rho \circ \tau = \tau \circ \rho^3 \neq \tau \circ \rho$.

Έτσι, βλέπουμε ότι δεν ισχύει η μεταβατικότητα στην περίπτωση ορθόθετων υποομάδων, δηλαδή μπορεί να ισχύει ότι $H \trianglelefteq K$ και $K \trianglelefteq G$, χωρίς όμως να ισχύει απαραίτητα ότι $H \trianglelefteq K$.

Παράδειγμα 1.6.5. Θεωρούμε την ομάδα $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ των αντιστρέψιμων $n \times n$ πινάκων με συνιστώσες από τους πραγματικούς αριθμούς και την υποομάδα της $\mathrm{SL}_n(\mathbb{R})$ που αποτελείται από τους πίνακες A με ορίζουσα $\det A = 1$, βλ. Παράδειγμα 1.3.5(στ′). Για κάθε $X \in \mathrm{GL}_n(\mathbb{R})$ και κάθε $A \in \mathrm{SL}_n(\mathbb{R})$, είναι $\det(XAX^{-1}) = \det(X)\det(A)\det(X)^{-1} = \det(A) = 1$. Επομένως, $\forall X \in \mathrm{GL}_n(\mathbb{R})$ είναι $X\mathrm{SL}_n(\mathbb{R})X^{-1} \subseteq \mathrm{SL}_n(\mathbb{R})$ και γι' αυτό $\mathrm{SL}_n(\mathbb{R}) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$.

[23] Αφού η K είναι αβελιανή!

Οι ορθόθετες υποομάδες τής διεδρικής ομάδας $(D_n, \circ)$

Από το Θεώρημα 1.5.24 γνωρίζουμε ότι όταν H είναι μια υποομάδα τής D_n, τότε ή $H = \langle \rho^{n/d} \rangle$ ή $H = \langle \{\rho^{n/d}, \tau \circ \rho^{\upsilon}\} \rangle$, όπου ο d είναι ένας φυσικός διαιρέτης τού n και όπου για κάθε τέτοιον d, ο αριθμός υ παίρνει τις τιμές $0, 1, \ldots, (n/d) - 1$.

Πρώτη Περίπτωση Κάθε υποομάδα τής μορφής $H = \langle \rho^{n/d} \rangle$ με $d \mid n$ είναι μια ορθόθετη υποομάδα τής D_n, αφού για κάθε $\tau \circ \rho^s \in D_n, 0 \leq s \leq n-1$ και κάθε στοιχείο $\rho^{\lambda(n/d)} \in H = \langle \rho^{n/d} \rangle$ είναι:

$$\tau \circ \rho^s \circ \rho^{\lambda(n/d)} \circ (\tau \circ \rho^s)^{-1} = \tau \circ \rho^s \circ \rho^{\lambda(n/d)} \circ \rho^{-s} \circ \tau = \tau \circ \rho^{\lambda(n/d)} \circ \tau =$$
$$\tau \circ \tau \circ \rho^{-\lambda(n/d)} = \rho^{-\lambda(n/d)} \in H = \langle \rho^{n/d} \rangle$$

και αφού προφανώς για κάθε $\rho^s \in D_n, 0 \leq s \leq n-1$ είναι $\rho^s \circ H \circ \rho^{-s} = \rho^s \circ \langle \rho^{n/d} \rangle \circ \rho^{-s} = \langle \rho^{n/d} \rangle = H$.

Δεύτερη Περίπτωση Για να είναι ορθόθετη μια υποομάδα τής μορφής $H = \langle \{\rho^{n/d}, \tau \circ \rho^{\upsilon}\} \rangle$, θα πρέπει ιδιαιτέρως να είναι το $\rho \circ (\tau \circ \rho^{\upsilon}) \circ \rho^{-1} = \rho \circ (\tau \circ \rho^{\upsilon-1}) = \tau \circ \rho^{\upsilon-2}$ ένα στοιχείο τής H. Αλλά όπως έχουμε ήδη διαπιστώσει η H είναι η ένωση των αριστερών πλευρικών κλάσεων $\mathrm{Id}_n \circ \langle \rho^{n/d} \rangle$ και $(\tau \circ \rho^{\upsilon}) \circ \langle \rho^{n/d} \rangle$. Επομένως, το $\tau \circ \rho^{\upsilon-2}$ θα πρέπει να ανήκει στην αριστερή πλευρική κλάση $(\tau \circ \rho^{\upsilon}) \circ \langle \rho^{n/d} \rangle$ και γι' αυτό θα πρέπει να είναι $\tau \circ \rho^{\upsilon-2} = \tau \circ \rho^{\upsilon} \circ \rho^{\lambda(n/d)}, \lambda \in \mathbb{Z}$. Η τελευταία ισότητα δίνει $\rho^{-2} = \rho^{\lambda(n/d)}$ ή ισοδύναμα $\mathrm{Id}_n = \rho^{\lambda(n/d)+2}$ και αφού $\circ(\rho) = n$, συμπεραίνουμε ότι $n \mid \lambda(n/d) + 2$. Επομένως, $nd \mid \lambda n + 2d$ και ως εκ τούτου $n \mid 2d$. Αφού, ο d είναι διαιρέτης τού n καταλήγουμε στο συμπέρασμα ότι $(n/d) \mid 2$ και $(n/d) = 1$ ή 2.

Αν ο n είναι περιττός, τότε $(n/d) = 1$ από όπου προκύπτει ότι η $H = \langle \{\rho, \tau \circ \rho^{\upsilon}\} \rangle$ με $\upsilon = 0$, δηλαδή η H ισούται με την $\langle \{\rho, \tau\} \rangle = D_n$. Προφανώς $D_n \trianglelefteq D_n$.

Αν ο n είναι άρτιος, τότε η περίπτωση $(n/d) = 1$, δίνει και πάλι $H = D_n$. Η περίπτωση $(n/d) = 2$ δίνει $H = \langle \{\rho^2, \tau \circ \rho^{\upsilon}\} \rangle$ με $\upsilon = 0$ ή 1. Έτσι προκύπτουν οι υποομάδες $H_0 = \langle \{\rho^2, \tau\} \rangle$ και $H_1 = \langle \{\rho^2, \tau \circ \rho\} \rangle$. Η τάξη τής H_0 καθώς και τής H_1 ισούται με n, βλ. Θεώρημα 1.5.24, και γι' αυτό και οι δύο τους έχουν δείκτη 2 στην D_n. Από την Άσκηση Α70, γνωρίζουμε ότι κάθε υποομάδα δείκτου 2 είναι ορθόθετη, επομένως $H_0 \trianglelefteq D_n$ και $H_1 \trianglelefteq D_n$. Συνοψίζοντας:

Θεώρημα 1.6.6. *Έστω $(D_n, \circ)$ η διεδρική ομάδα τάξης $2n$. Για κάθε φυσικό διαιρέτη d τού n, οι υποομάδες $\langle \rho^{n/d} \rangle$ τής διεδρικής ομάδας $(D_n, \circ)$ είναι ορθόθετες.*

(α′) *Όταν ο n είναι περιττός, τότε οι προηγούμενες υποομάδες $\langle \rho^{n/d} \rangle$ μαζί με την D_n απαρτίζουν το σύνολο των ορθόθετων υποομάδων τής D_n.*

(β′) *Όταν ο n είναι άρτιος, τότε οι $\langle \{\rho^2, \tau\} \rangle$, $\langle \{\rho^2, \tau \circ \rho\} \rangle$ μαζί με προηγούμενες υποομάδες $\langle \rho^{n/d} \rangle$ και την D_n απαρτίζουν το σύνολο των ορθόθετων υποομάδων τής D_n.*

Πόρισμα 1.6.7. *Το πλήθος των ορθόθετων υποομάδων τής $(D_n, \circ)$ ισούται με $\sigma_0(n) + 1$, όταν ο n είναι περιττός και με $\sigma_0(n) + 3$, όταν ο n είναι άρτιος.*

Πηλικοομάδες

Όταν $(G, \star)$ είναι μια ομάδα και K είναι μια ορθόθετη υποομάδα της, τότε το σύνολο των αριστερών πλευρικών κλάσεων τής K στην G συμπίπτει με το σύνολο των δεξιών πλευρικών κλάσεων τής K στην G. Στην περίπτωση αυτή συμβολίζουμε το σύνολο $\{gK \mid g \in G\}$ με G/K και τα στοιχεία του τα ονομάζουμε απλώς *πλευρικές κλάσεις*.

Υπενθυμίζουμε ότι γενικά όταν L και L' είναι δύο μη κενά υποσύνολα τής G, τότε παριστάνουμε με LL' το υποσύνολο τής G που αποτελείται από τα γινόμενα $\ell\ell'$, όπου $\ell \in L$ και $\ell' \in L'$, βλ. Άσκηση A37.

Παρατηρούμε ότι όταν gK και $g'K$ είναι δύο πλευρικές κλάσεις, τότε για το σύνολο $(gK)(g'K)$έχουμε:

$$(gK)(g'K) = g(Kg')K = g(g'K)K = (gg')(KK) = (gg')K.$$

Επομένως, το $(gK)(g'K)$ είναι και πάλι μια πλευρική κλάση, δηλαδή ένα στοιχείο τού συνόλου G/K των πλευρικών κλάσεων τής K στην G. Ως εκ τούτου, η αντιστοιχία

$$\circledast : G/K \times G/K \to G/K, (gK, g'K) \mapsto gK \circledast g'K := (gg')K$$

είναι μια πράξη επί τού G/K, η οποία είναι μάλιστα προσεταιριστική, αφού $\forall g, g', g'' \in G$ είναι

$$\begin{gathered} gK \circledast (g'K \circledast g''K) = gK \circledast ((g'g'')K) = (g(g'g''))K = \\ ((gg')g'')K = ((gg')K) \circledast g''K = (gK \circledast g'K) \circledast g''K. \end{gathered}$$

Πρόταση 1.6.8. *Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι $K \trianglelefteq G$ είναι μια ορθόθετη υποομάδα τής G. Το ζεύγος $(G/K, \circledast)$ αποτελεί μια ομάδα.*

Απόδειξη. Όπως έχουμε ήδη διαπιστώσει, η «$\circledast$» είναι μια προσεταιριστική πράξη επί τού συνόλου G/K των πλευρικών κλάσεων. Η κλάση e_GK είναι το ουδέτερο στοιχείο της, αφού $\forall gK \in G/K$ είναι $e_GK \circledast gK = (e_Gg)K = gK = (ge_G)K = gK \circledast e_GK$. Τέλος, όταν $gK \in G/K$, τότε θεωρώντας την πλευρική κλάση με αντιπρόσωπο το αντίστροφο τού g, δηλαδή θεωρώντας την πλευρική κλάση $g^{-1}K$, έχουμε: $gK \circledast g^{-1}K = (gg^{-1})K = e_GK = (g^{-1}gK) = g^{-1}K \circledast gK$. Επομένως, το $g^{-1}K$ είναι το αντίστροφο τού gK στην G/K, δηλαδή $(gK)^{-1} = g^{-1}K$. Άρα, το ζεύγος $(G/K, \circledast)$ είναι μια ομάδα. □

Ορισμός 1.6.9. Η ομάδα $(G/K, \circledast)$ ονομάζεται η *πηλικοομάδα* ή *ομάδα πηλίκο* τής G ως προς την ορθόθετη υποομάδα K.

Ακολουθώντας την πάγια πρακτική ως προς τον συμβολισμό των πράξεων, θα παριστάνουμε την πράξη μεταξύ δύο πλευρικών κλάσεων gK και $g'K$ γράφοντας απλώς $gKg'K$ αντί τού $gK \circledast g'K$.

Παράδειγμα 1.6.10. Έστω ότι $(\mathbb{Z}, +)$ είναι η ομάδα των ακεραίων και ότι H είναι μια μη τετριμμένη υποομάδα της. Από το Παράδειγμα 1.5.15 γνωρίζουμε ότι υπάρχει κάποιος ακέραιος αριθμός $n > 1$ με $H = \langle n \rangle = n\mathbb{Z}$. Θεωρούμε την πηλικοομάδα $\mathbb{Z}/\langle n \rangle = \{a + \langle n \rangle \mid a \in \mathbb{Z}\}$. Στην Άσκηση A43 διαπιστώσαμε ότι $a + \langle n \rangle = b + \langle n \rangle$, αν και μόνο αν, ο

n διαιρεί τη διαφορά $a - b$. Χάρις στην παρατήρηση αυτή, θα αποδείξουμε ότι το σύνολο των στοιχείων τής πηλικοομάδας $\mathbb{Z}/n\mathbb{Z}$ είναι το:

$$\mathbb{Z}/\langle n\rangle = \{0 + \langle n\rangle, 1 + \langle n\rangle, \dots, (n-1) + \langle n\rangle\}.$$

Κατ' αρχάς, ισχυριζόμαστε ότι οι κλάσεις $i + \langle n\rangle, 0 \leq i \leq (n-1)$ είναι ανά δύο διαφορετικές, αφού όταν ισχύει ότι $i + \langle n\rangle = j + \langle n\rangle, 0 \leq i, j \leq (n-1)$, τότε ο n διαιρεί τη διαφορά $i - j$ και την απόλυτη τιμή της $|i - j|$. Αφού όμως $0 \leq |i - j| \leq (n-1)$, συμπεραίνουμε ότι $|i - j| = 0$ και έτσι $i = j$.

Τώρα θα δείξουμε ότι κάθε κλάση $a + \langle n\rangle$ ισούται με κάποια από τις κλάσεις $i + \langle n\rangle, 0 \leq i \leq (n-1)$. Πράγματι, εκτελώντας διαίρεση με υπόλοιπο τού a διά τού n έχουμε $a = \lambda n + v, 0 \leq v \leq (n-1)$ και ως εκ τούτου, $a + \langle n\rangle = v + \langle n\rangle$.
Άρα, $[\mathbb{Z}/\langle n\rangle : 1] = n$ και γι' αυτό ο δείκτης $[\mathbb{Z} : \langle n\rangle]$ ισούται με n.

Τέλος, παρατηρούμε ότι η πηλικοομάδα $\mathbb{Z}/\langle n\rangle$ είναι κυκλική, αφού για κάθε $a + \langle n\rangle \in \mathbb{Z}/\langle n\rangle$ είναι[24] $a + \langle n\rangle = a(1 + \langle n\rangle)$.

Παράδειγμα 1.6.11. Θα υπολογίσουμε τον πίνακα πράξης τής πηλικοομάδας $D_4/\mathcal{Z}(D_4)$ τής διεδρικής ομάδας $(D_4, \circ)$ ως προς το κέντρο της $\mathcal{Z}(D_4)$. Υπενθυμίζουμε ότι το κέντρο οποιασδήποτε ομάδας είναι μια ορθόθετη υποομάδα και ότι το $\mathcal{Z}(D_4) = \{\mathrm{Id}_4, \rho^2\}$, βλ. Άσκηση Α40. Θα χρησιμοποιήσουμε επίσης τον πίνακα πράξης τής D_4 που υπολογίστηκε στην Άσκηση Α26. Η πηλικοομάδα $D_4/\mathcal{Z}(D_4)$ έχει τέσσερα στοιχεία, αφού ο δείκτης $[D_4 : \mathcal{Z}(D_4)] = [D_4 : 1]/[\mathcal{Z}(D_4) : 1] = 8/2$ ισούται με 4. Οι πλευρικές κλάσεις $L_1 = \mathrm{Id}_4\mathcal{Z}(D_4)$, $L_2 = \rho\mathcal{Z}(D_4)$, $L_3 = \tau\mathcal{Z}(D_4)$ και $L_4 = (\tau\rho)\mathcal{Z}(D_4)$ απαρτίζουν το σύνολο των στοιχείων τής $D_4/\mathcal{Z}(D_4)$. Το L_1 είναι το ουδέτερο στοιχείο τής $D_4/\mathcal{Z}(D_4)$. Για το L_2L_2, έχουμε $L_2L_2 = \rho^2\mathcal{Z}(D_4)$ και αφού το ρ^2 ανήκει στην L_1 συμπεραίνουμε ότι $L_2L_2 = L_1$. Όμοια έχουμε ότι $L_3L_3 = L_1$ και $L_4L_4 = L_1$. Για το γινόμενο L_2L_3 παίρνουμε:

$$L_2L_3 = (\rho\mathcal{Z}(D_4))(\tau\mathcal{Z}(D_4)) = (\rho\tau)\mathcal{Z}(D_4) = (\tau\rho^3)\mathcal{Z}(D_4) = L_4,$$

αφού το $\tau\rho^3 \in L_4$. Παρόμοια υπολογίζονται[25] και τα υπόλοιπα γινόμενα. Ο πίνακας τής πράξης «$\circledast$» τής $D_4/\mathcal{Z}(D_4)$ είναι ο εξής:

$\circledast$	L_1	L_2	L_3	L_4
L_1	L_1	L_2	L_3	L_4
L_2	L_2	L_1	L_4	L_3
L_3	L_3	L_4	L_1	L_2
L_4	L_4	L_3	L_2	L_1

Το Θεώρημα Αντιστοιχίας

Στο επόμενο θεώρημα θα περιγράψουμε πως συσχετίζονται οι υποομάδες μιας πηλικοομάδας $(G/K, \circledast)$ με τις υποομάδες τής $(G, \star)$, όπου K είναι μια ορθόθετη υποομάδα

[24] Κάνουμε χρήση τής προσθετικής σημειογραφίας και υπενθυμίζουμε τον ορισμό τού ακέραιου πολλαπλάσιου στοιχείου αβελιανής ομάδας, βλ. σελ. 27.

[25] Συχνά οι υπολογισμοί που απαιτούνται για τον σχηματισμό τού πίνακα πράξης μιας ομάδας τάξης n είναι λιγότεροι από n^2, αφού ως γνωστόν σε κάθε γραμμή και κάθε στήλη τού πίνακα εμφανίζεται κάθε στοιχείο τής ομάδας ακριβώς μία φορά.

της G. Θεωρούμε την απεικόνιση

$$\pi_K : G \to G/K, g \mapsto \pi_K(g) := gK,$$

δηλαδή την απεικόνιση, που αντιστοιχεί σε κάθε $g \in G$ την πλευρική κλάση $gK \in G/K$ στην οποία ανήκει το g. Προφανώς, η π_K είναι μια επιρριπτική απεικόνιση.

Λήμμα 1.6.12. (α′) *Όταν $H \leq G$, τότε το σύνολο $\pi_K(H) = \{\pi_K(h) \mid h \in H\}$ είναι υποομάδα τής G/K.*

(β′) *Όταν $L \leq G/K$, τότε το σύνολο $\pi_K^{-1}(L) = \{h \in G \mid \pi_K(g) \in L\}$ είναι μια υποομάδα τής G, η οποία περιέχει την υποομάδα K. Επιπλέον, όταν η L είναι μια ορθόθετη υποομάδα τής G/K, τότε η $\pi_K^{-1}(L)$ είναι μια ορθόθετη υποομάδα τής G.*

Απόδειξη. (α′) Προφανώς, το $\pi_K(H)$ είναι $\neq \emptyset$. Όταν οι πλευρικές κλάσεις xK και yK ανήκουν στο $\pi_K(H)$, τότε υπάρχουν $h, h' \in H$ με $\pi_K(h) = hK = xK$, $\pi_K(h') = h'K = yK$. Παρατηρούμε ότι $(yK)^{-1} = (h'K)^{-1} = h'^{-1}K$. Τώρα έχουμε:

$$xK(yK)^{-1} = hKh'^{-1}K = (hh'^{-1})K \in \pi_K(H),$$

αφού η H είναι υποομάδα τής G. Από το Λήμμα 1.3.6 συμπεραίνουμε ότι το $\pi_K(H)$ είναι μια υποομάδα τής G/K.
(β′) Το σύνολο $\pi_K^{-1}(L)$ είναι $\neq \emptyset$, αφού η π_K είναι επιρριπτική. Όταν τα $x, y \in \pi_K^{-1}(L)$, τότε τα $\pi_K(x) = xK$ και $\pi_K(y) = yK \in L$. Επιπλέον, τα $(yK)^{-1} = y^{-1}K \in L$ και $(xK)(yK)^{-1} = (xK)(y^{-1}K) = xy^{-1}K \in L$, αφού το L είναι υποομάδα τής G/K. Επομένως, το $\pi_K^{-1}(L)$ είναι μια υποομάδα τής G, σύμφωνα με το Λήμμα 1.3.6.

Η L περιέχει το ουδέτερο στοιχείο eK τής G/K, αφού είναι υποομάδα τής G/K. Συνεπώς, $\{eK\} \subseteq L$ και ως εκ τούτου $\pi_K^{-1}(\{eK\}) \subseteq \pi_K^{-1}(L)$. Παρατηρώντας ότι το σύνολο $\pi_K^{-1}(\{eK\}) = \{g \in G \mid \pi_K(g) = eK\}$ ισούται με K, αφού $\pi_K(g) = gK = eK \Leftrightarrow g \in K$, συμπεραίνουμε ότι $K \leq \pi_K^{-1}(L)$.

Έστω ότι $L \trianglelefteq G/K$. Θα δείξουμε ότι $\forall g \in G, g(\pi_K^{-1}(L))g^{-1} \subseteq \pi_K^{-1}(L)$. Πράγματι, όταν $x \in g(\pi_K^{-1}(L))g^{-1}$, τότε το $x = gyg^{-1}$, όπου το $y \in \pi_K^{-1}(L)$. Έτσι έχουμε ότι το $\pi_K(x) = xK = \pi_K(gyg^{-1}) = gyg^{-1}K = (gK)(yK)(gK)^{-1}$ ανήκει στην L, επειδή η $L \trianglelefteq G/K$ και το yK ανήκει στην L. Επομένως, το $x \in \pi_K^{-1}(L)$ και αφού $\forall g \in G, g(\pi_K^{-1}(L))g^{-1} \subseteq \pi_K^{-1}(L)$, συμπεραίνουμε ότι $\pi_K^{-1}(L) \trianglelefteq G$. □

Συμβολίζουμε με $\mathcal{SUB}(G/K) = \{L \mid L \leq G/K\}$ το υποσύνολο των υποομάδων τής G/K και με $\mathcal{SUB}_K(G) = \{\mathrm{H} \mid H \leq G \text{ και } K \leq H\}$ το υποσύνολο των υποομάδων τής G που περιέχουν την K.

Το προηγούμενο λήμμα βεβαιώνει ότι οι αντιστοιχίες:

$$\Phi_K : \mathcal{SUB}_K(G) \to \mathcal{SUB}(G/K), H \mapsto \Phi_K(H) := \pi_K(H)$$
$$\mathrm{X}_K : \mathcal{SUB}(G/K) \to \mathcal{SUB}_K(G), L \mapsto \mathrm{X}_K(L) := \pi_K^{-1}(L)$$

είναι απεικονίσεις.

Θεώρημα 1.6.13 (Το Θεώρημα Αντιστοιχίας). *Οι απεικονίσεις Φ_K και X_K είναι η μία αντίστροφη τής άλλης και ως εκ τούτου, οι συγκεκριμένες απεικονίσεις χορηγούν μία αμφιμονοσήμαντη αντιστοιχία μεταξύ τού συνόλου $\mathcal{SUB}_K(G)$ των υποομάδων τής G που περιέχουν το K και τού συνόλου $\mathcal{SUB}(G/K)$ των υποομάδων τής G/K. Επιπλέον, όταν $L \trianglelefteq G/K$, τότε $X_K(L) \trianglelefteq G$.*

Απόδειξη. Λόγω τού Λήμματος 1.6.12, το μόνο που μένει να αποδειχθεί είναι ότι η σύνθεση $\Phi_K \circ X_K$ ισούται με την ταυτοτική απεικόνιση επί τού συνόλου $\mathcal{SUB}(G/K)$ και αντίστοιχα ότι η σύνθεση $X_K \circ \Phi_K$ ισούται με την ταυτοτική απεικόνιση επί τού συνόλου $\mathcal{SUB}_K(G)$.

Για $L \in \mathcal{SUB}(G/K)$ είναι: $\Phi_K \circ X_K(L) = \Phi_K(\pi_K^{-1}(L)) = \pi_K(\pi_K^{-1}(L)) = L$, διότι η π_K είναι μια επιρριπτική απεικόνιση.

Όταν $H \in \mathcal{SUB}_K(G)$, τότε έχουμε ότι $X_K \circ \Phi_K(H) = X_K(\pi_K(H)) = \pi_K^{-1}(\pi_K(H))$. Για $g \in G$, είναι:

$$g \in \pi_K^{-1}(\pi_K(H)) \Leftrightarrow \pi_K(g) \in \pi_K(H) \Leftrightarrow \exists h \in H : gK = hK \Leftrightarrow \exists h \in H : h^{-1}g \in K.$$

Αφού όμως $K \subseteq H$, συμπεραίνουμε ότι από $g \in \pi_K^{-1}(\pi_K(H))$, έπεται ότι $\exists h \in H : h^{-1}g \in H$ και επομένως ότι $g \in H$. Άρα, $\pi_K^{-1}(\pi_K(H)) \subseteq H$. Επειδή προφανώς $H \subseteq \pi_K^{-1}(\pi_K(H))$, τελικά προκύπτει ότι $\pi_K^{-1}(\pi_K(H)) = H$. □

Παράδειγμα 1.6.14. Έστω η διεδρική ομάδα $(D_6, \circ)$ τάξης 12. Σύμφωνα με την Άσκηση Α40, το κέντρο της $\mathcal{Z}(D_6)$ ισούται με $\{\mathrm{Id}_6, \rho^2\}$ και επειδή το κέντρο οποιασδήποτε ομάδας είναι μια ορθόθετη υποομάδα, μπορούμε να σχηματίσουμε την πηλικοομάδα $D_6/\mathcal{Z}(D_6)$. Η τάξη $[(D_6/\mathcal{Z}(D_6)) : 1]$ ισούται με τον δείκτη $[D_6 : \mathcal{Z}(D_6)] = [D_6 : 1]/[\mathcal{Z}(D_6) : 1] = 12/2 = 6$.

Η $D_6/\mathcal{Z}(D_6)$ αποτελείται από τις κλάσεις

$$L_1 = \mathrm{Id}_6 \circ \mathcal{Z}(D_6) = \{\mathrm{Id}_6, \rho^3\}, L_2 = \rho \circ \mathcal{Z}(D_6) = \{\rho, \rho^4\}, L_3 = \rho^2 \circ \mathcal{Z}(D_6) = \{\rho^2, \rho^5\},$$
$$L_4 = \tau \circ \mathcal{Z}(D_6) = \{\tau, \tau \circ \rho^3\}, L_5 = (\tau \circ \rho) \circ \mathcal{Z}(D_6) = \{\tau \circ \rho, \tau \circ \rho^4\},$$
$$L_6 = (\tau \circ \rho^2) \circ \mathcal{Z}(D_6) = \{\tau \circ \rho^2, \tau \circ \rho^5\}.$$

Παρατηρούμε ότι η $D_6/\mathcal{Z}(D_6)$ δεν είναι μεταθετική, αφού $L_3 \circledast L_4 = L_5$, ενώ $L_4 \circledast L_3 = L_6$.

Θα προσδιορίσουμε όλες τις υποομάδες τής $D_6/\mathcal{Z}(D_6)$.

Από το Θεώρημα 1.6.13 γνωρίζουμε ότι οι υποομάδες τής $D_6/\mathcal{Z}(D_6)$ είναι τής μορφής $H/\mathcal{Z}(D_6)$, όπου H είναι υποομάδα τής D_6 με $\mathcal{Z}(D_6) \leq H$.

Από το Θεώρημα 1.5.24 γνωρίζουμε ότι οι υποομάδες τής D_6 είναι οι:

$$\{\mathrm{Id}_6\}, \langle\rho^3\rangle, \langle\rho^2\rangle, \langle\rho\rangle, \langle\tau\rangle, \langle\tau \circ \rho\rangle, \langle\tau \circ \rho^2\rangle, \langle\tau \circ \rho^3\rangle, \langle\tau \circ \rho^4\rangle, \langle\tau \circ \rho^5\rangle,$$
$$\langle\{\rho^3, \tau\}\rangle, \langle\{\rho^3, \tau \circ \rho\}\rangle, \langle\{\rho^3, \tau \circ \rho^2\}\rangle, \langle\{\rho^2, \tau\}\rangle, \langle\{\rho^2, \tau \circ \rho\}\rangle \text{ και } \langle\{\rho, \tau\}\rangle = D_6.$$

Το κέντρο $\mathcal{Z}(D_6) = \{\mathrm{Id}_3, \rho^3\}$ περιέχεται στις

$$\langle\rho^3\rangle, \langle\rho\rangle, \langle\{\rho^3, \tau\}\rangle, \langle\{\rho^3, \tau \circ \rho\}\rangle, \langle\{\rho^3, \tau \circ \rho^2\}\rangle, \text{ και } D_6.$$

Οι αντίστοιχες πηλικοομάδες είναι οι

$$\langle\rho^3\rangle/\mathcal{Z}(D_6), \langle\rho\rangle/\mathcal{Z}(D_6), \langle\{\rho^3, \tau\}\rangle/\mathcal{Z}(D_6), \langle\{\rho^3, \tau \circ \rho\}\rangle/\mathcal{Z}(D_6), \langle\{\rho^3, \tau \circ \rho^2\}\rangle/\mathcal{Z}(D_6)$$

και $D_6/\mathcal{Z}(D_6)$. Προσέξτε ότι η $\langle\rho^3\rangle/\mathcal{Z}(D_6)$ ισούται με την τετριμμένη υποομάδα $\{L_1\}$ τής $D_6/\mathcal{Z}(D_6)$ που αποτελείται μόνο από το ταυτοτικό στοιχείο.

Ολοκληρώνουμε την παρούσα ενότητα με το εξής πολύ ενδιαφέρον:

Θεώρημα 1.6.15. *Έστω $(G,\star)$ μια αβελιανή ομάδα τάξης n. Για κάθε θετικό διαιρέτη d τού n, υπάρχει υποομάδα $H\leq G$ τάξης $[H:1]=d$.*

Απόδειξη. **Ειδική Περίπτωση:** Κατ᾽ αρχάς θα εκτελέσουμε την απόδειξη για την περίπτωση, όπου ο d είναι ένας πρώτος αριθμός[26].

Επαγωγή ως προς την τάξη n τής G:
Για $n=1$, το σύνολο των πρώτων που διαιρεί την τάξη τής G είναι κενό και ο ισχυρισμός είναι προφανής.
Έστω ότι για κάθε $k\in\mathbb{N}, 1\leq k\leq m-1$ και κάθε πρώτο d με $d\mid k$, οποιαδήποτε ομάδα τάξης k διαθέτει μια υποομάδα τάξης d. Έστω G μια ομάδα τάξης m. Θεωρούμε ένα[27] στοιχείο $a\in G$ με $a\neq e_G$ και την αντίστοιχη κυκλική υποομάδα $\langle a\rangle$.

Αν ο d είναι διαιρέτης τής $[\langle a\rangle:1]$, τότε η κυκλική υποομάδα $\langle a\rangle\leq G$ διαθέτει μια υποομάδα H τάξης d, βλ. Πρόταση 1.5.16, και προφανώς, $H\leq G$.

Αν ο d δεν είναι διαιρέτης τής $[\langle a\rangle:1]$, τότε επειδή η G είναι αβελιανή μπορούμε να σχηματίσουμε την πηλικοομάδα $G/\langle a\rangle$. Αφού ο πρώτος $d\mid[G:1]=[G:\langle a\rangle][\langle a\rangle:1]$ και ο $d\nmid[\langle a\rangle:1]$, συμπεραίνουμε ότι $d\mid[G:\langle a\rangle]$ που είναι η τάξη τής $G/\langle a\rangle$. Η τάξη $[G:\langle a\rangle]\lneqq[G:1]$, διότι η $\langle a\rangle\neq\{e_G\}$. Ως εκ τούτου από την επαγωγική υπόθεση, προκύπτει ότι υπάρχει υποομάδα $L\leq G/\langle a\rangle$ τάξης d. Επειδή ο d είναι πρώτος, συμπεραίνουμε ότι η L είναι κυκλική τάξης d, ας πούμε $L=\langle\ell\rangle$, όπου $\circ(\ell)=d$. Άρα, η $G/\langle a\rangle$ έχει στοιχείο τάξης d και με τη βοήθεια τής Άσκησης 77 συμπεραίνουμε ότι η G έχει επίσης ένα στοιχείο τάξης d, άρα και μια (κυκλική) υποομάδα H τάξης d.

Γενική Περίπτωση: Θα εκτελέσουμε και πάλι μια επαγωγική απόδειξη ως προς την τάξη n τής G:
Για $n=1$, ο μοναδικός διαιρέτης d τής $[G:1]$ είναι ο 1 και ο ισχυρισμός είναι προφανής.
Έστω ότι για κάθε $k\in\mathbb{N}, 1\leq k\leq m-1$ και κάθε διαιρέτη d τού k, οποιαδήποτε ομάδα τάξης k διαθέτει μια υποομάδα τάξης d. Έστω G μια ομάδα τάξης m και d ένας διαιρέτης τού m. Μπορούμε χωρίς περιορισμό τής γενικότητας να δεχθούμε ότι $d>1$, διότι για $d=1$, η αλήθεια τού ισχυρισμού είναι φανερή. Έστω p ένας πρώτος διαιρέτης τού d. Τότε ο $p\mid[G:1]$ και από την προηγούμενη ειδική περίπτωση γνωρίζουμε ότι υπάρχει (κυκλική) υποομάδα H (πρώτης) τάξης p. Θεωρούμε την πηλικοομάδα G/H, η οποία είναι τάξης $[G:H]=\frac{[G:1]}{[H:1]}=\frac{m}{p}\lneqq m$. Ο θετικός ακέραιος d/p είναι διαιρέτης τού m/p. Ως εκ τούτου από την επαγωγική υπόθεση, προκύπτει ότι υπάρχει υποομάδα $L\leq G/H$ τάξης d/p. Θεωρούμε την απεικόνιση $\pi_H: G\to G/H, g\mapsto \pi_H(g):=gH$. Από το Θεώρημα Αντιστοιχίας, βλ. Θεώρημα 1.6.13, γνωρίζουμε ότι η $\pi_H^{-1}(L)$ είναι μια υποομάδα τής G με $H\leq\pi_H^{-1}(L)$ και $\pi(\pi_H^{-1}(L))=\pi_H^{-1}(L)/H=L$. Τώρα έχουμε $[\pi_H^{-1}(L):1]=[\pi_H^{-1}(L):H][H:1]$ και αφού $\pi_H^{-1}(L)/H=L$, συμπεραίνουμε ότι $[\pi_H^{-1}(L):1]=[L:1][H:1]=\frac{d}{p}p=d$. □

[26] Στην περίπτωση αυτή το θεώρημα ισχύει για οποιαδήποτε πεπερασμένη ομάδα και είναι το λεγόμενο Θεώρημα Cauchy, βλ. Θεώρημα 2.3.11.

[27] Υπάρχει τέτοιο $a\in G$, αφού $m\geq 2$.

Ας καταγράψουμε την ειδική περίπτωση, όπου ο διαιρέτης είναι πρώτος αριθμός στο εξής:

Πόρισμα 1.6.16. *Έστω $(G, \star)$ μια αβελιανή ομάδα τάξης n. Για κάθε πρώτο διαιρέτη p τού n, υπάρχει $a \in G$ τάξης $\circ(a) = p$.*

Παρατήρηση 1.6.17. Συνδυάζοντας το προηγούμενο πόρισμα με την Πρόταση 1.5.23, συμπεραίνουμε ότι για κάθε πρώτο διαιρέτη p τής τάξης n μιας αβελιανής ομάδας, το πλήθος των στοιχείων τάξης p είναι ένα θετικό πολλαπλάσιο τής τιμής $\varphi(p) = p - 1$, όπου φ είναι η φ–συνάρτηση Euler.

Ασκήσεις στις Ορθόθετες Υποομάδες και τις Πηλικοομάδες

Λυμένες Ασκήσεις

Α 69. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι $\{K_i \ i \in I\}$ είναι ένα σύνολο ορθόθετων υποομάδων τής G. Να δειχθεί ότι η τομή $\bigcap_{i \in I} K_i$ είναι μια ορθόθετη υποομάδα τής G.

Λύση. Από την Άσκηση Α30 γνωρίζουμε ότι η τομή $K = \bigcap_{i \in I} K_i$ είναι μια υποομάδα τής G. Έστω ότι $g \in G$ και $k \in K$. Τότε $\forall i \in I$, το k ανήκει στην K_i και αφού $K_i \trianglelefteq G$, συμπεραίνουμε ότι $\forall i \in I$, το $gkg^{-1} \in K_i$. Επομένως, το $gkg^{-1} \in K$ και $K \trianglelefteq G$.

Α 70. Να δειχθεί ότι κάθε υποομάδα $K \leq G$ μιας ομάδας $(G, \star)$ με δείκτη $[G : K] = 2$ είναι ορθόθετη υποομάδα τής G.

Λύση. Θα δείξουμε ότι για κάθε $a \in G$ είναι $aK = Ka$. Αν το $a \in K$, τότε προφανώς $aK = K = Ka$. Έστω ότι το $a \in G \setminus K$. Αφού ο $[G : K] = 2$, υπάρχουν ακριβώς δύο αριστερές και ακριβώς δύο πλευρικές κλάσεις. Το σύνολο των αριστερών πλευρικών κλάσεων είναι το $\{K, aK\}$ και των δεξιών το $\{K, Kx\}$ με $x \notin K$. Τα σύνολα αυτά απαρτίζουν διαμερίσεις τής G και ως εκ τούτου, $aK = Kx$. Άρα $a \in Kx$ και $Ka = Kx$. Συνεπώς, $aK = Ka$.

Α 71. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι $H \leq G$ είναι η μοναδική υποομάδα τής G με τάξη n. Να δειχθεί ότι η H είναι ορθόθετη υποομάδα τής G.

Λύση. Για κάθε $g \in G$ θεωρούμε το σύνολο $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$ και την απεικόνιση $\chi_g : H \to gHg^{-1}, h \mapsto \chi_g(h) := ghg^{-1}$. Η χ_g είναι ενριπτική («$1-1$»), αφού όταν $\chi_g(h_1) = \chi_g(h_2), h_1, h_2 \in H$, τότε $gh_1g^{-1} = gh_2g^{-1}$ και επομένως $h_1 = h_2$. Προφανώς, η χ_g είναι επιρριπτική («επί») και ως εκ τούτου, αμφιρριπτική Συνεπώς, το πλήθος των στοιχείων τού gHg^{-1} ισούται με n. Τέλος, επειδή η H είναι υποομάδα τής G, προκύπτει εύκολα ότι το σύνολο gHg^{-1} είναι μια υποομάδα τής G. Αφού η H είναι η μοναδική υποομάδα τής G τάξης n, συμπεραίνουμε ότι $\forall g \in G, H = gHg^{-1}$. Ως εκ τούτου, $H \trianglelefteq G$.

Α 72. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H και K είναι υποομάδες τής G. Αν η K είναι η μοναδική υποομάδα τής H τάξης n και η H είναι ορθόθετη υποομάδα τής G, τότε να δειχθεί ότι η K είναι επίσης ορθόθετη υποομάδα τής G.

Λύση. Για κάθε $g \in G$, είναι $gKg^{-1} \leq gHg^{-1} = H$, αφού $H \trianglelefteq G$. Επειδή όμως η K είναι η μοναδική υποομάδα τής H τάξης n και επειδή $n = [K : 1] = [gKg^{-1} : 1]$, συμπεραίνουμε ότι $gKg^{-1} = K$. Ως εκ τούτου, $K \trianglelefteq G$.

Α 73. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H και K είναι υποομάδες της με την K ορθόθετη υποομάδα τής G. Να δειχθεί ότι το σύνολο $HK = \{hk \mid h \in H, k \in K\}$ είναι υποομάδα τής G.

Λύση. Το σύνολο HK είναι $\neq \emptyset$. Όταν τα x, y ανήκουν στο HK, τότε $x = hk$ και $y = h_1k_1$, όπου $h, h_1 \in H$ και $k, k_1 \in K$. Έχουμε $xy^{-1} = hk(h_1k_1)^{-1} = hkk_1^{-1}h_1^{-1}, (*)$. Το $\bar{k} := kk_1^{-1}$ ανήκει στην υποομάδα K και η $(*)$ γράφεται $xy^{-1} = h\bar{k}h_1^{-1} = h(h_1^{-1}h_1)\bar{k}h_1^{-1} = hh_1^{-1}(h_1\bar{k}h_1^{-1}), (**)$. Παρατηρούμε ότι το $k' := h_1\bar{k}h_1^{-1}$ είναι και πάλι στοιχείο τής K, αφού $K \trianglelefteq G$. Έτσι, η $(**)$ δίνει $xy^{-1} = hh_1^{-1}\bar{k}$, το οποίο βέβαια είναι στοιχείο τού HK, αφού το hh_1^{-1} ανήκει στην υποομάδα H. Από το Λήμμα 1.3.6, συμπεραίνουμε ότι το HK είναι υποομάδα τής G.

Προτείνουμε στον αναγνώστη να εκτελέσει μια ταχύτερη απόδειξη με τη βοήθεια τής Άσκησης Α37.

Α 74. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H και K είναι ορθόθετες υποομάδες τής G. Να δειχθεί ότι η υποομάδα $\langle H \bigcup K \rangle$, που παράγεται από το σύνολο $H \bigcup K$, είναι ορθόθετη υποομάδα τής G.

Λύση. Έστω $x \in \langle H \bigcup K \rangle$. Τότε το $x = m_{i_1}^{\varepsilon_1} m_{i_2}^{\varepsilon_2} \ldots m_{i_s}^{\varepsilon_s}$, όπου $\forall j, 1 \leq j \leq s$ τα $m_{i_j} \in H \bigcup K$ και τα $\varepsilon_j \in \{1, -1\}$. Παρατηρούμε, ότι $\forall m \in H \bigcup K, g \in G,$ είναι $gmg^{-1} \in H \bigcup K$ και $gm^{-1}g^{-1} = (gmg^{-1})^{-1} \in H \bigcup K$, διότι οι H K είναι ορθόθετες υποομάδες και τα $m, m^{-1} \in H \bigcup K$. Για κάθε $g \in G$, είναι

$$\begin{aligned} gxg^{-1} = g(m_{i_1}^{\varepsilon_1} m_{i_2}^{\varepsilon_2} \ldots m_{i_s}^{\varepsilon_s})g^{-1} = gm_{i_1}^{\varepsilon_1}(gg^{-1})m_{i_2}^{\varepsilon_2}(gg^{-1}) \ldots (gg^{-1})m_{i_s}^{\varepsilon_s}g^{-1} = \\ (gm_{i_1}^{\varepsilon_1}g^{-1})(gm_{i_2}^{\varepsilon_2}g^{-1}) \ldots (gm_{i_j}^{\varepsilon_j}g^{-1}) \ldots (gm_{i_s}^{\varepsilon_s}g^{-1}) = \\ (gm_{i_1}g^{-1})^{\varepsilon_1}(gm_{i_2}g^{-1})^{\varepsilon_2} \ldots (gm_{i_j}g^{-1})^{\varepsilon_j} \ldots (gm_{i_s}g^{-1})^{\varepsilon_s}. \end{aligned}$$

Στο αμέσως προηγούμενο γινόμενο κάθε παράγοντας ανήκει στο $H \bigcup K$. Άρα, το gxg^{-1} ανήκει επίσης στην υποομάδα $\langle H \bigcup K \rangle$ και έτσι $\langle H \bigcup K \rangle \trianglelefteq G$.

Α 75. Έστω ότι $(G, \star)$ είναι μια αβελιανή (αντιστοίχως κυκλική) ομάδα και ότι $H \leq G$ είναι μια υποομάδα της. Να δειχθεί ότι η πηλικοομάδα $(G/H, \circledast)$ είναι επίσης αβελιανή (αντιστοίχως κυκλική).

Λύση. Έστω ότι η G είναι αβελιανή. Για κάθε $gH, g'H \in G/H$ είναι $(gH)(g'H) = (gg')H = (g'g)H = (g'H)(gH)$. Άρα, η G/H είναι αβελιανή.

Έστω ότι η G είναι κυκλική και ότι a είναι ένας γεννήτοράς της. Όταν gH είναι στοιχείο τής G/H, τότε υπάρχει κάποιος ακέραιος z με $g = a^z$. Συνεπώς, $gH = a^zH = (aH)^z$. Επομένως, η κλάση aH είναι ένας γεννήτορας τής G/H και η G/H είναι κυκλική.

Α 76. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H είναι μια ορθόθετη υποομάδα τής G με πεπερασμένο δείκτη $[G : H] = n$. Να δειχθεί ότι $\forall g \in G$, το g^n ανήκει στην H. Να δοθεί παράδειγμα όπου αυτό δεν ισχύει, όταν η H δεν είναι ορθόθετη.

Λύση. Επειδή η τάξη τής πηλικοομάδας $(G/H, \circledast)$ ισούται με n, συμπεραίνουμε με τη βοήθεια τού Πορίσματος 1.5.8 ότι $(gH)^n = g^nH = H$. Ως εκ τούτου, $g^n \in H$.

Θεωρούμε τη συμμετρική ομάδα $(S_3, \circ)$ και την κυκλική υποομάδα της $H = \langle \tau_3 \rangle = \{\mathrm{Id}_3, \tau_3\}$, όπου $\tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$. Η υποομάδα H δεν είναι ορθόθετη υποομάδα τής S_3 και ο δείκτης $[S_3 : H]$ ισούται με $[S_3 : 1]/[H : 1] = 6/2 = 3$. Για το στοιχείο $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, έχουμε $\tau_1^3 = \tau_1$ και $\tau_1 \notin \langle \tau_3 \rangle$.

Α 77. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι $H \trianglelefteq G$ είναι μια ορθόθετη υποομάδα τής G. Να δειχθεί ότι όταν η πηλικοομάδα $(G/H, \circledast)$ διαθέτει ένα στοιχείο τάξης d, τότε η G διαθέτει επίσης ένα στοιχείο τάξης d.

Λύση. Έστω gH ένα στοιχείο τής G/H τάξης $\circ(gH) = d$. Επειδή η τάξη $[G : 1]$ είναι πεπερασμένη, συμπεραίνουμε ότι η τάξη $\circ(g)$ είναι επίσης πεπερασμένη. Παρατηρούμε ότι $(gH)^{\circ(g)} = g^{\circ(g)}H = e_G H = H$. Επομένως, η τάξη d είναι διαιρέτης τής $\circ(g)$. Άρα, $\circ(g) = \lambda d$, $\lambda \in \mathbb{N}$. Από το Πόρισμα 1.5.11, γνωρίζουμε ότι η τάξη τού g^λ ισούται με n.

Α 78. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι $\mathcal{Z}(G)$ είναι το κέντρο της. Αν η πηλικοομάδα $G/\mathcal{Z}(G)$ είναι κυκλική, τότε να δειχθεί ότι η G είναι αβελιανή.

Λύση. Έστω ότι $G/\mathcal{Z}(G) = \langle a\mathcal{Z}(G) \rangle$ (δηλαδή η πλευρική κλάση $a\mathcal{Z}(G)$, $a \in G$ είναι ένας γεννήτορας τής πηλικοομάδας) και ότι g_1, g_2 είναι στοιχεία τής G. Θα δείξουμε ότι $g_1 g_2 = g_2 g_1$. Αφού οι αριστερές πλευρικές κλάσεις $g_i\mathcal{Z}(G)$, $i = 1, 2$ είναι στοιχεία τής $G/\mathcal{Z}(G)$, συμπεραίνουμε ότι $g_i\mathcal{Z}(G) = a^{z_i}\mathcal{Z}(G)$, $z_i \in \mathbb{Z}$, $i = 1, 2$. Επομένως, $g_i \in a^{z_i}\mathcal{Z}(G)$, $i = 1, 2$ και ως εκ τούτου, $g_i = a^{z_i}c_i$, $i = 1, 2$, όπου τα στοιχεία c_i, $i = 1, 2$ ανήκουν στο κέντρο $\mathcal{Z}(G)$ τής G. Τώρα

$$g_1 g_2 = (a^{z_1}c_1)(a^{z_2}c_2) = a^{z_1}(c_1 a^{z_2})c_2 = a^{z_1}(a^{z_2}c_1)c_2 = a^{z_1+z_2}c_1 c_2$$

και

$$g_2 g_1 = (a^{z_2}c_2)(a^{z_1}c_1) = a^{z_2}(c_2 a^{z_1})c_1 = a^{z_2}(a^{z_1}c_2)c_1 = a^{z_2+z_1}c_2 c_1 = a^{z_1+z_2}c_1 c_2.$$

Επομένως, $\forall g_1, g_2 \in G$ είναι $g_1 g_2 = g_2 g_1$ και η G είναι αβελιανή.

Α 79. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης $[G : 1] = pq$, όπου οι p και q είναι πρώτοι αριθμοί, όχι απαραίτητα διαφορετικοί. Να δειχθεί ή ότι η G είναι αβελιανή ή ότι το κέντρο της $\mathcal{Z}(G)$ ισούται με $\{e_G\}$.

Λύση. Αν το κέντρο $\mathcal{Z}(G)$ τής G δεν είναι τετριμμένο, τότε η τάξη του θα είναι ή p ή q ή pq και η τάξη τής αντίστοιχης πηλικοομάδας $G/\mathcal{Z}(G)$ θα είναι ή q ή p ή 1. Αλλά μια ομάδα που έχει τάξη ή 1 ή κάποιον πρώτο αριθμό είναι κυκλική και έτσι από την αμέσως προηγούμενη άσκηση συμπεραίνουμε ότι η G είναι αβελιανή.

Προτεινόμενες Ασκήσεις

ΠΑ 69. Έστω $(G, \star)$ μια κυκλική ομάδα και $H \neq \{e_G\}$ μια υποομάδα της. Να δειχθεί ότι η πηλικοομάδα $(G/H, \circledast)$ είναι πάντοτε πεπερασμένη. Επιπλέον, όταν $[G : 1] < \infty$, τότε $[G/H : 1] \lneqq [G : 1]$.

ΠΑ 70. Να προσδιοριστούν οι ορθόθετες υποομάδες των διεδρικών ομάδων $(D_6, \circ)$, $(D_7, \circ)$ και $(D_8, \circ)$.

ΠΑ 71. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι $H \trianglelefteq G$ είναι μια ορθόθετη υποομάδα της τάξης 2. Να δειχθεί ότι $H \leq \mathcal{Z}(G)$. Επιπλέον, να δειχθεί ότι αν α είναι το μοναδικό στοιχείο τάξης 2 μιας ομάδας $(G, \star)$, τότε $\langle \alpha \rangle \leq \mathcal{Z}(G)$.

ΠΑ 72. Έστω ότι $(G, \star)$ είναι μια ομάδα και H μια υποομάδα της που παράγεται από ένα σύνολο γεννητόρων M. Να δειχθεί ότι $H \trianglelefteq G$, αν και μόνο αν, $\forall m \in M$ και $\forall g \in G$, το gmg^{-1} ανήκει στην H.

ΠΑ 73. Να δειχθεί ότι κάθε υποομάδα τής τετρανιακής ομάδας $(\mathcal{Q}_8, \cdot)$, βλ. Άσκηση ΠΑ26 και Άσκηση Α58, είναι ορθόθετη. Να συμπεράνετε ότι υπάρχουν ομάδες που δεν είναι αβελιανές, αλλά όπου κάθε υποομάδα τους είναι ορθόθετη.

ΠΑ 74. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα τάξης m και ότι K είναι μια ορθόθετη υποομάδα τής G με δείκτη n σχετικώς πρώτο προς τον m. Να δειχθεί ότι κάθε $g \in G$ με $g^{[K:1]} = e_G$ ανήκει στην K.

ΠΑ 75. Έστω ότι $(G, \star)$ είναι μια αβελιανή ομάδα, ότι $G \times G$ είναι το ευθύ γινόμενο τής G με τον εαυτό της, βλ. Άσκηση Α18 και ότι $\mathcal{D}$ είναι το διαγώνιο σύνολο $\mathcal{D} = \{(g, g) \mid g \in G\}$. Να δειχθεί ότι το $\mathcal{D}$ είναι μια ορθόθετη υποομάδα τής $G \times G$.

ΠΑ 76. Έστω ότι $(S_3, \circ)$ είναι η συμμετρική ομάδα τού συνόλου $X = \{1, 2, 3\}$, ότι $S_3 \times S_3$ είναι το ευθύ γινόμενο τής G με τον εαυτό της και ότι Δ είναι το διαγώνιο σύνολο $\Delta = \{(g, g) \mid g \in S_3\}$. Να δειχθεί ότι το Δ είναι μια υποομάδα τής $S_3 \times S_3$, η οποία όμως δεν είναι ορθόθετη.

ΠΑ 77. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι οι K, L είναι ορθόθετες υποομάδες τής G με $K \bigcap L = \{e_G\}$. Να δειχθεί ότι $\forall k \in K, \ell \in L$, είναι $k\ell = \ell k$.

1.7 Ομομορφισμοί

Οι απεικονίσεις συνόλων είναι το εργαλείο που συσχετίζει τα σύνολα μεταξύ τους. Αντίστοιχα, οι απεικονίσεις μεταξύ ομάδων που έχουν την επιπλέον ιδιότητα «να διατηρούν τις πράξεις», είναι ακριβώς το μέσο που συσχετίζει τις ομάδες και επιτρέπει την εξαγωγή ιδιαιτέρως σημαντικών συμπερασμάτων γι' αυτές.

Ορισμός 1.7.1. Έστω ότι $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι δύο ομάδες και ότι $\varphi : G_1 \to G_2$ είναι μια απεικόνιση. Η φ ονομάζεται *ομομορφισμός ομάδων*, όταν

$$\forall g, g' \in G_1 : \ \varphi(g \star_1 g') = \varphi(g) \star_2 \varphi(g').$$

Παράδειγμα 1.7.2. Έστω ότι $(\mathbb{R}, +)$ είναι η ομάδα των πραγματικών αριθμών με πράξη τη συνήθη πρόσθεση και $(\mathbb{R}^{>0}, \cdot)$ η ομάδα των θετικών πραγματικών αριθμών με πράξη τον συνήθη πολλαπλασιασμό.

Η απεικόνιση[28] $\ln : \mathbb{R}^{>0} \to \mathbb{R}, a \mapsto \ln(a)$ είναι ομομορφισμός ομάδων, αφού $\forall a, b \in \mathbb{R}^{>0}$, είναι $\ln(a \cdot b) = \ln(a) + \ln(b)$.

Η απεικόνιση[29] $\exp : \mathbb{R} \to \mathbb{R}^{>0}, x \mapsto \exp(x) := e^x$ είναι ομομορφισμός ομάδων, αφού $\forall x, y \in \mathbb{R}$, είναι $\exp(x + y) = e^{(x+y)} = e^x \cdot e^y = \exp(x) \cdot \exp(y)$.

Υπενθυμίζουμε ότι η σύνθεση $\exp \circ \ln$ ισούται με την ταυτοτική απεικόνιση επί τού $\mathbb{R}^{>0}$, αφού $\forall a \in \mathbb{R}^{>0}$, είναι $\exp \circ \ln(a) = e^{\ln(a)} = a$ και η σύνθεση $\ln \circ \exp$ ισούται με την ταυτοτική απεικόνιση επί τού $\mathbb{R}$, αφού $\forall x \in \mathbb{R}$, είναι $\ln \circ \exp(x) = \ln(e^x) = x$

Παράδειγμα 1.7.3. Θεωρούμε την ομάδα $(\mathbb{R}, +)$ των πραγματικών αριθμών με πράξη τη συνήθη πρόσθεση πραγματικών και την ομάδα $(\mathbb{C}^\star, \cdot)$ των μη μηδενικών μιγαδικών αριθμών με πράξη τον πολλαπλασιασμό μιγαδικών.

Η απεικόνιση $\varphi : \mathbb{R} \to \mathbb{C}^\star, \alpha \mapsto \varphi(\alpha) := \cos(\alpha) + i \sin(\alpha)$, όπου $i^2 = -1$ είναι ομομορφισμός ομάδων, αφού $\forall \alpha, \beta \in \mathbb{R}$ είναι $\varphi(\alpha + \beta) = \varphi(\alpha) \cdot \varphi(\beta)$. Η αλήθεια τής συγκεκριμένης ισότητας προκύπτει[30] από τις τριγωνομετρικές ταυτότητες $\cos(\alpha + \beta) = \cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)$ και $\sin(\alpha + \beta) = \sin(\alpha)\cos(\beta) + \cos(\alpha)\sin(\beta)$.

Παράδειγμα 1.7.4. Έστω $(\mathrm{GL}_n(\mathbb{K}, \cdot)$ η ομάδα των αντιστρέψιμων $n \times n$ πινάκων, $n \in \mathbb{N}$, με συνιστώσες από το $\mathbb{K}$, όπου $\mathbb{K}$ είναι ένα από τα σώματα $\mathbb{Q}, \mathbb{R}$ ή $\mathbb{C}$. Υπενθυμίζουμε ότι το σύνολο $\mathbb{K}^\star = \mathbb{K} \setminus \{0\}$ με πράξη τον αντίστοιχο πολλαπλασιασμό «·» απαρτίζει μια αβελιανή ομάδα. Η απεικόνιση $\varphi : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\star, A \mapsto \varphi(A) := \det(A)$, όπου $\det(A)$ είναι η ορίζουσα τού A, αποτελεί έναν ομομορφισμό ομάδων, αφού από τη Γραμμική Άλγεβρα γνωρίζουμε ότι για οποιουσδήποτε $n \times n$ πίνακες A και B είναι $\det(A \cdot B) = \det(A) \cdot \det(B)$.

Αντίθετα, η απεικόνιση $\psi : \mathcal{M}_{n\times n}(\mathbb{K}) \to \mathbb{K}, A \mapsto \psi(A) := \det(A)$ από την αβελιανή ομάδα $(\mathcal{M}_{n\times n}(\mathbb{K}), +)$ των τετραγωνικών $n \times n$ πινάκων στην προσθετική ομάδα $(\mathbb{K}, +)$ τού σώματος $\mathbb{K}$, *δεν είναι ομομορφισμός* ομάδων, όταν το $n \geq 2$. Πράγματι, για $n \geq 2$ υπάρχουν, ως γνωστόν, τετραγωνικοί πίνακες A, B με $\psi(A+B) = \det(A+B) \neq \det(A) + \det(B) = \psi(A) + \psi(B)$.

Παράδειγμα 1.7.5. Έστω ότι $(G, \star)$ είναι μια ομάδα και K μια ορθόθετη υποομάδα της. Η απεικόνιση $\pi_K : G \to G/K, g \mapsto \pi_K(g) := gK$, που σε κάθε $g \in G$ αντιστοιχεί την κλάση του gK, είναι ένας ομομορφισμός ομάδων. Η π_K είχε ήδη οριστεί στο Θεώρημα Αντιστοιχίας, βλ. σελ. 105. Πράγματι, $\forall g, g' \in G$ είναι[31]:

$$\pi_K(gg') = (gg')K = (gK)(g'K).$$

Επιπλέον, ο π_K είναι μια επιρριπτική απεικόνιση, αφού κάθε πλευρική κλάση έχει (τουλάχιστον) έναν αντιπρόσωπο.

Ο ομομορφισμός π_K ονομάζεται συνήθως η *φυσική προβολή* τής $(G, \star)$ στην πηλικοομάδα $(G/K, \circledast)$.

[28]Ο φυσικός λογάριθμος.

[29]Η (φυσική) εκθετική συνάρτηση.

[30]Μπορεί επίσης να προκύψει και από το ότι $\forall \alpha \in \mathbb{R}$, είναι $\cos(\alpha) + i\sin(\alpha) = e^{i\alpha}$.

[31]Εδώ ακολουθούμε την πάγια πρακτική να παριστάνουμε την πράξη μεταξύ δύο στοιχείων g, g' τής G, αντιστοίχως μεταξύ δύο πλευρικών κλάσεων gK και $g'K$, γράφοντας απλώς gg' αντί τού $g' \star g'$, αντιστοίχως $gKg'K$ αντί τού $gK \circledast g'K$.

Ειδικότερα για κάθε $n \in \mathbb{N}$, η $\pi_n : \mathbb{Z} \to \mathbb{Z}/\langle n \rangle, a \mapsto a + \langle n \rangle$ είναι η φυσική προβολή τής ομάδας των ακέραιων αριθμών $(\mathbb{Z}, +)$ στην πηλικοομάδα της $(\mathbb{Z}/\langle n \rangle, +)$.

Θεώρημα 1.7.6. *Έστω ότι $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι δύο ομάδες. Όταν η απεικόνιση $\varphi : G_1 \to G_2$ είναι ένας ομομορφισμός ομάδων, τότε ισχύουν τα εξής:*

(α′) $\varphi(e_{G_1}) = e_{G_2}$,

(β′) $\forall g \in G_1 : \varphi(g^{-1}) = \varphi(g)^{-1}$,

(γ′) $\forall g \in G, \forall z \in \mathbb{Z} : \varphi(g^z) = \varphi(g)^z$.

Απόδειξη. (α′) Έχουμε:

$$\begin{aligned}
&\varphi(e_{G_1}) = \varphi(e_{G_1} \star_1 e_{G_1}) = \varphi(e_{G_1}) \star_2 \varphi(e_{G_1}) \Rightarrow \\
&\varphi(e_{G_1})^{-1} \star_2 \varphi(e_{G_1}) = \varphi(e_{G_1})^{-1} \star_2 \varphi(e_{G_1}) \star_2 \varphi(e_{G_1}) \Rightarrow e_{G_2} = \varphi(e_{G_1}).
\end{aligned}$$

(β′) Έχουμε

$$\begin{aligned}
\forall g \in G_1 : e_{G_2} = \varphi(e_{G_1}) = \varphi(g \star_1 g^{-1}) = \varphi(g) \star_2 \varphi(g^{-1}) \Rightarrow \\
\varphi(g)^{-1} \star_2 e_{G_2} = \varphi(g)^{-1} \star_2 \varphi(g) \star_2 \varphi(g^{-1}) \Rightarrow \varphi(g)^{-1} = \varphi(g^{-1}).
\end{aligned}$$

(γ′) Εκτελούμε την απόδειξη πρώτα για $z \in \mathbb{N} \bigcup \{0\}$ με τη βοήθεια επαγωγής.
Όταν $z = 0$, τότε προφανώς είναι $\varphi(g^0) = \varphi(e_{G_1}) = e_{G_2} = \varphi(g)^0$.
Επαγωγική Υπόθεση **(επ.υπ.)**: Έστω ότι είναι $\varphi(g^k) = \varphi(g)^k$, για $z = k \in \mathbb{N} \bigcup \{0\}$.
Θα δείξουμε ότι $\varphi(g^{k+1}) = \varphi(g)^{k+1}$. Πράγματι, έχουμε

$$\varphi(g^{k+1}) = \varphi(g^k \star_1 g) = \varphi(g^k) \star_2 \varphi(g) \underset{\textbf{(επ.υπ.)}}{=} \varphi(g)^k \star_2 \varphi(g) = \varphi(g)^{k+1}.$$

Άρα, $\forall g \in G, \forall k \in \mathbb{N} \bigcup \{0\}, \varphi(g^k) = \varphi(g)^k$.

Τώρα, έστω ότι $z \in \mathbb{Z}, z < 0$. Παρατηρώντας ότι $\forall g \in G$, είναι $g^z = (g^{-1})^{|z|}$, έχουμε

$$\varphi(g^z) = \varphi((g^{-1})^{|z|}) \underset{(\text{ διότι το } |z|>0)}{=} \varphi(g^{-1})^{|z|} = (\varphi(g)^{(-1)})^{|z|} = \varphi(g)^{(-1)|z|} = \varphi(g)^z.$$

□

Πόρισμα 1.7.7. *Όταν $\varphi : G_1 \to G_2$ είναι ένας ομομορφισμός ομάδων και $g \in G_1$ είναι ένα στοιχείο πεπερασμένης τάξης $\circ(g) < \infty$, τότε η τάξη $\circ(\varphi(g))$ τού $\varphi(g)$ είναι επίσης πεπερασμένη και μάλιστα η τάξη $\circ(\varphi(g))$ είναι διαιρέτης τής τάξης $\circ(g)$.*

Απόδειξη. Από το προηγούμενο θεώρημα είναι $\varphi(g)^{\circ(g)} = \varphi(g^{\circ(g)}) = \varphi(e_1) = e_{G_2}$. Επομένως, η $\circ(\varphi(g))$ είναι πεπερασμένη και από το Πόρισμα 1.5.11, έπεται ότι η $\circ(\varphi(g))$ διαιρεί την τάξη $\circ(g)$. □

Ορισμός 1.7.8. Ένας ομομορφισμός ομάδων $\varphi : G_1 \to G_2$ ονομάζεται:

(α′) *μονομορφισμός*, όταν ο φ είναι μια ενριπτική («$1-1$») απεικόνιση, (β′) *επιμορφισμός*, όταν ο φ είναι μια επιρριπτική («επί») απεικόνιση,

(γ′) *ισομορφισμός*, όταν ο φ είναι μια αμφιρριπτική («1 − 1» και «επί») απεικόνιση.

Για κάθε ομάδα $(G, \star)$, η ταυτοτική απεικόνιση $\mathrm{Id}_G : G \to G, g \mapsto \mathrm{Id}_G(g) := g$ είναι ένας ισομορφισμός.

Για κάθε ομάδα $(G, \star)$ και κάθε υποομάδα της $H \leq G$, η έγκλειση $\iota_H : H \to G, h \mapsto \iota_H(h) := h$ είναι ένας μονομορφισμός.

Για κάθε ομάδα $(G, \star)$ και κάθε ορθόθετη υποομάδα της $K \leq G$, η φυσική προβολή $\pi_K : G \to G/K, g \mapsto \pi_K(g) := gK$ είναι ένας επιμορφισμός.

Για οποιεσδήποτε δύο ομάδες $(G_1, \star_1)$ και $(G_2, \star_2)$, η απεικόνιση $\zeta : G_1 \to G_2, g \mapsto \zeta(g) := e_2$ που απεικονίζει κάθε στοιχείο τής G_1 στο ουδέτερο στοιχείο τής G_2 είναι ένας ομομορφισμός, ο οποίος ονομάζεται ο *τετριμμένος ομομορφισμός*.

Από εδώ και στο εξής ακολουθώντας την πάγια τακτική μας, δεν θα σημειώνουμε τις πράξεις των ομάδων εκτός και αν αυτό είναι απαραίτητο. Η παράθεση ενός στοιχείου δίπλα σε ένα άλλο θα υπονοεί και την αντίστοιχη πράξη μεταξύ τους.

Πρόταση 1.7.9. *Έστω ότι $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι ομάδες και ότι $\varphi : G_1 \to G_2$ είναι ένας ομομορφισμός ομάδων, τότε ισχύουν τα εξής:*

(α′) *Όταν H_1 είναι υποομάδα τής G_1, τότε η εικόνα της $\varphi(H_1)$ είναι υποομάδα τής G_2. Επιπλέον, όταν η H_1 είναι ορθόθετη και ο φ είναι ένας επιμορφισμός, τότε η $\varphi(H_1)$ είναι ορθόθετη υποομάδα τής G_2.*

(β′) *Όταν H_2 είναι υποομάδα τής G_2, τότε η προεικόνα της $\varphi^{-1}(H_2)$ είναι υποομάδα τής G_1. Επιπλέον, όταν η H_2 είναι ορθόθετη, τότε η $\varphi^{-1}(H_2)$ είναι επίσης ορθόθετη.*

Απόδειξη. Αποδεικνύουμε ότι ένα μη κενό υποσύνολο είναι υποομάδα, αντιστοίχως ορθόθετη, εφαρμόζοντας το Λήμμα 1.3.6, αντιστοίχως το Θεώρημα 1.6.3.

(α′) Αφού το H_1 είναι $\neq \emptyset$, συμπεραίνουμε ότι $\varphi(H_1) \neq \emptyset$. Όταν τα x, y είναι στοιχεία τής εικόνας $\varphi(H_1)$, τότε υπάρχουν $h, k \in H$ με $\varphi(h) = x$ και $\varphi(k) = y$. Για το στοιχείο xy^{-1}, έχουμε:

$$xy^{-1} = \varphi(h)\varphi(k)^{-1} \overset{(*)}{=} \varphi(h)\varphi(k^{-1}) \overset{(**)}{=} \varphi(hk^{-1}).$$

Η ισότητα $(*)$ ισχύει λόγω τού Θεωρήματος 1.7.6(β′) και η $(**)$ επειδή ο φ είναι μονομορφισμός. Τώρα, αφού η H_1 είναι μια υποομάδα τής G_1, το hk^{-1} ανήκει στην H_1 και ως εκ τούτου, η εικόνα του $\varphi(hk^{-1}) = xy^{-1}$ ανήκει στη $\varphi(H_1)$.

Ας υποθέσουμε τώρα ότι $H_1 \trianglelefteq G_1$ και ότι ο φ είναι ένας επιμορφισμός. Για να είναι $\varphi(H_1) \trianglelefteq G_2$, αρκεί $\forall x \in G_2$, να είναι $x\varphi(H_1)x^{-1} = \varphi(H_1)$. Αλλά για κάθε $x \in G_2$, υπάρχει $g \in G_1$ με $\varphi(g) = x$, διότι ο φ είναι επιρριπτικός. Έτσι έχουμε:

$$x\varphi(H_1)x^{-1} = \varphi(g)\varphi(H_1)\varphi(g)^{-1} \overset{(*)}{=} \varphi(g)\varphi(H_1)\varphi(g^{-1}) \overset{(**)}{=} \varphi(gH_1g^{-1}) \overset{(***)}{=} \varphi(H_1).$$

Η ισότητα $(*)$ ισχύει λόγω τού Θεωρήματος 1.7.6(β′), η $(**)$ ισχύει επειδή ο φ είναι ομομορφισμός και η $(***)$ επειδή $H_1 \trianglelefteq G_1$.

(β′) Το ουδέτερο e_2 τής G_2 είναι και το ουδέτερο τής H_2. Αφού $\varphi(e_1) = e_2$, συμπεραίνουμε ότι $e_1 \in \varphi^{-1}(H_2)$ και επομένως το $\varphi^{-1}(H_2)$ είναι $\neq \emptyset$. Όταν τα $h, k \in \varphi^{-1}(H_2)$, τότε τα $\varphi(h), \varphi(k) \in H_2$. Επειδή η H_2 είναι υποομάδα τής G_2, συμπεραίνουμε ότι τα $\varphi(k)^{-1}$ και $\varphi(h)\varphi(k)^{-1} = \varphi(hk^{-1})$ ανήκουν στην H_2. Επομένως, το hk^{-1} ανήκει στην προεικόνα $\varphi^{-1}(H_2)$ και ως εκ τούτου, $\varphi^{-1}(H_2) \leq G_1$.

Ας υποθέσουμε ότι επιπλέον είναι $H_2 \trianglelefteq G_2$. Θα δείξουμε ότι για κάθε $g \in G_1$ είναι $g\varphi^{-1}(H_2)g^{-1} \subseteq \varphi^{-1}(H_2)$, από όπου φυσικά θα προκύψει ότι $\varphi^{-1}(H_2) \trianglelefteq G_1$. Παρατηρούμε ότι $g\varphi^{-1}(H_2)g^{-1} \subseteq \varphi^{-1}(H_2) \iff \varphi(g\varphi^{-1}(H_2)g^{-1}) \subseteq H_2$. Έχουμε:

$$\begin{aligned}&\varphi(g\varphi^{-1}(H_2)g^{-1}) = \varphi(g)\varphi(\varphi^{-1}(H_2))\varphi(g^{-1}) \overset{(*)}{\subseteq} \varphi(g)H_2\varphi(g^{-1}) = \\ &\varphi(g)H_2\varphi(g)^{-1} \overset{(**)}{\subseteq} H_2.\end{aligned}$$

Η $(*)$ ισχύει, διότι $\varphi(\varphi^{-1}(H_2)) \subseteq H_2$ και η $(**)$ ισχύει, διότι $H_2 \trianglelefteq G_2$. Επομένως, $\varphi^{-1}(H_2) \trianglelefteq G_1$. □

Παρατήρηση 1.7.10. (α′) Όταν ο ομομορφισμός $\varphi : G_1 \to G_2$ δεν είναι επιμορφισμός, τότε η εικόνα μιας ορθόθετης υποομάδας τής G_1, δεν είναι απαραίτητα ορθόθετη υποομάδα τής G_2. Πράγματι, θεωρούμε τη συμμετρική ομάδα $(S_3, \circ)$ και την κυκλική υποομάδα της $T_1 = \langle \tau_1 \rangle$, όπου $\tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$. Η T_1 είναι ορθόθετη υποομάδα τού εαυτού της και η έγκλειση $\iota_{T_1} : T_1 \to S_3$ είναι ένας ομομορφισμός ομάδων. Αλλά η εικόνα $\iota_{T_1}(T_1) = T_1$ δεν είναι ορθόθετη υποομάδα τής S_3. Συνεπώς, η συνθήκη τού επιμορφισμού στο (α′) τής προηγούμενης πρότασης, είναι απαραίτητη, προκειμένου η εικόνα μιας ορθόθετης υποομάδας τής G_1 να είναι ορθόθετη στη G_2. Βέβαια, η εικόνα μιας ορθόθετης υποομάδας τής G_1 είναι πάντοτε ορθόθετη υποομάδα τής $\varphi(G_1)$, αφού κάθε ομομορφισμός ομάδων $\varphi : G_1 \to G_2, g \mapsto \varphi(g)$ δίνει τον επιμορφισμό ομάδων $\varphi : G_1 \to \varphi(G_1), g \mapsto \varphi(g)$

(β′) Ως γνωστόν, κάθε ομάδα G διαθέτει τις τετριμμένες ορθόθετες υποομάδες G και $\{e_G\}$. Επομένως, όταν $\varphi : G_1 \to G_2$ είναι ένας ομομορφισμός ομάδων, τότε οι $\varphi^{-1}(G_2) = G_1$ και $\varphi^{-1}(\{e_2\})$ είναι ορθόθετες υποομάδες τής G_1. Όπως θα δούμε αμέσως παρακάτω, η $\varphi^{-1}(\{e_2\}) \trianglelefteq G_1$ έχει πολύ μεγάλη σημασία στη Θεωρία Ομάδων και γι’ αυτό δίνουμε τον εξής ορισμό:

Ορισμός 1.7.11. Έστω $\varphi : G_1 \to G_2$ ένας ομομορφισμός ομάδων. Η προεικόνα

$$\varphi^{-1}(\{e_2\}) = \{g \in G_1 \mid \varphi(g) = e_2\}$$

ονομάζεται ο *πυρήνας* τού ομομορφισμού φ.

Συμβολισμός. Όταν $\varphi : G_1 \to G_2$ είναι ένας ομομορφισμός ομάδων, τότε ο πυρήνας του $\varphi^{-1}(\{e_2\}) = \{g \in G_1 \mid \varphi(g) = e_2\}$ συμβολίζεται με $\ker \varphi$ και η εικόνα του $\varphi(G_1) = \{\varphi(g) \mid g \in G\}$ συμβολίζεται με $\operatorname{im} \varphi$.

Σύμφωνα με όσα είπαμε προηγουμένως,

Πόρισμα 1.7.12. *Όταν $\varphi : G_1 \to G_2$ είναι ένας ομομορφισμός ομάδων, τότε $\ker \varphi \trianglelefteq G_1$ και $\operatorname{im} \varphi \leq G_2$.*

Πρόταση 1.7.13. *Έστω $\varphi : G_1 \to G_2$ ένας ομομορφισμός ομάδων. Ο φ είναι ένας μονομορφισμός, αν και μόνο αν, ο* $\ker \varphi = \{e_1\}$.

Απόδειξη. «$\Rightarrow$» Έστω ότι $g \in \ker \varphi$. Αφού $\varphi(g) = e_2 = \varphi(e_1)$ και επειδή ο φ είναι μονομορφισμός, συμπεραίνουμε ότι $g = e_1$.
«$\Leftarrow$» Έστω ότι $\varphi(g) = \varphi(k)$, όπου $g, k \in G_1$. Τότε,

$$\varphi(gk^{-1}) = \varphi(g)\varphi(k^{-1}) = \varphi(g)\varphi(k)^{-1} = e_2.$$

Επομένως, το gk^{-1} είναι στοιχείο τού $\ker \varphi = \{e_1\}$ και γι' αυτό το $gk^{-1} = e_1$. Άρα, $g = k$ και ο φ είναι μονομορφισμός. □

Θεώρημα 1.7.14. *Έστω $\varphi : G_1 \to G_2$ ένας ομομορφισμός ομάδων.*

(α′) *Ο φ είναι ένας μονομορφισμός* $\Longleftrightarrow \ker \varphi = \{e_1\}$.

(β′) *Ο φ είναι ένας επιμορφισμός* $\Longleftrightarrow \operatorname{im} \varphi = G_2$.

(γ′) *Ο φ είναι ένας ισομορφισμός* $\Longleftrightarrow \ker \varphi = \{e_1\}$ *και* $\operatorname{im} \varphi = G_2$.

(δ′) *Όταν ο φ είναι ισομορφισμός, τότε και η αντίστροφη απεικόνιση*[32] *$\psi : G_2 \to G_1$ είναι επίσης ισομορφισμός.*

Απόδειξη. Το (α′) έχει αποδειχθεί στην Πρόταση 1.7.13. Το (β′) είναι ουσιαστικά ο ορισμός τής επιρριπτικότητας μιας απεικόνισης. Το (γ′) είναι άμεση συνέπεια των δύο προηγουμένων.

Για το (δ′): Υπενθυμίζουμε τον ορισμό τής $\psi : G_2 \to G_1$. Είναι $\psi(g_2) = g_1$ ακριβώς τότε, όταν $\varphi(g_1) = g_2$, όπου $g_2 \in G_2, g_1 \in G_1$. Αφού η ψ είναι προφανώς αμφιρριπτική, υπολείπεται να δείξουμε ότι είναι ομομορφισμός, δηλαδή ότι $\forall g_2, g_2' \in G_2$ είναι $\psi(g_2 g_2') = \psi(g_2)\psi(g_2')$.

Παρατηρούμε ότι

$$\varphi(\psi(g_2 g_2')) = (\varphi \circ \psi)(g_2 g_2') = \mathrm{Id}_{G_2}(g_2 g_2') = g_2 g_2'$$

και ότι

$$\begin{aligned}&\varphi(\psi(g_2)\psi(g_2')) = \varphi(\psi(g_2))\varphi(\psi(g_2')) = (\varphi \circ \psi)(g_2)(\varphi \circ \psi)(g_2') = \\ &\mathrm{Id}_{G_2}(g_2)\mathrm{Id}_{G_2}(g_2') = g_2 g_2'.\end{aligned}$$

Συνεπώς, ο μονομορφισμός φ εφαρμοσμένος στα $\psi(g_2 g_2')$ και $\psi(g_2)\psi(g_2')$ παίρνει την ίδια τιμή. Άρα, $\psi(g_2 g_2') = \psi(g_2)\psi(g_2')$. □

Παράδειγμα 1.7.15. (α′) Στο Παράδειγμα 1.7.2 είδαμε τον ομομορφισμό $\ln : \mathbb{R}^{>0} \to \mathbb{R}, a \mapsto \ln(a)$, ο οποίος έχει την αντίστροφη απεικόνιση $\exp : \mathbb{R} \to \mathbb{R}^{>0}, x \mapsto \exp(x) := e^x$. Εκεί, είχαμε επιβεβαιώσει ότι η exp ήταν επίσης ένας ομομορφισμός. Τώρα όμως αυτό προκύπτει άμεσα από το (δ′) τού προηγούμενου θεωρήματος. Προφανώς, αυτοί οι δύο ομομορφισμοί είναι ισομορφισμοί.

[32] Η ψ υπάρχει, διότι η φ είναι μια αμφιρριπτική («$1-1$» και «επί») απεικόνιση.

(β′) Στο Παράδειγμα 1.7.3 είδαμε τον ομομορφισμό $\varphi : \mathbb{R} \to \mathbb{C}^\star, \alpha \mapsto \varphi(\alpha) := \cos(\alpha) + i\sin(\alpha)$. Το $\alpha \in \mathbb{R}$ ανήκει στον $\ker\varphi \Leftrightarrow \varphi(\alpha) = 1 \Leftrightarrow \cos(\alpha) = 1$ και $\sin(\alpha) = 0 \Leftrightarrow$ το α ανήκει στην κυκλική ομάδα $\langle 2\pi \rangle = \{2\lambda\pi \mid \lambda \in \mathbb{Z}\}$. Το $z \in \mathbb{C}^\star$ ανήκει στην $\operatorname{im}\varphi \Leftrightarrow z = \cos(\alpha) + i\sin(\alpha) \Leftrightarrow |z| = 1$. Επομένως, $\operatorname{im}\varphi = \{z \in \mathbb{C}^\star \mid |z| = 1\}$, που είναι το σύνολο των σημείων τής μοναδιαίας περιφέρειας τού επίπεδου Gauss. Ο φ δεν είναι μονομορφισμός, αφού $\ker\varphi \neq \{0\}$. Ο φ δεν είναι ούτε επιμορφισμός, αφού $\operatorname{im}\varphi \subsetneq \mathbb{C}^\star$.

(γ′) Στο Παράδειγμα 1.7.4 είδαμε τον ομομορφισμό $\varphi : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\star, A \mapsto \varphi(A) := \det(A)$. Ο πίνακας $A \in \mathrm{GL}_n(\mathbb{K})$ ανήκει στον $\ker\varphi \Leftrightarrow \det(A) = 1 \Leftrightarrow A \in \mathrm{SL}_n(\mathbb{K})$, η οποία είναι υποομάδα τής $\mathrm{GL}_n(\mathbb{K})$ με στοιχεία τους πίνακες με ορίζουσα 1 (η λεγόμενη *ειδική γραμμική ομάδα*). Το $k \in \mathbb{K}^\star$ ανήκει στην $\operatorname{im}\varphi \Leftrightarrow \exists A \in \mathrm{GL}_n(\mathbb{K})$ με $\varphi(A) = \det(A) = k$. Αυτό είναι αληθές $\forall k \in \mathbb{K}^\star$, αφού η $\det(kI_n) = k$, όπου I_n είναι ο ταυτοτικός $n \times n$ πίνακας. Όταν $n \geq 2$, ο φ δεν είναι μονομορφισμός, αφού ο $\ker\varphi$ δεν αποτελείται μόνο από το ταυτοτικό στοιχείο τής $\mathrm{GL}_n(\mathbb{K})$. Ο φ είναι πάντοτε επιμορφισμός. Τέλος για $n = 1$, ο φ είναι ισομορφισμός.

(δ′) Στο Παράδειγμα 1.7.5 είδαμε τον ομομορφισμό $\pi_K : G \to G/K, g \mapsto \pi_K(g) := gK$, όπου $K \trianglelefteq G$, τη λεγόμενη φυσική προβολή. Εκεί μάλιστα διαπιστώσαμε ότι ο π_K είναι ένας επιμορφισμός. Προφανώς, το $g \in G$ ανήκει στον $\ker\pi_K \Leftrightarrow g \in K$, δηλαδή $\ker\pi_K = K$.

Παρατήρηση 1.7.16. Σύμφωνα με το τελευταίο από τα προηγούμενα παραδείγματα, κάθε ορθόθετη υποομάδα K μιας ομάδας $(G, \star)$ χορηγεί έναν ομομορφισμό, τη φυσική προβολή π_K με πυρήνα την K. Αλλά και ο πυρήνας $\ker\varphi$ οποιουδήποτε ομομορφισμού $\varphi : G_1 \to G_2$ αποτελεί μια ορθόθετη υποομάδα τής G_1. Συχνά, αν θέλουμε να δείξουμε ότι ένα υποσύνολο K μιας ομάδας $(G, \star)$ είναι ορθόθετη υποομάδα τής G, τότε καταφεύγουμε στο τέχνασμα τής απόδειξης ότι το K είναι πυρήνας κάποιου ομομορφισμού με σύνολο εκκίνησης την ομάδα G.

Ορισμός 1.7.17. Μια ομάδα $(G_1, \star_1)$ ονομάζεται *ισόμορφη* προς μια ομάδα $(G_2, \star_2)$, όταν υπάρχει ένας ισομορφισμός $\varphi : G_1 \to G_2$.

Συμβολισμός. Δηλώνουμε ότι η $(G_1, \star_1)$ είναι *ισόμορφη* προς την $(G_2, \star_2)$, σημειώνοντας $G_1 \cong G_2$.

Θεώρημα 1.7.18. *Έστω ότι $\varphi_1 : G_1 \to G_2$ και $\varphi_2 : G_2 \to G_3$ είναι ομομορφισμοί ομάδων.*

(α′) *Η σύνθεση $\varphi_2 \circ \varphi_1 : G_1 \to G_3$ είναι ομομορφισμός.*

(β′) *Όταν οι φ_1 και φ_2 είναι μονομορφισμοί, τότε και ο $\varphi_2 \circ \varphi_1$ είναι επίσης μονομορφισμός.*

(γ′) *Όταν οι φ_1 και φ_2 είναι επιμορφισμοί, τότε και ο $\varphi_2 \circ \varphi_1$ είναι επίσης επιμορφισμός.*

(δ′) *Όταν οι φ_1 και φ_2 είναι ισομορφισμοί, τότε και ο $\varphi_2 \circ \varphi_1$ είναι επίσης ισομορφισμός.*

(ε′) *Όταν η σύνθεση $\varphi_2 \circ \varphi_1$ είναι μονομορφισμός, τότε ο φ_1 είναι μονομορφισμός.*

(στ′) *Όταν η σύνθεση $\varphi_2 \circ \varphi_1$ είναι επιμορφισμός, τότε ο φ_2 είναι επιμορφισμός.*

Απόδειξη. (α′) Για κάθε $g_1, g_1' \in G_1$ είναι

$$(\varphi_2 \circ \varphi_1)(g_1g_1') = \varphi_2(\varphi_1(g_1g_1')) = \varphi_2(\varphi_1(g_1)\varphi_1(g_1')) =$$
$$\varphi_2(\varphi_1(g_1))\varphi_2(\varphi_1(g_1')) = (\varphi_2 \circ \varphi_1)(g_1)(\varphi_2 \circ \varphi_1)(g_1').$$

(β′) Από τη Θεωρία Συνόλων, είναι γνωστό ότι η σύνθεση δύο ενριπτικών («1−1») απεικονίσεων είναι ενριπτική. Από το (α′), γνωρίζουμε ότι η σύνθεση $\varphi_2 \circ \varphi_1$ είναι ομομορφισμός.
(γ′) Από τη Θεωρία Συνόλων, είναι γνωστό ότι η σύνθεση δύο επιρριπτικών («επί») απεικονίσεων είναι επιρριπτική. Από το (α′), γνωρίζουμε ότι η σύνθεση $\varphi_2 \circ \varphi_1$ είναι ομομορφισμός.
(δ′) Προκύπτει άμεσα από τα (β′) και (γ′).
(ε′) Από τη Θεωρία Συνόλων, είναι γνωστό ότι όταν η σύνθεση $\chi \circ \psi$ δύο απεικονίσεων είναι «1 − 1», τότε η ψ είναι «1 − 1».
(στ′) Από τη Θεωρία Συνόλων, είναι γνωστό ότι όταν η σύνθεση $\chi \circ \psi$ δύο απεικονίσεων είναι «επί», τότε η χ είναι «επί». □

Παρατήρηση 1.7.19. Από το Θεώρημα 1.7.14, προκύπτει ότι όταν $G_1 \cong G_2$, τότε επίσης είναι $G_2 \cong G_1$. Ακόμα από το προηγούμενο θεώρημα προκύπτει ότι όταν $G_1 \cong G_2$ και $G_2 \cong G_3$, τότε επίσης είναι $G_1 \cong G_3$. Τέλος, επειδή για κάθε ομάδα $(G, \star)$, η ταυτοτική απεικόνιση Id_G είναι ένας ισομορφισμός, έπεται ότι $G \cong G$.
Όταν $\varphi : G_1 \to G_2$ είναι ένας ισομορφισμός ομάδων, τότε οι G_1 και G_2 έχουν ακριβώς τις ίδιες αλγεβρικές ιδιότητες και δεν ξεχωρίζουν καθόλου από τη σκοπιά τής Άλγεβρας. Επί παραδείγματι, δύο ισόμορφες ομάδες έχουν το ίδιο πλήθος στοιχείων τάξης n, το ίδιο πλήθος υποομάδων κ.λπ. Μέσω ενός ισομορφισμού υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ των υποομάδων τους, των ορθόθετων υποομάδων τους και γενικά οποιαδήποτε αλγεβρική ιδιότητα που ικανοποιείται στη G_1 ικανοποιείται στη G_2 και αντιστρόφως. Κατά κάποιον τρόπο η ισομορφία αποτελεί μια γενίκευση τής ισότητας.

Έτσι, ένα από τα κύρια ερωτήματα που τίθενται στη Θεωρία Ομάδων είναι ο προσδιορισμός των μη ισόμορφων ομάδων. Φυσικά πρόκειται για ένα πολύ μεγαλεπήβολο σχέδιο. Έτσι τίθενται απλούστερα ερωτήματα. Για παράδειγμα, ο προσδιορισμός των μη ισόμορφων ομάδων τάξης n. Σύντομα θα μπορέσουμε να δώσουμε κάποιες απαντήσεις. Προς τούτο χρειάζεται να αναπτύξουμε περισσότερο την εργαλειοθήκη μας.

Τα Θεωρήματα Ισομορφίας

Πρόταση 1.7.20. *Έστω ότι $\varphi : G_1 \to G_2$ ένας ομομορφισμός ομάδων με πυρήνα $K := \ker \varphi$, ότι $N \trianglelefteq G$ είναι μια ορθόθετη υποομάδα τής G με $N \leq K$ και ότι $\pi_N : G \to G/N$ είναι η φυσική προβολή. Τότε ισχύουν τα εξής:*

(α′) *Υπάρχει ένας μοναδικός ομομορφισμός $\tilde{\varphi} : G_1/N \to G_2$ με $\tilde{\varphi} \circ \pi_N = \varphi$.*

(β′) *Ο πυρήνας $\ker \tilde{\varphi}$ ισούται με $\ker \varphi/N$.*

(γ′) *Ο $\tilde{\varphi}$ είναι επιμορφισμός $\Longleftrightarrow$ ο φ είναι επιμορφισμός.*

Απόδειξη. (α′) **Μοναδικότητα.** Αν υπάρχουν ομομορφισμοί $\chi, \psi : G_1/N \to G_2$ με $\chi \circ \pi_N = \varphi = \psi \circ \pi_N$, τότε $\chi = \psi$, διότι ο π_N είναι μια επιρριπτική («επί») απεικόνιση.

Ύπαρξη. Θεωρούμε την αντιστοιχία $\tilde{\varphi} : G_1/N \to G_2, gN \mapsto \tilde{\varphi}(gN) := \varphi(g)$. Η $\tilde{\varphi}$ είναι μια καλά ορισμένη απεικόνιση, αφού από $gN = g'N, g, g' \in G_1$, έπεται ότι $g^{-1}g' \in N \leq K$. Άρα, $\varphi(g^{-1}g') = e_2$ και συνεπώς $\varphi(g) = \varphi(g')$. Επομένως, $\tilde{\varphi}(gN) = \varphi(g) = \varphi(g') = \tilde{\varphi}(g'N)$.
Η $\tilde{\varphi}$ είναι ένας ομομορφισμός, αφού $\forall gN, g'N \in G_1/N$ είναι

$$\tilde{\varphi}((gN)(g'N)) = \tilde{\varphi}(gg'N) = \varphi(gg') = \varphi(g)\varphi(g') = \tilde{\varphi}(gN)\tilde{\varphi}(g'N).$$

(β′) $gN \in \ker \tilde{\varphi} \Leftrightarrow \tilde{\varphi}(gN) = e_2 \Leftrightarrow \varphi(g) = e_2 \Leftrightarrow g \in \ker \varphi \Leftrightarrow gN \in \ker \varphi/N$. Επομένως, $\ker \tilde{\varphi} = \ker \varphi/N$.
(γ′) Όταν ο $\tilde{\varphi}$ είναι επιμορφισμός, τότε και ο $\varphi = \tilde{\varphi} \circ \pi_N$ είναι επιμορφισμός ως σύνθεση επιμορφισμών. Αντίστροφα, όταν ο $\varphi = \tilde{\varphi} \circ \pi_N$ είναι επιρριπτική («επί») απεικόνιση, τότε από τη Θεωρία Συνόλων γνωρίζουμε ότι ο $\tilde{\varphi}$ οφείλει να είναι επίσης μια επιρριπτική απεικόνιση. □

Θεώρημα 1.7.21 (Πρώτο Θεώρημα Ισομορφίας)**.** *Έστω ότι $\varphi : G_1 \to G_2$ ένας ομομορφισμός ομάδων. Τότε $G_1/\ker \varphi \cong \operatorname{im} \varphi$.*

Απόδειξη. Ο ομομορφισμός φ χορηγεί το επιμορφισμό $\varphi' : G_1 \to \operatorname{im} g \mapsto \varphi'(g) := \varphi(g)$ και προφανώς $\ker \varphi' = \ker \varphi$. Εφαρμόζοντας την προηγούμενη πρόταση στον φ' με $N = \ker \varphi$, παίρνουμε έναν επιμορφισμό $\tilde{\varphi}' : G_1/\ker \varphi \to \operatorname{im} \varphi$ με πυρήνα την τετριμμένη υποομάδα $\ker \varphi/\ker \varphi$ τής $G_1/\ker \varphi$. Επομένως, ο $\tilde{\varphi}'$ είναι μονομορφισμός και ως εκ τούτου, $G_1/\ker \varphi \cong \operatorname{im} \varphi$. □

Τα επόμενα δύο πορίσματα είναι προφανή.

Πόρισμα 1.7.22. *Έστω ότι $\varphi : G_1 \to G_2$ ένας ομομορφισμός μεταξύ δύο πεπερασμένων ομάδων. Τότε $[G_1 : 1] = [\ker \varphi : 1][\operatorname{im} \varphi : 1]$.*

Πόρισμα 1.7.23. *Έστω $(G_1, \star_1)$ και $(G_2, \star_2)$ δύο πεπερασμένες ομάδες, των οποίων οι τάξεις είναι σχετικώς πρώτοι αριθμοί. Τότε ο μοναδικός ομομορφισμός ανάμεσά τους είναι ο τετριμμένος ομομορφισμός.*

Ας δούμε τώρα την ταξινόμηση των κυκλικών ομάδων με τη βοήθεια τού Πρώτου Θεωρήματος Ισομορφίας.

Πόρισμα 1.7.24. *Έστω $(G, \star)$ μια κυκλική ομάδα. Όταν $[G : 1] = \infty$, τότε η G είναι ισόμορφη προς την ομάδα $(\mathbb{Z}, +)$. Όταν $[G : 1] = n \in \mathbb{N}$, τότε η G είναι ισόμορφη προς την πηλικοομάδα $(\mathbb{Z}/\langle n \rangle, +)$.*

Απόδειξη. Έστω ότι $G = \langle a \rangle$, όπου $a \in G$ είναι ένας γεννήτορας τής G. Θεωρούμε την απεικόνιση $\varphi : \mathbb{Z} \to g, z \mapsto \varphi(z) := a^z$. Από τους κανόνες δυνάμεων, βλ. Λήμμα 1.2.22, έπεται αμέσως ότι η φ είναι ένας ομομορφισμός, ο οποίος μάλιστα είναι επιμορφισμός, αφού η G είναι κυκλική. Από το Πρώτο Θεώρημα Ισομορφίας είναι $\mathbb{Z}/\ker \varphi \cong \operatorname{im} \varphi = G$. Θα υπολογίσουμε τον $\ker \varphi$.

Πρώτη Περίπτωση. Όταν $[G:1]=\infty$, τότε ο μοναδικός $z\in\mathbb{Z}$ με $a^z=e_G$ είναι ο $z=0$. Επομένως, $z\in\ker\varphi \Leftrightarrow z=0$ και $\ker\varphi=\{0\}$. Άρα, ο φ είναι ένας ισομορφισμός.
Δεύτερη Περίπτωση. Όταν $[G:1]=n$, τότε $\circ(a)=n$ και $a^z=e \Leftrightarrow z\in\langle n\rangle$. Επομένως, $\ker\varphi=\langle n\rangle$ και $\mathbb{Z}/\langle n\rangle\cong G$. □

Συνεπώς, δύο κυκλικές ομάδες είναι ισόμορφες, αν και μόνο αν, έχουν την ίδια τάξη. Επί παραδείγματι, η κυκλική ομάδα $(\mathbb{Z}_n,+)$ των κλάσεων ισοτιμίας mod n είναι ισόμορφη προς την κυκλική ομάδα $(\mathcal{E}_n,\cdot)$ των n-οστών ριζών τής μονάδας, αφού και οι δυο τους είναι ισόμορφες προς την πηλικοομάδα $(\mathbb{Z}/\langle n\rangle,+)$.

Προφανώς, μια πεπερασμένη (και ιδιαιτέρως πεπερασμένη κυκλική) ομάδα $(G,\star)$ δεν είναι ποτέ ισόμορφη με μια γνήσια υποομάδα της H, αφού δεν υπάρχει καμία αμφιμονοσήμαντη απεικόνιση μεταξύ ενός πεπερασμένου συνόλου και ενός γνήσιου υποσυνόλου του. Όμως όταν $(G,\star)$ είναι μια κυκλική ομάδα άπειρης τάξης, τότε κάθε υποομάδα της $H\neq\{e_G\}$ είναι επίσης κυκλική άπειρης τάξης, αφού $H=\langle a^n\rangle$, $n\in\mathbb{N}$ και $\circ(a^n)<\infty$, βλ. Θεώρημα 1.5.14. Επομένως, $H\cong\mathbb{Z}$ και συνεπώς $H\cong G$.

Πόρισμα 1.7.25. *Για κάθε πρώτο αριθμό p, οποιεσδήποτε δύο ομάδες τάξης p είναι ισόμορφες.*

Απόδειξη. Ως γνωστόν κάθε ομάδα $(G,\star)$ πρώτης τάξης p είναι κυκλική, βλ. Πρόταση 1.5.5. Επομένως, $G\cong\mathbb{Z}/\langle p\rangle$. □

Θεώρημα 1.7.26 (Δεύτερο Θεώρημα Ισομορφίας)**.** *Έστω ότι G είναι μια ομάδα, ότι $H\leq G$ είναι μια υποομάδα τής G και ότι $K\trianglelefteq G$ είναι μια ορθόθετη υποομάδα τής G. Τότε $HK\leq G$, $H\bigcap K\trianglelefteq H$ και $HK/K\cong H/H\bigcap K$.*

Απόδειξη. Θεωρούμε την απεικόνιση $\varphi: H\to G/K, h\mapsto \varphi(h):=hK$. Η φ είναι ένας ομομορφισμός ομάδων, αφού $\forall h,h'\in H$ είναι $\varphi(hh')=(hh')K=(hK)(h'K)=\varphi(h)\varphi(h')$. Η εικόνα $\operatorname{im}\varphi$ τής ομάδας H ισούται με $\varphi(H)=HK/K$, επομένως[33], το $HK\leq G$, σύμφωνα με το Λήμμα 1.6.12. Ο $\ker\varphi$ ισούται με $H\bigcap K$, διότι $h\in\ker\varphi \Leftrightarrow h\in H$ και $\varphi(h)=hK=K\Leftrightarrow h\in H\bigcap K$. Επομένως, $H\bigcap K\trianglelefteq H$. Από το Πρώτο Θεώρημα Ισομορφίας έπεται: $H/\ker\varphi=H/H\bigcap K\cong\operatorname{im}\varphi=HK/K$. □

Ας δούμε πώς ένα πολύ γνωστό αποτέλεσμα για τους φυσικούς αριθμούς, μπορεί να προκύψει από το προηγούμενο θεώρημα.

Έστω ότι $m,n\in\mathbb{N}$ και ότι $\langle m\rangle,\langle n\rangle$ είναι οι αντίστοιχες υποομάδες τής ομάδας των ακέραιων αριθμών $(\mathbb{Z},+)$.
Αφού η $\mathbb{Z}$ είναι αβελιανή, ικανοποιείται προφανώς η συνθήκη $\langle n\rangle\trianglelefteq\mathbb{Z}$ τού Δεύτερου Θεωρήματος Ισομορφίας και γι' αυτό $(\langle m\rangle+\langle n\rangle)/\langle n\rangle\cong\langle m\rangle/\langle m\rangle\bigcap\langle n\rangle$, $(*)$. Ως γνωστόν, βλ. Άσκηση ΠΑ58, η $\langle m\rangle+\langle n\rangle$ ισούται με τη $\langle\delta\rangle$, όπου $\delta=\text{ΜΚΔ}(m,n)$ και η $\langle m\rangle\bigcap\langle n\rangle$ ισούται με την $\langle\varepsilon\rangle$, όπου $\varepsilon=\text{ΕΚΠ}(m,n)$. Έτσι, η $(*)$ δίνει $\langle\delta\rangle/\langle n\rangle\cong\langle m\rangle/\langle\varepsilon\rangle$.

Η τάξη $[\langle\delta\rangle:\langle n\rangle]$ τής πηλικοομάδας $\langle\delta\rangle/\langle n\rangle$ ισούται με n/δ, αφού $\langle n\rangle\leq\langle\delta\rangle\leq\mathbb{Z}$ και επειδή από την Άσκηση Α45 γνωρίζουμε ότι $[\mathbb{Z}:\langle n\rangle]=[\mathbb{Z}:\langle\delta\rangle][\langle\delta\rangle:\langle n\rangle]$, δηλαδή $n=$

[33] Από την Άσκηση Α73, γνωρίζουμε ότι η HK είναι υποομάδα τής G με μία πολύ διαφορετική επιχειρηματολογία.

$\delta[\langle\delta\rangle : \langle n\rangle]$, $(**)$. (Βέβαια, αφού η $\langle\delta\rangle/\langle n\rangle$ είναι κυκλική, τώρα αμέσως συμπεραίνουμε ότι η ομάδα αυτή είναι ισόμορφη προς την $\mathbb{Z}/\langle(n/\delta)\rangle$).

Παρόμοια, η τάξη $[\langle m\rangle : \langle\varepsilon\rangle]$ τής πηλικοομάδας $\langle m\rangle/\langle\varepsilon\rangle$ ισούται με ε/m, διότι $\langle\varepsilon\rangle \leq \langle m\rangle \leq \mathbb{Z}$. (Όπως προηγούμενα συμπεραίνουμε επίσης ότι η $\langle m\rangle/\langle\varepsilon\rangle$ είναι ισόμορφη προς την $\mathbb{Z}/\langle(\varepsilon/m)\rangle$.)

Επειδή ισόμορφες ομάδες έχουν το ίδιο πλήθος στοιχείων, ο ισομορφισμός $(**)$ δίνει $n/\delta = \varepsilon/m$, δηλαδή $n \cdot m = \delta \cdot \varepsilon$. Ένας πολύ γνωστός τύπος, που διέπει τους φυσικούς αριθμούς.

Θεώρημα 1.7.27. *[Τρίτο Θεώρημα Ισομορφίας] Έστω ότι G είναι μια ομάδα, ότι H και K είναι ορθόθετες υποομάδες τής G με $K \leq H$. Τότε η H/K είναι ορθόθετη υποομάδα τής G/K και $(G/K)/(H/K) \cong G/H$.*

Απόδειξη. Θεωρούμε την αντιστοιχία $\varphi : G/K \to G/H, gK \mapsto \varphi(gK) := gH$. Η φ είναι μια καλά ορισμένη απεικόνιση, αφού όταν $gK = g'K, g, g' \in G$, τότε $g^{-1}g' \in K \leq H$ και συνεπώς $gH = g'H$, δηλαδή $\varphi(gK) = \varphi(g'K)$. Η φ είναι ένας ομομορφισμός, διότι $\forall gK, g'K \in G/K$ είναι $\varphi((gK)(g'K)) = \varphi(gg'K) = gg'H = (gH)(g'H) = \varphi(gK)\varphi(g'K)$. Το $gK \in \ker\varphi \Leftrightarrow \varphi(gK) = gH = H \Leftrightarrow g \in H$. Επομένως, $\ker\varphi = H/K$ και $H/K \trianglelefteq G/K$. Τέλος, είναι φανερό ότι ο φ είναι ένας επιμορφισμός, δηλαδή ότι $\operatorname{im}\varphi = G/H$. Από το Πρώτο Θεώρημα Ισομορφισμών είναι: $(G/K)/\ker\varphi = (G/K)/(H/K) \cong \operatorname{im}\varphi = G/H$. □

Πόσοι διαφορετικοί ομομορφισμοί υπάρχουν από μια κυκλική ομάδα τάξης m σε μια κυκλική ομάδα τάξης n;

Λήμμα 1.7.28. *Έστω ότι G και G' είναι δύο κυκλικές ομάδες τάξης m και n αντιστοίχως. Έστω a ένας γεννήτορας τής G και c ένα στοιχείο τής G'. Η απεικόνιση $\chi : G \to G', a^t \to \chi(a^t) := c^t, \forall t \in \mathbb{Z}$ είναι μια καλά ορισμένη απεικόνιση, αν και μόνο αν, η τάξη $\circ(c)$ διαιρεί την τάξη $m = \circ(a)$.*

Απόδειξη. «$\Rightarrow$» Αφού η χ είναι καλά ορισμένη, έχουμε $\forall t, r \in \mathbb{Z}$ ότι $a^t = a^r \Rightarrow c^t = c^r$. Ιδιαιτέρως, από $a^{\circ(m)} = a^0 = e_m$, έπεται $c^{\circ(m)} = c^0 = e_n$, όπου e_m και e_n είναι αντιστοίχως τα ουδέτερα στοιχεία των G και G'. Επομένως, η $\circ(c)$ είναι διαιρέτης τής $\circ(a)$.

«$\Leftarrow$» Όταν $a^t = a^r$, τότε $\circ(a) \mid t-r$ και αφού $\circ(c) \mid \circ(a)$, συμπεραίνουμε ότι $\circ(c) \mid t-r$. Άρα, $c^{t-r} = e_n$ και επομένως $c^t = c^r$. □

Παρατήρηση 1.7.29. Προσέξτε ότι με την υπόθεση $\circ(c) \mid \circ(a)$ τού προηγούμενου λήμματος, η καλά ορισμένη απεικόνιση $\chi : G \to G', a^t \mapsto c^t$ είναι ένας ομομορφισμός ομάδων, αφού $\forall a^t, a^s \in G$ είναι

$$\chi(a^t a^s) = \chi(a^{t+s}) = c^{t+s} = c^t c^s = \chi(a^t)\chi(a^s).$$

Πρόταση 1.7.30. *Έστω ότι G και G' είναι δύο κυκλικές ομάδες τάξης m και n αντιστοίχως. Το πλήθος των διαφορετικών ομομορφισμών $\chi : G \to G'$ ισούται με τον ΜΚΔ(m, n).*

Απόδειξη. Έστω ότι $\mathcal{H}_{nm}$ είναι το σύνολο των ομομορφισμών από την G στην G', ότι $\Delta = \{d_i \mid 1 \leq i \leq \rho\}$ είναι το σύνολο των κοινών διαιρετών των αριθμών n και m και ότι $\{C_d \mid d \in \Delta\}$ είναι το αντίστοιχο σύνολο των υποομάδων τής G' με τάξη $[C_d : 1] = d \in \Delta$. Υπενθυμίζουμε ότι για κάθε $d \in \Delta$, υπάρχει ακριβώς μία υποομάδα τής G' τάξης d. Συμβολίζουμε με $\mathcal{G}\{C_d\}$ το σύνολο των γεννητόρων τής C_d. Επιλέγουμε έναν γεννήτορα a τής G. Παρατηρούμε ότι για κάθε ομομορφισμό $\chi : G \to G'$, δηλαδή για κάθε $\chi \in \mathcal{H}_{nm}$, η εικόνα $\mathrm{im}\,\chi = \chi(\langle a \rangle)$ είναι μια (κυκλική) υποομάδα τής G' με γεννήτορα το στοιχείο $\chi(a)$, αφού $\chi(\langle a \rangle) = \langle \chi(a) \rangle$. Από το Θεώρημα Lagrange, γνωρίζουμε ότι η τάξη d τής $\chi(\langle a \rangle)$ είναι διαιρέτης τού n. Επιπλέον, η τάξη d είναι ένας διαιρέτης τού m, αφού από το Πρώτο Θεώρημα Ισομορφίας, βλ. Θεώρημα 1.7.21, έχουμε ότι $\chi(\langle a \rangle) = \mathrm{im}\,\chi \cong G/\ker\chi$ και ως εκ τούτου, $d = [\mathrm{im}\,\chi : 1] = [G : \ker\chi]$. Επομένως, η τάξη d ανήκει στο σύνολο Δ και γι' αυτό η αντιστοιχία

$$\Psi : \mathcal{H}_{nm} \longrightarrow \bigcup_{d \in \Delta} \mathcal{G}\{C_d\}, \chi \mapsto \Psi(\chi) := \chi(a)$$

είναι μια καλά ορισμένη απεικόνιση.

Ισχυριζόμαστε ότι η Ψ είναι αμφιρριπτική.

Πράγματι, η Ψ είναι ενριπτική, αφού όταν $\Psi(\chi_1) = \Psi(\chi_2)$, $\chi_1, \chi_2 \in \mathcal{H}_{nm}$, τότε $\chi_1(a) = \chi_2(a)$ και ως εκ τούτου, $\chi_1 = \chi_2$, διότι τα χ_1, χ_2 είναι ομομορφισμοί και η G είναι κυκλική με γεννήτορα το a.

Υπολείπεται η απόδειξη ότι η Ψ είναι επιρριπτική. Έστω $c \in \bigcup_{d \in \Delta} \mathcal{G}\{C_d\}$. Τότε υπάρχει ακριβώς ένα $d \in \Delta$ με $c \in \mathcal{G}\{C_d\}$, αφού τα $\mathcal{G}\{C_d\}$ είναι ανά δύο αποσυνδετά. Η τάξη $d = \circ(c)$ είναι διαιρέτης τού n και ο n ισούται με $\circ(a)$, διότι το a είναι γεννήτορας τής G. Θεωρούμε την αντιστοιχία $\chi : G \to G', a^t \mapsto \chi(a^t) = c^t, \forall t \in \mathbb{Z}$. Στο Λήμμα 1.7.28 διαπιστώσαμε ότι η χ είναι μια καλά ορισμένη απεικόνιση και στην Παρατήρηση 1.7.29 ότι η χ είναι ένας ομομορφισμός. Προφανώς, $\Psi(\chi) = \chi(a) = c^1 = c$. Άρα, η Ψ είναι επιρριπτική.

Τώρα, αφού η Ψ είναι μια αμφίρριψη, το πλήθος των στοιχείων τού $\mathcal{H}_{nm}$ ισούται με το πλήθος των στοιχείων τού $\bigcup_{d \in \Delta} \mathcal{G}\{C_d\}$. Σύμφωνα με την Άσκηση A68, το πλήθος των στοιχείων τού $\bigcup_{d \in \Delta} \mathcal{G}\{C_d\}$ ισούται με τον ΜΚΔ(m, n). □

Ενδομορφισμοί και Αυτομορφισμοί

Ορισμός 1.7.31. Ένας ομομορφισμός $\varphi : G \to G$ από μια ομάδα στον εαυτό της ονομάζεται *ενδομορφισμός* τής G.

Ορισμός 1.7.32. Ένας ενδομορφισμός $\varphi : G \to G$ ονομάζεται *αυτομορφισμός* τής G, αν είναι ισομορφισμός.

Θα συμβολίζουμε το σύνολο των ενδομορφισμών μιας ομάδας $(G, \star)$ με $\mathrm{End}(G)$ και το σύνολο των αυτομορφισμών της με $\mathrm{Aut}(G)$.

Η ταυτοτική απεικόνιση $\mathrm{Id}_G : G \to G$ είναι πάντοτε ένας ενδομορφισμός τής G και αφού $\mathrm{End}(G) \subseteq \mathrm{Aut}(G)$, τα δύο αυτά σύνολα είναι πάντοτε $\neq \emptyset$. Αφού η σύνθεση «$\circ$» ενδομορφισμών, αντιστοίχως αυτομορφισμών, μιας ομάδας G είναι ενδομορφισμός, αντιστοίχως αυτομορφισμός, τα $\mathrm{End}(G)$ και $\mathrm{Aut}(G)$ είναι κλειστά ως προς τη σύνθεση των απεικονίσεων. Γενικά, οι ενδομορφισμοί μιας ομάδας[34] δεν αποτελούν ομάδα ως προς τη σύνθεση των απεικονίσεων. Αντίθετα, το $\mathrm{Aut}(G)$ είναι πάντοτε ομάδα ως προς τη σύνθεση των απεικονίσεων.

Πρόταση 1.7.33. *Έστω $(G, \star)$ μια ομάδα και $\mathrm{Aut}(G)$ το σύνολο των αυτομορφισμών της. Το ζεύγος $(\mathrm{Aut}(G), \circ)$, όπου «$\circ$» είναι η σύνθεση των απεικονίσεων, αποτελεί μια ομάδα.*

Απόδειξη. Προτείνουμε την απόδειξη ως άσκηση για τον αναγνώστη. □

Ορισμός 1.7.34. Η $(\mathrm{Aut}(G), \circ)$ ονομάζεται η *ομάδα αυτομορφισμών* τής $(G, \star)$.

Όπως θα δούμε πολύ σύντομα, η ομάδα $\mathrm{Aut}(G)$ δίνει πολλές πληροφορίες και για την ίδια την ομάδα $(G, \star)$ και για τις υποομάδες της.

Παρατήρηση 1.7.35. Προφανώς, η ομάδα αυτομορφισμών $\mathrm{Aut}(G)$ οποιασδήποτε ομάδας $(G, \star)$ είναι υποομάδα τής συμμετρικής ομάδας $(S_G, \circ)$ των αμφιρριπτικών απεικονίσεων από το σύνολο G στον εαυτό του, αφού κάθε αυτομορφισμός τής G είναι ιδιαιτέρως μια αμφιρριπτική απεικόνιση. Όταν για κάποιον σταθερό φυσικό αριθμό n, το σύνολο $G_n = \{g \in G \mid \circ(g) = n\}$ είναι $\neq \emptyset$, τότε η απεικόνιση $\mathrm{Aut}(G) \to S_{G_n}, \chi \mapsto \chi_{|G_n}$, όπου $\chi_{|G_n}$ είναι ο περιορισμός τού χ στο σύνολο G_n, αποτελεί έναν ομομορφισμό ομάδων, αφού η εικόνα $\chi(g)$ οποιουδήποτε στοιχείου τής G έχει την ίδια τάξη με το g. Το ίδιο συμβαίνει με οποιοδήποτε αλγεβρικό αντικείμενο τής G που παραμένει αναλλοίωτο από τους αυτομορφισμούς τής G, όπως είναι το σύνολο $\mathcal{S}$ των υποομάδων τής G ή το σύνολο $\mathcal{S}_d$ των υποομάδων τής G τάξης d.

Η ομάδα αυτομορφισμών μιας κυκλικής ομάδας

Θα προσδιορίσουμε την ομάδα αυτομορφισμών $\mathrm{Aut}(G)$ μιας κυκλικής ομάδας $(G, \star)$. Ως γνωστόν, κάθε ομομορφισμός χ από την κυκλική ομάδα G σε οποιαδήποτε άλλη ομάδα (όχι απαραίτητα κυκλική) προσδιορίζεται μοναδικά από την τιμή $\chi(a)$, όπου a είναι ένας γεννήτορας τής G, αφού κάθε στοιχείο τής G είναι τής μορφής $a^z, z \in \mathbb{Z}$ και ως εκ τούτου, $\chi(a^z) = \chi(a)^z, \forall z \in \mathbb{Z}$. Με άλλα λόγια, κάθε ομομορφισμός $\chi : G \to G'$ είναι τής μορφής $a^z \mapsto \chi(a)^z, \forall z \in \mathbb{Z}$, όπου ο a είναι ένας γεννήτορας τής G.

Λήμμα 1.7.36. *Έστω ότι $(G, \star)$ είναι μια κυκλική ομάδα, ότι $\chi \in \mathrm{End}(G)$ και ότι a είναι ένας γεννήτορας τής G. Ο ενδομορφισμός χ ανήκει στην $\mathrm{Aut}(G)$, αν και μόνο αν, η εικόνα $\chi(a)$ είναι επίσης γεννήτορας τής G.*

Απόδειξη. Υπενθυμίζουμε ότι για κάθε $\chi \in \mathrm{End}(G)$, είναι $\mathrm{im}\,\chi = \langle \chi(a) \rangle$ και ως εκ τούτου, το $\chi(a)$ είναι πάντοτε ένας γεννήτορας τής εικόνας $\mathrm{im}\,\chi$.
«$\Rightarrow$» Αφού $\chi \in \mathrm{Aut}(G)$, συμπεραίνουμε ότι $\mathrm{im}\,\chi = G$ και επομένως το $\chi(a)$ είναι γεννήτορας τής G.
«$\Leftarrow$» Λόγω τής υπόθεσης, $\mathrm{im}\,\chi = \langle \chi(a) \rangle = G$, δηλαδή ο χ είναι επιμορφισμός.

[34]Ωστόσο, το σύνολο των ενδομορφισμών τής τετριμμένης ομάδας $\{e\}$, που είναι το $\{\mathrm{Id}_{\{e\}}\}$ ισούται με το σύνολο των αυτομορφισμών και φυσικά είναι ομάδα ως προς τη σύνθεση

Αν η τάξη τής G είναι πεπερασμένη, τότε προφανώς ο χ είναι μια ενριπτική απεικόνιση («$1-1$») και επομένως είναι αυτομορφισμός.

Αν η τάξη τής G είναι άπειρη, τότε γνωρίζουμε ότι οι μοναδικοί γεννήτορές της είναι οι a και a^{-1}, βλ. Πρόταση 1.5.13. Επομένως, η εικόνα $\chi(a)$ ισούται ή με a ή με a^{-1}. Στην πρώτη περίπτωση, η χ είναι η απεικόνιση με $\chi(a^z) = a^z, \forall z \in \mathbb{Z}$, δηλαδή είναι η ταυτοτική απεικόνιση, η οποία προφανώς είναι ενριπτική. Στη δεύτερη περίπτωση, η χ είναι η απεικόνιση με $\chi(a^z) = a^{-z}, \forall z \in \mathbb{Z}$. Αυτή είναι επίσης ενριπτική, αφού $\forall z, w \in \mathbb{Z}, a^{-z} = a^{-w} \Rightarrow a^z = a^w$. Σε αμφότερες τις περιπτώσεις, ο χ είναι αυτομορφισμός. □

Θεώρημα 1.7.37. *Έστω ότι $(G, \star)$ είναι μια κυκλική ομάδα.*

(α′) *Όταν $[G : 1] = \infty$, τότε η ομάδα $(\mathrm{Aut}(G), \circ)$ των αυτομορφισμών της είναι ισόμορφη προς την ομάδα $(\mathbb{Z}_2, +)$.*

(β′) *Όταν $[G : 1] = n \in \mathbb{N}$, τότε η ομάδα $(\mathrm{Aut}(G), \circ)$ των αυτομορφισμών της είναι ισόμορφη προς την ομάδα $(\mathbb{U}_n, \cdot)$ των αντιστρέψιμων στοιχείων τού $\mathbb{Z}_n$.* (Βλ. Παράδειγμα 1.2.21.)

Απόδειξη. (α′) Στο αμέσως προηγούμενο λήμμα διαπιστώσαμε ότι όταν η G είναι μια άπειρη κυκλική ομάδα, τότε υπάρχουν ακριβώς δύο αυτομορφισμοί, δηλαδή η τάξη τής $\mathrm{Aut}(G)$ ισούται με 2. Κάθε ομάδα τάξης 2 είναι ισόμορφη προς την $(\mathbb{Z}_2, +)$.
(β′) Έστω ότι a είναι ένας γεννήτορας τής G και ότι χ είναι ένας αυτομορφισμός της. Από το αμέσως προηγούμενο λήμμα, γνωρίζουμε ότι η εικόνα $\chi(a) = a^s, s \in \mathbb{N}$ είναι ένας γεννήτορας τής G και από την Πρόταση 1.5.13 γνωρίζουμε ότι αυτό συμβαίνει, αν και μόνο αν, ο $\mathrm{MK\Delta}(n, s) = 1$. Ως εκ τούτου, η αντιστοιχία

$$\Psi : \mathrm{Aut}(G) \to \mathbb{U}_n, \chi \mapsto \Psi(\chi) = [s]_n,$$

όπου $\chi(a) = a^s$, είναι μια καλά ορισμένη απεικόνιση.

Παρατηρούμε ότι ο Ψ είναι ομομορφισμός ομάδων. Πράγματι, όταν $\chi, \psi \in \mathrm{Aut}(G)$, με $\chi(a) = a^s$ και $\psi(a) = a^t$, τότε $(\chi \circ \psi)(a) = \chi(a^t) = a^{st}$ και $\Psi(\chi \circ \psi) = [st]_n = [s]_n[t]_n = \Psi(\chi)\Psi(\psi)$.

Ο ομομορφισμός Ψ είναι «επί», αφού όταν $[s]_n \in \mathbb{U}_n, 1 \leq s \leq n$, τότε ο ενδομορφισμός[35] $\chi : G \to G, a^z \mapsto \chi(a^z) := a^{sz}$ είναι ένας αυτομορφισμός. Πράγματι, η εικόνα $\chi(a) = a^s$ είναι ένας γεννήτορας τής G, επειδή ο $\mathrm{MK\Delta}(s, n) = 1$. Ως εκ τούτου, $\Psi(\chi) = [s]_n$.

Τέλος, θα αποδείξουμε ότι ο Ψ είναι μονομορφισμός, δείχνοντας ότι ο πυρήνας τού Ψ αποτελείται μόνο από το ουδέτερο στοιχείο της $\mathrm{Aut}(G)$. Έστω ότι ο $\chi \in \mathrm{Aut}(G)$ με $\chi(a) = a^s$ ανήκει στον $\ker \Psi$, τότε $\Psi(\chi) = [s]_n = [1]_n$. Συνεπώς, $s - 1 = n\lambda, \lambda \in \mathbb{Z}$ και επομένως $a^{s-1} = (a^n)^\lambda = e_G$. Άρα, $\chi(a) = a^s = a$ και ο χ είναι το ουδέτερο στοιχείο τής $\mathrm{Aut}(G)$, αφού $\chi(a^z) = \chi(a)^z = a^z, \forall z \in \mathbb{Z}$. □

Παρατήρηση 1.7.38. Όταν η $(G, \star)$ είναι μια πεπερασμένη κυκλική ομάδα, τότε σύμφωνα με την Πρόταση 1.7.30, το πλήθος των στοιχείων τού $\mathrm{End}(G)$ ισούται με $\mathrm{MK\Delta}(n, n) = n$

[35]Φυσικά πρόκειται για μια καλά ορισμένη απεικόνιση, διότι σε κάθε περίπτωση η τάξη $\circ(\chi(a))$ διαιρεί την $\circ(a)$ και κατόπιν προφανώς είναι ενδομορφισμός.

και σύμφωνα με το προηγούμενο θεώρημα η τάξη $[\mathrm{Aut}(G) : 1]$ τής $\mathrm{Aut}(G)$ ισούται με την τιμή $\varphi(n)$, όπου φ είναι η φ–συνάρτηση Euler.

Ας δούμε μια ενδιαφέρουσα εφαρμογή των Θεωρημάτων 1.7.21 και 1.7.37:

Το πλήθος των αυτομορφισμών τής διεδρικής ομάδας $\mathbf{D_n}$, $n \geq 3$ ισούται με $n \cdot \varphi(n)$

Υπενθυμίζουμε ότι η διεδρική ομάδα D_n ισούται με $\{\mathrm{Id}_n, \tau, \rho, \rho^2, \ldots, \rho^{n-1}, \tau \circ \rho, \tau \circ \rho^2, \ldots, \tau \circ \rho^{n-1}\}$, όπου οι δυνάμεις $\rho^i, i \in \mathbb{Z}$ απαρτίζουν την κυκλική υποομάδα $\langle \rho \rangle$ τής D_n τάξης $[\langle \rho \rangle : 1] = n$ και όπου τα n το πλήθος στοιχεία[36] $\tau \circ \rho^i, i \in \mathbb{Z}$ είναι τάξης 2. Επιπλέον, είναι $\rho \circ \tau = \tau \circ \rho^{-1}$ και γενικότερα, $\rho^i \circ \tau = \tau \circ \rho^{-i}, \forall i \in \mathbb{Z}$.

Αρχίζουμε με ένα απλό υπολογιστικό λήμμα:

Λήμμα 1.7.39. (α′) *Για κάθε φυσικό $s, 1 \leq s \leq n-1$ με $\mathrm{ΜΚΔ}(n, s) = 1$, η απεικόνιση $\chi : D_n \to D_n$ η οποία ορίζεται στα στοιχεία τής D_n, ως $\chi(\tau \circ \rho^i) := \tau \circ \rho^{is}, \forall i \in \mathbb{Z}$ και $\chi(\rho^i) := \rho^{is}, \forall i \in \mathbb{Z}$ είναι ένας αυτομορφισμός τής D_n.*

(β′) *Για κάθε $\alpha \in \mathbb{N} \bigcup \{0\}, 0 \leq \alpha \leq n-1$, η απεικόνιση $\psi : D_n \to D_n$ η οποία ορίζεται στα στοιχεία τής D_n, ως $\psi(\tau \circ \rho^i) := \tau \circ \rho^{i+\alpha}, \forall i \in \mathbb{Z}$ και $\psi(\rho^i) := \rho^i, \forall i \in \mathbb{Z}$ είναι ένας αυτομορφισμός τής D_n.*

Απόδειξη. Παρατηρούμε ότι οι χ και ψ είναι καλά ορισμένες απεικονίσεις. Θεωρούμε τα $x = \tau \circ \rho^i, x' = \tau \circ \rho^j, y = \rho^k, y' = \rho^\ell, i, j, k, \ell \in \mathbb{Z}$. Αν επιβεβαιώσουμε τις τέσσερεις ισότητες $\omega(x \circ x') = \omega(x) \circ (x'), \omega(x \circ y) = \omega(x) \circ (y), \omega(y \circ x) = \omega(y) \circ (x), \omega(y \circ y') = \omega(y) \circ (y')$, όπου $\omega = \chi$ ή ψ, τότε προκύπτει ότι οι χ και ψ είναι ενδομορφισμοί.

Υπολογίζουμε τα γινόμενα:

$$\begin{aligned}
&x \circ x' = (\tau \circ \rho^i) \circ (\tau \circ \rho^j) = \tau \circ (\rho^i \circ \tau) \circ \rho^j = \tau \circ \tau \circ \rho^{-i} \rho^j = \rho^{j-i} \\
&x \circ y = (\tau \circ \rho^i) \circ \rho^k = \tau \circ \rho^{i+k} \\
&y \circ x = \rho^k \circ (\tau \circ \rho^i) = (\rho^k \circ \tau) \circ \rho^i = \tau \circ \rho^{-k} \circ \rho^i = \tau \circ \rho^{i-k} \\
&y \circ y' = \rho^k \circ \rho^\ell = \rho^{k+\ell}.
\end{aligned}$$

(α′) Έχουμε:
$\chi(x \circ x') = \chi(\rho^{(j-i)}) = \rho^{(j-i)s}$ και $\chi(x) \circ \chi(x') = (\tau \circ \rho^{is}) \circ (\tau \circ \rho^{js}) = \rho^{js} \circ \rho^{-is} = \rho^{(j-i)s}$. Συνεπώς, $\chi(x \circ x') = \chi(x) \circ \chi(x')$.
$\chi(x \circ y) = \chi(\tau \circ \rho^{(i+k)}) = \tau \circ \rho^{(i+k)s}$ και $\chi(x) \circ \chi(y) = \tau \circ \rho^{is} \circ \rho^{ks} = \tau \circ \rho^{(i+k)s}$. Συνεπώς, $\chi(x \circ y) = \chi(x) \circ (y)$
$\chi(y \circ x) = \chi(\tau \circ \rho^{(i-k)}) = \tau \circ \rho^{(i-k)s}$ και $\chi(y) \circ \chi(x) = \rho^{ks} \circ \tau \circ \rho^{is} = \tau \circ \rho^{-ks} \circ \rho^{is} = \tau \circ \rho^{(i-k)s}$.
Η ισότητα $\chi(y \circ y') = \chi(y) \circ (y')$ είναι προφανής.

Υπολείπεται η απόδειξη ότι ο χ είναι αμφιρριπτικός. Αρκεί να αποδείξουμε ότι είναι επιρριπτικός. Αφού όμως το στοιχείο ρ^s είναι γεννήτορας τής ρ, για κάθε $\rho^\lambda, \lambda \in \mathbb{Z}$ είναι

[36] Κάθε $\rho^i, i \in \mathbb{Z}$ ισούται με κάποιο από τα σαφώς διακεκριμένα στοιχεία $\mathrm{Id}_n, \rho, \ldots, \rho^{n-1}$, αφού $\circ(\rho) = n$.

$\rho^\lambda = \rho^{\kappa s}, \kappa \in \mathbb{Z}$ και αντίστοιχα $\tau \circ \rho^\lambda = \tau \circ \rho^{\kappa s}, \kappa \in \mathbb{Z}$. Άρα, $\rho^\lambda = \rho^{\kappa s} = \chi(\rho^\kappa)$ και $\tau \circ \rho^\lambda = \tau \circ \rho^{\kappa s} = \chi(\tau \circ \rho^\kappa)$.
(β′) Έχουμε:
$\psi(x \circ x') = \psi(\rho^{(j-i)}) = \rho^{(j-i)}$ και $\psi(x) \circ \psi(x') = (\tau \circ \rho^{(i+\alpha)}) \circ (\tau \circ \rho^{(j+\alpha)}) = \rho^{-(i+\alpha)} \circ \rho^{(j+\alpha)} = \rho^{(j+\alpha)-(i+\alpha)} = \rho^{(j-i)}$. Συνεπώς, $\psi(x \circ x') = \psi(x) \circ \psi(x')$.
$\psi(x \circ y) = \psi(\tau \circ \rho^{(i+k)}) = \tau \circ \rho^{(i+k)+\alpha}$ και $\psi(x) \circ \psi(y) = \tau \circ \rho^{(i+\alpha)} \circ \rho^k = \tau \circ \rho^{(i+k)+\alpha}$. Συνεπώς, $\psi(x \circ y) = \psi(x) \circ (y)$
$\psi(y \circ x) = \psi(\tau \circ \rho^{(i-k)}) = \tau \circ \rho^{(i-k)+\alpha}$ και $\psi(y) \circ \psi(x) = \rho^k \circ \tau \circ \rho^{i+\alpha} = \tau \circ \rho^{-k} \circ \rho^{i+\alpha} = \tau \circ \rho^{(i-k)+\alpha}$.
Η ισότητα $\psi(y \circ y') = \psi(y) \circ (y')$ είναι προφανής.

Υπολείπεται η απόδειξη ότι ο ψ είναι αμφιρριπτικός. Αρκεί να αποδείξουμε ότι είναι επιρριπτικός. Παρατηρούμε ότι για κάθε $\rho^\lambda, \lambda \in \mathbb{Z}$ είναι $\rho^\lambda = \psi(\rho^\lambda)$ και για κάθε $\tau \circ \rho^\lambda, \lambda \in \mathbb{Z}$ είναι $\tau \circ \rho^\lambda = \psi(\tau \circ \rho^{\lambda-\alpha})$ □

Θεώρημα 1.7.40. *Η τάξη $\mathrm{Aut}(D_n)$ τής ομάδας αυτομορφισμών τής διεδρικής ομάδας $D_n, n \in \mathbb{N}, n \geq 3$, ισούται με $n \cdot \varphi(n)$, όπου φ είναι η φ–συνάρτηση Euler.*

Απόδειξη. Παρατηρούμε ότι ο περιορισμός $\chi_{|\langle\rho\rangle}$ οποιουδήποτε αυτομορφισμού $\chi \in \mathrm{Aut}(D_n)$ στην κυκλική υποομάδα $\langle\rho\rangle$ είναι ένας αυτομορφισμός τής $\langle\rho\rangle$. Πράγματι, έχουμε $\chi(\langle\rho\rangle) = \langle\chi(\rho)\rangle$ και τώρα επειδή ο χ διατηρεί την τάξη n τού ρ, πρέπει η τάξη $\circ(\chi(\rho))$ να ισούται επίσης με n. Αλλά τα μοναδικά στοιχεία τής D_n τάξης n είναι ακριβώς οι δυνάμεις ρ^s, όπου $\mathrm{MK\Delta}(s, n) = 1$, δηλαδή οι γεννήτορες τής υποομάδας $\langle\rho\rangle$. Επομένως, $\chi(\langle\rho\rangle) = \langle\chi(\rho)\rangle = \langle\rho^s\rangle = \langle\rho\rangle$. Συνεπώς, ο ομομορφισμός $\chi_{|\langle\rho\rangle} : \langle\rho\rangle \to \chi(\langle\rho\rangle)$ είναι ένας επιμορφισμός από τη $\langle\rho\rangle$ στη $\langle\rho\rangle$, ο οποίος προφανώς είναι αυτομορφισμός τής $\langle\rho\rangle$, αφού πρόκειται για μια πεπερασμένη ομάδα.

Θεωρούμε την αντιστοιχία:

$$\Psi : \mathrm{Aut}(D_n) \to \mathrm{Aut}(\langle\rho\rangle), \chi \mapsto \Psi(\chi) = \chi_{|\langle\rho\rangle}.$$

Σύμφωνα με όσα προαναφέραμε, η Ψ είναι μια καλά ορισμένη απεικόνιση, η οποία μάλιστα είναι ένας ομομορφισμός ομάδων, αφού προφανώς$(\chi \circ \chi')_{|\langle\rho\rangle} = \chi_{|\langle\rho\rangle} \circ \chi'_{|\langle\rho\rangle}$.

Από το πρώτο μέρος τού Λήμματος 1.7.39, διαπιστώνουμε αμέσως ότι ο Ψ είναι ένας επιμορφισμός, αφού κάθε αυτομορφισμός τής $\langle\rho\rangle$ είναι τής μορφής $\rho^i \mapsto \rho^{is}$, όπου $1 \leq s \leq n-1$ με $\mathrm{MK\Delta}(n, s) = 1$.

Συνεπώς, $\mathrm{Aut}(D_n)/\ker\Psi \cong \mathrm{im}\,\Psi = \mathrm{Aut}(\langle\rho\rangle)$ και υπολογίζοντας τις τάξεις έχουμε $[\mathrm{Aut}(D_n) : 1] = [\ker\Psi : 1][\mathrm{Aut}(\langle\rho\rangle) : 1] = [\ker\Psi : 1] \cdot \varphi(n)$. (Υπενθυμίζουμε $\mathrm{Aut}(\langle\rho\rangle) \cong \mathbb{U}_n$.)
Θα υπολογίσουμε τον $\ker\Psi$. Παρατηρούμε, ότι κάθε $\chi \in \mathrm{Aut}(D_n)$ απεικονίζει στοιχεία τάξης 2 σε στοιχεία τάξης 2. Επομένως, το $\chi(\tau) = \tau \circ \rho^\alpha$, για κάποιο $\alpha, 0 \leq \alpha \leq n-1$. Επιπλέον, αν ο χ ανήκει στον $\ker\Psi$, τότε $\chi_{|\langle\rho\rangle} = \mathrm{Id}_{\langle\rho\rangle}$. Ως εκ τούτου, $\chi(\rho^i) = \rho^i, \forall i \in \mathbb{Z}, (*)$ και $\chi(\tau \circ \rho^i) = \chi(\tau) \circ \chi(\rho^i) = \tau \circ \rho^{i+\alpha}, \forall i \in \mathbb{Z}, (**)$. Από το δεύτερο μέρος τού Λήμματος 1.7.39, γνωρίζουμε ότι κάθε απεικόνιση $\psi : D_n \to D_n$ που ικανοποιεί τις $(*)$ και $(**)$ είναι ένας αυτομορφισμός τής D_n. Επομένως, ο $\ker\Psi$ αποτελείται από ακριβώς αυτούς τους n το πλήθος αυτομορφισμούς.

Άρα, $[\mathrm{Aut}(D_n) : 1] = [\ker\Psi : 1] \cdot \varphi(n) = n \cdot \varphi(n)$.

Παρατήρηση 1.7.41. Σύμφωνα με το Λήμμα 1.7.39 και όσα αναφέραμε πιο πάνω ένας αυτομορφισμός χ τής D_n ανήκει στην ορθόθετη υποομάδα $\ker\Psi$, αν και μόνο αν, $\chi(\rho) = \rho$ και $\chi(\tau) = \tau \circ \rho^{\alpha}$, όπου $0 \le \alpha \le n-1$. Έστω $\psi \in \ker\Psi$ ο αυτομορφισμός τής D_n με $\psi(\rho) = \rho$ και $\psi(\tau) = \tau \circ \rho$. Η τάξη τού ψ είναι n, διότι $\forall i, 1 \le i \le n$ είναι $\psi^i(\rho) = \rho$ και $\psi^i(\tau) = \tau \circ \rho^i$. Τώρα επειδή η τάξη $[\ker\Psi : 1] = n$, συμπεραίνουμε ότι $\ker\Psi = \langle\psi\rangle$.

Στο Θεώρημα 7.2.20 θα αποδείξουμε ότι η ομάδα $\mathrm{Aut}(D_n)$, $n \ge 3$ είναι ισόμορφη προς το εξωτερικό ημιευθύ γινόμενο $\mathbb{Z}_n \rtimes_\theta \mathbb{U}_n$. □

Εσωτερικοί και εξωτερικοί αυτομορφισμοί ομάδας

Έστω $(G, \star)$ μια ομάδα και a οποιοδήποτε στοιχείο τής G. Διαπιστώνεται πολύ εύκολα ότι η απεικόνιση $\chi_a : G \to G, g \mapsto \chi_a(g) := aga^{-1}$ είναι ένας ενδομορφισμός τής G. Πράγματι,

$$\forall g, g' \in G : \chi_a(gg') = agg'a^{-1} = (aga^{-1})(ag'a^{-1}) = \chi_a(g)\chi_a(g').$$

Επιπλέον, ο ενδομορφισμός χ_a έχει ως αντίστροφο τον ενδομορφισμό $\chi_{a^{-1}}$ που ορίζεται από το αντίστροφο a^{-1} τού a. Πράγματι,

$$\begin{aligned}\forall g \in G :&(\chi_a \circ \chi_{a^{-1}})(g) = \chi_a(\chi_{a^{-1}}(g)) = \chi_a(a^{-1}g(a^{-1})^{-1}) = \\ &\chi_a(a^{-1}ga) = a(a^{-1}ga)a^{-1} = g.\end{aligned}$$

Επομένως, η σύνθεση $\chi_a \circ \chi_{a^{-1}}$ ισούται με τον ταυτοτικό αυτομορφισμό Id_G. Παρόμοια αποδεικνύεται ότι $\chi_{a^{-1}} \circ \chi_a = \mathrm{Id}_G$ και ως εκ τούτου, ο ενδομορφισμός χ_a ανήκει στην $\mathrm{Aut}(G)$.

Ορισμός 1.7.42. Ένας αυτομορφισμός $\chi \in \mathrm{Aut}(G)$ ονομάζεται *εσωτερικός*, όταν υπάρχει $a \in G$ με $\chi = \chi_a$. Διαφορετικά, ο αυτομορφισμός χ ονομάζεται *εξωτερικός*.

Το σύνολο των εσωτερικών αυτομορφισμών μιας ομάδας G, το συμβολίζουμε με $\mathrm{Inn}(G)$. Όταν η $(G, \star)$ είναι μια αβελιανή ομάδα, τότε κάθε εσωτερικός αυτομορφισμός χ_a συμπίπτει με τον ταυτοτικό αυτομορφισμό Id_G, αφού $\forall g \in G$, είναι $\chi_a(g) = aga^{-1} = aa^{-1}g = e_G g = g$. Συνεπώς, η ύπαρξη μη τετριμμένων εσωτερικών αυτομορφισμών μας πληροφορεί ότι η ομάδα G δεν είναι αβελιανή.

Προφανώς όλοι οι αυτομορφισμοί μιας κυκλικής ομάδας εκτός από τον ταυτοτικό είναι εξωτερικοί.

Θεώρημα 1.7.43. *Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι $H \le G$ είναι μια υποομάδα τής G. Ισχύουν τα εξής:*

(α′) *Ο κεντροποιητής $\mathcal{C}_G(H)$ τής H* (βλ. Άσκηση ΠΑ35) *είναι μια ορθόθετη υποομάδα τού ορθοθετοποιητή $\mathcal{N}_G(H)$ τής H* (βλ. Άσκηση Α38) *και η πηλικοομάδα $\mathcal{N}_G(H)/\mathcal{C}_G(H)$ είναι ισόμορφη προς μια υποομάδα τής $\mathrm{Aut}(H)$.*

(β′) *Το σύνολο $\mathrm{Inn}(G)$ των εσωτερικών αυτομορφισμών τής G είναι μια ορθόθετη υποομάδα τής $\mathrm{Aut}(G)$ και η $\mathrm{Inn}(G)$ είναι ισόμορφη προς την πηλικοομάδα $G/\mathcal{Z}(G)$, όπου $\mathcal{Z}(G)$ είναι το κέντρο τής G.*

Απόδειξη. (α′) Παρατηρούμε ότι για κάθε $a \in \mathcal{N}_G(H) = \{a \in G \mid aHa^{-1} = H\}$, ο περιορισμός $\chi_{a|H}$ τού εσωτερικού αυτομορφισμού χ_a στην H ανήκει στην $\mathrm{Aut}(H)$, διότι το a ανήκει στον $\mathcal{N}_G(H)$. Είναι εύκολη η επιβεβαίωση ότι η απεικόνιση $\Psi : \mathcal{N}_G(H) \to \mathrm{Aut}(H), a \in \Psi(a) := \chi_{a|H}$ είναι ένας ομομορφισμός ομάδων. Θα υπολογίσουμε τον $\ker \Psi$. Το στοιχείο

$$a \in \ker \Psi \Leftrightarrow \chi_{a|H} = \mathrm{Id}_H \Leftrightarrow \forall h \in H, \chi_{a|H}(h) = h \Leftrightarrow \forall h \in H, aha^{-1} = h \Leftrightarrow h \in \mathcal{C}_G(H).$$

Επομένως, $\ker \Psi = \mathcal{C}_G(H)$. Από το Πρώτο Θεώρημα Ισομορφίας, βλ. Θεώρημα 1.7.21, έπεται τώρα ότι $\mathcal{N}_G(H)/\mathcal{C}_G(H) \cong \mathrm{im}\,\Psi \leq \mathrm{Aut}(H)$.
(β′) Έστω ότι υποομάδα H ισούται με τη G. Τότε ο ορθοθετοποιητής $\mathcal{N}_G(G) = G$ και ο κεντροποιητής $\mathcal{C}_G(G) = \mathcal{Z}(G)$. Θεωρούμε τον προηγούμενο ομομορφισμό $\Psi : G \to \mathrm{Aut}(G), a \mapsto \Psi(a) := \chi_a$, όπου τώρα $H = G$. Η εικόνα $\mathrm{im}\,\Psi$ ισούται με $\mathrm{Inn}(G)$ και από το πρώτο μέρος έχουμε $G/\mathcal{Z}(G) \cong \mathrm{im}\,\Psi = \mathrm{Inn}(G)$.
Υπολείπεται η απόδειξη ότι $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. Έστω $\chi_a \in \mathrm{Inn}(G)$ και $\psi \in \mathrm{Aut}(G)$. Προτείνουμε να αποδείξει ο αναγνώστης ότι $\psi \circ \chi_a \circ \psi^{-1} = \chi_{\psi(a)}$. Επομένως, το $\psi \circ \chi_a \circ \psi^{-1} \in \mathrm{Inn}(G)$ και ως εκ τούτου, $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. □

Το (α′) τού προηγούμενου θεωρήματος αναφέρεται στη βιβλιογραφία ως το (N/C)-Λήμμα.

Παράδειγμα 1.7.44. Για κάθε $n \geq 3$, η ομάδα $\mathrm{Inn}(S_n)$ των εσωτερικών αυτομορφισμών τής συμμετρικής ομάδας $(S_n, \circ)$ είναι ισόμορφη προς την S_n. Πράγματι, $\mathrm{Inn}(S_n) \cong S_n/\mathcal{Z}(S_n)$. Από την Άσκηση A41, γνωρίζουμε ότι $\mathcal{Z}(S_n) = \{\mathrm{Id}_n\}$. Επομένως, $\mathrm{Inn}(S_n) \cong S_n$.

Για $n = 3$, είναι $\mathrm{Inn}(S_3) = \mathrm{Aut}(S_3)$. Πράγματι, το πλήθος των αυτομορφισμών τής S_3 ισούται με $3 \cdot \varphi(3) = 6$, διότι $S_3 \cong D_3$. Σύμφωνα με όσα είπαμε πιο πάνω, το πλήθος των εσωτερικών αυτομορφισμών τής S_3 ισούται επίσης με 6, διότι $\mathrm{Inn}(S_3) \cong S_3$. Άρα, $\mathrm{Inn}(S_3) = \mathrm{Aut}(S_3)$. Με άλλα λόγια η S_3 δεν διαθέτει εξωτερικούς αυτομορφισμούς.

Ας δούμε μια ενδιαφέρουσα εφαρμογή τού Θεωρήματος 1.7.43:

***Εφαρμογή* 1.7.45.** *Κάθε ομάδα $(G, \star)$ τάξης 77 είναι κυκλική.*

Απόδειξη. Θα δείξουμε ότι η παραδοχή $G \neq$ κυκλική, οδηγεί σε άτοπο. Έστω ότι όντως η G δεν είναι κυκλική, τότε από το Θεώρημα Lagrange συμπεραίνουμε ότι κάθε στοιχείο $g \neq e_G$ έχει τάξη ή 7 ή 11. Από την Πρόταση 1.5.24, γνωρίζουμε ότι το πλήθος των στοιχείων τής G τάξης 7 είναι πολλαπλάσιο τού $\varphi(7) = 6$. Αν ήταν όλα τα $g \in G, g \neq e_G$ τάξης 7, τότε θα έπρεπε το $77 - 1 = 76$ να είναι πολλαπλάσιο τού 6, το οποίο είναι άτοπο. Παρόμοια, αν ήταν όλα τα $g \in G, g \neq e_G$ τάξης 11, τότε θα έπρεπε το $77 - 1 = 76$ να είναι πολλαπλάσιο τού $\varphi(11) = 10$, το οποίο είναι επίσης άτοπο. Επομένως, η G διαθέτει και στοιχεία τάξης 7 και στοιχεία τάξης 11. Έστω h ένα στοιχείο τάξης 11 και $H = \langle h \rangle$ η αντίστοιχη κυκλική υποομάδα τής G. Ισχυριζόμαστε ότι αυτή είναι η μοναδική υποομάδα τής G τάξης 11. Έστω ότι K είναι ακόμα μία υποομάδα τής G με $[K : 1] = 11$. Επειδή ο 11 είναι πρώτος και αφού $K \neq H$, συμπεραίνουμε ότι $H \bigcap K = \{e_G\}$. Επομένως, το πλήθος τού συνόλου $HK = \{hk \mid h \in H, k \in K\} \subseteq G$ ισούται με $HK = \frac{[H:1][K:1]}{[H \bigcap K:1]} = 121$, βλ.

Θεώρημα 1.4.17. Άτοπο. Άρα, η H είναι η μοναδική υποομάδα τής G τάξης 11 και ως εκ τούτου, $H \trianglelefteq G$, βλ. Άσκηση Α71. Επομένως, $\mathcal{N}_G(H) = G$.

Έστω $\mathcal{C}_G(H) = \{g \in G \mid gh' = h'g, \forall h' \in H\}$ ο κεντροποιητής τής H. Προφανώς, $H \leq \mathcal{C}_G(H) \leq G$, διότι η H είναι αβελιανή (αφού είναι κυκλική). Από το Θεώρημα Lagrange, έπεται ή $[\mathcal{C}_G(H) : 1] = 11$ ή $[\mathcal{C}_G(H) : 1] = 77$. Όμως, αν ήταν $[\mathcal{C}_G(H) : 1] = 77$, τότε θα ήταν $\mathcal{C}_G(H) = G$ και τότε θα υπήρχε κάποιο $g \in G$ τάξης 7 με $gh' = h'g, \forall h' \in G$. Αυτό θα ίσχυε ιδιαιτέρως και για τον γεννήτορα h τής H, ο οποίος είναι τάξης 11. Τότε όμως, το gh θα ήταν τάξης $\circ(g) \cdot \circ(h) = 77$, βλ. Άσκηση 63, το οποίο θα οδηγούσε στο συμπέρασμα ότι η G είναι κυκλική, πράγμα που έχουμε εξαρχής υποθέσει ότι δεν ισχύει. Άρα, $\mathcal{C}_G(H) = H$.

Τώρα το (N/C)-Λήμμα μας πληροφορεί ότι η ομάδα $\mathcal{N}_G(H)/\mathcal{C}_G(H) = G/H$ είναι ισόμορφη προς μια υποομάδα τής $\mathrm{Aut}(H)$. Αυτό είναι αδύνατο, διότι $[G/H : 1] = 7$, ενώ $[\mathrm{Aut}(H) : 1] = \varphi(11) = 10$ και $7 \nmid 10$. □

Αργότερα με τη βοήθεια τής Θεωρίας Sylow θα δούμε, βλ. Πρόταση 3.2.2, ότι κάθε ομάδα τάξης pq, όπου p, q είναι πρώτοι αριθμοί με $p < q$ και με $p \nmid p - 1$ είναι κυκλική.

Ασκήσεις στους Ομομορφισμούς Ομάδων

Λυμένες Ασκήσεις

Α 80. Έστω $\chi : G_1 \to G_2$ ένας επιμορφισμός ομάδων, όπου η G_2 είναι μια κυκλική ομάδα τάξης 10. Να δειχθεί ότι η G_1 έχει ορθόθετες υποομάδες με δείκτες 2, 5 και 10.

Λύση. Επειδή ο χ είναι επιμορφισμός, έπεται ότι $\mathrm{im}\,\chi = G_2$ και λόγω τού Πρώτου Θεωρήματος Ισομορφίας, βλ. Θεώρημα 1.7.21, είναι $G_1/\ker\chi \cong G_2$. Αφού λόγω τού προηγούμενου ισομορφισμού, η $G_1/\ker\chi$ είναι κυκλική τάξης 10, συμπεραίνουμε ότι η $G_1/\ker\chi$ διαθέτει ορθόθετες υποομάδες L_1, L_2 και L_3 με δείκτες 2, 5 και 10 αντιστοίχως. Έστω $\pi_{\ker\chi} : G_1 \to G_1/\ker\chi$ η φυσική προβολή. Από το Θεώρημα Αντιστοιχίας, βλ. Θεώρημα 1.6.13, γνωρίζουμε ότι οι $\pi^{-1}_{\ker\chi}(L_i)$ είναι ορθόθετες υποομάδες τής G, που περιέχουν τον $\ker\chi$ και επιπλέον, ότι $\pi^{-1}_{\ker\chi}(L_i)/\ker\chi = L_i$.

Έτσι έχουμε:

$$(G/\ker\chi)/L_i = (G/\ker\chi)/(\pi^{-1}_{\ker\chi}(L_i)/\ker\chi) \cong G/\pi^{-1}_{\ker\chi}(L_i).$$

Οι τάξεις των πηλικοομάδων $(G/\ker\chi)/L_i, i = 1, 2$ και 3 είναι αντιστοίχως 2, 5 και 10. Επομένως, οι τάξεις των πηλικοομάδων $G/\pi^{-1}_{\ker\chi}(L_i), i = 1, 2$ και 3 είναι αντιστοίχως 2, 5 και 10. Άρα, οι δείκτες των $\pi^{-1}_{\ker\chi}(L_i), i = 1, 2$ και 3 είναι αντιστοίχως 2, 5 και 10.

Α 81. Έστω $(G, \star)$ μια ομάδα και $\mathcal{F}_1(G)$ το σύνολο των πηλικοομάδων τής G. Συμβολίζουμε με $\mathcal{F}_{i+1}(G)$, το σύνολο των ομάδων που είναι οι πηλικοομάδες των ομάδων που ανήκουν στο $\mathcal{F}_i(G)$. Έστω ότι η G είναι μια κυκλική ομάδα τάξης p^s, όπου ο p είναι ένας πρώτος αριθμός και ο s είναι ένας πάγιος φυσικός. Να βρεθούν όλες ομάδες τού συνόλου $\bigcup_{i=1}^{\infty} \mathcal{F}_i(G)$ με ακρίβεια ισομορφίας.

Λύση. Από το Τρίτο Θεώρημα Ισομορφίας, βλ. Θεώρημα 1.7.27, γνωρίζουμε ότι οι ομάδες τού $\mathcal{F}_2(G)$ είναι ισόμορφες προς κάποιες από τις ομάδες τού $\mathcal{F}_1(G)$, αφού η πηλικοομάδα μιας πηλικοομάδας τής G είναι ισόμορφη προς μια πηλικοομάδα τής G κ.ο.κ. Κατ' αυτόν τον τρόπο συμπεραίνουμε επαγωγικά ότι για κάθε $i \in \mathbb{N}$, οι πηλικοομάδες τού $\mathcal{F}_i(G)$ είναι ισόμορφες προς κάποιες από τις ομάδες τού $\mathcal{F}_1(G)$. Συνεπώς κάθε ομάδα τού $\bigcup_{i=1}^{\infty} \mathcal{F}_i(G)$ είναι ισόμορφη προς κάποια ομάδα τού $\mathcal{F}_1(G)$.

Έστω ότι η G είναι κυκλική τάξης p^s. Σε κάθε διαιρέτη p^t τού p^s υπάρχει ακριβώς μία υποομάδα $H \leq G$ τάξης p^t και επειδή η G είναι κυκλική (άρα αβελιανή) υπάρχει επίσης η πηλικοομάδα G/H, η οποία είναι κυκλική τάξης p^{s-t}. Επομένως, σε κάθε διαιρέτη t' τού s, υπάρχει μια πηλικοομάδα τάξης $p^{t'}$. Συνεπώς, το $\mathcal{F}_1(G)$ αποτελείται, με ακρίβεια ισομορφίας, από τις κυκλικές ομάδες C_{p^i} τάξης $p^0 = 1, p, p^2, \ldots, p^s$ και κάθε ομάδα τού $\bigcup_{i=1}^{\infty} \mathcal{F}_i(G)$ είναι ισόμορφη προς κάποια από αυτές.

Α 82. Έστω η ομάδα $(\mathbb{Q}^+, \cdot)$ των θετικών ρητών αριθμών με πράξη τον πολλαπλασιασμό ρητών και η ομάδα $(\mathbb{Z}[x], +)$ των πολυωνύμων μιας μεταβλητής που έχουν ακέραιους συντελεστές και πράξη την πρόσθεση πολυωνύμων. Να δειχθεί ότι $\mathbb{Q}^+ \cong \mathbb{Z}[x]$.

Λύση. Θεωρούμε το σύνολο $\mathcal{P} = \{p_i \mid i \in \mathbb{N} \cup \{0\}\}$ των πρώτων αριθμών διατεταγμένο με τη φυσική διάταξη

$$2 = p_0 < 3 = p_1 < 5 = p_2 < 7 = p_3 < \cdots < p_i < \ldots$$

Τότε κάθε θετικός ακέραιος α γράφεται κατά μοναδικό τρόπο ως $\alpha = \prod_{i \geq 0} p_i^{n_i}$, όπου οι $n_i \in \mathbb{N} \cup \{0\}$ και όπου σχεδόν όλοι είναι ίσοι με 0.

Κάθε θετικός ρητός $r = \frac{\alpha}{\beta} \in \mathbb{Q}^+$, όπου οι α, β είναι θετικοί ακέραιοι με ΜΚΔ$(\alpha, \beta) = 1$, γράφεται επίσης κατά μοναδικό τρόπο ως $r = \frac{\alpha}{\beta} = \prod_{i \geq 0} p_i^{n_i}$, όπου οι n_iανήκουν τώρα στους ακεραίους $\mathbb{Z}$ και όπου σχεδόν όλοι τους είναι ίσοι με 0. Προσέξτε ότι οι δυνάμεις με θετικό εκθέτη (αν υπάρχουν) αντιστοιχούν στην πρωτογενή ανάλυση τού α και οι δυνάμεις με αρνητικό εκθέτη (αν υπάρχουν) αντιστοιχούν στην πρωτογενή ανάλυση τού β. Θεωρούμε την απεικόνιση

$$\chi : \mathbb{Q}^+ \to \mathbb{Z}[x], \ \prod_{i \geq 0} p_i^{n_i} \mapsto \quad \chi(\prod_{i \geq 0} p_i^{n_i}) := \sum_{i \geq 0} n_i X^i$$

(Τα παραπάνω γινόμενα και αθροίσματα είναι πεπερασμένα, αφού σχεδόν όλοι οι n_i είναι ίσοι με μηδέν.)

Προφανώς η χ είναι μια αμφιρριπτική («$1-1$» και «επί») απεικόνιση. Επιπλέον, είναι

$$\chi(\prod_{i \geq 0} p_i^{n_i} \cdot \prod_{i \geq 0} p_i^{m_i}) = \chi(\prod_{i \geq 0} p_i^{n_i + m_i}) = \sum_{i \geq 0} (n_i + m_i) X^i =$$
$$\sum_{i \geq 0} n_i X^i + \sum_{i \geq 0} m_i X^i = \chi(\prod_{i \geq 0} p_i^{n_i}) + \chi(\prod_{i \geq 0} p_i^{m_i}).$$

Επομένως, η χ είναι ομομορφισμός και αφού πρόκειται για έναν αμφιρριπτικό ομομορφισμό, συμπεραίνουμε ότι η απεικόνιση χ είναι ένας ισομορφισμός.

Α 83. Έστω $(G, \star)$ μια ομάδα και $g \in G$ ένα πάγιο στοιχείο τής G. Στην Άσκηση ΠΑ15 διαπιστώθηκε ότι το ζεύγος $(G, \circledast)$ είναι επίσης μια ομάδα, όπου $\circledast$ είναι η πράξη $\circledast : G \times G \to G, (a, b) \mapsto a \star g \star b$. Να δειχθεί ότι οι δύο αυτές ομάδες είναι ισόμορφες.

Λύση. Θεωρούμε την απεικόνιση $\chi : G \to G, a \mapsto \chi(a) := a \star g^{-1}$. Προτείνουμε στον αναγνώστη να ελέγξει μόνος ότι η χ είναι αμφιρριπτική («1 − 1» και «επί»). Θα δείξουμε ότι η χ είναι ένας ομομορφισμός και ότι ως εκ τούτου, είναι ισομορφισμός.

$$\forall a, b \in G : \chi(a) \circledast \chi(b) = \chi(a) \star g \star \chi(b) = (a \star g^{-1}) \star g \star (b \star g^{-1}) = a \star b \star g^{-1} = \chi(a \star b).$$

Α 84. Έστω $(G, \star)$ μια ομάδα. Να δειχθούν τα εξής:

(α′) Όταν η απεικόνιση $\chi : G \to G, a \mapsto \chi(g) := g^2$ είναι ομομορφισμός, τότε η G είναι αβελιανή.

(β′) Όταν η απεικόνιση $\chi : G \to G, a \mapsto \chi(g) := g^{-1}$ είναι ομομορφισμός, τότε η G είναι αβελιανή.

(γ′) Όταν $\mathrm{Inn}(G) = \{\mathrm{Id}_G\}$, τότε η G είναι αβελιανή.

Λύση. (α′) Επειδή ο χ είναι ομομορφισμός, για κάθε $g, h \in G$ είναι $\chi(gh) = \chi(g)\chi(h)$. Συνεπώς, $\forall g, h \in G$ είναι $(gh)^2 = g^2h^2$, δηλαδή $ghgh = g^2h^2$. Άρα, $\forall g, h \in G$ είναι $hg = gh$.
(β′) Επειδή ο χ είναι ομομορφισμός, για κάθε $g, h \in G$ είναι $\chi(gh) = \chi(g)\chi(h)$. Συνεπώς, $\forall g, h \in G$ είναι $(gh)^{-1} = g^{-1}h^{-1}$. Άρα, $\forall g, h \in G$ είναι $hg = gh$.
(γ′) Από το Θεώρημα 1.7.43 έχουμε: $G/\mathcal{Z}(G) \cong \mathrm{Inn}(G)$. Αφού η $\mathrm{Inn}(G)$ είναι τετριμμένη, συμπεραίνουμε ότι και η ισόμορφή της πηλικοομάδα $G/\mathcal{Z}(G)$ θα αποτελείται από ακριβώς ένα στοιχείο. Γι' αυτό, όταν $g \in G$, τότε η πλευρική κλάση $g\mathcal{Z}(G) = \mathcal{Z}(G)$ και επομένως το $g \in \mathcal{Z}(G)$. Συνεπώς $G \leq \mathcal{Z}(G)$ και $G = \mathcal{Z}(G)$. Η ομάδα G είναι αβελιανή.

Α 85. Έστω ότι $(G_1, \star)$ είναι μια ομάδα που παράγεται από ένα σύνολο M, βλ. Άσκηση Α30. Έστω ότι $\varphi, \psi : G_1 \to G_2$ είναι δύο ομομορφισμοί με $\varphi(m) = \psi(m), \forall m \in M$. Να δειχθεί ότι $\varphi = \psi$.

Λύση. Αφού $\forall m \in M$ είναι $\varphi(m) = \psi(m)$ και οι φ, ψ είναι ομομορφισμοί, συμπεραίνουμε ότι $\forall m \in M$ είναι $\varphi(m^{-1}) = \psi(m^{-1})$. Συνεπώς, $\varphi(m^{\varepsilon}) = \psi(m^{\varepsilon})$, όπου $\varepsilon \in \{1, -1\}$. Επειδή $G_1 = \langle M \rangle$, κάθε στοιχείο g τής G_1 είναι τής μορφής $g = m_{i_1}^{\varepsilon_1} m_{i_2}^{\varepsilon_2} \ldots m_{i_s}^{\varepsilon_s}, m_{i_j} \in M, \varepsilon_j \in \{1, -1\}, \forall j, 1 \leq j \leq s$ και ως εκ τούτου

$$\varphi(g) = \varphi(m_{i_1}^{\varepsilon_1} m_{i_2}^{\varepsilon_2} \ldots m_{i_s}^{\varepsilon_s}) = \varphi(m_{i_1}^{\varepsilon_1})\varphi(m_{i_2}^{\varepsilon_2}) \ldots \varphi(m_{i_s}^{\varepsilon_s}) =$$
$$\psi(m_{i_1}^{\varepsilon_1})\psi(m_{i_2}^{\varepsilon_2}) \ldots \psi(m_{i_s}^{\varepsilon_s}) = \psi(m_{i_1}^{\varepsilon_1} m_{i_2}^{\varepsilon_2} \ldots m_{i_s}^{\varepsilon_s}) = \psi(g).$$

Α 86. Να προσδιοριστεί η ομάδα αυτομορφισμών $\mathrm{Aut}(V)$ τής ομάδας $(V, \star)$ των τεσσάρων στοιχείων.

Λύση. Υπενθυμίζουμε ότι όταν $V = \{e, a, b, c\}$, όπου e είναι το ουδέτερο στοιχείο της, τότε ο πίνακας πράξης της είναι ο:

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

Παρατηρούμε ότι κάθε αυτομορφισμός χ μετατάσσει τα στοιχεία τού συνόλου $X = \{a, b, c\}$ που είναι ακριβώς τα στοιχεία τάξης 2. Θεωρούμε τον ομομορφισμό $\mathrm{Aut}(V) \to S_3, \chi \to \chi_{|X}$. Προφανώς είναι μονομορφισμός. Άρα, η τάξη $[\mathrm{Aut}(V) : 1]$ είναι διαιρέτης τού 6. Για να δούμε ότι $[\mathrm{Aut}(V) : 1] \geq 4$, είναι επαρκές να κατασκευάσουμε τρεις μη τετριμμένους αυτομορφισμούς. Η V παράγεται από το σύνολο $\{a, b\}$ και οι απεικονίσεις με $\chi_1(a) = a, \chi_1(b) = c$, $\chi_2(a) = c, \chi_2(b) = b$ και $\chi_3(a) = b, \chi_2(b) = a$ είναι αυτομορφισμοί, όπως μπορεί κανείς να διαπιστώσει πολύ εύκολα με τη βοήθεια τού πίνακα πράξης τής V. Άρα, $\mathrm{Aut}(V) \cong S_3$. (Προσέξτε ότι ήδη έχουμε διαπιστώσει, βλ. Παράδειγμα 1.7.44, ότι $\mathrm{Aut}(S_3) \cong S_3$. Επομένως, μη ισόμορφες ομάδες μπορεί να έχουν ισόμορφες ομάδες αυτομορφισμών.)

Α 87. Το ευθύ γινόμενο $(G, \star)$ των πεπερασμένων ομάδων $(G_i, \star_i), i = 1, 2$ είναι κυκλική ομάδα, αν και μόνο αν, οι ομάδες $G_i, i = 1, 2$, είναι κυκλικές και ο μέγιστος κοινός διαιρέτης $\text{ΜΚΔ}([G_1 : 1], [G_2 : 1])$ ισούται με 1.

Λύση. «$\Rightarrow$» Υπενθυμίζουμε ότι όταν η ομάδα $(G, \star)$ είναι κυκλική, τότε και κάθε υποομάδα της είναι επίσης κυκλική. Οι απεικονίσεις

$$\iota_1 : G_1 \to G, g_1 \mapsto \iota_1(g_1) := (g_1, e_{G_2}) \text{ και } \iota_2 : G_2 \to G, g_2 \mapsto \iota_2(g_2) := (e_{G_1}, g_2)$$

αποτελούν μονομορφισμούς ομάδων. Αφού $G_i \cong \operatorname{im} \iota_i \leq G, i = 1, 2$, συμπεραίνουμε ότι η ομάδα $G_i, i = 1, 2$ είναι κυκλική. Επειδή η G είναι κυκλική, υπάρχει ένα στοιχείο της $a = (a_1, a_2)$ τάξης $[G : 1] = [G_1 : 1] \cdot [G_2 : 1]$. Από την Άσκηση 59, γνωρίζουμε ότι $\circ(a) = \text{ΕΚΠ}(\circ(a_1), \circ(a_2))$.
Επομένως, $\text{ΕΚΠ}(\circ(a_1), \circ(a_2)) = [G_1 : 1] \cdot [G_2 : 1], (*)$. Όμως τάξη κάθε στοιχείου $\circ(a_i), i = 1, 2$, είναι διαιρέτης τής αντίστοιχης τάξης $[G_i : 1], i = 1, 2$ και γι' αυτό η τάξη $\circ(a_i), i = 1, 2$ ισούται με $[G_i : 1]/d_i, d_i \in \mathbb{N}, i = 1, 2$.
Έτσι έχουμε:

$$\frac{[G_1 : 1]}{d_1} \cdot \frac{[G_2 : 1]}{d_2} = \circ(a_1) \cdot \circ(a_2) \geq \text{ΕΚΠ}(\circ(a_1), \circ(a_2)) = [G_1 : 1] \cdot [G_2 : 1],$$

από όπου προκύπτει ότι $d_i = 1, i = 1, 2$ και ως εκ τούτου, $\circ(a_i) = [G_i : 1], i = 1, 2$.
Τώρα η $(*)$ γράφεται ως $\text{ΕΚΠ}([G_1 : 1], [G_2 : 1]) = [G_1 : 1][G_2 : 1]$. Επειδή γενικώς για δύο φυσικούς αριθμούς ν_1, ν_2, είναι: $\text{ΕΚΠ}(\nu_1, \nu_2) \cdot \text{ΜΚΔ}(\nu_1, \nu_2) = \nu_1 \cdot \nu_2$ συμπεραίνουμε ότι ο $\text{ΜΚΔ}([G_1 : 1], [G_2 : 1])$ ισούται με 1.
«$\Leftarrow$» Η τάξη τού ευθέως γινομένου $(G, \star)$ ισούται με $[G_1 : 1] \cdot [G_2 : 1]$. Από την υπόθεση

οι ομάδες G_1 και G_2 είναι κυκλικές, δηλαδή για κάθε $i = 1, 2$, υπάρχει $a_i \in G_i$, $i = 1, 2$ με $G_i = \langle a_i \rangle$, $i = 1, 2$. Ιδιαιτέρως για $i = 1, 2$, ισχύει ότι $\circ(a_i) = [G_i : 1]$. Από την Άσκηση 59, γνωρίζουμε ότι η τάξη τού στοιχείου $a := (a_1, a_2) \in G$ ισούται με το ΕΚΠ$(\circ(a_1), \circ(a_2)) =$ ΕΚΠ$([G_1 : 1], [G_2 : 1])$. Αλλά το ΕΚΠ$([G_1 : 1], [G_2 : 1])$ ισούται με $[G_1 : 1] \cdot [G_2 : 1]$, διότι ο ΜΚΔ$([G_1 : 1], [G_2 : 1]) = 1$. Επομένως, $\circ(a) = [G_1 : 1] \cdot [G_2 : 1] = [G : 1]$ και η G είναι μια κυκλική ομάδα.

Α 88. Έστω ότι $(G, \star)$ είναι μια ομάδα ότι H, K είναι δύο ορθόθετες υποομάδες τής G και έστω $H \times K$ το ευθύ γινόμενο των H και K.
Να δειχθούν τα εξής:

(α′) Όταν $H \bigcap K = \{e_G\}$, τότε η ομάδα HK είναι ισόμορφη προς την $H \times K$,

(β′) Όταν η G είναι πεπερασμένη ομάδα και ο ΜΚΔ$([H : 1], [K : 1]) = 1$, τότε $\mathrm{Aut}(HK) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$.

Λύση. (α′) Από την Άσκηση Α73, γνωρίζουμε ότι το σύνολο $HK = \{hk \mid h \in H, k \in K\}$ είναι υποομάδα τής G και επομένως είναι ομάδα.

Όταν $g \in HK$, τότε υπάρχουν $h \in H, k \in K$ με $g = hk$. Ισχυριζόμαστε ότι η παράσταση αυτή τού g είναι μοναδική. Πράγματι, όταν $hk = \overline{h}\overline{k}, h, \overline{h} \in H, k, \overline{k} \in K, (*)$, τότε $k = h^{-1}\overline{h}\overline{k}$ και κατόπιν $\overline{k}^{-1}k = \overline{k}^{-1}(h^{-1}\overline{h})\overline{k}$. Επειδή $H \trianglelefteq G$, συμπεραίνουμε ότι $\overline{k}^{-1}(h^{-1}\overline{h})\overline{k} \in H$, δηλαδή το $\overline{k}^{-1}k \in H \bigcap K$. Αφού $H \bigcap K = \{e_G\}$, έπεται ότι $\overline{k} = k$ και από την $(*)$ ότι επίσης $h = \overline{h}$.

Επιπλέον, $\forall h \in H, k \in K$ είναι $hk = kh$. Πράγματι, το $h^{-1}k^{-1}hk$ ανήκει στην τομή $H \bigcap K = \{e_G\}$, διότι το $h^{-1}k^{-1}h \in K$ και το $k^{-1}hk \in H$, αφού $K \trianglelefteq G$ και $H \trianglelefteq G$. Επομένως, $h^{-1}k^{-1}hk = e_G$, δηλαδή $hk = kh$.

Θεωρούμε την απεικόνιση $\Psi : H \times K \to HK, (h, k) \mapsto \Psi((h, k)) := hk$. Προφανώς η απεικόνιση είναι επιρριπτική.
Ισχυριζόμαστε ότι η Ψ είναι ομομορφισμός. Πράγματι, $\forall (h, k), (\overline{h}, \overline{k}) \in H \times K$ είναι:

$$\Psi((h, k)(\overline{h}, \overline{k})) = \Psi((h\overline{h}, k\overline{k})) = h\overline{h}k\overline{k} = hk\overline{h}\overline{k} = \Psi((h, k))\Psi((\overline{h}, \overline{k})).$$

Τέλος, ο Ψ είναι μονομορφισμός, αφού $(h, k) \in \ker \Psi \Leftrightarrow \Psi((h, k)) = hk = e_G \Leftrightarrow h = k^{-1}$. Αλλά τότε το $h = k^{-1} \in H \bigcap K = \{e_G\}$ και ως εκ τούτου, $h = k = e_G$.
(β′) Παρατηρούμε ότι η τάξη $[H \bigcap K : 1]$ είναι κοινός διαιρέτης των $[H : 1]$ και $[K : 1]$. Όμως, αφού ΜΚΔ$([H : 1], [K : 1]) = 1$, συμπεραίνουμε ότι $[H \bigcap K : 1] = 1$ και ως εκ τούτου, $H \bigcap K = \{e_G\}$. Έτσι από το πρώτο μέρος τής άσκησης γνωρίζουμε ότι $HK \cong H \times K$. Όπως είδαμε, η παράσταση $g = hk$ είναι μοναδική όταν $h \in H$ και $k \in K$. Επομένως, οι αντιστοιχίες $\pi_H : HK \to H, hk \to \pi_H(hk) := h$ και $\pi_K : HK \to K, \pi_K(hk) := k$ είναι καλά ορισμένες απεικονίσεις, οι οποίες μάλιστα είναι επιμορφισμοί. Προφανώς, οι π_H και π_K είναι επιρριπτικές. Θα δείξουμε ότι η π_H είναι ομομορφισμός. Υπενθυμίζουμε ότι από το πρώτο μέρος τής άσκησης γνωρίζουμε ότι $hk - kh, \forall h \in H, k \in K$. Τώρα, $\forall h, \overline{h} \in H, k, \overline{k} \in K$ είναι $\pi_H(hk\overline{h}\overline{k}) = \pi_H(h\overline{h}k\overline{k}) = h\overline{h} = \pi_H(hk)\pi_H(\overline{h}\overline{k})$. Ανάλογα αποδεικνύεται ότι ο π_K είναι ομομορφισμός.

Έστω $\chi \in \mathrm{Aut}(HK)$. Ισχυριζόμαστε ότι η εικόνα τού περιορισμού $\chi_{|H} : H \to HK, h \mapsto \chi_{|H}(h) := \chi(h)$ ισούται με H. Θεωρούμε τη σύνθεση $\pi_H \circ \chi_{|H} : H \to K, h \mapsto \pi_H \circ \chi_{|H}(h) =$

$\pi_H(\chi(h)) = \bar{k}$, όπου $\chi(h) = \overline{hk}$. Παρατηρούμε ότι η τάξη $\circ(\bar{k}) = 1$. Πράγματι, η $\circ(\bar{k})$ είναι διαιρέτης τής $\circ(h)$, διότι ο $\pi_H \circ \chi_{|H}$ είναι ομομορφισμός και επομένως η $\circ(\bar{k})$ είναι επίσης διαιρέτης τής $[H : 1]$. Αλλά, η $\circ(\bar{k})$ είναι επίσης διαιρέτης τής $[K : 1]$. Άρα, $\circ(\bar{k}) = 1$, αφού ο ΜΚΔ$([H : 1], [K : 1]) = 1$. Επομένως, όταν $\chi(h) = \overline{hk}$, τότε $\bar{k} = e_G$ και γι' αυτό im $\chi_{|H} \leq H$. Άρα, ο περιορισμός $\chi_{|H}$ είναι ένας ομομορφισμός από την H στην H, ο οποίος είναι μονομορφισμός, αφού ο χ είναι αυτομορφισμός. Προφανώς, ο $\chi_{|H}$ είναι και επιμορφισμός, αφού η H είναι ένα πεπερασμένο σύνολο. Άρα $\chi_{|H} \in \mathrm{Aut}(H)$. Παρόμοια αποδεικνύεται ότι περιορισμός $\chi_{|K} \in \mathrm{Aut}(K)$ είναι ένας αυτομορφισμός τής K.

Επομένως η αντιστοιχία:

$$\Phi : \mathrm{Aut}(HK) \to \mathrm{Aut}(H) \times \mathrm{Aut}(K), \chi \mapsto \Phi(\chi) := (\chi_{|H}, \chi_{|K})$$

είναι μια καλά ορισμένη απεικόνιση. Προτείνουμε να αποδείξει μόνος του αναγνώστης ότι η Φ είναι ένας μονομορφισμός.

Θα δείξουμε ότι ο Φ είναι επιμορφισμός. Έστω $(\varphi, \psi) \in \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. Θεωρούμε την αντιστοιχία $\chi : HK \to HK, \chi(hk) := \varphi(h)\psi(k)$. Ήδη γνωρίζουμε ότι η χ είναι μια καλά ορισμένη απεικόνιση, αφού από $hk = \overline{hk}, h, \bar{h} \in H, k, \bar{k} \in K$, έπεται $h = \bar{h}, k = \bar{k}$. Η χ είναι ομομορφισμός, διότι

$$\begin{aligned}
&\forall h, \bar{h} \in H, k, \bar{k} \in K : \\
&\chi((hk)(\overline{hk})) = \chi((h\bar{h})(k\bar{k})) = \varphi(h\bar{h})\psi(k\bar{k}) = \varphi(h)\varphi(\bar{h})\psi(k)\psi(\bar{k}) = \\
&\varphi(h)\psi(k)\varphi(\bar{h})\psi(\bar{k}) = \chi(hk)\chi(\overline{hk}).
\end{aligned}$$

Ο χ είναι μονομορφισμός, διότι $hk \in \ker \chi \Leftrightarrow \varphi(h)\psi(k) = e_G \Leftrightarrow \varphi(h) = \psi(k^{-1})$. Αφού το $\varphi(h) \in H$ και το $\psi(k^{-1}) \in K$, έπεται $\varphi(h) = e_G$ και $\psi(k^{-1}) = e_G \in K$. Επειδή οι φ, ψ είναι αυτομορφισμοί, συμπεραίνουμε $h = e_G, k = e_G$. Αφού το HK είναι πεπερασμένο σύνολο , έπεται ότι ο χ είναι επίσης επιμορφισμός και τελικά ότι $\chi \in \mathrm{Aut}(HK)$.

Είναι εύκολη η διαπίστωση ότι $\chi_{|H} = \varphi$ ότι $\chi_{|K} = \psi$ και κατόπιν ότι $\Phi(\chi) = (\varphi, \psi)$. Συνεπώς, ο Φ είναι επιμορφισμός και επομένως ο Φ είναι ισομορφισμός.

Α 89. Έστω $(G, \star)$ μια ομάδα με τετριμμένο κέντρο $\mathcal{Z}(G) = \{e_G\}$. Να δειχθεί ότι το κέντρο τής ομάδας των αυτομορφισμών $\mathrm{Aut}(G)$ τής G είναι επίσης τετριμμένο, δηλαδή $\mathcal{Z}(\mathrm{Aut}(G)) = \{\mathrm{Id}_G\}$.

Λύση. Θα δείξουμε ότι αν $\tau \in \mathcal{Z}(\mathrm{Aut}(G))$, τότε $\forall g \in G$ είναι $\tau(g) = g$ και ως εκ τούτου, τότε ο αυτομορφισμός τ θα ισούται με τον ταυτοτικό αυτομορφισμό Id_G.

Για $g \in G$, θεωρούμε τον εσωτερικό αυτομορφισμό $\chi_g \in \mathrm{Inn}(G)$. Αφού $\tau \in \mathcal{Z}(\mathrm{Aut}(G))$, έχουμε $\tau \circ \chi_g = \chi_g \circ \tau$. Συνεπώς, $\forall h \in G$ είναι

$$\tau \circ \chi_g(h) = \chi_g \circ \tau(h) \Leftrightarrow \tau(ghg^{-1}) = g\tau(h)g^{-1} \Leftrightarrow \tau(g)\tau(h)\tau(g)^{-1} = g\tau(h)g^{-1}.$$

Αφού, ο τ είναι αυτομορφισμός, η τελευταία ισότητα ισχύει για κάθε $\alpha \in G$, αφού πάντοτε υπάρχει κάποιο $h \in G$ με $\alpha = \tau(h)$. Επομένως $\forall \alpha \in G$, είναι $\tau(g)\alpha\tau(g)^{-1} = g\alpha g^{-1}$ ή ισοδύναμα $\alpha(\tau(g)^{-1}g) = (\tau(g)^{-1}g)\alpha$. Συνεπώς, το $\tau(g)^{-1}g$ ανήκει στο τετριμμένο κέντρο $\mathcal{Z}(G) = \{e_G\}$ και γι' αυτό $g = \tau(g)$. Έτσι συμπεραίνουμε ότι $\tau = \mathrm{Id}_G$.

Α 90. Να δειχθούν τα εξής:

(α′) Κάθε ομάδα τάξης 4 είναι ισόμορφη ή προς την $(\mathbb{Z}_4, +)$ ή προς το ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_2$ τής $(\mathbb{Z}_2, +)$ με τον εαυτό της.

(β′) Κάθε ομάδα τάξης 6 είναι ισόμορφη ή προς τη συμμετρική ομάδα $(S_3, \circ)$ ή προς το ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_3$ τής $(\mathbb{Z}_2, +)$ με τη $(\mathbb{Z}_3, +)$.

Λύση. (α′) Έστω $(G, \star)$ με $[G : 1] = 4$. Από το Θεώρημα Lagrange γνωρίζουμε ότι οι πιθανές τάξεις ενός στοιχείου $a \in G, a \neq e_G$ είναι ή 2 ή 4.

Αν η G διαθέτει ένα στοιχείο a τάξης 4, τότε $\langle a \rangle = G$. Κάθε κυκλική ομάδα τάξης 4 είναι ισόμορφη προς την $(\mathbb{Z}_4, +)$.

Αν η G δεν διαθέτει κάποιο στοιχείο τάξης 4, τότε κάθε στοιχείο της $\neq e_G$ έχει τάξη 2. Ως γνωστόν, όταν σε μια ομάδα κάθε στοιχείο $\neq e_G$ έχει τάξη 2, τότε η G είναι αβελιανή, βλ. Άσκηση Α16. Έστω $a, b \in G$ με $a \neq e_G$, $b \neq e_G$ και $a \neq b$. Θεωρούμε τις κυκλικές υποομάδες $H = \langle a \rangle$ και $K = \langle b \rangle$. Προφανώς, $H \bigcap K = \{e_G\}$ και αφού πρόκειται για κυκλικές ομάδες τάξης 2 έχουμε $H \cong \mathbb{Z}_2$ και $K \cong \mathbb{Z}_2$. Επιπλέον, επειδή η G είναι αβελιανή οι H, K είναι ορθόθετες υποομάδες τής G. Επομένως, η HK ισούται με τη G, αφού είναι μια υποομάδα τάξης $[H : 1][K : 1] = 4$ και από την Άσκηση Α88, έχουμε $G = HK \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

(β′) Έστω $(G, \star)$ με $[G : 1] = 6$. Διακρίνουμε δύο περιπτώσεις:

Πρώτη Περίπτωση Η G είναι αβελιανή. Από το Θεώρημα 1.6.15, γνωρίζουμε ότι η G διαθέτει μια κυκλική υποομάδα H τάξης 2 και μια κυκλική υποομάδα K τάξης 3, διότι οι 2 και 3 είναι πρώτοι διαιρέτες τού 6. Αφού $H \bigcap K = \{e_G\}$ και αφού $H \trianglelefteq G, K \trianglelefteq G$, συμπεραίνουμε (όπως και στο πρώτο μέρος τής άσκησης) ότι $G = HK \cong H \times K \cong \mathbb{Z}_2 \times \mathbb{Z}_3$. (Σημειώστε ότι $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ *(γιατί;)*.)

Δεύτερη Περίπτωση Η G δεν είναι αβελιανή. Οι πιθανές τάξεις των στοιχείων $a \neq e_G$ τής G είναι ή 2 ή 3 ή 6. Αν όμως η G είχε στοιχείο τάξης 6, τότε θα ήταν κυκλική, άρα και αβελιανή, που είναι άτοπο. Επίσης, δεν μπορεί κάθε $a \in G, a \neq e_G$ να είναι τάξης 2, αφού τότε θα ήταν και πάλι αβελιανή, που είναι άτοπο. Άρα, η G διαθέτει ένα στοιχείο a με $\circ(a) = 3$. Θεωρούμε την κυκλική υποομάδα $H = \langle a \rangle = \{e_G, a, a^2\}$. Ο δείκτης $[G : H]$ ισούται με 2 και γι' αυτό σύμφωνα με την Άσκηση Α70, η H είναι ορθόθετη υποομάδα τής G. Έστω $b \in G \setminus H$. Παρατηρούμε ότι η τάξη τού b ισούται με 2. Πράγματι, αν $\circ(b) = 3$, τότε η κυκλική υποομάδα $K = \langle b \rangle$ θα ήταν τάξης 3 και τότε το σύνολο[37] HK θα είχε 9 στοιχεία, αφού $H \bigcap K = \{e_G\}$. Αφού $[G : H] = 2$, έχουμε $G = H \bigcup bH = \{e_G, a, a^2\} \bigcup \{b, ba, ba^2\}$, όπου $H \bigcap bH = \emptyset$ και επιπλέον, $\{b, ba, ba^2\} = bH = Hb = \{b, ab, a^2b\}$, διότι $H \trianglelefteq G$. Παρατηρούμε ότι δεν μπορεί να ισχύει $ba = ab$, διότι τότε ένας απλός υπολογισμός[38] δείχνει ότι η G θα ήταν αβελιανή. Γι' αυτό $ba = a^2b$ και $ba^2 = ab$. Γνωρίζοντας τις σχέσεις $a^3 = e_G$, $b^2 = e_G$, $ba = a^2b$ και $ba^2 = ab$, μπορεί κανείς να συμπληρώσει τον επόμενο πίνακα πράξης τής G. Για παράδειγμα $b(ab) = (ba)b = (a^2b)b = a^2b^2 = a^2$,

[37] Στην πραγματικότητα το HK είναι υποομάδα, αφού $H \trianglelefteq G$.

[38] Λίγο πιο θεωρητικά: Το b θα ανήκε στο κέντρο $\mathcal{Z}(G)$ τής G. Άρα, $[\mathcal{Z}(G) : 1] = 2$ ή 3 ή 6. Όμως, $[\mathcal{Z}(G) : 1] = 6$ δίνει $G = \mathcal{Z}(G)$ και κατόπιν ότι η G είναι αβελιανή. Άτοπο! Ενώ $[\mathcal{Z}(G) : 1] = 2$ ή 3 δίνει ότι η πηλικοομάδα $G/\mathcal{Z}(G)$ είναι αντιστοίχως τάξης 3 ή 2. Λόγω τής Άσκησης Α78, συμπεραίνουμε και πάλι ότι η G είναι αβελιανή. Άτοπο!

$b(a^2b) = (ba^2)b = (ab)b = a$, $(ab)(ab) = a(ba)b = a(a^2b)b = e_G$, $(ab)(a^2b) = a(ba^2)b = a(ab)b = a^2$, $(ab)a = a(ba) = a(a^2b) = b$, $(ab)a^2 = a(ba^2) = a(ab) = a^2b$, $(a^2b)(ab) = a^2(ba)b = a^2(a^2b)b = a$, $(a^2b)(a^2b) = a^2(ba^2)b = a^2(ab)b = e_G$, $(a^2b)a = a^2(ba) = a^2(a^2b) = ab$ και $(a^2b)a^2 = a^2(ba^2) = a^2(ab) = b$.

$\cdot$	e_G	b	ab	a^2b	a	a^2
e_G	e_G	b	ab	a^2b	a	a^2
b	b	e_G	a^2	a	a^2b	ab
ab	ab	a	e_G	a^2	b	a^2b
a^2b	a^2b	a^2	a	e_G	ab	b
a	a	ab	a^2b	b	a^2	e_G
a^2	a^2	a^2b	b	ab	e_G	a

Υπενθυμίζουμε ότι ο πίνακας πράξης τής S_3, βλ. σελ. 34, είναι ο εξής:

$\circ$	Id_3	τ_1	τ_2	τ_3	ρ	σ
Id_3	Id_3	τ_1	τ_2	τ_3	ρ	σ
τ_1	τ_1	Id_3	ρ	σ	τ_2	τ_3
τ_2	τ_2	σ	Id_3	ρ	τ_3	τ_1
τ_3	τ_3	ρ	σ	Id_3	τ_1	τ_2
ρ	ρ	τ_3	τ_1	τ_2	σ	Id_3
σ	σ	τ_2	τ_3	τ_1	Id_3	ρ

Η συνολοθεωρητική απεικόνιση $\chi : G \to S_3$ με $\chi(e_G) = \mathrm{Id}_3$, $\chi(b) = \tau_1$, $\chi(ab) = \tau_2$, $\chi(a^2b) = \tau_3$, $\chi(a) = \rho$ και $\chi(a^2) = \sigma$ είναι ένας ισομορφισμός ομάδων, όπως εύκολα μπορεί να διαπιστωθεί από τους πίνακες πράξης των δύο ομάδων. Άρα, $G \cong S_3$.

Α 91. Έστω φ η φ–συνάρτηση Euler και m, n δύο σχετικώς πρώτοι φυσικοί αριθμοί. Να δειχθεί ότι $\varphi(mn) = \varphi(m)\varphi(n)$. (*Η γνωστή, από τη Θεωρία Αριθμών, ιδιότητα τής φ-συνάρτησης Euler ότι είναι μια πολλαπλασιαστική συνάρτηση.*)

Λύση. Έστω ότι $(G, \star)$ είναι μια κυκλική ομάδα τάξης mn και ότι H και K είναι οι (μοναδικές) υποομάδες τής G με τάξεις m και n αντιστοίχως. Η υποομάδα HK τής G ισούται με G, αφού το πλήθος $|HK| = [HK : 1]$ των στοιχείων τού συνόλου HK είναι ίσο με $|HK| = \frac{[H:1][K:1]}{[H\bigcap K:1]} = mn$, βλ. Θεώρημα 1.4.17. Από την Άσκηση Α88, γνωρίζουμε ότι $\mathrm{Aut}(HK) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. Συνεπώς, $\mathrm{Aut}(G) \cong \mathrm{Aut}(H) \times \mathrm{Aut}(K)$. Από το Θεώρημα 1.7.37, γνωρίζουμε ότι $\mathrm{Aut}(G) \cong \mathbb{U}_{mn}$, $\mathrm{Aut}(H) \cong \mathbb{U}_m$ και $\mathrm{Aut}(K) \cong \mathbb{U}_n$, όπου $\mathbb{U}_k$ είναι η ομάδα των αντιστρέψιμων στοιχείων τού $\mathbb{Z}_k$, η οποία έχει τάξη $[\mathbb{U}_k : 1] = \varphi(k)$. Επομένως, $\mathbb{U}_{mn} \cong \mathbb{U}_m \times \mathbb{U}_n$ και $\varphi(mn) = \varphi(m)\varphi(n)$.

Προσεξτε ότι το συμπέρασμα τής άσκησης γενικεύεται άμεσα ως εξής:
Έστω $n = p_1^{i_1}p_2^{i_2}\dots p_s^{i_s}$ η πρωτογενής ανάλυση τού φυσικού n σε δυνάμεις διαφορετικών πρώτων αριθμών. Τότε

$$\mathbb{U}_n \cong \mathbb{U}_{p_1^{i_1}} \times \mathbb{U}_{p_2^{i_2}} \times \cdots \times \mathbb{U}_{p_s^{i_s}} \text{ και } \varphi(n) = \varphi(p_1^{i_1})\varphi(p_2^{i_2})\dots\varphi(p_s^{i_s}).$$

Α 92. Να εξεταστεί, αν είναι ισόμορφες οι $(\mathbb{U}_{20}, \cdot)$ και $(\mathbb{U}_{24}, \cdot)$

Λύση. Παρατηρούμε ότι $\varphi(20) = \varphi(2^2 \cdot 5) = \varphi(2^2)\varphi(5) = 2 \cdot 4 = 8$ και $\varphi(24) = \varphi(2^3) \cdot \varphi(3) = 4 \cdot 2$. Από την απόδειξη τής αμέσως προηγούμενης άσκησης, γνωρίζουμε ότι $\mathbb{U}_{20} \cong \mathbb{U}_{2^2} \times \mathbb{U}_5$ και ότι $\mathbb{U}_{24} \cong \mathbb{U}_{2^3} \times \mathbb{U}_3$. Η $\mathbb{U}_{2^2}$ είναι κυκλική τάξης 2, συνεπώς $\mathbb{U}_{2^2} \cong \mathbb{Z}_2$. Η $\mathbb{U}_5$ είναι κυκλική τάξης 4, συνεπώς $\mathbb{U}_5 \cong \mathbb{Z}_4$. Η $\mathbb{U}_{2^3}$ δεν είναι κυκλική, σύμφωνα με την Άσκηση Α64, αλλά είναι τάξης 4. Από την Άσκηση Α90, συμπεραίνουμε ότι $\mathbb{U}_{2^3} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Τέλος, η $\mathbb{U}_3$ είναι κυκλική τάξης 2, συνεπώς $\mathbb{U}_3 \cong \mathbb{Z}_2$. Άρα, $\mathbb{U}_{20} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ και $\mathbb{U}_{24} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Επομένως, η $\mathbb{U}_{20}$ έχει ένα στοιχείο τάξης 4 (*γιατί;*), ενώ κάθε στοιχείο τής $\mathbb{U}_{24}$ είναι τάξης 1 ή 2. Οι ομάδες $\mathbb{U}_{20}$ και $\mathbb{U}_{24}$ δεν είναι ισόμορφες.

Α 93. Έστω ότι $(G, \star)$ είναι μια ομάδα και $H \leq G$ μια υποομάδα τάξης 2. Να δειχθεί ότι ο κεντροποιητής $\mathcal{C}_G(H)$ τής H συμπίπτει με τον ορθοθετοποιητή $\mathcal{N}_G(H)$ τής H. Αν επιπλέον, $\mathcal{N}_G(H) = G$, τότε η H περιέχεται στο κέντρο $\mathcal{Z}(G)$ τής G.

Λύση. Από το (N/C)-Λήμμα, βλ. Θεώρημα 1.7.43, γνωρίζουμε ότι η πηλικοομάδα $\mathcal{N}_G(H)/\mathcal{C}_G(H)$ είναι ισόμορφη προς μια υποομάδα τής $\mathrm{Aut}(H)$. Αφού η H έχει μόνο δύο στοιχεία, η $\mathrm{Aut}(H)$ ισούται με την τετριμμένη ομάδα $\{\mathrm{Id}_H\}$ και ως εκ τούτου, $\mathcal{N}_G(H) = \mathcal{C}_G(H)$.

Τέλος, αν $\mathcal{N}_G(H) = G$, τότε $\mathcal{C}_G(H) = G$ και συνεπώς $H \leq \mathcal{Z}(G)$.

Α 94. Για οποιουσδήποτε δύο σχετικώς πρώτους αριθμούς $m, n \in \mathbb{N}$, η ομάδα $(\mathbb{U}_{mn}, \cdot)$ είναι ισόμορφη προς το (εξωτερικό) ευθύ γινόμενο $\mathbb{U}_m \times \mathbb{U}_n$ των ομάδων $(\mathbb{U}_m, \cdot)$ και $(\mathbb{U}_n, \cdot)$.

Λύση. Θεωρούμε την αντιστοιχία

$$\chi : \mathbb{U}_{mn} \to \mathbb{U}_m \times \mathbb{U}_n, [a]_{mn} \mapsto \chi([a]_{mn}) := ([a]_m, [a]_n).$$

Προφανώς, η χ είναι μια καλά ορισμένη απεικόνιση. Επίσης είναι εύκολη η διαπίστωση ότι η χ είναι ένας ομομορφισμός. Παρατηρούμε ότι

$$[a]_{mn} = [b]_{mn} \Leftrightarrow mn/a - b \Leftrightarrow m/a - b \text{ και } n/a - b \Leftrightarrow [a]_m = [b]_m \text{ και } [a]_n = [b]_n,$$

διότι οι m, n είναι σχετικώς πρώτοι αριθμοί. Ως εκ τούτου, $\chi([a]_{mn}) = \chi([b]_{mn})$ αν και μόνο αν, $[a]_{mn} = [b]_{mn}$. Επομένως, ο χ είναι ένας μονομορφισμός. Ισχυριζόμαστε ότι ο χ είναι ένας ισομορφισμός.

Πράγματι, επειδή ο $\text{ΜΚΔ}(m, n) = 1$ έχουμε:

$$[\mathbb{U}_{mn} : 1] = \varphi(mn) = \varphi(m) \cdot \varphi(n) = [\mathbb{U}_m : 1] \cdot [\mathbb{U}_n : 1],$$

όπου φ είναι η φ-συνάρτηση Euler, βλ. Άσκηση[39] Α91. Άρα, $[\mathbb{U}_{mn} : 1] = [\mathbb{U}_m \times \mathbb{U}_m : 1]$ και γι' αυτό ο μονομορφισμός χ είναι επίσης επιμορφισμός. Ως εκ τούτου, ο χ είναι ισομορφισμός.

Α 95. Η ομάδα $(\mathbb{U}_n, \cdot)$ είναι κυκλική, αν και μόνο αν, ο n ισούται με $1, 2, 4, p^k$ ή $2p^k$, όπου ο p είναι ένας περιττός πρώτος και ο $k \geq 1$.

[39] Ουσιαστικά στην Άσκηση Α91 έχουμε αποδείξει και τον ισχυρισμό τής παρούσας άσκησης.

Λύση. «$\Leftarrow$» Όταν $n = 1, 2, 4$, τότε οι ομάδες $\mathbb{U}_n$ είναι κυκλικές, αφού η τάξη τους είναι αντίστοιχα $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(4) = 2$. Για κάθε περιττό πρώτο αριθμό p, η $\mathbb{U}_{p^k}, k \geq 1$ είναι κυκλική, βλ. Άσκηση Α65. Τέλος, η $\mathbb{U}_{2p^k}, k \geq 1$ είναι ισόμορφη προς την $\mathbb{U}_2 \times \mathbb{U}_{p^k}$, βλ. Άσκηση Α94. Επειδή $\mathbb{U}_2 \times \mathbb{U}_{p^k} \cong \mathbb{U}_{p^k}$, διότι η $\mathbb{U}_2$ είναι τετριμμένη, συμπεραίνουμε ότι η $\mathbb{U}_{2p^k}, k \geq 1$ είναι κυκλική.
«$\Rightarrow$» Κάθε φυσικός αριθμός n, γράφεται ως $n = 2^\lambda m$ με $\lambda \in \mathbb{N} \cup \{0\}$, όπου ο m είναι ένας περιττός αριθμός. Επειδή ο ΜΚΔ$(2^\lambda, m) = 1$, η $\mathbb{U}_{2^\lambda m}$ είναι ισόμορφη προς την $\mathbb{U}_{2^\lambda} \times \mathbb{U}_m$. Αφού η $\mathbb{U}_{2^\lambda m}$ είναι κυκλική, συμπεραίνουμε ότι οι $\mathbb{U}_{2^\lambda}$ και $\mathbb{U}_m$ οφείλουν να είναι επίσης κυκλικές.

Για να είναι η $\mathbb{U}_{2^\lambda}$ κυκλική, πρέπει το λ να είναι ≤ 2, διότι από την Άσκηση Α64 γνωρίζουμε ότι για κάθε $\lambda \geq 3$, η $\mathbb{U}_{2^\lambda}$ δεν είναι κυκλική. Για $\lambda = 0, 1, 2$, οι αντίστοιχες ομάδες $\mathbb{U}_1$, $\mathbb{U}_2$ και $\mathbb{U}_4$ είναι προφανώς κυκλικές.
Ισχυριζόμαστε ότι η ομάδα $\mathbb{U}_m$, όπου ο m είναι περιττός, είναι κυκλική, αν και μόνο αν, είτε ο $m = 1$ είτε ο m είναι τής μορφής $m = p^k$, όπου ο p είναι περιττός πρώτος και ο k είναι φυσικός. Προφανώς, όταν ο $m = 1$, η $\mathbb{U}_1$ είναι κυκλική. Επίσης από την Άσκηση Α65, γνωρίζουμε ότι η $\mathbb{U}_m$ είναι κυκλική όταν ο $m = p^k$, όπου ο p περιττός πρώτος και ο k φυσικός.

Ας δούμε τι συμβαίνει όταν ο m διαθέτει δύο διαφορετικούς περιττούς πρώτους διαιρέτες. Στην περίπτωση αυτή ο m μπορεί να εκφραστεί ως $m = st$ όπου οι s, t είναι περιττοί αριθμοί ≥ 3 με ΜΚΔ$(s, t) = 1$. Τότε, σύμφωνα με την Άσκηση Α94, η $\mathbb{U}_m$ είναι ισόμορφη προς το (εξωτερικό) ευθύ γινόμενο $\mathbb{U}_s \times \mathbb{U}_t$. Παρατηρώντας ότι ο 2 είναι διαιρέτης των $\varphi(s) = [\mathbb{U}_s : 1]$ και $\varphi(t) = [\mathbb{U}_t : 1]$, διότι οι $\varphi(s)$ και $\varphi(t)$ είναι άρτιοι αριθμοί, αφού $s, t \geq 3$, βλ. Άσκηση Α51, συμπεραίνουμε ότι ο ΜΚΔ$([\mathbb{U}_s : 1], [\mathbb{U}_t : 1]) \neq 1$. Αν ήταν η $\mathbb{U}_m$ κυκλική ομάδα, τότε και το ευθύ γινόμενο $\mathbb{U}_s \times \mathbb{U}_t \cong \mathbb{U}_m$ θα ήταν μια κυκλική ομάδα και τότε, λόγω τής Άσκησης Α87, οι τάξεις $\varphi(s) = [\mathbb{U}_s : 1]$ και $\varphi(t) = [\mathbb{U}_t : 1]$ θα ήταν σχετικώς πρώτοι αριθμοί. Αυτό όμως δεν συμβαίνει.

Άρα, όταν η $\mathbb{U}_n$ είναι κυκλική ομάδα με $n = 2^\lambda m$ όπως πιο πάνω, τότε ο $\lambda = 0, 1$ και ο $m = p^k$, όπου ο p είναι περιττός πρώτος και ο k είναι φυσικός.

Προτεινόμενες Ασκήσεις

ΠΑ 78. Να δειχθούν τα εξής:

(α′) Η $(\mathbb{U}_8, \cdot)$ είναι ισόμορφη προς την $(\mathbb{U}_{12}, \cdot)$

(β′) Η $(\mathbb{U}_8, \cdot)$ δεν είναι ισόμορφη προς την $(\mathbb{U}_{10}, \cdot)$

ΠΑ 79. Έστω $(\mathbb{Q}^\star, \cdot)$ η ομάδα των μη μηδενικών ρητών αριθμών με πράξη τον πολλαπλασιασμό ρητών. Να δειχθεί ότι η απεικόνιση $\chi : \mathbb{Q}^\star \to \mathbb{Q}^\star, \alpha \mapsto \chi(a) := |\alpha|$, όπου $|\alpha|$ είναι η απόλυτη τιμή τού α, είναι ένας ομομορφισμός και να υπολογιστούν ο πυρήνας $\ker \chi$ και η εικόνα $\operatorname{im} \chi$ τού χ.

ΠΑ 80. Έστω ότι $(G_1, \star_1)$ είναι μια κυκλική ομάδα τάξης 12 και ότι $(G_2, \star_2)$ είναι μια κυκλική ομάδα τάξης 4. Να ευρεθούν όλοι οι ομομορφισμοί $\chi : G_1 \to G_2$.

ΠΑ 81. Έστω $(D_4, \circ)$ η διεδρική ομάδα $D_4 = \{\mathrm{Id}_4, \tau, \rho, \rho^2, \rho^3, \tau \circ \rho, \tau \circ \rho^2, \tau \circ \rho^3\}$ και $(\mathbb{Z}_2), +$ η ομάδα των ακεραίων κατά μόδιο (μέτρο 2). Να δειχθεί ότι η απεικόνιση

$\chi : D_4 \to \mathbb{Z}_2$ με $\chi(\rho^i) = [0]_2$ και $\chi(\tau \circ \rho^i) = [1]_2$ είναι ένας επιμορφισμός ομάδων και να υπολογιστεί ο $\ker \chi$.

ΠΑ 82. Έστω $(D_n, \circ), n \geq 3$ η διεδρική ομάδα τάξης $2n$, βλ. Άσκηση Α25.
Να δειχθούν τα εξής:

(α′) Όταν $n = 2^k m$, όπου ο $k \in \mathbb{N} \cup \{0\}$ και ο m είναι ένας περιττός πρώτος αριθμός > 1, τότε για κάθε $i, 0 \leq i \leq k$, η πηλικοομάδα $D_n/\langle \rho^{2^i m} \rangle$ είναι ισόμορφη προς τη διεδρική ομάδα $D_{2^i m}$.

(β′) Όταν $n = 2^k$, όπου ο $k \in \mathbb{N}, k \geq 3$, τότε για κάθε $i, 2 \leq i \leq k$, η πηλικοομάδα $D_n/\langle \rho^{2^i} \rangle$ είναι ισόμορφη προς τη διεδρική ομάδα D_{2^i}. Η πηλικοομάδα $D_n/\langle \rho^2 \rangle$ είναι ισόμορφη προς το ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_2$ τής $(\mathbb{Z}_2, +)$ με τον εαυτό της και η πηλικοομάδα $D_n/\langle \rho \rangle$ είναι ισόμορφη προς την $(\mathbb{Z}_2, +)$.

(γ′) Όταν $n = 2^2$, τότε η πηλικοομάδα $D_4/\langle \rho^2 \rangle$ είναι ισόμορφη προς τον ευθύ γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_2$ τής $(\mathbb{Z}_2, +)$ με τον εαυτό της και η πηλικοομάδα $D_4/\langle \rho \rangle$ είναι ισόμορφη προς την $(\mathbb{Z}_2, +)$.

ΠΑ 83. Έστω ότι $\varphi : G_1 \to G_2$ είναι ένας ομομορφισμός ομάδων και ότι $H \leq G_1$ είναι μια υποομάδα τής G_1. Θεωρούμε τον περιορισμό $\varphi_H : H \to G_2, h \mapsto \varphi_H(h) := \varphi(h)$ τού φ στην H. Να δειχθεί ότι ο φ_H είναι ένας ομομορφισμός.

ΠΑ 84. Έστω ότι $\varphi : G_1 \to G_2$ είναι ένας ομομορφισμός ομάδων, ότι $M \subseteq G_1$ είναι ένα υποσύνολο τής G_1 και ότι $\langle M \rangle$ είναι η υποομάδα τής G_1 που παράγεται από το M. Να δειχθεί ότι η εικόνα της $\varphi(\langle M \rangle)$ ισούται με $\langle \varphi(M) \rangle$, δηλαδή με την υποομάδα τής G_2, η οποία παράγεται από το σύνολο $\varphi(M) = \{\varphi(m) \mid m \in M\}$ των εικόνων τού M.

ΠΑ 85. Έστω ότι $\varphi : G_1 \to G_2$ είναι ένας ομομορφισμός ομάδων και ότι η G_2 είναι αβελιανή. Να δειχθεί ότι $\forall x, y \in G_1$ είναι $\varphi(xyx^{-1}) = \varphi(y)$.

ΠΑ 86. Έστω ότι $\varphi : G_1 \to G_2$ είναι ένας επιμορφισμός ομάδων και ότι η G_1 είναι αβελιανή. Να δειχθεί ότι η G_2 είναι επίσης αβελιανή.

ΠΑ 87. Έστω ότι G και G' είναι δύο κυκλικές ομάδες με τάξεις m και n αντίστοιχα. Να δειχθεί ότι υπάρχει κάποιος επιμορφισμός $\chi : G \to G'$, αν και μόνο αν, η τάξη $[G' : 1] = n$ είναι διαιρέτης τής τάξης $[G : 1] = m$. Στην περίπτωση αυτή, να δειχθεί ότι το πλήθος των διαφορετικών επιμορφισμών ισούται με την τιμή $\varphi(n)$ τής φ–συνάρτησης Euler και ότι το πλήθος όλων των ομομορφισμών από τη G στη G' ισούται με n.

ΠΑ 88. Έστω ότι $(G_i, \star_i), i = 1, 2$ είναι δύο ομάδες και $G_1 \times G_2$ το ευθύ γινόμενό τους. Θεωρούμε τις απεικονίσεις:

$$\begin{aligned}
&\iota_1 : G_1 \to G_1 \times G_2, g \mapsto \iota_1(g) := (g, e_{G_2}),\\
&\iota_2 : G_2 \to G_1 \times G_2, g' \mapsto \iota_2(g') := (e_{G_1}, g')\\
&\pi_1 : G_1 \times G_2 \to G_1, (g, g') \mapsto \pi_1((g, g')) := g,\\
&\pi_2 : G_1 \times G_2 \to G_2, (g, g') \mapsto \pi_2((g, g')) := g'
\end{aligned}$$

Να δειχθούν τα εξής:

(α′) Οι $\iota_i, i = 1, 2$ είναι μονομορφισμοί και οι $\pi_i, i = 1, 2$ είναι επιμορφισμοί.

(β′) $G_1 \times G_2 / \ker \pi_i \cong G_i, i = 1, 2$.

(γ′) Η σύνθεση $\pi_1 \circ \iota_1$, αντιστοίχως $\pi_2 \circ \iota_2$, είναι ο ταυτοτικός αυτομορφισμός τής G_1, αντιστοίχως τής G_2.

(δ′) Η σύνθεση $\pi_2 \circ \iota_1$, αντιστοίχως $\pi_1 \circ \iota_2$, είναι ο τετριμμένος ομομορφισμός $G_1 \to G_2, g \mapsto e_{G_2}$, αντιστοίχως ο τετριμμένος ομομορφισμός $G_2 \to G_1, g' \mapsto e_{G_1}$.

ΠΑ 89. Έστω ότι $(G_i, \star_i)$, $i = 1, 2$ είναι δύο ομάδες και ότι $K_i \trianglelefteq G_i, i = 1, 2$ είναι αντιστοίχως ορθόθετες υποομάδες των $G_i, i = 1, 2$. Να δειχθεί ότι η $K_1 \times K_2$ είναι ορθόθετη υποομάδα τού ευθέος γινομένου $G_1 \times G_2$ και ότι $(G_1 \times G_2)/(K_1 \times K_2) \cong (G_1/K_1) \times (G_2/K_2)$.

ΠΑ 90. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι $H, K \trianglelefteq G$ είναι ορθόθετες υποομάδες τής G με $HK = G$. Να δειχθεί ότι $G/H \bigcap K \cong (G/H) \times (G/K)$.

ΠΑ 91. Να δειχθεί ότι το ευθύ γινόμενο συμπεριφέρεται «προσεταιριστικά» και «μεταθετικά». Με άλλα λόγια, να δειχθεί ότι όταν $(G, \star)$, $(G', \star')$ και $(G'', \star'')$ είναι ομάδες, τότε $G \times G' \cong G' \times G$ και $(G \times G') \times G'' \cong G \times (G' \times G'')$.

ΠΑ 92. Να δειχθεί ότι κάθε ομάδα τάξης 35 είναι κυκλική.

1.8 Ομάδες Μετατάξεων

Στην παρούσα ενότητα θα αναπτύξουμε τη βασική θεωρία των μετατάξεων ενός πεπερασμένου συνόλου, με άλλα λόγια θα μελετήσουμε τη συμμετρική ομάδα $(S_n, \circ)$ ενός συνόλου X με n το πλήθος στοιχεία, βλ. Παράδειγμα 1.2.24(β′).

Τροχιές και ανάλυση σε κύκλους

Αρχίζουμε με το ακόλουθο:

Λήμμα 1.8.1. *Έστω ότι $\sigma \in S_n$ είναι μια μετάταξη τού συνόλου $X = \{1, 2, \ldots, n\}$ και ότι φ_σ είναι το υποσύνολο τού $X \times X$ που ορίζεται ως*

$$(x, y) \in \varphi_\sigma \iff \exists z \in \mathbb{Z} \text{ με } \sigma^z(x) = y.$$

Η σχέση φ_σ είναι μια σχέση ισοδυναμίας επί τού συνόλου X.

Απόδειξη. Πράγματι, $\forall x \in X$, το $(x, x) \in \varphi_\sigma$, αφού $\sigma^0(x) = x$.

Όταν $(x, y) \in \varphi_\sigma$, τότε $\exists z \in \mathbb{Z}$ με $\sigma^z(x) = y$. Συνεπώς, $\sigma^{-z}(y) = x$ και γι’ αυτό το $(y, x) \in \varphi_\sigma$.

Τέλος, όταν τα $(x, y) \in \varphi_\sigma$ και $(y, w) \in \varphi_\sigma$, τότε $\exists z_1, z_2 \in \mathbb{Z}$ με $\sigma^{z_1}(x) = y$ και $\sigma^{z_2}(y) = w$. Συνεπώς, $\sigma^{z_2+z_1}(x) = \sigma^{z_2} \circ \sigma^{z_1}(x) = \sigma^{z_2}(y) = w$ και γι’ αυτό το $(x, w) \in \varphi_\sigma$.

Επειδή λοιπόν το σύνολο φ_σ ικανοποιεί την ανακλαστική, τη συμμετρική και τη μεταβατική ιδιότητα, έπεται ότι είναι μια σχέση ισοδυναμίας επί τού X. □

Ως εκ τούτου, το σύνολο X διαμερίζεται στις κλάσεις ισοδυναμίας τής φ_σ.

Ορισμός 1.8.2. Ονομάζουμε σ-**τροχιά** τού στοιχείου $x \in X$ την κλάση ισοδυναμίας τού x ως προς τη σχέση ισοδυναμίας φ_σ.

Η σ–*τροχιά* τού $x \in X$, δηλαδή το σύνολο $\{\sigma^z(x) \mid z \in \mathbb{Z}\}$, συμβολίζεται με $\mathcal{O}_{\sigma,x}$.

Παράδειγμα 1.8.3. Θα προσδιορίσουμε τις τροχιές των στοιχείων τού συνόλου $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$, για καθεμία από τις επόμενες μετατάξεις:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 2 & 5 & 7 & 6 & 1 & 4 & 8 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 3 & 2 & 1 & 4 & 5 & 6 & 9 & 7 \end{pmatrix} \text{ και}$$

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 3 & 2 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix},$$

Παρατηρούμε ότι

$$1 \xrightarrow{\sigma} 9 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 1,$$
$$2 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 2 \quad \text{και} \quad 6 \xrightarrow{\sigma} 6.$$

Ως εκ τούτου, η σ διαθέτει τις ακόλουθες τρεις τροχιές:

$$\mathcal{O}_{\sigma,1} = \{1, 9, 8, 4, 5, 7\}, \quad \mathcal{O}_{\sigma,2} = \{2, 3\}, \text{ και}$$
$$\mathcal{O}_{\sigma,6} = \{6\}.$$

Παρατηρούμε ότι

$$1 \xrightarrow{\tau} 8 \xrightarrow{\tau} 9 \xrightarrow{\tau} 7 \xrightarrow{\tau} 6 \xrightarrow{\tau} 5 \xrightarrow{\tau} 4 \xrightarrow{\tau} 1,$$
$$2 \xrightarrow{\tau} 3 \xrightarrow{\tau} 2.$$

Ως εκ τούτου, η τ διαθέτει τις ακόλουθες δύο τροχιές:

$$\mathcal{O}_{\tau,1} = \{1, 8, 9, 7, 6, 5, 4\} \text{ και } \mathcal{O}_{\tau,2} = \{2, 3\}.$$

Παρατηρούμε ότι

$$1 \xrightarrow{\rho} 9 \xrightarrow{\rho} 1, \ 2 \xrightarrow{\rho} 3 \xrightarrow{\rho} 2, \ 4 \xrightarrow{\rho} 4,$$
$$5 \xrightarrow{\rho} 5, \ 6 \xrightarrow{\rho} 6, \ 7 \xrightarrow{\rho} 7, \ 8 \xrightarrow{\rho} 8.$$

Ως εκ τούτου, η ρ διαθέτει τις ακόλουθες επτά τροχιές:

$$\mathcal{O}_{\rho,1} = \{1, 9\}, \mathcal{O}_{\rho,2} = \{2, 3\}, \ \mathcal{O}_{\rho,4} = \{4\}, \mathcal{O}_{\rho,5} = \{5\},$$
$$\mathcal{O}_{\rho,6} = \{6\}, \mathcal{O}_{\rho,7} = \{7\} \text{ και } \mathcal{O}_{\rho,8} = \{8\}.$$

Παρατήρηση 1.8.4. Έστω ότι $\sigma \in S_n$, ότι $x \in X$ και ότι $\mathcal{O}_{\sigma,x} = \{\sigma^z(x) \mid z \in \mathbb{Z}\}$ είναι η σ–τροχιά τού x. Επειδή $\mathcal{O}_{\sigma,x} \subseteq X$ και επειδή $|X| = n$, έπεται ότι το πλήθος των στοιχείων τής $\mathcal{O}_{\sigma,x}$ είναι πεπερασμένο. Έτσι συμπεραίνουμε ότι υπάρχουν ακέραιοι $z_1 \neq z_2$, ας πούμε $z_1 > z_2$, με $\sigma^{z_1}(x) = \sigma^{z_2}(x)$, αφού στην αντίθετη περίπτωση το πλήθος των στοιχείων τής $\mathcal{O}_{\sigma,x}$ θα ήταν άπειρο. Τώρα είναι $\sigma^{z_1 - z_2}(x) = x$ με $z_1 - z_2 \in \mathbb{N}$ και επομένως το σύνολο

$$\mathcal{M}(\sigma, x) = \{m \in \mathbb{N} \mid \sigma^m(x) = x\}$$

είναι πάντοτε $\neq \emptyset$. Έστω s το ελάχιστο τού $\mathcal{M}(\sigma, x)$, δηλαδή το s είναι ο ελάχιστος φυσικός αριθμός με $\sigma^s(x) = x$.

Ισχυριζόμαστε ότι

$$\mathcal{O}_{\sigma,x} = \{x, \sigma(x), \sigma^2(x), \ldots, \sigma^i(x), \sigma^{i+1}(x), \ldots, \sigma^{s-1}(x)\}.$$

Πράγματι, τα $\sigma^i(x), 0 \leq i \leq s-1$ είναι σαφώς διακεκριμένα στοιχεία, αφού όταν $\sigma^i(x) = \sigma^j(x), 0 \leq i, j \leq s-1$ με $i \neq j$, ας πούμε $i > j$, τότε $\sigma^{(i-j)}(x) = x$. Όμως το τελευταίο αντίκειται στο ότι το s είναι το ελάχιστο τού $\mathcal{M}(\sigma, x)$, αφού $i - j \in \mathbb{N}$, $i - j < s$ και $\sigma^{(i-j)}(x) = x$.
Επιπλέον, κάθε στοιχείο $\sigma^z(x) \in \mathcal{O}_{\sigma,x}$ ισούται με κάποιο από τα $\sigma^i(x), 0 \leq i \leq s-1$, αφού εκτελώντας ευκλείδεια διαίρεση τού z διά s έχουμε $z = \lambda s + v$, όπου $v = 0, 1, \ldots, s-1$ και γι' αυτό

$$\sigma^z(x) = \sigma^{(\lambda s + v)}(x) = \sigma^v(\sigma^{\lambda s}(x)) = \sigma^v(x).$$

Εδώ χρησιμοποιούμε ότι $\forall \lambda \in \mathbb{Z}$, το $\sigma^{\lambda s}(x) = x$, αφού όταν $\lambda = 0$, τότε $\sigma^{\lambda s}(x) = \sigma^0(x) = \mathrm{Id}_n(x) = x$, όταν $\lambda > 0$, τότε $\sigma^{\lambda s}(x) = \underbrace{\sigma^s \circ \sigma^s \circ \cdots \circ \sigma^s}_{\lambda\text{ -φορές}}(x) = x$, αφού $\sigma^s(x) = x$ και όταν $\lambda < 0$, τότε $\sigma^{\lambda s}(x) = \underbrace{\sigma^{-s} \circ \sigma^{-s} \circ \cdots \circ \sigma^{-s}}_{|\lambda|\text{ -φορές}}(x) = x$, αφού $\sigma^{-s}(x) = x$, επειδή από $\sigma^s(x) = x$, έπεται $\sigma^{-s}(x) = x$.

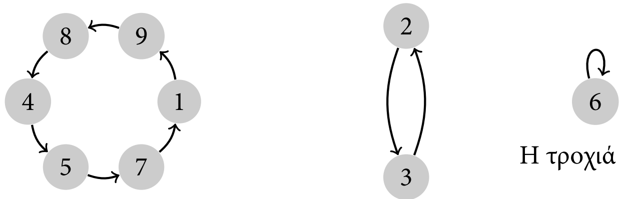
Παράσταση Τροχιών και Κύκλοι

Κάθε τροχιά $\mathcal{O}_{\sigma,x}$ μιας μετάταξης σ μπορεί να αναπαρασταθεί με τη βοήθεια ενός προσανατολισμένου γραφήματος. Το γράφημα αυτό αποτελείται από κορυφές και προσανατολισμένες ακμές[40]. Κορυφές τού γραφήματος είναι τα στοιχεία i τής τροχιάς $\mathcal{O}_{\sigma,x}$. Για κάθε $i \in \mathcal{O}_{\sigma,x}$, υπάρχει μια προσανατολισμένη ακμή με αρχή την κορυφή i και τέλος την κορυφή j, ακριβώς όταν $j = \sigma(i)$.

Συνεπώς, οι κορυφές τού γραφήματος τής τροχιάς $\mathcal{O}_{\sigma,x}$ είναι τα $x, \sigma(x), \ldots, \sigma^{s-1}(x)$. Για $0 \leq i \leq s-2$, κάθε κορυφή $\sigma^i(x)$ είναι αρχή μιας προσανατολισμένης ακμής που έχει ως τέλος την κορυφή $\sigma^{i+1}(x)$. Επιπλέον, η κορυφή $\sigma^{(s-1)}(x)$ είναι αρχή μιας προσανατολισμένης ακμής, η οποία έχει ως τέλος την κορυφή $\sigma^s(x) = x$. Γι' αυτό το γράφημα έχει κυκλική μορφή.

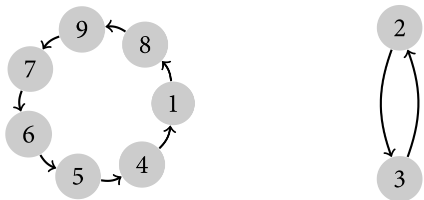
Παράδειγμα 1.8.5. Τα γραφήματα των τροχιών των μεταθέσεων σ, τ και ρ, βλ. Παράδειγμα 1.8.3.

[40]Δηλαδή, τμήματα γραμμών που το ένα σημείο τους θεωρείται η αρχή και το άλλο το τέλος.



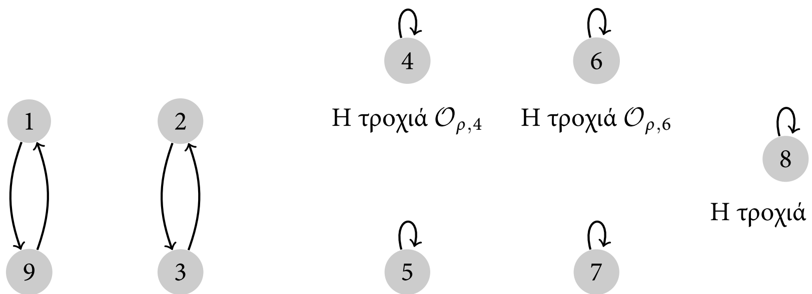
Η τροχιά $\mathcal{O}_{\sigma,1}$ Η τροχιά $\mathcal{O}_{\sigma,2}$ Η τροχιά $\mathcal{O}_{\sigma,6}$

Τα γραφήματα των σ-τροχιών



Η τροχιά $\mathcal{O}_{\tau,1}$ Η τροχιά $\mathcal{O}_{\tau,2}$

Τα γραφήματα των τ-τροχιών



Η τροχιά $\mathcal{O}_{\rho,4}$ Η τροχιά $\mathcal{O}_{\rho,6}$ Η τροχιά $\mathcal{O}_{\rho,8}$

Η τροχιά $\mathcal{O}_{\rho,1}$ Η τροχιά $\mathcal{O}_{\rho,2}$ Η τροχιά $\mathcal{O}_{\rho,5}$ Η τροχιά $\mathcal{O}_{\rho,7}$

Τα γραφήματα των ρ-τροχιών

Ορισμός 1.8.6. Μια μετάταξη $\sigma \in S_n$ ονομάζεται **κύκλος**, όταν διαθέτει *το πολύ* μία τροχιά $\mathcal{O}_{\sigma,x}$ με περισσότερα τού ενός στοιχεία.

Ορισμός 1.8.7. **Μήκος** $\ell(\sigma)$ ενός κύκλου σ ονομάζεται το πλήθος των στοιχείων εκείνης τής τροχιάς του, που έχει το μεγαλύτερο πλήθος στοιχείων.

Για παράδειγμα η μετάταξη

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix} \in S_8$$

είναι ένας κύκλος τής S_8, αφού $\mathcal{O}_{\mu,1} = \{1,2,3,4,5,6,7,8\}$. Το μήκος $\ell(\mu)$ ισούται με 8. Αλλά και η

$$\nu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 2 & 4 & 5 & 6 & 7 & 3 \end{pmatrix} \in S_8$$

είναι επίσης ένας κύκλος τής S_8, αφού $\mathcal{O}_{\nu,1} = \{1\}$, $\mathcal{O}_{\nu,2} = \{2,8,3\}$, $\mathcal{O}_{\nu,4} = \{4\}$, $\mathcal{O}_{\nu,5} = \{5\}$, $\mathcal{O}_{\nu,6} = \{6\}$ και $\mathcal{O}_{\nu,7} = \{7\}$. Το μήκος $\ell(\nu)$ ισούται με 3.
Αντίθετα, η μετάταξη

$$\xi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 5 & 6 & 7 & 8 \end{pmatrix} \in S_8$$

δεν είναι ένας κύκλος τής S_8, αφού έχει περισσότερες από μία τροχιές με περισσότερα τού ενός στοιχεία. Πράγματι, $\mathcal{O}_{\xi,1} = \{1,2\}$ και $\mathcal{O}_{\xi,3} = \{3,4\}$. Εδώ δεν ορίζεται το μήκος τής ξ, αφού η ξ δεν είναι κύκλος.

Παρατήρηση 1.8.8. (α′) Το ταυτοτικό στοιχείο

$$\mathrm{Id}_n = \begin{pmatrix} 1 & 2 & \dots & i & i+1 & \dots & n \\ 1 & 2 & \dots & i & i+1 & \dots & n \end{pmatrix}$$

τής S_n είναι ένας κύκλος, αφού κάθε τροχιά του αποτελείται από ακριβώς ένα στοιχείο. Αλλά και αντίστροφα, όταν κάθε τροχιά μιας μετάταξης $\sigma \in S_n$ αποτελείται από ακριβώς ένα στοιχείο, τότε η σ ισούται με το Id_n. Προφανώς, $\ell(\mathrm{Id}_n) = 1$.

(β′) Όταν μια μετάταξη $\sigma \in S_n$ είναι ένας κύκλος $\neq \mathrm{Id}_n$, τότε υπάρχει κάποιο $x \in X = \{1,2,\dots,n\}$ με $\sigma(x) \neq x$. Γι' αυτό ο σ διαθέτει ακριβώς μία τροχιά, την $\mathcal{O}_{\sigma,x}$, η οποία αποτελείται από περισσότερα τού ενός στοιχεία και μάλιστα

$$\mathcal{O}_{\sigma,x} = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^i(x), \sigma^{i+1}(x), \dots, \sigma^{s-1}(x)\},$$

όπου, σύμφωνα με την Παρατήρηση 1.8.4, ο s είναι ο μικρότερος φυσικός με $\sigma^s(x) = x$.

Συνεπώς,

Το μήκος $\ell(\sigma)$ ενός κύκλου $\sigma \neq \mathrm{Id}_n$ ισούται με τον μικρότερο φυσικό s με $\sigma^s(x) = x$, όπου x είναι ένα οποιοδήποτε στοιχείο τής τροχιάς τού σ που έχει περισσότερα τού ενός στοιχεία.

Χάρις σε αυτήν την παρατήρηση μπορούμε να παραστήσουμε έναν κύκλο σ, που διαθέτει μία τροχιά με περισσότερα από ένα στοιχεία, ας πούμε την

$$\mathcal{O}_{\sigma,x} = \{x, \sigma(x), \sigma^2(x), \dots, \sigma^i(x), \sigma^{i+1}(x), \dots, \sigma^{s-1}(x)\}, s \geq 2,$$

για κάποιο $x \in X = \{1,2,\dots,n\}$, ως εξής:

$$\sigma = \begin{pmatrix} x & \sigma(x) & \sigma^2(x) & \dots & \sigma^i(x) & \sigma^{i+1}(x) & \dots & \sigma^{s-1}(x) \end{pmatrix},$$

ερμηνεύοντας την ανωτέρω σημειογραφία κατά τον εξής τρόπο:

Όταν $x \in X = \{1, 2, \ldots, n\}$, τότε

$$\sigma(x) = \begin{cases} x, & \text{αν } x \neq \sigma^i(x), 1 \leq i \leq s-1, \text{ δηλαδή όταν } x \notin \mathcal{O}_{\sigma,x} \\ \sigma^{i+1}(x), & \text{αν } x = \sigma^i(x), 1 \leq i \leq s-2 \\ x, & \text{αν } x = \sigma^{s-1}(x) \end{cases} \tag{*}$$

Παράδειγμα 1.8.9. (α′) Θεωρούμε τη μετάταξη

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & 9 & 12 & 11 & 2 \end{pmatrix} \in S_{12}.$$

Η σ είναι κύκλος, αφού έχει ακριβώς μία τροχιά με περισσότερα τού ενός στοιχεία. Αυτή είναι η τροχιά

$$\mathcal{O}_{\sigma,2} = \{2, \sigma^1(2) = 4, \sigma^2(2) = 6, \sigma^3(2) = 8, \sigma^4(2) = 10, \sigma^5(2) = 12\}.$$

Το μήκος $\ell(\sigma)$ ισούται με 6. Τώρα, χρησιμοποιώντας τη νέα σημειογραφία, που μόλις είδαμε, έχουμε:

$$\sigma = \begin{pmatrix} 2 & 4 & 6 & 8 & 10 & 12 \end{pmatrix}.$$

Προσέξτε ότι θα μπορούσαμε να σχηματίζαμε την προηγούμενη τροχιά αρχίζοντας από κάποιο άλλο στοιχείο της, ας πούμε το 10. Στην περίπτωση αυτή θα είχαμε:

$$\mathcal{O}_{\sigma,10} = \{10, \sigma^1(10) = 12, \sigma^2(10) = 2, \sigma^3(10) = 4, \sigma^4(10) = 6, \sigma^5(10) = 8\}$$

και ο κύκλος θα γράφονταν ως

$$\sigma = \begin{pmatrix} 10 & 12 & 2 & 4 & 6 & 8 \end{pmatrix}.$$

Η σειρά εμφάνισης των στοιχείων στις δύο προηγούμενες παραστάσεις είναι διαφορετική, ωστόσο αυτές ορίζουν το ίδιο στοιχείο τής S_{12}, δηλαδή το σ.

(β′) Ας δούμε ποιο στοιχείο σ τής S_{12} παριστάνει το

$$\begin{pmatrix} 8 & 5 & 11 & 3 \end{pmatrix}.$$

Σύμφωνα με την ερμηνεία τής σημειογραφίας που δόθηκε στην Παρατήρηση 1.8.8,(2)(*) έχουμε:

$$\sigma(x) = x, \forall x \in \{1, 2, \ldots, 11, 12\} \setminus \{8, 5, 11, 3\},$$
$$\sigma(8) = 5, \ \ \sigma^2(8) = \sigma(5) = 11, \ \ \sigma^3(8) = \sigma(11) = 3, \ \ \sigma^4(8) = \sigma(3) = 8.$$

Συνεπώς, η συγκεκριμένη μετάταξη σ είναι η

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 1 & 4 & 8 & 6 & 11 & 8 & 7 & 5 & 9 & 12 & 3 & 2 \end{pmatrix}.$$

Ορισμός 1.8.10. Οι κύκλοι τής $(S_n, \circ)$ μήκους s ονομάζονται **s–κύκλοι.**
Οι κύκλοι τής $(S_n, \circ)$ μήκους 2, δηλαδή οι 2–κύκλοι, ονομάζονται **αντιμεταθέσεις**.

Παρατήρηση 1.8.11. (α′) Κάθε 1–κύκλος τής S_n παριστάνει το ταυτοτικό στοιχείο Id_n.
Πράγματι, έστω ότι $x \in X = \{1, 2, \ldots, n\}$ και έστω ο 1–κύκλος $\tau = (x)$.

Σύμφωνα με την Παρατήρηση 1.8.8.(2)(*) έχουμε,

$$\tau(y) = \begin{cases} y, & \text{όταν } y \in X \setminus \{x\} \\ x, & \text{όταν } y = x. \end{cases}$$

Επομένως, στην S_n όλοι οι 1–κύκλοι είναι ίσοι μεταξύ τους, αφού οποιοσδήποτε από αυτούς συμπίπτει με το ταυτοτικό στοιχείο Id_n.

(β′) Ένας κύκλος μήκους 2 ονομάζεται αντιμετάθεση , επειδή εναλλάσσει ακριβώς δύο διαφορετικά στοιχεία τού συνόλου $X = \{1, 2, \ldots, n\}$.

Πράγματι, αν $\tau = (x \ \ y)$, όπου $x, y \in X = \{1, 2, \ldots, n\}, x \neq y$, τότε

$$\tau(w) = \begin{cases} w, & \text{όταν } w \in X \setminus \{x, y\} \\ y, & \text{όταν } w = x \\ x, & \text{όταν } w = y. \end{cases}$$

Ορισμός 1.8.12. Δύο κύκλοι τής $(S_n, \circ)$ ονομάζονται **αποσυνδετοί** ή **ξένοι**, όταν οι τροχιές τους με το μεγαλύτερο πλήθος στοιχείων δεν έχουν κοινά στοιχεία.

Παρατήρηση 1.8.13. Από τον προηγούμενο ορισμό προκύπτει ότι για να είναι δύο κύκλοι τής S_n αποσυνδετοί, πρέπει να έχουν και οι δύο μήκος ≥ 2, αφού όταν ένας από τους δύο έχει μήκος 1, τότε αυτός συμπίπτει με το ταυτοτικό στοιχείο Id_n τής S_n. Όμως τότε, κάθε τροχιά τού Id_n έχει μήκος 1, δηλαδή είναι μια τροχιά που έχει το μεγαλύτερο πλήθος στοιχείων, και είναι σαφές ότι όποιος και αν είναι ο άλλος κύκλος, η αντίστοιχη τροχιά του με το μεγαλύτερο πλήθος στοιχείων έχει μη κενή τομή με κάποια από τις τροχιές τού Id_n.

Παράδειγμα 1.8.14. Οι κύκλοι $\sigma = \begin{pmatrix} 1 & 9 & 8 \end{pmatrix}$ και $\tau = \begin{pmatrix} 11 & 1 & 12 \end{pmatrix}$ τής S_{12} δεν είναι αποσυνδετοί. Η μοναδική τροχιά τού σ με μήκος > 1 είναι η $\mathcal{O}_{\sigma,1} = \{1, 9, 8\}$. Η μοναδική τροχιά τού τ με μήκος > 1 είναι η $\mathcal{O}_{\tau,11} = \{11, 1, 12\}$ και $\mathcal{O}_{\sigma,1} \bigcap \mathcal{O}_{\tau,11} = \{1\} \neq \emptyset$.
Αντίθετα οι κύκλοι $\sigma = \begin{pmatrix} 1 & 9 & 8 \end{pmatrix}$ και $\rho = \begin{pmatrix} 6 & 3 & 7 \end{pmatrix}$ τής S_{12} είναι αποσυνδετοί, αφού $\mathcal{O}_{\rho,6} = \{6, 3, 7\}$ και $\mathcal{O}_{\sigma,1} \bigcap \mathcal{O}_{\rho,6} = \emptyset$.

Πρόταση 1.8.15. *Κάθε στοιχείο τής $(S_n, \circ)$ ή είναι κύκλος ή είναι σύνθεση κύκλων αποσυνδετών ανά δύο, όπου το μήκος εκάστου είναι ≥ 2.*

Απόδειξη. Έστω $\sigma \in S_n$.
Εάν η μετάταξη σ είναι ένας κύκλος δεν χρειάζεται να αποδειχθεί τίποτα.
Ας υποθέσουμε ότι η σ δεν είναι κύκλος. Τότε η σ διαθέτει $s \geq 2$ το πλήθος τροχιές που καθεμιά τους έχει $t_i \geq 2$ πλήθος στοιχείων. Ας υποθέσουμε ότι αυτές είναι οι:

$$\mathcal{O}_{\sigma,x_1} = \{x_1, \sigma(x_1), \ldots, \sigma^{t_1-1}(x_1)\}, \mathcal{O}_{\sigma,x_2} = \{x_2, \sigma(x_2), \ldots, \sigma^{t_2-1}(x_2)\}, \ldots,$$
$$\mathcal{O}_{\sigma,x_i} = \{x_i, \sigma(x_i), \ldots, \sigma^{t_i-1}(x_i)\}, \ldots, \mathcal{O}_{\sigma,x_s} = \{x_s, \sigma(x_s), \ldots, \sigma^{t_s-1}(x_s)\}.$$

Για κάθε $i, 1 \leq i \leq s$ ορίζουμε τον κύκλο $\gamma_i = \begin{pmatrix} x_i & \sigma(x_i) & \dots & \sigma^{t_i-1}(x_i) \end{pmatrix}$. Προσέξτε ότι το μήκος $\ell(\gamma_i)$ είναι ≥ 2, αφού το $\ell(\gamma_i)$ ισούται με το πλήθος t_i των στοιχείων τής τροχιάς $\mathcal{O}_{x_i}$.
Ισχυριζόμαστε ότι $\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_i \circ \dots \circ \gamma_s$.

Πράγματι, αν το x είναι ένα στοιχείο τού $\{1, 2, \dots, n\} \setminus (\mathcal{O}_{x_1} \bigcup \mathcal{O}_{x_2} \bigcup \dots \bigcup \mathcal{O}_{x_s})$, τότε $\sigma(x) = x$ και $\gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_i \circ \dots \circ \gamma_s(x) = x$, αφού το x δεν εμφανίζεται σε κανέναν από τους κύκλους γ_i.

Αν το x είναι ένα στοιχείο από το σύνολο $\mathcal{O}_{x_1} \bigcup \mathcal{O}_{x_2} \bigcup \dots \bigcup \mathcal{O}_{x_s}$, τότε το x ανήκει σε ακριβώς μία τροχιά, ας πούμε την $\mathcal{O}_{x_i}$, αφού τα σύνολα $\mathcal{O}_{x_1}, \mathcal{O}_{x_2}, \dots, \mathcal{O}_{x_s}$ είναι ανά δύο αποσυνδετά (ξένα). Έστω ότι $x = \sigma^k(x_i) = \gamma_i^k(x_i), 0 \leq k \leq t_i - 1$. Τότε το $\sigma(x) = \sigma^{k+1}(x_i) = \gamma_i^{k+1}(x_i)$. Παρατηρώντας ότι το στοιχείο αυτό ανήκει επίσης στην $\mathcal{O}_{x_i}$, έχουμε:

$$\begin{aligned}
&\gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_{i-1} \circ \gamma_i \circ \dots \circ \gamma_s(x) = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_{i-1} \circ \gamma_i \circ \dots \circ \gamma_s(\gamma_i^k(x_i)) = \\
&\gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_{i-1} \circ \gamma_i(\gamma_i^k(x_i)) = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_{i-1}(\gamma_i^{k+1}(x_i)) = \gamma_i^{k+1}(x_i) = \sigma(x),
\end{aligned}$$

αφού $\gamma_j(\gamma_i^k(x_i)) = \gamma_i^k(x_i), \forall j, i+1 \leq j \leq s$ και $\gamma_j(\gamma_i^{k+1}(x_i)) = \gamma_i^{k+1}(x_i), \forall j, 1 \leq j \leq i-1$.
Επομένως για κάθε $x \in X := \{1, 2, \dots, n\}$, είναι $\sigma(x) = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_i \circ \dots \circ \gamma_s(x)$ και συνεπώς, $\sigma = \gamma_1 \circ \gamma_2 \circ \dots \circ \gamma_i \circ \dots \circ \gamma_s$, όπου $\forall i, 1 \leq i \leq s$, το μήκος $\ell(\gamma_i)$ ισούται με $t_i \geq 2$, όπως ακριβώς ισχυριστήκαμε. □

Λήμμα 1.8.16. *Έστω ότι γ και δ είναι δύο αποσυνδετοί κύκλοι τής $(S_n, \circ)$, τότε οι κύκλοι μετατίθενται μεταξύ τους, δηλαδή $\gamma \circ \delta = \delta \circ \gamma$.*

Απόδειξη. Σύμφωνα με την Παρατήρηση 1.8.13, το μήκος των γ και δ είναι ≥ 2. Έστω ότι

$$\gamma = \begin{pmatrix} x_1 & x_2 & \dots & x_r \end{pmatrix}, \delta = \begin{pmatrix} y_1 & y_2 & \dots & y_t \end{pmatrix}, \text{ όπου } r, t \geq 2.$$

Για κάθε $a \in \{1, 2, \dots, n\} \setminus (\{x_1, x_2, \dots, x_r\} \bigcup \{y_1, y_2, \dots, y_t\})$, είναι

$$\gamma \circ \delta(a) = a = \delta \circ \gamma(a).$$

Για κάθε $a \in \{x_1, x_2, \dots, x_r\}$, είναι

$$\gamma \circ \delta(a) = \gamma(\delta(a)) = \gamma(a) = \delta(\gamma(a)) = \delta \circ \gamma(a),$$

αφού $a \in \{x_1, x_2, \dots, x_r\}$ συνεπάγεται επίσης ότι $\gamma(a) \in \{x_1, x_2, \dots, x_r\}$ και γι' αυτό τα a και $\gamma(a) \notin \{y_1, y_2, \dots, y_t\}$, επειδή οι γ, δ είναι αποσυνδετοί κύκλοι. Έτσι $\delta(a) = a$ και $\delta(\gamma(a)) = \gamma(a)$. Ακριβώς ανάλογα αποδεικνύεται ότι, για κάθε $a \in \{y_1, y_2, \dots, y_t\}$ είναι

$$\gamma \circ \delta(a) = \gamma(\delta(a)) = \delta(a) = \delta(\gamma(a)) = \delta \circ \gamma(a),$$

αφού $a = \gamma(a)$ και $\delta(a) = \gamma(\delta(a))$. □

Πόρισμα 1.8.17. *Αν $\gamma_1, \gamma_2, \ldots, \gamma_s$ είναι κύκλοι τής $(S_n, \circ)$ ανά δύο αποσυνδετοί, τότε*

$$\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s = \gamma_{i_1} \circ \gamma_{i_2} \circ \cdots \circ \gamma_{i_s}$$

όπου $i_1, i_2, \ldots, i_s$ είναι μια οποιαδήποτε αναδιάταξη των $1, 2, \ldots, s$.

Παρατήρηση 1.8.18. Όταν $\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$ είναι μια σύνθεση κύκλων αποσυνδετών ανά δύο και ρ είναι οποιοσδήποτε ακέραιος αριθμός, τότε

$$(\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s)^\rho = \gamma_1^\rho \circ \gamma_2^\rho \circ \cdots \circ \gamma_s^\rho.$$

Αυτό είναι αληθές, για οποιαδήποτε στοιχεία μιας ομάδας τα οποία μετατίθενται ανά δύο.

Θεώρημα 1.8.19. *Κάθε $\sigma \in S_n$ με $\sigma \neq \mathrm{Id}_n$ παρίσταται ως γινόμενο αποσυνδετών κύκλων μήκους ≥ 2 κατά μοναδικό τρόπο, ανεξαρτήτως από τη σειρά των παραγόντων.*

Απόδειξη. Έστω ότι $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$ και $\sigma = \delta_1 \circ \delta_2 \circ \cdots \circ \delta_t$ είναι δύο παραστάσεις τού σ, όπως περιγράφονται στο θεώρημα. Χωρίς περιορισμό τής γενικότητας, μπορούμε να υποθέσουμε ότι $s \geq t$. Θα εκτελέσουμε μια επαγωγική απόδειξη ως προς s. Όταν $s = 1$, τότε βέβαια $t = 1$ και δεν χρειάζεται να αποδείξουμε κάτι. Έστω ότι το θεώρημα είναι αληθές για κάποιο $s - 1 \geq 1$, θα το αποδείξουμε για s. Επειδή $\sigma \neq \mathrm{Id}_n$, υπάρχει κάποιο $x \in X = \{1, 2, \ldots, n\}$ με $\sigma(x) \neq x$. Αφού το σ είναι σύνθεση των αποσυνδετών κύκλων γ_i, υπάρχει κάποιο μοναδικό $\alpha, 1 \leq \alpha \leq s$ με $\gamma_\alpha(x) = \sigma(x) \neq x$, δηλαδή $\gamma_i(x) = x, \forall i \neq \alpha, 1 \leq i \leq s$. Έστω ότι $\gamma_\alpha = \begin{pmatrix} x_{\alpha 1} & x_{\alpha 2} & \ldots & x_{\alpha t_\alpha} \end{pmatrix}$. Για οποιαδήποτε ακέραια δύναμη $\sigma^\rho(x)$, έχουμε

$$\sigma^\rho(x) = (\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s)^\rho(x) = \gamma_1^\rho \circ \gamma_2^\rho \circ \cdots \circ \gamma_s^\rho(x) = \gamma_\alpha^\rho(x),$$

αφού το $\gamma_\alpha(x)$ και ως εκ τούτου και το $\gamma_\alpha^\rho(x)$ ανήκει στη μοναδική τροχιά $\{x_{\alpha 1}, x_{\alpha 2}, \ldots, x_{\alpha t_\alpha}\}$ τού γ_α με $t_\alpha \geq 2$. (Βλ. και την παρεμφερή επιχειρηματολογία στην απόδειξη τής Πρότασης 1.8.15.) Με την ίδια ακριβώς επιχειρηματολογία συμπεραίνουμε ότι υπάρχει ένας μοναδικός κύκλος δ_β από τη δεύτερη παράσταση τού σ με $\delta_\beta(x) = \sigma(x) \neq x$, δηλαδή $\delta_j(x) = x, \forall j \neq \beta, 1 \leq j \leq t$ και κατόπιν ότι $\sigma^\rho(x) = \delta_\beta^\rho(x)$, για οποιαδήποτε ακέραια δύναμη ρ. Επομένως, για κάθε ακέραια δύναμη ρ είναι $\gamma_\alpha^\rho(x) = \delta_\beta^\rho(x)$. Όμως κάθε κύκλος θ μήκους $\ell(\theta) \geq 2$ είναι τής μορφής $\theta = \begin{pmatrix} y & \theta(y) & \ldots & \theta^{\ell(\theta)-1}(y) \end{pmatrix}$, όπου y είναι οποιοδήποτε στοιχείο τής μοναδικής τροχιάς με μήκος ≥ 2. Άρα, $\gamma_\alpha = \delta_\beta$. Οι κύκλοι αυτών των δύο παραστάσεων τού σ είναι αποσυνδετοί και γι' αυτό, σύμφωνα με την Παρατήρηση 1.8.18 μπορούμε να γράψουμε:

$$\sigma = \gamma_\alpha \circ \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_{\alpha-1} \circ \gamma_{\alpha+1} \circ \cdots \circ \gamma_s = \delta_\beta \circ \delta_1 \circ \delta_2 \cdots \circ \delta_{\beta-1} \circ \delta_{\beta+1} \circ \cdots \circ \delta_t.$$

Εκτελώντας την πράξη από αριστερά με το αντίστροφο τού $\gamma_\alpha = \delta_\beta$, έχουμε:

$$\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_{\alpha-1} \circ \gamma_{\alpha+1} \circ \cdots \circ \gamma_s = \delta_1 \circ \delta_2 \cdots \circ \delta_{\beta-1} \circ \delta_{\beta+1} \circ \cdots \circ \delta_t.$$

Τώρα μπορούμε να εφαρμόσουμε την επαγωγική υπόθεση, αφού η αριστερή πλευρά τής ισότητας αποτελείται από $s-1$ το πλήθος αποσυνδετούς κύκλους. Επομένως, $s-1 = t-1$ και με μια νέα αρίθμηση (αν είναι απαραίτητο) έχουμε ότι $\gamma_i = \delta_i, \forall i, 1 \leq i \leq s-1$. Λαμβάνοντας υπ' όψιν ότι $\gamma_\alpha = \delta_\beta$, διαπιστώνουμε ότι η απόδειξη τού θεωρήματος είναι πλέον ολοκληρωμένη. $\square$

Τάξη Μετατάξεων

Πρόταση 1.8.20. *Έστω ότι σ είναι ένα στοιχείο τής $(S_n, \circ)$.*

(α′) *Όταν το σ είναι ένας κύκλος τής S_n, τότε η τάξη $\circ(\sigma)$ ισούται με το μήκος $\ell(\sigma)$.*

(β′) *Όταν το σ είναι μια σύνθεση $\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s$, $s \geq 2$, κύκλων αποσυνδετών ανά δύο, όπου $\ell(\gamma_i) \geq 2, \forall i, 1 \leq i \leq s$, τότε η τάξη $\circ(\sigma)$ ισούται με το ελάχιστο κοινό πολλαπλάσιο ε των μηκών $\ell(\gamma_i), 1 \leq i \leq s$.*

Απόδειξη. (α′) Όταν ο σ είναι ένας κύκλος μήκους $\ell(\sigma) = 1$, τότε $\sigma = \mathrm{Id}_n$ και συνεπώς, $\circ(\sigma) = 1 = \ell(\sigma)$. Έστω ότι ο $\sigma = \begin{pmatrix} x & \sigma(x) & \ldots & \sigma^{t-1}(x) \end{pmatrix}$ είναι ένας κύκλος μήκους $\ell(\sigma) = t \geq 2$, όπου $x \in X := \{1, 2, \ldots, n\}$. Θα δείξουμε ότι ο t είναι ο μικρότερος φυσικός με $\sigma^t = \mathrm{Id}_n$.

Κατ' αρχάς, δεν υπάρχει φυσικός $k < t$ με $\sigma^k = \mathrm{Id}_n$, αφού τα $\sigma(x), \sigma^2(x) \ldots, \sigma^{t-1}(x)$ είναι όλα διαφορετικά από το x. Θα δείξουμε ότι $\sigma^t(y) = y, \forall y \in X$. Πράγματι, αν το $y \in X \setminus \{\sigma(x), \sigma^2(x) \ldots, \sigma^{t-1}(x)\}$, τότε $\sigma(y) = y$. Αν το $y \in \{\sigma(x), \sigma^2(x) \ldots, \sigma^{t-1}(x)\}$, ας πούμε $y = \sigma^k(x), 0 \leq k \leq t-1$, τότε $\sigma^t(y) = \sigma^t(\sigma^k(x)) = \sigma^k(\sigma^t(x)) = \sigma^k(x)$, αφού $\sigma^t(x) = x$. Επομένως, η τάξη $\circ(\sigma) = t = \ell(\sigma)$.

(β′) Οι γ_i μετατίθενται ανά δύο, αφού είναι αποσυνδετοί, βλ. Πόρισμα 1.8.17 και γι' αυτό $\forall \rho \in \mathbb{Z}$, έχουμε:

$$(\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s)^\rho = \gamma_1^\rho \circ \gamma_2^\rho \circ \cdots \circ \gamma_i^\rho \circ \cdots \circ \gamma_{s-1}^\rho \circ \gamma_s^\rho.$$

Έστω ότι για κάποιον $k \in \mathbb{N}$ είναι $\sigma^k = \mathrm{Id}_n$, τότε βέβαια

$$\sigma^k = \gamma_1^k \circ \gamma_2^k \circ \cdots \circ \gamma_i^k \circ \cdots \circ \gamma_{s-1}^k \circ \gamma_s^k = \mathrm{Id}_n.$$

Θα δείξουμε ότι $\gamma_i^k = \mathrm{Id}_n, \forall i, 1 \leq i \leq s$. Έστω ότι $\gamma_i = \begin{pmatrix} x_i & \gamma(x_i) & \ldots & \gamma^{t_i-1}(x_i) \end{pmatrix}$ και ότι $y \in X = \{1, 2, \ldots, n\}$. Αν το $y \in X \setminus \{x_i, \gamma(x_i), \ldots, \gamma^{t_i-1}(x_i)\}$, τότε $\gamma_i(y) = y$ και προφανώς $\gamma_i^k(y) = y$. Αν το $y \in \{x_i, \gamma(x_i), \ldots, \gamma^{t_i-1}(x_i)\}$, τότε $\gamma_j(y) = y, \forall j, i+1 \leq j \leq s$, διότι οι κύκλοι είναι αποσυνδετοί. Άρα

$$y = \sigma^k(y) = \gamma_1^k \circ \gamma_2^k \circ \cdots \circ \gamma_i^k \circ \cdots \circ \gamma_{s-1}^k \circ \gamma_s^k = \gamma_1^k \circ \gamma_2^k \circ \cdots \circ \gamma_i^k(y). \qquad (*)$$

Επειδή το $\gamma_i^k(y)$ είναι επίσης κάποιο από τα στοιχεία τού $\{x_i, \gamma(x_i), \ldots, \gamma^{t_i-1}(x_i)\}$, συμπεραίνουμε ότι $\gamma_j(\gamma_i^k(y)) = \gamma_i^k(y), \forall j, 1 \leq j \leq i-1$, διότι οι κύκλοι είναι αποσυνδετοί. Έτσι από την $(*)$ έπεται

$$y = \sigma^k(y) = \gamma_1^k \circ \gamma_2^k \circ \cdots \circ \gamma_i^k(y) = \gamma_i^k(y).$$

Έτσι αποδείξαμε ότι $\forall y \in X, \gamma_i^k(y) = y$ και επομένως $\gamma_i^k = \mathrm{Id}_n$.

Συνεπώς, όταν $\sigma^k = \mathrm{Id}_n$, τότε $\forall i, 1 \leq i \leq s$, η τάξη $\ell(\gamma_i)$ είναι διαιρέτης k. Αφού ιδιαιτέρως[41], $\sigma^{\circ(\sigma)} = \mathrm{Id}_n$, συμπεραίνουμε ότι $\forall i, 1 \leq i \leq s$, η $\ell(\gamma_i)$ είναι διαιρέτης τής τάξης $\circ(\sigma)$ τού σ και επομένως η $\circ(\sigma)$ είναι ένα κοινό πολλαπλάσιο των $\ell(\gamma_i), 1 \leq i \leq s$.

[41] Είναι προφανές ότι $\circ(\sigma) < \infty$, αφού $\circ(S_n) = n! < \infty$.

Έστω ε το ελάχιστο κοινό πολλαπλάσιο των $\ell(\gamma_i), 1 \leq i \leq s$. Προφανώς, $\varepsilon \leq \circ(\sigma)$. Επιπλέον, είναι

$$\sigma^\varepsilon = \gamma_1^\varepsilon \circ \gamma_2^\varepsilon \circ \cdots \circ \gamma_i^\varepsilon \circ \cdots \circ \gamma_{s-1}^\varepsilon \circ \gamma_s^\varepsilon = \mathrm{Id}_n,$$

αφού $\forall i, 1 \leq i \leq s, \gamma_i^\varepsilon = \mathrm{Id}_n$. Άρα, $\circ(\sigma) \leq \varepsilon$. Επομένως, $\circ(\sigma) = \varepsilon$. □

Παράδειγμα 1.8.21. Η τάξη τού

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 6 & 3 & 4 & 5 & 1 & 10 & 9 & 2 & 8 \end{pmatrix} \in S_{10}$$

είναι 7 αφού

$$\sigma = \begin{pmatrix} 1 & 7 & 10 & 8 & 9 & 2 & 6 \end{pmatrix},$$

δηλαδή είναι ένας κύκλος μήκους 7. Η τάξη τού

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 9 & 1 & 4 & 5 & 3 & 7 & 6 & 10 & 2 & 8 \end{pmatrix} \in S_{10}$$

είναι το ελάχιστο κοινό πολλαπλάσιο των τάξεων των κύκλων $\begin{pmatrix} 1 & 9 & 2 \end{pmatrix}$, $\begin{pmatrix} 3 & 4 & 5 \end{pmatrix}$, $\begin{pmatrix} 6 & 7 \end{pmatrix}$ και $\begin{pmatrix} 8 & 10 \end{pmatrix}$, αφού

$$\tau = \begin{pmatrix} 1 & 9 & 2 \end{pmatrix} \circ \begin{pmatrix} 3 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 6 & 7 \end{pmatrix} \circ \begin{pmatrix} 8 & 10 \end{pmatrix}.$$

Επομένως $\circ(\tau) = 6$.

Η τάξη τού $\sigma \circ \tau$ **δεν είναι** $\circ(\sigma) \cdot \circ(\tau) = 7 \cdot 6 = 42$. Για να υπολογίσουμε τη συγκεκριμένη τάξη πρέπει πρώτα να εκφράσουμε το $\sigma \circ \tau$ ως σύνθεση αποσυνδετών κύκλων. Έχουμε

$$\begin{array}{llll} \sigma \circ \tau(1) = \sigma(9) = 2 & \sigma \circ \tau(2) = \sigma(1) = 7 & \sigma \circ \tau(3) = \sigma(4) = 4 & \sigma \circ \tau(4) = \sigma(5) = 5 \\ \sigma \circ \tau(5) = \sigma(3) = 3 & \sigma \circ \tau(6) = \sigma(7) = 10 & \sigma \circ \tau(7) = \sigma(6) = 1 & \sigma \circ \tau(8) = \sigma(10) = 8 \\ \sigma \circ \tau(9) = \sigma(2) = 6 & \sigma \circ \tau(10) = \sigma(8) = 9. & & \end{array}$$

Επομένως,

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 7 & 4 & 5 & 3 & 10 & 1 & 8 & 6 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 7 \end{pmatrix} \circ \begin{pmatrix} 3 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 6 & 10 & 9 \end{pmatrix} \in S_{10}$$

Γι' αυτό, η τάξη τού $\sigma \circ \tau$ είναι το ελάχιστο κοινό πολλαπλάσιο των $\circ\left(\begin{pmatrix} 1 & 2 & 7 \end{pmatrix}\right) = 3$, $\circ\left(\begin{pmatrix} 3 & 4 & 5 \end{pmatrix}\right) = 3$ και $\circ\left(\begin{pmatrix} 6 & 10 & 9 \end{pmatrix}\right) = 3$, δηλαδή $\circ(\sigma \circ \tau) = 3$.

Συμπληρώνουμε την παρούσα υποενότητα με τα ακόλουθα:

Πρόταση 1.8.22. *Ο k–κύκλος $\gamma = \begin{pmatrix} x_1 & x_2 & \ldots & x_k \end{pmatrix}, k \geq 2$ τής $(S_n, \circ), n \geq 2$, έχει ως αντίστροφο στοιχείο τον k–κύκλο $\delta = \begin{pmatrix} x_k & x_{k-1} & \ldots & x_1 \end{pmatrix}$.*

Απόδειξη. Αφού η S_n είναι ομάδα αρκεί να αποδείξουμε ότι $\gamma \circ \delta = \mathrm{Id}_n(*)$. Θα δείξουμε ότι $\forall x \in X := \{1, 2, \ldots, n\}$ είναι $\gamma \circ \delta(x) = x$. Πράγματι, αν $x \in X \setminus \{x_1, x_2, \ldots, x_k\}$, τότε

$$\gamma \circ \delta(x) = \gamma \circ \begin{pmatrix} x_k & x_{k-1} & \ldots & x_1 \end{pmatrix}(x) = \begin{pmatrix} x_1 & x_2 & \ldots & x_k \end{pmatrix}(x) = x.$$

Αν $x \in \{x_1, x_2, \ldots, x_k\}$, ας πούμε $x = x_i$, τότε

$$\gamma\circ\delta(x_i) = \begin{cases} \gamma \circ \begin{pmatrix} x_k & x_{k-1} & \ldots & x_1 \end{pmatrix}(x_i) = \begin{pmatrix} x_1 & x_2 & \ldots & x_k \end{pmatrix}(x_{i-1}) = x_i, \text{ αν } i \neq 1 \\ \gamma \circ \begin{pmatrix} x_k & x_{k-1} & \ldots & x_1 \end{pmatrix}(x_1) = \begin{pmatrix} x_1 & x_2 & \ldots & x_k \end{pmatrix}(x_k) = x_1, \text{ αν } i = 1. \end{cases}$$

Έτσι διαπιστώνουμε ότι η $(*)$ είναι αληθής και συνεπώς $\delta = \begin{pmatrix} x_k & x_{k-1} & \ldots & x_1 \end{pmatrix} = \gamma^{-1}$. □

Πρόταση 1.8.23. *Έστω ότι σ είναι μια μετάταξη τής $(S_n, \circ)$, $n \geq 2$, και ότι $\gamma = \begin{pmatrix} x_1 & x_2 & \ldots & x_k \end{pmatrix}$ είναι ένας k–κύκλος, $k \geq 2$. Τότε*

$$\sigma \circ \gamma \circ \sigma^{-1} = \begin{pmatrix} \sigma(x_1) & \sigma(x_2) & \ldots & \sigma(x_k) \end{pmatrix}.$$

Απόδειξη. Επειδή η S_n είναι ομάδα, για την απόδειξη τής πρότασης αρκεί να δείξουμε ότι

$$\sigma \circ \gamma = \begin{pmatrix} \sigma(x_1) & \sigma(x_2) & \ldots & \sigma(x_k) \end{pmatrix} \circ \sigma.$$

Έστω $x \in X := \{1, 2, \ldots, n\}$. Αν $x \notin \{x_1, x_2, \ldots, x_k\}$, το οποίο είναι ισοδύναμο με $\sigma(x) \notin \{\sigma(x_1), \sigma(x_2), \ldots, \sigma(x_k)\}$, αφού η σ είναι αμφιρριπτική, τότε έχουμε:

$$\sigma \circ \gamma(x) = \sigma(x) \text{ και } \begin{pmatrix} \sigma(x_1) & \sigma(x_2) & \ldots & \sigma(x_k) \end{pmatrix} \circ \sigma(x) = \sigma(x).$$

Αν $x \in \{x_1, x_2, \ldots, x_k\}$, δηλαδή αν $x = x_i$, για κάποιο $i, 1 \leq i \leq k$, το οποίο είναι ισοδύναμο με ότι $\sigma(x) = \sigma(x_i)$, διότι το $\sigma \in S_n$, τότε έχουμε:

$$\sigma \circ \gamma(x) = \begin{cases} \sigma(x_{i+1}), & \text{όταν } i = 1, 2, \ldots, k-1, \text{ αφού } \gamma(x_i) = x_{i+1} \\ \sigma(x_1), & \text{όταν } i = k, , \text{ αφού } \gamma(x_k) = x_1 \end{cases}$$

και

$$\begin{pmatrix} \sigma(x_1) & \sigma(x_2) & \ldots & \sigma(x_k) \end{pmatrix} \circ \sigma(x) = \begin{cases} \sigma(x_{i+1}), & \text{όταν } i = 1, 2, \ldots, k-1 \\ \sigma(x_1), & \text{όταν } i = k. \end{cases}$$

Ώστε, $\forall x \in X$ είναι $\sigma \circ \gamma(x) = \begin{pmatrix} \sigma(x_1) & \sigma(x_2) & \ldots & \sigma(x_k) \end{pmatrix} \circ \sigma(x)$ και γι' αυτό οι $\sigma \circ \gamma$ και $\begin{pmatrix} \sigma(x_1) & \sigma(x_2) & \ldots & \sigma(x_k) \end{pmatrix} \circ \sigma$ είναι ίσες απεικονίσεις. □

Γενικά σε μια ομάδα $(G, \star)$, δύο στοιχεία $g, h \in G$ ονομάζονται συζυγή, όταν υπάρχει κάποιο $\alpha \in G$ με $\alpha h \alpha^{-1} = g$. Στο επόμενο κεφάλαιο θα δούμε ότι η έννοια τής συζυγίας είναι μια σχέση ισοδυναμίας και έχει μεγάλη σημασία στη Θεωρία Ομάδων.

Εδώ, η προηγούμενη πρόταση αναδιατυπώνεται ως εξής:

Οποιοδήποτε συζυγές στοιχείο ενός κύκλου τής S_n είναι και πάλι ένας κύκλος.

Οι τάξεις των στοιχείων τής $(S_n, \circ)$ και οι διαμερίσεις τού n.

Σύμφωνα με τις Προτάσεις 1.8.15 και 1.8.20 για να υπολογιστεί η τάξη μιας μετάταξης $\sigma \in S_n$, πρέπει η σ να εκφραστεί ως σύνθεση αποσυνδετών κύκλων και κατόπιν να ευρεθεί το ελάχιστο κοινό πολλαπλάσιο από τα μήκη των κύκλων.

Έστω ότι σ είναι ένα στοιχείο τής S_n και ότι $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$ είναι μια παράσταση ως σύνθεση αποσυνδετών κύκλων. Παρατηρούμε ότι μπορούμε να συμπληρώσουμε την ανάλυση με κύκλους μήκους 1 (αν υπάρχουν), οι οποίοι αντιστοιχούν ακριβώς στις τροχιές τού σ με ακριβώς ένα στοιχείο.
Για παράδειγμα, όταν

$$\sigma = \begin{pmatrix} 4 & 12 & 8 \end{pmatrix} \circ \begin{pmatrix} 2 & 7 & 9 & 11 \end{pmatrix} \in S_{12},$$

τότε το σ εκφράζεται και ως

$$\sigma = \begin{pmatrix} 1 \end{pmatrix} \circ \begin{pmatrix} 3 \end{pmatrix} \circ \begin{pmatrix} 5 \end{pmatrix} \circ \begin{pmatrix} 6 \end{pmatrix} \circ \begin{pmatrix} 10 \end{pmatrix} \circ \begin{pmatrix} 4 & 12 & 8 \end{pmatrix} \circ \begin{pmatrix} 2 & 7 & 9 & 11 \end{pmatrix}.$$

Γενικά, όταν $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$ είναι μια παράσταση τού $\sigma \in S_n$ ως σύνθεση αποσυνδετών κύκλων $\gamma_i = \begin{pmatrix} x_{i1} & x_{i2} & \dots & x_{i\ell(\gamma_i)} \end{pmatrix}, 1 \leq i \leq s$ με αντίστοιχα μήκη $\ell(\gamma_i)$, τότε μπορούμε να συμπληρώσουμε την ανάλυση με $m = n - \sum_{i=1}^{s} \ell(\gamma_i)$ το πλήθος 1–κύκλους $\begin{pmatrix} b_1 \end{pmatrix}, \begin{pmatrix} b_2 \end{pmatrix}, \dots, \begin{pmatrix} b_m \end{pmatrix}$, όπου

$$\forall j, 1 \leq j \leq m, b_j \in \{1, 2, \dots, n\} \setminus \bigcup_{i=1}^{s} \{x_{i1}, x_{i2}, \dots, x_{i\ell(\gamma_i)}\}.$$

και συνεπώς

$$\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s = \begin{pmatrix} b_1 \end{pmatrix} \circ \begin{pmatrix} b_2 \end{pmatrix} \circ \cdots \circ \begin{pmatrix} b_m \end{pmatrix} \circ \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s.$$

Τώρα το άθροισμα από τα μήκη των κύκλων τής προηγούμενης ανάλυσης ισούται με n. Επειδή αποσυνδετοί κύκλοι μετατίθενται, βλ. Πόρισμα 1.8.17, μπορούμε επιπλέον να δεχθούμε ότι οι κύκλοι $\gamma_i, 1 \leq i \leq s$ είναι διατεταγμένοι με αύξουσα σειρά ως προς τα μήκη τους, δηλαδή αν $i < j$, τότε $\ell(\gamma_i) \leq \ell(\gamma_j)$.
Έτσι έχουμε

$$n = \underbrace{1 + 1 + \cdots + 1}_{m-\text{φορές}} + \sum_{i=1}^{s} \ell(\gamma_i)$$

Ορισμός 1.8.24. Κάθε ακολουθία φυσικών αριθμών $(n_1, n_2, \dots, n_r)$ με $n_1 \leq n_2 \leq \cdots \leq n_r$ και $n_1 + n_2 + \cdots + n_r = n$ ονομάζεται μια **διαμέριση** τού φυσικού αριθμού $n \in \mathbb{N}$.

Επομένως, κάθε $\sigma \in S_n$ χορηγεί μια διαμέριση τού n, αλλά και αντίστροφα κάθε διαμέριση $(n_1, n_2, \dots, n_r)$ τού n χορηγεί μια μετάταξη (όχι απαραίτητα μοναδική) τής S_n, αφού μπορούμε να προσδιορίσουμε r κύκλους μήκους n_i, οι οποίοι μάλιστα μπορεί να είναι αποσυνδετοί ανά δύο για κάθε $n_i \geq 2$.

Για παράδειγμα, η διαμέριση $(1, 2, 3, 3, 3)$ τού 12 δίνει τη μετάταξη

$$\sigma = \begin{pmatrix}4\end{pmatrix} \circ \begin{pmatrix}5 & 6\end{pmatrix} \circ \begin{pmatrix}3 & 11 & 12\end{pmatrix} \circ \begin{pmatrix}1 & 7 & 8\end{pmatrix} \circ \begin{pmatrix}2 & 10 & 9\end{pmatrix}$$

καθώς επίσης και τη μετάταξη

$$\tau = \begin{pmatrix}5\end{pmatrix} \circ \begin{pmatrix}2 & 7\end{pmatrix} \circ \begin{pmatrix}4 & 8 & 10\end{pmatrix} \circ \begin{pmatrix}3 & 6 & 9\end{pmatrix} \circ \begin{pmatrix}1 & 11 & 12\end{pmatrix}$$

Οι σ και τ επειδή προκύπτουν από την ίδια διαμέριση τού 12, που είναι η $(1, 2, 3, 3, 3)$, έχουν την ίδια τάξη, αφού το ελάχιστο κοινό πολλαπλάσιο των μηκών των αποσυνδετών κύκλων τους ισούται και στις δύο περιπτώσεις με $2 \cdot 3 = 6$.

Ορισμός 1.8.25. Ονομάζουμε *κυκλικό τύπο* μιας μετάταξης $\sigma \in S_n$, την αντίστοιχη διαμέριση τού n, που προκύπτει αναλύοντας τη σ σε γινόμενο αποσυνδετών κύκλων $\gamma_i, 1 \leq i \leq s$ διατεταγμένων με αύξουσα σειρά, συμπληρώνοντας (αν είναι απαραίτητο) την αρχή τής ακολουθίας με τόσες μονάδες, όση είναι η διαφορά $n - \sum_{i=1}^{s} \ell(\gamma_i)$.

Για παράδειγμα ο κυκλικός τύπος τής

$$\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 1 & 3 & 5 & 4\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}4 & 5\end{pmatrix} \in S_5$$

είναι $(1, 2, 2)$ ενώ τής

$$\tau = \begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9\\ 2 & 1 & 3 & 5 & 4 & 6 & 7 & 8 & 9\end{pmatrix} = \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}4 & 5\end{pmatrix} \in S_9$$

είναι $(1, 1, 1, 1, 1, 2, 2)$.

Πρόταση 1.8.26. *Αν ο κυκλικός τύπος μιας μετάταξης $\sigma \in S_n$ είναι $(n_1, n_2, \ldots, n_t)$, τότε η τάξη $\circ(\sigma)$ ισούται με το ελάχιστο κοινό πολλαπλάσιο των αριθμών $n_1, n_2, \ldots, n_t$.*

Απόδειξη. Ήδη γνωρίζουμε ότι η τάξη τής σ ισούται με το ελάχιστο κοινό πολλαπλάσιο των μηκών των αποσυνδετών κύκλων μήκους ≥ 2 που εμφανίζονται σε μια ανάλυσή τής. Αν κάποιοι από τους φυσικούς αριθμούς που εμφανίζονται στην αρχή τού κυκλικού τύπου $(n_1, n_2, \ldots, n_t)$ είναι ίσοι με 1, αυτό δεν επιδρά στον υπολογισμό τού ελάχιστου κοινού πολλαπλάσιου. □

Μέγιστη Τάξη: Αν λοιπόν θέλουμε να υπολογίσουμε ποια είναι η μέγιστη τάξη των στοιχείων τής S_n, οφείλουμε να υπολογίσουμε όλες τις διαμερίσεις $(n_1, n_2, \ldots, n_t)$ τού συγκεκριμένου n και κατόπιν να προσδιορίσουμε για καθεμία το ελάχιστο κοινό πολλαπλάσιο των αριθμών τού συνόλου $\{n_1, n_2, \ldots, n_t\}$. Το μεγαλύτερο ελάχιστο κοινό πολλαπλάσιο δίνει και τη μέγιστη τάξη των στοιχείων τής S_n, πρόκειται δηλαδή για τον αριθμό

$$m = \max\left\{\text{ελάχιστο κοινό πολλαπλάσιο}(n_1, n_2, \ldots, n_t) \mid (n_1, n_2, \ldots, n_t) \text{ διαμέριση τού } n\right\}$$

Για παράδειγμα οι διαμερίσεις τού φυσικού αριθμού 5 είναι οι:

1	1	1	1	1
1	1	1	2	
1	2	2		
1	1	3		
2	3			
1	4			
5				

Συνεπώς, η μέγιστη τάξη ενός στοιχείου τής S_5 είναι το ελάχιστο κοινό πολλαπλάσιο των 2 και 3, δηλαδή το 6. Τα στοιχεία τής S_5 που έχουν τάξη 6 είναι ακριβώς τα στοιχεία που είναι συνθέσεις δύο αποσυνδετών κύκλων μήκους 2 και 3 αντιστοίχως. Έτσι τα $\sigma_1 = \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4 & 5\end{pmatrix}$, $\sigma_2 = \begin{pmatrix}3 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 5\end{pmatrix}$, $\sigma_3 = \begin{pmatrix}4 & 5\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\end{pmatrix}$ είναι στοιχεία τής S_5 τάξης 6.
Φυσικά, γνωρίζοντας όλες τις διαμερίσεις τού n γνωρίζουμε και όλες τις τάξεις των στοιχείων τής S_n. Γι' αυτό οι τάξεις των στοιχείων τής S_5 είναι οι $1, 2, 3, 6, 4, 5$ αφού αυτοί οι αριθμοί είναι ακριβώς τα διαφορετικά ελάχιστα κοινά πολλαπλάσια που προκύπτουν από τις διαμερίσεις τού 5. Συνεπώς ο προσδιορισμός των τάξεων όλων των στοιχείων τής S_n ανάγεται στον υπολογισμό όλων των δυνατών διαμερίσεων τού n. Αυτό δεν είναι καθόλου απλό, επειδή δεν υπάρχει τύπος που να δίνει το πλήθος $P(n)$ των διαμερίσεων ενός φυσικού n, το οποίο σημειωτέον ότι αυξάνει πολύ γρήγορα, όπως διαπιστώνει κανείς και από τους επόμενους δύο πίνακες:

Φυσικός n	1	2	3	4	5	6	7	8	9	10
Πλήθος Διαμερίσεων $P(n)$	1	2	3	5	7	11	15	22	30	42

Πίνακας 1.1: Το πλήθος $P(n)$ των διαμερίσεων τού $n = 1, 2, \ldots, 10$

Φυσικός n	100	200
Πλήθος Διαμερίσεων $P(n)$	190569292	3972999029388
Φυσικός n	300	400
Πλήθος Διαμερίσεων $P(n)$	9253082936723602	6727090051741041926

Πίνακας 1.2: Το πλήθος $P(n)$ των διαμερίσεων τού $n = 100, 200, 300, 400$

Το πρόσημο μιας μετάταξης

Μέχρι τώρα είδαμε ότι κάθε μετάταξη $\sigma \in S_n$ έχει μια μοναδική παράσταση ως σύνθεση αποσυνδετών κύκλων ανεξάρτητα από τη σειρά παραγόντων. Στην παρούσα υποενότητα θα διαπιστώσουμε ότι κάθε μετάταξη σ παρίσταται επίσης ως σύνθεση αντιμεταθέσεων. Για τη σ, η σύνθεση αυτή δεν είναι μοναδική, αλλά το πλήθος των παραγόντων τής σύνθεσης είναι πάντοτε ή άρτιο ή περιττό. Για τις συμμετρικές ομάδες $(S_n, \circ)$ αλλά και γενικότερα για τη Θεωρία Ομάδων, θα δούμε η διαπίστωση αυτή είναι πολύ σημαντική.

Λήμμα 1.8.27. *Κάθε s–κύκλος $\gamma = \begin{pmatrix} x_1 & x_2 & \dots & x_s \end{pmatrix}$ τής $(S_n, \circ), n \geq 2$, είναι σύνθεση αντιμεταθέσεων. Αν $s \geq 2$, τότε ο γ είναι σύνθεση $(s-1)$ το πλήθος αντιμεταθέσεων*

Απόδειξη. Αν ο γ έχει μήκος $s = 1$, τότε ισούται με την ταυτοτική απεικόνιση Id_n, και $\gamma = \mathrm{Id}_n = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}$. Αν ο κύκλος γ έχει μήκος $s \geq 2$, τότε θα δείξουμε ότι:

$$\begin{aligned} &\gamma = \begin{pmatrix} x_1 & x_2 & \dots & x_s \end{pmatrix} = \\ &\begin{pmatrix} x_1 & x_s \end{pmatrix} \circ \begin{pmatrix} x_1 & x_{s-1} \end{pmatrix} \circ \dots \circ \begin{pmatrix} x_1 & x_{i+1} \end{pmatrix} \circ \begin{pmatrix} x_1 & x_i \end{pmatrix} \circ \dots \circ \\ &\begin{pmatrix} x_1 & x_3 \end{pmatrix} \circ \begin{pmatrix} x_1 & x_2 \end{pmatrix}. \end{aligned} \tag{*}$$

Πράγματι, όταν $x \in \{1, 2, \dots, n\} \setminus \{x_1, x_2 \dots, x_s\}$, τότε $\gamma(x) = x$ και

$$\begin{pmatrix} x_1 & x_s \end{pmatrix} \begin{pmatrix} x_1 & x_{s-1} \end{pmatrix} \circ \dots \circ \begin{pmatrix} x_1 & x_{i+1} \end{pmatrix} \circ \begin{pmatrix} x_1 & x_i \end{pmatrix} \circ \dots \circ \begin{pmatrix} x_1 & x_3 \end{pmatrix} \circ \begin{pmatrix} x_1 & x_2 \end{pmatrix} (x) = x.$$

Όταν $x \in \{x_1, x_2 \dots, x_s\}, x \neq x_s$, ας πούμε $x = x_i$ με $i \neq s$, τότε $\gamma(x_i) = x_{i+1}$ και

$$\begin{aligned} &\begin{pmatrix} x_1 & x_s \end{pmatrix} \circ \begin{pmatrix} x_1 & x_{s-1} \end{pmatrix} \circ \dots \circ \begin{pmatrix} x_1 & x_{i+1} \end{pmatrix} \circ \begin{pmatrix} x_1 & x_i \end{pmatrix} \circ \dots \circ \begin{pmatrix} x_1 & x_3 \end{pmatrix} \circ \begin{pmatrix} x_1 & x_2 \end{pmatrix} (x_i) = \\ &\begin{pmatrix} x_1 & x_s \end{pmatrix} \circ \begin{pmatrix} x_1 & x_{s-1} \end{pmatrix} \circ \dots \circ \begin{pmatrix} x_1 & x_{i+1} \end{pmatrix} \circ \begin{pmatrix} x_1 & x_i \end{pmatrix} (x_i) = \\ &\begin{pmatrix} x_1 & x_s \end{pmatrix} \circ \begin{pmatrix} x_1 & x_{s-1} \end{pmatrix} \circ \dots \circ \begin{pmatrix} x_1 & x_{i+1} \end{pmatrix} (x_1) = \\ &\begin{pmatrix} x_1 & x_s \end{pmatrix} \circ \begin{pmatrix} x_1 & x_{s-1} \end{pmatrix} \circ \dots \circ \begin{pmatrix} x_1 & x_{i+2} \end{pmatrix} (x_{i+1}) = x_{i+1}. \end{aligned}$$

Τέλος, όταν $x = x_s$, τότε $\gamma(x_s) = x_1$ και

$$\begin{aligned} &\begin{pmatrix} x_1 & x_s \end{pmatrix} \circ \begin{pmatrix} x_1 & x_{s-1} \end{pmatrix} \circ \dots \circ \begin{pmatrix} x_1 & x_{i+1} \end{pmatrix} \circ \begin{pmatrix} x_1 & x_i \end{pmatrix} \circ \dots \circ \begin{pmatrix} x_1 & x_3 \end{pmatrix} \circ \begin{pmatrix} x_1 & x_2 \end{pmatrix} (x_s) = \\ &\begin{pmatrix} x_1 & x_s \end{pmatrix} (x_s) = x_1. \end{aligned}$$

Επομένως $\forall x \in \{1, 2, \dots, n\}$, είναι:

$$\gamma(x) = \begin{pmatrix} x_1 & x_s \end{pmatrix} \circ \begin{pmatrix} x_1 & x_{s-1} \end{pmatrix} \circ \dots \circ \begin{pmatrix} x_1 & x_{i+1} \end{pmatrix} \circ \begin{pmatrix} x_1 & x_i \end{pmatrix} \circ \dots \circ \begin{pmatrix} x_1 & x_3 \end{pmatrix} \circ \begin{pmatrix} x_1 & x_2 \end{pmatrix} (x)$$

Συνεπώς η $(*)$ είναι αληθής. Προφανώς, το πλήθος των αντιμεταθέσεων είναι $(s-1)$. □

Πρόταση 1.8.28. *Κάθε στοιχείο $\sigma \in S_n, n \geq 2$, είναι σύνθεση αντιμεταθέσεων.*

Απόδειξη. Σύμφωνα με την Πρόταση 1.8.20, κάθε μετάταξη είναι σύνθεση κύκλων και από το προηγούμενο λήμμα, κάθε κύκλος είναι σύνθεση αντιμεταθέσεων. Επομένως, κάθε μετάταξη είναι σύνθεση αντιμεταθέσεων. □

Η προηγούμενη πρόταση αναδιατυπώνεται ως

Πόρισμα 1.8.29. *Έστω ότι $(S_n, \circ)$, $n \geq 2$, είναι η ομάδα μετατάξεων τού $X = \{1, 2, \ldots, n\}$ και ότι $M = \{\begin{pmatrix} i & j \end{pmatrix} \mid 1 \leq i, j \leq n, i \neq j\}$ είναι το σύνολο των αντιμεταθέσεών της. Τότε η ομάδα S_n παράγεται από το σύνολο των αντιμεταθέσεων M, δηλαδή $S_n = \langle M \rangle$.*

Πρόταση 1.8.30. *Έστω ότι $(S_n, \circ)$, $n \geq 2$, είναι η ομάδα μετατάξεων τού $X = \{1, 2, \ldots, n\}$ και ότι T είναι το σύνολο των αντιμεταθέσεων τής μορφής $\begin{pmatrix} 1 & i \end{pmatrix}$, $i \neq 1$. Τότε $S_n = \langle T \rangle$.*

Απόδειξη. Από το προηγούμενο πόρισμα γνωρίζουμε ότι η S_n παράγεται από το σύνολο των αντιμεταθέσεων. Επομένως για την απόδειξη τού ισχυρισμού, αρκεί να δείξουμε ότι κάθε αντιμετάθεση είναι γινόμενο από στοιχεία τού συνόλου T. Έστω ότι $\tau = \begin{pmatrix} i & j \end{pmatrix} \in M$ είναι μια αντιμετάθεση. Αν $i = 1$, τότε δεν χρειάζεται να αποδείξουμε κάτι, αφού η τ ανήκει στο T. Αν $i \neq 1$, τότε θεωρούμε τις αντιμεταθέσεις $\sigma = \begin{pmatrix} 1 & i \end{pmatrix}$ και $\rho = \begin{pmatrix} 1 & j \end{pmatrix}$ και έχουμε $\tau = \sigma \circ \rho \circ \sigma$. Πράγματι, $\sigma \circ \rho \circ \sigma = \sigma \circ \rho \circ \sigma^{-1}$, διότι $\sigma^2 = \mathrm{Id}_n$ και τώρα από την Πρόταση 1.8.23, προκύπτει $\sigma \circ \rho \circ \sigma^{-1} = \sigma \circ \begin{pmatrix} 1 & j \end{pmatrix} \sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(j) \end{pmatrix} = \begin{pmatrix} i & j \end{pmatrix} = \tau$. □

Υπάρχουν αρκετοί τρόποι για την εισαγωγή τού πρόσημου μιας μετάταξης. Σκοπεύουμε να ακολουθήσουμε έναν τρόπο που ουσιαστικά αποτελεί εισαγωγή στην έννοια τής δράσης που θα δούμε στο επόμενο κεφάλαιο.

Έστω $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ το σύνολο των πολυωνύμων n μεταβλητών με ακέραιους συντελεστές και $(S_n, \circ)$ η συμμετρική ομάδα τού συνόλου $X = \{1, 2, \ldots, n\}$.
Όταν το $f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ και το $\sigma \in S_n$, τότε θέτουμε

$$\sigma(f) := f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).$$

Επειδή κάθε $\sigma \in S_n$ είναι μια αμφιρριπτική απεικόνιση από X επί τού X, συμπεραίνουμε ότι το $\sigma(f)$ είναι και πάλι ένα στοιχείο τού $\mathbb{Z}[x_1, x_2, \ldots, x_n]$, αφού τα $x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}$ αποτελούν μια αναδιάταξη των $x_1, x_2, \ldots, x_n$. Κατ' αυτόν τον τρόπο ορίζεται μια απεικόνιση

$$\begin{aligned} \star : S_n \times \mathbb{Z}[x_1, x_2, \ldots, x_n] &\to \mathbb{Z}[x_1, x_2, \ldots, x_n], \\ f(x_1, x_2, \ldots, x_n) &\mapsto \sigma \star f(x_1, x_2, \ldots, x_n) := f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}). \end{aligned}$$

Παρατήρηση 1.8.31.

(α') $\forall f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, η απεικόνιση $\star$ ικανοποιεί την $\mathrm{Id}_n \star f = f$, αφού
$\mathrm{Id}_n \star f(x_1, x_2, \ldots, x_n) = f(x_{\mathrm{Id}_n(1)}, x_{\mathrm{Id}_n(2)}, \ldots, x_{\mathrm{Id}_n(n)}) = f(x_1, x_2, \ldots, x_n)$.

(β') $\forall \sigma, \tau \in S_n$ και $\forall f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, είναι:

$$\begin{aligned} &(\sigma \circ \tau) \star f(x_1, x_2, \ldots, x_n) = f(x_{\sigma\circ\tau(1)}, x_{\sigma\circ\tau(2)}, \ldots, x_{\sigma\circ\tau(n)}) = \\ &f(x_{\sigma(\tau(1))}, x_{\sigma(\tau(2))}, \ldots, x_{\sigma(\tau(n))}) = \sigma \star f(x_{\tau(1)}, x_{\tau(2)}, \ldots, x_{\tau(n)}) = \\ &\sigma \star (\tau \star f(x_1, x_2, \ldots, x_n)). \end{aligned}$$

(γ') $\forall \lambda \in \mathbb{Z}$, $\forall \sigma \in S_n$ και $\forall f(x_1, x_2, \ldots, x_n) \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$, είναι:

$$\sigma \star (\lambda f(x_1, x_2, \ldots, x_n)) = \lambda f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}) = \lambda(\sigma \star f(x_1, x_2, \ldots, x_n)).$$

Θεωρούμε το πολυώνυμο

$$\Delta_n := \Delta_n(x_1, x_2, \dots, x_n) = \prod_{1\leq i<j\leq n} (x_j - x_i) \in \mathbb{Z}[x_1, x_2, \dots, x_n], n \geq 2.$$

Λήμμα 1.8.32. *Για κάθε $\sigma \in S_n, n \geq 2$, είναι*

$$\sigma \star \Delta_n(x_1, x_2, \dots, x_n) = \pm\Delta_n(x_1, x_2, \dots, x_n).$$

Απόδειξη. Έχουμε:

$$\sigma \star \Delta_n(x_1, x_2, \dots, x_n) = \Delta_n(x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}) = \prod_{1\leq i<j\leq n} (x_{\sigma(j)} - x_{\sigma(i)}).$$

Ισχυριζόμαστε ότι οι παράγοντες τού $\sigma \star \Delta_n$ συμπίπτουν με τους παράγοντες τού Δ_n με πιθανή εξαίρεση τού πρόσημου τους. Πράγματι, για κάθε i, j με $1 \leq i < j \leq n$, είναι ή $\sigma(i) < \sigma(j)$ ή $\sigma(j) < \sigma(i)$, αφού $\sigma \in S_n$ και ως εκ τούτου, $\sigma(i) \neq \sigma(j)$. Έτσι, όταν $\sigma(i) < \sigma(j)$ τότε ο παράγοντας $(x_{\sigma(j)} - x_{\sigma(i)})$ τού $\sigma \star \Delta_n$ είναι παράγοντας τού Δ_n, ενώ όταν $\sigma(j) < \sigma(i)$, τότε ο αντίθετός του $-(x_{\sigma(j)} - x_{\sigma(i)})$ είναι παράγοντας τού Δ_n. Αν το πλήθος των παραγόντων $(x_{\sigma(j)} - x_{\sigma(i)})$ με $\sigma(j) < \sigma(i)$ είναι άρτιο, τότε $\sigma \star \Delta_n = \Delta_n$ και αν το πλήθος είναι περιττό, τότε $\sigma \star \Delta_n = -\Delta_n$. □

Επομένως, όταν $\sigma \in S_n$, τότε $\sigma \star \Delta_n = \varepsilon(\sigma)\Delta_n$, όπου $\varepsilon(\sigma) = 1$ ή $\varepsilon(\sigma) = -1$. Το $\varepsilon(\sigma)$ ονομάζεται το *πρόσημο* τής μετάταξης σ.

Ορισμός 1.8.33. Μια μετάταξη $\sigma \in S_n$ ονομάζεται *άρτια*, όταν το $\varepsilon(\sigma) = 1$ και περιττή όταν $\varepsilon(\sigma) = -1$.

Λήμμα 1.8.34. *Οποιαδήποτε αντιμετάθεση $\tau = \begin{pmatrix}\alpha & \beta\end{pmatrix}$ τής συμμετρικής ομάδας $(S_n, \circ), n \geq 2$, είναι περιττή μετάθεση.*

Απόδειξη. Θα αποδείξουμε ότι $\tau(\Delta_n) = -\Delta_n$. Χωρίς περιορισμό τής γενικότητας $\alpha < \beta$. Παρατηρούμε ότι οι μοναδικοί παράγοντες $(x_j - x_i)$ τού Δ_n, επί των οποίων η αντιμετάθεση τ δεν δρα ταυτοτικώς, είναι εκείνοι που τουλάχιστον ένας από τους δείκτες τους είναι ή ο δείκτης α ή ο δείκτης β.
Διακρίνουμε τις περιπτώσεις:

(α′) Όταν $j = \beta, i = \alpha$, δηλαδή $(x_j - x_i) = (x_\beta - x_\alpha)$, τότε η εικόνα τού $(x_\beta - x_\alpha)$ είναι η $(x_{\tau(\beta)} - x_{\tau(\alpha)}) = (x_\alpha - x_\beta) = -(x_\beta - x_\alpha)$ και στο $\tau(\Delta_n)$ υπάρχει μία αλλαγή ως προς το πρόσημο τού Δ_n.

(β′) Όταν $k < \alpha < \beta$, τότε η εικόνα τού $(x_\alpha - x_k)$ είναι η $(x_{\tau(\alpha)} - x_{\tau(k)}) = (x_\beta - x_k)$ και η εικόνα τού $(x_\beta - x_k)$ είναι η $(x_{\tau(\beta)} - x_{\tau(k)}) = (x_\alpha - x_k)$ και στο $\tau(\Delta_n)$ δεν υπάρχει καμία αλλαγή ως προς το πρόσημο τού Δ_n.

(γ′) Όταν $\alpha < k < \beta$, τότε η εικόνα τού $(x_k - x_\alpha)$ είναι η $(x_{\tau(k)} - x_{\tau(\alpha)}) = (x_k - x_\beta) = -(x_\beta - x_k)$ και η εικόνα τού $(x_\beta - x_k)$ είναι η $(x_{\tau(\beta)} - x_{\tau(k)}) = (x_\alpha - x_k) = -(x_k - x_\alpha)$ και στο $\tau(\Delta_n)$ δεν υπάρχει καμία αλλαγή ως προς το πρόσημο τού Δ_n, επειδή το πρόσημο άλλαξε δύο φορές.

(δ′) Όταν $\alpha < \beta < k$, τότε η εικόνα τού $(x_k - x_\alpha)$ είναι η $(x_{\tau(k)} - x_{\tau(\alpha)}) = (x_k - x_\beta)$ και η εικόνα τού $(x_k - x_\beta)$ είναι η $(x_{\tau(k)} - x_{\tau(\beta)}) = (x_k - x_\alpha)$ και στο $\tau(\Delta_n)$ δεν υπάρχει καμία αλλαγή ως προς το πρόσημο τού Δ_n.

Επομένως, $\tau(\Delta_n) = -\Delta_n$. □

Με τη βοήθεια τού $\varepsilon(\sigma)$ ορίζεται η απεικόνιση πρόσημου:

$$\varepsilon : S_n \to \{1, -1\}, \sigma \mapsto \varepsilon(\sigma),$$

με το $\{1, -1\} \subset \mathbb{Z}$. Θεωρούμε την ομάδα $(\{1, -1\}, \cdot)$, όπου «$\cdot$» είναι ο συνήθης πολλαπλασιασμός ακεραίων.

Πρόταση 1.8.35. *Η απεικόνιση πρόσημου $\varepsilon : S_n \to \{1, -1\}, n \geq 2$, είναι ένας επιμορφισμός.*

Απόδειξη. Προφανώς η απεικόνιση ε είναι επιρριπτική («επί»), αφού το το πρόσημο τής $\begin{pmatrix}1 & 2\end{pmatrix}$ ισούται με -1 και το πρόσημο τής ταυτοτικής απεικόνισης ισούται με 1.

Θα δείξουμε ότι η ε είναι ομομορφισμός, δηλαδή θα δείξουμε ότι $\forall \sigma, \tau \in S_n$ είναι $\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma)\varepsilon(\tau)$. Διακρίνουμε τις περιπτώσεις $\varepsilon(\sigma \circ \tau) = 1$ και $\varepsilon(\sigma \circ \tau) = -1$.

Παρατηρούμε ότι $\varepsilon(\sigma \circ \tau) = 1 \Leftrightarrow (\sigma \circ \tau) \star \Delta_n = \sigma \star (\tau \star \Delta_n) = \Delta_n, (\dagger)$. Όταν $\tau \star \Delta_n = \Delta_n$, δηλαδή όταν $\varepsilon(\tau) = 1$, τότε από την $(\dagger)$ συμπεραίνουμε ότι το $\sigma(\Delta_n)$ οφείλει να ισούται με Δ_n, δηλαδή $\varepsilon(\sigma) = 1$. Επομένως, $\varepsilon(\sigma \circ \tau) = 1 = 1 \cdot 1 = \varepsilon(\sigma)\varepsilon(\tau)$.

Όταν $\tau \star \Delta_n = -\Delta_n$, δηλαδή όταν $\varepsilon(\tau) = -1$, τότε από την Παρατήρηση 1.8.31, είναι $\sigma \star (\tau \star \Delta_n) = -\sigma(\Delta_n)$ και λόγω τής $(\dagger)$ το $\sigma(\Delta_n)$ οφείλει να ισούται με $-\Delta_n$, δηλαδή $\varepsilon(\sigma) = -1$. Επομένως, $\varepsilon(\sigma \circ \tau) = 1 = (-1) \cdot (-1) = \varepsilon(\sigma)\varepsilon(\tau)$.

Η περίπτωση $\varepsilon(\sigma \circ \tau) = -1 \Leftrightarrow (\sigma \circ \tau) \star \Delta_n = \sigma \star (\tau \star \Delta_n) = -\Delta_n, (\dagger\dagger)$ είναι ανάλογη και προτείνουμε να εκτελέσει την απόδειξη ο αναγνώστης μόνος του.

᾿Αρα, ο ε είναι ένας επιμορφισμός. □

Τώρα θα αποδείξουμε το ιδιαιτέρως σημαντικό:

Θεώρημα 1.8.36. *Κάθε μετάταξη $\sigma \in S_n, n \geq 2$, είναι σύνθεση ή ενός άρτιου ή ενός περιττού πλήθους αντιμεταθέσεων. Δηλαδή δεν υπάρχει μετάταξη που να είναι σύνθεση ταυτοχρόνως και ενός άρτιου και ενός περιττού πλήθους αντιμεταθέσεων.*

Απόδειξη. Έστω ότι για κάποιο $\sigma \in S_n$ είναι $\sigma = \prod_{i=1}^{2\kappa} \tau_i, \ (*)$ και $\sigma = \prod_{i=1}^{2\lambda+1} \tau'_i, \ (**)$, όπου οι τ_i και τ'_i είναι αντιμεταθέσεις, για κάθε i. Εφαρμόζοντας τον ομομορφισμό ε στις $(*)$ και $(**)$, έπεται $\varepsilon(\sigma) = (-1)^{2\kappa} = 1$ και $\varepsilon(\sigma) = (-1)^{2\lambda+1} = -1$. Άτοπο. □

Παρατήρηση 1.8.37. Ένας s–κύκλος $\gamma = \begin{pmatrix}x_1 & x_2 & \ldots & x_s\end{pmatrix}, s \geq 2$ είναι άρτια μετάταξη, όταν το μήκος του s είναι περιττός αριθμός και είναι περιττή μετάταξη όταν το μήκος του s είναι άρτιος αριθμός. Πράγματι από το Λήμμα 1.8.27, γνωρίζουμε ότι ένας s–κύκλος είναι σύνθεση $(s-1)$ το πλήθος αντιμεταθέσεων.

Για παράδειγμα οι κύκλοι μήκους 3 είναι άρτιες μετατάξεις.

Η εναλλάσσουσα ομάδα $\mathbb{A}_n$

Προφανώς, το υποσύνολο $\mathbb{A}_n$ των άρτιων μετατάξεων τής $(S_n, \circ), n \geq 2$, αποτελεί μια υποομάδα τής S_n, αφού είναι ένα μη κενό και πεπερασμένο σύνολο, κλειστό ως προς την πράξη τής S_n. Ωστόσο, υπάρχει ένας πολύ καλύτερος τρόπος για να το διαπιστώσουμε αυτό, ο οποίος οδηγεί σε πολύ ενδιαφέροντα συμπεράσματα.

Παρατηρούμε ότι ο πυρήνας $\ker \varepsilon = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}$ τού επιμορφισμού πρόσημου $\varepsilon : S_n \to \{1, -1\}$ αποτελείται ακριβώς από τις άρτιες μετατάξεις, δηλαδή ισούται με την υποομάδα $\mathbb{A}_n$ που είδαμε μόλις πιο πάνω.

Θεώρημα 1.8.38. *Το σύνολο $\mathbb{A}_n$ των άρτιων μετατάξεων τής $(S_n, \circ), n \geq 2$, είναι μια υποομάδα τής S_n, που είναι ορθόθετη και τής οποίας η τάξη ισούται με $\frac{n!}{2}$.*

Απόδειξη. Ήδη γνωρίζουμε ότι $\ker \varepsilon = \mathbb{A}_n$. Επειδή ο πυρήνας οποιουδήποτε ομομορφισμού είναι ορθόθετη υποομάδα, συμπεραίνουμε ότι $\mathbb{A}_n \trianglelefteq S_n$. Από το Πρώτο Θεώρημα Ισομορφίας, βλ. Θεώρημα 1.7.21, έχουμε ότι $S_n/\mathbb{A}_n = S_n/\ker \varepsilon \cong \operatorname{im} \varepsilon = \{1, -1\}$. Επομένως, $[S_n : \mathbb{A}_n] = [\operatorname{im} \varepsilon : 2] = 2$ και αφού $n! = [S_n : 1] = [S_n : \mathbb{A}_n : 1][\mathbb{A}_n : 1] = 2[\mathbb{A}_n : 1]$, συμπεραίνουμε ότι $[\mathbb{A}_n : 1] = \frac{n!}{2}$. □

Ορισμός 1.8.39. Η υποομάδα $\mathbb{A}_n$ τής $(S_n, \circ), n \geq 2$, ονομάζεται η *εναλλάσσουσα ομάδα* βαθμού n.

Στο επόμενο κεφάλαιο, βλ. για παράδειγμα υποενότητα 3.2.2, θα έχουμε την ευκαιρία να συζητήσουμε αρκετές φορές για την εναλλάσσουσα ομάδα $\mathbb{A}_n$. Εδώ θα παρουσιάσουμε μόνο το εξής στοιχειώδες αλλά σημαντικό αποτέλεσμα:

Πρόταση 1.8.40. *Η εναλλάσσουσα ομάδα $\mathbb{A}_4$, η οποία είναι τάξης 12, δεν διαθέτει υποομάδα τάξης 6.*

Απόδειξη. Ας υποθέσουμε ότι η $\mathbb{A}_4$ διαθέτει μια υποομάδα H τάξης 6. Ο δείκτης $[G : H] = 2$ και γι' αυτό για κάθε μετάταξη $\sigma \in A_4$, το τετράγωνό της σ^2 ανήκει στην H, βλ. Άσκηση A76. Η S_4 έχει οκτώ το πλήθος 3-κύκλους, οι οποίοι ανήκουν στην $\mathbb{A}_4$, αφού είναι άρτιες μετατάξεις. Επιπλέον, επειδή η τάξη οποιουδήποτε 3-κύκλου α ισούται με 3, έχουμε $\alpha = (\alpha^2)^2$. Συνεπώς, το $\alpha^2 \in H$ και κατόπιν επίσης το $\alpha \in H$. Άρα κάθε 3-κύκλος ανήκει στην H. Άτοπο! □

Ασκήσεις στις Ομάδες Μετατάξεων

Λυμένες Ασκήσεις

A 96. Να υπολογιστεί το πρόσημο $\varepsilon(\sigma)$ τής μετάταξης

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

Λύση. Μια παράσταση τής σ ως γινόμενο αποσυνδετών κύκλων είναι η $\sigma = \tau_1 \circ \tau_2 \circ \tau_3 \circ \tau_4$, όπου $\tau_1 = \begin{pmatrix} 1 & 9 \end{pmatrix}$, $\tau_2 = \begin{pmatrix} 2 & 8 \end{pmatrix}$, $\tau_3 = \begin{pmatrix} 3 & 7 \end{pmatrix}$ και $\tau_4 = \begin{pmatrix} 4 & 6 \end{pmatrix}$. Έχουμε:

$$\varepsilon(\sigma) = \varepsilon(\tau_1 \circ \tau_2 \circ \tau_3 \circ \tau_4) = \varepsilon(\tau_1)\varepsilon(\tau_2)\varepsilon(\tau_3)\varepsilon(\tau_4) = (-1)^4$$

και ως εκ τούτου, η σ είναι άρτια μετάταξη.

Α 97. Να δειχθεί η σ^2 είναι άρτια μετάταξη, για κάθε $\sigma \in S_n, n \geq 2$.

Λύση. Θεωρούμε τον επιμορφισμό πρόσημου $\varepsilon : S_n \to \{1, -1\}$. Όταν $\sigma \in S_n$, τότε $\varepsilon(\sigma^2) = \varepsilon(\sigma \circ \sigma) = \varepsilon(\sigma)^2$=1, αφού $\varepsilon(\sigma) = \pm 1$. Άρα, η σ^2 είναι άρτια μετάταξη.

Α 98. Να δειχθεί ότι η $(S_n, \circ), n \geq 2$, παράγεται από το σύνολο $\Sigma = \{\begin{pmatrix} i & i+1 \end{pmatrix} \mid 1 \leq i \leq n-1\}$.

Λύση. Θεωρούμε την υποομάδα $\langle\Sigma\rangle$, η οποία παράγεται από το σύνολο Σ. Αν δείξουμε ότι το υποσύνολο $T = \{\begin{pmatrix} 1 & i \end{pmatrix} \mid 2 \leq i \leq n\}$ τής S_n περιέχεται στην υποομάδα $\langle\Sigma\rangle$, τότε και υποομάδα $\langle T\rangle$ περιέχεται στη $\langle\Sigma\rangle$ και αφού $\langle T\rangle = S_n$, βλ. Πρόταση 1.8.30, θα συμπεράνουμε ότι επίσης $\langle\Sigma\rangle = S_n$.

Θα εκτελέσουμε μια απλή απόδειξη για τον ισχυρισμό *η μετάταξη* $\begin{pmatrix} i & i+1 \end{pmatrix}$ *ανήκει στην υποομάδα* $\langle\Sigma\rangle$.
Η $\begin{pmatrix} 1 & 2 \end{pmatrix}$ ανήκει ήδη στο Σ. Αφού η $\begin{pmatrix} 2 & 3 \end{pmatrix} \in \Sigma$, συμπεραίνουμε ότι η $\begin{pmatrix} 1 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 2 & 3 \end{pmatrix}^{-1} \in \langle\Sigma\rangle$. Συνεχίζοντας κατ' αυτόν τον τρόπο, θα δείξουμε ότι όταν η μετάταξη $\begin{pmatrix} 1 & i \end{pmatrix} \in \langle\Sigma\rangle, 2 \leq i \leq n-1$, τότε και η μετάταξη $\begin{pmatrix} 1 & i+1 \end{pmatrix} \in \langle\Sigma\rangle$.
Πράγματι, η $\begin{pmatrix} 1 & i+1 \end{pmatrix} = \begin{pmatrix} i & i+1 \end{pmatrix} \circ \begin{pmatrix} 1 & i \end{pmatrix} \circ \begin{pmatrix} i & i+1 \end{pmatrix}^{-1} \in \langle\Sigma\rangle$, αφού οι $\begin{pmatrix} i & i+1 \end{pmatrix}$ και $\begin{pmatrix} 1 & i \end{pmatrix} \in \langle\Sigma\rangle$. Άρα, κάθε $\begin{pmatrix} 1 & i \end{pmatrix}, 2 \leq i \leq n$ είναι στοιχείο τής $\langle\Sigma\rangle$ και ως εκ τούτου, $\langle\Sigma\rangle = S_n$.

Α 99. Να δειχθούν τα εξής:

(α′) Η $(S_n, \circ), n \geq 2$ παράγεται από το σύνολο $\mathrm{P} = \{\begin{pmatrix} 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & \ldots & n \end{pmatrix}\}$.

(β′) Η $(S_n, \circ), n \geq 2$ παράγεται από το σύνολο $\mathrm{P}' = \{\begin{pmatrix} i_1 & i_2 \end{pmatrix}, \begin{pmatrix} i_1 & i_2 & \ldots & i_n \end{pmatrix}\}$, όπου οι $\{i_1, i_2, \ldots, i_n\} = \{1, 2, \ldots, n\}$.

Λύση. (α′) Σύμφωνα και με όσα αναπτύξαμε στην προηγούμενη άσκηση, αρκεί να δείξουμε ότι κάθε στοιχείο τού συνόλου $\Sigma = \{\begin{pmatrix} i & i+1 \end{pmatrix} \mid 1 \leq i \leq n-1\}$ ανήκει στην υποομάδα $\langle\mathrm{P}\rangle$, διότι ήδη γνωρίζουμε ότι $\langle\Sigma\rangle = S_n$.
Έχουμε $\begin{pmatrix} 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \ldots & n \end{pmatrix}^{-1} \in \langle\mathrm{P}\rangle$. Συνεχίζοντας κατ' αυτόν τον τρόπο, θα δείξουμε ότι όταν η μετάταξη $\begin{pmatrix} i-1 & i \end{pmatrix} \in \langle\mathrm{P}\rangle, 2 \leq i \leq n-1$, τότε και η μετάταξη $\begin{pmatrix} i & i+1 \end{pmatrix} \in \langle\mathrm{P}\rangle$. Πράγματι, $\begin{pmatrix} i & i+1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & n \end{pmatrix} \circ \begin{pmatrix} i-1 & i \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \ldots & n \end{pmatrix}^{-1} \in \langle\mathrm{P}\rangle$. Άρα, $\langle\mathrm{P}\rangle = S_n$.
(β′) Θεωρούμε το στοιχείο $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$ και τον εσωτερικό αυτομορφισμό

$$\chi_\sigma : S_n \to S_n, \tau \mapsto \chi_\sigma(\tau) := \sigma \circ \tau \circ \sigma^{-1}$$

Ο αυτομορφισμός χ_σ εφαρμοσμένος στα στοιχεία τού συνόλου P δίνει $\chi_\sigma\left(\begin{pmatrix} 1 & 2 \end{pmatrix}\right) = \begin{pmatrix} i_1 & i_2 \end{pmatrix}$ και $\chi_\sigma\left(\begin{pmatrix} 1 & 2 & \ldots & n \end{pmatrix}\right) = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \end{pmatrix}$. Επομένως, $\chi_\sigma(\mathrm{P}) = \mathrm{P}'$ και ως εκ τούτου, $\langle \chi_\sigma(\mathrm{P})\rangle = \langle \mathrm{P}'\rangle$. Από την Άσκηση ΠΑ84, γνωρίζουμε ότι $\chi_\sigma(\langle \mathrm{P}\rangle) = \langle \chi_\sigma(\mathrm{P})\rangle$ και από το πρώτο μέρος τής παρούσας άσκησης, έχουμε $\langle \mathrm{P}\rangle = S_n$. Επομένως,

$$S_n = \chi_\sigma(S_n) = \chi_\sigma(\langle \mathrm{P}\rangle) = \langle \chi_\sigma(\mathrm{P})\rangle = \langle \mathrm{P}'\rangle.$$

Άρα, το σύνολο P' παράγει την S_n.

Α 100. Να βρεθούν οι κυκλικοί τύποι και οι τάξεις των στοιχείων τής $(S_4, \circ)$ και τής εναλλάσσουσας υποομάδας της $\mathbb{A}_4$. Κατόπιν να βρεθούν όλα τα στοιχεία τής

Λύση. Οι διαμερίσεις τού φυσικού αριθμού 4 είναι οι:

1	1	1	1
1	1	2	
1	3		
2	2		
4			

Έστω $\sigma \neq \mathrm{Id}_4$ τής S_4. Τότε η μετάταξη σ είναι ή ένας κύκλος μήκος 2 με $\circ(\sigma) = 2$ ή ένας κύκλος μήκους 3 με τάξη $\circ(\sigma) = 3$, ή σύνθεση δύο αποσυνδετών κύκλων μήκους δύο με $\circ(\sigma) = \text{ΕΚΠ}\{2, 2\} = 2$ ή ένας κύκλος μήκους 4 με $\circ(\sigma) = 4$.

Τα στοιχεία τής $\mathbb{A}_4$ είναι οι άρτιες μετατάξεις. Επομένως, η $\mathbb{A}_4$ αποτελείται από το ταυτοτικό στοιχείο Id_4, τους 3-κύκλους $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$, $\begin{pmatrix}2 & 1 & 3\end{pmatrix}$, $\begin{pmatrix}1 & 2 & 4\end{pmatrix}$, $\begin{pmatrix}2 & 1 & 4\end{pmatrix}$, $\begin{pmatrix}1 & 3 & 4\end{pmatrix}$, $\begin{pmatrix}3 & 1 & 4\end{pmatrix}$, $\begin{pmatrix}2 & 3 & 4\end{pmatrix}$ και $\begin{pmatrix}2 & 4 & 3\end{pmatrix}$ και τα γινόμενα από δύο αποσυνδετές αντιμεταθέσεις $\begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}$, $\begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}$, $\begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}$.

Α 101. Έστω ότι γ και δ είναι δύο κύκλοι μήκους ≥ 2 τής $(S_n, \circ)$, $n \geq 2$. Αν οι γ και δ είναι αποσυνδετοί και σ είναι οποιοδήποτε στοιχείο τής S_n, τότε οι συζυγείς κύκλοι $\sigma \circ \gamma \circ \rho^{-1}$ και $\sigma \circ \delta \circ \rho^{-1}$ είναι επίσης αποσυνδετοί.

Λύση. Έστω ότι $\gamma = \begin{pmatrix}x_1 & x_2 & \dots & x_s\end{pmatrix}$ και $\delta = \begin{pmatrix}y_1 & y_2 & \dots & y_t\end{pmatrix}$. Όταν $\sigma \in S_n$, τότε τα αντίστοιχα συζυγή στοιχεία είναι τα $\sigma \circ \gamma \circ \sigma^{-1} = \begin{pmatrix}\sigma(x_1) & \sigma(x_2) & \dots & \sigma(x_s)\end{pmatrix}$ και $\sigma \circ \delta \circ \sigma^{-1} = \begin{pmatrix}\sigma(y_1) & \sigma(y_2) & \dots & \sigma(y_t)\end{pmatrix}$, βλ. Πρόταση 1.8.23. Αν δεν ήταν αποσυνδετοί οι κύκλοι $\sigma \circ \gamma \circ \sigma^{-1}$ και $\sigma \circ \delta \circ \sigma^{-1}$, τότε η τομή των τροχιών $\{\sigma(x_1), \sigma(x_2), \dots, \sigma(x_s)\}$ και $\{\sigma(y_1), \sigma(y_2), \dots, \sigma(y_t)\}$ θα ήταν $\neq \emptyset$. Όμως, αν ήταν $\sigma(x_i) = \sigma(y_j), 1 \leq i \leq s, 1 \leq j \leq t$ κάποιο στοιχείο τής τομής, τότε θα ήταν $x_i = y_j$ και ως εκ τούτου, οι γ και δ δεν θα ήταν αποσυνδετοί. Άτοπο.

Α 102. Να δειχθεί ότι το σύνολο

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

είναι η μοναδική (ορθόθετη) υποομάδα τής εναλλάσσουσας ομάδας $\mathbb{A}_4$ τάξης 4.

Λύση. Είναι εύκολη η διαπίστωση ότι το V είναι υποομάδα τής $\mathbb{A}_4$, αφού το V είναι ένα πεπερασμένο υποσύνολο τής $\mathbb{A}_4$ κλειστό ως προς την πράξη «$\circ$» . Για παράδειγμα:

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

Θα δείξουμε ότι η V είναι η μοναδική υποομάδα τής $\mathbb{A}_4$ τάξης 4. Πράγματι, αν υπάρχει ακόμα μία υποομάδα K τής $\mathbb{A}_4$ με $[K:1] = 4$, τότε κάθε στοιχείο $\neq \mathrm{Id}_4$ τής K είναι τάξης 2 ή 4. Όμως η $\mathbb{A}_4$ δεν έχει στοιχεία τάξης 4, διότι τα μοναδικά στοιχεία τάξης 4 τής S_4 είναι οι κύκλοι μήκους τέσσερα, οι οποίοι είναι περιττές μετατάξεις. Ως εκ τούτου, κάθε στοιχείο $\neq \mathrm{Id}_4$ τής K θα ήταν τότε τάξης 2. Όμως όλα τα στοιχεία τής $\mathbb{A}_4$ τάξης 2 μαζί με το ταυτοτικό απαρτίζουν τη V. Άρα, $K = V$. Αφού η V είναι η μοναδική υποομάδα τής $\mathbb{A}_4$ που έχει τάξη 4, συμπεραίνουμε από την Άσκηση 71, ότι $V \trianglelefteq \mathbb{A}_4$.

Α 103. Να δειχθεί ότι η $\mathbb{A}_4$ είναι η μοναδική υποομάδα τής $(S_4, \circ)$ τάξης 12.

Λύση. Αν η S_4 είχε ακόμα μία ομάδα τάξης 12, τότε σύμφωνα με την Πόρισμα 1.4.18, η τομή $\mathbb{A}_4 \bigcap H \leq \mathbb{A}_4$ θα ήταν τάξης $[H:1]/2 = 6$. Άτοπο, αφού από την Πρόταση 1.8.40, γνωρίζουμε ότι η $\mathbb{A}_4$ δεν διαθέτει υποομάδα τάξης 6.

Α 104. Έστω ότι H είναι μια υποομάδα τής συμμετρικής ομάδας $(S_n, \circ), n \geq 3$. Αν η H περιέχει μια περιττή μετάταξη σ, τότε να δειχθεί ότι η H περιέχει μια υποομάδα K με δείκτη $[H:K] = 2$.

Λύση. Επειδή η $\mathbb{A}_n$ είναι μια ορθόθετη υποομάδα τής S_n, το σύνολο $H\mathbb{A}_n$ είναι υποομάδα τής S_n. Το πλήθος των στοιχείων τού συνόλου $\sigma\mathbb{A}_n \bigcup \mathbb{A}_n$ ισούται με $n! = [S_n:1]$, διότι τα σύνολα $\sigma\mathbb{A}_n$ και $\mathbb{A}_n$ διαμερίζουν την S_n, αφού η σ είναι περιττή μετάταξη. Άρα, $|\sigma\mathbb{A}_n| = [\mathbb{A}_n:1]$. Επομένως, $[H\mathbb{A}_n:1] = (n!/2) + (n!/2) = n!$ και $H\mathbb{A}_n = S_n$. Ως γνωστόν, βλ. Θεώρημα 1.4.17, $n! = [S_n:1] = [H\mathbb{A}_n:1] = \frac{[H:1][\mathbb{A}_n:1]}{[H \bigcap \mathbb{A}_n:1]}$. Συνεπώς, $\frac{[H:1]}{[H \bigcap \mathbb{A}_n:1]} = \frac{[S_n:1]}{[\mathbb{A}_n:1]} = 2$.

Προτεινόμενες Ασκήσεις

ΠΑ 93. Να δειχθεί ότι μια μετάταξη τής $(S_n, \circ), n \geq 2$ είναι περιττή, όταν σε οποιαδήποτε διάσπασή της σε γινόμενο αποσυνδετών κύκλων, το πλήθος των κύκλων άρτιου μήκους είναι περιττό. (Υπόδειξη: *Οι κύκλοι άρτιου μήκους είναι περιττές μετατάξεις.*)

ΠΑ 94. Να δειχθεί ότι το σύνολο

$$V = \left\{\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}\right\}$$

είναι ορθόθετη υποομάδα τής $(S_4, \circ)$,

ΠΑ 95. Έστω η συμμετρική ομάδα $(S_{13}, \circ)$ τού συνόλου $X = \{1, 2, \ldots, 13\}$. Ποιός είναι ο μικρότερος φυσικός, ο οποίος δεν είναι τάξη κάποιου στοιχείου τής S_{13}; Να δικαιολογήσετε την απάντησή σας.

ΠΑ 96. (α′) Να δειχθεί ότι η μετάταξη $\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix} \circ \begin{pmatrix}5 & 6 & 7 & 8\end{pmatrix} \in S_8$ είναι περιττή.

(β′) Να δειχθεί ότι η αντίστροφη μιας περιττής μετάταξης είναι περιττή.

Κεφάλαιο 2

Δράση Ομάδας επί ενός Συνόλου

2.1 Δράσεις και μετατακτικές Αναπαραστάσεις

Έστω $(G, \star)$ μια ομάδα και A ένα μη κενό σύνολο.

Ορισμός 2.1.1. Μια απεικόνιση $\varphi : G \times A \to A$, $(g, a) \mapsto \varphi((g, a))$ που ικανοποιεί τα:

$$\forall g_1, g_2 \in G, \forall a \in A, \varphi((g_1 \star g_2, a)) = \varphi\left((g_1, \varphi\left((g_2, a)\right))\right) \qquad (*)$$

και

$$\forall a \in A, \varphi((e_G, a)) = a, \text{ όπου } e_G \text{ το ουδέτερο στοιχείο τής } G \qquad (**)$$

ονομάζεται *δράση τής ομάδας G επί τού συνόλου A.*

Συμβολισμός. Συνήθως, γράφουμε $g\varphi a$ αντί τού $\varphi((g, a))$, όπου $g \in G, a \in A$. Έτσι, οι δύο προηγούμενες σχέσεις γράφονται:

$$\forall g_1, g_2 \in G, \forall a \in A, (g_1 g_2)\varphi a = g_1\varphi(g_2\varphi a) \qquad (*)$$

και

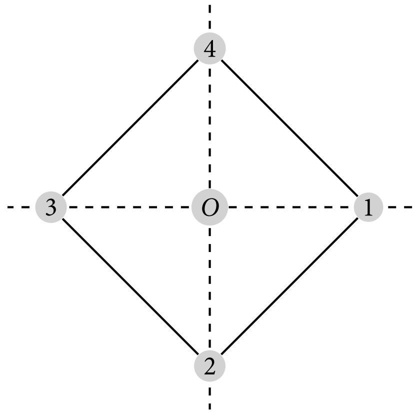
$$\forall a \in A, e_G\varphi a = a. \qquad (**)$$

(*Υπενθυμίζουμε ότι η παράθεση* $g_1 g_2$ το ένα δίπλα στο άλλο, δύο στοιχείων g_1, g_2 μιας ομάδας $(G, \star)$, παριστάνει το αποτέλεσμα τής πράξης $g_1 \star g_2$.)

Παράδειγμα 2.1.2. Θεωρούμε ένα τετράγωνο, βλ. Σχήμα 2.1, και τη διεδρική ομάδα D_4 των στερεών κινήσεών[1] του. Υπενθυμίζουμε, βλ. σελ. 18, ότι η πράξη τής D_4 είναι η σύνθεση των στερεών κινήσεων και ότι το σύνολο των στοιχείων τής D_4 περιγράφεται ως

$$D_4 = \{\mathrm{Id}_4, \tau, \rho, \rho^2, \rho^3, \tau \circ \rho, \tau \circ \rho^2, \tau \circ \rho^3\}.$$

[1] των ισομετριών τού χώρου που απεικονίζουν το τετράγωνο στον εαυτό του



Σχήμα 2.1:

όπου $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ είναι η στροφή κατά γωνία $\pi/4$ γύρω από τον άξονα, ο οποίος είναι κάθετος στο επίπεδο τού τετραγώνου, με φορά αυτήν που ακολουθούν κατά την κίνησή τους οι δείκτες τού ρολογιού
και $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ είναι ο κατοπτρισμός ως προς τον άξονα συμμετρίας που διέρχεται από τις κορυφές 1 και 3.
Το στοιχείο ρ είναι τάξης 4 και το στοιχείο τ είναι τάξης 2. Επιπλέον, $\rho \circ \tau = \tau \circ \rho^{-1}$.

Θεωρούμε το σύνολο $K = \{1, 2, 3, 4\}$ των κορυφών τού τετραγώνου, βλ. Σχήμα 2.1, και την απεικόνιση φ, που επάγεται από τις στερεές κινήσεις τού τετραγώνου επί τού συνόλου K, δηλαδή την

$$\varphi : D_4 \times K \to K, \ \ (\sigma, i) \mapsto \sigma\varphi i := \sigma(i).$$

Η φ είναι μια δράση τής διεδρικής ομάδας D_4 επί τού συνόλου $K = \{1, 2, 3, 4\}$ των κορυφών τού τετραγώνου, αφού

$$\forall \sigma, \sigma' \in D_4, \forall i \in K : (\sigma \circ \sigma')\varphi i = (\sigma \circ \sigma')(i) = \sigma(\sigma'(i)) = \sigma\varphi(\sigma'\varphi i)$$

και

$$\forall i \in K : (\mathrm{Id}_4, i) \mapsto \mathrm{Id}_4\varphi i = \mathrm{Id}_4(i) = i.$$

Θεωρούμε το σύνολο $\Delta = \{\delta_1 = \{1, 3\}, \delta_2 = \{2, 4\}\}$ των διαγωνίων τού τετραγώνου. Κάθε ένα από τα οκτώ στοιχεία σ τής D_4 απεικονίζει τις διαγώνιους τού τετραγώνου σε διαγώνιους και ως εκ τούτου ορίζεται η απεικόνιση

$$\psi : D_4 \times \Delta \to \Delta,$$

όπου

$$(\sigma, \{i,j\}) \mapsto \sigma\psi\{i,j\} := \{\sigma(i), \sigma(j)\}.$$

Η ψ είναι μια δράση τής D_4 επί τού συνόλου Δ.

Πράγματι, $\forall \sigma, \sigma' \in D_4, \forall \{i,j\} \in \Delta$ είναι

$$(\sigma \circ \sigma')\psi(\{i,j\}) = \{\sigma \circ \sigma'(i), \sigma \circ \sigma'(i)\} = \{\sigma(\sigma'(i)), \sigma(\sigma'(i))\} = \sigma\psi\{\sigma'(i), \sigma'(i)\}$$

και

$$\forall \{i,j\} \in \Delta : \mathrm{Id}_4\psi\{i,j\} = \{\mathrm{Id}_4(i), \mathrm{Id}_4(j)\} = \{i,j\}.$$

Αντίθετα, θεωρώντας το σύνολο $L = \{\ell_1 = \{1,2\}, \ell_2 = \{3,4\}\}$ δύο παράλληλων πλευρών τού τετραγώνου, παρατηρούμε ότι η απεικόνιση που επάγεται από τη δράση τής D_4 επί τού τετραγώνου δεν ορίζει μια δράση επί τού L, αφού η πλευρά $\rho(\ell_1) = \{\rho(1), \rho(2)\} = \{4,1\}$ δεν ανήκει στο σύνολο L.

Παρατήρηση 2.1.3. Προφανώς, όταν μια ομάδα $(G, \star)$ δρα επί ενός συνόλου A, τότε και κάθε υποομάδα $H \leq G$ δρα επί τού A, περιορίζοντας απλώς τη δράση τής G στην H.

Έστω A ένα μη κενό σύνολο και $(S_A, \circ)$ η συμμετρική ομάδα τού A, δηλαδή η ομάδα που απαρτίζεται από τις «$1-1$» και «επί» απεικονίσεις από το A στο A και έχει ως πράξη τη σύνθεση των απεικονίσεων.

Θεώρημα 2.1.4. *Αν $\varphi : G \times A \to G$ είναι μια δράση τής ομάδας G επί τού A, τότε η αντιστοιχία*

$$\begin{aligned} \mathrm{X}(\varphi) : G \to S_A, g \mapsto \mathrm{X}(\varphi)(g) : A &\to A \\ a &\mapsto \mathrm{X}(\varphi)(g)(a) := g\varphi a \end{aligned}$$

είναι ένας ομομορφισμός ομάδων.
Αν $\chi : G \to S_A$ είναι ένας ομομορφισμός ομάδων, τότε η απεικόνιση

$$\Phi(\chi) : G \times A \to A, \ \ (g,a) \mapsto g\Phi(\chi)a := \chi(g)(a)$$

είναι μια δράση τής G επί τού A.
Έστω ότι $\mathcal{D}(G,A)$ είναι το σύνολο δράσεων $\varphi : G \times A \to A$ και $\mathrm{Hom}(G, S_A)$ είναι το σύνολο των ομομορφισμών χ από την G στη συμμετρική ομάδα S_A τού A.
Οι απεικονίσεις

$$\mathrm{X} : \mathcal{D}(G,A) \to \mathrm{Hom}(G, S_A), \varphi \mapsto \mathrm{X}(\varphi)$$

και

$$\Phi : \mathrm{Hom}(G, S_A) \to \mathcal{D}(G,A), \chi \mapsto \Phi(\chi)$$

είναι η μία αντίστροφη τής άλλης.

Απόδειξη. Πρώτα, πρέπει να αποδείξουμε ότι η $X(\varphi)$ είναι μια καλά ορισμένη απεικόνιση, δηλαδή ότι $\forall g \in G$, η $X(\varphi)(g)$ είναι μια «1–1» και «επί» απεικόνιση και ως εκ τούτου ανήκει στην S_A.

Αν $a \in A$, τότε

$$X(\varphi)(g)(g^{-1}\varphi a) = g\varphi(g^{-1}\varphi a) = (gg^{-1})\varphi a = e_G \varphi a = a.$$

Ώστε, $\forall g \in G$, η $X(\varphi)(g)$ είναι «επί».

Έστω ότι $\exists a, a' \in A, g \in G$ με $X(\varphi)(g)(a) = X(\varphi)(g)(a')$. Τότε,

$$X(\varphi)(g)(a) = X(\varphi)(g)(a') \Leftrightarrow g\varphi a = g\varphi a' \Leftrightarrow g^{-1}\varphi(g\varphi a) = g^{-1}\varphi(g\varphi a') \Leftrightarrow$$
$$(g^{-1}g)\varphi a = (g^{-1}g)\varphi a' \Leftrightarrow e_G \varphi a = e_G \varphi a' \Leftrightarrow a = a'.$$

Ώστε, $\forall g \in G$, η $X(\varphi)(g)$ είναι «$1-1$» και τελικώς η $X(\varphi) : G \to S_A$ είναι μια καλά ορισμένη απεικόνιση.

Θα δείξουμε τώρα ότι $X(\varphi)$ είναι ένας ομομορφισμός ομάδων, δηλαδή ότι $\forall g_1, g_2 \in G$ οι απεικονίσεις $X(\varphi)(g_1g_2)$ και $X(\varphi)(g_1) \circ X(\varphi)(g_2)$ είναι ίσες. Πράγματι, $\forall a \in G$ έχουμε

$$X(\varphi)(g_1g_2)(a) = (g_1g_2)\varphi a = g_1\varphi(g_2\varphi a) = X(\varphi)(g_1)[(X(\varphi)(g_2)(a))] =$$
$$(X(\varphi)(g_1) \circ (X(\varphi)(g_2))(a).$$

Επομένως, $\forall \varphi \in \mathcal{D}(G, A)$ το $X(\varphi) : G \to S_A$ είναι ένας ομομορφισμός και ως εκ τούτου, ανήκει στο σύνολο $\mathrm{Hom}(G, S_A)$.

Τώρα θα αποδείξουμε ότι αν $\chi : G \to S_A$ είναι ένας ομομορφισμός ομάδων, τότε η απεικόνιση

$$\Phi(\chi) : G \times A \to A, \ \ (g, a) \mapsto g\Phi(\chi)a := \chi(g)(a)$$

είναι μια δράση τής G επί τού A.

Για κάθε $g_1, g_2 \in G$, $a \in A$, έχουμε:

$$(g_1g_2)\Phi(\chi)a = \chi(g_1g_2)(a) = (\chi(g_1) \circ \chi(g_2))(a) = \chi(g_1)(\chi(g_2)(a)) =$$
$$g_1\Phi(\chi)(g_2\Phi(\chi)a)$$

Επιπλέον, για κάθε $a \in A$, έχουμε:

$$e_G\Phi(\chi)a = \chi(e_G)(a) = \mathrm{Id}_A(a) = a.$$

Επομένως, $\forall \chi \in \mathrm{Hom}(G, S_A)$ η $\Phi(\chi)$ ανήκει στο σύνολο $\mathcal{D}(G, A)$.

Υπολείπεται να δείξουμε ότι οι απεικονίσεις

$$X : \mathcal{D}(G, A) \to \mathrm{Hom}(G, S_A), \varphi \mapsto X(\varphi)$$

και

$$\Phi : \mathrm{Hom}(G, S_A) \to \mathcal{D}(G, A), \chi \mapsto \Phi(\chi)$$

είναι η μία αντίστροφη τής άλλης, δηλαδή ότι $\forall \varphi \in \mathcal{D}(G, A)$ είναι $\Phi \circ X(\varphi) = \varphi$ και ότι $\forall \chi \in \mathrm{Hom}(G, S_A)$ είναι $X \circ \Phi(\chi) = \chi$.

Για κάθε $\varphi \in \mathcal{D}(G, A)$, το $\mathrm{X}(\varphi)$ ανήκει στο $\mathrm{Hom}(G, S_A)$ και το $\Phi(\mathrm{X}(\varphi))$ ανήκει στο $\mathcal{D}(G, A)$. Έχουμε:

$$\forall (g, a) \in G \times A : g\Phi(\mathrm{X}(\varphi))(a) = \mathrm{X}(\varphi)(g)(a) = g\varphi a.$$

Συνεπώς, η δράση $(\Phi \circ \mathrm{X})(\varphi) : G \times A \to A$ συμπίπτει με τη δράση $\varphi : G \times A \to A$. Επομένως, η $\Phi \circ \mathrm{X} : \mathcal{D}(G, A) \to \mathcal{D}(G, A)$ είναι η ταυτοτική απεικόνιση.

Για κάθε $\chi \in \mathrm{Hom}(G, S_A)$, το $\Phi(\chi)$ ανήκει στο $\mathcal{D}(G, A)$ και το $\mathrm{X}(\Phi(\chi))$ ανήκει στο $\mathrm{Hom}(G, S_A)$. Έχουμε:

$$\forall g \in G, \forall a \in A : \mathrm{X}(\Phi(\chi))(g)(a) = g\Phi(\chi)a = \chi(g)(a).$$

Συνεπώς, για κάθε $g \in G$, το στοιχείο $\mathrm{X}(\Phi(\chi))(g)$ τής συμμετρικής ομάδας S_A συμπίπτει με το στοιχείο τής $\chi(g)$. Επομένως, η $\mathrm{X} \circ \Phi : \mathrm{Hom}(G, S_A) \to \mathrm{Hom}(G, S_A)$ είναι η ταυτοτική απεικόνιση □

Ορισμός 2.1.5. Κάθε ομομορφισμός από μια ομάδα G στην ομάδα συμμετρίας S_A ενός συνόλου A ονομάζεται μια *μετατακτική αναπαράσταση* τής G.

Παρατήρηση 2.1.6. Το γεγονός ότι μια δράση χορηγεί έναν ομομορφισμό και αντιστρόφως, βοηθά στον προσδιορισμό *όλων των δράσεων* μιας ομάδας επί ενός συνόλου.

Για παράδειγμα, αν η G είναι η κυκλική ομάδα $(\mathbb{Z}_{25}, +)$ και A είναι ένα σύνολο με τέσσερα στοιχεία, τότε η μοναδική δράση τής $\mathbb{Z}_{25}$ που ορίζεται επί τού A είναι η τετριμμένη, δηλαδή η

$$\varphi : \mathbb{Z}_{25} \times A \to A, ([z], a) \mapsto [z]\varphi a := a, \forall [z] \in \mathbb{Z}_{25}, \forall a \in A,$$

αφού οποιαδήποτε δράση χορηγεί έναν ομομορφισμό $\mathbb{Z}_{25} \to S_A$ και στη συγκεκριμένη περίπτωση, επειδή ο $\text{ΜΚΔ}(25, 4!) = 1$, υπάρχει μόνον ο τετριμμένος ομομορφισμός από την $\mathbb{Z}_{25}$ στην S_A , βλ. Πόρισμα 1.7.23.

Ορισμός 2.1.7. *Πυρήνας μιας δράσης* $\varphi : G \times A \to G$ είναι το υποσύνολο

$$K_\varphi := \{g \in G \mid g\varphi a = a, \forall a \in A\}.$$

Λήμμα 2.1.8. *Ο πυρήνας K_φ μιας δράσης $\varphi : G\times A \to G$ συμπίπτει με τον πυρήνα* $\ker \mathrm{X}(\varphi)$ *τού επαγόμενου ομομορφισμού $\mathrm{X}(\varphi) : G \to S_A$ και συνεπώς είναι μια ορθόθετη υποομάδα τής G.*

Απόδειξη. Πράγματι,

$$g \in K_\varphi \Leftrightarrow \forall a \in A, g\varphi a = a \Leftrightarrow \mathrm{X}(\varphi)(g) = \mathrm{Id}_A \Leftrightarrow g \in \ker \mathrm{X}(\varphi).$$

□

Ορισμός 2.1.9. Μια δράση $\varphi : G \times A \to G$ ονομάζεται *πιστή*, αν ο πυρήνας της είναι η τετριμμένη υποομάδα $K_\varphi = \{e_G\}$.

Όταν η G δρα πιστά επί του A, τότε η G μπορεί να θεωρηθεί ως υποομάδα τής συμμετρικής ομάδας S_A, αφού $K_\varphi = \ker \mathrm{X}(\varphi) = \{e_G\}$.
Προσέξτε, ότι οποιαδήποτε δράση $\varphi : G \times A \to G$ χορηγεί μια πιστή δράση τής πηλικο-ομάδας G/K_φ επί τού A, ως ακολούθως

$$\overline{\varphi} : G/K_\varphi \times A \to G, \ \ (gK_\varphi, a) \ \ \mapsto (gK_\varphi)\overline{\varphi}a := g\varphi a$$

Προτείνουμε να ελέγξει μόνος του ο αναγνώστης, πρώτα ότι η $\overline{\varphi}$ είναι μια καλά ορισμένη απεικόνιση και κατόπιν ότι ορίζει μια πιστή δράση τής G/K_φ επί τού A.

Παράδειγμα 2.1.10. Έστω $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ το σύνολο των πολυωνύμων n μεταβλητών με ακέραιους συντελεστές και $(S_n, \circ)$ η συμμετρική ομάδα τού συνόλου $X = \{1, 2, \ldots, n\}$. Στην Ενότητα 1.8 θεωρήσαμε την απεικόνιση

$$\begin{aligned}\star : S_n \times \mathbb{Z}[x_1, x_2, \ldots, x_n] &\to \mathbb{Z}[x_1, x_2, \ldots, x_n],\\ f(x_1, x_2, \ldots, x_n) &\mapsto \sigma \star f(x_1, x_2, \ldots, x_n) := f(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)}).\end{aligned}$$

και διαπιστώσαμε ότι $\forall f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ είναι $\mathrm{Id}_n \star f = f$ και $\forall \sigma, \tau \in S_n$ είναι $(\sigma \circ \tau) \star f = (\sigma \star (\tau \star f))$. Επομένως, η απεικόνιση «$\star$» αποτελεί μια δράση τής S_n επί τού $\mathbb{Z}[x_1, x_2, \ldots, x_n]$. Η δράση «$\star$» τής S_n επί τού $\mathbb{Z}[x_1, x_2, \ldots, x_n]$ είναι πιστή. Πράγματι, όταν σ είναι στοιχείο τού πυρήνα τής «$\star$», τότε $\sigma \star f = f, \forall f \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$. Ιδιαιτέρως, για τα πολυώνυμα $f_i := x_i, 1 \leq i \leq n$, θα πρέπει να ισχύει $f_i = \sigma \star f_i, \forall i, 1 \leq i \leq n$, δηλαδή $x_i = x_{\sigma(i)}, \forall i, 1 \leq i \leq n$. Συνεπώς, $i = \sigma(i), \forall i, 1 \leq i \leq n$ και ως εκ τούτου, $\sigma = \mathrm{Id}_n$.

2.2 Τροχιές και Σταθεροποιητές

Έστω ότι $\varphi : G \times A \to A$ μια δράση τής G επί τού A και ότι $\mathcal{R}_\varphi \subseteq A \times A$ είναι η σχέση επί τού A, η οποία ορίζεται ως εξής:

$$\text{Το ζεύγος } (a, b) \in A \text{ ανήκει στο } \mathcal{R}_\varphi \iff \exists g \in G : g\varphi a = b.$$

Λήμμα 2.2.1. *Το $\mathcal{R}_\varphi \subseteq A \times A$ είναι μια σχέση ισοδυναμίας επί τού A*

Απόδειξη. Πράγματι,
(α′) $\forall a \in A$, το $(a, a) \in \mathcal{R}_\varphi$, αφού $e_G \varphi a = a$.
(β′) Αν $(a, b) \in \mathcal{R}_\varphi$, τότε $\exists g \in G$ με $b = g\varphi a$. Συνεπώς, $g^{-1}\varphi b = a$ και $(b, a) \in \mathcal{R}_\varphi$.
(γ′) Αν $(a, b) \in \mathcal{R}_\varphi$ και $(b, c) \in \mathcal{R}_\varphi$, τότε $\exists g_1, g_2 \in G$ με $b = g_1\varphi a$ και $c = g_2\varphi b$. Επομένως, $c = g_2\varphi(g_1\varphi a) = (g_2 g_1)\varphi a$ και γι' αυτό $(a, c) \in \mathcal{R}_\varphi$. □

Έστω ότι $\varphi : G \times A \to A$ είναι μια δράση τής G επί τού A, ότι $\mathcal{R}_\varphi$ είναι η αντίστοιχη σχέση ισοδυναμίας και ότι a είναι ένα στοιχείο τού A.

Ορισμός 2.2.2. Ονομάζουμε *τροχιά* τού στοιχείου $a \in A$ την κλάση ισοδυναμίας $[a]_{\mathcal{R}_\varphi}$ τού a ως προς τη σχέση $\mathcal{R}_\varphi$.

Προφανώς,
$$[a]_{\mathcal{R}_\varphi} = \{g\varphi a \mid g \in G\}.$$
Θα συμβολίζουμε την κλάση $[a]_{\mathcal{R}_\varphi}$ ως $G\varphi a$.

Προσέξτε ότι επειδή η $\mathcal{R}_\varphi$ είναι σχέση ισοδυναμίας, το σύνολο A διαμερίζεται στις τροχιές του $G\varphi a$, δηλαδή

$$A = \bigcup_{a\in A} G\varphi a \text{ και αν } a, b \in A \text{ με } G\varphi a \bigcap G\varphi b \neq \emptyset, \text{ τότε } G\varphi a = G\varphi b.$$

Ορισμός 2.2.3. Ένα στοιχείο $a \in A$ ονομάζεται *φ-σταθερό* ως προς τη δράση $\varphi : G\times A \to A$, όταν η τροχιά του $G\varphi a$ αποτελείται μόνο από το στοιχείο a.

Με άλλα λόγια το $a \in A$ είναι φ-σταθερό στοιχείο ως προς τη δράση φ, αν $g\varphi a = a, \forall g \in G$.

Ορισμός 2.2.4. Η G δρα *μεταβατικώς* επί τού συνόλου A , όταν υπάρχει ακριβώς μία τροχιά.

Συνεπώς, αν η G δρα μεταβατικώς επί τού A και α, β είναι οποιαδήποτε στοιχεία τού A, τότε $\exists g \in G$ με $g\varphi\alpha = \beta$.

Ορισμός 2.2.5. Ονομάζουμε *σταθεροποιητή* τού στοιχείου $a \in A$ το υποσύνολο
$$G_a = \{g \in G \mid g\varphi a = a\} \subseteq G.$$

Λήμμα 2.2.6. (α′) *Ο σταθεροποιητής G_a είναι μια υποομάδα τής G.*

(β′) *Αν a και b είναι δυο στοιχεία τού A, τα οποία ανήκουν στην ίδια τροχιά, τότε οι αντίστοιχοι σταθεροποιητές τους G_a και G_b είναι συζυγείς υποομάδες τής G.*

(Υπενθυμίζουμε ότι όταν H και K είναι δύο υποομάδες μιας ομάδας G, τότε η K ονομάζεται ***συζυγής*** *τής H, αν υπάρχει $g \in G$ με $K = gHg^{-1}$. Επειδή τότε και $H = g^{-1}Kg$, έπεται ότι η H είναι συζυγής τής K.*
Οι συζυγείς υποομάδες μιας ομάδας έχουν πάντοτε το ίδιο πλήθος στοιχείων, αφού για κάθε $g \in G$, η απεικόνιση $\chi_g : G \to G, a \mapsto gag^{-1}$ είναι ένας εσωτερικός αυτομορφισμός τής G, βλ. Ορισμό 1.7.42. Γι αυτό, ο χ_g χορηγεί μια αμφιμονοσήμαντη αντιστοιχία μεταξύ οποιουδήποτε υποσυνόλου M τής G και τής εικόνας του gMg^{-1}.)

Απόδειξη. (α′) Το σύνολο G_a δεν είναι κενό, αφού $e_G \in G_a$. Επιπλέον, αν $g_1, g_2 \in G_a$, τότε $g_1\varphi a = a$ και $g_2\varphi a = a$. Από την τελευταία ισότητα προκύπτει επίσης ότι $g_2^{-1}\varphi a = a$. Τώρα έχουμε:
$$(g_1g_2^{-1})\varphi a = g_1\varphi(g_2^{-1}\varphi a) = g_1\varphi a = a$$
Ώστε, το G_a είναι μια υποομάδα τής G, βλ. Λήμμα 1.3.6.
(β′) Αφού τα a, b ανήκουν στη ίδια τροχιά, υπάρχει κάποιο $g \in G$ με $g\varphi a = b$. Προτρέπουμε τον αναγνώστη να αποδείξει μόνος του ότι $G_b = gG_ag^{-1}$. □

Με τη βοήθεια τής έννοιας τού σταθεροποιητή, μπορούμε να περιγράψουμε εκ νέου τον πυρήνα K_φ, οποιασδήποτε δράσης $\varphi : G \times A \to A$.

Παρατήρηση 2.2.7. Ο πυρήνας K_φ τής φ ισούται με την τομή $\bigcap_{a\in A} G_a$ όλων των σταθεροποιητών G_a καθώς το a διατρέχει τα στοιχεία τού A.

Πράγματι, όταν $g \in K_\varphi$, τότε $g\varphi a = a, \forall a \in A$ και ως εκ τούτου, $g \in \bigcap_{a\in A} G_a$. Αντίστροφα, όταν $g \in \bigcap_{a\in A} G_a$, τότε $g\varphi a = a, \forall a \in G$ και συνεπώς $g \in K_\varphi$.

Θεώρημα 2.2.8. *Έστω ότι $\varphi : G\times A \to G$ είναι μια δράση τής G επί τού A και ότι G_a είναι ο σταθεροποιητής ενός στοιχείου $a \in A$. Υπάρχει μια «$1-1$» και «επί» απεικόνιση μεταξύ τού συνόλου $G/G_a = \{gG_a \mid g \in G\}$ των αριστερών πλευρικών κλάσεων τού σταθεροποιητή G_a στη G και τής τροχιάς $G\varphi a$.*

Απόδειξη. Θεωρούμε την αντιστοιχία

$$G/G_a \longrightarrow G\varphi a, \;\; gG_a \;\; \mapsto \;\; g\varphi a.$$

Η συγκεκριμένη αντιστοιχία είναι μια καλά ορισμένη απεικόνιση, δηλαδή ανεξάρτητη από την επιλογή τού αντιπροσώπου g τής πλευρικής κλάσης gG_a. Πράγματι, αν $g_1G_a = g_2G_a$, τότε $g_2^{-1}g_1 \in G_a$. Συνεπώς,

$$\begin{aligned}&(g_2^{-1}g_1)\varphi a = a \Leftrightarrow g_2\varphi[(g_2^{-1}g_1)\varphi a] = g_2\varphi a \Leftrightarrow\\ &((g_2g_2^{-1})g_1)\varphi a = g_2\varphi a \Leftrightarrow g_1\varphi a = g_2\varphi a.\end{aligned}$$

Ο ίδιος ακριβώς υπολογισμός δείχνει ότι η απεικόνιση είναι «$1-1$», αφού από $g_1\varphi a = g_2\varphi a$, έπεται $(g_2^{-1}g_1)\varphi a = a$. Άρα, $g_2^{-1}g_1 \in G_a$ και ως εκ τούτου, $g_1G_a = g_2G_a$. Τέλος, η απεικόνιση είναι «επί», αφού το στοιχείο $g\varphi a$ τής τροχιάς $G\varphi a$ είναι εικόνα τής αριστερής πλευρικής κλάσης gG_a. □

Το επόμενο συμπέρασμα είναι άμεσο αλλά ιδιαιτέρως σημαντικό:

Πόρισμα 2.2.9. *Το πλήθος των στοιχείων τής τροχιάς $G\varphi a$ τού $a \in A$ ισούται με τον δείκτη $[G : G_a]$ τού σταθεροποιητή G_a τού στοιχείου $a \in G$.*

Παράδειγμα 2.2.10. Θεωρούμε τη δράση τής ομάδας $G = S_4$ επί τού συνόλου $\mathbb{Z}[x_1, x_2, x_3, x_4]$ των πολυωνύμων στις τέσσερεις μεταβλητές με ακέραιους συντελεστές, βλ. Παράδειγμα 2.1.10:

$$\begin{aligned}&\star : G \times \mathbb{Z}[x_1, x_2, x_3, x_4] \to \mathbb{Z}[x_1, x_2, x_3, x_4],\\ &(\sigma, f(x_1, x_2, x_3, x_4)) \mapsto \sigma * f := f(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)}).\end{aligned}$$

Θα υπολογίσουμε τους σταθεροποιητές και τις τροχιές των πολυωνύμων $f(x_1, x_2, x_3, x_4) = x_1 + x_2$ και $g(x_1, x_2, x_3, x_4) = x_1x_2 + x_3x_4$.

Για λόγους ευκολίας υπενθυμίζουμε ότι τα $4!$ το πλήθος στοιχεία τής $G = S_4$ είναι τα:

$$\begin{aligned}&\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix}, \begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 3 & 2\end{pmatrix},\\ &\begin{pmatrix}1 & 2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4 & 2\end{pmatrix}, \begin{pmatrix}1 & 3 & 4\end{pmatrix}, \begin{pmatrix}1 & 4 & 3\end{pmatrix}, \begin{pmatrix}2 & 3 & 4\end{pmatrix}, \begin{pmatrix}2 & 4 & 3\end{pmatrix},\\ &\begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}, \begin{pmatrix}1 & 2 & 4 & 3\end{pmatrix},\\ &\begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix}, \begin{pmatrix}1 & 3 & 4 & 2\end{pmatrix}, \begin{pmatrix}1 & 4 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 4 & 3 & 2\end{pmatrix}.\end{aligned}$$

Για το πολυώνυμο f: Υπολογίζουμε τον σταθεροποιητή $G_f = \{\sigma \in G \mid \sigma(x_1 + x_2) = x_{\sigma(1)} + x_{\sigma(2)} = x_1 + x_2\}$. Παρατηρούμε. ότι $\sigma \in G_f$, αν και μόνο αν, $\sigma(1) = 1$ και $\sigma(2) = 2$ ή $\sigma(1) = 2$ και $\sigma(2) = 1$. Επομένως, $G_f = \{\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}\}$. Από το Πόρισμα 2.2.9, συμπεραίνουμε ότι η τροχιά $G \star f$ έχει $[G : G_f] = 24/4 = 6$ στοιχεία. Τα στοιχεία $x_1+x_2, x_1+x_3, x_2+x_3, x_1+x_4, x_2+x_4, x_3+x_4$ ανήκουν στην $G\star f$. (Για παράδειγμα, το $x_3 + x_4 = x_{\sigma(1)} + x_{\sigma(2)}$ με $\sigma = \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}$.) Αφού το πλήθος αυτών των στοιχείων ισούται με 6, συμπεραίνουμε ότι $G\star f = \{x_1 + x_2, x_1 + x_3, x_2 + x_3, x_1 + x_4, x_2 + x_4, x_3 + x_4\}$.

Για το πολυώνυμο g: Εδώ θα υπολογίσουμε πρώτα την τροχιά $G \star g$. Παρατηρούμε, ότι η τροχιά $G\star g$ ισούται με το σύνολο $L = \{x_{i_1}x_{i_2} + x_{i_3}x_{i_4} \mid \{i_1, i_2, i_3, i_4\} = \{1, 2, 3, 4\}\}$. Πράγματι για κάθε $\sigma \in G$, το $x_{\sigma(1)}x_{\sigma(2)} + x_{\sigma(3)}x_{\sigma(4)} \in L$ και αντίστροφα κάθε $x_{i_1}x_{i_2} + x_{i_3}x_{i_4} \in L$, ανήκει και στην τροχιά $G \star g$, διότι $x_{i_1}x_{i_2} + x_{i_3}x_{i_4} = \sigma \star g$, όπου $\sigma = \begin{pmatrix}1 & 2 & 3 & 4\\ i_1 & i_2 & i_3 & i_4\end{pmatrix}$. Ως εκ τούτου, $G \star g = \{x_1x_2 + x_3x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3\}$. Αφού ο δείκτης $[G : G_g]$ τού σταθεροποιητή G_g ισούται με $|G \star g| = 3$, συμπεραίνουμε ότι $[G_g : 1] = [G : 1]/[G : G_g] = 24/3 = 8$. Ένας απλός υπολογισμός δίνει

$$\begin{aligned} G_g = \{&\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4 & 2 & 3\end{pmatrix},\\ &\begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}\}\end{aligned}$$

2.2.1 Το Θεώρημα Burnside

Αν $g \in G$, τότε συμβολίζουμε με A^g το υποσύνολο τού A που αποτελείται από τα στοιχεία τού $a \in A$ που παραμένουν σταθερά κάτω από τη φ-δράση τού $g \in G$, δηλαδή

$$A^g = \{a \in A \mid g\varphi a = a\}$$

Θεώρημα 2.2.11 (Burnside). *Έστω ότι $\varphi : G \times A \to G$ είναι δράση μιας **πεπερασμένης ομάδας** G επί ενός **πεπερασμένου** συνόλου A.*
Το πλήθος k των τροχιών στις οποίες διαμερίζεται το σύνολο A ισούται με

$$k := \frac{1}{[G : 1]} \sum_{g \in G} |A^g|.$$

Απόδειξη. Θα υπολογίσουμε με δύο διαφορετικούς τρόπους το πλήθος των στοιχείων τού συνόλου

$$\mathcal{L} = \{(g, a) \in G \times A \mid g\varphi a = a\}.$$

Για κάθε $g \in G$, θεωρούμε το σύνολο των στοιχείων $a \in A$ που παραμένουν αναλλοίωτα από τη φ-δράση τού g, δηλαδή θεωρούμε το σύνολο A^g. Συνεπώς,

$$|\mathcal{L}| = \sum_{g \in G} |A^g|. \tag{*}$$

Για κάθε $a \in A$, θεωρούμε τον σταθεροποιητή τού a, δηλαδή την υποομάδα $G_a = \{g \in G \mid g\varphi a = a\}$. Επομένως,

$$|\mathcal{L}| = \sum_{a \in A} [G_a : 1].$$

Αν το πλήθος των τροχιών ισούται με k, τότε το A διαμερίζεται στις k διαφορετικές τροχιές $G\varphi a_1, G\varphi a_2, \ldots, G\varphi a_k$. Επομένως,

$$|\mathcal{L}| = \sum_{a\in A}[G_a : 1] = \sum_{i=1}^{k} \sum_{a\in G\varphi a_i} [G_a : 1], \tag{**}$$

αφού από το Λήμμα 2.2.6 γνωρίζουμε ότι όλοι οι σταθεροποιητές που αντιστοιχούν στα στοιχεία a τής τροχιάς $G\varphi a_i$ έχουν το ίδιο πλήθος στοιχείων, δηλαδή

$$\forall a \in G\varphi a_i, [G_a : 1] = [G_{a_i} : 1].$$

Από το Θεώρημα 2.2.8 γνωρίζουμε ότι το πλήθος των στοιχείων τής τροχιάς $G\varphi a_i$ ισούται με τον δείκτη $[G : G_{a_i}] = \frac{[G:1]}{[G_{a_i}:1]}$.
Συνεπώς, η σχέση (**) γίνεται

$$|\mathcal{L}| = \sum_{a\in A}[G_a : 1] = \sum_{i=1}^{k} \sum_{a\in G\varphi a_i} [G_a : 1] = \sum_{i=1}^{k} \frac{[G : 1]}{[G_{a_i} : 1]}[G_{a_i} : 1] = k[G : 1]. \tag{***}$$

Από τις σχέσεις (***) και (*) προκύπτει ότι

$$k[G : 1] = \sum_{g\in G} |A^g| \implies k = \frac{1}{[G : 1]} \sum_{g\in G} |A^g|.$$

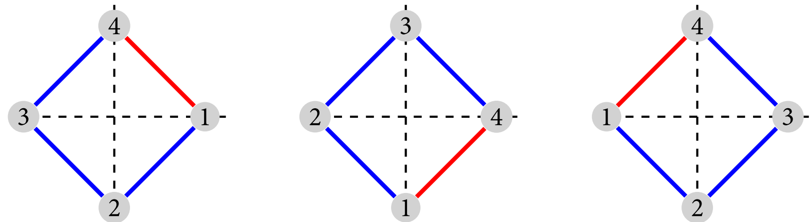
□

Πόρισμα 2.2.12. *Όταν ότι μια πεπερασμένη ομάδα $(G, \star)$ με $[G : 1] \geq 2$ δρα μεταβατικά επί ενός πεπερασμένου συνόλου A με $|A| \geq 2$, τότε υπάρχει κάποιο $g \in G$, το οποίο δεν διατηρεί σταθερό κανένα στοιχείο $a \in A$.*

Απόδειξη. Από το Θεώρημα Burnside, βλ. Θεώρημα 2.2.11, έχουμε $1 = \frac{1}{[G:1]} \sum_{g\in G} |A^g|, (*)$. Θεωρώντας ξεχωριστά το $A^{e_G} = \{a \in A \mid e_G\varphi a = a\} = A$, η $(*)$ επαναδιατυπώνεται ως $1 = \frac{1}{[G:1]}(|A| + \sum_{g\in G, g\neq e_G} |A^g|)$. Αν διέθετε κάθε στοιχείο $g \in G$ τουλάχιστον ένα φ-σταθερό στοιχείο, τότε θα ήταν $1 \geq \frac{1}{[G:1]}(|A| + [G : 1] - 1) = 1 + \frac{|A|-1}{[G:1]}$ και ως εκ τούτου, $0 \geq |A| - 1$. Άρα, $|A| = 1$, το οποίο είναι άτοπο, λόγω τής υπόθεσης. □

Ας δούμε τώρα μια ενδιαφέρουσα εφαρμογή τού Θεωρήματος Burnside:

***Εφαρμογή* 2.2.13.** *Θεωρούμε ένα τετράγωνο τού οποίου κάθε πλευρά τη χρωματίζουμε κόκκινη ή μπλε. Δύο τέτοια χρωματισμένα τετράγωνα λέμε ότι δεν διαφέρουν ουσιαστικώς, αν είτε περιστρέφοντας είτε αναποδογυρίζοντας το ένα από αυτά προκύπτει το άλλο χρωματισμένο τετράγωνο, βλ. Σχήμα 2.2.*



Αρχικό τετράγωνο. — Από το αρχικό κατόπιν στροφής κατά $\pi/4$ από αριστερά προς τα δεξιά. — Από το αρχικό κατόπιν κατοπτρισμού ως προς τον άξονα 4–2.

Σχήμα 2.2: Τα ανωτέρω τρία χρωματισμένα τετράγωνα δεν διαφέρουν ουσιαστικώς.

Θα υπολογίσουμε το πλήθος των ουσιαστικώς διαφορετικών τετραγώνων εφαρμόζοντας το Θεώρημα Burnside.

Έστω A το σύνολο των χρωματισμένων τετραγώνων. Το A αποτελείται από 2^4 στοιχεία, αφού κάθε πλευρά τού τετραγώνου μπορεί να χρωματιστεί κόκκινη ή μπλε.

Στο A δρα η διεδρική ομάδα D_4, αφού αυτή ακριβώς η ομάδα περιστρέφει η αναποδογυρίζει το τετράγωνο και το πλήθος των χρωματισμένων τετραγώνων που διαφέρουν ουσιαστικά συμπίπτει με το πλήθος k των τροχιών τού A κάτω από τη δράση τής D_4.
Η D_4 αποτελείται από τα στοιχεία:

$$\mathrm{Id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \text{ στροφή κατά } \pi/4 \text{ από αριστερά προς τα δεξιά,}$$

$$\rho^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \text{ στροφή κατά } \pi/2, \rho^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \text{ στροφή κατά } 3\pi/4,$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \text{ κατοπτρισμός ως προς τον άξονα } 4-2,$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ κατοπτρισμός ως προς τον άξονα } 3-1,$$

$$\begin{aligned} \mu &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} && \text{κατοπτρισμός ως προς τον άξονα διερχόμενο} \\ & && \text{από τα μέσα των } 3-4 \text{ και } 2-1, \\ \nu &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} && \text{κατοπτρισμός ως προς τον άξονα διερχόμενο} \\ & && \text{από τα μέσα των } 1-4 \text{ και } 2-3. \end{aligned}$$

Για κάθε $g \in D_4$, θα υπολογίσουμε το πλήθος $|A^g|$ των στοιχείων τού A^g.

(α′) Προφανώς, $|A^{\mathrm{Id}}| = 2^4$, αφού κάθε στοιχείο τού A παραμένει αναλλοίωτο από το ταυτοτικό στοιχείο τής D_4.

(β′) Το $|A^{\rho}|$ ισούται με 2, αφού για να ανήκει ένα στοιχείο τού A στο A^{ρ} θα πρέπει όλες οι πλευρές του να έχουν το ίδιο χρώμα, αφού διαφορετικά τουλάχιστον μια πλευρά θα απεικονιζόταν σε μια πλευρά διαφορετικού χρώματος. Επειδή διαθέτουμε δύο χρώματα, έχουμε $|A^{\rho}| = 2$.

(γ′) Το $|A^{\rho^2}|$ ισούται με 4. Εδώ ένα στοιχείο τού A ανήκει στο A^{ρ^2} ακριβώς τότε, όταν οι απέναντι πλευρές του τετραγώνου έχουν το ίδιο χρώμα, αφού κατά την περιστροφή κατά $\pi/2$ απεικονίζεται κάθε πλευρά στην απέναντί της. Συνεπώς υπάρχουν δύο επιλογές χρώματος για τη μία πλευρά (ας πούμε την $1-4$) και δύο για μια γειτονική της (ας πούμε την $1-2$).

(δ′) Το $|A^{\rho^3}|$ ισούται με 2. Η επιχειρηματολογία είναι αντίστοιχη τής περίπτωσης A^{ρ}.

(ε′) Το $|A^{\sigma}|$ ισούται με 2^2. Εδώ, για να ανήκει ένα χρωματισμένο τετράγωνο στο A^{σ}, οφείλουν οι πλευρές $1-4$ και $3-4$ να έχουν το ίδιο χρώμα καθώς επίσης και οι πλευρές $2-3$ και $1-2$.

(στ′) Το $|A^{\tau}|$ ισούται με 2^2. Η επιχειρηματολογία είναι αντίστοιχη τής περίπτωσης A^{σ}.

(ζ′) Το $|A^{\mu}|$ ισούται με 2^3. Εδώ παρατηρούμε ότι οι πλευρές $3-4$ και $1-2$ απεικονίζονται μέσω τού μ στον εαυτό τους, ενώ οι πλευρές $1-4$ και $2-3$ εναλλάσσονται. Συνεπώς, οι τελευταίες οφείλουν να έχουν το ίδιο χρώμα. Γι' αυτό έχουμε δύο επιλογές χρώματος για την πλευρά $3-4$, δύο επιλογές χρώματος για την πλευρά $1-2$ και δύο επιλογές χρώματος (ας πούμε) για την πλευρά $1-4$. Το χρώμα τής πλευράς $2-3$ οφείλει να είναι το ίδιο με το χρώμα τής πλευράς $1-4$.

(η′) Το $|A^{\nu}|$ ισούται με 2^3. Η επιχειρηματολογία είναι αντίστοιχη τής περίπτωσης A^{μ}.

Τώρα εφαρμόζοντας το Θεώρημα Burnside παίρνουμε

$$\begin{aligned} k = & \frac{1}{[D_4:1]}\left\{|A^{\mathrm{Id}}| + |A^{\rho}| + |A^{\rho^2}| + |A^{\rho^3}| + |A^{\sigma}| + |A^{\tau}| + |A^{\mu}| + |A^{\nu}|\right\} = \\ & \frac{1}{8}\left\{2^4 + 2 + 4 + 2 + 2^2 + 2^2 + 2^3 + 2^3\right\} = 6. \end{aligned}$$

Ώστε υπάρχουν έξι ουσιαστικώς διαφορετικά χρωματισμένα τετράγωνα.

2.3 Δράση Ομάδας επί Υποσυνόλων της και Πλευρικών Κλάσεών της

2.3.1 Αριστερή Δράση

Θεωρούμε μια ομάδα $(G, \star)$ και την απεικόνιση

$$\ell : G \times G \to G, (g, \alpha) \mapsto g\ell\alpha := g \star \alpha.$$

Μπορεί πολύ εύκολα να επαληθευθεί ότι η ℓ συνιστά μια δράση τής G επί τού εαυτού της, αφού κατ' ουσίαν η επαλήθευση βασίζεται στα αξιώματα που διέπουν την πράξη «$\star$» τής ομάδας.
Ως συνήθως, θα σημειώνουμε με $g\alpha$ το αποτέλεσμα $g \star \alpha$ τής πράξης «$\star$» στα $g, \alpha \in G$.

2.3.2 Δράση στις αριστερές πλευρικές Κλάσεις

Έστω ότι $H \leq G$ είναι μια υποομάδα τής G και $G/H = \{\alpha H \mid \alpha \in G\}$ το σύνολο των αριστερών πλευρικών κλάσεων τής H στην G.
Παρατηρούμε ότι η αντιστοιχία

$$\pi_H : G \times G/H \to G/H, (g, \alpha H) \mapsto g\pi_H \alpha H := g\alpha H$$

είναι ανεξάρτητη από την επιλογή τού αντιπροσώπου α τής πλευρικής κλάσης αH και συνεπώς είναι μια καλά ορισμένη απεικόνιση.
Πράγματι,

$$\forall g, \alpha_1, \alpha_2 \in G, \alpha_1 H = \alpha_2 H \Leftrightarrow g\alpha_1 H = g\alpha_2 H \text{ (γιατί;)}.$$

Επιπλέον,

$$\forall g_1, g_2 \in G, \alpha H \in G/H, (g_1g_2)\pi_H \alpha H = (g_1g_2)\alpha H = g_1(g_2\alpha H) = g_1\pi_H(g_2\pi_H\alpha H),$$
$$\forall \alpha H \in G/H, e_G\pi_H\alpha H = (e_G\alpha)H = \alpha H, (e_G \text{ το ουδέτερο τής } G).$$

Επομένως, η π_H είναι μια δράση τής G επί τού συνόλου G/H των αριστερών πλευρικών κλάσεων τής H στη G.

Παρατήρηση 2.3.1. Επιλέγοντας ως H την τετριμμένη υποομάδα $\{e_G\}$, διαπιστώνουμε ότι η δράση π_H συμπίπτει κατ' ουσίαν με τη δράση ℓ, αφού $\forall \alpha \in G$, οι πλευρικές κλάσεις αH συμπίπτουν με τα μονοσύνολα $\{\alpha\}$.

Θεώρημα 2.3.2. (α$'$) *Η δράση $\pi_H : G \times G/H \to G/H$ είναι μεταβατική.*

(β$'$) *Ο σταθεροποιητής G_{aH} τής αριστερής πλευρικής κλάσης aH ισούται με aHa^{-1}.*

(γ$'$) *Ο πυρήνας τής δράσης π_H ισούται με την υποομάδα $\bigcap_{\alpha \in G} \alpha H \alpha^{-1}$, η οποία είναι η μεγαλύτερη (ως προς τη σχέση υποσυνόλου «$\subseteq$») ορθόθετη (κανονική) υποομάδα τής G που περιέχεται στην H.*

Απόδειξη. (α$'$) Αν $\alpha H, \beta H \in G/H$, τότε επιλέγοντας $g = \beta\alpha^{-1} \in G$ έχουμε $g\alpha H = \beta H$, δηλαδή $g\pi_H\alpha H = \beta H$ και συνεπώς η π_H είναι μια μεταβατική δράση.
(β$'$)

$$g \in G_{aH} \Leftrightarrow g\pi_H aH = aH \Leftrightarrow gaH = aH \Leftrightarrow a^{-1}ga \in H \Leftrightarrow g \in aHa^{-1}.$$

(γ$'$) Από την Παρατήρηση 2.2.7 γνωρίζουμε ότι ο πυρήνας K_{π_H} ισούται με $\bigcap_{aH \in G/H} G_{aH}$, όπου G_{aH} είναι ο σταθεροποιητής τής αριστερής πλευρικής κλάσης aH.
Προφανώς, $\bigcap_{aH \in G/H} G_{aH} = \bigcap_{a \in G} G_{aH}$, διότι $\forall b \in aH$ είναι $bH = aH$ και ως εκ τούτου $G_{aH} = G_{bH}$. Άρα, $K_{\pi_H} = \bigcap_{a \in G} G_{aH}$. Επειδή τώρα $G_{aH} = aHa^{-1}$, συμπεραίνουμε ότι

$K_{\pi_H} = \bigcap_{a\in G} aHa^{-1}$. Αφού ο πυρήνας τής δράσης π_H ισούται με τον πυρήνα τού επαγόμενου ομομορφισμού $\mathrm{X}(\pi_H) : G \to S_{G/H}$, βλ. Θεώρημα 2.1.4, έπεται ότι ο K_{π_H} είναι ορθόθετη υποομάδα τής G.
Αν $N \leq H$ είναι μια ορθόθετη υποομάδα τής G που περιέχεται στην H, τότε $\forall \alpha \in G$, $\alpha^{-1}N\alpha = N \leq H$. Συνεπώς, $\forall \alpha \in G$, $N \leq \alpha H\alpha^{-1}$ και επομένως $N \leq \bigcap_{\alpha\in G} \alpha H\alpha^{-1}$. □

Το προηγούμενο αναδιατυπώνεται με τη βοήθεια τού Θεωρήματος 2.1.4 στο

Θεώρημα 2.3.3. *Έστω ότι $(G, \star)$ είναι μια ομάδα, ότι H είναι μια υποομάδα της και ότι $(S_{G/H}, \circ)$ είναι η συμμετρική ομάδα τού συνόλου G/H των αριστερών πλευρικών κλάσεων τής H στην G. Τότε υπάρχει ένας ομομορφισμός $\chi : G \to S_{G/H}$, τού οποίου ο πυρήνας $\ker \chi$ περιέχει οποιαδήποτε ορθόθετη υποομάδα $N \trianglelefteq G$ τής G με $N \leq H$.*

Πόρισμα 2.3.4 (Θεώρημα Cayley). *Κάθε ομάδα $(G, \star)$ είναι ισόμορφη προς μια υποομάδα τής συμμετρικής ομάδας $(S_G, \circ)$.*

Απόδειξη. Θεωρούμε την τετριμμένη υποομάδα $H = \{e_G\}$ τής G και τον επαγόμενο ομομορφισμό ομάδων
$$\mathrm{X}(\pi_{\{e_G\}}) : G \to S_{G/\{e_G\}}.$$
Σύμφωνα με το Θεώρημα 2.3.2, ο πυρήνας $K_{\pi_H} = \ker \mathrm{X}(\pi_{\{e_G\}})$ τής δράσης π_H ισούται με
$$\bigcap_{\alpha\in G} \alpha H\alpha^{-1} = \bigcap_{\alpha\in G} \alpha\{e_G\}\alpha^{-1} = \{e_G\}.$$
Επομένως, ο $\mathrm{X}(\pi_{\{e_G\}})$ είναι ένας μονομορφισμός ομάδων και γι' αυτό η G είναι ισόμορφη προς μια υποομάδα τής $S_{G/\{e_G\}}$. Αλλά η $S_{G/\{e_G\}}$ μπορεί να ταυτιστεί με την S_G, αφού το σύνολο των αριστερών πλευρικών κλάσεων τής $\{e_G\}$ στην G, δηλαδή το $G/\{e_G\} = \{\alpha\{e_G\} \mid \alpha \in G\}$, μπορεί να ταυτιστεί με το σύνολο $G = \{\alpha \mid \alpha \in G\}$ των στοιχείων τής G. □

Πόρισμα 2.3.5. *Έστω ότι $(G, \star)$ είναι μια ομάδα πεπερασμένης τάξης. Αν υπάρχει μια γνήσια υποομάδα $H < G$ με την ιδιότητα: ο αριθμός $[G : H]!$ να μην διαιρείται από την τάξη $[G : 1]$ τής ομάδας, τότε η H περιέχει μια μη τετριμμένη ορθόθετη υποομάδα τής G.*

Απόδειξη. Θεωρούμε τη δράση $\pi_H : G \times G/H \to G/H$ και τον επαγόμενο ομομορφισμό ομάδων $\mathrm{X}(\pi_H) : G \to S_{G/H}$. Από το Θεώρημα 2.3.2 γνωρίζουμε ότι ο πυρήνας π_H τής δράσης π_H, ο οποίος ισούται με $\ker \mathrm{X}(\pi_H)$ περιέχεται στην υποομάδα H.

Η πηλικοομάδα $G/\ker \mathrm{X}(\pi_H)$ είναι ισόμορφη προς μια υποομάδα τής $S_{G/H}$ και αφού το πλήθος των στοιχείων τού συνόλου G/H ισούται με $[G : H]$, η τάξη τής $S_{G/H}$ ισούται με $[G : H]!$. Σύμφωνα με το Θεώρημα Lagrange, η τάξη $[G : \ker \mathrm{X}(\pi_H)]$ τής $G/\ker \mathrm{X}(\pi_H)$ είναι ένας διαιρέτης τής τάξης $[G : H]!$ τής $S_{G/H}$.
Αν ήταν ο $\ker \mathrm{X}(\pi_H) = \{e_G\}$, τότε η τάξη $[G : \ker \mathrm{X}(\pi_H)] = [G : 1]$ θα διαιρούσε τον αριθμό $[G : H]!$. Αυτό όμως έχει αποκλειστεί από την υπόθεση. Επομένως, η ορθόθετη υποομάδα $\ker \mathrm{X}(\pi_H)$ τής G, που όπως γνωρίζουμε περιέχεται στην H, είναι μη τετριμμένη, αφού περιέχει γνήσια την $\{e_G\}$. □

Παράδειγμα 2.3.6. Κάθε ομάδα $(G, \star)$ τάξης $80 = 2^4 5$, διαθέτει μια μη τετριμμένη ορθόθετη υποομάδα. Πράγματι, από τα Θεωρήματα Sylow που θα συναντήσουμε στην ενότητα 3.1, συμπεραίνουμε ότι η G διαθέτει μια υποομάδα H τάξης 2^4. Η τάξη $[G : 1] = 80$ δεν διαιρεί τον αριθμό $[G : H]! = 5! = 120$. Επομένως, η H περιέχει μια μη τετριμμένη ορθόθετη υποομάδα τής G.

Πόρισμα 2.3.7. *Έστω ότι $(G, \star)$ είναι μια ομάδα πεπερασμένης τάξης. Αν υπάρχει μια γνήσια υποομάδα $H \leq G$ με δείκτη $[G : H] = p$, όπου p είναι ο μικρότερος πρώτος διαιρέτης τής τάξης τής G, τότε η H είναι μια ορθόθετη υποομάδα τής G.*

Απόδειξη. Θεωρούμε, όπως προηγουμένως τη δράση $\pi_H : G \times G/H \to G/H$ και τον επαγόμενο ομομορφισμό ομάδων $\mathrm{X}(\pi_H) : G \to S_{G/H}$. Από το Θεώρημα 2.3.2 γνωρίζουμε ότι $\ker \mathrm{X}(\pi_H) \leq H$. Θα δείξουμε ότι $\ker \mathrm{X}(\pi_H) = H$.

Αφού $G/\ker \mathrm{X}(\pi_H) \cong \mathrm{im}\,(\mathrm{X}(\pi_H))$, συμπεραίνουμε ότι ο δείκτης $[G : \ker \mathrm{X}(\pi_H)]$ είναι ένας διαιρέτης τής τάξης $[G : H]! = p!$ τής συμμετρικής ομάδας $S_{G/H}$. Αλλά $[G : \ker \mathrm{X}(\pi_H)] = [G : H][H : \ker \mathrm{X}(\pi_H)]$. Συνεπώς, ο $[G : H][H : \ker \mathrm{X}(\pi_H)] = p[H : \ker \mathrm{X}(\pi_H)]$ είναι διαιρέτης τού $p!$ και ως εκ τούτου ο $[H : \ker \mathrm{X}(\pi_H)]$ είναι διαιρέτης τού $(p-1)!$. Αν ήταν $[H : \ker \mathrm{X}(\pi_H)] > 1$, τότε και κάθε πρώτος διαιρέτης q τού $[H : \ker \mathrm{X}(\pi_H)]$, ο οποίος είναι πάντοτε διαιρέτης τής τάξης $[G : 1]$, θα ήταν επίσης διαιρέτης τού $(p-1)!$. Όμως τέτοιος πρώτος q δεν μπορεί να υπάρχει, αφού τότε θα είχαμε $q < p$. Ώστε, $[H : \ker \mathrm{X}(\pi_H)] = 1$ και $H = \ker \mathrm{X}(\pi_H)$. □

Το προηγούμενο πόρισμα αποτελεί τη γενίκευση, στην περίπτωση των πεπερασμένων ομάδων, τής πολύ γνωστής πρότασης ότι *κάθε υποομάδα H μια ομάδας G με $[G : H] = 2$ είναι ορθόθετη*. Ας δούμε μια ενδιαφέρουσα εφαρμογή του:

***Εφαρμογή* 2.3.8.** *Όταν $(G, \star)$ μια ομάδα τάξης p^n, $n \in \mathbb{N}$, όπου ο p είναι πρώτος αριθμός, τότε κάθε υποομάδα H με δείκτη $[G : H] = p$ είναι ορθόθετη υποομάδα τής G. Συνεπώς, κάθε ομάδα τάξης p^2 διαθέτει μια ορθόθετη υποομάδα τάξης p.*

Απόδειξη. Ο p είναι μικρότερος πρώτος διαιρέτης τής τάξης τής G, αφού η $[G : 1]$ δεν έχει άλλους πρώτους διαιρέτες. Σύμφωνα με το προηγούμενο πόρισμα, κάθε υποομάδα H με δείκτη $[G : H] = p$ είναι ορθόθετη.

Ας δούμε τώρα τι συμβαίνει όταν $[G : 1] = p^2$.

Αν η G έχει κάποιο στοιχείο τάξης p^2, τότε η G είναι κυκλική και σε κάθε διαιρέτη d τής τάξης της, έχει μια υποομάδα H τάξης d, η οποία προφανώς είναι ορθόθετη, αφού η G είναι αβελιανή. Εδώ, οι μοναδικοί διαιρέτες τής τάξης είναι οι $1, p, p^2$. Επομένως, υπάρχει υποομάδα H τάξης p, που είναι ορθόθετη.

Αν η G δεν έχει κάποιο στοιχείο τάξης p^2, τότε κάθε $a \in G$, $a \neq e_G$, έχει τάξη p και ο δείκτης τής κυκλικής υποομάδας $\langle a \rangle$ ισούται με $p^2/p = p$. Επομένως, η $\langle a \rangle$ είναι ορθόθετη υποομάδα τής G. □

Θα εφαρμόσουμε τη θεωρία των δράσεων ομάδων, για να αποδείξουμε εκ νέου, το επόμενο το πολύ χρήσιμο αποτέλεσμα, τού οποίου μια διαφορετική απόδειξη έχουμε ήδη δώσει στο Θεώρημα 1.4.17.

Πρόταση 2.3.9. *Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και $H, K \leq G$ δύο υποομάδες τής G.*
Το πλήθος $|HK|$ των στοιχείων τού συνόλου $HK = \{hk \mid h \in H, k \in K\}$ ισούται με

$$|HK| = \frac{[H:1][K:1]}{[H \bigcap K:1]}.$$

Απόδειξη. Θεωρούμε το σύνολο $G/K = \{gK \mid g \in G\}$ των αριστερών πλευρικών κλάσεων τής K στην G. Η απεικόνιση

$$\varphi : H \times G/K \to G/K, (h, gK) \quad \mapsto \quad h\varphi gK := hgK$$

είναι μια δράση τής H επί τού συνόλου G/K. (Πρόκειται για τον περιορισμό στην H τής δράσης π_K τής ομάδας G στο σύνολο των αριστερών πλευρικών κλάσεων G/K.)

Το σύνολο HK ισούται με την ένωση $\bigcup_{h \in H} hK$. Παρατηρούμε ότι τα σύνολα $hK, h \in H$ είναι ακριβώς τα στοιχεία τής τροχιάς $\mathcal{O}_H(K)$ τού στοιχείου $eK = K \in G/K$ ως προς τη δράση φ τής H.
Επειδή η τροχιά $\mathcal{O}_H(K)$ περιέχεται στο σύνολο G/K το οποίο είναι πεπερασμένο, έπεται ότι και η τροχιά $\mathcal{O}_H(K)$ αποτελείται από πεπερασμένο το πλήθος στοιχεία, ας πούμε ότι $\mathcal{O}_H(K) = \{h_1K, h_2K, \ldots, h_\ell K\}$.
Συνεπώς,

$$HK = \bigcup_{h \in H} hK = \bigcup_{i=1}^{\ell} h_iK, \quad \text{όπου } \ell \text{ το πλήθος των στοιχείων τής τροχιάς } \mathcal{O}_H(K).$$

Παρατηρούμε ότι αν $i \neq j$, τότε $h_iK \bigcap h_jK = \emptyset$, αφού πρόκειται για διαφορετικές αριστερές πλευρικές κλάσεις τής K στην G. Επιπλέον, επειδή το πλήθος των στοιχείων οποιασδήποτε αριστερής πλευρικής κλάσης hK ισούται με $[K:1]$, έπεται ότι

$$|HK| = \left| \bigcup_{i=1}^{\ell} h_iK \right| = \sum_{i=1}^{\ell} |h_iK| = \ell[K:1]. \tag{*}$$

Αλλά το πλήθος ℓ των στοιχείων τής τροχιάς $\mathcal{O}_H(K)$ ισούται με τον δείκτη $[H : H_{eK}]$, όπου $H_{eK} = \{h \in H \mid heK = eK\}$ είναι ο σταθεροποιητής τής κλάσης eK ως προς τη δράση φ τής H.
Τώρα, $H_{eK} = \{h \in H \mid heK = eK\} = \{h \in H \mid h \in K\} = H \bigcap K$ και έτσι από τη σχέση (*) έπεται

$$|HK| = [H : H_{eK}][K:1] = [H : H \bigcap K][K:1] = \frac{[H:1][K:1]}{[H \bigcap K:1]}.$$

□

Ασκήσεις στις Δράσεις, τις Τροχιές και τους Σταθεροποιητές

Λυμένες Ασκήσεις

Α 105. Έστω S_X η συμμετρική ομάδα ενός μη κενού συνόλου X με πλήθος στοιχείων $|X| \geq 2$.

(α′) Να δειχθεί ότι η αντιστοιχία $\varphi : S_X \times X \to X, (\sigma, x) \mapsto \sigma\varphi x := \sigma(x)$ αποτελεί μια δράση τής S_X επί τού X. (Η φ ονομάζεται η *φυσιολογική δράση* τής S_X επί τού X.) Να δειχθεί ότι η δράση φ είναι μεταβατική και να υπολογιστεί ο πυρήνας K_φ τής φ.

(β′) Έστω ότι $X = \{1, 2, 3, 4\}$ και η δράση $\varphi : S_4 \times X \to X$ τής S_4 επί τού X που ορίστηκε προηγουμένως. Θεωρούμε τις υποομάδες τής S_4:

$$V = \{\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}\} \text{ και}$$
$$H = \{\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix}, \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}\}.$$

Να υπολογιστούν οι τροχιές και οι σταθεροποιητές των στοιχείων τού X που προκύπτουν από τον περιορισμό τής δράσης φ στις υποομάδες V και H αντιστοίχως.

Λύση. (α′) Για κάθε $x \in X$, είναι $\mathrm{Id}_n(x) = x$ και για κάθε $\sigma, \tau \in S_n$ και κάθε $x \in X$ είναι

$$(\sigma \circ \tau)\varphi x = (\sigma \circ \tau)(x) = \sigma(\tau(x)) = \sigma\varphi(\tau(x)) = \sigma\varphi(\tau\varphi x).$$

Επομένως, η φ είναι μια δράση τής S_n επί τού X.

Θα δείξουμε ότι για κάθε[2] $i \in X$, η τροχιά $G\varphi i$ ισούται με το σύνολο X, από όπου θα προκύψει ότι η φ είναι μεταβατική δράση. Πράγματι, όταν $i, j \in X, i \neq j$, τότε η απεικόνιση $\tau : X \to X$ με $\tau(i) = j, \tau(j) = i$ και $\tau(x) = x, \forall x \in X, x \neq i, j$ ανήκει στην S_n και επομένως το $j \in G\varphi i$. Αφού επιπλέον, $i \in G\varphi i$, συμπεραίνουμε ότι $X \subseteq G\varphi i$ και ως εκ τούτου, $G\varphi i = X$.

Ένα $\sigma \in S_n$ ανήκει στον πυρήνα K_φ, αν και μόνο αν, $\forall x \in X, \sigma(x) = \sigma\varphi x = x$, αν και μόνο αν, $\sigma = \mathrm{Id}_n$. Επομένως, $K_\varphi = \{\mathrm{Id}_n\}$.

(β′) Για την V: Η τροχιά $V\varphi 1$ τού 1 συμπίπτει με ολόκληρο το σύνολο X. Πράγματι, επειδή $\begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}(1) = 2$, συμπεραίνουμε ότι το $2 \in V\varphi 1$. Όμοια το $3 \in V\varphi 1$, διότι $\begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}(1) = 3$ και με τον ίδιο τρόπο συμπεραίνουμε ότι και το $4 \in V\varphi 1$.

Ο σταθεροποιητής V_1 τού 1 ισούται με $\{\mathrm{Id}_4\}$, αφού δεν υπάρχει στοιχείο τής V που να διατηρεί σταθερό το 1 με εξαίρεση το Id_4. Κάθε στοιχείο που ανήκει στην τροχιά $V\varphi 1$ τού 1, έχει έναν σταθεροποιητή συζυγή προς τον σταθεροποιητή V_1 τού 1. Αλλά οποιαδήποτε συζυγής υποομάδα τής τετριμμένης υποομάδας είναι και πάλι η τετριμμένη υποομάδα. Επομένως $\{\mathrm{Id}_4\} = V_1 = V_2 = V_3 = V_4$.

Για την H: Εδώ η τροχιά $H\varphi 1 = \{1, 2\}$ και η τροχιά $H\varphi 3 = \{3, 4\}$. Ο σταθεροποιητής H_1 τού 1 ισούται με την υποομάδα $\{\mathrm{Id}_4, \begin{pmatrix}3 & 4\end{pmatrix}\}$. Ο σταθεροποιητής H_2 τού 2 ισούται με την υποομάδα $\{\mathrm{Id}_4, \begin{pmatrix}3 & 4\end{pmatrix}\} = H_1$. Ο $H_3 = \{\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix}\}$ και ο $H_4 = \{\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix}\}$. Προσέξτε ότι ο σταθεροποιητής H_2 τού 2 είναι μια υποομάδα τής H συζυγής προς την H_1, αφού τα 1 και 2 ανήκουν στην ίδια τροχιά. Οι συζυγείς υποομάδες τής H_1 είναι οι $\sigma H_1 \sigma^{-1}$ με $\sigma \in H$. Όμως η μοναδική συζυγής τής H_1 είναι η ίδια η H_1 και επομένως ο σταθεροποιητής τού H_2 τού 2 είναι η υποομάδα H_1. Με την ίδια ακριβώς επιχειρηματολογία διαπιστώνουμε ότι $H_3 = H_4$.

[2] Φυσικά, είναι αρκετό να εκτελέσουμε την απόδειξη μόνο για κάποιο $i \in X$, αφού οι τροχιές απαρτίζουν μια διαμέριση τού X.

Α 106. Να δειχθεί ότι η $(S_3, \circ)$ δεν μπορεί να δράσει μεταβατικά επί ενός συνόλου A με πλήθος στοιχείων $|A| = 5$.

Λύση. Αν η S_3 δρούσε μεταβατικά επί τού A, τότε θα υπήρχε μόνο μία τροχιά, η οποία θα ήταν ίση με A. Σύμφωνα με Πόρισμα 2.2.9, θα έπρεπε το 5 να ήταν διαιρέτης τού $3! = 6$.

Α 107. Έστω ότι $\varphi : G \times A \to A$ είναι μια δράση μιας ομάδας $(G, \star)$ επί ενός συνόλου A. Έστω ότι η G είναι κυκλική με $G = \langle g \rangle$. Να δειχθεί το στοιχείο $a \in A$ είναι φ-σταθερό, αν και μόνο αν, $g\varphi a = a$.

Λύση. Όταν το $a \in A$ είναι φ-σταθερό, τότε προφανώς $g\varphi a = a$.

Αντίστροφα, έστω ότι για κάποιο $a \in A$, είναι $g\varphi a = a$. Βέβαια, τότε επίσης είναι $g^{-1}\varphi a = a$, διότι $a = e_G\varphi a = (g^{-1}g)\varphi a = g^{-1}\varphi(g\varphi a) = g^{-1}\varphi a$.

Παρατηρούμε ότι $g^2\varphi a = g\varphi(g\varphi a) = a$ και γενικά ότι $g^n\varphi a = a, \forall n \in \mathbb{N} \cup \{0\}$. Όμοια, ισχύει ότι $(g^{-1})^n\varphi a = a, \forall n \in \mathbb{N}$, διότι $g^{-1}\varphi a = a$.

Επειδή η G είναι κυκλική, κάθε $h \in G$ είναι μια ακέραια δύναμη τού g και ως εκ τούτου, $h\varphi a = a$. Επομένως, το $a \in A$ είναι φ-σταθερό.

Α 108. Έστω $(\mathcal{Q}_8, \circ)$ η τετρανιακή ομάδα, βλ. Άσκηση ΠΑ26. Να δειχθούν τα εξής:

(α′) Η $\mathcal{Q}_8$ είναι ισόμορφη προς μια υποομάδα τής συμμετρικής ομάδας $(S_8, \circ)$.

(β′) Η $\mathcal{Q}_8$ δεν μπορεί να είναι ισόμορφη προς μια υποομάδα τής συμμετρικής ομάδας $(S_7, \circ)$.

Λύση. (α′) Από το Θεώρημα Cayley, βλ. Πόρισμα 2.3.4, γνωρίζουμε ότι η τετρανιακή ομάδα $\mathcal{Q}_8$ είναι ισόμορφη προς μια ομάδα τής $(S_{\mathcal{Q}_8}, \circ)$. Επειδή η τάξη $[\mathcal{Q}_8 : 1] = 8$, συμπεραίνουμε ότι η $\mathcal{Q}_8$ είναι ισόμορφη προς μια υποομάδα τής S_8.
(β′) Κατ' αρχάς θα δείξουμε ότι η $\mathcal{Q}_8$ δεν μπορεί να δράσει πιστά σε ένα σύνολο A με πλήθος στοιχείων $|A| = 7$. Πράγματι, έστω ότι $\varphi : \mathcal{Q}_8 \times A \to A$ είναι μια δράση τής τετρανιακής ομάδας $\mathcal{Q}_8$ επί ενός συνόλου A με $|A| = 7$. Παρατηρούμε ότι αν $\mathcal{Q}_8\varphi a$ είναι η τροχιά ενός $a \in A$, τότε το πλήθος των στοιχείων τής τροχιάς είναι ίσο ή με 1 ή με 2 ή με 2^2, επειδή $|\mathcal{Q}_8\varphi a| = [G : G_a] = 2^\kappa \leq |A| = 7, 0 \leq \kappa \leq 3$, όπου G_a είναι ο σταθεροποιητής τού a. Επομένως, ο σταθεροποιητής G_a έχει τάξη $[G : 1]/[G : G_a]$ ίση ή με 8 ή με 4 ή με 2. Επειδή, η $\mathcal{Q}_8$ έχει μια μοναδική υποομάδα τάξης 2, την $\{E, -E\}$ και επειδή ο πυρήνας K_φ τής δράσης φ, βλ. Παρατήρηση 2.2.7, ισούται με $\bigcap_{a \in A} G_a$, συμπεραίνουμε ότι $\{E, -E\} \leq K_\varphi$ και ως εκ τούτου, ο K_φ είναι πάντοτε $\neq \{E\}$.

Αν η $\mathcal{Q}_8$ ήταν ισόμορφη προς μια υποομάδα τής $(S_7, \circ)$, τότε θα υπήρχε ένας μονομορφισμός $\iota : \mathcal{Q}_8 \to S_7, \iota \in \mathrm{Hom}(\mathcal{Q}_8, S_7)$, ο οποίος θα έδινε μια πιστή δράση $\Phi(\iota) : \mathcal{Q}_8 \times \{1, 2, \ldots, 7\} \to \{1, 2, \ldots, 7\}$, βλ. Θεώρημα 2.1.4. Αυτό όμως είναι αδύνατο, διότι όπως είδαμε ο πυρήνας οποιασδήποτε δράσης τής $\mathcal{Q}_8$ επί ενός συνόλου με επτά στοιχεία είναι $\neq \{E\}$.

Προτεινόμενες Ασκήσεις

ΠΑ 97. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα, η οποία έχει μια υποομάδα H με $[G : H] = 5$. Να δειχθεί ότι η G διαθέτει μια ορθόθετη υποομάδα K με δείκτη $[G : K]$ πολλαπλάσιο τού 5 και διαιρέτη τού 5!.

ΠΑ 98. Έστω ότι $(S_4, \circ)$ είναι η συμμετρική ομάδα τού συνόλου $X = \{1, 2, 3, 4\}$ και ότι $\varphi : S_4 \times X \to X$ είναι η (φυσιολογική) δράση τής S_4 επί τού X, που ορίστηκε στην Άσκηση Α105.
Για καθεμία από τις υποομάδες $H = \langle\begin{pmatrix}1 & 2 & 3\end{pmatrix}\rangle$, $K = \langle\begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}\rangle$ και $\mathbb{A}_4$ τής S_4, να προσδιοριστούν οι τροχιές τού συνόλου X και οι σταθεροποιητές κάθε στοιχείου $x \in X$, ως προς τη δράση τής H, τής K και αντιστοίχως τής $\mathbb{A}_4$. Για καθεμία από τις $H, K, \mathbb{A}_4$ να επαληθευτεί το Θεώρημα 2.2.8.

ΠΑ 99. Έστω ότι $n \geq 2$ και ότι $\varphi : S_n \times X \to X$ είναι η φυσιολογική δράση τής συμμετρικής ομάδας S_n επί τού συνόλου $X = \{1, 2, \ldots, n\}$, βλ. Άσκηση Α105.

(α′) Έστω ότι $H = \langle\sigma\rangle$ είναι μια κυκλική υποομάδα τής S_n, η οποία παράγεται από έναν n-κύκλο $\sigma \in S_n$. Να δειχθεί ότι ο περιορισμός τής δράσης φ στην H ορίζει μια μεταβατική δράση τής H επί τού X.

(β′) Έστω ότι $n \geq 3$. Να δειχθεί ότι ο περιορισμός τής δράσης φ στην εναλλάσσουσα υποομάδα $\mathbb{A}_n$ ορίζει μια μεταβατική δράση τής $\mathbb{A}_n$ επί τού X.

ΠΑ 100. Έστω ότι $A = \{1, 2, 3\}$ και ότι $\Omega = A \times A$ είναι το σύνολο των διατεταγμένων ζευγών με συνιστώσες από το A. Η συμμετρική ομάδα S_3 δρα επί τού Ω μέσω τής επαγόμενης απεικόνισης:

$$\varphi : S_3 \times \Omega \to \Omega, (\sigma, (i, j)) \mapsto (\sigma(i), \sigma(j)).$$

(α′) Να προσδιοριστεί ο πυρήνας K_φ τής φ.

(β′) Να προσδιοριστεί η μετατακτική αναπαράσταση $X(\varphi) : S_3 \to S_9$.

(γ′) Να προσδιοριστούν οι S_3–τροχιές στις οποίες διαμερίζεται το σύνολο Ω.

(δ′) Επιλέγοντας ένα στοιχείο $\alpha \in \Omega$ από κάθε διαφορετική τροχιά, να προσδιοριστεί ο σταθεροποιητής S_{3_α} τού στοιχείου α.

ΠΑ 101. Έστω ένας F-διανυσματικός χώρος V υπεράνω ενός σώματος F με $\dim_F V = n, n \in \mathbb{N}$. Θεωρούμε την πολλαπλασιαστική ομάδα $(F^\star, \cdot)$ τού σώματος, όπου $F^\star = F \setminus \{0_F\}$ και «·» είναι ο πολλαπλασιασμός τού σώματος.

(α′) Να δειχθεί ότι η απεικόνιση $\varphi : F^\star \times V \to V, (g, v) \mapsto g\varphi v := gv$ (ο βαθμωτός πολλαπλασιασμός) αποτελεί μια δράση τής $F^\star$ επί τού V.

(β′) Για κάθε $v \in V$, να βρεθεί η τροχιά του $F^\star \varphi v$ και ο αντίστοιχος σταθεροποιητής ως προς τη δράση φ.

(γ′) Να επαληθευτεί το αποτέλεσμα τού Θεωρήματος 2.2.8.

(δ′) Πόσες τροχιές υπάρχουν, όταν το F είναι ένα πεπερασμένο σώμα με q στοιχεία;

ΠΑ 102. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης[3] $[G : 1] = p^n$, όπου ο p είναι ένας πρώτος αριθμός, ότι το A είναι ένα πεπερασμένο σύνολο και ότι η $\varphi : G \times A \to A$ είναι μια δράση τής G επί τού A.
Να δειχθούν τα εξής:

(α′) Αν το πλήθος $|A|$ των στοιχείων τού A δεν διαιρείται από τον p, τότε το A διαθέτει φ-σταθερά στοιχεία.

(β′) Αν το πλήθος $|A|$ των στοιχείων τού A διαιρείται από τον p, τότε το πλήθος των φ-σταθερών στοιχείων είναι λp, όπου $\lambda \in \mathbb{N} \cup \{0\}$.

ΠΑ 103. Πόσα ουσιαστικώς διαφορετικά περιδέραια αποτελούμενα από έξι χάντρες μπορούμε να κατασκευάσουμε χρησιμοποιώντας ακριβώς τρεις λευκές και ακριβώς τρεις μαύρες χάντρες;

2.3.3 Το Θεώρημα Cauchy

Έστω ότι $\varphi : G \times A \to A$ είναι δράση μιας ομάδας G επί ενός συνόλου A.
Το σύνολο των στοιχείων τού A που παραμένουν σταθερά από τη δράση φ τής G, δηλαδή το $\{\alpha \in A \mid g\varphi a = a, \forall g \in G\}$, το ονομάζουμε *σύνολο των φ-σταθερών στοιχείων* τού A και το συμβολίζουμε με $\mathrm{Fix}_\varphi(A)$.

Σημειώνουμε με $|A|$ (αντιστοίχως με $|\mathrm{Fix}_\varphi(A)|$) το πλήθος των στοιχείων τού A (αντιστοίχως τού $\mathrm{Fix}_\varphi(A)$).

Λήμμα 2.3.10. *Έστω ότι $\varphi : G \times A \to A$ είναι δράση μιας ομάδας $(G, \star)$ επί ενός πεπερασμένου συνόλου A.
Αν η τάξη τής G είναι p^n, όπου ο p είναι ένας πρώτος αριθμός και ο n είναι ένας φυσικός, τότε ο p διαιρεί τη διαφορά $|A| - |\mathrm{Fix}_\varphi(A)|$.*

Απόδειξη. Το A διαμερίζεται μέσω τής δράσης φ σε ένα πεπερασμένο πλήθος r τροχιών $\mathcal{O}_i, 1 \leq i \leq r$, αφού $|A| < \infty$. Έτσι έχουμε:

$$A = \mathcal{O}_1 \bigcup \mathcal{O}_2 \bigcup \cdots \bigcup \mathcal{O}_\ell \bigcup \mathcal{O}_{\ell+1} \bigcup \cdots \bigcup \mathcal{O}_r,$$

όπου το πλήθος $|\mathcal{O}_i|$ των στοιχείων τής $\mathcal{O}_i, 1 \leq i \leq \ell$ ισούται με 1 και το πλήθος $|\mathcal{O}_i|$ των στοιχείων τής $\mathcal{O}_i, \ell + 1 \leq i \leq r$ είναι ίσο ή μεγαλύτερο τού 2.

Το σύνολο $\mathrm{Fix}_\varphi(A)$ των φ-σταθερών στοιχείων τού A ισούται με $\mathcal{O}_1 \bigcup \mathcal{O}_2 \bigcup \cdots \bigcup \mathcal{O}_\ell$ και γι' αυτό $|\mathrm{Fix}_\varphi(A)| = \ell$. Παρατηρούμε ότι όταν $|\mathcal{O}_i| \geq 2$, τότε ο πρώτος p διαιρεί τον αριθμό $|\mathcal{O}_i|$, αφού $|\mathcal{O}_i| = [G : G_{a_i}]$, όπου a_i είναι οποιοδήποτε στοιχείο τής τροχιάς $\mathcal{O}_i$. Ώστε ο p διαιρεί τον $|\mathcal{O}_i|, \forall i, \ell + 1 \leq i \leq r$.
Συνεπώς,

$$|A| = \sum_{i=1}^{r} |\mathcal{O}_i| = \sum_{i=1}^{\ell} |\mathcal{O}_i| + \sum_{i=\ell+1}^{r} |\mathcal{O}_i| = |\mathrm{Fix}_\varphi(A)| + \kappa p.$$

Επομένως, ο p διαιρεί τη διαφορά $|A| - |\mathrm{Fix}_\varphi(A)|$. □

[3] Αργότερα μια ομάδα τάξης p^n, όπου p πρώτος και $n \in \mathbb{N} \cup \{0\}$ θα την ονομάσουμε *p-ομάδα*.

Θεώρημα 2.3.11 (Cauchy). *Έστω $(G, \star)$ μια ομάδα τάξης $[G : 1] = n \in \mathbb{N}$ και p ένας πρώτος διαιρέτης τού n. Τότε υπάρχει ένα στοιχείο $g \in G$ με τάξη p.*

Απόδειξη. Είναι αρκετό να αποδείξουμε ότι υπάρχει κάποιο $g \neq e_G$ με $g^p = e_G$, αφού τότε η τάξη τού g είναι ένας διαιρέτης τού p και επειδή ο p είναι πρώτος και $g \neq e_G$ έχουμε ότι η τάξη τού g είναι p.
Σχηματίζουμε το σύνολο

$$A = \{(g_1, g_2, \ldots, g_p) | g_i \in G, \forall i, 1 \leq i \leq p \text{ με } g_1 g_2 \ldots g_p = e_G\}.$$

Το πλήθος $|A|$ των στοιχείων τού A ισούται με $[G : 1]^{(p-1)}$, αφού τα $g_1, g_2, \ldots, g_{p-1}$ μπορεί να είναι οποιαδήποτε στοιχεία τής G, ενώ το g_p είναι μοναδικά καθορισμένο από τα $g_1, g_2, \ldots, g_{p-1}$, αφού $g_p = (g_1 g_2 \ldots g_{p-1})^{-1}$.
Επειδή ο p διαιρεί τον n έχουμε $n = \kappa p$ και συνεπώς

$$|A| = [G : 1]^{(p-1)} = \kappa^{(p-1)} p^{(p-1)}. \tag{*}$$

Παρατηρούμε ότι αν

$$g_1 g_2 \ldots g_i g_{i+1} \ldots g_p = e_G, \text{ τότε } g_{i+1} g_{i+2} \ldots g_p = (g_1, g_2 \ldots g_i)^{-1},$$

και γι' αυτό $(g_{i+1} g_{i+2} \ldots g_p)(g_1 g_2 \ldots g_i) = e_G$.

Συνεπώς, όταν η p–άδα $(g_1, g_2, \ldots, g_p)$ ανήκει στο A, τότε και οποιαδήποτε άλλη p–άδα $(g_{i+1}, g_{i+2}, \ldots, g_p, g_1, g_2, \ldots, g_i)$, η οποία προκύπτει από την πρώτη κατόπιν κυκλικής εναλλαγής των συνιστωσών της, ανήκει επίσης στο A.

Θεωρούμε την κυκλική ομάδα $(\mathbb{Z}_p, +)$ και ορίζουμε την απεικόνιση

$$\varphi : \mathbb{Z}_p \times A \to A, ([i], (g_1, g_2, \ldots, g_p)) \mapsto (g_{(i+1)\mathrm{mod}p}, g_{(i+2)\mathrm{mod}p}, \ldots, g_{(i+p)\mathrm{mod}p}),$$

όπου οι δείκτες $(i+1)\mathrm{mod}p, (i+2)\mathrm{mod}p, \ldots, (i+p)\mathrm{mod}p$ διατρέχουν τους αντιπροσώπους j των κλάσεων $\mathrm{mod}p$ με j μεταξύ των αριθμών 1 και p.

Αφήνουμε ως άσκηση στον αναγνώστη τον έλεγχο ότι η απεικόνιση φ αποτελεί μια δράση τής ομάδας $\mathbb{Z}_p$ επί τού συνόλου A.
Παρατηρούμε ότι ένα στοιχείο $(g_1, g_2, \ldots, g_p) \in A$ ανήκει στο σύνολο $\mathrm{Fix}_\varphi(A)$ των φ–σταθερών στοιχείων τού A, αν και μόνο αν, βλ. Άσκηση Α107,

$$\begin{aligned}
&[1]\varphi(g_1, g_2, \ldots, g_{p-1}, g_p) = (g_1, g_2, \ldots, g_{p-1}, g_p) \Leftrightarrow \\
&(g_{(1+1)\mathrm{mod}p}, g_{(1+2)\mathrm{mod}p}, \ldots, g_{(1+(p-1))\mathrm{mod}p}, g_{(1+p)\mathrm{mod}p}) = (g_1, g_2, \ldots, g_p) \Leftrightarrow \\
&(g_2, g_3, \ldots, g_p, g_1) = (g_1, g_2, \ldots, g_p) \Leftrightarrow g_1 = g_2 = g_3 = \cdots = g_p.
\end{aligned}$$

Συνεπώς, τα στοιχεία τού συνόλου $\mathrm{Fix}_\varphi(A)$ συμπίπτουν με τις p–άδες $(g, g, \ldots, g)$, όπου $g \in G$ με $g^p = e_G$. Το πλήθος $|\mathrm{Fix}_\varphi(A)|$ τού $\mathrm{Fix}_\varphi(A)$ είναι ≥ 1, επειδή η p–άδα $(e_G, e_G, \ldots, e_G)$ ανήκει στο $\mathrm{Fix}_\varphi(A)$.
Σύμφωνα με το προηγούμενο λήμμα, η τάξη p τής $\mathbb{Z}_p$ διαιρεί τη διαφορά $|A| - |\mathrm{Fix}_\varphi(A)|$ και επειδή, λόγω τής $(*)$, η τάξη τού A είναι πολλαπλάσιο τού p, έπεται ότι ο p διαιρεί τον αριθμό $|\mathrm{Fix}_\varphi(A)| \geq 1$. Επομένως, $|\mathrm{Fix}_\varphi(A)| \geq p \geq 2$ και γι' αυτό υπάρχει ένα στοιχείο $(g, g, \ldots, g) \in \mathrm{Fix}_\varphi(A) \subseteq A$ με $g \neq e_G$. Ώστε, $g^p = e_G$ με $g \neq e_G$. Προφανώς, το g έχει τάξη p. □

2.4 Συζυγία

Θεωρούμε τώρα μία ακόμα δράση μιας ομάδας επί τού εαυτού της, η οποία όπως θα δούμε σύντομα θα χορηγήσει πολλά και ουσιαστικά αποτελέσματα στη Θεωρία Ομάδων.

Η απεικόνιση

$$\sigma : G \times G \to G, (g, \alpha) \ \mapsto \ g\sigma\alpha := g\alpha g^{-1}$$

ορίζει μια δράση τής G επί του εαυτού της, αφού

$$\forall g_1, g_2, \alpha \in G : (g_1g_2)\sigma\alpha = (g_1g_2)\alpha(g_1g_2)^{-1} = g_1(g_2\alpha g_2^{-1})g_1^{-1} = g_1\sigma(g_2\sigma\alpha) \text{ και}$$
$$\forall \alpha \in G : e_G\sigma\alpha = e_G\alpha(e_G)^{-1} = \alpha.$$

Ορισμός 2.4.1. Η δράση $\sigma : G \times G \to G, (g, \alpha) \mapsto g\sigma\alpha := g\alpha g^{-1}$ ονομάζεται *δράση συζυγίας* επί των στοιχείων τής G.

Στη συγκεκριμένη περίπτωση οι τροχιές στις οποίες διαμερίζεται η G μέσω τής δράσης συζυγίας σ ονομάζονται *κλάσεις συζυγίας*.

Δύο στοιχεία $\alpha, \beta \in G$ ανήκουν στην ίδια κλάση, αν και μόνο αν, $\exists g \in G$ με $g\alpha g^{-1} = \beta$.

Στοιχεία που ανήκουν στην ίδια κλάση συζυγίας ονομάζονται *συζυγή στοιχεία*.

Η κλάση συζυγίας τού στοιχείου $\alpha \in G$ είναι το σύνολο $\mathcal{K}_\alpha = \{g\alpha g^{-1} | g \in G\}$.

Αν η G είναι μια πεπερασμένη ομάδα, τότε το πλήθος των κλάσεων συζυγίας είναι επίσης πεπερασμένο, αφού οι κλάσεις συζυγίας αποτελούν μια διαμέριση τής G.

Παρατήρηση 2.4.2. (α′) Αν η G είναι μια αβελιανή ομάδα, τότε η δράση τής συζυγίας είναι τετριμμένη, αφού $\forall g, \alpha \in G$ είναι $g\sigma\alpha = g\alpha g^{-1} = gg^{-1}\alpha = e_G\alpha = \alpha$.

(β′) Αν $[G : 1] > 1$, τότε η δράση τής συζυγίας δεν είναι ποτέ μεταβατική, αφού η κλάση συζυγίας $\mathcal{K}_{e_G}$ τού ουδέτερου στοιχείου e_G τής G είναι το μονοσύνολο $\mathcal{K}_{e_G} = \{e_G\}$.

(γ′) Γενικώς, η κλάση συζυγίας $\mathcal{K}_\alpha$ ενός στοιχείου $\alpha \in G$ είναι μονοσύνολο (και τότε βέβαια αποτελείται μόνο από το στοιχείο α), αν και μόνο αν, το α ανήκει στο *κέντρο*, βλ. Άσκηση Α39, τής ομάδας

$$\mathcal{Z}(G) = \{\alpha \in G \mid \alpha g = g\alpha, \forall g \in G\}.$$

(δ′) Κάθε στοιχείο $\beta \in G$ που ανήκει στην κλάση συζυγίας $\mathcal{K}_\alpha$ τού $\alpha \in G$ έχει την ίδια τάξη με το α, αφού $\forall g \in G$, η απεικόνιση $\chi_g : G \to G, \alpha \mapsto g\alpha g^{-1}$ είναι ένας εσωτερικός αυτομορφισμός τής G.

Παράδειγμα 2.4.3. Οι κλάσεις συζυγίας τής συμμετρικής ομάδας $(S_3, \circ)$ είναι οι:

$$\mathcal{K}_{\mathrm{Id}_3} = \{\mathrm{Id}_3\}, \ \ \mathcal{K}_{(12)} = \{(12), (13), (23)\} \ \text{ και } \ \mathcal{K}_{(123)} = \{(123), (132)\}.$$

Οι κλάσεις συζυγίας τής $(S_n, \circ), n \geq 2$

Υπενθυμίζουμε, βλ. Ορισμό 1.8.25 ότι ο κυκλικός τύπος μιας μετάταξης $\sigma \in S_n$ ορίζεται ως εξής:

Όταν $\sigma = \mathrm{Id}_n$, τότε ο κυκλικός τύπος είναι η n–άδα $(1, 1, \ldots, 1)$.

Όταν $\sigma \neq \mathrm{Id}_n$, τότε θεωρούμε την ανάλυση τού σ σε γινόμενο αποσυνδετών κύκλων $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s$, $s \geq 1$, με μήκη $\ell(\gamma_i) \geq 2, \forall i, 1 \leq i \leq s$ και $\ell(\gamma_i) \leq \ell(\gamma_j)$ όταν $i < j$. Στην περίπτωση αυτή ο κυκλικός τύπος τού σ είναι η n–άδα

$$(1, 1, \ldots, 1, \ell(\gamma_1), \ell(\gamma_2), \ldots, \ell(\gamma_s)),$$

όπου το πλήθος m των συνιστωσών που είναι ίσες με 1 είναι $m = n - \sum_{i=1}^{s} \ell(\gamma_i)$. (Προσέξτε ότι το m μπορεί να ισούται με 0.)

Θεώρημα 2.4.4. *Δύο μετατάξεις $\sigma, \tau \in S_n$ είναι συζυγή στοιχεία, αν και μόνο αν, έχουν τον ίδιο κυκλικό τύπο.*

Απόδειξη. Προφανώς, δύο μετατάξεις με κυκλικό τύπο την n–άδα $(1, 1, \ldots, 1)$ είναι ίσες με την Id_n, άρα είναι συζυγείς. Αντίστροφα, κάθε $\sigma \in S_n$ που είναι συζυγής με την Id_n συμπίπτει με την ταυτοτική μετάταξη και ως εκ τούτου, έχει κυκλικό τύπο την n–άδα $(1, 1, \ldots, 1)$.

Επομένως, μπορούμε χωρίς περιορισμό τής γενικότητας να υποθέσουμε ότι $\sigma, \tau \in S_n$ με $\sigma, \tau \neq \mathrm{Id}_n$.

Όταν οι σ, τ είναι συζυγείς, τότε υπάρχει κάποιο $\rho \in S_n$ με $\tau = \rho \circ \sigma \circ \rho^{-1}$. Αν $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s$ είναι η ανάλυση τού σ σε γινόμενο αποσυνδετών κύκλων μήκους ≥ 2, τότε

$$\begin{aligned}\tau =& \rho \circ (\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s)\rho^{-1} = \\ & (\rho \circ \gamma_1 \circ \rho^{-1}) \circ (\rho \circ \gamma_2 \circ \rho^{-1}) \circ \cdots \circ (\rho \circ \gamma_i \circ \rho^{-1}) \circ \cdots \circ (\rho \circ \gamma_s \circ \rho^{-1})\end{aligned}$$

Από την Πρόταση 1.8.23 γνωρίζουμε ότι κάθε $\rho \circ \gamma_i \circ \rho^{-1}$ είναι ένας κύκλος μήκους $\ell(\gamma_i)$ και από την Άσκηση 101 γνωρίζουμε ότι οι $\rho \circ \gamma_i \circ \rho^{-1}, 1 \leq i \leq s$ είναι ανά δύο αποσυνδετοί. Ως εκ τούτου, οι σ και τ έχουν τον ίδιο κυκλικό τύπο.

Αντίστροφα, έστω ότι οι σ και τ έχουν τον ίδιο κυκλικό τύπο

$$(1, 1, \ldots, 1, n_1, n_2, \ldots n_i, \ldots, n_s),$$

όπου το πλήθος των 1 ισούται με $m = n - \sum_{i=1}^{s} n_i$. Τότε η σ (αντιστοίχως η τ) εκφράζεται ως $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \cdots \circ \gamma_s$ (αντιστοίχως $\tau = \delta_1 \circ \delta_2 \circ \cdots \circ \cdots \circ \delta_s$), όπου $\forall i, 1 \leq i \leq s$ οι γ_i, (αντιστοίχως οι δ_i) είναι ανά δύο αποσυνδετοί κύκλοι μήκους n_i. Έστω ότι $\forall i, 1 \leq i \leq s$, ο $\gamma_i = \begin{pmatrix} x_{i1} & x_{i2} & \ldots & x_{in_i} \end{pmatrix}$ (αντιστοίχως ο $\delta_i = \begin{pmatrix} y_{i1} & y_{i2} & \ldots & y_{in_i} \end{pmatrix}$) είναι ο κύκλος μήκους $\ell(\gamma_i) = n_i$ (αντιστοίχως μήκους $\ell(\delta_i) = n_i$). Θεωρούμε την απεικόνιση, η οποία ορίζεται ως εξής: $\forall i, j, 1 \leq i \leq s, 1 \leq j \leq n_i : \rho(x_{ij}) = y_{ij}$. Τέλος, αν $m \neq 0$ και $a_1, a_2, \ldots, a_m \in \{1, 2, \ldots, n\}$ είναι ακριβώς τα στοιχεία με $\sigma(a_i) = a_i$ και $b_1, b_2, \ldots, b_m \in \{1, 2, \ldots, n\}$ είναι ακριβώς τα στοιχεία με $\tau(b_i) = b_i$, τότε ορίζουμε $\rho(a_i) = b_i, \forall i, 1 \leq i \leq m$. Η ρ είναι μια μετάταξη, επειδή η ρ από την κατασκευή της είναι μια ενριπτική απεικόνιση («$1 - 1$») και επειδή η ένωση $\{x_{ij} \mid 1 \leq i \leq s, 1 \leq j \leq n_i\} \bigcup \{a_1, a_2, \ldots, a_m\}$

είναι ακριβώς το σύνολο $\{1, 2, \ldots, n\}$. Τώρα είναι εύκολη η επιβεβαίωση ότι $\rho \circ \sigma \circ \rho^{-1} = \tau$, διότι

$$\rho \circ \gamma_i \circ \rho^{-1} = \rho \circ \begin{pmatrix} x_{i1} & x_{i2} & \ldots & x_{in_i} \end{pmatrix} \circ \rho^{-1} = \begin{pmatrix} \rho(x_{i1}) & \rho(x_{i2}) & \ldots & \rho(x_{in_i}) \end{pmatrix} = \begin{pmatrix} y_{i1} & y_{i2} & \ldots & y_{in_i} \end{pmatrix} = \delta_i.$$

Άρα, οι σ και τ είναι συζυγείς □

Παράδειγμα 2.4.5. Στην $(S_{10}, \circ)$ θεωρούμε τις μετατάξεις $\sigma = \begin{pmatrix} 4 & 10 \end{pmatrix} \circ \begin{pmatrix} 3 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 7 & 9 \end{pmatrix}$ και $\tau = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 5 & 6 & 7 \end{pmatrix}$. Ο κυκλικός τύπος και των δύο είναι ο $(1, 1, 1, 2, 2, 3)$. Τα σταθερά στοιχεία τής σ (αντιστοίχως τής τ) είναι τα 2, 6, 8 (αντιστοίχως τα 8, 9, 10). Σύμφωνα με το προηγούμενο θεώρημα οι σ και τ είναι συζυγείς.
Πράγματι, θεωρώντας τη μετάταξη $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 3 & 1 & 4 & 9 & 6 & 10 & 7 & 2 \end{pmatrix}$ έχουμε

$$\rho \circ \sigma \circ \rho^{-1} = \begin{pmatrix} \rho(4) & \rho(10) \end{pmatrix} \circ \begin{pmatrix} \rho(3) & \rho(5) \end{pmatrix} \circ \begin{pmatrix} \rho(1) & \rho(7) & \rho(9) \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 5 & 6 & 7 \end{pmatrix} = \tau.$$

Προσέξτε ότι η ρ δεν είναι η μοναδική μετάταξη που επιβεβαιώνει ότι οι σ και τ είναι συζυγείς. Για παράδειγμα, η $\rho' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 8 & 1 & 3 & 2 & 9 & 6 & 10 & 7 & 4 \end{pmatrix}$ ικανοποιεί την ισότητα $\rho' \circ \sigma \circ {\rho'}^{-1} = \tau$.

Παρατήρηση 2.4.6. Το πλήθος των κλάσεων συζυγίας τής $(S_n, \circ), n \geq 2$ ισούται με το πλήθος των διαμερίσεων τού n, αφού δύο στοιχεία τής S_n είναι συζυγή, αν και μόνο αν, έχουν τον ίδιο κυκλικό τύπο.

2.4.1 Επεκτείνοντας τη Δράση Συζυγίας

Η δράση τής συζυγίας πάνω στο σύνολο των στοιχείων τής ομάδας G επεκτείνεται σε μια δράση $\tilde{\sigma}$ επί τού συνόλου $\mathcal{P}^\star(G)$ όλων των μη κενών υποσυνόλων τής G:

$$\tilde{\sigma} : G \times \mathcal{P}^\star(G) \to \mathcal{P}^\star(G), (g, A) \mapsto g\tilde{\sigma}A := gAg^{-1}.$$

Αν η G είναι μια πεπερασμένη ομάδα, τότε το πλήθος των στοιχείων τής τροχιάς $\mathcal{O}_A$ τού $A \subseteq G$ ισούται με τον δείκτη $[G : G_A]$, όπου $G_A = \{g \in G \mid gAg^{-1} = A\}$ είναι ο σταθεροποιητής τού συνόλου A.

Όταν το A είναι ένα μονοσύνολο, ας πούμε $A = \{\alpha\}$, τότε ο σταθεροποιητής $G_{\{\alpha\}}$ ονομάζεται ο *κεντροποιητής* τού στοιχείου α και συμβολίζεται με $C_G(\alpha)$, βλ. Άσκηση ΠΑ35. Ώστε,

$$C_G(\alpha) = \{g \in G \mid g\alpha g^{-1} = \alpha\} = \{g \in G \mid g\alpha = \alpha g\}.$$

Όταν η G είναι μια πεπερασμένη ομάδα, τότε το πλήθος των συζυγών στοιχείων τού α, δηλαδή το πλήθος των στοιχείων τής κλάσης συζυγίας $\mathcal{K}_\alpha$ ισούται με $[G : C_G(\alpha)]$. Προφανώς, για το κέντρο $\mathcal{Z}(G)$ μιας ομάδας G έχουμε:

$$\mathcal{Z}(G) = \bigcap_{\alpha \in G} C_G(\alpha).$$

Όταν το $H \leq G$ είναι μια υποομάδα τής G, τότε ο σταθεροποιητής G_H τής H ονομάζεται ο *ορθοθετοποιητής* ή *ορθοθετοποιούσα υποομάδα* τής H και συμβολίζεται με $\mathcal{N}_G(H)$, βλ. Άσκηση Α38. Συνεπώς,

$$\mathcal{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Παρατήρηση 2.4.7. (α′) Αν $H \leq G$ είναι μια υποομάδα τής G, τότε ο ορθοθετοποιητής $\mathcal{N}_G(H)$ τής G είναι η μεγαλύτερη (ως προς τη σχέση υποσυνόλου «$\subseteq$») υποομάδα τής G, εντός τής οποίας η H είναι ορθόθετη, δηλαδή $H \trianglelefteq \mathcal{N}_G(H)$.

(β′) Μια υποομάδα H τής G είναι ορθόθετη, αν και μόνο αν, $\mathcal{N}_G(H) = G$.

(γ′) Αν η ομάδα G είναι πεπερασμένη και H είναι μια υποομάδα της, τότε, λόγω τού Θεωρήματος 2.2.8, ο δείκτης $[G : \mathcal{N}_G(H)]$ ισούται με το πλήθος των στοιχείων τής τροχιάς $\mathcal{O}_H = \{gHg^{-1} \mid g \in G\}$, δηλαδή το πλήθος των υποομάδων τής G, οι οποίες είναι συζυγείς προς την H.

2.4.2 Η Εξίσωση των Κλάσεων

Θεώρημα 2.4.8. *Αν, G είναι μια ομάδα με πεπερασμένη τάξη $[G:1] < \infty$ και αν $\alpha_1, \alpha_2, \ldots, \alpha_\ell$ είναι οι αντιπρόσωποι από τις διαφορετικές κλάσεις συζυγίας που αποτελούνται από περισσότερα τού ενός στοιχεία, τότε*

$$[G:1] = [\mathcal{Z}(G):1] + \sum_{j=1}^{\ell} [G : C_G(\alpha_j)].$$

Απόδειξη. Θεωρούμε τη διαμέριση τής G στις κλάσεις συζυγίας:

$$G = \mathcal{Z}_1 \bigcup \mathcal{Z}_2 \bigcup \cdots \bigcup \mathcal{Z}_t \bigcup \mathcal{K}_1 \bigcup \mathcal{K}_2 \bigcup \cdots \bigcup \mathcal{K}_\ell, \tag{*}$$

όπου $\mathcal{Z}_i, 1 \leq i \leq t$ είναι οι κλάσεις συζυγίας που καθεμιά τους αποτελείται από ακριβώς ένα στοιχείο και $\mathcal{K}_j, 1 \leq j \leq \ell$ είναι οι κλάσεις που καθεμιά τους αποτελείται από περισσότερα τού ενός στοιχεία. Όπως έχουμε ήδη διαπιστώσει, η κλάση συζυγίας ενός στοιχείου $\alpha \in G$ αποτελείται μόνο από το α, αν και μόνο αν, το α ανήκει στο κέντρο $\mathcal{Z}(G)$ τής G. Γι' αυτό το πλήθος t των κλάσεων συζυγίας, που έχουν μόνο ένα στοιχείο, είναι ίσο με την τάξη $[\mathcal{Z}(G) : 1]$ τού κέντρου $\mathcal{Z}(G)$ τής G. Επιπλέον, το πλήθος των στοιχείων τής $\mathcal{K}_j, 1 \leq j \leq \ell$ ισούται με τον δείκτη $[G : C_G(\alpha_j)]$, όπου α_j είναι οποιοδήποτε στοιχείο τής κλάσης συζυγίας $\mathcal{K}_j$.

Γι΄αυτό από την (*) προκύπτει η

$$[G:1] = [\mathcal{Z}(G):1] + \sum_{j=1}^{\ell} [G : C_G(\alpha_j)]. \tag{**}$$

□

Η ισότητα (**) ονομάζεται η *Εξίσωση των Κλάσεων*.

Παρατήρηση 2.4.9. Αν η G είναι μια πεπερασμένη αβελιανή ομάδα, τότε η Εξίσωση των Κλάσεων χορηγεί την ισότητα $[G : 1] = [\mathcal{Z}(G) : 1]$, που προφανώς είναι αληθής, αφού $G = \mathcal{Z}(G)$.

Παράδειγμα 2.4.10.
(α′) **Οι κλάσεις συζυγίας τής ομάδας τετρανίων** $(\mathcal{Q}_8, \circ)$. Υπενθυμίζουμε, βλ. Άσκηση Α58, ότι το σύνολο των στοιχείων της $\mathcal{Q}_8$ ισούται με τους 2×2 μιγαδικούς πίνακες $\{\pm E,\ \pm I,\ \pm J,\ \pm K\}$, όπου $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, J = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ και $K = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$ με $i^2 = -1$. Η πράξη «$\circ$» τής $\mathcal{Q}_8$ είναι ο πολλαπλασιασμός πινάκων.

Στην Άσκηση Α58 υπολογίσαμε επίσης τον πίνακα τής πράξης «$\circ$». Από αυτόν προκύπτει εύκολα ότι το κέντρο $\mathcal{Z}(\mathcal{Q}_8)$ τής $\mathcal{Q}_8$ ισούται με $\{E, -E\}$. Συνεπώς έχουμε ακριβώς δύο κλάσεις συζυγίας τις $\mathcal{K}_E, \mathcal{K}_{-E}$ που καθεμιά τους έχει μόνο ένα στοιχείο.

Η κλάση συζυγίας $\mathcal{K}_I$ έχει $[\mathcal{Q}_8 : \mathcal{C}_{\mathcal{Q}_8}(I)]$ το πλήθος στοιχεία, όπου $\mathcal{C}_{\mathcal{Q}_8}(I)$ είναι ο κεντροποιητής τού I. Ισχυριζόμαστε ότι $\mathcal{C}_{\mathcal{Q}_8}(I) = \langle I \rangle$. Πράγματι, η κυκλική υποομάδα $\langle I \rangle$, η οποία είναι τάξης 4, περιέχεται στον $\mathcal{C}_{\mathcal{Q}_8}(I)$. Άρα, ή $\mathcal{Q}_8 = \mathcal{C}_{\mathcal{Q}_8}(I)$ ή $\langle I \rangle = \mathcal{C}_{\mathcal{Q}_8}(I)$. Αν ήταν $\mathcal{Q}_8 = \mathcal{C}_{\mathcal{Q}_8}(I)$, τότε θα ανήκε το I στον κέντρο $\mathcal{Z}(\mathcal{Q}_8)$, το οποίο δεν ισχύει. Επομένως, $\langle I \rangle = \mathcal{C}_{\mathcal{Q}_8}(I)$ και η $\mathcal{K}_I$ έχει $[\mathcal{Q}_8 : \mathcal{C}_{\mathcal{Q}_8}(I)] = 8/4$ στοιχεία. Επειδή, $JIJ^{-1} = -I$, συμπεραίνουμε ότι $\mathcal{K}_I = \{I, -I\}$.

Παρόμοια προκύπτει $\mathcal{K}_J = \{J, -J\}$ και $\mathcal{K}_K = \{K, -K\}$.
(β′) **Οι κλάσεις συζυγίας τής διεδρικής ομάδας** $(D_4, \circ)$.
Υπενθυμίζουμε, βλ. σελ. 18, ότι η $(D_4, \circ)$ είναι η ομάδα στερεών κινήσεων (ισομετριών) τού τετραγώνου και ότι το σύνολο των στοιχείων τής D_4 είναι το

$$D_4 = \{\mathrm{Id}_4, \tau, \rho, \rho^2, \rho^3, \tau \circ \rho, \tau \circ \rho^2, \tau \circ \rho^3\}.$$

με $\rho^4 = \mathrm{Id}_4$, $\tau^2 = \mathrm{Id}_4$ και $\rho \circ \tau = \tau \circ \rho^{-1}$.

Το κέντρο $\mathcal{Z}(D_4)$ τής D_4 ισούται με $\{\mathrm{Id}_4, \rho^2\}$, βλ. Άσκηση Α40. Συνεπώς, έχουμε ακριβώς δύο κλάσεις συζυγίας τις $\mathcal{K}_{\mathrm{Id}_4}, \mathcal{K}_{\rho^2}$ που καθεμιά τους έχει μόνο ένα στοιχείο.

Θεωρούμε τις υποομάδες τάξης 4 τής D_4:

$$H_1 = \{\mathrm{Id}, \rho, \rho^2, \rho^3\}, H_2 = \{\mathrm{Id}_4, \rho^2, \tau, \tau\rho^2\}, H_3 = \{\mathrm{Id}_4, \rho^2, \tau\rho, \tau\rho^3\}.$$

Παρατηρούμε ότι $\forall \alpha \in H_i \setminus \mathcal{Z}(D_4), i = 1, 2, 3$ η υποομάδα H_i περιέχεται στον κεντροποιητή $\mathcal{C}_{D_4}(\alpha)$, ο οποίος είναι γνήσια υποομάδα τής D_4, αφού $\alpha \notin \mathcal{Z}(D_4)$. Για παράδειγμα, η $H_3 \leq C_{D_4}(\tau\rho^3)$, διότι $(\tau\rho)(\tau\rho^3) = \tau(\rho\tau)\rho^3 = \tau(\tau\rho^3)\rho^3 = \rho^2$ και $(\tau\rho^3)(\tau\rho) = \tau(\rho^3\tau)\rho = \tau(\tau\rho)\rho = \rho^2$. Επειδή ο δείκτης $[D_4 : H_i] = 2, \forall i, i = 1, 2, 3$, έχουμε $H_i = C_{D_4}(\alpha), \forall \alpha \in H_i \setminus \mathcal{Z}(G), i = 1, 2, 3$ και γι' αυτό η κλάση συζυγίας κάθε $\alpha \in H_1 \bigcup H_2 \bigcup H_3 \setminus \mathcal{Z}(G)$ αποτελείται από ακριβώς δύο στοιχεία. Έχουμε $\mathcal{K}_\rho = \{\rho, \rho^3\}$, $\mathcal{K}_\tau = \{\tau, \tau\rho^2\}, \mathcal{K}_{\tau\rho} = \{\tau\rho, \tau\rho^3\}$.

***Εφαρμογή* 2.4.11.** *Κάθε ομάδα $(G, \star)$ τάξης 15 είναι κυκλική.*

Απόδειξη. Κατ' αρχάς θα δείξουμε ότι οποιαδήποτε ομάδα τάξης 15 είναι αβελιανή.

Ας υποθέσουμε ότι υπάρχει μια ομάδα G με 15 στοιχεία που δεν είναι αβελιανή. Υπολογίζοντας την Εξίσωση των Κλάσεων για τη συγκεκριμένη ομάδα θα καταλήξουμε σε άτοπο.

Κατ' αρχάς, η τάξη $[\mathcal{Z}(G) : 1]$ τού κέντρου της οφείλει να είναι ένας διαιρέτης δ τού 15 με $\delta \lneqq 15$, αφού υποθέσαμε ότι η G δεν είναι αβελιανή. Αλλά $[\mathcal{Z}(G) : 1] \neq 5$ (αντιστοίχως $\neq 3$), αφού διαφορετικά η πηλικοομάδα $G/\mathcal{Z}(G)$ θα ήταν κυκλική, διότι θα ήταν πρώτης τάξης 3 (αντιστοίχως 5) και επομένως τότε η G θα ήταν μια αβελιανή ομάδα, βλ. Άσκηση Α78. Άρα, $[\mathcal{Z}(G) : 1] = 1$.

Από το Θεώρημα Cauchy, γνωρίζουμε ότι η G διαθέτει και στοιχεία τάξης 3 και στοιχεία τάξης 5, αλλά δεν διαθέτει στοιχείο τάξης 15, διότι έχουμε υποθέσει ότι δεν είναι αβελιανή.

Έστω $g \neq e_G$ ένα στοιχείο τής G. Επειδή το $g \notin \mathcal{Z}(G) = \{e_G\}$, διαπιστώνουμε ότι ο κεντροποιητής $\mathcal{C}_G(g)$ τού g είναι μια γνήσια υποομάδα τής G.

Ισχυριζόμαστε ότι $\circ(g) = 3$, αν και μόνο αν, το πλήθος των στοιχείων τής κλάσης συζυγίας $\mathcal{K}_g$ ισούται με 5. Κατ' αρχάς παρατηρούμε ότι

$$|\mathcal{K}_g| = 5 \Leftrightarrow [G : \mathcal{C}_G(g)] = 5 \Leftrightarrow [\mathcal{C}_G(g) : 1] = 3. \tag{*}$$

Αν είναι $[\mathcal{C}_G(g) : 1] = 3$, τότε επειδή η $\langle g \rangle$ είναι πάντοτε υποομάδα τού $\mathcal{C}_G(g)$ και αφού $\langle g \rangle \neq \{e_G\}$, συμπεραίνουμε ότι $\langle g \rangle = \mathcal{C}_G(g)$ και ως εκ τούτου $\circ(g) = 3$.

Αντίστροφα, αν είναι $\circ(g) = 3$, τότε $[\langle g \rangle : 1] = 3$ και αφού $\langle g \rangle \leq \mathcal{C}_G(g) \neq G$, συμπεραίνουμε ότι $[\mathcal{C}_G(g) : 1] = 3$, επειδή οι μη τετριμμένες υποομάδες τής G είναι τάξης ή 3 ή 5. Ως εκ τούτου, η $(*)$ δίνει ότι $|\mathcal{K}_g| = 5$

Εντελώς ανάλογα αποδεικνύεται ότι $\circ(g) = 5$, αν και μόνο αν, το πλήθος των στοιχείων τής κλάσης συζυγίας $\mathcal{K}_g$ ισούται με 3.

Έστω ότι α είναι ένα στοιχείο τής G με $\circ(\alpha) = 3$ και ότι β είναι ένα στοιχείο τής G με $\circ(\beta) = 5$. Σύμφωνα με όσα προείπαμε, η κλάση συζυγίας $\mathcal{K}_\alpha$ έχει 5 το πλήθος στοιχεία και η κλάση συζυγίας $\mathcal{K}_\beta$ έχει 3 το πλήθος στοιχεία.

Η Εξίσωση των Κλάσεων δίνει:

$$15 = [\mathcal{Z}(G) : 1] + |\ \mathcal{K}_\alpha\ | + |\ \mathcal{K}_\beta\ | + \sum_{i=1}^{t} |\mathcal{K}_i{}'| = 1 + 5 + 3 + \sum_{i=1}^{t} |\mathcal{K}_i{}'|,$$

όπου $\mathcal{K}_i{}', 1 \leq i \leq t$ είναι οι επιπλέον κλάσεις συζυγίας. Όμως το πλήθος κ_i των στοιχείων οποιασδήποτε επιπλέον κλάσης συζυγίας $\mathcal{K}_i{}'$ πρέπει να ισούται με 3, αφού αν κάποια κλάση $\mathcal{K}_i{}'$ διέθετε 5 στοιχεία, τότε η ισότητα

$$15 = 1 + 5 + 3 + 5 + \ldots$$

δεν μπορεί να συμπληρωθεί με κατάλληλα $\kappa_i = 3$ ή 5 ώστε να δώσει το 15. Γι΄αυτό η μοναδική περίπτωση είναι

$$15 = 1 + 5 + 3 + 3 + 3.$$

Αφού λοιπόν η G έχει μόνο μία κλάση συζυγίας με πέντε στοιχεία, συμπεραίνουμε ότι η G έχει ακριβώς πέντε στοιχεία τάξης 3.

Όμως από την Πρόταση 1.5.16, γνωρίζουμε ότι το πλήθος των στοιχείων τής G τάξης 3 είναι πολλαπλάσιο τού $\varphi(3) = 2$, δηλαδή είναι άρτιος αριθμός. Άτοπο! Άρα, η G είναι αβελιανή ομάδα.

Έστω ότι $\alpha \in G$ είναι ένα στοιχείο τάξης 3 και $\beta \in G$ είναι ένα στοιχείο τάξης 5. Τότε $[\langle\alpha\rangle : 1] = 3$, $[\langle\beta\rangle : 1] = 5$. Παρατηρούμε ότι οι $\langle\alpha\rangle$ και $\langle\beta\rangle$ είναι ορθόθετες υποομάδες τής G, αφού η G είναι αβελιανή και προφανώς $\langle\alpha\rangle \bigcap \langle\beta\rangle = \{e_G\}$. Από την Άσκηση A88, γνωρίζουμε ότι η $\langle\alpha\rangle\langle\beta\rangle$ είναι ισόμορφη προς την $\langle a\rangle \times \langle\beta\rangle$. Η τάξη τής $[\langle\alpha\rangle\langle\beta\rangle : 1] = 15$ και ως εκ τούτου, $G = \langle\alpha\rangle\langle\beta\rangle$. Επιπλέον, η $\langle\alpha\rangle \times \langle\beta\rangle$ είναι ισόμορφη προς την κυκλική ομάδα $(\mathbb{Z}_{15}, +)$, αφού η τάξη τού $(\alpha, \beta) \in \langle\alpha\rangle \times \langle\beta\rangle$ ισούται με 15, βλ. Άσκηση 59. Άρα, $G \cong \mathbb{Z}_{15}$. □

Παρατήρηση 2.4.12. Το προηγούμενο αποτέλεσμα αποτελεί παράδειγμα ενός γενικού θεωρήματος, βλ. Θεώρημα 7.3.1, που θα αποδείξουμε στο τελευταίο κεφάλαιο και στο οποίο αποδεικνύεται ότι μια ομάδα τάξης n είναι κυκλική, αν και μόνο αν, ο ΜΚΔ$(n, \varphi(n))$ ισούται με 1.

Θεώρημα 2.4.13. *Κάθε ομάδα $(G, \star)$ τάξης p^α, $\alpha \geq 1$, όπου p είναι ένας πρώτος αριθμός, έχει μη τετριμμένο κέντρο.*

Απόδειξη. Από την εξίσωση κλάσεων γνωρίζουμε ότι

$$[G : 1] = [\mathcal{Z}(G) : 1] + \sum_{j=1}^{\ell} [G : \mathcal{C}_G(\alpha_j)],$$

όπου τα $\alpha_j, j = 1, \ldots, \ell$ είναι οι αντιπρόσωποι των κλάσεων με περισσότερα τού ενός στοιχεία. Ο πρώτος αριθμός p διαιρεί την τάξη $[G : 1]$ τής G καθώς και κάθε δείκτη $[G : \mathcal{C}_G(\alpha_j)]$, αφού $[G : \mathcal{C}_G(\alpha_j)] \geq 2$. Επομένως, ο p διαιρεί την τάξη $[\mathcal{Z}(G) : 1]$ τού κέντρου τής G και γι' αυτό $[\mathcal{Z}(G) : 1] \geq p \geq 2$. □

Θεώρημα 2.4.14. *Κάθε ομάδα $(G, \star)$ τάξης p^2, όπου ο p είναι πρώτος αριθμός, είναι αβελιανή και μάλιστα ισόμορφη ή προς την $\mathbb{Z}_{p^2}$ ή προς την $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Απόδειξη. Το κέντρο $\mathcal{Z}(G)$ τής G είναι μη τετριμμένο και γι' αυτό $[\mathcal{Z}(G) : 1] = p^2$ ή $[\mathcal{Z}(G) : 1] = p$. Στην πρώτη περίπτωση η G είναι αβελιανή, αφού $G = \mathcal{Z}(G)$ και στη δεύτερη περίπτωση η G είναι και πάλι αβελιανή, αφού η πηλικοομάδα $G/\mathcal{Z}(G)$ είναι κυκλική ως έχουσα τάξη τον πρώτο αριθμό p.
Ώστε η G είναι σε κάθε περίπτωση αβελιανή.

Αν η G διαθέτει ένα στοιχείο τάξης p^2, τότε $G \cong \mathbb{Z}_{p^2}$.
Διαφορετικά κάθε στοιχείο τής G, που δεν είναι το ουδέτερο, έχει τάξη p. Θεωρούμε ένα τέτοιο στοιχείο $x \in G, x \neq e_G$ και ένα ακόμα στοιχείο $y \in G \setminus \langle x\rangle$. Αμφότερα τα x, y έχουν τάξη p και $\langle x\rangle \bigcap \langle y\rangle = \{e_G\}$, αφού η τάξη $[\langle x\rangle \bigcap \langle y\rangle : 1]$ είναι, ως διαιρέτης τής τάξης $[\langle x\rangle : 1]$, ή 1 ή p. Αλλά, αν $[\langle x\rangle \bigcap \langle y\rangle : 1] = p$, τότε $y \in \langle x\rangle$, πράγμα άτοπο.

Επειδή η G είναι αβελιανή, οι $\langle x\rangle$ και $\langle y\rangle$ είναι ορθόθετες υποομάδες και αφού $\langle x\rangle \bigcap \langle y\rangle = \{e_G\}$, συμπεραίνουμε, σύμφωνα με την Άσκηση A88, ότι η $\langle x\rangle\langle y\rangle$ είναι ισόμορφη προς το ευθύ γινόμενο $\langle x\rangle \times \langle y\rangle$ με $[\langle x\rangle\langle y\rangle : 1] = p^2$. Επομένως, $G = \langle x\rangle\langle y\rangle \cong \langle x\rangle \times \langle y\rangle \cong \mathbb{Z}_p \times \mathbb{Z}_p$. □

2.5 Ποια είναι η Τιμή τής Πιθανότητας δύο Στοιχεία μιας Ομάδας να μετατίθενται;

Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης $[G:1] < \infty$ και g, α δύο οποιαδήποτε στοιχεία της, όχι απαραιτήτως διαφορετικά. Θα εξετάσουμε ποιες τιμές μπορεί να λάβει η πιθανότητα $\mathrm{Pr}(G)$ ώστε $g\alpha = \alpha g$, βλ. [14].

Παρατηρούμε ότι αν η G είναι μια αβελιανή ομάδα, τότε $\mathrm{Pr}(G) = 1$, αφού $\forall (g, \alpha) \in G \times G$ είναι $g\alpha = \alpha g$.

Γενικώς, θεωρούμε το σύνολο

$$L = \{(g, \alpha) \in G \times G \mid g\alpha = \alpha g\},$$

τότε,

$$\mathrm{Pr}(G) = \frac{|L|}{|G \times G|} = \frac{|L|}{[G:1]^2},$$

όπου με $|S|$ συμβολίζουμε, ως συνήθως, το πλήθος των στοιχείων ενός συνόλου S.

Θεώρημα 2.5.1. *Αν $(G, \star)$ είναι μια ομάδα τάξης $[G:1] < \infty$, τότε*

$$\mathrm{Pr}(G) = \frac{r}{[G:1]}, \text{ όπου } r \text{ είναι το πλήθος των κλάσεων συζυγίας τής } G.$$

Επιπλέον, αν η G δεν είναι αβελιανή, τότε $\mathrm{Pr}(G) \leq \frac{5}{8}$.

Απόδειξη. Παρατηρούμε ότι

$$L = \bigcup_{g \in G} L_g, \text{ όπου } L_g = \{(g, \alpha) \mid \alpha \in G, g\alpha = \alpha g\}.$$

Τα σύνολα $L_g, g \in G$ χορηγούν μια διαμέριση τού L, αφού αν $L_g \bigcap L_h \neq \emptyset$, τότε $\exists (x, y) \in L_g \bigcap L_h$ και τότε $g = x = h$. Επομένως, $L_g = L_h$.

Έτσι έχουμε

$$|L| = \sum_{g \in G} |L_g|.$$

Αλλά $\forall g \in G$, το πλήθος $|L_g|$ ισούται με το πλήθος των στοιχείων τού συνόλου $G^g := \{\alpha \in G \mid g\alpha g^{-1} = \alpha\}$, αφού η απεικόνιση

$$L_g \to G^g, (g, \alpha) \mapsto \alpha$$

είναι αμφιρριπτική, δηλαδή «$1-1$» και «επί», επειδή

$$(g, \alpha) \in L_g \Leftrightarrow g\alpha = \alpha g \Leftrightarrow g\alpha g^{-1} = \alpha \Leftrightarrow \alpha \in G^g.$$

Επομένως,

$$|L| = \sum_{g \in G} | L_g | = \sum_{g \in G} | G^g | \tag{*}$$

Όμως για κάθε $g \in G$, το $G^g = \{\alpha \in G \mid g\alpha g^{-1} = \alpha\}$ είναι το σύνολο των στοιχείων τής G που μένουν σταθερά από το g ως προς τη δράση τής συζυγίας $G \times G \to G, (g, \alpha) \mapsto g\alpha g^{-1}$ και από τον τύπο τού Burnside, βλ. Θεώρημα 2.2.11, έχουμε ότι το πλήθος r των κλάσεων συζυγίας ισούται με

$$r = \frac{1}{[G:1]} \sum_{g \in G} |G^g|. \tag{**}$$

Από τις (*) και (**) έπεται $[G:1]r = |L|$ και συνεπώς

$$\Pr(G) = \frac{|L|}{[G:1]^2} = \frac{[G:1]r}{[G:1]^2} = \frac{r}{[G:1]}.$$

Θα αποδείξουμε τώρα ότι αν η G δεν είναι αβελιανή, τότε για την πιθανότητα $\Pr(G)$, το κλάσμα $5/8$ είναι το ελάχιστο άνω φράγμα.

Θεωρούμε τη διαμέριση τής G στις κλάσεις συζυγίας της:

$$G = \mathcal{Z}_1 \bigcup \mathcal{Z}_2 \bigcup \cdots \bigcup \mathcal{Z}_t \bigcup \mathcal{K}_1 \bigcup \mathcal{K}_2 \bigcup \cdots \bigcup \mathcal{K}_\ell,$$

όπου οι $\mathcal{Z}_i, 1 \leq i \leq t$ είναι οι κλάσεις συζυγίας με ένα στοιχείο και $\mathcal{K}_j, 1 \leq j \leq \ell$ οι κλάσεις συζυγίας με τουλάχιστον δύο στοιχεία. Η ένωση $\mathcal{Z}_1 \bigcup \mathcal{Z}_2 \bigcup \cdots \bigcup \mathcal{Z}_t$ ισούται με το κέντρο $\mathcal{Z}(G)$ τής G και γι' αυτό $[\mathcal{Z}(G):1] = t$.

Από την Εξίσωση των Κλάσεων παίρνουμε

$$[G:1] = [\mathcal{Z}(G):1)] + \sum_{j=1}^{\ell} |\mathcal{K}_j| \geq [\mathcal{Z}(G):1)] + 2\ell,$$

επειδή $|\mathcal{K}_j| \geq 2$.

Συνεπώς,

$$\frac{[G:1] - [\mathcal{Z}(G):1]}{2} \geq \ell.$$

Επομένως, για το πλήθος r των κλάσεων συζυγίας έχουμε ότι

$$r = [\mathcal{Z}(G):1] + \ell \leq [\mathcal{Z}(G):1] + \frac{[G:1] - [\mathcal{Z}(G):1]}{2} = \frac{[G:1] + [\mathcal{Z}(G):1]}{2}$$

Όμως, αφού η G δεν είναι αβελιανή, πρέπει να ισχύει $[\mathcal{Z}(G):1] \leq [G:1]/4$. Επειδή διαφορετικά, δηλαδή αν ήταν$[\mathcal{Z}(G):1] > [G:1]/4$, τότε θα είχαμε ότι το $4 > ([G:1]/[\mathcal{Z}(G):1]) = [G/\mathcal{Z}(G):1]$ και τότε η $G/\mathcal{Z}(G)$ είναι κυκλική, που συνεπάγει ότι η G είναι αβελιανή, βλ. Άσκηση A78.

Έτσι διαπιστώνουμε ότι για το πλήθος r των κλάσεων συζυγίας έχουμε

$$r = [\mathcal{Z}(G):1] + \ell \leq \frac{[G:1] + [\mathcal{Z}(G):1]}{2} \leq \frac{[G:1]}{2} + \frac{[G:1]/4}{2} = \frac{5}{8}[G:1].$$

Επομένως,

$$\Pr(G) = \frac{r}{[G:1]} \leq \frac{\frac{5}{8}[G:1]}{[G:1]} = \frac{5}{8}.$$

□

Παρατήρηση 2.5.2. Ο αριθμός $5/8$ είναι όντως το ελάχιστο άνω φράγμα στην περίπτωση των μη αβελιανών ομάδων. Για παράδειγμα, αν η ομάδα G είναι η διεδρική ομάδα D_4 ή η ομάδα των τετρανίων $\mathcal{Q}_8$, τότε $\Pr(G) = 5/8$, αφού και στις δύο συγκεκριμένες περιπτώσεις, το πλήθος των κλάσεων συζυγίας ισούται με 5 και το πλήθος των στοιχείων των ομάδων ισούται με 8.

Ασκήσεις στη Δράση Συζυγίας

Λυμένες Ασκήσεις

Α 109. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι κ είναι το πλήθος των κλάσεων συζυγίας της. Να δειχθεί ότι

$$\kappa = \frac{1}{[G:1]} \sum_{g \in G} [\mathcal{C}_G(g) : 1],$$

όπου $\mathcal{C}_G(g)$ είναι ο κεντροποιητής τού $g \in G$.

Λύση. Από το Θεώρημα Burnside, βλ. Θεώρημα 2.2.11, γνωρίζουμε ότι όταν η $\varphi : G \times A \to A$ είναι δράση μιας ομάδας G επί ενός συνόλου A, τότε το πλήθος κ των τροχιών τού A δίνεται από τον τύπο:

$$\kappa = \frac{1}{[G:1]} \sum_{g \in G} |A^g|,$$

όπου $A^g = \{a \in A \mid g\varphi a = a\}$ είναι το σύνολο των $a \in A$ που μένουν σταθερά από τη δράση φ τού στοιχείου $g \in G$. Εδώ το σύνολο A ισούται με την ίδια την ομάδα G και η δράση φ είναι η συζυγία. Γι' αυτό το G^g ισούται με το σύνολο $\{a \in G \mid gag^{-1} = a\}$, το οποίο είναι ο κεντροποιητής $\mathcal{C}_G(g)$. Άρα,

$$\kappa = \frac{1}{[G:1]} \sum_{g \in G} [\mathcal{C}_G(g) : 1].$$

Α 110. Έστω $(G, \star)$ μια ομάδα και $\mathcal{Z}(G)$ το κέντρο της. Αν $[G : \mathcal{Z}(G)] = n \in \mathbb{N}$, τότε να δειχθεί ότι οποιαδήποτε κλάση συζυγίας αποτελείται από το πολύ n το πλήθος στοιχεία.

Λύση. Έστω ότι a είναι ένα στοιχείο τής G και ότι $\mathcal{K}_a$ είναι η κλάση συζυγίας του. Το πλήθος των στοιχείων τής $\mathcal{K}_a$ ισούται με τον δείκτη $[G : \mathcal{C}_G(a)]$, όπου $\mathcal{C}_G(a) = \{g \in G \mid ga = ag\}$ είναι ο κεντροποιητής τού στοιχείου a. Ως γνωστόν, το κέντρο $\mathcal{Z}(G)$ τής G περιέχεται στον $\mathcal{C}_G(a)$. Επιπλέον, επειδή ο δείκτης $[G : \mathcal{Z}(G)]$ είναι πεπερασμένος, γνωρίζουμε από την Άσκηση Α45 ότι $n = [G : \mathcal{Z}(G)] = [G : \mathcal{C}_G(a)][\mathcal{C}_G(a) : \mathcal{Z}(G)]$. Επομένως, $|\mathcal{K}_a| = [\mathcal{C}_G(a) : \mathcal{Z}(G)] \leq n$.

Α 111. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης p^α, $\alpha \in \mathbb{N}$, όπου ο p είναι ένας πρώτος αριθμός και ότι $K \trianglelefteq G$ είναι μια ορθόθετη υποομάδα τής G με $K \neq \{e_G\}$. Να δειχθεί ότι η τομή $K \bigcap \mathcal{Z}(G)$ είναι $\neq \{e_G\}$.

Λύση. Κατ' αρχάς υπενθυμίζουμε, βλ. Θεώρημα 2.4.13, ότι το κέντρο $\mathcal{Z}(G)$ είναι $\neq \{e_G\}$. Η αντιστοιχία $\sigma : G \times K \to K$, $(g,k) \mapsto g\sigma k := gkg^{-1}$ είναι μια καλά ορισμένη απεικόνιση, διότι η K είναι ορθόθετη υποομάδα τής G. Είναι εύκολη η διαπίστωση ότι πρόκειται για μια δράση τής G επί τού K (ουσιαστικά η δράση τής G είναι η συζυγία επί τού K). Από το Λήμμα 2.3.10, γνωρίζουμε ότι ο p διαιρεί τη διαφορά $|K| - |\mathrm{Fix}_\sigma(K)|$, όπου $\mathrm{Fix}_\sigma(K) = \{k \in K \mid gkg^{-1} = k\}$ είναι το σύνολο των σταθερών στοιχείων τής K. Ο p είναι διαιρέτης τού $|K| = [K : 1]$ διότι ο $[K : 1]$ είναι διαιρέτης τής τάξης $p^\alpha = [G : 1]$ και $[K : 1] \geq 2$. Επομένως, ο p διαιρεί το $|\mathrm{Fix}_\sigma(K)|$, που ως εκ τούτου είναι ένα θετικό πολλαπλάσιο τού p, αφού $|\mathrm{Fix}_\sigma(K)| \geq 1$ (το ουδέτερο e_G ανήκει στο σύνολο των σταθερών στοιχείων). Επομένως, υπάρχει κάποιο $k \in \mathrm{Fix}_\sigma(K), k \neq e_G$. Προφανώς, το $k \in \mathcal{Z}(G)$ και επομένως $K \bigcap \mathcal{Z}(G) \neq \{e_G\}$.

Α 112. Έστω γ ένας κύκλος μήκους n τής συμμετρικής ομάδας S_n. Να δειχθεί ότι ο κεντροποιητής $\mathcal{C}_{S_n}(\gamma)$ τού γ ισούται με την κυκλική υποομάδα $\langle\gamma\rangle$.

Λύση. Το πλήθος των κύκλων μήκους n στην S_n ισούται με

$$\frac{n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1}{n} = (n-1)!$$

Θεωρούμε τη δράση σ τής S_n επί τού εαυτού της μέσω συζυγίας:

$$\sigma : S_n \times S_n \to S_n, (\tau, \alpha) \mapsto \tau \circ \alpha \circ \tau^{-1}.$$

Αν γ είναι οποιοσδήποτε κύκλος μήκους n, τότε η κλάση συζυγίας του $\mathcal{K}_\gamma$ αποτελείται από όλους τους κύκλους μήκους n, αφού γνωρίζουμε ότι αν γ_1, γ_2 είναι δύο κύκλοι n, τότε υπάρχει $\tau \in S_n$ με $\tau \circ \gamma_1 \circ \tau^{-1} = \gamma_2$, βλ. Θεώρημα 2.4.4. Γι' αυτό το πλήθος $|\mathcal{K}_\gamma|$ των στοιχείων τής $\mathcal{K}_\gamma$ ισούται με $(n-1)!$.
Γνωρίζουμε επίσης ότι $|\mathcal{K}_\gamma| = [S_n : \mathcal{C}_{S_n}(\gamma)]$, όπου $\mathcal{C}_{S_n}(\gamma)$ είναι ο κεντροποιητής τού γ, δηλαδή η υποομάδα

$$\mathcal{C}_{S_n}(\gamma) = \{\sigma \in G \mid \sigma \circ \gamma \circ \sigma^{-1} = \gamma\} = \{\sigma \in G \mid \sigma \circ \gamma = \gamma \circ \sigma^{-1}\}.$$

Επομένως, $[S_n : \mathcal{C}_{S_n}(\gamma)] = (n-1)! \Rightarrow [\mathcal{C}_{S_n}(\gamma) : 1] = n$. Όμως επειδή $\langle\gamma\rangle \leq \mathcal{C}_{S_n}(\gamma)$ και $[\langle\gamma\rangle : 1] = n$, έπεται $\mathcal{C}_{S_n}(\gamma) = \langle\gamma\rangle$.

Α 113. Να προσδιοριστούν όλες οι πεπερασμένες ομάδες με ακριβώς δύο κλάσεις συζυγίας.

Λύση. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης n με ακριβώς δύο κλάσεις συζυγίας. Επειδή πάντοτε το $\{e_G\}$ είναι μια κλάση συζυγίας, συμπεραίνουμε ότι η άλλη κλάση συζυγίας $\mathcal{K}$ έχει $n-1$ το πλήθος στοιχεία. Αν $b \in \mathcal{K}$, τότε το πλήθος τής $\mathcal{K}$ ισούται με τον δείκτη $[G : \mathcal{C}_G(b)]$, όπου $\mathcal{C}_G(b)$ είναι ο κεντροποιητής τού b. Άρα, το $n-1$ είναι διαιρέτης τού n και ως εκ τούτου, το $n = 2$ και η G είναι ισόμορφη προς την $(\mathbb{Z}_2, +)$.

Προτεινόμενες Ασκήσεις

ΠΑ 104. Να προσδιοριστεί ένας αντιπρόσωπος από κάθε κλάση συζυγίας των στοιχείων τάξης 4 των συμμετρικών ομάδων $(S_4, \circ)$ και $(S_8, \circ)$.

ΠΑ 105. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι a είναι ένα στοιχείο τής G. Να δειχθεί ότι το πλήθος των στοιχείων τής κλάσης συζυγίας $\mathcal{K}_a$ τού a ισούται με το πλήθος των στοιχείων τής κλάσης συζυγίας $\mathcal{K}_{a^{-1}}$ τού a^{-1}.

Αν επιπλέον η G έχει άρτια τάξη, τότε να δειχθεί ότι υπάρχει τουλάχιστον ένα $a \in G$ με $a \neq e_G$, τέτοιο ώστε τα a και a^{-1} να ανήκουν στην ίδια κλάση συζυγίας.

ΠΑ 106. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης n και ότι g είναι ένα στοιχείο $\in G$ τάξης m. Αν το πλήθος των στοιχείων τής κλάσης συζυγίας $\mathcal{K}_g$ τού g ισούται με κ, τότε να δειχθεί ότι το κ είναι διαιρέτης τού ακέραιου n/m.

ΠΑ 107. Έστω ότι $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι δύο πεπερασμένες ομάδες και ότι $G_1 \times G_2$ είναι το ευθύ γινόμενό τους. Να δειχθεί ότι το πλήθος των κλάσεων συζυγίας τής $G_1 \times G_2$ ισούται με γινόμενο τού πλήθους των κλάσεων συζυγίας τής G_1 επί το πλήθος των κλάσεων συζυγίας τής G_2.

ΠΑ 108. Να δειχθεί ότι μια μη αβελιανή ομάδα $(G, \star)$ τάξης p^3, όπου ο p είναι πρώτος αριθμός, έχει μη τετριμμένο κέντρο.

Κεφάλαιο 3

Θεωρία Sylow

3.1 Τα Θεωρήματα Sylow

Ορισμός 3.1.1. Μια ομάδα $(G, \star)$ τάξης p^α, όπου p είναι ένας πρώτος αριθμός και $\alpha \in \mathbb{N} \bigcup \{0\}$ ονομάζεται μια *p–ομάδα*.

Παρατήρηση 3.1.2. (α′) Σύμφωνα με τον προηγούμενο ορισμό για κάθε πρώτο p, η τετριμμένη ομάδα που αποτελείται από ένα και μόνο στοιχείο είναι p–ομάδα.

(β′) Όταν κάθε στοιχείο μιας πεπερασμένης ομάδας $G \neq \{e_G\}$ είναι δύναμη ενός πάγιου πρώτου αριθμού p, τότε η G είναι μια p–ομάδα. Πράγματι, ο πρώτος αριθμός p διαιρεί την τάξη $[G : 1]$, αφού υπάρχουν στοιχεία με τάξη δύναμη τού συγκεκριμένου p. Αν q είναι ένας πρώτος διαιρέτης τής $[G : 1]$, τότε από το Θεώρημα Cauchy, βλ. Θεώρημα 2.3.11, υπάρχει ένα στοιχείο τής G τάξης q. Συνεπώς, $q = p$ και η τάξη $[G : 1]$ είναι δύναμη τού p.

Για τις p–ομάδες ισχύουν τα ακόλουθα:

Πρόταση 3.1.3. *Έστω ότι $(G, \star)$ είναι μια p–ομάδα τάξης p^α, $\alpha \in \mathbb{N} \bigcup \{0\}$.*

(α′) *Για κάθε $\beta \in \mathbb{N} \bigcup \{0\}$ με $\beta \leq \alpha$, υπάρχει μια υποομάδα $H \leq G$ με τάξη p^β.*

(β′) *Αν $\alpha \in \mathbb{N}$, τότε κάθε υποομάδα H τής G τάξης $p^{\alpha-1}$ είναι μια ορθόθετη υποομάδα τής G και επιπλέον, υπάρχει μια αλυσίδα υποομάδων:*

$$G_0 = \{e_G\} \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_{\alpha-1} \trianglelefteq G_\alpha = G$$

με $[G_i : 1] = p^i, i = 0, \ldots, \alpha$ και όπου $\forall i, 0 \leq i \leq \alpha - 1$ η G_i είναι μια ορθόθετη υποομάδα τής G_{i+1}.

Απόδειξη. (α′) Θα εκτελέσουμε την απόδειξη με επαγωγή ως προς τη δύναμη $\alpha \in \mathbb{N} \bigcup \{0\}$ τού p. Για $\alpha = 0$ ή 1 ο ισχυρισμός είναι προφανής. Από το Θεώρημα 2.4.14, προκύπτει ότι για $\alpha = 2$, ο ισχυρισμός είναι επίσης αληθής. Έστω ότι η πρόταση είναι αληθής $\forall m, 2 \leq$

$m < n$. Θα την αποδείξουμε για μια ομάδα G τάξης p^n.
Από το Θεώρημα 2.4.13, γνωρίζουμε ότι το κέντρο $\mathcal{Z}(G)$ τής G είναι μη τετριμμένο. Ως εκ τούτου, η τάξη τού $\mathcal{Z}(G)$ είναι μια θετική δύναμη τού πρώτου p. Από το Θεώρημα Cauchy, βλ. Θεώρημα 2.3.11, γνωρίζουμε ότι υπάρχει κάποιο $x \in \mathcal{Z}(G)$ τάξης p. Προφανώς, η κυκλική υποομάδα $\langle x \rangle$ είναι ορθόθετη υποομάδα τής G.
Θεωρούμε τον φυσικό επιμορφισμό $\pi : G \to G/\langle x \rangle, g \mapsto g\langle x \rangle$. Η τάξη τής πηλικοομάδας $G/\langle x \rangle$ είναι p^{n-1} και λόγω τής επαγωγικής υπόθεσης, η $G/\langle x \rangle$ διαθέτει $\forall \beta \in \mathbb{N} \bigcup \{0\}, 0 \leq \beta \leq n-1$, μια υποομάδα $\overline{H}$ τάξης p^{β}. Η προεικόνα της $H = \pi^{-1}(\overline{H})$ είναι μια υποομάδα τής G τάξης $p^{\beta+1}$. Συνεπώς, η G διαθέτει $\forall \beta \in \mathbb{N} \bigcup \{0\}, 0 \leq \beta \leq n$, μια υποομάδα τάξης p^{β}.

(β′) Σύμφωνα με το (α′) υπάρχει μια αλυσίδα υποομάδων

$$G_0 = \{e_G\} \leq G_1 \leq G_2 \leq \cdots \leq G_{\alpha-1} \leq G_\alpha = G,$$

όπου $\forall i, 0 \leq i \leq \alpha$, η τάξη τής G_i είναι p^i. Παρατηρούμε ότι $\forall i, 1 \leq i \leq \alpha$ ο δείκτης $[G_i : G_{i-1}]$ ισούται με τον πρώτο αριθμό p και επειδή πρόκειται για τον μικρότερο πρώτο που διαιρεί την τάξη τής ομάδας (αφού δεν υπάρχει άλλος), έπεται από το Πόρισμα 2.3.7 ότι η G_{i-1} είναι ορθόθετη υποομάδα τής G_i. □

Η προηγούμενη πρόταση γενικεύεται στη λεγόμενη Θεωρία Sylow που θα παρουσιάσουμε αμέσως.

Ορισμός 3.1.4. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης $p^{\alpha}m$, όπου p είναι ένας πρώτος αριθμός, $\alpha \in \mathbb{N} \bigcup \{0\}$ και $p \nmid m$. Κάθε υποομάδα τής G τάξης p^{α} ονομάζεται μια *p–Sylow υποομάδα* τής G.

Συμβολίζουμε με $\mathrm{Syl}_p(G)$ το σύνολο των p–Sylow υποομάδων τής G και με $n_p(G)$, ή απλώς με n_p όταν είναι σαφές για ποια ομάδα πρόκειται, το πλήθος των στοιχείων τού συνόλου $\mathrm{Syl}_p(G)$.

Θα αποδείξουμε ένα από τα σημαντικότερα θεωρήματα τής κλασικής Θεωρίας Ομάδων.

Θεώρημα 3.1.5 (Sylow). *Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης $p^{\alpha}m$, όπου p είναι ένας πρώτος αριθμός, $\alpha \in \mathbb{N} \bigcup \{0\}$ και $p \nmid m$. Τότε ισχύουν τα επόμενα:*

(α′) *Το σύνολο $\mathrm{Syl}_p(G)$ δεν είναι κενό.*

(β′) *Αν P είναι οποιαδήποτε p–Sylow υποομάδα τής G και Q είναι οποιαδήποτε p–υποομάδα τής G, τότε υπάρχει $g \in G$ με $Q \leq gPg^{-1}$. Ιδιαιτέρως, όλες οι p–Sylow υποομάδες τής G είναι συζυγείς.*

(γ′) *Για το πλήθος $n_p(G)$ των p–Sylow υποομάδων τής G έχουμε:*

$$n_p(G) \equiv 1 \bmod p \text{ και } n_p(G) = [G : \mathcal{N}_G(P)],$$

όπου $P \in \mathrm{Syl}_p(G)$ και $\mathcal{N}_G(P) = \{g \in G \mid gPg^{-1} = P\}$ είναι ο ορθοθετοποιητής τής P.
Ιδιαιτέρως, $n_G(P) | m$.

Πριν από την απόδειξη τού θεωρήματος αποδεικνύουμε το

Λήμμα 3.1.6. *Αν P είναι μια p–Sylow υποομάδα τής G και Q είναι οποιαδήποτε p–υποομάδα τής G, τότε $\mathcal{N}_G(P) \bigcap Q = P \bigcap Q$.*

Απόδειξη. Θέτουμε $H = \mathcal{N}_G(P) \bigcap Q$. Από $P \leq \mathcal{N}_G(P)$ έπεται ότι $P \bigcap Q \leq \mathcal{N}_G(P) \bigcap Q = H$. Συνεπώς, για να δειχθεί η ισότητα τού λήμματος είναι αρκετό να δειχθεί ότι η $H = \mathcal{N}_G(P) \bigcap Q$ περιέχεται στην $P \bigcap Q$. Αλλά $H \leq Q$ και γι' αυτό υπολείπεται η απόδειξη ότι $H \leq P$.

Είναι αρκετό να αποδείξουμε ότι:

(Π) *Το σύνολο PH είναι μια υποομάδα τής G και μάλιστα μια p–υποομάδα.*

Αφού τότε από $P \leq PH$, συμπεραίνουμε ότι $P = PH$, διότι η τάξη τής P είναι η μεγαλύτερη δύναμη τού p που διαιρεί την τάξη $[G : 1] = p^{\alpha} m$. Κατόπιν από την ισότητα $P = PH$, συμπεραίνουμε ότι $H \leq P$ που ολοκληρώνει την απόδειξη.

Η απόδειξη τής (Π) Επειδή $H \leq \mathcal{N}_G(P)$, έχουμε $\forall h \in H, hP = Ph$ και γι' αυτό, βλ. Άσκηση A37, η PH είναι μια υποομάδα τής G. Υπολείπεται η απόδειξη ότι η τάξη τής PH είναι δύναμη τού p.

Για το πλήθος των στοιχείων τής PH γνωρίζουμε, βλ. Πρόταση 2.3.9, ότι

$$[PH : 1] = \frac{[P : 1][H : 1]}{[P \bigcap H : 1]}. \tag{*}$$

Ο αριθμητής τής σχέσης (*) είναι δύναμη τού p, επειδή και η $[P : 1]$ είναι δύναμη τού p, αφού η P είναι p–Sylow υποομάδα τής G, και η $[H : 1]$ είναι δύναμη τού p, αφού η H είναι μια p–υποομάδα, ως υποομάδα τής p–υποομάδας Q. Για τους ίδιους λόγους και ο παρονομαστής τής σχέσης (*) είναι μια δύναμη τού p.

Συνεπώς, η PH είναι μια p–υποομάδα. □

Είμαστε τώρα σε θέση να αποδείξουμε τον πρώτο ισχυρισμό τού Θεωρήματος Sylow, βλ. Θεώρημα 3.1.5: (α′) *Το σύνολο* $\mathrm{Syl}_p(G)$ *δεν είναι κενό.*

Απόδειξη. Η απόδειξη θα εκτελεστεί με επαγωγή ως προς $[G : 1]$. Αν $[G : 1] = 1$ δεν χρειάζεται να αποδειχθεί κάτι. Ας δούμε τι συμβαίνει στην περίπτωση $[G : 1] = 2$. Η G είναι μια 2–ομάδα και $Syl_2(G) = \{G\}$.

Έστω ότι ο ισχυρισμός είναι αληθής για κάθε ομάδα G' με τάξη $[G' : 1] < [G : 1]$, δηλαδή ότι $\mathrm{Syl}_p(G') \neq \emptyset$, όταν $p \mid [G' : 1]$.

Για την ομάδα G, θεωρούμε την Εξίσωση των Κλάσεων, βλ. Θεώρημα 2.4.8:

$$[G : 1] = [\mathcal{Z}(G) : 1] + \sum_{j=1}^{\ell} [G : \mathcal{C}_G(g_j)],$$

όπου τα στοιχεία g_j διατρέχουν τους αντιπροσώπους από τις κλάσεις συζυγίας με περισσότερα τού ενός στοιχεία. Συνεπώς, $\forall j, 1 \leq j \leq \ell, [G : \mathcal{C}_G(g_j)] \geq 2$

Αν ο πρώτος p διαιρεί την τάξη τού κέντρου $\mathcal{Z}(G)$, τότε από το Θεώρημα Cauchy, υπάρχει $x \in \mathcal{Z}(G)$ τάξης p. Η κυκλική υποομάδα $\langle x \rangle$ περιέχεται στο $\mathcal{Z}(G)$ και συνεπώς είναι ορθόθετη. Θεωρούμε τον φυσικό επιμορφισμό $\pi : G \to G/\langle x\rangle$. Η τάξη τής $G/\langle x\rangle$ ισούται με $[G : 1]/p = p^{\alpha-1}m$. Λόγω της επαγωγικής υπόθεσης, η $G/\langle x\rangle$ διαθέτει μια υποομάδα P' τάξης $p^{\alpha-1}$. Τώρα η υποομάδα $P = \pi^{-1}(P')$ τής G έχει τάξη p^{α} και $P \in \mathrm{Syl}_p(G)$.

Αν ο πρώτος p δεν διαιρεί την τάξη τού κέντρου $\mathcal{Z}(G)$, τότε δεν διαιρεί τουλάχιστον για ένα $k, 1 \le k \le \ell$ κάποιον προσθετέο $[G : \mathcal{C}_G(g_k)] \ge 2$. Επειδή

$$p^{\alpha}m = [G : 1] = [G : \mathcal{C}_G(g_k)][\mathcal{C}_G(g_k) : 1],$$

έπεται ότι ο p^{α} διαιρεί την τάξη $[\mathcal{C}_G(g_k) : 1]$, η οποία είναι γνησίως μικρότερη από την τάξη $[G : 1]$ τής G. Λόγω τής επαγωγικής υπόθεσης, η υποομάδα $\mathcal{C}_G(g_k)$ διαθέτει μια p–Sylow υποομάδα P τάξης p^{α}. Η P ως έχουσα τάξη p^{α} είναι μια p–Sylow υποομάδα τής G. $\square$

Πριν προχωρήσουμε στην απόδειξη των (β′) και (γ′) τού Θεωρήματος 3.1.5 θα κάνουμε ορισμένες παρατηρήσεις.

Ήδη έχουμε αποδείξει ότι $\mathrm{Syl}_p(G) \neq \emptyset$. Έστω ότι P είναι μια υποομάδα με $P \in \mathrm{Syl}_p(G)$ και ότι

$$\mathcal{S} = \{gPg^{-1} \mid g \in G\} = \{P_1, P_2, \ldots, P_r\}$$

είναι το σύνολο των υποομάδων τής G που είναι συζυγείς τής P. Οποιαδήποτε υποομάδα H τής G δρα μέσω συζυγίας επί τού $\mathcal{S}$, δηλαδή

$$H \times \mathcal{S} \to \mathcal{S}, (h, P_i) \mapsto hP_ih^{-1}$$

και διαμερίζει το $\mathcal{S}$ σε s το πλήθος τροχιές $\mathcal{O}_i, 1 \le i \le s$. Ως εκ τούτου, $r = \sum_{i=1}^{s} |\mathcal{O}_i|$. Προσέξτε, ότι ενώ το πλήθος r των στοιχείων τού $\mathcal{S}$ είναι σταθερό, το πλήθος s των τροχιών μπορεί να μεταβάλλεται, ανάλογα με την υποομάδα H. Για παράδειγμα, αν $H = G$, τότε $s = 1$, ενώ αν $H = \{e_G\}$, τότε $s = r$. Βέβαια, ισχύει πάντοτε ότι $s \le r$.

Επιλέγουμε ως H μια p–υποομάδα Q τής G και αριθμούμε εκ νέου, αν είναι απαραίτητο, τα στοιχεία τού $\mathcal{S}$ έτσι ώστε τα πρώτα s να είναι οι αντιπρόσωποι των διαφορετικών τροχιών $\mathcal{O}_i, 1 \le i \le s$ τής δράσης συζυγίας $Q \times \mathcal{S} \to \mathcal{S}$. Από το Θεώρημα 2.2.8 γνωρίζουμε ότι το πλήθος των στοιχείων τής τροχιάς $\mathcal{O}_i$ ισούται με τον δείκτη $[Q : \mathcal{N}_Q(P_i)]$, αφού ο σταθεροποιητής τού P_i ως προς τη δράση τής συζυγίας είναι ο ορθοθετοποιητής $\mathcal{N}_Q(P_i) = \{q \in Q \mid qP_iq^{-1} = P_i\}$. Παρατηρούμε ότι $\mathcal{N}_Q(P_i) = \mathcal{N}_G(P_i) \bigcap Q$ και επειδή από το Λήμμα 3.1.6 γνωρίζουμε ότι $\mathcal{N}_G(P_i) \bigcap Q = P_i \bigcap Q$, συμπεραίνουμε ότι $\mathcal{N}_Q(P_i) = P_i \bigcap Q$. Συνεπώς,

$$|\mathcal{O}_i| = [Q : P_i \bigcap Q], \forall i, 1 \le i \le s.$$

Θα δείξουμε ότι για το πλήθος $|\mathcal{S}|$ των στοιχείων τού συνόλου $\mathcal{S}$ ισχύει

$$|\mathcal{S}| \equiv 1 \bmod p.$$

Απόδειξη. Επιλέγουμε να δράσει επί τού $\mathcal{S}$, μέσω συζυγίας, η p–Sylow υποομάδα P_1, η οποία είναι βεβαίως και στοιχείο τού $\mathcal{S}$.

Για το πλήθος των στοιχείων τής τροχιάς $\mathcal{O}_1$, έχουμε $|\mathcal{O}_1| = [P_1 : P_1 \bigcap P_1] = 1$. (Θυμηθείτε με ποιον τρόπο αριθμούμε κάθε φορά τα στοιχεία τού $\mathcal{S}$).
Ενώ για το πλήθος των στοιχείων οποιασδήποτε άλλης τροχιάς $\mathcal{O}_i, i \geq 2$, έχουμε $|\mathcal{O}_i| = [P_1 : P_i \bigcap P_1] \geq 2$. Αυτό είναι αληθές, επειδή η τομή $P_i \bigcap P_1$ περιέχεται γνήσια εντός τής P_i, αφού αν ήταν $P_i \bigcap P_1 = P_i$, τότε θα προέκυπτε $P_i = P_1$, διότι τα P_i και P_1 έχουν το ίδιο πλήθος στοιχείων. Συνεπώς για κάθε $i, 2 \leq i \leq s$, το πλήθος $|\mathcal{O}_i| = [P_1 : P_i \bigcap P_1]$ είναι μια θετική δύναμη n_i τού πρώτου αριθμού p, αφού ο συγκεκριμένος δείκτης είναι ένας διαιρέτης ≥ 2 τής τάξης $[P_1 : 1] = p^{\alpha}$.

Έτσι έχουμε:

$$|\mathcal{S}| = \sum_{i=1}^{s} |\mathcal{O}_i| = 1 + p^{n_2} + \cdots + p^{n_s}, \text{ όπου } n_i \in \mathbb{N}, \forall i = 2, \ldots, s.$$

Ώστε,

$$|\mathcal{S}| \equiv 1 \bmod p.$$

□

Θα αποδείξουμε τώρα τα (β′) και (γ′) τού Θεωρήματος 3.1.5.

(β′) *Αν P είναι οποιαδήποτε p–Sylow υποομάδα τής G και Q είναι οποιαδήποτε p–υποομάδα τής G, τότε υπάρχει $g \in G$ με $Q \leq gPg^{-1}$. Ιδιαιτέρως, όλες οι p–Sylow υποομάδες τής G είναι συζυγείς.*

Απόδειξη. Έστω μια p–υποομάδα Q και P μια σταθερώς επιλεγμένη p–Sylow υποομάδα τής G. Αν δεν υπάρχει $g \in G$ με $Q \leq gPg^{-1}$, τότε η Q δεν περιέχεται σε κανένα από τα στοιχεία τού $\mathcal{S} = \{gPg^{-1} \mid g \in G\} = \{P_1, P_2, \ldots, P_r\}$. Επομένως, $\forall i, 1 \leq i \leq r, Q \bigcap P_i \lneqq Q$ και γι' αυτό $\forall i, 1 \leq i \leq r, [Q : Q \bigcap P_i] \gneqq 1$. Συνεπώς, $\forall i, 1 \leq i \leq r$, ο δείκτης $[Q : Q \bigcap P_i]$ είναι μια θετική δύναμη τού πρώτου p, επειδή η Q είναι μια p–υποομάδα τής G. Τότε όμως επιτρέποντας να δράσει η Q μέσω συζυγίας επί τού $\mathcal{S}$ διαπιστώνουμε ότι ο p διαιρεί το πλήθος των στοιχείων οποιασδήποτε τροχιάς $\mathcal{O}$, αφού το πλήθος $|\mathcal{O}|$ ισούται με τον δείκτη $[Q : Q \bigcap P_i]$, όπου P_i είναι οποιοδήποτε στοιχείο τής τροχιάς $\mathcal{O}$. Όμως τότε ο p διαιρεί και το πλήθος $|\mathcal{S}|$, το οποίο μόλις προηγουμένως είδαμε ότι ικανοποιεί την $|\mathcal{S}| \equiv 1 \bmod p$. Αυτό είναι άτοπο. Επομένως, υπάρχει $g \in G$ με $Q \leq gPg^{-1}$.

Επιλέγοντας ως Q οποιαδήποτε p–Sylow υποομάδα P', διαπιστώνουμε ότι $\exists g \in G$ με $P' \leq gPg^{-1}$ και αφού πρόκειται για πεπερασμένα σύνολα με το ίδιο πλήθος στοιχείων , έπεται $P' = gPg^{-1}$. Συνεπώς, οποιαδήποτε p–Sylow υποομάδα είναι συζυγής με την P και $\mathrm{Syl}_p(G) = \mathcal{S} = \{gPg^{-1} \mid g \in G\}$. □

(γ′) *Για το πλήθος $n_p(G)$ των p–Sylow υποομάδων τής G έχουμε:*

$$n_p(G) \equiv 1 \bmod p \text{ και } n_p(G) = [G : \mathcal{N}_G(P)],$$

όπου $P \in \mathrm{Syl}_p(G)$ και $\mathcal{N}_G(P) = \{g \in G \mid gPg^{-1} = P\}$ είναι ο ορθοθετοποιητής τής P. Ιδιαιτέρως, $n_p(G) \mid m$.

Απόδειξη. Προηγουμένως διαπιστώσαμε ότι $\mathrm{Syl}_p(G) = \mathcal{S} = \{gPg^{-1} \mid g \in G\}$. Αφού $|\mathcal{S}| \equiv 1 \bmod p$ και $n_p(G)$ είναι το πλήθος των στοιχείων τού $\mathrm{Syl}_p(G)$, συμπεραίνουμε ότι $n_p(G) \equiv 1 \bmod p$.

Στο σύνολο $\mathrm{Syl}_p(G)$ δρα μέσω συζυγίας και η ίδια η ομάδα G και μάλιστα μεταβατικώς. Το πλήθος $n_p(G)$ των στοιχείων τής μοναδικής τροχιάς ως προς αυτή τη δράση ισούται με τον δείκτη $[G : \mathcal{N}_G(P)]$ τού σταθεροποιητή $\mathcal{N}_G(P)$ οποιουδήποτε στοιχείου $P \in \mathrm{Syl}_p(G)$. Επομένως, $n_p(G) \mid p^\alpha m$ και αφού $n_p(G) \equiv 1 \bmod p$, συμπεραίνουμε ότι $n_p(G) \mid m$. □

Παρατήρηση 3.1.7. Όταν το πλήθος n_p των p-Sylow υποομάδων μιας ομάδας $(G, \star)$ ισούται με 1, τότε αυτή η μοναδική p-Sylow υποομάδα είναι ορθόθετη υποομάδα τής G, βλ. επίσης Πρόταση 3.2.12. Πράγματι, όταν P είναι αυτή η μοναδική p-Sylow υποομάδα, τότε συμπεραίνουμε ότι για κάθε $g \in G$, η συζυγής υποομάδα gPg^{-1} ισούται με P, αφού η gPg^{-1} είναι επίσης μια p-Sylow υποομάδα και το $n_p = 1$.

Παράδειγμα 3.1.8. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι p είναι ένας πρώτος αριθμός.

(α′) Αν $p \nmid [G : 1]$, τότε $\mathrm{Syl}_p(G) = \{e_G\}$.

(β′) Αν $[G : 1] = p^n$, τότε $\mathrm{Syl}_p(G) = \{G\}$.

(γ′) Αν A είναι μια αβελιανή ομάδα, τότε για κάθε πρώτο διαιρέτη p τής τάξης τής A, υπάρχει ακριβώς μία p–Sylow υποομάδα. Πράγματι, το σύνολο των p–Sylow υποομάδων $\mathrm{Syl}_p(G)$ δεν είναι κενό και δύο οποιεσδήποτε p–Sylow υποομάδες P, P' που ανήκουν σε αυτό είναι συζυγείς. Δηλαδή, υπάρχει $a \in A$ με $aP'a^{-1} = P$. Επειδή η A είναι μια αβελιανή ομάδα, έχουμε $aP'a^{-1} = P'aa^{-1} = P'$. Επομένως, $P' = P$.

Ολοκληρώνουμε την παρούσα ενότητα με μια πρόταση που θα χρησιμοποιηθεί κατά την ταξινόμηση των πεπερασμένων μηδενοδύναμων ομάδων, βλ. Ενότητα 6.3.

Πρόταση 3.1.9. *Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι p είναι ένας πρώτος αριθμός που διαιρεί την τάξη της. Αν P είναι μια p–Sylow υποομάδα τής G, τότε ο ορθοθετοποιητής τού ορθοθετοποιητή τής P συμπίπτει με τον ορθοθετοποιητή τής P, δηλαδή $\mathcal{N}_G(\mathcal{N}_G(P)) = \mathcal{N}_G(P)$.*

Απόδειξη. Η υποομάδα P είναι ορθόθετη υποομάδα τού ορθοθετοποιητή της $\mathcal{N}_G(P)$ και προφανώς είναι μια p–Sylow υποομάδα τού $\mathcal{N}_G(P)$, αφού η τάξη της είναι η μέγιστη δύναμη τού p μεταξύ των τάξεων όλων των p–υποομάδων τής G, άρα και μεταξύ των τάξεων όλων των p–υποομάδων τού $\mathcal{N}_G(P)$. Επιπλέον, η P είναι η μοναδική p–Sylow υποομάδα τού $\mathcal{N}_G(P)$, αφού είναι ορθόθετη εντός τής $\mathcal{N}_G(P)$.
Για να αποδείξουμε τον ισχυρισμό τής πρότασης είναι αρκετό να αποδείξουμε ότι $\mathcal{N}_G(\mathcal{N}_G(P)) \subseteq \mathcal{N}_G(P)$, αφού προφανώς $\mathcal{N}_G(P) \subseteq \mathcal{N}_G(\mathcal{N}_G(P))$. Αν $g \in \mathcal{N}_G(\mathcal{N}_G(P))$, τότε $g\mathcal{N}_G(P)g^{-1} = \mathcal{N}_G(P)$. Αφού $P \leq \mathcal{N}_G(P)$, τότε $gPg^{-1} \leq g\mathcal{N}_G(P)g^{-1} = \mathcal{N}_G(P)$. Όντας η gPg^{-1} συζυγής τής P, είναι και αυτή μια p–Sylow υποομάδα τού $\mathcal{N}_G(P)$. Επομένως, $gPg^{-1} = P$ και γι΄αυτό το στοιχείο $g \in \mathcal{N}_G(\mathcal{N}_G(P))$ είναι στοιχείο τού $\mathcal{N}_G(P)$. Ώστε, $\mathcal{N}_G(\mathcal{N}_G(P)) \subseteq \mathcal{N}_G(P)$. □

Παράδειγμα 3.1.10. Οι Sylow υποομάδες τής συμμετρικής ομάδας $(S_3, \circ)$.
Η τάξη τής S_3 είναι $[S_3 : 1] = 3! = 2 \cdot 3$.
Για το πλήθος n_3 των 3–Sylow υποομάδων γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \ \text{ και } n_3 \mid 2 \Rightarrow n_3 = 1.$$

Συνεπώς, η S_3 έχει μια ορθόθετη υποομάδα τάξης 3. Πρόκειται για την εναλλάσσουσα υποομάδα $\mathbb{A}_3$. Για το πλήθος n_2 των 2–Sylow υποομάδων γνωρίζουμε ότι

$$n_2 \equiv 1 \bmod 2 \ \text{ και } n_2 \mid 3 \Rightarrow n_2 = 1 \ \text{ ή } 3.$$

Συνεπώς, η S_3 έχει ή μία ορθόθετη υποομάδα τάξης 2 ή τρεις υποομάδες τάξης 2. Αλλά αφού έχει τουλάχιστον δύο διαφορετικά στοιχεία τάξης 2, που προφανώς δεν μπορεί να ανήκουν στην ίδια υποομάδα τάξης 2, έπεται ότι έχει τρεις υποομάδες τάξης 2. Πρόκειται για τις υποομάδες $\langle\begin{pmatrix}1 & 2\end{pmatrix}\rangle$, $\langle\begin{pmatrix}1 & 3\end{pmatrix}\rangle$ και $\langle\begin{pmatrix}2 & 3\end{pmatrix}\rangle$.

Παράδειγμα 3.1.11. Οι Sylow υποομάδες τής εναλλάσσουσας ομάδας $\mathbb{A}_4$.
Η τάξη τής $\mathbb{A}_4$ είναι $[S_4 : 1]/2 = 4!/2 = 12 = 2^2 \cdot 3$.
Για το πλήθος n_2 των 2–Sylow υποομάδων γνωρίζουμε ότι

$$n_2 \equiv 1 \bmod 2 \ \text{ και } n_2 \mid 3 \Rightarrow n_2 = 1 \ \text{ ή } 3.$$

Αλλά μεταξύ των υποομάδων τής $\mathbb{A}_4$, οι οποίες έχουν τάξη 4 είναι και η

$$V = \{\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}\}.$$

Η συγκεκριμένη υποομάδα V είναι μια 2–Sylow υποομάδα τής $\mathbb{A}_4$ και επιπλέον είναι ορθόθετη υποομάδα τής $\mathbb{A}_4$. Επειδή κάθε 2–Sylow υποομάδα H τής $\mathbb{A}_4$ είναι συζυγής με την ορθόθετη V, έπεται ότι $H = V$ και γι' αυτό $n_2 = 1$
Για το πλήθος n_3 των 3–Sylow υποομάδων γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \ \text{ και } n_3 \mid 4 \Rightarrow n_3 = 1 \ \text{ ή } 4.$$

Επειδή η $\mathbb{A}_4$ διαθέτει τουλάχιστον δύο υποομάδες τάξης 3, τις $\langle\begin{pmatrix}1 & 2 & 3\end{pmatrix}\rangle$ και $\langle\begin{pmatrix}1 & 2 & 4\end{pmatrix}\rangle$, έπεται ότι $n_3 \geq 2$ και επομένως $n_3 = 4$. Οι υπόλοιπες 3–Sylow υποομάδες είναι οι $\langle\begin{pmatrix}2 & 3 & 4\end{pmatrix}\rangle$ και $\langle\begin{pmatrix}1 & 3 & 4\end{pmatrix}\rangle$.

Παράδειγμα 3.1.12. Οι Sylow υποομάδες τής συμμετρικής ομάδας $(S_4, \circ)$.
Η τάξη τής S_4 είναι $[S_4 : 1] = 4! = 2^3 \cdot 3$.
Για το πλήθος n_3 των 3–Sylow υποομάδων γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \ \text{ και } n_3 \mid 8 \Rightarrow n_3 = 1 \text{ ή } 4, \ \text{ ή } 8.$$

Όμως κάθε 3–Sylow υποομάδα τής S_4 είναι τάξης 3 και παράγεται από έναν 3-κύκλο. Γι' αυτό κάθε υποομάδα τάξης 3 είναι και υποομάδα τής $\mathbb{A}_4$. Όπως είδαμε στο αμέσως προηγούμενο παράδειγμα, η $\mathbb{A}_4$ έχει τέσσερεις 3–Sylow υποομάδες. Επομένως, $n_3 = 4$.

Για το πλήθος n_2 των 2–Sylow υποομάδων γνωρίζουμε ότι

$$n_2 \equiv 1 \bmod 2 \;\; \text{και}\; n_2 \mid 3 \Rightarrow n_2 = 1 \text{ ή } 3.$$

Κάθε 2–Sylow υποομάδα τής S_4 έχει 8 οκτώ στοιχεία. Μεταξύ των υποομάδων τάξης 8 είναι και η διεδρική υποομάδα $D_4 = \langle \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}, \begin{pmatrix}2 & 4\end{pmatrix} \rangle$, βλ. Παράδειγμα 2.1.2. Κάθε άλλη 2–Sylow υποομάδα είναι συζυγής τής D_4.
Παρατηρούμε ότι η η υποομάδα $\langle \begin{pmatrix}1 & 2 & 4 & 3\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix} \rangle$ είναι συζυγής τής D_4 και δεν ταυτίζεται με αυτήν. Αφού λοιπόν έχουμε τουλάχιστον δύο διαφορετικές 2–Sylow υποομάδες τάξης, το πλήθος τους n_2 δεν ισούται με 1 και έτσι $n_2 = 3$. Η τρίτη 2–Sylow υποομάδα είναι η $\langle \begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix}, \begin{pmatrix}3 & 4\end{pmatrix} \rangle$.

Παράδειγμα 3.1.13. Οι Sylow υποομάδες τής συμμετρικής ομάδας $(S_5, \circ)$.
Η τάξη τής S_5 είναι $[S_5 : 1] = 4! = 2^3 \cdot 3 \cdot 5$.
Για το πλήθος n_5 των 5–Sylow υποομάδων γνωρίζουμε ότι

$$n_5 \equiv 1 \bmod 5 \;\; \text{και}\; n_5 \mid 2^3 \cdot 3 = 24 \Rightarrow n_5 = 1 \text{ ή } 6.$$

Όμως κάθε 5–Sylow υποομάδα τής S_5 είναι τάξης 5 και παράγεται από έναν 5-κύκλο. Αλλά υπάρχουν τουλάχιστον δύο διαφορετικές υποομάδες τής S_5 τάξης 5. Επί παραδείγματι, οι $\langle \begin{pmatrix}1 & 2 & 3 & 4 & 5\end{pmatrix} \rangle$ και $\langle \begin{pmatrix}1 & 2 & 4 & 3 & 5\end{pmatrix} \rangle$ είναι δύο διαφορετικές υποομάδες τάξης 5. Γι' αυτό $n_5 = 6$.
Για το πλήθος n_3 των 3–Sylow υποομάδων γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \;\; \text{και}\; n_3 \mid 2^3 \cdot 5 = 40 \Rightarrow n_3 = 1 \text{ ή } 4 \text{ ή } 10 \text{ ή } 40.$$

Το πλήθος των στοιχείων τάξης 3 τής S_5, δηλαδή των 3-κύκλων, ισούται με $(5 \cdot 4 \cdot 3)/3 = 20$. Επομένως, $n_3 > 1$. Αν $n_3 = 4$, τότε το πλήθος των στοιχείων τάξης 3 ισούται με $4 \cdot 2 = 8$, επειδή η τομή δύο διαφορετικών κυκλικών ομάδων με τάξη πρώτο αριθμό ισούται πάντοτε με την τετριμμένη υποομάδα που αποτελείται από το ουδέτερο στοιχείο. Ώστε, $n_3 \neq 4$. Χρησιμοποιώντας το ίδιο επιχείρημα διαπιστώνουμε ότι είναι αδύνατο να έχουμε $n_3 = 40$, αφού τότε προκύπτουν $40 \cdot 2 = 80$ στοιχεία τάξης 3. Επομένως, $n_3 = 10$.
Για το πλήθος n_2 των 2–Sylow υποομάδων γνωρίζουμε ότι

$$n_2 \equiv 1 \bmod 2 \;\; \text{και}\; n_2 \mid 3 \cdot 5 = 15 \Rightarrow n_2 = 1 \text{ ή } 3 \text{ ή } 5 \text{ ή } 15.$$

Κάθε 2–Sylow υποομάδα τής S_5 έχει $2^3 = 8$ στοιχεία. Επειδή κάθε υποομάδα τής S_4 είναι και υποομάδα τής S_5, οι 2–Sylow υποομάδες τής S_4, που έχουν 8 στοιχεία, είναι και 2–Sylow υποομάδες τής S_5. Γι' αυτό η S_5 έχει τουλάχιστον τις 2–Sylow υποομάδες τις

$$\langle \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}, \begin{pmatrix}2 & 4\end{pmatrix} \rangle, \langle \begin{pmatrix}1 & 2 & 4 & 3\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix} \rangle \text{ και } \langle \begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix}, \begin{pmatrix}3 & 4\end{pmatrix} \rangle.$$

Επιπλέον τρεις διαφορετικές από τις προηγούμενες 2–Sylow υποομάδες τής S_5 προκύπτουν αντικαθιστώντας, ας πούμε το 2 από το 5. Έτσι προκύπτουν οι

$$\langle \begin{pmatrix}1 & 5 & 3 & 4\end{pmatrix}, \begin{pmatrix}5 & 4\end{pmatrix} \rangle, \langle \begin{pmatrix}1 & 5 & 4 & 3\end{pmatrix}, \begin{pmatrix}5 & 3\end{pmatrix} \rangle \text{ και } \langle \begin{pmatrix}1 & 3 & 5 & 4\end{pmatrix}, \begin{pmatrix}3 & 4\end{pmatrix} \rangle.$$

Γι' αυτό $n_2 > 6$ και επομένως $n_2 = 15$.

3.2 Εφαρμογές τής Θεωρίας Sylow

Πρόταση 3.2.1. *Κάθε ομάδα $(G, \star)$ τάξης $2p$, όπου ο p είναι ένας περιττός πρώτος, είναι ισόμορφη ή προς την κυκλική ομάδα $\mathbb{Z}_{2p}$ ή προς τη διεδρική ομάδα D_p.*

Απόδειξη. Για το πλήθος n_p των p–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_p \equiv 1 \bmod p \;\text{ και } n_p \mid 2 \Rightarrow n_p = 1.$$

Ώστε, υπάρχει μια ορθόθετη υποομάδα R τής G με τάξη τον πρώτο αριθμό p. Γι' αυτό $R = \langle r \rangle$, όπου η τάξη τού r ισούται με p.

Για το πλήθος n_2 των 2–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_2 \equiv 1 \mathrm{mod} 2 \;\text{ και } n_2 \mid p \Rightarrow n_2 = 1 \text{ ή } p.$$

Έστω T μια 2–Sylow υποομάδα τής G. Η T είναι κυκλική, δηλαδή $T = \langle t \rangle$ και η τάξη τού t ισούται με 2. Επειδή $R \bigcap T = \{e_G\}$, τα στοιχεία τής G

$$e_G, r, r^2, \ldots, r^{p-1}, t, tr, tr^2, \ldots, tr^{p-1}$$

είναι ανά δύο διαφορετικά και αφού το πλήθος τους ισούται με $2p$, έπεται ότι

$$G = \{e_G, r, r^2, \ldots, r^{p-1}, t, tr, tr^2, \ldots, tr^{p-1}\}.$$

Παρατηρούμε ότι το στοιχείο trt^{-1} οφείλει να ανήκει στην ορθόθετη υποομάδα R. Ας πούμε ότι $trt^{-1} = r^i, 1 \leq i \leq p-1$. Τότε $tr^\ell t^{-1} = r^{i\ell}$. Λαμβάνοντας υπ' όψιν ότι $t^{-1} = t$ έχουμε $r = t(trt)t = tr^i t^{-1} = (trt^{-1})^i = r^{i^2}$ (*) και γι' αυτό $p \mid (i^2 - 1)$. Επομένως, ή $i = 1$ ή $i = p - 1$.

Στην περίπτωση $i = 1$, η σχέση (*) δίνει $trt^{-1} = r \Leftrightarrow tr = rt$ και η G είναι μια αβελιανή ομάδα. Επιπλέον, η απεικόνιση

$$\varphi : R \times T \to G, (\alpha, \beta) \mapsto \alpha\beta$$

είναι ένας ομομορφισμός ομάδων με $\ker \varphi = \{e_G\}$, αφού $R \bigcap T = \{e_G\}$. Επειδή $[R \times T : 1] = 2p = [G : 1]$, ο φ είναι ισομορφισμός. Το ευθύ γινόμενο $R \times T$ είναι ισόμορφο προς το $\mathbb{Z}_p \times \mathbb{Z}_2$ που με τη σειρά του είναι ισόμορφο προς την κυκλική ομάδα $\mathbb{Z}_{2p}$.

Στην περίπτωση $i = p - 1$, η σχέση (*) δίνει $trt^{-1} = r^{p-1} \Leftrightarrow rt = tr^{p-1}$. Η G είναι ισόμορφη προς τη διεδρική ομάδα

$$D_p = \{\mathrm{Id}_p, \tau, \rho, \rho^2, \ldots, \rho^{n-1}, \tau \circ \rho, \tau \circ \rho^2, \ldots, \tau \circ \rho^{p-1}\},$$

τής οποίας τα στοιχεία τ και ρ ικανοποιούν τις ισότητες $\tau^2 = \mathrm{Id}_p, \rho^p = \mathrm{Id}_p$ και $\rho \circ \tau = \tau \circ \rho^{p-1}$. Ο ισομορφισμός $\sigma : G \to D_p$ ορίζεται από τις τιμές $\sigma(t) = \tau$ και $\sigma(r) = \rho$. □

Πρόταση 3.2.2. *Κάθε ομάδα $(G, \star)$ τάξης pq, όπου οι p, q είναι πρώτοι αριθμοί με $p < q$ διαθέτει μια ορθόθετη q–Sylow υποομάδα και αν επιπλέον $p \nmid q - 1$, τότε η G είναι ισόμορφη προς την κυκλική ομάδα $\mathbb{Z}_{pq}$.*

Απόδειξη. Για το πλήθος n_q των q–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_q \equiv 1 \bmod q \ \text{ και } n_q \mid p \Rightarrow n_q = 1 \text{ ή } p.$$

Όμως $p < q$ και έτσι $n_q = 1$. Συνεπώς, υπάρχει μία ορθόθετη q–Sylow υποομάδα $Q = \langle \beta \rangle$ τής G, η οποία είναι κυκλική, αφού η τάξη της είναι ο πρώτος αριθμός q.

Για το πλήθος n_p των p–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_p \equiv 1 \bmod p \ \text{ και } n_p \mid q \Rightarrow n_p = 1 \text{ ή } q.$$

Αν τώρα επιπλέον έχουμε $p \nmid q - 1$ και είναι $n_p = q$, τότε $q \equiv 1 \bmod p$. Πράγμα άτοπο. Επομένως, $n_p = 1$ και έτσι υπάρχει μία ορθόθετη p–Sylow υποομάδα $P = \langle \alpha \rangle$ τής G, η οποία είναι κυκλική, αφού η τάξη της είναι ο πρώτος αριθμός p.

Παρατηρούμε ότι $\alpha\beta = \beta\alpha$, επειδή το στοιχείο $\alpha\beta\alpha^{-1}\beta^{-1} = e_G$, αφού ανήκει στην τομή $P \bigcap Q = \{e_G\}$. Γι' αυτό ορίζεται η απεικόνιση $P \times Q \to G, (\alpha^i, \beta^j) \mapsto \alpha^i\beta^j$, η οποία είναι μονομορφισμός και συνεπώς ισομορφισμός, διότι $[P \times Q : 1] = pq = [G : 1]$.

Επομένως η G είναι ισόμορφη προς την ομάδα $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. $\square$

Αν $p \mid q - 1$, τότε αποδεικνύεται, βλ. Πρόταση 7.2.11, ότι υπάρχει μια μοναδική (με ακρίβεια ισομορφίας) ομάδα τάξης pq, η οποία δεν είναι αβελιανή.

Πρόταση 3.2.3. *Κάθε ομάδα $(G, \star)$ τάξης 12 διαθέτει μια μη τετριμμένη ορθόθετη υποομάδα τάξης ή 3 ή 4.*

Απόδειξη. Για το πλήθος n_3 των 3–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \ \text{ και } n_3 \mid 4 \Rightarrow n_3 = 1 \text{ ή } 4.$$

Αν $n_3 = 1$, τότε βέβαια υπάρχει μία ορθόθετη υποομάδα τής G τάξης 3 που ικανοποιεί τον ισχυρισμό τής πρότασής μας.

Αν $n_3 \neq 1$, τότε θα αποδείξουμε ότι το πλήθος n_2 των 2–Sylow υποομάδων τής G ισούται με 1 και γι' αυτό θα υπάρχει μία ορθόθετη υποομάδα τής G τάξης 4, η οποία θα ικανοποιεί τον ισχυρισμό τής πρότασής μας. Ας δούμε πως θα το πετύχουμε αυτό.

Πράγματι, αν $n_3 \neq 1 \Rightarrow n_3 = 4$ και ως εκ τούτου η G διαθέτει $4 \cdot (3 - 1) = 8$ στοιχεία τάξης 3, βλ. Άσκηση ΠΑ66. Αν P είναι οποιαδήποτε 3–Sylow υποομάδα, τότε γνωρίζουμε ότι κάθε άλλη 3–Sylow υποομάδα είναι συζυγής τής P και ότι το πλήθος τους n_3 ισούται με τον δείκτη $[G : \mathcal{N}_G(P)]$. Επομένως, $4 = n_3 = [G : \mathcal{N}_G(P)]$. Προσέξτε ότι επειδή $[G : P] = 4 = [G : \mathcal{N}_G(P)]$ και αφού $P \leqq \mathcal{N}_G(P)$, έχουμε $\mathcal{N}_G(P) = P$.

Η G δρα μέσω συζυγίας επί τού συνόλου $\mathrm{Syl}_3(G)$ που έχει τέσσερα στοιχεία και η συγκεκριμένη δράση χορηγεί έναν ομομορφισμό

$$\chi : G \to S_{\mathrm{Syl}_3(G)}, \text{ όπου } S_{\mathrm{Syl}_3(G)} \text{ η συμμετρική ομάδα τού συνόλου } \mathrm{Syl}_3(G).$$

Ένα στοιχείο $g \in G$ ανήκει στον $\ker\chi$, αν και μόνο αν, $\forall \overline{P} \in \mathrm{Syl}_3(G), g\overline{P}g^{-1} = \overline{P}$. Ιδιαιτέρως, $gPg^{-1} = P$ και γι' αυτό $g \in \ker\chi \Rightarrow g \in \mathcal{N}_G(P) = P$. Ώστε, $\ker\chi \leq P$. Συνεπώς, $\ker\chi = \{e_G\}$ ή $\ker\chi = P$, αφού $[P : 1] = 3$. Αλλά $\ker\chi \neq P$, διότι η P δεν είναι ορθόθετη υποομάδα[1] τής G. Επομένως, $\ker \chi = \{e_G\}$ και η G είναι ισόμορφη προς την εικόνα της $\chi(G)$. Ως εκ τούτου, η εικόνα $\operatorname{im} \chi$ τής G περιέχει ακριβώς 8 στοιχεία τάξης 3. Ταυτίζοντας την $S_{\mathrm{Syl}_3(G)}$ με την S_4 παρατηρούμε ότι όλα τα στοιχεία τάξης 3 είναι άρτιες μετατάξεις και γι' αυτό περιέχονται στην εναλλάσσουσα υποομάδα $\mathbb{A}_4$. Γι' αυτό η τομή $\operatorname{im} \chi \bigcap \mathbb{A}_4$, που είναι μια υποομάδα τής $\mathbb{A}_4$, έχει τουλάχιστον οκτώ στοιχεία. Αφού όμως $[\mathbb{A}_4 : 1] = 12$ συμπεραίνουμε, χρησιμοποιώντας το Θεώρημα Lagrange, ότι $\operatorname{im} \chi \bigcap \mathbb{A}_4 = \mathbb{A}_4$ και αφού και η $\operatorname{im} \chi$ έχει 12 στοιχεία, καταλήγουμε στο ότι $\operatorname{im} \chi = \mathbb{A}_4$. Επομένως, $G \cong \mathbb{A}_4$. Όμως επειδή η $\mathbb{A}_4$ διαθέτει μια ορθόθετη υποομάδα τάξης 4, βλ. Παράδειγμα 3.1.11, το ίδιο συμβαίνει και με την ισόμορφή της G. Ώστε $n_2(G) = 1$ και η G διαθέτει μια ορθόθετη 2–Sylow υποομάδα τάξης 4. □

Οι ομάδες τάξης $12 = 2^2 \cdot 3$ εμπεριέχονται στην επόμενη γενική περίπτωση:

Πρόταση 3.2.4. *Κάθε ομάδα $(G, \star)$ τάξης $p^2 q$, όπου οι p, q είναι πρώτοι αριθμοί με $p \neq q$, διαθέτει μια μη τετριμμένη ορθόθετη υποομάδα.*

Απόδειξη. Αν $p > q$, τότε από $n_p \equiv 1 \bmod p$ και $n_p \mid q \Rightarrow n_p = 1$ και γι' αυτό η G διαθέτει μια ορθόθετη p–Sylow υποομάδα.

Αν $p < q$, τότε από $n_q \equiv 1 \bmod q$ και $n_q \mid p^2 \Rightarrow n_p = 1$ ή $n_p = p$ ή $n_p = p^2$.

(α′) Η περίπτωση $n_q = 1$, οδηγεί αμέσως στο συμπέρασμα ότι η G διαθέτει μια ορθόθετη q–Sylow υποομάδα.

(β′) Η περίπτωση $n_q = p$ είναι αδύνατη, αφού από $p = n_q \equiv 1 \bmod q$, έπεται $q \mid p - 1$. Πράγμα άτοπο, επειδή $p < q$.

(γ′) Η περίπτωση $n_q = p^2$ και αφού $n_q \equiv 1 \bmod q$, δίνει είτε $q \mid p - 1$ είτε $q \mid p + 1$ και αφού η περίπτωση $q \mid p - 1$ οδηγεί σε άτοπο, βλ. την αμέσως προηγούμενη περίπτωση (β′), έπεται $q \mid p + 1$. Αφού όμως, $p < q$, έπεται $q = p + 1$ και επειδή οι p, q είναι πρώτοι αριθμοί, συμπεραίνουμε ότι $p = 2$ και $q = 3$. Ώστε η G είναι μια ομάδα τάξης 12, που μόλις προηγουμένως αποδείξαμε ότι διαθέτει μια μη τετριμμένη ορθόθετη υποομάδα. □

Πρόταση 3.2.5. *Κάθε ομάδα $(G, \star)$ τάξης 99 είναι ισόμορφη ή προς την κυκλική ομάδα $\mathbb{Z}_{99}$ ή προς την αβελιανή ομάδα $\mathbb{Z}_{11} \times \mathbb{Z}_3 \times \mathbb{Z}_3$.*

Απόδειξη. Για το πλήθος n_{11} των 11–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_{11} \equiv 1 \bmod 11 \;\text{ και }\; n_{11} \mid 9 \Rightarrow n_{11} = 1.$$

Συνεπώς, η G διαθέτει μια ορθόθετη υποομάδα P τάξης 11 και γι' αυτό $P \cong \mathbb{Z}_{11}$. Για το πλήθος n_3 των 3–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \;\text{ και }\; n_3 \mid 9 \Rightarrow n_3 = 1.$$

Συνεπώς, η G διαθέτει μια ορθόθετη υποομάδα Q τάξης 9. Κάθε ομάδα τάξης p^2 ή είναι κυκλική ή είναι ισόμορφη προς την $\mathbb{Z}_p \times \mathbb{Z}_p$, βλ. Θεώρημα 2.4.14. Εδώ επομένως έχουμε ή ότι $Q \cong \mathbb{Z}_9$ ή ότι $Q \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

[1] Αν ήταν θα είχαμε $n_3 = 1$.

Αφού οι P, Q είναι ορθόθετες υποομάδες τής G με $P \bigcap Q = \{e_G\}$, διότι ο ΜΚΔ$(11, 9) = 1$, συμπεραίνουμε ότι η PQ είναι μια υποομάδα τής G τάξης $[PQ : 1] = \frac{[P:1][Q:1]}{[P \bigcap Q:1]} = \frac{11 \cdot 9}{1} = 99$ και ως εκ τούτου, $PQ = G$. Ακόμα, η PQ είναι ισόμορφη προς το ευθύ γινόμενο $P \times Q$, βλ. Άσκηση Α88. Επομένως, $G \cong P \times Q$ και επειδή $P \cong \mathbb{Z}_{11}$ και ή $Q \cong \mathbb{Z}_9$ ή $Q \cong \mathbb{Z}_3 \times \mathbb{Z}_3$, συμπεραίνουμε ότι ή $G \cong \mathbb{Z}_{11} \times \mathbb{Z}_9$ ή $G \cong \mathbb{Z}_{11} \times \mathbb{Z}_3 \times \mathbb{Z}_3$. □

Πρόταση 3.2.6. *Κάθε ομάδα $(G, \star)$ τάξης 66 είναι ισόμορφη ή προς την κυκλική ομάδα $\mathbb{Z}_{66}$ ή προς τη διεδρική ομάδα D_{33} ή προς το ευθύ γινόμενο $D_{11} \times \mathbb{Z}_3$ ή προς το ευθύ γινόμενο $D_3 \times \mathbb{Z}_{11}$, όπου D_3 και D_{11} είναι οι διεδρικές ομάδες.*

Απόδειξη. Για το πλήθος n_{11} των 11–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_{11} \equiv 1 \bmod 11 \text{ και } n_{11} \mid 6 \Rightarrow n_{11} = 1.$$

Επομένως, η G διαθέτει μια ορθόθετη 11–Sylow υποομάδα K.

Έστω H οποιαδήποτε 3–Sylow υποομάδα τής G. Το σύνολο HK είναι μια υποομάδα τής G, αφού $HK = KH$. Επιπλέον,

$$[HK : 1] = \frac{[H : 1][K : 1]}{[H \bigcap K : 1]} = \frac{11 \cdot 3}{1} = 33.$$

Η HK είναι τάξης $33 = 3 \cdot 11$ και αφού το $3 \nmid (11 - 1)$ έπεται, βλ. Πρόταση 3.2.2, ότι η HK είναι κυκλική, ας πούμε ότι η HK ισούται με την κυκλική ομάδα $\langle a \rangle$, η οποία είναι ισόμορφη προς την $\mathbb{Z}_{33}$. Ο δείκτης $[G : HK]$ ισούται με 2 και γι' αυτό η HK είναι μια ορθόθετη υποομάδα τής G. Έστω $\langle b \rangle$ μια οποιαδήποτε 2–Sylow υποομάδα τής G. Παρατηρούμε ότι $HK \bigcap \langle b \rangle = \{e_G\}$.

Τα στοιχεία

$$e_G, a, a^2, \ldots, a^{31}, a^{32}, b, ab, a^2b, \ldots, a^{31}b, a^{32}b$$

είναι ανά δύο διαφορετικά και το πλήθος τους ισούται με 66. Συνεπώς, το σύνολο αυτών των στοιχείων είναι ακριβώς το σύνολο των στοιχείων τής G και επομένως $G = \langle \{a, b\} \rangle$ με $a^{33} = e_G$ και $b^2 = e_G$.

Με ποιό από τα προηγούμενα στοιχεία είναι ίσο το γινόμενο ba;

Επειδή η $HK = \langle a \rangle$ είναι ορθόθετη υποομάδα τής G, έχουμε ότι $bab^{-1} = a^i \in HK$ και αφού $b = b^{-1}$, έχουμε $ba = a^i b$ (*).

Ποιές είναι οι δυνατές τιμές που μπορεί να λάβει το $i, 1 \leq i \leq 32$;

Έχουμε $a = b(bab^{-1})b^{-1} = ba^i b^{-1} = a^{i^2}$. Συνεπώς, $a^{i^2 - 1} = e_G$ και γι' αυτό $33 \mid i^2 - 1$. Άρα, $i = 1, 10, 23, 32$.

Έτσι με τη βοήθεια τής (*) συμπεραίνουμε ότι τα a, b ικανοποιούν ακριβώς μία από τις επόμενες σχέσεις:

$$ba = ab, \quad ba = a^{10}b, \quad ba = a^{23}b, \quad ba = a^{32}b$$

και τελικώς διαπιστώνουμε ότι οι γεννήτορες a και b μιας ομάδας τάξης 66 ικανοποιούν ακριβώς μία από τις ακόλουθες τέσσερεις περιπτώσεις σχέσεων:

$$a^{33} = e_G, b^2 = e_G, ba = ab, \qquad a^{33} = e_G, b^2 = e_G, ba = a^{32}b,$$
$$a^{33} = e_G, b^2 = e_G, ba = a^{23}b, \qquad a^{33} = e_G, b^2 = e_G, ba = a^{10}b.$$

Προφανώς, οι περιπτώσεις αυτές αντιστοιχούν σε μη ισόμορφες ομάδες, αφού κάθε φορά το γινόμενο ba είναι διαφορετικό. Αν βρούμε λοιπόν τέσσερεις μη ισόμορφες ομάδες τάξης 66, τότε θα έχουμε ταξινομήσει με ακρίβεια ισομορφίας και όλες τις ομάδες τάξης 66. Ισχυριζόμαστε ότι οι ακόλουθες τέσσερεις ομάδες $\mathbb{Z}_{66}, D_{33}, D_{11} \times \mathbb{Z}_3, D_3 \times \mathbb{Z}_{11}$ τάξης 66 ανά δύο δεν είναι ισόμορφες. Πράγματι, η αβελιανή ομάδα $\mathbb{Z}_{66}$ δεν είναι ισόμορφη με καμιά από τις άλλες τρεις διότι αυτές δεν είναι αβελιανές. Επίσης οι υπόλοιπες τρεις ομάδες ανά δύο δεν είναι ισόμορφες, διότι η D_{33} διαθέτει 33 στοιχεία τάξης 2, ενώ η $D_{11} \times \mathbb{Z}_3$ διαθέτει μόνο 11 στοιχεία τάξης 2 και η $D_3 \times \mathbb{Z}_{11}$ διαθέτει μόνο 3 στοιχεία τάξης 2. □

Πρόταση 3.2.7. *Κάθε ομάδα $(G, \star)$ τάξης 30 διαθέτει μια μη τετριμμένη ορθόθετη υποομάδα τάξης 15.*

Απόδειξη. Για το πλήθος n_3 των 3–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \ \text{ και } n_3 \mid 10 \Rightarrow n_3 = 1 \text{ ή } 10.$$

Για το πλήθος n_5 των 5–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_5 \equiv 1 \bmod 5 \ \text{ και } n_5 \mid 6 \Rightarrow n_3 = 1 \text{ ή } 6.$$

Αν $n_3 = 1$ (αντιστοίχως $n_5 = 1$), τότε υπάρχει μια ορθόθετη 3–Sylow υποομάδα P (αντιστοίχως 5–Sylow υποομάδα Q), η οποία μαζί με μια οποιαδήποτε 5–Sylow υποομάδα Q (αντιστοίχως 3–Sylow υποομάδα P), δίνει την υποομάδα PQ, η οποία έχει τάξη 15 και δείκτη $[G : PQ] = 2$ και γι' αυτό είναι μια μη τετριμμένη ορθόθετη υποομάδα τής G. (Η απόδειξη αυτών των παρατηρήσεων εκτελείται όπως και στην αρχή τής απόδειξης τής Πρότασης 3.2.6.)

Υπολείπεται να αποδείξουμε ότι είτε $n_3 = 1$ είτε $n_5 = 1$. Πράγματι, αν ήταν $n_3 \neq 1$ και $n_5 \neq 1$, τότε θα ήταν $n_3 = 10$ και $n_5 = 6$ και γι' αυτό θα είχαμε μια συλλογή Λ αποτελούμενη από 10 υποομάδες τής G που η καθεμιά τους θα είχε τρία στοιχεία και από 6 υποομάδες τής G που η καθεμιά τους θα είχε πέντε στοιχεία. Επειδή η τομή δύο διαφορετικών υποομάδων τής Λ ισούται πάντοτε με το ουδέτερο στοιχείο, συμπεραίνουμε ότι η G θα διέθετε $10 \times 2 = 20$ στοιχεία τάξης 3 και $6 \times 4 = 24$ στοιχεία τάξης 5. Αλλά 44 στοιχεία είναι πάρα πολλά για μια ομάδα που έχει μόνο 30 στοιχεία. Επομένως, είτε $n_3 = 1$ είτε $n_5 = 1$. □

Σύντομα θα αποδείξουμε ότι στην περίπτωση μιας ομάδας με 30 στοιχεία υπάρχει και μια ορθόθετη 3–Sylow υποομάδα και μια ορθόθετη 5–Sylow υποομάδα. Για τη συγκεκριμένη απόδειξη θα χρειαστούμε ορισμένα επιπλέον εργαλεία που θα αναπτύξουμε στην επόμενη ενότητα.

Ας δούμε τη γενική περίπτωση μιας ομάδας που η τάξη της είναι γινόμενο τριών διαφορετικών πρώτων αριθμών:

Πρόταση 3.2.8. *Κάθε ομάδα $(G, \star)$ τάξης pqr, όπου οι p, q, r είναι πρώτοι αριθμοί ανά δύο διαφορετικοί, διαθέτει μια ορθόθετη υποομάδα τάξης ή p ή q ή r.*

Απόδειξη. Μπορούμε να υποθέσουμε χωρίς περιορισμό τής γενικότητας ότι $p > q > r$.

Παραδοχή: Για να καταλήξουμε σε άτοπο, ας δεχθούμε ότι δεν υπάρχουν ορθόθετες υποομάδες τής G τάξης ή p ή q ή r. Το πλήθος n_p των p-Sylow υποομάδων τής G ικανοποιεί την $n_p \equiv 1 \bmod p$ με το $n_p \mid qr$. Άρα, το n_p ισούται ή με 1 ή με q ή με r ή με qr. Λόγω τής παραδοχής που κάναμε, το n_p είναι > 1. Άρα, το $n_p = 1 + \lambda p$ με $\lambda \in \mathbb{N}$. Ως εκ τούτου $n_p > p$ και επομένως $n_p = qr$. Το πλήθος n_q των q-Sylow υποομάδων τής G ικανοποιεί την $n_q \equiv 1 \bmod q$ με το $n_q \mid pr$. Λόγω τής παραδοχής που κάναμε, το n_q είναι > 1 και όπως προηγουμένως το $n_q > q$. Άρα, το $n_q = p$ ή $n_q = pr$. Σε κάθε περίπτωση, το $n_q \geq p$. Τέλος, το πλήθος n_r των r-Sylow υποομάδων τής G είναι και αυτό > 1 και αφού $n_r \mid pq$, συμπεραίνουμε ότι $n_r \geq q$. Υπενθυμίζοντας ότι δύο οποιεσδήποτε διαφορετικές υποομάδες πρώτης τάξης έχουν τομή ίση με $\{e_G\}$, συμπεραίνουμε ότι η G διαθέτει ακριβώς $qr(p-1)$ το πλήθος στοιχεία τάξης p, τουλάχιστον $p(q-1)$ το πλήθος στοιχεία τάξης q και τουλάχιστον $q(r-1)$ το πλήθος στοιχεία τάξης r. Προσμετρώντας και το ταυτοτικό στοιχείο e_G, προκύπτει η ακόλουθη σχέση για το πλήθος pqr των στοιχείων τής G:

$$pqr \geq qr(p-1) + p(q-1) + q(r-1) + 1 = pqr + (p-1)(q-1).$$

Αυτό όμως είναι άτοπο. Επομένως η G διαθέτει μια μη τετριμμένη ορθόθετη υποομάδα τάξης ή p ή q ή r. □

3.2.1 Αυτομορφισμοί Ομάδας και χαρακτηριστικές Υποομάδες

Υπενθυμίζουμε, βλ. σελ. 123, ότι για κάθε ομάδα $(G, \star)$, συμβολίζουμε με $\mathrm{Aut}(G)$ το σύνολο

$$\{\chi : G \to G \mid \chi \text{ ισομορφισμός ομάδων }\}.$$

Επίσης υπενθυμίζουμε ότι το ζεύγος $(\mathrm{Aut}(G), \circ)$ αποτελεί μια ομάδα, τη λεγόμενη ομάδα αυτομορφισμών τής G, όπου «$\circ$» είναι η σύνθεση απεικονίσεων. Η μελέτη μιας ομάδας $(G, \star)$ είναι στενά συνδεδεμένη με την ομάδα των αυτομορφισμών της $(\mathrm{Aut}(G), \circ)$.

Ορισμός 3.2.9. Μια υποομάδα $H \leq G$ μιας ομάδας $(G, \star)$ ονομάζεται *χαρακτηριστική*, αν για κάθε αυτομορφισμό $\chi \in \mathrm{Aut}(G)$ είναι $\chi(H) = H$.

Παράδειγμα 3.2.10. Κάθε υποομάδα μιας κυκλικής ομάδας είναι χαρακτηριστική.

Πράγματι, αν η $(G, \star)$ είναι μια κυκλική ομάδα με άπειρο το πλήθος στοιχείων, τότε η $\mathrm{Aut}(G)$ αποτελείται μόνο από δύο αυτομορφισμούς:

$$\mathrm{Id} : G \to G, g \mapsto g \text{ και } \chi : G \to G, g \mapsto g^{-1}.$$

Προφανώς, κάθε υποομάδα τής G είναι χαρακτηριστική.

Όταν $(G, \star)$ είναι μια κυκλική ομάδα με πεπερασμένο το πλήθος στοιχείων, τότε για κάθε διαιρέτη d τής τάξης της υπάρχει ακριβώς μία υποομάδα τάξης d, βλ. Πρόταση 1.5.16. Γι' αυτό, όταν χ είναι οποιοσδήποτε αυτομορφισμός τής G και $H \leq G$ είναι οποιαδήποτε υποομάδα της, τότε η τάξη τής εικόνας $\chi(H)$ ισούται με την τάξη τής H και έτσι $\chi(H) = H$. Επομένως, κάθε υποομάδα τής G είναι χαρακτηριστική.

Παρατήρηση 3.2.11. Για να είναι μια υπομάδα H μιας ομάδας G χαρακτηριστική, αρκεί $\forall \chi \in \mathrm{Aut}(G)$, να είναι $\chi(H) \leq H$. Πράγματι, αν $\chi \in \mathrm{Aut}(G)$, τότε επίσης $\chi^{-1} \in \mathrm{Aut}(G)$. Τώρα από $\chi^{-1}(H) \leq H$, έπεται $H = \chi(\chi^{-1}(H)) \leq \chi(H) \leq H$. Συνεπώς, $\chi(H) = H$.

Πρόταση 3.2.12. *Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα, ότι p είναι ένας πρώτος με $p \mid [G:1]$ και ότι P είναι μια p–Sylow υποομάδα της. Τα επόμενα είναι ισοδύναμα:*

(α′) *Η υποομάδα P είναι η μοναδική p–Sylow υποομάδα τής G.*

(β′) *Η υποομάδα P είναι μια ορθόθετη υποομάδα τής G.*

(γ′) *Η υποομάδα P είναι μια χαρακτηριστική υποομάδα τής G.*

(δ′) *Κάθε υποομάδα τής G, η οποία παράγεται από ένα σύνολο στοιχείων X, όπου κάθε $x \in X$ έχει τάξη μια δύναμη τού p, είναι μια p–υποομάδα τής G.*

Απόδειξη. (α′) $\Leftrightarrow$ (β′) Όλες οι p–Sylow υποομάδες είναι συζυγείς. Επομένως, υπάρχει μία μοναδική p–Sylow υποομάδα P, αν και μόνο αν, η P είναι μια ορθόθετη υποομάδα.
(γ′) $\Rightarrow$ (β′) Κάθε στοιχείο $g \in G$ χορηγεί τον εσωτερικό αυτομορφισμό
$\chi_g : G \to G,\ \alpha \to g\alpha g^{-1}$. Αφού η P είναι μια χαρακτηριστική υποομάδα τής G, αυτή παραμένει αναλλοίωτη κάτω από οποιονδήποτε εσωτερικό αυτομορφισμό $\chi_g, g \in G$. Γι' αυτό $\forall g \in G, \chi_g(P) = P$, δηλαδή $\forall g \in G, gPg^{-1} = P$.
(α′) $\Rightarrow$ (γ′) Αν χ είναι οποιοδήποτε στοιχείο τής $\mathrm{Aut}(G)$, τότε η $\chi(P)$ είναι επίσης μια p–Sylow υποομάδα τής G, αφού $[\chi(P):1] = [P:1]$. Αλλά η P είναι η μοναδική p–Sylow υποομάδα, επομένως $P = \chi(P)$.
(α′) $\Rightarrow$ (δ′) Κάθε $x \in X$ παράγει μια κυκλική υποομάδα $\langle x \rangle$ τάξης p. Αυτή περιέχεται σε κάποια p–Sylow υποομάδα P τής G. Λόγω τής υπόθεσης, η $\langle x \rangle$ περιέχεται στη μοναδική p–Sylow υποομάδα P. Επομένως, $\forall x \in X$ έχουμε $x \in P$. Ώστε, $X \subseteq P$ και συνεπώς $\langle X \rangle \subseteq P$. Αλλά κάθε υποομάδα τής P έχει τάξη μια δύναμη τού πρώτου p. Επομένως, η $\langle X \rangle$ είναι μια p–υποομάδα τής G.
(δ′) $\Rightarrow$ (α′) Θεωρούμε όλες τις p–Sylow υποομάδες τής G και ας είναι X η ένωσή τους, δηλαδή $X = \bigcup_{P \in \mathrm{Syl}_p(G)} P$. Επειδή κάθε στοιχείο $x \in X$ περιέχεται σε τουλάχιστον μία p–Sylow υποομάδα, διαπιστώνουμε ότι η τάξη τού x είναι μια δύναμη τού p και έτσι, σύμφωνα με την υπόθεση, έχουμε ότι η $\langle X \rangle$ είναι μια p–υποομάδα. Συνεπώς, η $\langle X \rangle$ οφείλει, ως p–υποομάδα, να περιέχεται σε κάποια συγκεκριμένη p–Sylow υποομάδα $\overline{P}$. Επομένως έχουμε:

$$X = \bigcup_{P \in \mathrm{Syl}_p(G)} P \subseteq \langle X \rangle \subseteq \overline{P}.$$

Επομένως για κάθε $P \in \mathrm{Syl}_p(G)$, είναι $P \subseteq \overline{P}$. Αλλά οι P και $\overline{P}$ έχουν το ίδιο πλήθος στοιχείων, εφόσον πρόκειται για p–Sylow υποομάδες. Επομένως $\forall P \in \mathrm{Syl}_p(G), P = \overline{P}$. □

Παρατήρηση 3.2.13. Αν H, K είναι δυο υποομάδες μιας ομάδας $(G, \star)$ με την H χαρακτηριστική υποομάδα τής K και την K ορθόθετη υποομάδα τής G, τότε και η H είναι ορθόθετη υποομάδα τής G.

Πράγματι, για κάθε $g \in G$, ο εσωτερικός αυτομορφισμός $\chi_g : G \to G, \alpha \to g\alpha g^{-1}$ περιορισμένος στην υποομάδα K αποτελεί έναν αυτομορφισμό τής K, αφού πρόκειται για μια ορθόθετη υποομάδα τής G. Η υποομάδα H είναι χαρακτηριστική υποομάδα τής K, επομένως $\forall g \in G, \chi_g(H) = H$, δηλαδή $\forall g \in G, gHg^{-1} = H$ και συνεπώς η H είναι μια ορθόθετη υποομάδα τής G.

Από την Πρόταση 3.2.8, γνωρίζουμε ότι μια ομάδα τάξης $30 = 2 \cdot 3 \cdot 5$ έχει μια ορθόθετη υποομάδα τάξης ή 2 ή 3 ή 5. Όμως τώρα μπορούμε να πούμε περισσότερα:

Πρόταση 3.2.14. *Κάθε ομάδα $(G, \star)$ τάξης 30 διαθέτει μια ορθόθετη υποομάδα τάξης 5 και μια ορθόθετη υποομάδα τάξης 3.*

Απόδειξη. Από την Πρόταση 3.2.7, γνωρίζουμε ότι η G διαθέτει μια ορθόθετη υποομάδα K τάξης 15. Η K είναι κυκλική και κάθε υποομάδα της είναι χαρακτηριστική. Σε κάθε διαιρέτη d τής τάξης υπάρχει μια υποομάδα τάξης d, που όπως έχουμε διαπιστώσει είναι χαρακτηριστική υποομάδα τής K, άρα ορθόθετη υποομάδα τής G. Η K έχει υποομάδες τάξης 5 και 3. Αυτές είναι ορθόθετες υποομάδες τής G. $\square$

Πρόταση 3.2.15. *Κάθε ομάδα $(G, \star)$ τάξης 105 διαθέτει μια ορθόθετη υποομάδα τάξης 5 και μια ορθόθετη υποομάδα τάξης 7.*

Απόδειξη. Από το Θεώρημα Sylow, βλ. Θεώρημα 3.1.5, γνωρίζουμε ότι το πλήθος n_5 των 5-Sylow υποομάδων τής G ικανοποιεί την $n_5 \equiv 1 \bmod 5$ με το $n_5 \mid 21$ και ως εκ τούτου, ή $n_5 = 1$ ή $n_5 = 21$. Παρόμοια, το πλήθος των 7-Sylow υποομάδων τής G ικανοποιεί την $n_7 \equiv 1 \bmod 7$ με το $n_7 \mid 15$ και ως εκ τούτου, ή $n_7 = 1$ ή $n_7 = 15$.
Ισχυριζόμαστε ότι η περίπτωση $n_5 = 21$ και $n_7 = 15$ είναι αδύνατη. Πράγματι, αν ήταν $n_5 = 21$ και $n_7 = 15$, τότε θα υπήρχαν 21 το πλήθος ομάδες τάξης 5 και 15 το πλήθος ομάδες τάξης 7. Τότε η G θα διέθετε $21(5-1) = 84$ το πλήθος στοιχεία τάξης 5 και $15(7-1) = 90$ το πλήθος στοιχεία τάξης 7, βλ. Άσκηση ΠΑ66. Τότε όμως η G θα είχε τουλάχιστον $84 + 90 + 1$ το πλήθος στοιχεία, τα οποία είναι πάρα πολλά για μια ομάδα τάξης 105. Επομένως, είτε $n_5 = 1$ είτε $n_7 = 1$, δηλαδή η G έχει είτε μια ορθόθετη υποομάδα K_5 τάξης 5 είτε μια ορθόθετη υποομάδα K_7 τάξης 7.
Τώρα ισχυριζόμαστε ότι η G διαθέτει μια υποομάδα τάξης 35. Πράγματι, όταν η K_5 είναι η ορθόθετη υποομάδα και H είναι οποιαδήποτε υποομάδα τής G τάξης 7, τότε το σύνολο K_5H είναι μια υποομάδα τής G τάξης 35 (*γιατί;*). Παρόμοια, αν $K_7 \trianglelefteq G$ και H είναι οποιαδήποτε υποομάδα τής G τάξης 5, τότε το σύνολο K_7H είναι μια υποομάδα τάξης 35 (*γιατί;*). Άρα σε κάθε περίπτωση υπάρχει μια υποομάδα L τής G τάξης 35, η οποία είναι μάλιστα κυκλική, βλ. Πρόταση 3.2.2.
Η L είναι ορθόθετη υποομάδα τής G, διότι ο δείκτης $[G : L] = 3$ είναι ο μικρότερος πρώτος που διαιρεί την τάξη τής G, βλ. Πόρισμα 2.3.7. Αφού η L είναι κυκλική, κάθε υποομάδα της $N \leq L$ είναι χαρακτηριστική, βλ. Παράδειγμα 3.2.10. Επιπλέον, επειδή η L είναι ορθόθετη υποομάδα τής G, συμπεραίνουμε, βλ. Παρατήρηση 3.2.13, ότι η N είναι ορθόθετη υποομάδα τής G. Επειδή η L είναι κυκλική, διαθέτει μια υποομάδα τάξης 5 (αντιστοίχως τάξης 7), η οποία είναι μια 5-Sylow (αντιστοίχως 7-Sylow) ορθόθετη υποομάδα τής G. Άρα, $n_5 = 1$ και $n_7 = 1$. $\square$

3.2.2 Η εναλλάσσουσα ομάδα $\mathbb{A}_5$ είναι απλή

Υπενθυμίζουμε ότι

Ορισμός 3.2.16. Μια ομάδα $(G, \star)$ με $[G:1] > 1$, ονομάζεται *απλή*, αν διαθέτει ως ορθόθετες υποομάδες μόνο τις $\{e_G\}$ και G.

Πρόταση 3.2.17. *Οι απλές ομάδες οι οποίες είναι αβελιανές, είναι ακριβώς οι κυκλικές ομάδες πρώτης τάξης.*

Απόδειξη. Έστω ότι η G είναι μια απλή αβελιανή ομάδα. Η G διαθέτει κάποιο $x \in G$ με $x \neq e_G$, επειδή $[G:1] > 1$.
Η κυκλική υποομάδα $\langle x \rangle$ οφείλει να συμπίπτει με την G, διότι $\{e_G\} \subsetneq \langle x \rangle$ και $\langle x \rangle \trianglelefteq G$. Θεωρούμε το στοιχείο $x^2 \in G$.
Αν $x^2 = e_G$, τότε η G είναι κυκλική υποομάδα με τάξη τον πρώτο αριθμό 2.
Αν $x^2 \neq e_G$, τότε $\langle x^2 \rangle = G = \langle x \rangle$. Επομένως, $x \in \langle x^2 \rangle$ και γι' αυτό $x = x^{2r}$. Έτσι συμπεραίνουμε ότι το x είναι πεπερασμένης τάξης, έστω $n > 1$. Εφόσον η $\langle x \rangle = G$ είναι κυκλική τάξης n, τότε ως γνωστόν για κάθε διαιρέτη m τού n υπάρχει μια (κυκλική) υποομάδα τάξης m. Ιδιαιτέρως, όταν ο p είναι ένας πρώτος διαιρέτης τού n, τότε υπάρχει μια κυκλική υποομάδα $\langle y \rangle \geq G$ τάξης p και αφού $\langle y \rangle \neq \{e_G\}$ και $\langle y \rangle \trianglelefteq G$, συμπεραίνουμε ότι η απλή ομάδα G ισούται με την $\langle y \rangle$. Επομένως, η G είναι κυκλική ομάδα πρώτης τάξης. □

Πρόταση 3.2.18. *Κάθε ομάδα $(G, \star)$ τάξης 60 που έχει περισσότερες από μία 5–Sylow υποομάδες είναι απλή.*

Απόδειξη. Παρατηρούμε ότι το πλήθος n_5 των 5–Sylow υποομάδων τής G ισούται με 6, επειδή $n_5 \equiv 1 \mathrm{mod} 5$, $n_5 \mid 12$ και αφού έχουμε υποθέσει ότι $n_5 \geq 2$.

Έστω ότι η G δεν είναι απλή και ότι $H \trianglelefteq G$ είναι μια μη τετριμμένη ορθόθετη υποομάδα της.

Αν ο 5 είναι διαιρέτης τής $[H:1]$, τότε η H περιέχει μια υποομάδα P τάξης 5, η οποία προφανώς είναι μια 5–Sylow υποομάδα τής G. Αφού όμως η H είναι ορθόθετη, περιέχει $\forall g \in G$ και κάθε συζυγή υποομάδα gPg^{-1} τής P, δηλαδή περιέχει και τις έξι 5–Sylow υποομάδες τής G. Επομένως, η H περιέχει $6 \times 4 = 24$ στοιχεία τάξης 5. Άρα $[H:1] \geq 24$ και γι' αυτό $[H:1] = 30$. Όμως σύμφωνα με την Πρόταση 3.2.14 μια ομάδα τάξης 30 διαθέτει ακριβώς μία 5–Sylow υποομάδα. Ώστε $5 \nmid [H:1]$.

Αν ο 5 δεν είναι διαιρέτης τής $[H:1]$, τότε η τάξη $[H:1]$ είναι ένας διαιρέτης τού 12, δηλαδή $2, 3, 4, 6$, ή 12. Σύμφωνα με την Πρόταση 3.2.3, μια ομάδα τάξης 12 έχει είτε μια ορθόθετη 3–Sylow υποομάδα K_1 τάξης 3 είτε μια ορθόθετη 2–Sylow υποομάδα K_2 τάξης 4. Από την Πρόταση 3.2.12, γνωρίζουμε ότι αυτή η K_i, $i = 1$ είτε 2, είναι χαρακτηριστική υποομάδα τής H και λόγω τής Παρατήρησης 3.2.13 είναι ορθόθετη υποομάδα τής G. Συνεπώς, μπορούμε να δεχθούμε ότι η G διαθέτει μια ορθόθετη υποομάδα H' τάξης 3 ή 4. Όταν $[H:1] = 6$, τότε με παρόμοια επιχειρηματολογία μπορούμε, χωρίς περιορισμό τής γενικότητας, να δεχθούμε ότι η G διαθέτει μια ορθόθετη υποομάδα H' τάξης 2 ή 3. Σχηματίζουμε την πηλικοομάδα G/H' και παρατηρούμε ότι η τάξη $[G/H':1]$ θα είναι είτε 30 είτε 20 είτε 15. Ως εκ τούτου, η G/H' διαθέτει μια ορθόθετη υποομάδα $\overline{H}$ τάξης 5. (Όταν η τάξη τής G/H' είναι 30 ή 15, τότε το έχουμε ήδη αποδείξει. Όταν η τάξη είναι $20 = 2^2 \cdot 5$, τότε η ύπαρξη μιας ορθόθετης υποομάδας τάξης 5 αποδεικνύεται στην Πρόταση 3.2.4.) Θεωρούμε τον φυσικό επιμορφισμό $\pi : G \to G/H'$ και την αντίστροφη εικόνα $\pi^{-1}(\overline{H})$ τής ορθόθετης υποομάδας $\overline{H}$. Η $\pi^{-1}(\overline{H})$ είναι μια γνήσια ορθόθετη υποομάδα τής G που η τάξη της διαιρείται από τον αριθμό 5. Αυτό όμως οδηγεί σε άτοπο, όπως ήδη έχουμε διαπιστώσει. Συνεπώς, η G δεν διαθέτει μη τετριμμένες ορθόθετες υποομάδες, άρα πρόκειται για απλή ομάδα. □

Θεώρημα 3.2.19. *Η εναλλάσσουσα ομάδα $\mathbb{A}_5$ είναι απλή ομάδα.*

Απόδειξη. Η τάξη τής $\mathbb{A}_5$ είναι 60. Η $\mathbb{A}_5$ διαθέτει περισσότερα από 4 στοιχεία τάξης 5, δηλαδή περισσότερες από μία υποομάδες τάξης 5. Επομένως είναι μια απλή ομάδα. □

Ας δούμε τώρα τη γενική περίπτωση:

3.2.3 Η απλότητα τής $\mathbb{A}_n$, για $n \geq 5$

Λήμμα 3.2.20. *Η εναλλάσσουσα υποομάδα $\mathbb{A}_n$ τής συμμετρικής ομάδας $(S_n, \circ), n \geq 3$ παράγεται από τους κύκλους μήκους τρία.*

Απόδειξη. Κάθε στοιχείο τής $\mathbb{A}_n$ είναι μια σύνθεση άρτιου πλήθους αντιμεταθέσεων[2], αφού η $\mathbb{A}_n$ αποτελείται ακριβώς από τις άρτιες μετατάξεις τής S_n. Συνεπώς, η $\mathbb{A}_n$ παράγεται από τις συνθέσεις ζευγών αντιμεταθέσεων. Αρκεί να δείξουμε ότι οι συνθέσεις ζευγών αντιμεταθέσεων, είναι συνθέσεις κύκλων μήκους τρία.
Κάθε ζεύγος αντιμεταθέσεων διαθέτει ένα ή δεν διαθέτει κανένα κοινό στοιχείο[3].

Στην πρώτη περίπτωση, όπου τα $i, j, s \in \{1, 2, \ldots, n\}$ είναι ανά δύο διαφορετικά, έχουμε

$$\begin{pmatrix} i & j \end{pmatrix} \circ \begin{pmatrix} i & s \end{pmatrix} = \begin{pmatrix} i & s & j \end{pmatrix}$$

και στη δεύτερη περίπτωση, όπου τα $i, j, r, s \in \{1, 2, \ldots, n\}$ είναι ανά δύο διαφορετικά, έχουμε

$$\begin{pmatrix} i & j \end{pmatrix} \circ \begin{pmatrix} r & s \end{pmatrix} = \begin{pmatrix} i & r & j \end{pmatrix} \circ \begin{pmatrix} i & r & s \end{pmatrix}.$$

□

Πόρισμα 3.2.21. *Αν μια ορθόθετη υποομάδα N τής $\mathbb{A}_n, n \geq 3$ περιέχει έναν κύκλο μήκους τρία, τότε συμπίπτει με την $\mathbb{A}_n$.*

Απόδειξη. Προτρέπουμε τον αναγνώστη να επιβεβαιώσει τον ισχυρισμό στην περίπτωση όπου $n = 3$ ή 4. Εδώ θα εξετάσουμε την περίπτωση $n \geq 5$.

Παρατηρούμε ότι δοθέντος οποιουδήποτε 3–κύκλου $\sigma = \begin{pmatrix} i & j & k \end{pmatrix} \in S_n$, υπάρχει μια αντιμετάθεση $\tau = \begin{pmatrix} r & s \end{pmatrix} \in S_n$ με $\sigma \circ \tau = \tau \circ \sigma$. Πράγματι, αφού $n \geq 5$ μπορούμε να επιλέξουμε από το σύνολο $\{1, 2, \ldots, n\} \setminus \{i, j, k\}$ δύο στοιχεία r, s με $r \neq s$. Οι κύκλοι $\sigma = \begin{pmatrix} i & j & k \end{pmatrix}$ και $\tau = \begin{pmatrix} r & s \end{pmatrix} \in S_n$ είναι αποσυνδετοί και ως εκ τούτου μετατίθενται. Συνεπώς, δοθέντος οποιουδήποτε 3–κύκλου σ, ο κεντροποιητής του

$$\mathcal{C}_{S_n}(\sigma) = \{\varphi \in S_n \mid \varphi \circ \sigma \circ \varphi^{-1} = \sigma\}$$

[2] αντιμεταθέσεις ονομάζονται οι κύκλοι μήκους δύο

[3] αν το ζεύγος διαθέτει δύο κοινά στοιχεία, τότε η σύνθεση των ζευγών δίνει το ταυτοτικό στοιχείο τής S_n

περιέχει πάντοτε μια αντιμετάθεση τ.
Έτσι συμπεραίνουμε ότι η υποομάδα $\mathcal{C}_{S_n}(\sigma)\mathbb{A}_n$ τής S_n ισούται με την S_n, αφού $S_n = \tau\mathbb{A}_n \bigcup \mathbb{A}_n \subseteq \mathcal{C}_{S_n}(\sigma)\mathbb{A}_n$.
Θεωρούμε επίσης τον κεντροποιητή

$$\mathcal{C}_{\mathbb{A}_n}(\sigma) = \{\psi \in \mathbb{A}_n \mid \psi \circ \sigma \circ \psi^{-1} = \sigma\}$$

τού σ εντός τής $\mathbb{A}_n$. Προφανώς, $\mathcal{C}_{S_n}(\sigma) \bigcap \mathbb{A}_n = \mathcal{C}_{\mathbb{A}_n}(\sigma)$.

Τώρα υπολογίζουμε με τη βοήθεια τής Πρότασης 2.3.9 τον δείκτη $[\mathcal{C}_{S_n}(\sigma) : \mathcal{C}_{\mathbb{A}_n}(\sigma)]$.

$$[\mathcal{C}_{S_n}(\sigma) : \mathcal{C}_{\mathbb{A}_n}(\sigma)] = [\mathcal{C}_{S_n}(\sigma) : \mathcal{C}_{S_n}(\sigma) \bigcap \mathbb{A}_n] = [\mathcal{C}_{S_n}(\sigma)\mathbb{A}_n : \mathbb{A}_n] = [S_n : \mathbb{A}_n] = 2.$$

Επειδή

$$[S_n : \mathcal{C}_{S_n}(\sigma)][\mathcal{C}_{S_n}(\sigma) : \mathcal{C}_{\mathbb{A}_n}(\sigma)] = [S_n : \mathbb{A}_n][\mathbb{A}_n : \mathcal{C}_{\mathbb{A}_n}(\sigma)]$$

συμπεραίνουμε ότι

$$[S_n : \mathcal{C}_{S_n}(\sigma)] = [\mathbb{A}_n : \mathcal{C}_{\mathbb{A}_n}(\sigma)]. \tag{*}$$

Έστω ότι $\mathcal{O}_{S_n}(\sigma)$ (αντιστοίχως $\mathcal{O}_{\mathbb{A}_n}(\sigma)$) είναι η τροχιά τού σ που αποτελείται από τα στοιχεία τής S_n (αντιστοίχως τής $\mathbb{A}_n$) τα οποία είναι S_n–συζυγή (αντιστοίχως $\mathbb{A}_n$–συζυγή) τού σ. Ο πρώτος δείκτης $[S_n : \mathcal{C}_{S_n}(\sigma)]$ στην ισότητα (*) μετρά το πλήθος των στοιχείων τής $\mathcal{O}_{S_n}(\sigma)$ και ο δεύτερος $[\mathbb{A}_n : \mathcal{C}_{\mathbb{A}_n}(\sigma)]$ μετρά το πλήθος των στοιχείων τής $\mathcal{O}_{\mathbb{A}_n}(\sigma)$, δηλαδή το πλήθος των $\mathbb{A}_n$–συζυγών τού σ. Αφού $\mathcal{O}_{\mathbb{A}_n}(\sigma) \subseteq \mathcal{O}_{S_n}(\sigma)$ και επειδή πρόκειται για πεπερασμένα το πλήθος σύνολα με το ίδιο πλήθος στοιχείων συμπεραίνουμε ότι $\mathcal{O}_{S_n}(\sigma) = \mathcal{O}_{\mathbb{A}_n}(\sigma)$. Η τροχιά $\mathcal{O}_{S_n}(\sigma)$ συμπίπτει με το σύνολο όλων των 3–κύκλων τής S_n, αφού δύο οποιοιδήποτε 3–κύκλοι είναι S_n–συζυγείς. Συνεπώς, δύο οποιοιδήποτε 3–κύκλοι τής S_n είναι επίσης $\mathbb{A}_n$–συζυγείς, επειδή $\mathcal{O}_{S_n}(\sigma) = \mathcal{O}_{\mathbb{A}_n}(\sigma)$.
Αν λοιπόν μια ορθόθετη υποομάδα N τής $\mathbb{A}_n$ περιέχει έναν 3-κύκλο, τότε περιέχει και όλα τα στοιχεία τής $\mathbb{A}_n$–τροχιάς του. Αφού όμως όλοι οι 3–κύκλοι τής S_n είναι $\mathbb{A}_n$–συζυγείς, συμπεραίνουμε ότι η ορθόθετη υποομάδα N περιέχει όλους τους 3–κύκλους, επομένως και την υποομάδα που παράγεται από αυτούς, η οποία είναι η $\mathbb{A}_n$, λόγω τού Λήμματος 3.2.20.
Ώστε $\mathbb{A}_n \leq N$ και τελικώς $N = \mathbb{A}_n$. □

Θεώρημα 3.2.22. *Η εναλλάσσουσα υποομάδα $\mathbb{A}_n$ τής συμμετρικής ομάδας $(S_n, \circ)$ είναι απλή όταν $n \geq 5$.*

Απόδειξη. Ο ισχυρισμός θα αποδειχθεί με επαγωγή ως προς $n \geq 5$.
Για $n = 5$ γνωρίζουμε, βλ. Θεώρημα 3.2.19, ότι η $\mathbb{A}_5$ είναι απλή ομάδα.

Έστω ότι η $\mathbb{A}_m$ είναι απλή ομάδα, για κάθε $m \lneqq n$. Θα αποδείξουμε ότι η $\mathbb{A}_n$ είναι απλή ομάδα, όπου προφανώς το δοθέν n είναι ≥ 6. Συγκεκριμένα θα αποδείξουμε ότι κάθε ορθόθετη υποομάδα N τής $\mathbb{A}_n$ με $N \neq \{\mathrm{Id}_n\}$ ισούται με την $\mathbb{A}_n$.

Έστω $N \trianglelefteq \mathbb{A}_n$ με $N \neq \{\mathrm{Id}_n\}$. Ισχυριζόμαστε ότι υπάρχει $\sigma \in N, \sigma \neq \mathrm{Id}_n$ και $i \in \{1, 2, \ldots, n\}$ με $\sigma(i) = i$. Ας υποθέσουμε το αντίθετο, δηλαδή ότι

$$\boxed{(*)\ \forall \sigma \in N,\ \sigma \neq \mathrm{Id}_n \text{ και } \forall i \in \{1, 2, \ldots, n\}, \text{ έχουμε } \sigma(i) \neq i.}$$

Έστω $\sigma \in N, \sigma \neq \mathrm{Id}_n$. Η παράσταση τού σ είναι

$$ή\ \sigma = \begin{pmatrix} 1 & \dots & & a & \dots \\ a & \dots & 1 & & \dots \end{pmatrix}\ ή\ \sigma = \begin{pmatrix} 1 & \dots & a & \dots \\ a & \dots & 1 & \dots \end{pmatrix},\ όπου\ a \neq 1.$$

Επειδή $n \geq 6$, μπορούμε στην ανωτέρω παράσταση τού σ να επιλέξουμε μια στήλη η οποία να μην περιέχει ούτε στην πάνω ούτε στην κάτω γραμμή τα στοιχεία 1 ή a και έτσι θα έχουμε

$$ή\ \sigma = \begin{pmatrix} 1 & \dots & & a & \dots & b & \dots \\ a & \dots & 1 & & \dots & c & \dots \end{pmatrix}\ ή\ \sigma = \begin{pmatrix} 1 & \dots & a & \dots & b & \dots \\ a & \dots & 1 & \dots & c & \dots \end{pmatrix}.$$

Με άλλα λόγια μπορούμε να βρούμε $b \in \{1, 2, \dots, n\}$ με $b \neq 1, a$ και $\sigma(b) = c \neq 1, a$. Επιπλέον έχουμε $b \neq c$, λόγω τής παραδοχής (*). Τα στοιχεία $1, a, b, c$ είναι ανά δύο διαφορετικά, και απαρτίζουν ένα σύνολο τεσσάρων στοιχείων. Επειδή $n \geq 6$ μπορούμε να επιλέξουμε στοιχεία $d, e \in \{1, 2, \dots, n\} \setminus \{1, a, b, c\}$ με $d \neq e$.
Θεωρούμε το στοιχείο $\rho = \begin{pmatrix} 1 & a \end{pmatrix} \circ \begin{pmatrix} b & c & d & e \end{pmatrix} \in S_n$.
Το ρ είναι στοιχείο τής $\mathbb{A}_n$ ως γινόμενο δύο περιττών κύκλων τής S_n. Το $\rho \circ \sigma \circ \rho^{-1}$ ανήκει στην N, αφού $N \trianglelefteq \mathbb{A}_n$ και το $\rho \circ \sigma \circ \rho^{-1} \circ \sigma$ ανήκει επίσης στην N ως γινόμενο στοιχείων τής N.
Έχουμε

$$(\rho \circ \sigma \circ \rho^{-1} \circ \sigma)(1) = (\rho \circ \sigma \circ \rho^{-1})(a) = (\rho \circ \sigma)(1) = \rho(a) = 1.$$

Αλλά το $\rho \circ \sigma \circ \rho^{-1} \circ \sigma \neq \mathrm{Id}_n$, επειδή

$$\rho \circ \sigma \circ \rho^{-1} \circ \sigma(b) = \rho \circ \sigma \circ \rho^{-1}(c) = \rho \circ \sigma(b) = \rho(c) = d.$$

Συνεπώς, η παραδοχή (*) που κάναμε δεν είναι αληθής, αφού η ύπαρξη τού στοιχείου $\rho \circ \sigma \circ \rho^{-1} \circ \sigma$ τη διαψεύδει. Επομένως, υπάρχει κάποιο $\sigma \in N, \sigma \neq \mathrm{Id}_n$ και κάποιο $i \in \{1, 2, \dots, n\}$ με $\sigma(i) = i$.
Θεωρούμε το σύνολο $A_i = \{\varphi \in \mathbb{A}_n \mid \varphi(i) = i\}$ που αποτελείται από τα στοιχεία τής $\mathbb{A}_n$ τα οποία διατηρούν σταθερό το συγκεκριμένο i. Το A_i είναι μια υποομάδα τής $\mathbb{A}_n$ με $N \bigcap A_i \neq \{\mathrm{Id}_n\}$, αφού όπως αποδείξαμε υπάρχουν μη τετριμμένα στοιχεία τής N που έχουν αυτήν ακριβώς την ιδιότητα. Αλλά η A_i είναι ισόμορφη προς την εναλλάσσουσα υποομάδα $\mathbb{A}_{n-1}$ τής S_{n-1}, η οποία λόγω τής επαγωγικής υπόθεσης είναι απλή ομάδα. Επομένως, η τομή $N \bigcap A_i = A_i$ και επειδή η A_i περιέχει 3–κύκλους, συμπεραίνουμε ότι η N περιέχει 3–κύκλους. Όμως σύμφωνα με το Πόρισμα 3.2.21, η μοναδική ορθόθετη υποομάδα τής $\mathbb{A}_n$ που περιέχει έναν 3–κύκλο είναι η ίδια η $\mathbb{A}_n$. Ώστε η μοναδική ορθόθετη υποομάδα $N \neq \{\mathrm{Id}_n\}$ τής $\mathbb{A}_n$ είναι η $\mathbb{A}_n$ και γι' αυτό η $\mathbb{A}_n$ είναι απλή ομάδα. □

3.2.4 Κριτήρια για το πότε μια Ομάδα δεν είναι απλή

Πρόταση 3.2.23. *Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης n, όπου ο n είναι ένας σύνθετος αριθμός και ότι p είναι ένας πρώτος διαιρέτης τού n. Αν ο μόνος διαιρέτης τού n που ισούται με $1 \bmod p$ είναι ο 1, τότε η G δεν είναι απλή.*

Απόδειξη. Χωρίς περιορισμό τής γενικότητας μπορούμε να υποθέσουμε ότι η G δεν είναι p–ομάδα, αφού μια p–ομάδα έχει μη τετριμμένο κέντρο, το οποίο είναι ορθόθετη υποομάδα τής G.

Έστω n_p το πλήθος των p–Sylow υποομάδων για τον συγκεκριμένο p τής πρότασης. Από το Θεώρημα Sylow, βλ. Θεώρημα 3.1.5, γνωρίζουμε ότι ο n_p είναι ισοδύναμος με $1 \bmod p$ και ότι είναι διαιρέτης τού n. Από την υπόθεση τής πρότασης συμπεραίνουμε ότι $n_p = 1$. Ώστε, υπάρχει ακριβώς μία p–Sylow υποομάδα N τής G, η οποία είναι ορθόθετη. Η N είναι μια μη τετριμμένη υποομάδα τής G, επειδή η τάξη της είναι τουλάχιστον p και περιέχεται γνήσια στην G, αφού η G δεν είναι p–ομάδα. Επομένως, η G δεν είναι απλή. □

Για παράδειγμα, το κριτήριο αυτό πληροφορεί (για $p = 5$) ότι μια ομάδα τάξης $3^m 5^n$, $m, n \in \mathbb{N}$ δεν είναι απλή, όταν $m = 1, 2, 3$ και $n \in \mathbb{N}$. Παρομοίως, μια ομάδα τάξης $3^m 7^n$, $m, n \in \mathbb{N}$ δεν είναι απλή, όταν $1 \leq m \leq 5$ και $n \in \mathbb{N}$ (εδώ εφαρμόζουμε το κριτήριο με $p = 7$.).

Πρόταση 3.2.24. *Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης $2n$, όπου ο $n > 1$ είναι ένας περιττός αριθμός, τότε η G δεν είναι απλή.*

Απόδειξη. Υπενθυμίζουμε ότι από το Θεώρημα Cayley, βλ. Πόρισμα 2.3.4, γνωρίζουμε ότι η G εμφυτεύεται μέσω ενός μονομορφισμού $\chi : G \to S_{2n}$ στη συμμετρική ομάδα S_{2n} και αριθμώντας τα στοιχεία τού συνόλου τής G ως $\{g_1, g_2, \ldots, g_{2n}\}$, τότε διαπιστώνουμε εύκολα ότι το στοιχείο $g \in G$ αντιστοιχεί στη μετάταξη $\chi(g) \in S_{2n}$ με $\chi(g)(i) = j, 1 \leq i, j \leq 2n$, όταν $gg_i = g_j$. Παρατηρούμε ότι αν υπάρχει $i, 1 \leq i \leq 2n$ με $gg_i = g_i$, τότε $g = e_G$. Γι' αυτό όταν $g \neq e_G$, τότε για τη μετάταξη $\chi(g)$ έχουμε: $\forall i, 1 \leq i \leq 2n$, $\chi(g)(i) \neq i$, δηλαδή κανένα στοιχείο τού $\{1, 2, \ldots, 2n\}$ δεν μένει σταθερό από αυτήν.

Από το Θεώρημα Cauchy, βλ. Θεώρημα 2.3.11, γνωρίζουμε ότι η G διαθέτει ένα στοιχείο g με τάξη 2. Η αντίστοιχη μετάταξη $\chi(g)$ είναι μια σύνθεση αποσυνδετών κύκλων τ. Η τάξη $\circ(\chi(g))$ τής $\chi(g)$ είναι ίση με την τάξη τού g, δηλαδή 2. Η $\circ(\chi(g))$ ισούται επίσης με το ελάχιστο κοινό πολλαπλάσιο των μηκών των κύκλων τ. Επομένως, κάθε κύκλος τ οφείλει να έχει μήκος 2, δηλαδή να είναι μια αντιμετάθεση. Επειδή κανένα $i, 1 \leq i \leq 2n$, δεν μένει σταθερό από τη $\chi(g)$, συμπεραίνουμε ότι η $\chi(g)$ αποτελείται από ακριβώς n το πλήθος αντιμεταθέσεις και ότι η $\chi(g)$ είναι μια περιττή μετάταξη, αφού ο n είναι περιττός.

Από το Πόρισμα 1.4.18, προκύπτει ότι κάθε υποομάδα H μιας συμμετρικής ομάδας S_m αποτελείται ή εξολοκλήρου από άρτιες μετατάξεις ή αποτελείται από $(1/2)[H : 1]$ το πλήθος άρτιες μετατάξεις και $(1/2)[H : 1]$ το πλήθος περιττές. Στη δεύτερη περίπτωση το σύνολο H^+ των άρτιων μετατάξεων είναι μια ορθόθετη υποομάδα τής H.

Αφού λοιπόν η υποομάδα $\operatorname{im}\chi$ τής S_{2n} περιέχει περιττές μετατάξεις, έπεται ότι το υποσύνολο $\operatorname{im}\chi^+$ των άρτιων μετατάξεων τής $\operatorname{im}\chi$ είναι μια ορθόθετη υποομάδα τής $\operatorname{im}\chi$ με $(2n/2) = n$ το πλήθος στοιχεία. Επειδή η G είναι ισόμορφη προς την $\operatorname{im}\chi$, συμπεραίνουμε ότι η G περιέχει μια ορθόθετη υποομάδα τάξης n. Επομένως η G δεν είναι απλή. □

Συμπληρώνουμε τα κριτήρια με τρία ακόμα συμπεράσματα:

Πρόταση 3.2.25. *Αν $(G, \star)$ είναι μια ομάδα με πεπερασμένη τάξη και αν υπάρχει μια γνήσια υποομάδα $H < G$ με την ιδιότητα: ο αριθμός $[G : H]!$ να μην διαιρείται από την τάξη $[G : 1]$*

τής ομάδας, τότε η H περιέχει μια μη τετριμμένη ορθόθετη υποομάδα τής G και η G δεν είναι απλή.

Πρόταση 3.2.26. *Αν $(G, \star)$ είναι μια ομάδα με πεπερασμένη τάξη και αν υπάρχει μια γνήσια υποομάδα $H \leq G$ με δείκτη $[G : H] = p$ τον μικρότερο πρώτο αριθμό που διαιρεί την τάξη τής G, τότε η H είναι μια ορθόθετη υποομάδα τής G και η G δεν είναι απλή.*

(Βλ. Ενότητα 2.3.2, Πορίσματα 2.3.5 και 2.3.7.)

Πρόταση 3.2.27. *Κάθε ομάδα $(G, \star)$ τάξης pq ή p^2q ή pqr, όπου οι p, q, r είναι πρώτοι αριθμοί διαφορετικοί ανά δύο, διαθέτει μια μη τετριμμένη ορθόθετη υποομάδα και ως εκ τούτου δεν είναι απλή.*

(Βλ. Πρόταση 3.2.2, Πρόταση 3.2.4 και Πρόταση 3.2.8.)

3.2.5 Πεπερασμένες Υποομάδες τής Ομάδας των αντιστρέψιμων Στοιχείων ενός Σώματος

Η τελευταία εφαρμογή που θα παρουσιάσουμε συνδέεται με ένα πολύ ενδιαφέρον αποτέλεσμα τής Θεωρίας Σωμάτων. Κατ' αρχάς αποδεικνύουμε με τη βοήθεια τής Θεωρίας Sylow την επόμενη πρόταση, η οποία είναι παρεμφερής τού Θεωρήματος 1.5.20.

Πρόταση 3.2.28. *Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα με την ιδιότητα:*
Για κάθε $n \in \mathbb{N}$, υπάρχουν το πολύ n το πλήθος στοιχεία $g \in G$ με $g^n = e_G$. Τότε η G είναι μια κυκλική ομάδα.

Απόδειξη. Έστω p ένας πρώτος αριθμός με $p \mid [G : 1]$ και P μια p–Sylow υποομάδα τής G με τάξη $[P : 1] = p^\alpha$. Παρατηρούμε ότι τα p^α στο πλήθος στοιχεία g τής P ικανοποιούν την ισότητα $g^{p^\alpha} = e_G$. Αν τώρα P' είναι μια p–Sylow υποομάδα τής G με $P' \neq P$, τότε υπάρχει κάποιο $\xi \in P', \xi \notin P$ που ικανοποιεί την $\xi^{p^\alpha} = e_G$. Τότε όμως τουλάχιστον $p^\alpha + 1$ στο πλήθος στοιχεία τής G ικανοποιούν την $g^{p^\alpha} = e_G$. Αυτό αντίκειται στην υπόθεσή μας και γι' αυτό όλες οι p–Sylow υποομάδες τής G συμπίπτουν με την P. Συνεπώς, η P είναι μια ορθόθετη υποομάδα τής G.

Τώρα θα δείξουμε ότι η P είναι μια κυκλική υποομάδα τής G. Θεωρούμε το μέγιστο $m = \max\{\circ(g) \mid g \in P\}$ των τάξεων των στοιχείων τής P.

Επειδή η τάξη κάθε στοιχείου τής P είναι διαιρέτης τής $[P : 1] = p^\alpha$, έπεται ότι $m = p^\beta$. Θα δείξουμε ότι $\beta = \alpha$, από όπου προφανώς προκύπτει ότι η P είναι κυκλική.

Επειδή κάθε στοιχείο $g \in P$ έχει $\circ(g) = p^\gamma$, $\gamma \leq \beta$, έχουμε

$$g^{p^\beta} = \left(g^{p^\gamma}\right)^{p^{\beta-\gamma}} = (e_G)^{p^{\beta-\gamma}} = e_G.$$

Επομένως, τα p^α στο πλήθος στοιχεία g τής P ικανοποιούν την $g^{p^\beta} = e_G$. Αν όμως το β ήταν γνησίως μικρότερο τού α, τότε αυτό δεν θα συμφωνούσε με την υπόθεση τής πρότασής μας. Επομένως, $p^\alpha = p^\beta$ και γι' αυτό η P είναι κυκλική και ισόμορφη προς την $\mathbb{Z}_{p^\alpha}$.

Θεωρούμε την ανάλυση τής τάξης τής $[G:1]$ σε δυνάμεις διαφορετικών πρώτων αριθμών, ας πούμε $[G:1] = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, όπου οι $p_i, i = 1, \dots, s$ είναι πρώτοι αριθμοί και οι $\alpha_i, i = 1, \dots, s$ είναι φυσικοί.

Από τα προηγούμενα γνωρίζουμε ότι κάθε p_i–Sylow υποομάδα P_i είναι κυκλική τάξης $p_i^{\alpha_i}$ και ορθόθετη. Θεωρούμε την απεικόνιση

$$\varphi : P_1 \times P_2 \times \cdots \times P_s \to G, (x_1, x_2, \dots, x_s) \mapsto x_1 x_2 \dots x_s.$$

Παρατηρούμε ότι $\forall i = 1, 2, \dots, s, P_i \bigcap (P_1 P_2 \dots P_{i-1} P_{i+1} \dots P_s) = \{e_G\}$, επειδή η τάξη τής P_i είναι $p_i^{\alpha_i}$ ενώ η τάξη τής $P_1 P_2 \dots P_{i-1} P_{i+1} \dots P_s$ είναι $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_{i-1}{}^{\alpha_{i-1}} p_{i+1}{}^{\alpha_{i+1}} \dots p_s^{\alpha_s}$. Επιπλέον παρατηρούμε ότι γινόμενα στοιχείων από διαφορετικές υποομάδες P_i και P_j μετατίθενται μεταξύ τους. Γι' αυτό η φ είναι ένας ομομορφισμός ομάδων, ο οποίος μάλιστα είναι και μονομορφισμός. Επιπλέον, επειδή το πλήθος των στοιχείων τού γινομένου $P_1 \times P_2 \times \cdots \times P_s$ είναι ίδιο με την τάξη $[G:1]$ έπεται ότι ο φ είναι ισομορφισμός.

Έτσι

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}} \cong \mathbb{Z}_{p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}}.$$

Ώστε η G είναι μια κυκλική ομάδα. □

Θεώρημα 3.2.29. *Έστω K ένα σώμα και $(K^\star, \cdot)$ η πολλαπλασιαστική ομάδα των αντιστρέψιμων στοιχείων του. Κάθε πεπερασμένη υποομάδα G τής $K^\star$ είναι κυκλική.*

Απόδειξη. Παρατηρούμε ότι $\forall n \in \mathbb{N}$, το πολυώνυμο $x^n - 1_K \in K[x]$ έχει το πολύ n το πλήθος θέσεις μηδενισμού στο K. Συνεπώς, $\forall n \in \mathbb{N}$, υπάρχουν το πολύ n το πλήθος στοιχεία g τής G που ικανοποιούν την $g^n = 1_K$. Σύμφωνα με την προηγούμενη πρόταση, η G είναι μια κυκλική ομάδα. □

Παρατήρηση 3.2.30. Το προηγούμενο θεώρημα εφαρμόζεται άμεσα στο σύνολο των n–οστών ριζών τής μονάδας ενός σώματος K, δηλαδή στο σύνολο

$$\Omega_n = \{\omega \in K \mid \omega^n = 1_K\}.$$

Το σύνολο Ω_n είναι μια πεπερασμένη υποομάδα τής πολλαπλασιαστικής ομάδας $(K^\star, \cdot)$ των αντιστρέψιμων στοιχείων τού K. Σύμφωνα με το Θεώρημα 3.2.29, η Ω_n είναι κυκλική.

Οι γεννήτορες τής Ω_n είναι οι λεγόμενες *πρωταρχικές n–οστές ρίζες τής μονάδας* που περιέχονται στο σώμα K.

Ασκήσεις στη Θεωρία Sylow

Λυμένες Ασκήσεις

Α 114. Να δειχθεί ότι μια ομάδα $(G, \star)$ τάξης 351 έχει μια ορθόθετη p-Sylow υποομάδα, για κάποιον πρώτο p που διαιρεί την τάξη της.

Λύση. Η ομάδα G έχει τάξη $351 = 3^3 \cdot 13$. Το πλήθος n_3 των 3-Sylow υποομάδων της ικανοποιεί την ισοτιμία $n_3 \equiv 1 \bmod 3$ και είναι ένας διαιρέτης τού 13. Επομένως ή $n_3 = 1$ ή $n_3 = 13$. Το πλήθος n_{13} των 13-Sylow υποομάδων της ικανοποιεί την ισοτιμία $n_{13} \equiv 1 \bmod 13$ και είναι ένας διαιρέτης τού 3^3. Επομένως ή $n_{13} = 1$ ή $n_{13} = 3^3 = 27$.

Αν ήταν $n_3 \neq 1$ και $n_{13} \neq 1$, τότε θα είχαμε $n_3 = 13$ το πλήθος υποομάδες τάξης $3^3 = 27$ και $n_{13} = 27$ το πλήθος υποομάδες τάξης 13. Τότε οι 27 το πλήθος υποομάδες τάξης 13 θα χορηγούσαν $27(13-1) = 324$ διαφορετικά στοιχεία τάξης 13. Αν οι H_1 και H_2 ήταν δύο υποομάδες τάξης 27 με $H_1 \neq H_2$, τότε η ένωσή τους $H_1 \bigcup H_2$ θα περιείχε τουλάχιστον $27 + 1 = 28$ διαφορετικά στοιχεία που κανένα τους δεν θα ήταν τάξης 13, αφού $13 \nmid 27$. Ως εκ τούτου, η G θα είχε τουλάχιστον $324 + 28 = 352$ στοιχεία, το οποίο είναι άτοπο.

Α 115. Έστω $S_3 \times S_3$ το ευθύ γινόμενο τής συμμετρικής ομάδας $(S_3, \circ)$ με τον εαυτό της. Για κάθε πρώτο διαιρέτη p τής τάξης τής $S_3 \times S_3$, να βρεθούν οι p-Sylow υποομάδες τής $S_3 \times S_3$.

Λύση. Η τάξη ευθέως γινομένου ισούται με $[S_3 : 1]^2 = (3!)^2 = 2^2 3^2$.

Οι 2-Sylow υποομάδες είναι τάξης $2^2 = 4$ και σύμφωνα με το Θεώρημα Sylow, βλ. Θεώρημα 3.1.5, το πλήθος τους n_2 ικανοποιεί την $n_2 \equiv 1 \bmod 2$ με το $n_2 \mid 3^2$. Άρα, το n_2 ισούται ή με 1 ή με 3 ή με 9. Είναι πολύ εύκολος ο εντοπισμός 3^2 το πλήθος 2-Sylow υποομάδων. Πράγματι, έστω ότι τ_1, τ_2 και τ_3 είναι οι τρεις αντιμεταθέσεις τής S_3. Οι ομάδες $\langle \tau_i \rangle \times \langle \tau_j \rangle, 1 \leq i, j \leq 3$ είναι τάξης 4 και προφανώς είναι υποομάδες τής $S_3 \times S_3$. Το πλήθος τους ισούται με εννέα. Επομένως, αυτές ακριβώς είναι οι 2-Sylow υποομάδες τής $S_3 \times S_3$.

Οι 3-Sylow υποομάδες είναι τάξης $3^2 = 9$ και σύμφωνα με το Θεώρημα Sylow, το πλήθος τους n_3 ικανοποιεί την $n_3 \equiv 1 \bmod 3$ με το $n_3 \mid 2^2$. Άρα, το n_3 ισούται ή με 1 ή με 4. Έστω ότι K είναι μια 3-Sylow υποομάδα τής $S_3 \times S_3$. Επειδή κάθε στοιχείο τής $S_3 \times S_3$ είναι τάξης ή 1 ή 2 ή 3 ή 6 (*γιατί;*), συμπεραίνουμε ότι η K δεν μπορεί να είναι μια κυκλική υποομάδα τής K τάξης 9 και ως εκ τούτου, κάθε μη ταυτοτικό στοιχείο $a \in K$ είναι τάξης 3. Τα στοιχεία τάξης 3 τής $S_3 \times S_3$ είναι ακριβώς τα οκτώ στοιχεία τού συνόλου

$$C = \{(\sigma, \rho) \mid \circ(\sigma) = 1 \text{ ή } 3, \circ(\rho) = 1 \text{ ή } 3, \} \setminus \{(\mathrm{Id}_3, \mathrm{Id}_3)\}.$$

Η $S_3 \times S_3$ δεν έχει κανένα άλλο στοιχείο τάξης 3. Αν υπήρχαν δύο 3-Sylow υποομάδες τής $S_3 \times S_3$, τότε θα υπήρχε τουλάχιστον ακόμα ένα στοιχείο τάξης 3 διαφορετικό από τα στοιχεία τού C, το οποίο είναι αδύνατο. Επομένως, η K είναι η μοναδική 3-Sylow υποομάδα τής $S_3 \times S_3$. Παρατηρούμε ότι το σύνολο $C \bigcup \{(\mathrm{Id}_3, \mathrm{Id}_3)\}$ είναι ακριβώς το σύνολο των στοιχείων τής υποομάδας $\langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \rangle \times \langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \rangle$ τής $S_3 \times S_3$, διότι η τάξης 3 υποομάδα $\langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \rangle$ τής S_3 περιέχει και τα δύο στοιχεία τάξης 3 τής S_3 Επομένως, η μοναδική 3-Sylow υποομάδα τής $S_3 \times S_3$ είναι η $K = \langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \rangle \times \langle \begin{pmatrix} 1 & 2 & 3 \end{pmatrix} \rangle$.

Α 116. Πόσα στοιχεία τάξης 7 έχει μια απλή ομάδα $(G, \star)$ τάξης 168;

Λύση. Η ομάδα G έχει τάξη $168 = 2^3 \cdot 3 \cdot 7 \cdot 13$. Το πλήθος n_7 των 7-Sylow υποομάδων της ικανοποιεί την ισοτιμία $n_7 \equiv 1 \bmod 7$ και είναι ένας διαιρέτης τού $2^3 \cdot 3$. Επομένως ή $n_7 = 1$ ή $n_7 = 8$. Αν όμως ήταν $n_7 = 1$, τότε η G θα είχε μια ορθόθετη υποομάδα τάξης 7, το οποίο είναι αδύνατο διότι έχουμε υποθέσει ότι η G είναι απλή. Επομένως, $n_7 = 8$ και η G έχει 8 το πλήθος υποομάδες τάξης 7. Ως εκ τούτου, η G έχει ακριβώς $8(7-1) = 48$ στοιχεία τάξης 7, βλ. Άσκηση ΠΑ66.

Α 117. Να δειχθεί ότι μια ομάδα $(G, \star)$ τάξης 24 διαθέτει μια ορθόθετη υποομάδα τάξης 4 ή 8.

Λύση. Η G διαθέτει μια 2-Sylow υποομάδα P τάξης $2^3 = 8$, διότι $24 = 2^3 \cdot 3$. Θεωρούμε τη δράση $\pi_P : G \times G/P \to G/P, (g, hP) \mapsto ghP$ τής G επί τού συνόλου G/P των αριστερών πλευρικών κλάσεων τής P στην G και τον αντίστοιχο ομομορφισμό $X(\pi_P) : G \to S_{G/P}$, όπου $S_{G/P}$ είναι η συμμετρική ομάδα τού συνόλου G/P. Η $S_{G/P}$ έχει $3! = 6$ στοιχεία, διότι ο δείκτης $[G : P] = 3$. Η τάξη τού πυρήνα $\ker X(\pi_P)$ είναι διαιρέτης τής τάξης 8 τής P, διότι $\ker X(\pi_P) \leq P$, βλ. Θεώρημα 2.3.3. Επιπλέον αφού $G/X(\pi_P) \cong \operatorname{im} X(\pi_P)$, συμπεραίνουμε ότι ο $[G : \ker X(\pi_P)] \mid 6$ και ως εκ τούτου, $[\ker X(\pi_P) : 1] = 4$ ή 8.

Α 118. Παρατηρώντας ότι το πλήθος των κύκλων μήκους $\ell \leq n$ τής συμμετρικής ομάδας S_n, ισούται με $n(n-1)\ldots(n-(\ell-1))/\ell$ να αποδείξετε ότι

(α′) το πλήθος των p–Sylow υποομάδων τής S_p, όπου ο p είναι ένας πρώτος αριθμός, ισούται με $(p-2)!$ και κατόπιν να συμπεράνετε ότι

(β′) ο p διαιρεί τον αριθμό $(p-1)! + 1$ (Το Θεώρημα Wilson).

Λύση. (α′) Το πλήθος των κύκλων μήκους p ισούται με $(p-1)!$. Κάθε κύκλος μήκους p χορηγεί μια κυκλική υποομάδα τάξης p και αντίστροφα κάθε κυκλική υποομάδα τάξης p έχει ως γεννήτορα έναν κύκλο μήκους p. Επιπλέον, η τομή δύο οποιωνδήποτε διαφορετικών υποομάδων τάξης p είναι μόνο το ταυτοτικό στοιχείο, αφού ο p είναι ένας πρώτος αριθμός. Αν k είναι το πλήθος των διαφορετικών κυκλικών υποομάδων τάξης p, τότε η S_p διαθέτει $k(p-1)$ στοιχεία τάξης p. Έτσι έχουμε $k(p-1) = (p-1)! \Rightarrow k = (p-2)!$.

(β′) Αφού $[S_p : 1] = 1 \cdot 2 \cdot \ldots \cdot (p-1) \cdot p$, συμπεραίνουμε ότι οι p–Sylow υποομάδες συμπίπτουν με τις κυκλικές υποομάδες τάξης p και γι’ αυτό, λόγω τής Θεωρίας Sylow, γνωρίζουμε ότι το πλήθος τους n_p ικανοποιεί την $n_p \equiv 1 \bmod p$. Αλλά $n_p = (p-2)!$. Επομένως,

$$(p-2)! \equiv 1 \bmod p \Leftrightarrow (p-2)! = 1 + \lambda p, \text{ με } \lambda \in \mathbb{N} \cup \{0\} \text{ και } p \text{ πρώτο } \Leftrightarrow$$
$$(p-1)! = (p-1) + \lambda p(p-1) \Leftrightarrow p \mid (p-1)! + 1.$$

Α 119. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα, ότι $K \trianglelefteq G$ είναι μια ορθόθετη υποομάδα τής G και ότι P είναι μια p-Sylow υποομάδα τής K. Να δειχθεί ότι $K\mathcal{N}_G(P) = G$, όπου $\mathcal{N}_G(P)$ είναι ο ορθοθετοποιητής τής P στην G.

Λύση. Για κάθε $g \in G$, είναι $gKg^{-1} = K$, διότι $K \trianglelefteq G$. Για κάθε $g \in G$, έχουμε $gPg^{-1} \leq gKg^{-1} = K$, αφού $P \leq K$. Η gPg^{-1} είναι μια p-Sylow υποομάδα τής K, διότι είναι μια υποομάδα τής K που έχει το ίδιο πλήθος στοιχείων με την P. Ως εκ τούτου, υπάρχει κάποιο $k \in K$ με $kPk^{-1} = gPg^{-1}$, αφού όλες οι p-Sylow υποομάδες μιας ομάδας είναι συζυγείς. Επειδή $P = k^{-1}gPg^{-1}k$, συμπεραίνουμε ότι το $k^{-1}g$ ανήκει στον ορθοθετοποιητή $\mathcal{N}_G(P)$ και ως εκ τούτου, το $g \in G$ ανήκει στην αριστερή πλευρική κλάση $k\mathcal{N}_G(P)$. Άρα, $K\mathcal{N}_G(P) = G$.

Α 120. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι P είναι μια p-Sylow υποομάδα της. Για κάθε ορθόθετη υποομάδα K τής G, να δειχθεί ότι η $P \bigcap K$ είναι μια p-Sylow υποομάδα τής K και η KP/K είναι μια p-Sylow υποομάδα τής G/K.

Λύση. Η τάξη τής $P \bigcap K$ είναι μια δύναμη του p, διότι η τάξη $[P \bigcap K : 1]$ είναι διαιρέτης τής τάξης $[P : 1]$. Παρατηρούμε ότι ο p δεν είναι διαιρέτης τού δείκτη $[K : P \bigcap K]$, επειδή ο $[K : P \bigcap K] = \frac{[K:1]}{[P \bigcap K:1]} = \frac{[KP:1]}{[P:1]}$, βλ. Πρόταση 2.3.9, και αφού προφανώς η P είναι μια p-Sylow υποομάδα τής ομάδας KP. Επομένως, η $P \bigcap K$ είναι μια p-υποομάδα τής K μέγιστης p-δύναμης, άρα είναι μια p-Sylow υποομάδα τής K.
Η τάξη τής πηλικοομάδας KP/K είναι μια δύναμη τού p, διότι $KP/K \cong P/P \bigcap K$. Από το Τρίτο Θεώρημα Ισομορφίας, βλ. Θεώρημα 1.7.27, έχουμε ότι $(G/K)/(KP/K) \cong G/KP$ και αφού η τάξη $[G : KP]$ είναι διαιρέτης τής τάξης $[G : P]$ (διότι $P \leq KP$) συμπεραίνουμε ότι ο p δεν διαιρεί την τάξη $[G : KP]$. Ως εκ τούτου, ο p δεν διαιρεί την τάξη $[(G/K)/(KP/K) : 1] = [G/K : KP/K]$ και γι' αυτό η KP/K είναι μια p-υποομάδα τής G/K μέγιστης p-δύναμης, άρα είναι μια p-Sylow υποομάδα τής G/K.

Α 121. Έστω ότι $H \trianglelefteq \mathbb{A}_n$ είναι μια ορθόθετη υποομάδα τής $\mathbb{A}_n$, η οποία περιέχει το γινόμενο δύο αποσυνδετών (ξένων) αντιμεταθέσεων τής συμμετρικής ομάδας S_n.

Όταν $n \geq 5$, τότε χωρίς να χρησιμοποιήσετε το ότι η $\mathbb{A}_n$ είναι απλή, να δείξετε ότι $H = \mathbb{A}_n$,

Λύση. Από το Πόρισμα 3.2.21, γνωρίζουμε ότι για $n \geq 3$, κάθε ορθόθετη υποομάδα H τής $\mathbb{A}_n$ που περιέχει έναν κύκλο μήκους τρία, συμπίπτει με την $\mathbb{A}_n$.
Αρκεί λοιπόν να αποδείξουμε ότι η H περιέχει έναν κύκλο μήκους 3. Ας είναι $\sigma = \begin{pmatrix} i & j \end{pmatrix} \circ \begin{pmatrix} k & \ell \end{pmatrix} \in H$ το γινόμενο των αποσυνδετών κύκλων μήκους 2 που περιέχονται στην H, όπου οι $i, j, k, \ell \in \{1, 2, \ldots, n\}$ είναι ανά δύο διαφορετικοί φυσικοί. Αφού $n \geq 5$, υπάρχει κάποιος $m \in \{1, 2, \ldots, n\}$ διαφορετικός από τους i, j, k, ℓ. Θεωρούμε το στοιχείο $\tau = \begin{pmatrix} i & j \end{pmatrix} \circ \begin{pmatrix} k & m \end{pmatrix}$ τής $\mathbb{A}_n$.
Το γινόμενο $\tau \circ \sigma \circ \tau^{-1}$ ανήκει στην H, αφού $H \trianglelefteq \mathbb{A}_n$ και το $\tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1}$ ανήκει επίσης στην H, αφού $\sigma^{-1} \in H$. Είναι:

$$(\tau \circ \sigma \circ \tau^{-1}) \circ \sigma^{-1} = \begin{pmatrix} i & j \end{pmatrix} \circ \begin{pmatrix} m & \ell \end{pmatrix} \circ \begin{pmatrix} i & j \end{pmatrix} \circ \begin{pmatrix} k & \ell \end{pmatrix} =$$
$$\begin{pmatrix} m & \ell \end{pmatrix} \circ \begin{pmatrix} k & \ell \end{pmatrix} = \begin{pmatrix} k & m & \ell \end{pmatrix}.$$

Προτεινόμενες Ασκήσεις

ΠΑ 109. Έστω ότι $(G, \star)$ είναι μια ομάδα και H, K είναι υποομάδες τής G. Να δειχθούν τα εξής:

(α′) Αν η H είναι χαρακτηριστική υποομάδα τής K και η K είναι χαρακτηριστική υποομάδα τής G, τότε η H είναι χαρακτηριστική υποομάδα τής G.

(β′) Αν οι H και K είναι χαρακτηριστικές υποομάδες τής G, τότε οι HK και $H \bigcap K$ είναι επίσης χαρακτηριστικές υποομάδες τής G.

ΠΑ 110. Να δειχθεί ότι μια ομάδα τάξης 312 έχει μια ορθόθετη p-Sylow υποομάδα, για κάποιον πρώτο p που διαιρεί την τάξη της.

ΠΑ 111. Να δειχθεί ότι μια ομάδα τάξης 50 διαθέτει μια μη τετριμμένη ορθόθετη υποομάδα.

ΠΑ 112. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης 21 που δεν είναι κυκλική. Να βρεθεί το πλήθος n_3 των 3-Sylow υποομάδων της.

ΠΑ 113. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης 168. Αν η G έχει μια ορθόθετη υποομάδα τάξης 4, τότε να δειχθεί ότι έχει μια ορθόθετη υποομάδα τάξης 28.

ΠΑ 114. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι P και P' είναι δύο p–Sylow υποομάδες τής G. Αν οι P, P' περιέχονται σε μια υποομάδα H τής G, τότε να δειχθεί ότι είναι συζυγείς εντός τής H.

ΠΑ 115. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης $p^n m$, όπου ο p είναι ένας πρώτος αριθμός με $p > m$. Να δειχθεί ότι η G διαθέτει μια ορθόθετη υποομάδα τάξης p^n.

ΠΑ 116. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και $\mathrm{Syl}_p(G)$ το σύνολο των p–Sylow υποομάδων της. Να δειχθεί ότι η υποομάδα τής G, που παράγεται από το σύνολο $\bigcup_{P \in \mathrm{Syl}_p(G)} P$, είναι μια ορθόθετη υποομάδα τής G.

ΠΑ 117. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα, ότι $K \trianglelefteq G$ είναι μια ορθόθετη υποομάδα τής G και ότι p είναι ένας πρώτος αριθμός με $p \mid [G : 1]$ και $p \nmid [G : K]$. Να δειχθεί ότι κάθε p-Sylow υποομάδα τής G περιέχεται στην K.

ΠΑ 118. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα, ότι $H \leq G$ είναι μια υποομάδα τής G και ότι P είναι μια ορθόθετη p-Sylow υποομάδα τής G. Να δειχθεί ότι η $P \bigcap H$ είναι η μοναδική p-Sylow υποομάδα τής H

ΠΑ 119. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι $K \trianglelefteq G$ είναι μια ορθόθετη υποομάδα τής G. Να δειχθεί ότι $n_p(G/K) \leq n_p(G)$.

Κεφάλαιο 4

Ευθέα Γινόμενα Ομάδων

Για την περαιτέρω ανάπτυξη τής θεωρίας θα χρειαστούμε ορισμένα στοιχεία από τα ευθέα γινόμενα[1] ομάδων τα οποία παρουσιάζουμε παρακάτω.

4.1 Εξωτερικό και Εσωτερικό ευθύ Γινόμενο

4.1.1 Εξωτερικό ευθύ Γινόμενο

Ορισμός 4.1.1. Έστω ότι $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι δύο ομάδες. Ονομάζουμε *εξωτερικό ευθύ γινόμενο των ομάδων* G_1 και G_2 την ομάδα $(G_1 \times G_2, \star)$, όπου $G_1 \times G_2$ είναι το καρτεσιανό γινόμενο των G_1 και G_2 και όπου η πράξη «$\star$» ορίζεται ως

$$\begin{aligned} &\star : (G_1 \times G_2) \times (G_1 \times G_2) \to (G_1 \times G_2)\,, \\ &((g_1, g_2), (h_1, h_2)) \mapsto (g_1, g_2) \star (h_1, h_2) := (g_1 \star_1 h_1, g_2 \star_2 h_2) \end{aligned}$$

Ο προηγούμενος ορισμός γενικεύεται στο εξωτερικό ευθύ γινόμενο $(\prod_{i \in I} G_i, \star)$ οποιασδήποτε οικογένειας ομάδων $((G_i, \star_i))_{i \in I}$.

Παράδειγμα 4.1.2. Η ομάδα $(\mathcal{R}, +)$ με στοιχεία τις ακολουθίες $(\alpha_i)_{i \in \mathbb{N}}$ των πραγματικών αριθμών και πράξη

$$+ : \mathcal{R} \times \mathcal{R} \to \mathcal{R},\ \big((\alpha_i)_{i \in \mathbb{N}}, (\beta_i)_{i \in \mathbb{N}}\big) \mapsto \big((\alpha_i + \beta_i)_{i \in \mathbb{N}}\big)$$

την πρόσθεση των ακολουθιών συμπίπτει με το εξωτερικό ευθύ γινόμενο τής οικογένειας ομάδων $((G_i, \star_i))_{i \in \mathbb{N}}$, όπου για κάθε δείκτη $i \in \mathbb{N}$, η ομάδα $(G_i, \star_i)$ ισούται με την ομάδα $(\mathbb{R}, +)$ των πραγματικών αριθμών με πράξη τη συνηθισμένη πρόσθεση των πραγματικών.

Η επόμενη πρόταση αποδεικνύεται σε οποιοδήποτε εισαγωγικό μάθημα άλγεβρας, βλ. επίσης Ασκήσεις Α88 και ΠΑ91:

[1] Στο κείμενο έχουμε ήδη συζητήσει διάσπαρτα το (εξωτερικό) ευθύ γινόμενο, για παράδειγμα βλ. Άσκηση Α18.

Πρόταση 4.1.3. *Έστω ότι $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι δύο ομάδες.*

(α′) *Το εξωτερικό ευθύ γινόμενο $(G_1 \times G_2, \star)$ των G_1 και G_2 είναι μια αβελιανή ομάδα, αν και μόνο αν, οι $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι αβελιανές.*

(β′) *Το εξωτερικό ευθύ γινόμενο $(G_1 \times G_2, \star)$ είναι ισόμορφο προς το εξωτερικό ευθύ γινόμενο $(G_2 \times G_1, \star')$.*

(γ′) *Αν οι G_1 και G_2 είναι πεπερασμένες κυκλικές ομάδες με τάξεις σχετικώς πρώτες, δηλαδή με $\text{ΜΚΔ}([G_1 : 1], [G_2 : 1]) = 1$, τότε το εξωτερικό ευθύ γινόμενο $(G_1 \times G_2, \star)$ είναι κυκλική ομάδα τάξης $[G_1 : 1] \cdot [G_2 : 1]$.*

Πόρισμα 4.1.4. *Έστω ότι $((G_i, \star_i))_{i\in I}, I = \{1, 2, \ldots, s \in \mathbb{N}\}$, είναι μια πεπερασμένη οικογένεια κυκλικών ομάδων, όπου οι τάξεις $[G_i : 1] = n_i$ είναι ανά δύο σχετικώς πρώτες, δηλαδή όπου $\text{ΜΚΔ}(n_i, n_j) = 1, \forall i, j, 1 \leq i, j \leq s, i \neq j$. Τότε το εξωτερικό ευθύ γινόμενο $(\prod_{i=1}^{s} G_i, \star)$ τής οικογένειας $((G_i, \star_i))_{i\in I}$ είναι μια κυκλική ομάδα τάξης $\prod_{i=1}^{s} n_i$.*

Απόδειξη. Επαγωγή ως προς το πλήθος s των ομάδων. □

Παρατήρηση 4.1.5. (α′) Το εξωτερικό ευθύ γινόμενο $(G_1 \times G_2, \star)$ δύο κυκλικών ομάδων $(G_1, \star_1)$ και $(G_2, \star_2)$ δεν είναι απαραιτήτως κυκλική ομάδα.

Για παράδειγμα, το εξωτερικό ευθύ γινόμενο τής κυκλικής ομάδας C_n με $n > 1$ στοιχεία, δηλαδή η $C_n \times C_n$, δεν είναι **ποτέ** μια κυκλική ομάδα, αφού η τάξη οποιουδήποτε στοιχείου $(a, b) \in C_n \times C_n$ είναι πάντοτε ένας διαιρέτης τού n (γιατί;), ενώ η τάξη της $[C_n \times C_n : 1]$ ισούται με n^2. (Βλ. Ασκήσεις Α59 και Α61.)

(β′) Είναι εύκολη η διαπίστωση ότι αν $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι δύο ομάδες και $H_i \leq G_i, i = 1, 2$, είναι αντιστοίχως δύο υποομάδες τους, τότε το εξωτερικό ευθύ γινόμενο $H_1 \times H_2$ είναι μια υποομάδα τού εξωτερικού ευθέος γινομένου $G_1 \times G_2$. (Βλ. Άσκηση Α29.) Ωστόσο, δεν έχει κάθε υποομάδα $H \leq G_1 \times G_2$ απαραιτήτως τη συγκεκριμένη μορφή.

Επί παραδείγματι, το εξωτερικό ευθύ γινόμενο $\mathbb{Z} \times \mathbb{Z}$ διαθέτει ως υποομάδα τη

$$\Delta = \{(z, z) \mid z \in \mathbb{Z}\}.$$

Ωστόσο, δεν υπάρχουν υποομάδες H_1, H_2 τής $\mathbb{Z}$ με $H_1 \times H_2 = \Delta$. Αφού, αν υπήρχαν $H_1, H_2 \leq \mathbb{Z}$ με $H_1 \times H_2 = \Delta$, τότε κάθε $(h_1, h_2) \in H_1 \times H_2$ θα ήταν ίσο με κάποιο $(z, z) \in \Delta$ και γι' αυτό τελικώς θα ήταν $H_1 = H_2$. Τώρα επειδή η $\mathbb{Z}$ είναι κυκλική, έπεται ότι η H είναι επίσης κυκλική. Συνεπώς, θα υπήρχε $a \in \mathbb{Z}, a \geq 0$ με $H = \langle a \rangle$. Αλλά τώρα αφού $H \times H = \Delta$, πρέπει όλα τα στοιχεία τής H να είναι ίσα, το οποίο μπορεί να συμβεί μόνο στην περίπτωση όπου $H = \{0\}$. Αυτό είναι άτοπο, διότι η τάξη τής $H \times H$ ισούται με 1, ενώ η τάξη τής Δ είναι άπειρη.

Ορισμός 4.1.6. Τα εξωτερικά ευθέα γινόμενα $(\prod_{i=1}^{n} G_i, \star)$, όπου κάθε ομάδα G_i είναι ισόμορφη προς την κυκλική ομάδα C_p, p πρώτος αριθμός, ονομάζονται *στοιχειώδεις αβελιανές p–ομάδες*.

Προσέξτε ότι το εξωτερικό ευθύ γινόμενο $(G_1 \times G_2, \star)$ δύο ομάδων $(G_1, \star_1)$ και $(G_2, \star_2)$ δεν έχει ως υποομάδες τις G_1 και G_2. Ωστόσο, η συγκεκριμένη «ιδιάζουσα συμπεριφορά» αίρεται με την εισαγωγή τής έννοιας τού εσωτερικού ευθέος γινομένου.

4.1.2 Εσωτερικό ευθύ Γινόμενο

Ορισμός 4.1.7. Έστω ότι $\{G_i \mid i = 1, 2, \ldots, s\}$ είναι ένα πεπερασμένο σύνολο υποομάδων μιας ομάδας $(G, \star)$. Η G ονομάζεται το *εσωτερικό ευθύ γινόμενο* των υποομάδων $G_i, i = 1, 2, \ldots, s$, όταν για κάθε $1 \leq i \leq s$, η $G_i \trianglelefteq G$ είναι ορθόθετη υποομάδα τής G και όταν κάθε $g \in G$ γράφεται κατά μοναδικό τρόπο ως γινόμενο τής μορφής $g = g_1 g_2 \ldots g_s$, όπου $g_i \in G_i, \forall i, 1 \leq i \leq s$.

Γενικά ονομάζουμε την G ένα γινόμενο των υποομάδων της $\{G_i \mid i = 1, 2, \ldots, s\}$, όπου $G_i \trianglelefteq G, \forall i, 1 \leq i \leq s$, όταν $G = G_1 \cdot G_2 \cdot \ldots \cdot G_s$, δηλαδή όταν κάθε στοιχείο $g \in G$ ισούται με ένα γινόμενο τής μορφής $g_1 g_2 \ldots g_s$, όπου $g \in G_i, \forall i, 1 \leq i \leq s$.

Παράδειγμα 4.1.8. Η κυκλική ομάδα $(C_6 = \langle x \rangle, \star)$ τάξης 6 είναι το εσωτερικό ευθύ γινόμενο των κυκλικών υποομάδων $C_2 = \langle x^3 \rangle$ και $C_3 = \langle x^2 \rangle$ των οποίων οι τάξεις είναι 2 και 3 αντιστοίχως.

Προφανώς $C_2 \trianglelefteq C_6$ και $C_3 \trianglelefteq C_6$. Για τα στοιχεία τής C_6 έχουμε:

$$\begin{array}{lll} e_{C_6} = e_{C_6} \star e_{C_6}, & x = x^3 \star (x^2)^2, & x^2 = e_{C_6} \star x^2, \\ x^3 = x^3 \star e_{C_6}, & x^4 = e_{C_6} \star x^4, & x^5 = x^3 \star x^2. \end{array} \tag{*}$$

Συνεπώς, $C_6 = \langle x^3 \rangle \cdot \langle x^2 \rangle$. Υπολείπεται η απόδειξη ότι τα ανωτέρω γινόμενα (*) είναι μοναδικά ως γινόμενα, όπου ο πρώτος παράγοντας ανήκει στην C_2 και ο δεύτερος στην C_3. Όμως αυτό διαπιστώνεται αμέσως λαμβάνοντας υπ' όψιν την αμέσως πρόταση.

Πρόταση 4.1.9. *Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι $G_i \trianglelefteq G, 1 \leq i \leq s$ είναι ορθόθετες υποομάδες τής G με $G = G_1 \cdot G_2 \cdot \ldots \cdot G_s$.*

Η ομάδα G είναι το εσωτερικό ευθύ γινόμενο των $G_1, G_2, \ldots, G_s$, αν και μόνο αν, $\forall i, 2 \leq i \leq s, (G_1 \cdot G_2 \cdot \cdots \cdot G_{i-1}) \bigcap G_i = \{e_G\}$.

Απόδειξη. «$\Leftarrow$» Σύμφωνα με τον ορισμό τού ευθέος γινομένου, υπολείπεται η απόδειξη τής μοναδικότητας τής παράστασης κάθε στοιχείου τής G ως γινόμενο στοιχείων από τις υποομάδες $G_1, G_2, \ldots, G_s$.
Έστω ότι $g = g_1 g_2 \ldots g_s = h_1 h_2 \ldots h_s (*)$, όπου $\forall i, 1 \leq i \leq s, g_i, h_i \in G_i$. Τότε $g_s h_s^{-1} = (g_1 g_2 \ldots g_{s-1})^{-1} (h_1 h_2 \ldots h_{s-1})$.
Αλλά $g_s h_s^{-1} \in G_s$ και $(g_1 g_2 \ldots g_{s-1})^{-1} (h_1 h_2 \ldots h_{s-1}) \in G_1 \cdot G_2 \cdot \ldots \cdot G_{s-1}$. Επομένως, $g_s h_s^{-1} \in (G_1 \cdot G_2 \cdot \ldots \cdot G_{s-1}) \bigcap G_s = \{e_G\}$ και γι' αυτό $g_s = h_s$. Τώρα η σχέση $(*)$ παίρνει τη μορφή $g = g_1 g_2 \ldots g_{s-1} = h_1 h_2 \ldots h_{s-1}$ από όπου, ακριβώς όπως προηγουμένως, συμπεραίνουμε ότι $g_{s-1} h_{s-1}^{-1} = e_G$, δηλαδή $g_{s-1} = h_{s-1}$. Συνεχίζοντας έτσι καταλήγουμε ότι $g_s = h_s, g_{s-1} = h_{s-1}, \ldots, g_2 = h_2, g_1 = h_1$.
«$\Rightarrow$» Έστω ότι α είναι ένα στοιχείο τής G, το οποίο ανήκει στην τομή $(G_1 \cdot G_2 \cdot \ldots \cdot G_{i-1}) \bigcap G_i$.
Τότε $\alpha = g_1 g_2 \ldots g_{i-1}$ με $g_j \in G_j, j = 1, 2, \ldots i-1$ και $\alpha \in G_i$.
Τότε $e_G = g_1 g_2 \ldots g_{i-1} \alpha^{-1} g_{i+1} \ldots g_s$, όπου $\forall j, i+1 \leq j \leq s, g_j = e_G$ και όπου $\alpha^{-1} \in G_i$.

Όμως η μοναδική παράσταση τού e_G ως γινόμενο στοιχείων $g_i \in G_i, i = 1, 2, \ldots, s$ είναι η τετριμμένη $e_G = e_G \ldots e_G$. Επομένως, $\alpha^{-1} = e_G = \alpha$. □

Επιστρέφοντας στο Παράδειγμα 4.1.8, διαπιστώνουμε τώρα ότι η C_6 είναι το εσωτερικό ευθύ γινόμενο των δύο κυκλικών υποομάδων της C_2 και C_3, αφού $C_2 \bigcap C_3 = \{e_{C_6}\}$

Πόρισμα 4.1.10. *Έστω ότι μια ομάδα $(G, \star)$ είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της $G_1, G_2, \ldots, G_s$. Τότε $\forall g_i \in G_i, g_j \in G_j$ με $i \neq j, 1 \leq i, j \leq s$ είναι $g_i g_j = g_j g_i$.*

Απόδειξη. Παρατηρούμε ότι το στοιχείο $g_i g_j g_i^{-1} g_j^{-1}$ ανήκει στην τομή $G_i \bigcap G_j = \{e_G\}$, επειδή $g_i g_j g_i^{-1} \in G_j$ και $g_j g_i^{-1} g_j^{-1} \in G_i$, αφού $G_i \trianglelefteq G$ και $G_j \trianglelefteq G$. Επομένως, $g_i g_j g_i^{-1} g_j^{-1} = e_G$, δηλαδή $g_i g_j = g_j g_i$. □

Στο σημείο αυτό θα παρουσιάσουμε ένα σημαντικό λήμμα που θα χρησιμοποιήσουμε αμέσως, αλλά και αργότερα κατά τη μελέτη των μηδενοδύναμων ομάδων, βλ. Θεώρημα 6.3.13.

Λήμμα 4.1.11. *Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα. Όταν για κάθε πρώτο διαιρέτη p τής τάξης τής ομάδας, υπάρχει ακριβώς μία p–Sylow υποομάδα, τότε η G είναι το εσωτερικό ευθύ γινόμενο των Sylow υποομάδων της.*

Απόδειξη. Έστω $P_1, P_2, \ldots, P_s$ οι Sylow υποομάδες τής G, που αντιστοιχούν στους διαφορετικούς πρώτους διαιρέτες $p_1, p_2, \ldots, p_s$ τής τάξης τής G. Θα δείξουμε ότι οι $P_1, P_2, \ldots, P_s$ ικανοποιούν τις υποθέσεις τής Πρότασης 4.1.9.

Αφού οι Sylow υποομάδες που αντιστοιχούν στον ίδιο πρώτο αριθμό είναι πάντοτε συζυγείς, συμπεραίνουμε από την υπόθεση τής εφαρμογής ότι οι P_i είναι ορθόθετες υποομάδες τής G, $\forall i, 1 \leq i \leq s$.

Τώρα θα αποδείξουμε ότι $\forall i, 2 \leq i \leq s$ είναι $(P_1 \cdot P_2 \cdot \cdots \cdot P_{i-1}) \bigcap P_i = \{e_G\}$ και ότι $|P_1 \cdot P_2 \cdot \ldots \cdot P_i| = |P_1||P_2| \ldots |P_i|$.
Πράγματι, $P_1 \bigcap P_2 = \{e_G\}$, αφού οι τάξεις $|P_1|$ και $|P_2|$ είναι σχετικώς πρώτοι αριθμοί. Επιπλέον, $|P_1 \cdot P_2| = |P_1||P_2|$, αφού $|P_1 \cdot P_2| = |P_1||P_2|/|P_1 \bigcap P_2|$.
Τώρα, $(P_1 \cdot P_2) \bigcap P_3 = \{e_G\}$, αφού οι τάξεις $|P_1 \cdot P_2|$ και $|P_3|$ είναι σχετικώς πρώτοι αριθμοί. Επομένως, $|P_1 \cdot P_2 \cdot P_3| = |P_1||P_2||P_3|$, αφού $|(P_1 \cdot P_2) \cdot P_3| = |P_1 \cdot P_2||P_3|/|(P_1 \cdot P_2) \bigcap P_3|$.

Υποθέτοντας ότι $(P_1 \cdot P_2 \cdot \cdots \cdot P_{i-1}) \bigcap P_i = \{e_G\}$ και ότι $|P_1 \cdot P_2 \cdot \ldots \cdot P_i| = |P_1||P_2| \ldots |P_i|$, θα δείξουμε ότι

$$(P_1 \cdot P_2 \cdot \cdots \cdot P_i) \bigcap P_{i+1} = \{e_G\} \tag{*}$$

και ότι

$$|P_1 \cdot P_2 \cdot \ldots \cdot P_{i+1}| = |P_1||P_2| \ldots |P_{i+1}|. \tag{**}$$

Πράγματι, η (*) είναι αληθής, αφού οι τάξεις $|P_1 \cdot P_2 \cdot \ldots \cdot P_i| = |P_1||P_2| \ldots |P_i|$ και $|P_{i+1}|$ είναι σχετικώς πρώτοι αριθμοί. Επιπλέον, η (**) είναι αληθής, αφού

$$|(P_1 \cdot P_2 \cdot \ldots \cdot P_i) \cdot P_{i+1}| = \frac{|P_1 \cdot P_2 \cdot \ldots \cdot P_i||P_{i+1}|}{|(P_1 \cdot P_2 \cdot \cdots \cdot P_i) \bigcap P_{i+1}|} = \frac{|P_1||P_2| \ldots |P_i||P_{i+1}|}{1}.$$

Τέλος, η G ισούται με την υποομάδα $P_1 \cdot P_2 \cdot \ldots \cdot P_{s-1} \cdot P_s$, αφού η τάξη τής τελευταίας ισούται με $|P_1||P_2| \ldots |P_{s-1}||P_s|$ που είναι ακριβώς η τάξη τής G.
Επομένως, η G είναι το εσωτερικό ευθύ γινόμενο των $P_1, P_2, \ldots, P_s$. □

Πρόταση 4.1.12. *Κάθε πεπερασμένη αβελιανή ομάδα $(G, \star)$ είναι το εσωτερικό ευθύ γινόμενο των Sylow υποομάδων της.*

Απόδειξη. Σε κάθε πρώτο διαιρέτη p τής τάξης τής G, η αντίστοιχη p–Sylow υποομάδα είναι ορθόθετη, αφού η G είναι αβελιανή, και ως εκ τούτου μοναδική. Επομένως, το συμπέρασμα τού θεωρήματος είναι άμεση συνέπεια τού Λήμματος 4.1.11. □

4.1.3 Σχέση εξωτερικού και εσωτερικού ευθέος Γινομένου

Πρόταση 4.1.13. *Μια ομάδα $(G, \star)$ είναι ισόμορφη προς το εξωτερικό ευθύ γινόμενο $(\prod_{i=1}^{s} G_i, \cdot)$ των ομάδων $(G_i, \star_i), i = 1, 2, \ldots, s, s \geq 2$, αν και μόνο αν, υπάρχουν ορθόθετες υποομάδες $N_i \trianglelefteq G$ τής G, όπου για κάθε $i, 1 \leq i \leq s$, η υποομάδα N_i είναι ισόμορφη προς την G_i έτσι, ώστε η G να ισούται με το εσωτερικό ευθύ γινόμενο των $N_i, 1 \leq i \leq s$.*

(*Για να γίνει πιο εύληπτη η απόδειξη θα αναγράφουμε την πράξη «$\cdot$» τού ευθέος γινομένου $\prod_{i=1}^{s} G_i$ και την πράξη «$\star$» τής ομάδας G.*)

Απόδειξη. «$\Rightarrow$» Κατ' αρχάς θεωρούμε το ευθύ γινόμενο $\prod_{i=1}^{s} G_i$ και για κάθε $i, 1 \leq i \leq s$ το σύνολο $M_i = \{e_{G_1}\} \times \{e_{G_2}\} \times \cdots \times \{e_{G_{i-1}}\} \times G_i \times \{e_{G_{i+1}}\} \times \cdots \times \{e_{G_s}\}$. Κάθε $M_i, 1 \leq i \leq s$ είναι μια ορθόθετη υποομάδα τού ευθέος γινομένου $\prod_{i=1}^{s} G_i$, η οποία είναι ισόμορφη προς την G_i. (*Απλή άσκηση για τον αναγνώστη!*) Επίσης εύκολα διαπιστώνεται ότι $\prod_{i=1}^{s} G_i = M_1 \cdot M_2 \cdot \ldots \cdot M_s, (*)$, διότι $\forall \alpha = (g_1, g_2, \ldots, g_s) \in \prod_{i=1}^{s} G_i$, είναι

$$\alpha = (g_1, e_{G_2}, \ldots, e_{G_{i-1}}, e_{G_i}, e_{G_{i+1}}, \ldots, e_{G_s}) \cdot \ldots \cdot$$
$$(e_{G_1}, e_{G_2}, \ldots, e_{G_{i-1}}, g_i, e_{G_{i+1}}, \ldots, e_{G_s}) \cdot \ldots \cdot (e_{G_1}, e_{G_2}, \ldots, e_{G_{i-1}}, e_{G_i}, e_{G_{i+1}}, \ldots, g_s),$$

όπου $\forall i, 1 \leq i \leq s$, το $m_i = (e_{G_1}, e_{G_2}, \ldots, e_{G_{i-1}}, g_i, e_{G_{i+1}}, \ldots, e_{G_s}) \in M_i$.
Από την υπόθεση υπάρχει ένας ισομορφισμός $\sigma : G \to \prod_{i=1}^{s} G_i$. Για κάθε $i, 1 \leq i \leq s$, θεωρούμε την αντίστροφη εικόνα $N_i = \sigma^{-1}(M_i)$. Επειδή ο σ είναι ισομορφισμός, κάθε $N_i, 1 \leq i \leq s$ είναι μια ορθόθετη υποομάδα τής G με $N_i \cong G_i$, διότι $N_i \cong M_i$ και $M_i \cong G_i$.
Παρατηρούμε ότι λόγω τής $(*)$ είναι $G = N_1 \star N_2 \star \cdots \star N_i \star \cdots \star N_s$.
Για να δείξουμε ότι η G είναι το εσωτερικό ευθύ γινόμενο των N_i υπολείπεται η απόδειξη ότι $\forall i, 2 \leq i \leq s$, έχουμε $(N_1 \star N_2 \star \cdots \star N_{i-1}) \bigcap N_i = \{e_G\}$. Όταν $\alpha \in (N_1 \star N_2 \star \cdots \star N_{i-1}) \bigcap N_i$, τότε $\sigma(\alpha) \in M_1 \cdot M_2 \cdot \ldots \cdot M_{i-1}$ και $\sigma(\alpha) \in M_i$. Ως εκ τούτου, υπάρχουν $g_j \in G_j, 1 \leq j \leq i$ με $\sigma(\alpha) = (g_1, g_2, \ldots, g_{i-1}, e_{G_i}, \ldots, e_{G_s})$ και $\sigma(\alpha) = (e_{G_1}, e_{G_2}, \ldots, e_{G_{i-1}}, g_i, \ldots, e_{G_s})$. Αλλά τότε $g_j = e_{G_j}, \forall j, 1 \leq j \leq i$ και γι' αυτό το $\sigma(\alpha)$ ισούται με το ουδέτερο στοιχείο τού ευθέος γινομένου $\prod_{i=1}^{s} G_i$. Αφού όμως ο σ είναι ισομορφισμός, συμπεραίνουμε ότι $\alpha = e_G$.
«$\Leftarrow$» Έστω ότι η G ισούται με το εσωτερικό ευθύ γινόμενο $G = N_1 \star N_2 \star \ldots \star N_s$ των ορθόθετων υποομάδων της $N_i \trianglelefteq G, 1 \leq i \leq s$. Θεωρούμε το εξωτερικό ευθύ γινόμενο $(\prod_{i=1}^{s} N_i, \cdot)$ των N_i και την απεικόνιση

$$\tau : \prod_{i=1}^{s} N_i \to G = N_1 \star N_2 \star \ldots \star N_s, (n_1, n_2, \ldots, n_s) \mapsto n_1 \star n_2 \star \cdots \star n_s.$$

Παρατηρούμε ότι η τ είναι ένας ομομορφισμός ομάδων, αφού

$$\tau\left((n_1, n_2, \ldots, n_s)\cdot(n_1', n_2', \ldots, n_s')\right) = \tau\left((n_1 \star n_1', n_2'\star, \ldots, n_s \star n_s')\right) =$$
$$(n_1 \star n_1') \star (n_2 \star n_2') \star \cdots \star (n_s \star n_s') = (n_1 \star n_2 \star \cdots \star n_s) \star (n_1' \star n_2' \star \cdots \star n_s') =$$
$$\tau\left((n_1, n_2, \ldots, n_s)\right) \cdot \tau\left((n_1', n_2', \ldots, n_s')\right),$$

διότι $n_i \star n_j' = n_j' \star n_i, \forall i, j, i \neq j, 1 \leq i, j \leq n$, βλ. Πόρισμα 4.1.10. Προφανώς ο τ είναι ένας επιμορφισμός. Επιπλέον αν, $(n_1, n_2, \ldots, n_s) \in \ker \tau$, τότε $n_1 \star n_2 \star \cdots \star n_s = e_G$. Αλλά αφού η $G = N_1 \star N_2 \star \ldots \star N_s$ είναι το εσωτερικό γινόμενο των $N_i, 1 \leq i \leq n$, η παράσταση τού e_G ως γινόμενο στοιχείων $n_i \in N_i, 1 \leq i \leq n$ είναι μοναδική και γι' αυτό $n_i = e_G, \forall i, 1 \leq i \leq s$. Επομένως, $\ker \tau = \{(e_{G_1}, e_{G_2}, \ldots, e_{G_2})\}$ και ο επιμορφισμός σ είναι ένας ισομορφισμός. □

Παράδειγμα 4.1.14. Η διεδρική ομάδα $(D_4, \circ)$ των στερεών κινήσεων τού τετραγώνου δεν ισούται με ένα εσωτερικό ευθύ γινόμενο δύο γνησίων υποομάδων της. Πράγματι, οι γνήσιες υποομάδες τής D_4 έχουν τάξη 1, 2 ή 4. Αν ήταν η D_4 το εσωτερικό ευθύ γινόμενο δύο υποομάδων της, τότε θα ήταν και η ίδια αβελιανή. Πράγμα άτοπο, αφού η D_4 δεν είναι αβελιανή.

Παράδειγμα 4.1.15. Έστω ότι $(S_n, \circ)$ είναι η συμμετρική ομάδα των αμφιμονοσήμαντων, δηλαδή των «1–1» και «επί», απεικονίσεων από το σύνολο $N = \{1, 2, \ldots, n\}$ στον εαυτό του και ότι I είναι ένα γνήσιο μη κενό υποσύνολο τού N.

Έστω G το υποσύνολο τής S_n που αποτελείται από τα $\sigma \in S_n$ με $\sigma(I) = I$, δηλαδή από τα στοιχεία τής S_n που απεικονίζουν το υποσύνολο I στον εαυτό του.
Προτείνουμε στον αναγνώστη να αποδείξει ότι το σύνολο G είναι μια υποομάδα τής S_n.
Έστω ότι J είναι το συνολοθεωρητικό συμπλήρωμα το I ως προς N, δηλαδή $J = N \setminus I$. Παρατηρούμε ότι τα στοιχεία σ τής G διατηρούν το υποσύνολο J, δηλαδή $\sigma(J) = J$, επειδή αυτά διατηρούν το I και επειδή το N είναι μια αποσυνδετή[2] ένωση των υποσυνόλων I και J.
Θεωρούμε το υποσύνολο H (αντιστοίχως K) τής G που αποτελείται από τα $\sigma \in G$ (αντιστοίχως $\tau \in G$) που διατηρούν σημειακά το I (αντιστοίχως σημειακά το J), δηλαδή $\sigma \in H \Leftrightarrow \forall i \in I, \sigma(i) = i$ (αντιστοίχως $\tau \in K \Leftrightarrow \forall j \in J, \tau(j) = j$).
Προτείνουμε στον αναγνώστη να αποδείξει ότι τα υποσύνολα I και J είναι υποομάδες τής G. Πρόκειται μάλιστα για ορθόθετες υποομάδες τής G, αφού είναι πυρήνες των δράσεων τής G επί των συνόλων I και J, βλ. Ορισμό 2.1.7.

Ισχυριζόμαστε ότι η G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της H και K. Παρατηρούμε ότι $H \bigcap K = \{\mathrm{Id}_n\}$, αφού αν, $\sigma \in H \bigcap K$, τότε $\sigma(\alpha) = \alpha, \forall \alpha \in I \bigcup J = N$. Αν αποδείξουμε τώρα ότι κάθε $\sigma \in G$ είναι σύνθεση ενός στοιχείου από την H με ένα στοιχείο από την K, τότε από την Πρόταση 4.1.13, θα προκύψει ότι η G είναι το εσωτερικό ευθύ γινόμενο των H και K.

Έστω $\sigma \in G$ και μια ανάλυσή του $\sigma = c_1 \circ \cdots \circ c_t$ σε αποσυνδετούς κύκλους. Παρατηρούμε ότι κάθε κύκλος $c_\ell, \ell = 1, \ldots, t$ περιέχει ή μόνο στοιχεία από το I ή μόνο στοιχεία από το J αφού αν, σε κάποιον c_ℓ υπήρχαν στοιχεία και από το I και από το J, τότε το σ

[2] Η τομή $I \bigcap J = \emptyset$.

δεν θα σταθεροποιούσε το σύνολο I, πράγμα άτοπο αφού το σ είναι στοιχείο τής G. Γι' αυτό σχηματίζοντας το γινόμενο σ_I (αντιστοίχως σ_J) των κύκλων τού σ που δεν περιέχουν στοιχεία από το I (αντιστοίχως που δεν περιέχουν στοιχεία από το J), διαπιστώνουμε ότι το σ_I ανήκει στο H και το σ_J ανήκει στο K και $\sigma = \sigma_I \circ \sigma_J$.

Ώστε η G είναι το εσωτερικό ευθύ γινόμενο των H και K και $[G : 1] = [H : 1][K : 1]$. Προφανώς, η H (αντιστοίχως η K) είναι ισόμορφη προς τη συμμετρική ομάδα S_J τού συνόλου J (αντιστοίχως με τη συμμετρική ομάδα S_I τού συνόλου I) και γι' αυτό $G \cong S_J \times S_I$ και $[G : 1] = (n - m)!m!$, όπου m είναι το πλήθος των στοιχείων τού συνόλου I.

4.2 Η Ταξινόμηση των πεπερασμένων αβελιανών Ομάδων

Έστω ότι $(G, \star)$ είναι μια αβελιανή ομάδα τάξης $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, όπου οι αριθμοί $p_i, 1 \leq i \leq s$ είναι ανά δύο διαφορετικοί πρώτοι και οι $\alpha_i, 1 \leq i \leq s$, είναι φυσικοί.

Από την Πρόταση 4.1.12 γνωρίζουμε ότι η G ισούται με το εσωτερικό ευθύ γινόμενο $P_1 \cdot P_2 \cdot \ldots \cdot P_s$ των p_i–Sylow υποομάδων της $P_i, 1 \leq i \leq s$, που έχουν αντίστοιχες τάξεις $|P_i| = p_i^{\alpha_i}, 1 \leq i \leq s$ και γι' αυτό, βλ. Πρόταση 4.1.13, η G είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο p–ομάδων $\mathcal{P}_1 \times \mathcal{P}_2 \times \cdots \times \mathcal{P}_s$, όπου $|\mathcal{P}_i| = p_i^{\alpha_i}, 1 \leq i \leq s$. Οι $\mathcal{P}_i$ είναι αβελιανές p–ομάδες και για κάθε $i, 1 \leq i \leq s$, η $\mathcal{P}_i$ είναι ισόμορφη προς την αντίστοιχη p_i–Sylow υποομάδα P_i.

Παρατηρούμε ότι αν, $\sigma : \mathcal{Q}_1 \times \mathcal{Q}_2 \times \cdots \times \mathcal{Q}_t \to G$ είναι ένας ισομορφισμός από ένα εξωτερικό ευθύ γινόμενο p–ομάδων $\mathcal{Q}_1 \times \mathcal{Q}_2 \times \cdots \times \mathcal{Q}_t$ στην G με $|\mathcal{Q}_j| = q_j^{\beta_j}, 1 \leq j \leq t$, όπου οι αριθμοί $q_j, 1 \leq j \leq t$ είναι ανά δύο διαφορετικοί πρώτοι και οι $\beta_j, 1 \leq j \leq t$ είναι φυσικοί, τότε από τη μοναδικότητα τής ανάλυσης τής τάξης n τής G σε γινόμενο δυνάμεων πρώτων αριθμών, προκύπτει ότι $s = t$ και κατόπιν ότι υπάρχει μια μετάταξη $\tau \in S_s$, ούτως ώστε $\forall i, 1 \leq i \leq s$ η τάξη τής $\mathcal{Q}_{\tau(i)}$ να ισούται με την τάξη τής αντίστοιχης p_i–Sylow υποομάδας P_i. Επομένως, η εικόνα τής $\mathcal{Q}_{\tau(i)}$, μέσω τού ισομορφισμού σ, είναι μια p_i–Sylow υποομάδα τής G και γι' αυτό συμπίπτει με την P_i. Ώστε, για κάθε $i, 1 \leq i \leq s$, η $\mathcal{Q}_{\tau(i)}$ είναι ισόμορφη προς την p_i–Sylow υποομάδα P_i και ως εκ τούτου και με την αντίστοιχη p–ομάδα $\mathcal{P}_i$ τάξης $p_i^{\alpha_i}$.

Έτσι προκύπτει η

Πρόταση 4.2.1. *Έστω ότι $(G, \star)$ είναι μια αβελιανή ομάδα τάξης $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, όπου οι αριθμοί $p_i, 1 \leq i \leq s$ είναι πρώτοι, διαφορετικοί ανά δύο, και οι αριθμοί $\alpha_i, 1 \leq i \leq s$, είναι φυσικοί. Τότε υπάρχει ένας ισομορφισμός ομάδων*

$$\sigma : G \to \mathcal{P}_1 \times \mathcal{P}_2 \times \cdots \times \mathcal{P}_s,$$

όπου $\forall i, 1 \leq i \leq s, |\mathcal{P}_i| = p_i^{\alpha_i}$.

Επιπλέον, αν η G είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο p–ομάδων $\mathcal{Q}_1 \times \mathcal{Q}_2 \times \cdots \times \mathcal{Q}_t$, τότε $s = t$ και υπάρχει μια μετάταξη $\tau \in S_s$, ούτως ώστε $\forall i, 1 \leq i \leq s$, $\mathcal{Q}_{\tau(i)} \cong \mathcal{P}_i$.

Με άλλα λόγια μια πεπερασμένη αβελιανή ομάδα G είναι «με ακρίβεια μετάταξης» κατά μοναδικό τρόπο ισόμορφη προς ένα ευθύ γινόμενο πεπερασμένων αβελιανών p–ομάδων.

Τώρα θα αποδείξουμε ότι και οι p–ομάδες είναι ισόμορφες προς ευθέα γινόμενα κυκλικών ομάδων.

Λήμμα 4.2.2. *Έστω ότι p είναι ένας πρώτος αριθμός και ότι $(G, \star)$ είναι μια πεπερασμένη αβελιανή p–ομάδα. Η G είναι κυκλική ομάδα, αν και μόνο αν, διαθέτει ακριβώς μία κυκλική υποομάδα τάξης p.*

Απόδειξη. «$\Rightarrow$». Προφανώς, αν η G είναι κυκλική, τότε σε κάθε διαιρέτη τής τάξης της διαθέτει ακριβώς μία κυκλική υποομάδα, επομένως αυτό συμβαίνει και για τον διαιρέτη p.

«$\Leftarrow$» Η απόδειξη θα γίνει με επαγωγή ως προς την τάξη p^m τής ομάδας G. Πριν προχωρήσουμε υπενθυμίζουμε, βλ. Πρόταση 3.1.3, ότι για κάθε $p^n, n \leq m$, η G διαθέτει υποομάδα τάξης p^n. Ιδιαιτέρως, η G διαθέτει πάντοτε τουλάχιστον μία υποομάδα τάξης p, γεγονός που έπεται και από το Θεώρημα Cauchy, σελ. 184.
Για $m = 1$, η ομάδα G είναι πρώτης τάξης p και ως εκ τούτου κυκλική. Έστω ότι ο ισχυρισμός είναι αληθής για τις ομάδες τάξης p^k, θα αποδείξουμε ότι αυτός είναι αληθής και για κάθε ομάδα G τάξης p^{k+1}.

Ας είναι C_p η μοναδική κυκλική υποομάδα τάξης p τής G. Θεωρούμε τον ενδομορφισμό $\varphi : G \to G, g \mapsto \varphi(g) = g^p$. Προφανώς, $C_p \leq \ker\varphi$. Κάθε $g \in \ker\varphi, g \neq e_G$ παράγει μια υποομάδα $\langle g \rangle$ τής G τάξης p. Επομένως, $\langle g \rangle = C_p$ και γι' αυτό $g \in C_p$. Ώστε, $\ker\varphi = C_p$.
Η πηλικοομάδα G/C_p είναι τάξης p^k και γι' αυτό διαθέτει τουλάχιστον μία υποομάδα $\mathcal{S}$ τάξης p. Ισχυριζόμαστε ότι η $\mathcal{S}$ είναι η μοναδική κυκλική υποομάδα τής G/C_p τάξης p. Πράγματι, αν οι $\mathcal{S}_1$ και $\mathcal{S}_2$ ήταν δύο διαφορετικές κυκλικές υποομάδες τής G/C_p τάξης p, τότε και η $\varphi(G)$ θα διέθετε δύο διαφορετικές κυκλικές υποομάδες τάξης p, αφού $\varphi(G) \cong G/\ker\varphi = G/C_p$. Τότε όμως θα διέθετε και η G δύο διαφορετικές κυκλικές υποομάδες τάξης p, πράγμα άτοπο. Επειδή τώρα η G/C_p είναι τάξης p^k και διαθέτει ακριβώς μία κυκλική υποομάδα τάξης p, μπορούμε να εφαρμόσουμε την επαγωγική υπόθεσή μας και να συμπεράνουμε ότι η G/C_p είναι κυκλική. Ώστε, $G/C_p = \langle aC_p \rangle, a \in G$.
Ισχυριζόμαστε ότι $\langle a \rangle = G$. Πράγματι, αν $g \in G$, τότε $gC_p = a^n C_p, n \in \mathbb{N} \bigcup \{0\}$ και επομένως $g^{-1}a^n = c \in C_p$ (*). Αλλά $C_p \leq \langle a \rangle$, αφού η $\langle a \rangle \leq G$ ως p–ομάδα διαθέτει κυκλικές υποομάδες τάξης p, οι οποίες είναι και κυκλικές υποομάδες τάξης p τής G. Άρα η μοναδική κυκλική υποομάδα τάξης p τής $\langle a \rangle$ είναι η C_p. Ώστε, το c στη σχέση (*) είναι στοιχείο τής $\langle a \rangle$. Έστω ότι $c = a^s, s \in \mathbb{N} \bigcup \{0\}$. Τώρα, η (*) γράφεται $g^{-1}a^n = a^s$ και επομένως, $g = a^{n-s}$, δηλαδή $G \leq \langle a \rangle$ και γι' αυτό $G = \langle a \rangle$. □

Λήμμα 4.2.3. *Έστω $(G, \star)$ μια αβελιανή p–ομάδα. Όταν $K \leq G$ είναι μια μέγιστης τάξης κυκλική υποομάδα της, τότε υπάρχει μια υποομάδα G' τής G, τέτοια ώστε η G να είναι το εσωτερικό ευθύ γινόμενο των K και G'.*

Απόδειξη. Θα εκτελέσουμε την απόδειξη με επαγωγή ως προς την τάξη p^m τής G.

Για $m = 1$, η ομάδα G είναι πρώτης τάξης p και ως εκ τούτου κυκλική. Προφανώς, η G είναι το εσωτερικό ευθύ γινόμενο των $K = G$ και $G' = \{e_G\}$.

Έστω ότι ο ισχυρισμός είναι αληθής για τις ομάδες τάξης p^k, θα αποδείξουμε ότι είναι αληθής και για κάθε ομάδα G τάξης p^{k+1}.

Αν η G είναι κυκλική, τότε η G είναι το εσωτερικό ευθύ γινόμενο των $K = G$ και $G' = \{e_G\}$.

Αν η G δεν είναι κυκλική, τότε θεωρούμε μια μέγιστης τάξης κυκλική υποομάδα $\langle a\rangle = K < G$. Προφανώς, η K διαθέτει μια μοναδική κυκλική υποομάδα K_p τάξης p. Επειδή η G δεν είναι κυκλική, περιέχει τουλάχιστον ακόμα μία κυκλική υποομάδα $C_p \neq K_p$ τάξης p, βλ. Λήμμα 4.2.2. Αφού $K_p \bigcap C_p = \{e_G\}$, συμπεραίνουμε ότι $K \bigcap C_p = \{e_G\}$.

Θεωρούμε την πηλικοομάδα G/C_p και την υποομάδα της $(K \cdot C_p)/C_p$. Παρατηρούμε ότι

$$[(K \cdot C_p)/C_p : 1] = \frac{[K \cdot C_p : 1]}{[C_p : 1]} = \frac{[K : 1][C_p : 1]}{[C_p : 1]} = [K : 1] \tag{1}$$

αφού

$$[K \cdot C_p : 1] = \frac{[K : 1][C_p : 1]}{[K \bigcap C_p : 1]} = [K : 1][C_p : 1]$$

και επειδή $[K \bigcap C_p : 1] = 1$, διότι $K \bigcap C_p = \{e_G\}$.

Επειδή, $\forall b \in K, \forall c \in C_p$, είναι $(bc)C_p = bC_p$, διαπιστώνουμε ότι η $(K \cdot C_p)/C_p$ είναι κυκλική, εφόσον παράγεται από το στοιχείο aC_p.

Λόγω τής (1), η τάξη $\circ(aC_p)$ τού στοιχείου aC_p είναι:

$$\circ(aC_p) = [(K \cdot C_p)/C_p : 1] = [K : 1] = \circ(a).$$

Επομένως, η $(K \cdot C_p)/C_p$ είναι μια μέγιστης τάξης κυκλική υποομάδα τής G/C_p, αφού $\forall gC_p \in G/C_p$ είναι $\circ(gC_p) \leq \circ(g)$.

Η G/C_p είναι μια p–ομάδα τάξης p^k. Γι' αυτό, χρησιμοποιώντας τη μέγιστης τάξης κυκλική υποομάδα της $(K \cdot C_p)/C_p$, συμπεραίνουμε με τη βοήθεια τής επαγωγικής υπόθεσης, ότι υπάρχει μια υποομάδα $L = G'/C_p$ τής G/C_p, όπου η G' είναι μια υποομάδα τής G με $C_p \leq G'$, έτσι ώστε η G/C_p να είναι το εσωτερικό ευθύ γινόμενο των $(K \cdot C_p)/C_p$ και G'/C_p. Δηλαδή, $G/C_p = \big((K \cdot C_p)/C_p) \cdot (G'/C_p)\big)$ και $((K \cdot C_p)/C_p) \bigcap (G'/C_p) = \{C_p\}$.

Ισχυριζόμαστε ότι η G είναι το εσωτερικό ευθύ γινόμενο των K και G'.

Αν $g \in K \bigcap G'$, τότε $gC_p \in ((K \cdot C_p)/C_p) \bigcap (G'/C_p) = \{C_p\}$. Συνεπώς, $gC_p = C_p$ και $g \in C_p$. Αλλά τότε $g \in K \bigcap C_p = \{e_G\}$. Ώστε $g = e_G$ και $K \bigcap G' = \{e_G\}$.

Υπολείπεται η απόδειξη ότι $G = K \cdot G'$ και επειδή η G είναι μια πεπερασμένη ομάδα, αρκεί να δείξουμε ότι $[K \cdot G' : 1] = [G : 1]$. Αλλά $[K \bigcap G' : 1] = 1$, αφού $K \bigcap G' = \{e_G\}$ και γι' αυτό

$$[(K \cdot G') : 1] = \frac{[K : 1][G' : 1]}{[K \bigcap G' : 1]} = [K : 1][G' : 1].$$

Συνεπώς, αρκεί να δείξουμε ότι $[G : 1] = [K : 1][G' : 1]$.

Επειδή, η G/C_p είναι το εσωτερικό ευθύ γινόμενο των $(K \cdot C_p)/C_p$ και G'/C_p, έχουμε

$$[G/C_p : 1] = [(K \cdot C_p)/C_p : 1][G'/C_p : 1] = [(K \cdot C_p)/C_p : 1]\frac{[G' : 1]}{[C_p : 1]}. \tag{2}$$

Τώρα χρησιμοποιώντας την (1), η (2) γίνεται

$$[G/C_p : 1] = [K : 1]\frac{[G' : 1]}{[C_p : 1]}. \tag{3}$$

Έτσι, λόγω τής (3), έπεται

$$[G:1] = [G/C_p:1][C_p:1] = [K:1]\frac{[G':1]}{[C_p:1]}[C_p:1] = [K:1][G':1].$$

Αυτό ακριβώς που θέλαμε να αποδείξουμε. □

Πρόταση 4.2.4. (α′) *Κάθε πεπερασμένη αβελιανή p–ομάδα $(G,\star)$ είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο κυκλικών ομάδων $\mathcal{K}_1 \times \mathcal{K}_2 \times \cdots \times \mathcal{K}_s$.*

(β′) *Επιπλέον αν στο ως άνω ευθύ γινόμενο οι κυκλικές ομάδες $\mathcal{K}_i, 1 \leq i \leq s$ είναι διατεταγμένες κατά διάταξη αντίστροφη των τάξεών τους, δηλαδή $i \leq j$, αν και μόνο αν, $[\mathcal{K}_i : 1] \geq [\mathcal{K}_j : 1]$ και αν η $(G,\star)$ είναι ισόμορφη προς ένα ακόμη εξωτερικό ευθύ γινόμενο κυκλικών ομάδων $\mathcal{H}_1 \times \mathcal{H}_2 \times \cdots \times \mathcal{H}_t$, οι οποίες είναι επίσης διατεταγμένες στο συγκεκριμένο ευθύ γινόμενο κατά διάταξη αντίστροφη των τάξεών τους, δηλαδή $i \leq j$ αν και μόνο αν, $[\mathcal{H}_i : 1] \geq [\mathcal{H}_j : 1]$, τότε $s = t$ και $\forall i, 1 \leq i \leq s, \mathcal{K}_i \cong \mathcal{H}_i$.*

Απόδειξη. Θα αποδείξουμε και τα δύο μέρη τής πρότασης με επαγωγή ως προς την τάξη p^m τής G.

(α′) Για $m = 1$, η ομάδα G είναι πρώτης τάξης p και ως εκ τούτου κυκλική. Έστω ότι ο ισχυρισμός είναι αληθής για κάθε ομάδα τάξης $\leq p^k$, θα αποδείξουμε ότι είναι αληθής και για κάθε ομάδα τάξης p^{k+1}.

Έστω G μια ομάδα τάξης p^{k+1}. Αν η G είναι κυκλική, τότε δεν χρειάζεται να αποδείξουμε κάτι. Αν η G δεν είναι κυκλική, τότε θεωρούμε μια μέγιστης τάξης κυκλική υποομάδα $K < G$, η οποία προφανώς είναι γνήσια υποομάδα τής G, και από το Λήμμα 4.2.3 συμπεραίνουμε ότι υπάρχει μια υποομάδα G' τής G, ώστε η G να είναι το εσωτερικό ευθύ γινόμενο των K και G'. Τώρα η G είναι ισόμορφη προς το εξωτερικό ευθύ γινόμενο $\mathcal{K}_1 \times G'$, όπου η $\mathcal{K}_1$ είναι μια ομάδα ισόμορφη προς την κυκλική υποομάδα K τής G. Η G' είναι μια p–ομάδα με τάξη γνήσια μικρότερη από p^{k+1}, αφού η K είναι μια γνήσια υποομάδα τής G, και χρησιμοποιώντας την επαγωγική υπόθεση, συμπεραίνουμε ότι η G' είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο $\mathcal{K}_2 \times \cdots \times \mathcal{K}_s$ κυκλικών ομάδων. Συνεπώς, η G είναι ισόμορφη προς το εξωτερικό ευθύ γινόμενο $\mathcal{K}_1 \times \mathcal{K}_2 \times \cdots \times \mathcal{K}_s$ των κυκλικών ομάδων $\mathcal{K}_i, 1 \leq i \leq s$.

(β′) Για $m = 1$, η ομάδα G είναι πρώτης τάξης p και ως εκ τούτου κυκλική. Αν τώρα η G είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο κυκλικών ομάδων $\mathcal{H}_1 \times \mathcal{H}_2 \times \cdots \times \mathcal{H}_t$, τότε θα είναι και το εξωτερικό ευθύ γινόμενο μια κυκλική ομάδα και αυτό μπορεί να γίνει μόνο αν $t = 1$ και $G \cong \mathcal{H}_1$.

Έστω ότι ο ισχυρισμός είναι αληθής για κάθε ομάδα τάξης $\leq p^k$, θα αποδείξουμε ότι είναι αληθής και για κάθε ομάδα τάξης p^{k+1}.

Έστω G μια ομάδα τάξης p^{k+1}. Αν η G είναι κυκλική, τότε η απόδειξη εκτελείται όπως και στην περίπτωση $m = 1$. Έστω ότι η G δεν είναι κυκλική και ότι η G είναι ισόμορφη προς δύο εξωτερικά ευθέα γινόμενα $\mathcal{K}_1 \times \mathcal{K}_2 \times \cdots \times \mathcal{K}_s$ και $\mathcal{H}_1 \times \mathcal{H}_2 \times \cdots \times \mathcal{H}_t$ οι παράγοντες των οποίων είναι διατεταγμένοι κατά διάταξη αντίστροφη των τάξεών τους, όπως ακριβώς περιγράφεται στη διατύπωση τής πρότασης.

Υπενθυμίζουμε ότι αν, A είναι οποιαδήποτε αβελιανή ομάδα και m είναι ένας φυσικός, τότε το σύνολο $A^m := \{a^m \mid a \in A\}$ είναι μια υποομάδα τής A (*γιατί;*). Επιπλέον αν, η $A = \langle a \rangle$ είναι κυκλική και παράγεται από το στοιχείο a, τότε η A^m είναι (προφανώς!) επίσης κυκλική και παράγεται από το στοιχείο a^m (*γιατί;*).

Στην περίπτωση τής G θεωρούμε τον πρώτο p και την υποομάδα G^p. Η G^p είναι μια γνήσια υποομάδα τής G, επειδή υπάρχουν στοιχεία τής G τάξης p, λόγω τού Θεωρήματος Cauchy (Θεώρημα 2.3.11). Επιπλέον, η G^p είναι ισόμορφη προς το εξωτερικό ευθύ γινόμενο $\mathcal{K}_1{}^p \times \mathcal{K}_2{}^p \times \cdots \times \mathcal{K}_s{}^p$ καθώς επίσης και με το εξωτερικό ευθύ γινόμενο $\mathcal{H}_1{}^p \times \mathcal{H}_2{}^p \times \cdots \times \mathcal{H}_t{}^p$.

Διακρίνουμε δύο περιπτώσεις:

I. Περίπτωση. $G^p = \{e_G\}$. Τότε $\forall i, 1 \leq i \leq s$ η κυκλική ομάδα $\mathcal{K}_i{}^p$ αποτελείται μόνο από το ουδέτερο στοιχείο $e_{\mathcal{K}_i}$. Συνεπώς $\forall i, 1 \leq i \leq s$, η $\mathcal{K}_i$ είναι κυκλική τάξης p. Με το ακριβώς ίδιο επιχείρημα συμπεραίνουμε ότι $\forall j, 1 \leq j \leq t$, η $\mathcal{H}_j$ είναι κυκλική τάξης p. Αφού, $G \cong \mathcal{K}_1 \times \mathcal{K}_2 \times \cdots \times \mathcal{K}_s$ είναι φανερό ότι οι δύο ομάδες έχουν την ίδια τάξη και γι' αυτό $[G:1] = p^s$. Επίσης αφού $G \cong \mathcal{H}_1 \times \mathcal{H}_2 \times \cdots \times \mathcal{H}_t$ συμπεραίνουμε ότι $[G:1] = p^t$. Επομένως, $s = t$ και $\forall i, 1 \leq i \leq s, \mathcal{K}_i \cong \mathcal{H}_i$. Στη συγκεκριμένη περίπτωση μάλιστα, όλες οι ομάδες $\mathcal{K}_i, \mathcal{H}_j$ είναι ισόμορφες προς την κυκλική ομάδα C_p με p το πλήθος στοιχεία.

II. Περίπτωση. $G^p \neq \{e_G\}$. Αφού $G^p \cong \mathcal{K}_1{}^p \times \mathcal{K}_2{}^p \times \cdots \times \mathcal{K}_s{}^p$, συμπεραίνουμε ότι και το εξωτερικό ευθύ γινόμενο $\mathcal{K}_1{}^p \times \mathcal{K}_2{}^p \times \cdots \times \mathcal{K}_s{}^p$ έχει περισσότερα τού ενός στοιχεία και ως εκ τούτου υπάρχουν παράγοντες $\mathcal{K}_i{}^p$ με περισσότερα τού ενός στοιχεία. Έστω s' ο μεγαλύτερος δείκτης μεταξύ των 1 και s, ούτως ώστε η ομάδα $\mathcal{K}_{s'}{}^p$ να έχει περισσότερα τού ενός στοιχεία. Τότε λόγω τού τρόπου με τον οποίο έχουν αριθμηθεί οι παράγοντες έχουμε ότι

$$\mathcal{K}_{s'+1}{}^p = \{e_{\mathcal{K}_{s'+1}}\}, \mathcal{K}_{s'+2}{}^p = \{e_{\mathcal{K}_{s'+2}}\}, \ldots, \mathcal{K}_s{}^p = \{e_{\mathcal{K}_s}\}. \tag{*}$$

Συνεπώς, η G^p είναι επίσης ισόμορφη και προς το εξωτερικό ευθύ γινόμενο $\mathcal{K}_1{}^p \times \mathcal{K}_2{}^p \times \cdots \times \mathcal{K}_{s'}{}^p$. Προσέξτε ότι από τη σχέση (*) συμπεραίνουμε ότι όλες οι ομάδες $\mathcal{K}_{s'+1}, \mathcal{K}_{s'+2}, \ldots, \mathcal{K}_s$ είναι κυκλικές τάξης p.

Τώρα, αφού η G^p είναι επίσης ισόμορφη προς το εξωτερικό ευθύ γινόμενο $\mathcal{H}_1{}^p \times \mathcal{H}_2{}^p \times \cdots \times \mathcal{H}_t{}^p$, εργαζόμαστε παρομοίως με αυτό. Έτσι θεωρούμε τον μεγαλύτερο δείκτη t' μεταξύ των 1 και t, ούτως ώστε η ομάδα $\mathcal{H}_{t'}{}^p$ να έχει περισσότερα τού ενός στοιχεία. Τότε λόγω τού τρόπου με τον οποίο είναι αριθμημένες οι παράγοντες έχουμε ότι

$$\mathcal{H}_{t'+1}{}^p = \{e_{\mathcal{H}_{t'+1}}\}, \mathcal{H}_{t'+2}{}^p = \{e_{\mathcal{H}_{t'+2}}\}, \ldots, \mathcal{H}_t{}^p = \{e_{\mathcal{H}_t}\}. \tag{**}$$

Συνεπώς, η G^p είναι επίσης ισόμορφη προς το εξωτερικό ευθύ γινόμενο $\mathcal{H}_1{}^p \times \mathcal{H}_2{}^p \times \cdots \times \mathcal{H}_{t'}{}^p$. Προσέξτε ότι από τη σχέση (**) συμπεραίνουμε ότι όλες οι ομάδες $\mathcal{H}_{t'+1}, \mathcal{H}_{t'+2}, \ldots, \mathcal{H}_t$ είναι κυκλικές τάξης p.

Όπως έχουμε ήδη παρατηρήσει η G^p είναι μια γνήσια υποομάδα τής G και γι' αυτό εφαρμόζοντας την επαγωγική υπόθεση στην ομάδα G^p, όπου $G^p \cong \mathcal{K}_1{}^p \times \mathcal{K}_2{}^p \times \cdots \times \mathcal{K}_{s'}{}^p$ και $G^p \cong \mathcal{H}_1{}^p \times \mathcal{H}_2{}^p \times \cdots \times \mathcal{H}_{t'}{}^p$, συμπεραίνουμε ότι $s' = t'$ και ότι $\forall i, 1 \leq i \leq s', \mathcal{K}_i^p \cong \mathcal{H}_i^p$ και ιδιαιτέρως έχουν ίσες τάξεις, δηλαδή $[\mathcal{K}_i^p : 1] = [\mathcal{H}_i^p : 1]$. Επειδή η τάξη τής κυκλικής ομάδας $\mathcal{K}_i$ (αντιστοίχως τής $\mathcal{H}_i$) ισούται με $p[\mathcal{K}_i^p : 1]$ (αντιστοίχως με $p[\mathcal{H}_i^p : 1]$ συμπεραίνουμε ότι για κάθε $i, 1 \leq i \leq s'$, οι τάξεις των κυκλικών ομάδων $\mathcal{K}_i$ και $\mathcal{H}_i$ είναι ίσες και ως εκ τούτου $\forall i, 1 \leq i \leq s', \mathcal{K}_i \cong \mathcal{H}_i$.

Υπολείπεται η απόδειξη ότι $s = t$, αφού ήδη γνωρίζουμε ότι οι ομάδες $\mathcal{K}_{s'+1}, \mathcal{K}_{s'+2}, \ldots, \mathcal{K}_s$ και $\mathcal{H}_{s'+1}, \mathcal{H}_{s'+2}, \ldots, \mathcal{H}_t$ είναι κυκλικές τάξης p και ως εκ τούτου, ισόμορφες μεταξύ τους.

Θέτουμε $G_{\mathcal{K}}$ για το εξωτερικό ευθύ γινόμενο $\mathcal{K}_1 \times \mathcal{K}_2 \times \cdots \times \mathcal{K}_{s'}$ και $G_{\mathcal{H}}$ για το εξωτερικό ευθύ γινόμενο $\mathcal{H}_1 \times \mathcal{H}_2 \times \cdots \times \mathcal{H}_{s'}$.

Τώρα $G_{\mathcal{K}} \cong G_{\mathcal{H}}$ και η ομάδα G είναι ισόμορφη προς τα εξωτερικά ευθέα γινόμενα

$$G_{\mathcal{K}} \times \mathcal{K}_{s'+1} \times \mathcal{K}_{s'+2} \times \cdots \times \mathcal{K}_s \text{ και } G_{\mathcal{H}} \times \mathcal{H}_{s'+1} \times \mathcal{H}_{s'+2} \times \cdots \times \mathcal{H}_t.$$

Συνεπώς, έχουμε:

$$[G_{\mathcal{K}} : 1]p^{s-s'} = [G : 1] = [G_{\mathcal{H}} : 1]p^{t-s'}$$

και αφού $[G_{\mathcal{K}} : 1] = [G_{\mathcal{H}} : 1]$, συμπεραίνουμε ότι $p^{s-s'} = p^{t-s'}$ και τελικώς $s = t$. □

Διαμερίσεις

Για να δούμε το πώς ακριβώς εφαρμόζεται η ανωτέρω πρόταση επαναλαμβάνουμε[3] τον Ορισμό1.8.24.

Ορισμός 4.2.5. Έστω $n \in \mathbb{N}$ ένας φυσικός αριθμός. Κάθε ακολουθία $(m_1, m_2, \ldots, m_t)$ φυσικών αριθμών ονομάζεται μια *διαμέριση* τού n αν,

$$n = \sum_{i=1}^{t} m_i \text{ και } m_1 \geq m_2 \geq \cdots \geq m_i \geq m_{i+1} \geq \cdots \geq m_t.$$

Έτσι, οι διαμερίσεις τού 3 είναι οι ακολουθίες $\delta_1(3) = (3), \delta_2(3) = (2,1)$ και $\delta_3(3) = (1,1,1)$, τού 4 είναι οι ακολουθίες $\delta_1(4) = (4), \delta_2(4) = (3,1,1), \delta_3(4) = (2,2), \delta_4(4) = (2,1,1)$ και $\delta_5(4) = (1,1,1,1)$.

Έστω $P(n)$ το πλήθος των διαμερίσεων τού φυσικού n και $\Delta(n) = \{\delta_i(n) \mid i = 1, 2, \ldots, P(n)\}$ οι διαμερίσεις του. Διατάσσουμε τα στοιχεία τού $\Delta(n)$ κατά την αντίστροφη λεξικογραφική διάταξη «$\preceq$» και σχηματίζουμε με αυτά έναν πίνακα, που κάθε γραμμή του είναι ένα στοιχείο τού $\Delta(n)$. Η διάταξη των γραμμών τού πίνακα είναι τέτοια ώστε αν, το $\delta(n)$ είναι η i–οστή γραμμή και $\delta'(n)$ είναι j–οστή με $j \leq i$, τότε $\delta'(n) \preceq \delta(n)$.

Ο συγκεκριμένος πίνακας είναι μοναδικός, ονομάζεται *πίνακας Young*. Θα τον συμβολίζουμε με $Y(n)$.

Το πλήθος των στοιχείων τής στήλης τού $Y(n)$ με τα περισσότερα στοιχεία ισούται με το πλήθος $P(n)$ των διαμερίσεων τού φυσικού n.

Επί παραδείγματι,

$$Y(3) = \begin{array}{ccc} 1 & 1 & 1 \\ 2 & 1 & \\ 3 & & \end{array}, \quad Y(4) = \begin{array}{cccc} 1 & 1 & 1 & 1 \\ 2 & 1 & 1 & \\ 2 & 2 & & \\ 3 & 1 & & \\ 4 & & & \end{array} \text{ και } Y(5) = \begin{array}{ccccc} 1 & 1 & 1 & 1 & 1 \\ 2 & 1 & 1 & 1 & \\ 2 & 2 & 1 & & \\ 3 & 1 & 1 & & \\ 3 & 2 & & & \\ 4 & 1 & & & \\ 5 & & & & \end{array},$$

[3]Στον παρόντα ορισμό για τον ορισμό τής διαμέρισης χρησιμοποιούμε την αύξουσα διάταξη των m_i.

$P(3) = 3, P(4) = 5$ και $P(5) = 7$.

Πρόταση 4.2.6. *Έστω ότι q είναι ένας πρώτος αριθμός και ότι n είναι ένας φυσικός αριθμός. Το πλήθος $f_G(q^n)$ των μη ισόμορφων αβελιανών p–ομάδων $(G, \star)$ τάξης q^n ισούται με το πλήθος $P(n)$ των διαμερίσεων τού n.*

Απόδειξη. Έστω ότι $\Delta(n)$ είναι το σύνολο των διαμερίσεων τού φυσικού n και ότι $\mathcal{C}(n)$ είναι το σύνολο των εξωτερικών ευθέων γινομένων $C_{q^{m_1}} \times C_{q^{m_2}} \times \cdots \times C_{q^{m_t}}$ όπου $(m_1, m_2, \ldots, m_t)$ είναι μια διαμέριση τού n. Σύμφωνα με την Πρόταση 4.2.4 (β′), οι ομάδες που ανήκουν στο σύνολο $\mathcal{C}(n)$ δεν είναι ισόμορφες. Παρατηρούμε ότι τα $\Delta(n)$ και $\mathcal{C}(n)$ βρίσκονται σε μια «$1 - 1$» και «επί» αντιστοιχία.
Λόγω τής Πρότασης 4.2.4 (α′), γνωρίζουμε ότι κάθε αβελιανή ομάδα G τάξης q^n είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο κυκλικών ομάδων C_{q^m} που καθεμιά τους έχει ως τάξη μια δύναμη q^m τού q, ας πούμε $G \cong C_{q^{m_1}} \times C_{q^{m_2}} \times \cdots \times C_{q^{m_t}}$. Συνεπώς, $q^n = q^{m_1+m_2+\cdots+m_t}$ και γι' αυτό $n = m_1 + m_2 + \cdots + m_t$. Επιπλέον, μπορούμε να διατάξουμε τους παράγοντες τού εξωτερικού ευθέος γινομένου κατά τέτοιον τρόπο, ώστε $q^{m_1} \geq q^{m_2} \geq \cdots \geq q^{m_t}$. Συνεπώς, $m_1 \geq m_2 \geq \cdots \geq m_t$ και γι' αυτό τώρα, η ακολουθία $(m_1, m_2, \ldots, m_t)$ είναι μια διαμέριση τού n. Επομένως, κάθε αβελιανή ομάδα G τάξης q^n είναι ισόμορφη προς ακριβώς μία από τις ομάδες τού συνόλου $\mathcal{C}(n)$. Το πλήθος των στοιχείων τού $\mathcal{C}(n)$ ισούται με $P(n)$, δηλαδή το πλήθος των διαμερίσεων τού n. Συνεπώς, $f_G(q^n) = P(n)$. □

Παρατήρηση 4.2.7. Προσέξτε ότι ο πρώτος q δεν επηρεάζει καθόλου το πλήθος $f_G(q^n)$ των μη ισόμορφων αβελιανών ομάδων G τάξης q^n. Το πλήθος $f_G(13^{200})$ των μη ισόμορφων αβελιανών ομάδων G τάξης 13^{200} είναι το ίδιο με το πλήθος $f_G(541^{200})$ των μη ισόμορφων αβελιανών ομάδων G τάξης 541^{200}. Το πλήθος αυτό είναι ίσο με το πλήθος των διαμερίσεων τού 200, δηλαδή με $P(200)$ και το $P(200)$ είναι ίσο με 3972999029388. Ένας αρκετά μεγάλος αριθμός!

Παράδειγμα 4.2.8. Ας δούμε με ποιες ομάδες μπορεί να είναι ισόμορφη μια αβελιανή ομάδα G τάξης q^3, όπου ο q είναι πρώτος αριθμός. Από τον αντίστοιχο πίνακα $Y(3)$ έχουμε ότι η G είναι ισόμορφη προς ακριβώς μία από τις

$$C_q^3, \; C_q^2 \times C_q, \; C_q \times C_q \times C_q.$$

Ενώ μια αβελιανή ομάδα G τάξης q^5, όπου ο q πρώτος αριθμός, είναι ισόμορφη προς ακριβώς μία από τις

$$\begin{array}{l} C_{q^5}, \; C_{q^4} \times C_q, \; C_{q^3} \times C_{q^2}, \; C_{q^3} \times C_q \times C_q \;\; C_{q^2} \times C_{q^2} \times C_q \\ C_{q^2} \times C_q \times C_q \times C_q \;\; C_q \times C_q \times C_q \times C_q \times C_q. \end{array}$$

Πρόταση 4.2.9. *Έστω ότι n είναι ένας φυσικός αριθμός και ότι $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ είναι μια ανάλυσή του σε γινόμενο θετικών δυνάμεων πρώτων αριθμών $p_i, 1 \leq i \leq s$, διαφορετικών ανά δύο.*

Το πλήθος $f_G(n)$ των μη ισόμορφων αβελιανών ομάδων G τάξης n ισούται με το γινόμενο $P(\alpha_1) \cdot P(\alpha_s) \cdot \ldots \cdot P(\alpha_s)$, όπου $P(\alpha_i)$ είναι το πλήθος των διαμερίσεων τού θετικού αριθμού $\alpha_i, 1 \leq i \leq s$.

Απόδειξη. Σύμφωνα με την Πρόταση 4.2.1, μια αβελιανή ομάδα τάξης $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο s το πλήθος p–ομάδων με αντίστοιχες τάξεις $p_1^{\alpha_1}, p_2^{\alpha_2}, \dots, p_s^{\alpha_s}$. Ο ισομορφισμός είναι ανεξάρτητος από τη σειρά με την οποία εμφανίζονται οι παράγοντες στο εξωτερικό ευθύ γινόμενο. Ως εκ τούτου

$$f_G(n) = f_G(p_1^{\alpha_1}) \cdot f_G(p_2^{\alpha_2}) \cdot \dots \cdot f_G(p_s^{\alpha_s}) = P(\alpha_1) \cdot P(\alpha_s) \cdot \dots \cdot P(\alpha_s),$$

αφού λόγω τής Πρότασης 4.2.6, γνωρίζουμε ότι $\forall i, 1 \leq i \leq s$, είναι $f_G(p_i^{\alpha_i}) = P(\alpha_i)$. $\square$

Πόρισμα 4.2.10. *Έστω n ένας φυσικός αριθμός τής μορφής $n = p_1 p_2 \dots p_s$, όπου οι $p_i, 1 \leq i \leq s$ είναι πρώτοι αριθμοί διαφορετικοί ανά δύο.*
Κάθε αβελιανή ομάδα τάξης n είναι ισόμορφη προς την κυκλική ομάδα C_n τάξης n.

Απόδειξη. Από την προηγούμενη πρόταση γνωρίζουμε ότι

$$f_G(n) = P(1) \cdot P(1) \cdot \dots \cdot P(1) = 1 \cdot 1 \cdot \dots \cdot 1 = 1 \ \ (s \text{ το πλήθος παράγοντες }).$$

Ώστε, υπάρχει (με ακρίβεια ισομορφίας) μόνο μία αβελιανή ομάδα τάξης n. Προφανώς, αυτή η ομάδα είναι η κυκλική C_n τάξης n. $\square$

Παράδειγμα 4.2.11. Πόσες μη ισόμορφες αβελιανές ομάδες G τάξης 600 υπάρχουν;

Η ανάλυση τού 600 σε δυνάμεις πρώτων είναι η $600 = 2^3 \cdot 3 \cdot 5^2$. Συνεπώς, $f_G(600) = P(3) \cdot P(1) \cdot P(2) = 6$.

Κάθε αβελιανή ομάδα τάξης 600 είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο από τρεις p–ομάδες με αντίστοιχες τάξεις 2^3, 3 και 5^2. Γι' αυτό κάθε αβελιανή ομάδα G τάξης 600 είναι ισόμορφη προς μια από τις επόμενες ομάδες:

$$\begin{array}{ccc} C_{2^3} \times C_3 \times C_{5^2}, & C_{2^2} \times C_2 \times C_3 \times C_{5^2}, & C_2 \times C_2 \times C_2 \times C_3 \times C_{5^2}, \\ C_{2^3} \times C_3 \times C_5 \times C_5, & C_{2^2} \times C_2 \times C_3 \times C_5 \times C_5, & C_2 \times C_2 \times C_2 \times C_3 \times C_5 \times C_5. \end{array}$$

Αλλά και το πλήθος των μη ισόμορφων αβελιανών ομάδων G τάξης p^3qr^2, όπου p, q, r είναι οποιοιδήποτε πρώτοι αριθμοί, διαφορετικοί ανά δύο, είναι επίσης 6 και κάθε τέτοια ομάδα είναι ισόμορφη προς μια από τις

$$\begin{array}{ccc} C_{p^3} \times C_q \times C_{r^2}, & C_{p^2} \times C_p \times C_q \times C_{r^2}, & C_p \times C_p \times C_p \times C_q \times C_{r^2}, \\ C_{p^3} \times C_q \times C_r \times C_r, & C_{p^2} \times C_p \times C_q \times C_r \times C_r, & C_p \times C_p \times C_p \times C_q \times C_r \times C_r. \end{array}$$

Τα ανωτέρω συνοψίζονται στο

Θεώρημα 4.2.12 (Το Θεώρημα Ταξινόμησης των πεπερασμένων αβελιανών Ομάδων). *Κάθε πεπερασμένη αβελιανή ομάδα είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο κυκλικών p–ομάδων. Το πλήθος των παραγόντων τού εξωτερικού ευθέος γινομένου καθώς και οι τάξεις των κυκλικών ομάδων προσδιορίζονται μοναδικά από την ομάδα.*

Αν η τάξη τής αβελιανής ομάδας είναι $n = \prod_{i=1}^{s} p_i^{\alpha_i}$, όπου οι $p_i, 1 \leq i \leq s$ είναι πρώτοι αριθμοί διαφορετικοί ανά δύο και οι $\alpha_i, 1 \leq i \leq s$ είναι φυσικοί, τότε το πλήθος των μη ισόμορφων αβελιανών ομάδων τάξης n είναι $\prod_{i=1}^{s} P(\alpha_i)$, όπου $P(\alpha_i), 1 \leq i \leq s$ είναι το πλήθος των διαμερίσεων τού $\alpha_i, 1 \leq i \leq s$.

Ασκήσεις στις πεπερασμένες αβελιανές Ομάδες

Λυμένες Ασκήσεις

Α 122. Έστω $(G, \star)$ μια πεπερασμένη αβελιανή ομάδα η οποία αποτελείται από ακριβώς οκτώ στοιχεία τάξης 3, από ακριβώς δεκαοκτώ στοιχεία τάξης 9 και από το ουδέτερο στοιχείο. Προς ποιά ομάδα είναι η G ισόμορφη;

Λύση. Η τάξη τής G ισούται με $8 + 18 + 1 = 27 = 3^3$. Επομένως η G θα είναι ισόμορφη με μια από τις ομάδες

$$C_3^3, \;\; C_3^2 \times C_3, \;\; C_3 \times C_3 \times C_3.$$

Η G δεν είναι ισόμορφη προς την C_3^3, διότι η G δεν διαθέτει στοιχείο τάξης $3^3 = 27$. Επίσης η G δεν είναι ισόμορφη προς την $C_3 \times C_3 \times C_3$, διότι η τάξη κάθε στοιχείου τής τελευταίας είναι ή 1 ή 3. Επομένως $G \cong C_3^2 \times C_3$.

Α 123. Έστω ότι $(G, \star)$ είναι μια αβελιανή ομάδα τάξης 216. Αν η υποομάδα $G^6 = \{g^6 \mid g \in G\}$ τής G είναι τάξης 6, βλ. Άσκηση ΠΑ39, τότε να προσδιοριστεί η G με ακρίβεια ισομορφίας.

Λύση. Για την τάξη τής G έχουμε $[G : 1] = 216 = 2^3 \cdot 3^3$. Επομένως, η G είναι ισόμορφη με ένα εξωτερικό ευθύ γινόμενο $A \times B$, όπου A είναι μια ομάδα από το σύνολο $\mathcal{C}_2 = \{C_{2^3}, C_{2^2} \times C_2, C_2 \times C_2 \times C_2\}$ και B είναι μια ομάδα από το σύνολο $\mathcal{C}_3 = \{C_{3^3}, C_{3^2} \times C_3, C_3 \times C_3 \times C_3\}$.

Γενικά, όταν $C_n = \langle a \rangle$ είναι μια κυκλική ομάδα τάξης n, τότε η $C_n^s, s \in \mathbb{N}$, ισούται με την κυκλική υποομάδα $\langle a^s \rangle$, η οποία ως γνωστόν είναι τάξης $\frac{n}{\text{ΜΚΔ}(s,n)}$. Ως εκ τούτου, οι C_2^6 και C_3^6 είναι οι τετριμμένες ομάδες με ακριβώς ένα στοιχείο. Επιπλέον, $C_{2^2}^6 \cong C_2$, $C_{2^3}^6 \cong C_{2^2}$, $C_{3^2}^6 \cong C_3$ και $C_{3^3}^6 \cong C_{3^2}$.

Επειδή $[G^6 : 1] = 6 = 2 \cdot 3$, έχουμε ότι η $G^6 \cong C_2 \times C_3$ και αφού $G \cong A \times B$ συμπεραίνουμε ότι $G^6 \cong A^6 \times B^6$, βλ. και Άσκηση ΠΑ40. Γι' αυτό, $A^6 \times B^6 \cong C_2 \times C_3$. Μεταξύ των ομάδων τού συνόλου $\mathcal{C}_2$ (αντιστοίχως τού συνόλου $\mathcal{C}_3$) μόνο η $C_{2^2} \times C_2$ (αντιστοίχως η $C_{3^2} \times C_3$) έχει την ιδιότητα $(C_{2^2} \times C_2)^6 \cong C_2$ (αντιστοίχως $(C_{3^2} \times C_3)^6 \cong C_3$). Άρα, $A \cong C_{2^2} \times C_2$, $B \cong C_{3^2} \times C_3$ και ως εκ τούτου, $G \cong C_{2^2} \times C_2 \times C_{3^2} \times C_3$.

Α 124. Το σύνολο $G = \{[1]_{96}, [7]_{96}, [17]_{96}, [23]_{96}, [49]_{96}, [55]_{96}, [65]_{96}, [71]_{96}\}$ των κλάσεων ισοτιμίας mod 96 αποτελεί μια ομάδα με πράξη τον πολλαπλασιασμό κατά μόδιο (μέτρο) 96. Να εκφραστεί η G ως εξωτερικό ευθύ γινόμενο κυκλικών ομάδων και κατόπιν ως εσωτερικό ευθύ γινόμενο κυκλικών υποομάδων της.

Λύση. Η G είναι μια πεπερασμένη αβελιανή ομάδα τάξης $[G : 1] = 8 = 2^3$. Επομένως, θα είναι ισόμορφη ή προς τη C_{2^3} ή προς το εξωτερικό ευθύ γινόμενο $C_{2^2} \times C_2$ ή προς το εξωτερικό ευθύ γινόμενο $C_2 \times C_2 \times C_2$. Οι τάξεις των στοιχείων τής G έχουν ως εξής:

Στοιχείο	$[1]_{96}$	$[7]_{96}$	$[17]_{96}$	$[23]_{96}$	$[49]_{96}$	$[55]_{96}$	$[65]_{96}$	$[71]_{96}$
Τάξη	1	4	2	4	2	4	2	4

Αφού η ομάδα G δεν έχει στοιχείο τάξης 8 και αφού έχει στοιχεία τάξης 4, συμπεραίνουμε ότι $G \cong C_{2^2} \times C_2$, $(*)$.

Για να εκφράσουμε τη G ως εσωτερικό ευθύ γινόμενο, θα ακολουθήσουμε τη διαδικασία που παρουσιάζεται στην απόδειξη τού Λήμματος 4.2.3. Από την $(*)$ διαπιστώνουμε ότι η G έχει μια μέγιστη υποομάδα τάξης 4, η οποία μάλιστα είναι κυκλική. Από τον προηγούμενο πίνακα των τάξεων των στοιχείων τής G επιλέγουμε ένα στοιχείο τάξης 4, για παράδειγμα το $[7]_{96}$. Το σύνολο των στοιχείων τής κυκλικής υποομάδας $H = \langle [7]_{96} \rangle < G$ είναι το $\{[1]_{96}, [7]_{96}, [49]_{96}, [55]_{96}\}$. Η τάξης 2 υποομάδα $K = \langle [17]_{96} \rangle$ δεν περιέχεται στην H. Ως εκ τούτου, $H \bigcap K = \{[1]_{96}\}$ και η G είναι το εσωτερικό ευθύ γινόμενο των H και K.

Α 125. (α′) Έστω ότι $\mathcal{P}$ είναι μια ομάδα τάξης p^α και ότι $\mathcal{Q}$ είναι μια ομάδα τάξης q^β, όπου οι p, q είναι πρώτοι αριθμοί και οι α, β είναι φυσικοί. Να δειχθεί ότι όταν το εξωτερικό ευθύ γινόμενο $\mathcal{P} \times \mathcal{P}$ είναι ισόμορφο προς το εξωτερικό ευθύ γινόμενο $\mathcal{Q} \times \mathcal{Q}$, τότε η $\mathcal{P}$ είναι ισόμορφη προς την $\mathcal{Q}$.

(β′) Έστω ότι $(G, \star)$ και $(G', \star')$ είναι δύο πεπερασμένες αβελιανές ομάδες. Να δειχθεί ότι $G \cong G'$, αν και μόνο αν, $G \times G \cong G' \times G'$.

Λύση. (α′) Σύμφωνα με την Πρόταση 4.2.4, η $\mathcal{P}$ είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο $\mathcal{K}_1 \times \cdots \times \mathcal{K}_s$ κυκλικών ομάδων $\mathcal{K}_i, 1 \leq i \leq s$ με τάξεις $[\mathcal{K}_i : 1] = p^{\alpha_i}, 1 \leq i \leq s$. Χωρίς περιορισμό τής γενικότητας μπορούμε να δεχθούμε, όπως και στην Πρόταση 4.2.4, ότι όταν $i \leq j$, τότε $p^{\alpha_i} \geq p^{\alpha_j}$. Παρόμοια, η $\mathcal{Q}$ είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο $\mathcal{H}_1 \times \cdots \times \mathcal{H}_t$ κυκλικών ομάδων $\mathcal{H}_j, 1 \leq j \leq t$ με τάξεις $[\mathcal{H}_j : 1] = q^{\beta_j}, 1 \leq j \leq t$, όπου και πάλι μπορούμε να δεχθούμε ότι όταν $i \leq j$, τότε $q^{\beta_i} \geq q^{\beta_j}$. Αφού το εξωτερικό ευθύ γινόμενο $\mathcal{P} \times \mathcal{P}$ είναι ισόμορφο προς το εξωτερικό ευθύ γινόμενο $\mathcal{Q} \times \mathcal{Q}$, συμπεραίνουμε ότι $p^{2\alpha} = q^{2\beta}$ και επομένως $p = q$. Παρατηρούμε ότι

$$\mathcal{P} \times \mathcal{P} \cong (\mathcal{K}_1 \times \mathcal{K}_1) \times \cdots \times (\mathcal{K}_s \times \mathcal{K}_s) \text{ και } \mathcal{Q} \times \mathcal{Q} \cong (\mathcal{H}_1 \times \mathcal{H}_1) \times \cdots \times (\mathcal{H}_t \times \mathcal{H}_t).$$

Στα ανωτέρω δύο ισόμορφα εξωτερικά ευθέα γινόμενα, οι παράγοντες εμφανίζονται κατά διάταξη αντίστροφη των τάξεών τους και γι' αυτό από την Πρόταση 4.2.4, συμπεραίνουμε $2s = 2t$ και ότι $\mathcal{K}_i \cong \mathcal{H}_i, \forall i, 1 \leq i \leq s$. Επομένως $\mathcal{P} \cong \mathcal{Q}$.

(β′) «$\Rightarrow$» Όταν $\sigma : G \to G'$ είναι ένας ισομορφισμός, τότε η απεικόνιση $\varphi : G \times G \to G' \times G', (g_1, g_2) \mapsto \varphi((g_1, g_2)) := (\sigma(g_1), \sigma(g_2))$ είναι ένας ισομορφισμός (*γιατί;*).
«$\Leftarrow$» Ο ισομορφισμός $\sigma : G \times G \to G' \times G'$ δίνει ότι η τάξη $[G : 1]^2$ τού εξωτερικού ευθέως γινομένου $G \times G$ ισούται με την τάξη $[G' : 1]^2$ τού εξωτερικού ευθέως γινομένου $G' \times G'$. Επομένως, $[G : 1] = [G' : 1] = n$.Έστω ότι p_i είναι ένας πρώτος διαιρέτης τής κοινής τάξης n, ότι $\mathcal{P}_i$ είναι η p_i-Sylow υποομάδα τής G και ότι $\mathcal{P}'_i$ είναι η p_i-Sylow υποομάδα τής G'. Για κάθε διαιρέτη p_i τής κοινής τάξης n^2 των $G \times G$ και $G' \times G'$, τα ισόμορφα εξωτερικά ευθέα γινόμενα $G \times G$ και $G' \times G'$ έχουν ισόμορφες p_i-Sylow υποομάδες. Η p_i-Sylow υποομάδα τής $G \times G$ είναι ισόμορφη προς την $\mathcal{P}_i \times \mathcal{P}_i$ και η αντίστοιχη p_i-Sylow υποομάδα τής $G' \times G'$ είναι ισόμορφη προς την $\mathcal{P}'_i \times \mathcal{P}'_i$. (Υπενθυμίζουμε ότι κάθε πεπερασμένη αβελιανή ομάδα έχει για κάθε πρώτο διαιρέτη p τής τάξης της ακριβώς μία p-Sylow υποομάδα.) Επειδή $\mathcal{P}_i \times \mathcal{P}_i \cong \mathcal{P}'_i \times \mathcal{P}'_i$, συμπεραίνουμε από το πρώτο μέρος τής άσκησης ότι $\mathcal{P}_i \cong \mathcal{P}'_i$. Άρα, $G \cong G'$, αφού κάθε πεπερασμένη αβελιανή ομάδα είναι ισόμορφη προς το εξωτερικό ευθύ γινόμενο των Sylow υποομάδων της, βλ. Πρόταση 4.2.1.

A 126. Έστω $(G, \star)$ μια αβελιανή ομάδα τάξης $[G:1] < \infty$. Για κάθε διαιρέτη d τής τάξης $[G:1]$, συμβολίζουμε με $G(d)$ την υποομάδα $\{g \in G \mid g^d = e_G\}$. Όταν $[G:1] = mn$ με ΜΚΔ$(m,n) = 1$, τότε να δειχθεί ότι $G \cong G(m) \times G(n)$.

Λύση. Επειδή η G είναι αβελιανή, έχουμε $G(m) \trianglelefteq G$ και $G(n) \trianglelefteq G$. Παρατηρούμε ότι $G(m) \bigcap G(n) = \{e_G\}$. Πράγματι, όταν $g \in G(m) \bigcap G(n)$, τότε $g^m = e_G$ και $g^n = e_G$. Επειδή ο ΜΚΔ$(m,n) = 1$, συμπεραίνουμε ότι υπάρχουν $\kappa, \lambda \in \mathbb{Z}$ με $1 = m\kappa + n\lambda$, $(*)$. Ως εκ τούτου, $g = g^{m\kappa + n\lambda} = (g^m)^\kappa (g^n)^\lambda = e_G$. Από την Άσκηση A88 ή/και την Πρόταση 4.1.13, συμπεραίνουμε ότι $G(m)G(n) \cong G(m) \times G(n)$.

Υπολείπεται η απόδειξη ότι $G = G(m)G(n)$. Όταν $g \in G$, τότε, όπως και στην $(*)$, υπάρχουν $\kappa, \lambda \in \mathbb{Z}$ με $1 = m\kappa + n\lambda$ και έτσι $g = g^{n\lambda + m\kappa} = (g^\lambda)^n (g^\kappa)^m$. Το στοιχείο $(g^\lambda)^n$ ανήκει στη $G(m)$, αφού $((g^\lambda)^n)^m = (g^{mn})^\lambda = e_G$, διότι $\forall g \in G$ είναι $g^{[G:1]} = g^{mn} = e_G$. Επιχειρηματολογώντας εντελώς όμοια, προκύπτει ότι το $(g^\kappa)^m$ ανήκει στη $G(n)$. Επομένως, κάθε $g \in G$ ανήκει στη $G(m)G(n)$ και συνεπώς $G = G(m)G(n)$.

A 127. Έστω $(G, \star)$ μια αβελιανή ομάδα τάξης $[G:1] = mn$, όπου ο ΜΚΔ$(m,n) = 1$. Να δειχθεί ότι $[G(m):1] = m$ και $[G(n):1] = n$.
(Για τον ορισμό των $G(m), G(n)$, βλ. την αμέσως προηγούμενη άσκηση).

Λύση. Ο ισχυρισμός τής άσκησης είναι προφανής, όταν είτε $m = 1$ είτε $n = 1$. Συνεπώς, χωρίς περιορισμό τής γενικότητας μπορούμε να υποθέσουμε ότι $m, n \geq 2$.

Ισχυριζόμαστε ότι αν p είναι ένας πρώτος με $p \mid m$, τότε ο $p \nmid [G(n):1]$. Πράγματι, αν ο p διαιρούσε την τάξη $[G(n):1]$, τότε λόγω τού Θεωρήματος Cauchy, βλ. Θεώρημα 2.3.11, θα υπήρχε $g \in G(n)$ τάξης p. Όμως $g^n = e_G$, διότι $g \in G(n)$ και τότε η τάξη $\circ(g) = p$ θα διαιρούσε το n. Αυτό όμως είναι άτοπο, αφού ο ΜΚΔ$(m,n) = 1$. Εντελώς όμοια αποδεικνύεται ότι όταν p είναι ένας πρώτος με $p \mid n$, τότε $p \nmid [G(m):1]$.

Από την αμέσως προηγούμενη άσκηση, γνωρίζουμε ότι $G \cong G(m) \times G(n)$ και ως εκ τούτου, $[G:1] = mn = [G(m):1][G(n):1]$. Μόλις αποδείξαμε ότι κάθε πρώτος διαιρέτης p τού m δεν διαιρεί την τάξη $[G(n):1]$. Ως εκ τούτου κάθε πρώτος διαιρέτης p τού m διαιρεί την τάξη $[G(m):1]$ και είναι ΜΚΔ$(p, [G(n):1]) = 1$. Όμοια, κάθε πρώτος διαιρέτης p τού n διαιρεί την τάξη $[G(n):1]$ και επιπλέον είναι ΜΚΔ$(p, [G(m):1]) = 1$. Με τη βοήθεια τού Θεμελιώδους Θεωρήματος τής στοιχειώδους Θεωρίας Αριθμών, προκύπτει τώρα αμέσως ότι $m = [G(m):1]$ και $n = [G(n):1]$.

A 128. Έστω ότι η αβελιανή ομάδα $(G, \star)$ είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της H, K. Έστω ότι η H_1 είναι μια υποομάδα τής H και K_1 είναι μια υποομάδα τής K. Να δειχθεί ότι η πηλικοομάδα G/H_1K_1 είναι ισόμορφη προς το εξωτερικό ευθύ γινόμενο $H/H_1 \times K/K_1$.

Λύση. Οι φυσικοί επιμορφισμοί $\pi_H : H \to H/H_1, h \mapsto hH_1$ και $\pi_K : K \to K/K_1, k \mapsto kK_1$ επάγουν τον επιμορφισμό $\pi : H \times K \to H/H_1 \times K/K_1, (h,k) \mapsto (hH_1, kK_1)$. Επειδή η G ισούται με το εσωτερικό ευθύ γινόμενο HK των H και K και επειδή η αντιστοιχία $\sigma : HK \to H \times K, hk \mapsto (h,k)$ είναι μια καλά ορισμένη απεικόνιση, η οποία μάλιστα είναι ισομορφισμός, συμπεραίνουμε ότι η σύνθεση

$$\pi \circ \sigma : G = HK \to H/H_1 \times K/K_1, hk \mapsto (hH_1, kK_1)$$

είναι ένας επιμορφισμός. Για τον πυρήνα $\ker \pi \circ \sigma$ τού ομομορφισμού, έχουμε:

$$g = hk \in \ker \Leftrightarrow \pi \circ \sigma(hk) = (hH_1, kK_1) = (e_G, e_G) \Leftrightarrow h \in H_1, k \in K_1 \Leftrightarrow hk \in H_1K_1.$$

Επομένως, $\ker \pi\circ\sigma = H_1K_1$. Τώρα από το Πρώτο Θεώρημα Ισομορφίας, βλ. Θεώρημα 1.7.21, προκύπτει ότι $G/H_1K_1 \cong H/H_1 \times K/K_1$.

Α 129. Να δειχθεί ότι για $n \in \mathbb{N}$, οι ακόλουθες προτάσεις είναι ισοδύναμες:

(α′) Όλες οι αβελιανές ομάδες τάξης n είναι ισόμορφες.

(β′) Όλες οι αβελιανές ομάδες τάξης n είναι κυκλικές.

(γ′) Ο φυσικός n είναι ελεύθερος τετραγώνων, δηλαδή δεν υπάρχει πρώτος p με $p^2 \mid n$.

(Σημείωση: Στο Θεώρημα 7.3.1, δίνεται η ικανή και αναγκαία συνθήκη για τον φυσικό n, ώστε κάθε ομάδα τάξης n να είναι κυκλική.)

Λύση. «(α′) ⇒ (β′)» Ιδιαιτέρως, κάθε αβελιανή ομάδα G τάξης n είναι ισόμορφη προς μια κυκλική ομάδα C_n τάξης n και επομένως $G \cong C_n$.
«(β′) ⇒ (γ′)» Έστω ότι $n = p_1^{\alpha_1} \ldots p_s^{\alpha_s}$ είναι η ανάλυση τού n σε γινόμενο δυνάμεων, ανά δύο διαφορετικών, πρώτων αριθμών p_i. Αν ο n δεν είναι ελεύθερος τετραγώνων, τότε μπορούμε να υποθέσουμε χωρίς περιορισμό τής γενικότητας ότι $\alpha_1 \geq 2$. Το εξωτερικό ευθύ γινόμενο $G = C_{p_1} \times C_{p_1^{(\alpha_1-1)}} \times C_{p_2^{\alpha_2} \ldots p_s^{\alpha_s}}$ δεν είναι κυκλική ομάδα, διότι $\forall g \in G$ είναι $g^{n/p_1} = g^{p_1^{(\alpha_1-1)} p_2^{\alpha_2} \cdots p_s^{\alpha_s}} = e_G$. Αυτό όμως αντιβαίνει στην υπόθεση. Άρα ο n είναι ελεύθερος τετραγώνων.
«(γ′) ⇒ (α′)» Η ανάλυση τού n σε γινόμενο δυνάμεων, ανά δύο διαφορετικών, πρώτων αριθμών p_i είναι η $n = p_1 p_2 \ldots p_s$, διότι ο n είναι ελεύθερος τετραγώνων. Κάθε αβελιανή ομάδα G τάξης n είναι ισόμορφη προς το εξωτερικό ευθύ γινόμενο των Sylow υποομάδων της, βλ. Πρόταση 4.2.1. Για κάθε $i, 1 \leq i \leq s$, η p_i-Sylow υποομάδα $\mathcal{P}_i$ τής G είναι ισόμορφη προς την κυκλική ομάδα C_{p_i}, διότι η τάξη τής $\mathcal{P}_i$ είναι ίση με τον πρώτο αριθμό p_i. Επομένως κάθε αβελιανή ομάδα G τάξης n είναι ισόμορφη προς το εξωτερικό ευθύ γινόμενο, $C_{p_1} \times C_{p_2} \times \cdots \times C_{p_s}$.

Προτεινόμενες Ασκήσεις

ΠΑ 120. Έστω ότι $(G, \star)$ είναι μια αβελιανή ομάδα τάξης 36. Να δειχθούν τα εξής:

(α′) Κάθε στοιχείο $g \in G$, εκφράζεται ως $g = g_1 g_2$, όπου η τάξη τού $g_1 \in G$ είναι ένας διαιρέτης τού 4 και η τάξη τού $g_2 \in G$ είναι ένας διαιρέτης τού 9.

(β′) Η ομάδα G ισούται με το εσωτερικό ευθύ γινόμενο των υποομάδων της H και K, όπου η H είναι η 2-Sylow υποομάδα τής G και η K είναι η 3-Sylow υποομάδα τής G.

ΠΑ 121. Πόσες κλάσεις ισομορφίας αβελιανών ομάδων τάξης 1024 υπάρχουν;

ΠΑ 122. Να βρεθούν όλες οι κλάσεις ισομορφίας αβελιανών ομάδων

(α′) τάξης 108,

(β′) τάξης 200,

(γ′) τάξης 900.

ΠΑ 123. Να δειχθεί ότι (με ακρίβεια ισομορφίας) υπάρχουν μόνο δύο αβελιανές ομάδες τάξης 108, που έχουν ακριβώς μία κυκλική υποομάδα τάξης 3.

ΠΑ 124. Να δειχθεί ότι (με ακρίβεια ισομορφίας) υπάρχουν μόνο δύο αβελιανές ομάδες τάξης 108, που έχουν ακριβώς τέσσερεις κυκλικές υποομάδες τάξης 3.

ΠΑ 125. Να δειχθεί ότι (με ακρίβεια ισομορφίας) υπάρχουν μόνο δύο αβελιανές ομάδες τάξης 108, που έχουν ακριβώς δεκατρείς κυκλικές υποομάδες τάξης 3.

ΠΑ 126. Έστω ότι $(G, \star)$ είναι μια αβελιανή ομάδα τάξης 120, η οποία έχει ακριβώς τρία στοιχεία τάξης 2. Να βρεθεί η κλάση ισομορφίας τής G.

ΠΑ 127. Το σύνολο $\{[1]_{91}, [9]_{91}, [16]_{91}, [22]_{91}, [29]_{91}, [53]_{91}, [74]_{91}, [79]_{91}, [81]_{91}\}$ των κλάσεων ισοτιμίας mod 91 αποτελεί μια ομάδα με πράξη τον πολλαπλασιασμό κατά μόδιο (μέτρο) 91. Να βρεθεί η κλάση ισομορφίας τής δοσμένης ομάδας.

ΠΑ 128. Να εκφραστούν ως εσωτερικό ευθύ γινόμενο κυκλικών υποομάδων με τάξεις δυνάμεις πρώτων, οι ακόλουθες ομάδες:

(α′) $(\mathbb{U}_{20}, \cdot)$,

(β′) $(\mathbb{U}_{54}, \cdot)$,

(γ′) $(\mathbb{U}_{70}, \cdot)$,

(δ′) $(\mathbb{U}_{180}, \cdot)$.

ΠΑ 129. Έστω ότι η ομάδα $(G, \star)$ είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της H και K και ότι η H είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της L και M. Να δειχθεί ότι ότι η G είναι το εσωτερικό ευθύ γινόμενο των υποομάδων της L, M και K.

ΠΑ 130. Έστω το εξωτερικό ευθύ γινόμενο $C_p \times C_p \times \cdots \times C_p$ από n το πλήθος αντίγραφα τής κυκλικής ομάδας C_p τάξης p, όπου ο p είναι πρώτος αριθμός. Πόσα στοιχεία τάξης p έχει αυτό το εξωτερικό ευθύ γινόμενο;

ΠΑ 131. Έστω ότι $(G, \star)$ είναι μια αβελιανή ομάδα, η οποία είναι το εσωτερικό ευθύ γινόμενο δύο υποομάδων της H και K, όπου η H είναι τάξης 5^2 και η K είναι τάξης 7^2. Να υπολογιστεί το πλήθος των στοιχείων τής ομάδας αυτομορφισμών $\mathrm{Aut}(G)$ τής G.
(Υπόδειξη: Βλ. Άσκηση Α88.)

Κεφάλαιο 5

Το Θεώρημα Jordan–Hölder

5.1 Προκαταρκτικές Έννοιες

5.1.1 Υποορθόθετες και ορθόθετες Σειρές για μια Ομάδα

Ορισμός 5.1.1. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = \{e_G\} \tag{*}$$

είναι μια πεπερασμένη ακολουθία υποομάδων τής G.

Η ακολουθία (*) ονομάζεται μια *υποορθόθετη σειρά* για την G, αν $\forall i, i \in \{1, 2, \ldots, r\}$ είναι $G_i \trianglelefteq G_{i-1}$, δηλαδή αν $\forall i, i \in \{1, 2, \ldots, r\}$ η G_i είναι ορθόθετη υποομάδα τής G_{i-1}.

Η ακολουθία (*) ονομάζεται μια *ορθόθετη σειρά* για την G, αν $\forall i, i \in \{1, 2, \ldots, r\}$ είναι $G_i \trianglelefteq G$, δηλαδή αν $\forall i, i \in \{1, 2, \ldots, r\}$ η G_i είναι ορθόθετη υποομάδα τής G.

Οι υποομάδες $G_i, i \in \{1, 2, \ldots, r\}$ ονομάζονται οι *όροι* τής σειράς. Οι πηλικοομάδες $G_i/G_{i+1}, 0 \leq i \leq r-1$ ονομάζονται οι *παράγοντες* τής σειράς.

Λέμε ότι μια υποορθόθετη (αντιστοίχως ορθόθετη) σειρά (*), *δεν διαθέτει επαναλήψεις* αν, για κάθε $i, 1 \leq i \leq r-1$, η G_i περιέχει γνήσια την G_{i+1}, διαφορετικά λέμε ότι η (*) *διαθέτει επαναλήψεις*..

Προφανώς, κάθε ορθόθετη σειρά για την G είναι και μια υποορθόθετη σειρά για την G. Ωστόσο, κάθε υποορθόθετη σειρά για μια ομάδα δεν είναι απαραίτητο να αποτελεί και μια ορθόθετη σειρά για την G.

Παράδειγμα 5.1.2. (α′) Έστω $G = \langle x \rangle$ μια κυκλική ομάδα. Οι σειρές

$$G \geq \langle x^2 \rangle \geq \{e_G\} \text{ και } G \geq \langle x^3 \rangle \geq \{e_G\}$$

είναι υποορθόθετες και ταυτοχρόνως ορθόθετες σειρές για την G.

Γενικότερα, κάθε πεπερασμένη ακολουθία

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = \{e_G\}$$

υποομάδων μιας αβελιανής ομάδας G είναι μια υποορθόθετη και ταυτοχρόνως μια ορθόθετη σειρά για την G.

(β′) Θεωρούμε την εναλλάσσουσα υποομάδα $\mathbb{A}_4$ τής συμμετρικής ομάδας $(S_4, \circ)$ και την ακολουθία
$$\mathbb{A}_4 \geq V \geq H \geq \{\mathrm{Id}_4\}, \tag{**}$$
όπου $V = \{\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}\}$ και $H = \{\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}\}$.

Η V είναι ορθόθετη υποομάδα τής S_4 επειδή είναι ένωση τής κλάσης συζυγίας τού στοιχείου Id_4 και τής κλάσης συζυγίας τού στοιχείου $\begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}$. Η V είναι υποομάδα τής $\mathbb{A}_4$ και ως εκ τούτου, η V είναι ορθόθετη υποομάδα τής $\mathbb{A}_4$, βλ. και Άσκηση Α102.

Η H είναι ορθόθετη υποομάδα τής V, αφού η V είναι αβελιανή. Ωστόσο, η H δεν είναι ορθόθετη υποομάδα τής $\mathbb{A}_4$, αφού το στοιχείο
$$\begin{pmatrix}1 & 2 & 3\end{pmatrix} \circ \left(\begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}\right) \circ \begin{pmatrix}1 & 2 & 3\end{pmatrix}^{-1} = \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix} \notin H.$$
Επομένως, η (**) είναι μια υποορθόθετη σειρά για την $\mathbb{A}_4$, η οποία δεν είναι ορθόθετη.

Ορισμός 5.1.3. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι
$$G = K_0 \geq K_1 \geq \cdots \geq K_r = \{e_G\} \tag{I}$$
$$G = H_0 \geq H_1 \geq \cdots \geq H_s = \{e_G\} \tag{II}$$
είναι δύο υποορθόθετες (αντιστοίχως ορθόθετες) σειρές για την G.

Η σειρά (II) ονομάζεται μια *υποορθόθετη* (αντιστοίχως *ορθόθετη*) *εκλέπτυνση* τής (I), αν, η οικογένεια $\{K_0, K_1, \ldots, K_r\}$ των όρων τής (I) περιέχεται στην οικογένεια $\{H_0, H_1, \ldots, H_s\}$ των όρων τής (II).

Παράδειγμα 5.1.4. Έστω η κυκλική ομάδα $G = \langle x \rangle$ τάξης 48 και οι ορθόθετες σειρές
$$G = \langle x \rangle \geq \langle x^6 \rangle \geq \langle x^{24} \rangle \geq \{e_G\}, \tag{*}$$
$$G = \langle x \rangle \geq \langle x^3 \rangle \geq \langle x^6 \rangle \geq \langle x^{12} \rangle \geq \langle x^{24} \rangle \geq \{e_G\}, \tag{**}$$
$$G = \langle x \rangle \geq \langle x^2 \rangle \geq \langle x^6 \rangle \geq \langle x^{12} \rangle \geq \{e_G\}, \tag{***}$$
Η (**) αποτελεί εκλέπτυνση τής (*). Η (***) δεν αποτελεί εκλέπτυνση τής (*) και η (**) δεν αποτελεί εκλέπτυνση τής (***).

Ορισμός 5.1.5. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι
$$G = K_0 \geq K_1 \geq \cdots \geq K_r = \{e_G\} \tag{I}$$
$$G = H_0 \geq H_1 \geq \cdots \geq H_s = \{e_G\} \tag{II}$$
είναι δύο υποορθόθετες (αντιστοίχως ορθόθετες) σειρές για την G.

Οι υποορθόθετες (αντιστοίχως ορθόθετες) σειρές (I) και (II) ονομάζονται *ισόμορφες* αν, υπάρχει μια «1−1» και «επί» αντιστοιχία φ από την οικογένεια $(K_i/K_{i+1}, 0 \leq i \leq r-1)$ των παραγόντων τής (I) στην οικογένεια $(H_j/H_{j+1}, 0 \leq j \leq s-1)$ των παραγόντων τής (II), τέτοια ώστε $\forall i, 0 \leq i \leq r-1$ ο παράγοντας (K_i/K_{i+1}) να είναι ισόμορφος (ως ομάδα) με τον παράγοντα $\varphi(K_i/K_{i+1})$

Προσέξτε ότι όταν οι υποορθόθετες ή οι ορθόθετες σειρές είναι ισοδύναμες, τότε η προηγούμενη «1 − 1» και «επί» αντιστοιχία φ, εξασφαλίζει ότι $r = s$.

Παράδειγμα 5.1.6. Έστω η κυκλική ομάδα $G = \langle x \rangle$ τάξης 12 και οι ορθόθετες σειρές

$$G = \langle x \rangle \geq \langle x^2 \rangle \geq \langle x^4 \rangle \geq \{e_G\}, \qquad (*)$$
$$G = \langle x \rangle \geq \langle x^3 \rangle \geq \langle x^6 \rangle \geq \{e_G\}. \qquad (**)$$

Η (*) είναι ισόμορφη τής (**), αφού η οικογένεια των παραγόντων τής (*) είναι το

$$\big(\langle x \rangle/\langle x^2 \rangle \cong \mathbb{Z}_2,\ \ \langle x^2 \rangle/\langle x^4 \rangle \cong \mathbb{Z}_2,\ \ \langle x^4 \rangle/\{e_G\} \cong \mathbb{Z}_3\big)\,.$$

και η οικογένεια των παραγόντων τής (**) είναι το

$$\big(\langle x \rangle/\langle x^3 \rangle \cong \mathbb{Z}_3,\ \ \langle x^3 \rangle/\langle x^6 \rangle \cong \mathbb{Z}_2,\ \ \langle x^6 \rangle/\{e_G\} \cong \mathbb{Z}_2\big)\,.$$

5.2 Το Θεώρημα Εκλέπτυνσης Schreier

Θα αποδείξουμε ότι δύο οποιεσδήποτε υποορθόθετες (αντιστοίχως ορθόθετες) σειρές μιας ομάδας διαθέτουν ισόμορφες εκλεπτύνσεις.

5.2.1 Το Λήμμα τής Πεταλούδας

Αρχίζουμε με το εξής πολύ απλό:

Λήμμα 5.2.1. *Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι A, B, C είναι υποομάδες τής G με την $B \trianglelefteq C$ ορθόθετη υποομάδα τής C. Τότε*

(α′) *η $A \bigcap B$ είναι ορθόθετη υποομάδα τής $A \bigcap C$,*

(β′) *επιπλέον αν $A \trianglelefteq G$, τότε η AB είναι υποομάδα τής AC και μάλιστα $AB \trianglelefteq AC$.*

Απόδειξη. (α′) Έστω ότι $x \in A \bigcap C$ και $y \in A \bigcap B$. Τότε $xyx^{-1} \in A$ και $xyx^{-1} \in$ B, αφού $B \trianglelefteq C$. Επομένως, $A \bigcap B \trianglelefteq A \bigcap C$.

(β′) Αφού η A είναι ορθόθετη υποομάδα τής G, οι AB και AC είναι υποομάδες τής G και προφανώς $AB \leq AC$. Υπολείπεται η απόδειξη ότι $AB \trianglelefteq AC$.
Θα αποδείξουμε ότι για κάθε $a \in A, c \in C$ είναι $(ac)AB(ac)^{-1} = AB$. Έχουμε:

$$(ac)AB(ac)^{-1} = ((ac)A)Bc^{-1}a^{-1} = ((Aa)c)Bc^{-1}a^{-1} = A(cBc^{-1})a^{-1} =$$
$$(AB)a^{-1} = B(Aa^{-1}) = BA = AB,$$

αφού $\forall x \in G, xA = Ax$ και $\forall c \in C, cB = Bc$. □

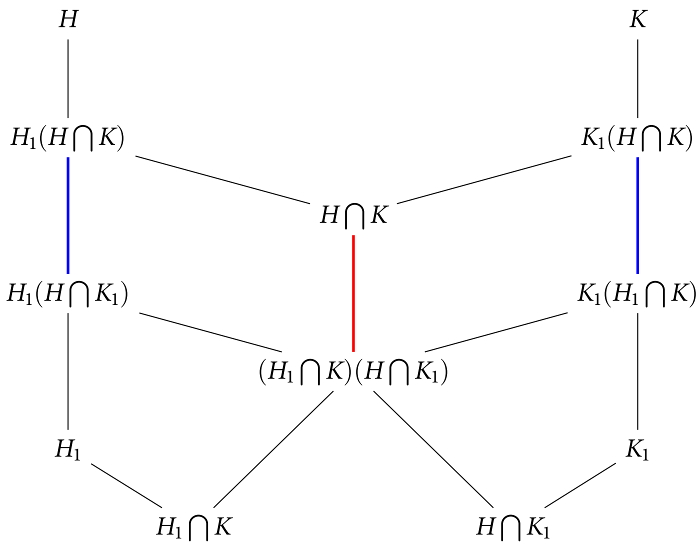
Λήμμα 5.2.2 (Το Λήμμα Πεταλούδας τού Zassenhaus). *Έστω ότι H_1, H και K_1, K είναι υποομάδες μιας ομάδας $(G, \star)$ με $H_1 \trianglelefteq H$ και $K_1 \trianglelefteq K$. Τότε*

$$H_1(H\bigcap K_1) \trianglelefteq H_1(H\bigcap K)$$
$$K_1(K\bigcap H_1) \trianglelefteq K_1(K\bigcap H)$$

και υπάρχει ένας ισομορφισμός

$$\frac{H_1(H\bigcap K)}{H_1(H\bigcap K_1)} \cong \frac{K_1(K\bigcap H)}{K_1(K\bigcap H_1)}$$

Απόδειξη. Θεωρούμε το επόμενο διάγραμμα υποομάδων τής G, στο οποίο όταν δύο υποομάδες συνδέονται με ένα ευθύγραμμο τμήμα, τότε αυτή που βρίσκεται στο χαμηλότερο άκρο τού ευθύγραμμου τμήματος είναι υποομάδα εκείνης που βρίσκεται στο υψηλότερο άκρο.



Παρατηρούμε ότι επειδή $K_1 \trianglelefteq K \leq G$ και $H \leq G$ έπεται, από το Λήμμα 5.2.1(α′), ότι $H\bigcap K_1 \trianglelefteq H\bigcap K$ και παρομοίως συμπεραίνουμε ότι $K\bigcap H_1 \trianglelefteq K\bigcap H$.
Τώρα επειδή $H\bigcap K_1 \trianglelefteq H\bigcap K \leq H$ και $H_1 \trianglelefteq H$, έπεται, από το Λήμμα 5.2.1(β′), ότι $H_1(H\bigcap K_1) \trianglelefteq H_1(H\bigcap K)$.

Εντελώς ανάλογα αποδεικνύεται ότι $K_1(K\bigcap H_1) \trianglelefteq K_1(K\bigcap H)$.
Επειδή $H_1\bigcap K \trianglelefteq H\bigcap K$ και $H\bigcap K_1 \trianglelefteq H\bigcap K$, συμπεραίνουμε ότι $(H_1\bigcap K)(H\bigcap K_1) \trianglelefteq H\bigcap K$.

Θα δείξουμε ότι

$$(H_1\bigcap K)(H\bigcap K_1) = (H\bigcap K)\bigcap[H_1(H\bigcap K_1)]. \tag{*}$$

Αφού $(H_1 \bigcap K) \leq H_1$ έπεται $(H_1 \bigcap K)(H \bigcap K_1) \leq H_1(H \bigcap K_1)$. Αφού $H_1 \bigcap K \leq H \bigcap K$ και $H \bigcap K_1 \leq H \bigcap K$ έπεται $(H_1 \bigcap K)(H \bigcap K_1) \leq H \bigcap K$. Συνεπώς,

$$(H_1 \bigcap K)(H \bigcap K_1) \leq (H \bigcap K) \bigcap [H_1(H \bigcap K_1)].$$

Υπολείπεται η απόδειξη ότι

$$(H \bigcap K) \bigcap [H_1(H \bigcap K_1)] \leq (H_1 \bigcap K)(H \bigcap K_1).$$

Έστω $\alpha \in (H \bigcap K) \bigcap [H_1(H \bigcap K_1)]$. Τότε $\alpha \in H \bigcap K$ και $\alpha \in H_1(H \bigcap K_1)$. Επομένως, $\alpha = \beta\gamma$ με $\beta \in H_1$, $\gamma \in H \bigcap K_1$. Επομένως, το $\beta = \gamma^{-1}\alpha$ ανήκει στο $H_1 \bigcap K$ και γι' αυτό το α ανήκει στο $(H_1 \bigcap K)(H \bigcap K_1)$.

Θέτοντας $A = H \bigcap K$ και $B = H_1(H \bigcap K_1)$, διαπιστώνουμε ότι

$$AB = [(H \bigcap K)H_1](H \bigcap K_1) = [H_1(H \bigcap K)](H \bigcap K_1) = H_1[(H \bigcap K)(H \bigcap K_1)] = H_1(H \bigcap K),$$

αφού $H_1 \trianglelefteq H$ και $H \bigcap K_1 \leq H \bigcap K$.

Θεωρούμε την πηλικοομάδα

$$\frac{H_1(H \bigcap K)}{H_1(H \bigcap K_1)} = \frac{AB}{B},$$

η οποία είναι, ως γνωστόν, ισόμορφη προς την

$$\frac{A}{A \bigcap B} = \frac{H \bigcap K}{(H \bigcap K) \bigcap [H_1(H \bigcap K_1)]} = \frac{H \bigcap K}{(H_1 \bigcap K)(H \bigcap K_1)},$$

αφού, λόγω τής (*), $(H_1 \bigcap K)(H \bigcap K_1) = (H \bigcap K) \bigcap [H_1(H \bigcap K_1)]$.

Χρησιμοποιώντας την αριστερή πλευρά τού σχήματος τής πεταλούδας αποδείξαμε ότι

$$\frac{H_1(H \bigcap K)}{H_1(H \bigcap K_1)} \cong \frac{H \bigcap K}{(H_1 \bigcap K)(H \bigcap K_1)}.$$

Εντελώς ανάλογα, χρησιμοποιώντας τη δεξιά πλευρά τού σχήματος τής πεταλούδας αποδεικνύεται ότι

$$\frac{K_1(K \bigcap H)}{K_1(K \bigcap H_1)} \cong \frac{H \bigcap K}{(H_1 \bigcap K)(H \bigcap K_1)}$$

και γι' αυτό τελικά παίρνουμε

$$\frac{H_1(H \bigcap K)}{H_1(H \bigcap K_1)} \cong \frac{K_1(K \bigcap H)}{K_1(K \bigcap H_1)}.$$

□

Θεώρημα 5.2.3 (Το Θεώρημα Εκλέπτυνσης τού Schreier). *Δύο οποιεσδήποτε υποορθόθετες (αντιστοίχως ορθόθετες) σειρές μιας ομάδας $(G, \star)$ διαθέτουν ισόμορφες εκλεπτύνσεις.*

Απόδειξη. Έστω ότι

$$G = K_0 \geq K_1 \geq \cdots \geq K_i \geq K_{i+1} \geq \cdots \geq K_r = \{e_G\} \tag{I}$$
$$G = H_0 \geq H_1 \geq \cdots \geq H_j \geq H_{j+1} \geq \cdots \geq H_s = \{e_G\} \tag{II}$$

είναι δύο υποορθόθετες (αντιστοίχως ορθόθετες) σειρές τής ομάδας G.

Θα εκλεπτύνουμε την (I) σε μια νέα υποορθόθετη σειρά (I′).
Ορίζουμε $K_{i,j} = (K_i \bigcap H_j)K_{i+1}, 0 \leq j \leq s, 0 \leq i \leq r-1$ και παρατηρούμε ότι $K_{i,j} \leq K_i$, αφού $K_{i+1} \trianglelefteq K_i$ και $K_i \bigcap H_j \leq K_i$. Επιπλέον,

$$\begin{aligned}
&K_{i,0} = (K_i \bigcap H_0)K_{i+1} = K_i,\\
&K_{i,j} = (K_i \bigcap H_j)K_{i+1} \geq K_{i,j+1} = (K_i \bigcap H_{j+1})K_{i+1}, \forall j 0 \leq j \leq s\\
&\text{και } K_{i,s} = (K_i \bigcap H_s)K_{i+1} = K_{i+1} = K_{i+1,0}.
\end{aligned}$$

Έτσι επιτυγχάνουμε μια εκλέπτυνση τής (I)

$$K_i = K_{i,0} \geq K_{i,1} \geq \cdots \geq K_{i,s} = K_{i+1}$$

μεταξύ των όρων K_i και K_{i+1}.

Παρατηρούμε ακόμη ότι για i με $0 \leq i \leq r-2$, έχουμε $K_{i,s} = (K_i \bigcap H_s)K_{i+1} = K_{i+1} = K_{i+1,0}$, και γι’ αυτό μπορούμε να παραλείψουμε τους όρους $K_{i,s}$. Έτσι το πλήθος των όρων $K_{i,j}$ τής (I′) ισούται με το άθροισμα $(r-1)s$ όρων (όταν $0 \leq i \leq r-2$) συν $(s+1)$ όρων (όταν $i = r-2$). Δηλαδή, η (I′) διαθέτει συνολικά $rs+1$ όρους.

Τώρα εργαζόμενοι παρομοίως εκλεπτύνουμε την (II) σε μια νέα υποορθόθετη σειρά (II′). Ορίζουμε $H_{i,j} = (H_j \bigcap K_i)H_{j+1}, 0 \leq i \leq r, 0 \leq j \leq s-1$ και παρατηρούμε ότι $H_{i,j} \leq H_j$, αφού $H_{j+1} \trianglelefteq H_j$ και $H_j \bigcap K_i \leq H_j$. Επιπλέον,

$$\begin{aligned}
&H_{0,j} = (H_j \bigcap K_0)H_{j+1} = H_j,\\
&H_{i,j} = (H_j \bigcap K_i)H_{j+1} \geq H_{i+1,j} = (H_j \bigcap K_{i+1})H_{j+1}\\
&\text{και } H_{r,j} = (H_j \bigcap K_r)H_{j+1} = H_{j+1} = H_{0,j+1}.
\end{aligned}$$

Έτσι επιτυγχάνουμε μια εκλέπτυνση τής (II)

$$H_j = H_{0,j} \geq H_{1,j} \geq \cdots \geq H_{r,j} = H_{j+1}$$

μεταξύ των όρων H_j και H_{j+1}.

Παρατηρούμε ακόμη ότι για j με $0 \leq j \leq s-2$, έχουμε $H_{r,j} = (H_j \bigcap K_r)H_{j+1} = H_{j+1} = H_{0,j+1}$ και γι’ αυτό μπορούμε να παραλείψουμε τους όρους $H_{r,j}$. Έτσι το πλήθος των όρων $H_{i,j}$ τής (II′) ισούται με το άθροισμα $(s-1)r$ όρων (όταν $0 \leq j \leq s-2$) συν $(r+1)$ όρων (όταν $j = s-1$). Δηλαδή, η (II′) διαθέτει συνολικά $sr+1$ όρους.

Συνεπώς, οι δύο εκλεπτύνσεις διαθέτουν το ίδιο πλήθος όρων.

Τέλος παρατηρούμε ότι, λόγω τού Λήμματος τής Πεταλούδας, βλ. Λήμμα 5.2.2, οι (I′) και (II′) είναι ισόμορφες, αφού

$$\forall i, 0 \leq i \leq r-1, \text{ και } \forall j, 0 \leq j \leq s-1 \text{ είναι } \frac{K_{i,j}}{K_{i,j+1}} \cong \frac{H_{i,j}}{H_{i,j+1}}.$$

Στην περίπτωση που οι αρχικές σειρές (I) και (II) ήταν ορθόθετες, τότε και οι εκλεπτύνσεις τους (I′) και (II′) είναι επίσης ορθόθετες, επειδή οι υποομάδες $K_{i,j} = (K_i \bigcap H_j)K_{i+1}$ και $H_{i,j} = (H_j \bigcap K_i)H_{j+1}$ είναι ορθόθετες υποομάδες τής G, αφού οι $K_i \bigcap H_j, K_{i+1}, H_j \bigcap K_i, H_{j+1}$ είναι για κάθε i και j, ορθόθετες υποομάδες τής G. □

Παράδειγμα 5.2.4. Θεωρούμε την κυκλική ομάδα $(\mathbb{Z}, +)$ και τις ορθόθετες σειρές

$$\mathbb{Z} \geq \langle 2 \rangle \geq \langle 4 \rangle \geq \{0\},$$
$$\mathbb{Z} \geq \langle 5 \rangle \geq \langle 10 \rangle \geq \{0\}.$$

Οι δύο προηγούμενες σειρές διαθέτουν αντιστοίχως τις επόμενες εκλεπτύνσεις

$$\mathbb{Z} \geq \langle 2 \rangle \geq \langle 4 \rangle \geq \langle 20 \rangle \geq \langle 40 \rangle \geq \{0\},$$
$$\mathbb{Z} \geq \langle 5 \rangle \geq \langle 10 \rangle \geq \langle 20 \rangle \geq \langle 40 \rangle \geq \{0\}.$$

Οι συγκεκριμένες εκλεπτύνσεις είναι ισόμορφες, αφού η οικογένεια παραγόντων τής πρώτης είναι η $(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_5, \mathbb{Z}_2, \mathbb{Z})$ και η οικογένεια παραγόντων τής δεύτερης είναι η $(\mathbb{Z}_5, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z})$

Ορισμός 5.2.5. Μια *συνθετική σειρά* (αντιστοίχως *κυρίαρχη σειρά*) για μια ομάδα G, είναι μια υποορθόθετη (αντιστοίχως ορθόθετη) σειρά χωρίς επαναλήψεις, τής οποίας κάθε εκλέπτυνση με περισσότερους όρους οφείλει να περιέχει επαναλήψεις.

Οι παράγοντες μια συνθετικής (αντιστοίχως κυρίαρχης) σειράς

$$G = G_0 > G_1 > \cdots > G_r = \{e_G\} \tag{*}$$

ονομάζονται *οι συνθετικοί* (αντιστοίχως *οι κυρίαρχοι*) *παράγοντες* τής (*).

Παρατήρηση 5.2.6. Όπως θα δούμε στο αμέσως επόμενο παράδειγμα, υπάρχουν ομάδες που δεν διαθέτουν ούτε συνθετικές ούτε κυρίαρχες σειρές.
Ωστόσο, κάθε πεπερασμένη ομάδα διαθέτει και συνθετικές και κυρίαρχες σειρές, αφού οποιαδήποτε εκλέπτυνση χωρίς επαναλήψεις τής σειράς $G \geq \{e_G\}$ οφείλει να περατώνεται κατόπιν ενός πεπερασμένου πλήθους βημάτων.

Παράδειγμα 5.2.7. (α′) Η άπειρη κυκλική ομάδα $(\mathbb{Z}, +)$ δεν διαθέτει ούτε συνθετικές ούτε κυρίαρχες σειρές.

Έστω ότι η

$$\mathbb{Z} = \langle 1 \rangle > \langle n_1 \rangle > \langle n_2 \rangle > \cdots > \langle n_s \rangle > \{0\}, n_i \in \mathbb{N}, \forall i, i = 1, 2, \ldots, s. \tag{*}$$

είναι μια υποορθόθετη και συνεπώς ορθόθετη σειρά χωρίς επαναλήψεις για την άπειρη κυκλική ομάδα $\mathbb{Z}$. Τότε η

$$\mathbb{Z} = \langle 1 \rangle > \langle n_1 \rangle > \langle n_2 \rangle > \cdots > \langle n_s \rangle > \langle 2n_s \rangle > \{0\}$$

είναι μια εκλέπτυνση τής (*) χωρίς επαναλήψεις.
Γι' αυτό καμιά υποορθόθετη και συνεπώς ορθόθετη σειρά για την ομάδα $\mathbb{Z}$ δεν είναι ούτε συνθετική ούτε κυρίαρχη.

(β′) Η σειρά

$$\mathbb{Z}_{12} = \langle [1]_{12} \rangle > \langle \langle [3]_{12} \rangle > \langle [6]_{12} \rangle > \{0\}$$

είναι κυρίαρχη και προφανώς συνθετική, αφού πρόκειται για μια ορθόθετη σειρά, όπου οι τάξεις των παραγόντων της είναι

$$[\langle [1]_{12} \rangle : \langle [3]_{12} \rangle] = 3, \quad [\langle [3]_{12} \rangle : \langle [6]_{12} \rangle] = 2, \quad [\langle [6]_{12} \rangle : \{0\} \rangle] = 2. \qquad (*)$$

Αφού η τάξη κάθε παράγοντα είναι πρώτος αριθμός είναι προφανές ότι κάθε γνήσια εκλέπτυνση τής (*) οφείλει να περιέχει επαναλήψεις.

(γ′) Η υποορθόθετη σειρά τής $\mathbb{A}_4$

$$\mathbb{A}_4 \geq V \geq H \geq \{\mathrm{Id}_4\}, \qquad (**)$$

βλ. Παράδειγμα 5.1.2(β′), είναι μια συνθετική σειρά. Πράγματι, για τις τάξεις των παραγόντων τής σειράς έχουμε

$$[\mathbb{A}_4 : V] = 3, \quad [V : H] = 2, \quad [H : \mathrm{Id}_4] = 2.$$

Αφού λοιπόν αυτές οι τάξεις είναι πρώτοι αριθμοί, έπεται ότι κάθε γνήσια εκλέπτυνση τής (**) οφείλει να περιέχει επαναλήψεις.

Θεώρημα 5.2.8 (Το Θεώρημα Jordan–Hölder). *Όταν μια ομάδα $(G, \star)$ διαθέτει συνθετικές (αντιστοίχως κυρίαρχες) σειρές, τότε αυτές είναι ισόμορφες.*

Απόδειξη. Έστω ότι

$$G = K_0 \geq K_1 \geq \cdots \geq K_i \geq K_{i+1} \geq \cdots \geq K_r = \{e_G\} \qquad (\mathrm{I})$$
$$G = H_0 \geq H_1 \geq \cdots \geq H_j \geq H_{j+1} \geq \cdots \geq H_s = \{e_G\} \qquad (\mathrm{II})$$

είναι δύο συνθετικές (αντιστοίχως κυρίαρχες) σειρές τής ομάδας G. Σύμφωνα με το Θεώρημα Schreier, βλ. Θεώρημα 5.2.3, οι συγκεκριμένες σειρές διαθέτουν ισόμορφες εκλεπτύνσεις. Αφού όμως είναι συνθετικές (αντιστοίχως κυρίαρχες) σειρές, κάθε εκλέπτυνσή τους οφείλει να διαθέτει επαναλήψεις. Επομένως, οι (I) και (II) ήταν εξαρχής ισόμορφες, γεγονός που αποδεικνύει τον ισχυρισμό τού θεωρήματος. □

Ιδιαιτέρως, δύο συνθετικές (αντιστοίχως κυρίαρχες) σειρές μιας ομάδας G έχουν πάντοτε το ίδιο πλήθος παραγόντων, το οποίο ονομάζουμε το *μήκος τής συνθετικής* (αντιστοίχως κυρίαρχης) σειράς.

Παράδειγμα 5.2.9. Στο Παράδειγμα 5.2.7(β′) διαπιστώσαμε ότι η

$$\mathbb{Z}_{12} = \langle [1]_{12} \rangle > \langle \langle [3]_{12} \rangle > \langle [6]_{12} \rangle > \{0\}$$

είναι μια κυρίαρχη και προφανώς συνθετική σειρά, τής οποίας η οικογένεια των συνθετικών παραγόντων της είναι η

$$(\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_2).$$

Παρατηρούμε ότι και η

$$\mathbb{Z}_{12} = \langle [1]_{12} \rangle > \langle \langle [2]_{12} \rangle > \langle [4]_{12} \rangle > \{0\}$$

είναι ακόμη μία κυρίαρχη και συνθετική σειρά. Η οικογένεια των συνθετικών παραγόντων της είναι η

$$(\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3)$$

και προφανώς οι συνθετικές και κυρίαρχες σειρές είναι ισόμορφες.

5.3 Συνθετικοί και κυρίαρχοι Παράγοντες

5.3.1 Περιγραφή συνθετικών ή κυρίαρχων Παραγόντων

Πρόταση 5.3.1. *Έστω ότι $(G, \star)$ είναι μια ομάδα με $[G : 1] > 1$. Αν η*

$$G = G_0 > G_1 > \cdots > G_i > G_{i+1} > \cdots > G_r = \{e_G\} \tag{*}$$

είναι μια συνθετική σειρά για την G, τότε για κάθε i, $0 \leq i \leq r-1$, ο συνθετικός παράγοντας G_i/G_{i+1} είναι απλή ομάδα.

Απόδειξη. Ας υποθέσουμε ότι για κάποιον δείκτη $i \in \{0, 1, \ldots, r-1\}$ η G_i/G_{i+1} δεν είναι απλή. Τότε θα υπήρχε μια γνήσια και ορθόθετη υποομάδα H τής G_i/G_{i+1}, η οποία θα περιείχε γνησίως την τετριμμένη υποομάδα G_{i+1}/G_{i+1}. Συνεπώς, θα υπήρχε μια γνήσια και ορθόθετη υποομάδα N τής G_i, η οποία θα περιείχε γνησίως την G_{i+1} με $N/G_{i+1} = H$ και ακόμα, η G_{i+1} θα ήταν ορθόθετη υποομάδα τής H, αφού $G_{i+1} \trianglelefteq G_i$. Όμως τότε η υποορθόθετη σειρά

$$G = G_0 > G_1 > \cdots > G_i > H > G_{i+1} > \cdots > G_r = \{e_G\}$$

θα ήταν μια εκλέπτυνση τής $(*)$ χωρίς επαναλήψεις και με περισσότερους όρους. Αυτό είναι αδύνατο αφού, η $(*)$ είναι μια συνθετική σειρά.
Επομένως, κάθε συνθετικός παράγοντας G_i/G_{i+1}, $i \in \{0, 1, \ldots, r-1\}$ είναι μια απλή ομάδα. □

Πρόταση 5.3.2. *Οι συνθετικοί παράγοντες μια πεπερασμένης αβελιανής ομάδας $(G, \star)$ είναι κυκλικές ομάδες πρώτης τάξης.*

Απόδειξη. Οι συνθετικοί παράγοντες είναι πεπερασμένες αβελιανές και απλές ομάδες. Από την Πρόταση 3.2.17, συμπεραίνουμε ότι οι συνθετικοί παράγοντες είναι κυκλικές ομάδες πρώτης τάξης. □

Παρατήρηση 5.3.3. Το Θεώρημα Jordan-Hölder μπορεί να θεωρηθεί ως μια γενίκευση τού Θεμελιώδους Θεωρήματος τής Αριθμητικής.
Πράγματι, αν n είναι οποιοσδήποτε φυσικός αριθμός, τότε θεωρούμε την κυκλική ομάδα $(\mathbb{Z}_n, +)$ και μια συνθετική σειρά της:

$$\mathbb{Z}_n = \langle a_0 \rangle > \langle a_1 \rangle > \cdots > \langle a_i \rangle > \langle a_{i+1} \rangle > \cdots > \langle a_r \rangle = \{[0]_n\},$$

Οι τάξεις $[\langle a_i \rangle : \langle a_{i+1} \rangle] = p_{i+1}$ των συνθετικών παραγόντων $\langle a_i \rangle / \langle a_{i+1} \rangle$ είναι πρώτοι αριθμοί, αφού όλοι οι συνθετικοί παράγοντες είναι κυκλικές ομάδες πρώτης τάξης. Παρατηρούμε ότι

$$\prod_1^r p_i = [\langle a_0 \rangle : \langle a_1 \rangle] \cdot [\langle a_1 \rangle : \langle a_2 \rangle] \cdot \ldots \cdot [\langle a_{r-1} \rangle : \langle a_r \rangle] = [\mathbb{Z}_n : 1] = n.$$

Συνεπώς, κάθε συνθετική σειρά τής $\mathbb{Z}_n$ χορηγεί μια ανάλυση τού n σε γινόμενο πρώτων παραγόντων.

Αντίστροφα, κάθε ανάλυση τού n σε γινόμενο πρώτων παραγόντων, ας πούμε $n = \prod_1^s q_i$ χορηγεί τη συνθετική σειρά

$$\begin{aligned} \mathbb{Z}_n = \langle [1]_n \rangle > \langle [q_1]_n \rangle > \langle [q_1 q_2]_n \rangle > \cdots > \langle [q_1 q_2 \ldots q_i]_n \rangle > \langle [q_1 q_2 \ldots q_{i+1}]_n \rangle > \\ > \cdots > \langle [q_1 q_2 \ldots q_s]_n \rangle = \{[0]_n\}, \end{aligned}$$

όπου η τάξη τού συνθετικού παράγοντα $\langle [1]_n \rangle / \langle [q_1]_n \rangle$ ισούται με $(q_1 q_2 \ldots q_s / q_2 \ldots q_s) = q_1$ και οι τάξεις των υπόλοιπων συνθετικών παραγόντων $\langle [q_1 q_2 \ldots q_i]_n \rangle / \langle [q_1 q_2 \ldots q_{i+1}]_n \rangle$ ισούνται με $(q_{i+1} q_{i+2} \ldots q_s / q_{i+2} q_{i+3} \ldots q_s) = q_{i+1}$, $i \in \{1, 2, \ldots, s-1\}$. Αφού όμως οι παράγοντες οποιασδήποτε συνθετικής σειράς είναι μοναδικοί (με ακρίβεια ισομορφίας), έπεται ότι υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ τής οικογένειας των πρώτων $(p_i), i \in \{1, 2, \ldots, r\}$ και τής οικογένειας των πρώτων $(q_j), j \in \{1, 2, \ldots, s\}$ και γι' αυτό η ανάλυση τού n σε γινόμενο πρώτων είναι μοναδική (μέχρι τη σειρά εμφάνισης των παραγόντων).

Ας δούμε τώρα τι συμβαίνει με τους κυρίαρχους παράγοντες.

Ορισμός 5.3.4. Μια ομάδα $(G, \star)$ ονομάζεται *χαρακτηριστικώς απλή* αν, $G \neq \{e_G\}$ και οι μοναδικές χαρακτηριστικές υποομάδες της είναι οι τετριμμένες υποομάδες G και $\{e_G\}$.

Πρόταση 5.3.5. *Έστω ότι $(G, \star)$ είναι μια ομάδα με $[G : 1] > 1$. Αν η*

$$G = G_0 > G_1 > \cdots > G_i > G_{i+1} > \cdots > G_r = \{e_G\} \tag{*}$$

είναι μια κυρίαρχη σειρά για την G, τότε για κάθε $i, 0 \leq i \leq r-1$, ο κυρίαρχος παράγοντας G_i/G_{i+1} είναι μια χαρακτηριστικώς απλή ομάδα.

Απόδειξη. Ας υποθέσουμε ότι για κάποιον δείκτη $i \in \{0, 1, \ldots, r-1\}$ η G_i/G_{i+1} δεν είναι χαρακτηριστικώς απλή. Τότε θα υπήρχε μια γνήσια χαρακτηριστική υποομάδα H τής G_i/G_{i+1}, η οποία θα περιείχε γνησίως την τετριμμένη υποομάδα G_{i+1}/G_{i+1}. Λόγω τής αντιστοιχίας μεταξύ των υποομάδων τής G_i/G_{i+1} και των υποομάδων τής G_i που περιέχουν το G_{i+1}, θα υπήρχε μια γνήσια υποομάδα K τής G_i που θα περιείχε γνησίως την G_{i+1} με $H = K/G_{i+1}$. Αλλά αφού η K/G_{i+1} θα ήταν μια χαρακτηριστική υποομάδα τής G_i/G_{i+1} και αφού η G_i/G_{i+1} είναι ορθόθετη υποομάδα τής G/G_{i+1}, τότε η K/G_{i+1} θα ήταν μια ορθόθετη υποομάδα τής G/G_{i+1}, βλ. Παρατήρηση 3.2.13. Ως εκ τούτου, η K θα ήταν μια γνήσια και ορθόθετη υποομάδα τής G, η οποία θα περιείχε γνησίως την G_{i+1}. Όμως τότε η ορθόθετη σειρά

$$G = G_0 > G_1 > \cdots > G_i > K > G_{i+1} > \cdots > G_r = \{e_G\}$$

θα ήταν μια εκλέπτυνση χωρίς επαναλήψεις, η οποία θα είχε περισσότερους όρους από την κυρίαρχη σειρά $(*)$. Αυτό είναι αδύνατο. Επομένως, κάθε κυρίαρχος παράγοντας G_i/G_{i+1}, $i \in \{0, 1, \ldots, r-1\}$ είναι μια χαρακτηριστικώς απλή ομάδα. □

5.3.2 Οι χαρακτηριστικώς απλές πεπερασμένες Ομάδες

Θεώρημα 5.3.6. *Μια πεπερασμένη και χαρακτηριστικώς απλή ομάδα $(G, \star)$ είναι ένα εσωτερικό ευθύ γινόμενο υποομάδων, οι οποίες είναι όλες απλές και ισόμορφες.*

Απόδειξη. Έστω ότι G_1 είναι μια ορθόθετη υποομάδα τής G με $G_1 \neq \{e_G\}$ με τον μικρότερο αριθμό στοιχείων, δηλαδή αν μια υποομάδα $L \neq \{e_G\}$ τής G έχει λιγότερα από $[G_1 : 1]$ στοιχεία, τότε η L δεν είναι ορθόθετη υποομάδα τής G.
Θεωρούμε τώρα όλα τα εσωτερικά ευθέα γινόμενα τής μορφής $G_1 \cdot G_2 \cdot \ldots \cdot G_s$, όπου $G_i \cong G_1, \forall i, 2 \leq i \leq s$ και μεταξύ αυτών διαλέγουμε μια υποομάδα $H = G_1 \cdot G_2 \cdot \ldots \cdot G_r$, η οποία έχει τον μέγιστο αριθμό στοιχείων. Παρατηρούμε ότι η H είναι μια ορθόθετη υποομάδα τής G, αφού είναι γινόμενο των ορθόθετων υποομάδων $G_i, 1 \leq i \leq r$ τής G.
Ισχυριζόμαστε ότι η H είναι μια χαρακτηριστική υποομάδα τής G. Προφανώς, αρκεί να δείξουμε ότι για κάθε αυτομορφισμό $\varphi \in \mathrm{Aut}(G)$ έχουμε $\varphi(H) \leq H$, αφού τότε $\varphi(H) = H$, διότι τα H και $\varphi(H)$ είναι πεπερασμένα σύνολα με το ίδιο πλήθος στοιχείων.
Παρατηρούμε ότι για να δείξουμε $\forall \varphi \in \mathrm{Aut}(G), \varphi(H) \leq H$, αρκεί να δείξουμε ότι $\forall \varphi \in \mathrm{Aut}(G)$ και $\forall i = 1, 2, \ldots, r, \varphi(G_i) \leq H$, αφού $\varphi(H) = \varphi(G_1 \cdot G_2 \cdot \ldots \cdot G_r) = \varphi(G_1) \cdot \varphi(G_2) \cdot \ldots \cdot \varphi(G_r)$.
Έστω ότι υπάρχουν κάποια $\varphi \in \mathrm{Aut}(G)$ και $j, 1 \leq j \leq r$ τέτοια, ώστε $\varphi(G_j) \nsubseteq H$. Τότε η τομή $\varphi(G_j) \bigcap H$ περιέχεται γνησίως εντός τής $\varphi(G_j)$ και γι' αυτό $[\varphi(G_j) \bigcap H : 1] \lneqq [\varphi(G_j) : 1] = [G_1 : 1]$. Αλλά η $\varphi(G_j)$ είναι ορθόθετη υποομάδα τής G, επειδή η G_j είναι ορθόθετη υποομάδα τής G και έτσι η $\varphi(G_j) \bigcap H$ είναι ορθόθετη υποομάδα τής G, αφού πρόκειται για τομή ορθόθετων υποομάδων. Όμως επειδή η $\varphi(G_j) \bigcap H$ έχει λιγότερα στοιχεία από την G_1 και η G_1 ήταν μια ορθόθετη υποομάδα τής G με τον ελάχιστο αριθμό στοιχείων, συμπεραίνουμε ότι $\varphi(G_j) \bigcap H = \{e_G\}$. Τώρα όμως αμφότερες οι υποομάδες H και $\varphi(G_j)$ είναι ορθόθετες υποομάδες τής G με $\varphi(G_j) \bigcap H = \{e_G\}$ και γι' αυτό το $H \cdot \varphi(G_j)$ είναι ένα ευθύ εσωτερικό γινόμενο με περισσότερα από $[H : 1]$ στοιχεία, όπου μάλιστα η $\varphi(G_j)$ είναι ισόμορφη τής G_1. Αυτό αντίκειται στον τρόπο επιλογής τής H ως μιας τέτοιου είδους υποομάδας με τον μέγιστο αριθμό στοιχείων. Ώστε $\forall \varphi \in \mathrm{Aut}(G)$ και $\forall i = 1, 2, \ldots, r, \varphi(G_i) \leq H$ και έτσι διαπιστώνουμε ότι η H είναι μια χαρακτηριστική υποομάδα τής G.

Αλλά η G είναι μια χαρακτηριστικώς απλή ομάδα και η H είναι μια χαρακτηριστική υποομάδα με $\{e_G\} \lneqq G_1 \leq H$. Επομένως, $H = G$, δηλαδή η G ισούται με το ευθύ εσωτερικό γινόμενο $G_1 \cdot G_2 \cdot \ldots \cdot G_s$, όπου $G_i \cong G_1, \forall i, 2 \leq i \leq s$.

Υπολείπεται η απόδειξη ότι η G_1 (συνεπώς και κάθε $G_i, \forall i, 2 \leq i \leq r$) είναι απλή ομάδα. Έστω ότι $N \trianglelefteq G_1$ είναι μια γνήσια ορθόθετη υποομάδα τής G_1. Ισχυριζόμαστε ότι $\forall g \in G, gN = Ng$ από όπου συμπεραίνουμε ότι η N είναι μια ορθόθετη υποομάδα της G. Πράγματι, αφού $g \in G = G_1 \cdot G_2 \cdot \ldots \cdot G_s$, έπεται ότι $g = g_1 g_2 \ldots g_r$, όπου $g_i \in G_i, \forall i, 1 \leq i \leq r$. Τώρα επειδή η N είναι υποομάδα τής G_1 και επειδή $xy = yx, \forall x \in G_i, y \in G_j$ όταν $i \neq j$, βλ. Πόρισμα 4.1.10, έπεται

$$gN = (g_1 g_2 \ldots g_r)N = g_1(g_2 \ldots g_r N) = g_1(N g_2 \ldots g_r) = (g_1 N) g_2 \ldots g_r =$$
$$(N g_1) g_2 \ldots g_r = N(g_1 g_2 \ldots g_r) = Ng,$$

όπου $g_1 N = N g_1, \forall g_1 \in G_1$, επειδή $N \trianglelefteq G_1$. Ώστε, $N \trianglelefteq G$.

Αλλά τώρα η N οφείλει να ισούται με $\{e_G\}$, αφού η G_1 είναι μια ορθόθετη υποομάδα τής G με τον ελάχιστο αριθμό στοιχείων. Επομένως η G_1 είναι απλή. □

Παρατήρηση 5.3.7. Κάθε πεπερασμένη και χαρακτηριστικώς απλή ομάδα είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο πεπερασμένου πλήθους απλών ισόμορφων ομάδων.

Πόρισμα 5.3.8. *Κάθε πεπερασμένος αβελιανός κυρίαρχος παράγοντας μιας ομάδας, είναι μια στοιχειώδης αβελιανή p–ομάδα, για κάποιον πρώτο αριθμό p.*

Απόδειξη. Κάθε πεπερασμένος αβελιανός κυρίαρχος παράγοντας K είναι μια πεπερασμένη χαρακτηριστικώς απλή αβελιανή ομάδα. Ως εκ τούτου, ο K είναι ισόμορφος προς ένα εξωτερικό ευθύ γινόμενο πεπερασμένου πλήθους απλών ισόμορφων ομάδων, οι οποίες είναι αβελιανές. Αλλά οι απλές αβελιανές ομάδες είναι κυκλικές πρώτης τάξης. Συνεπώς, ο K ι ισόμορφος προς ένα πεπερασμένο εξωτερικό ευθύ γινόμενο $\mathbb{Z}_p \times \ldots \mathbb{Z}_p$, δηλαδή ισόμορφος προς μια στοιχειώδη αβελιανή p–ομάδα. □

Ασκήσεις στο Θεώρημα Jordan–Hölder

Λυμένες Ασκήσεις

Α 130. Να δοθεί παράδειγμα δύο μη ισόμορφων ομάδων που να διαθέτουν ισόμορφες κυρίαρχες σειρές.

Λύση. Θεωρούμε τις μη ισόμορφες ομάδες $\mathbb{Z}_2 \times \mathbb{Z}_2$ και $\mathbb{Z}_4$ και τις αντίστοιχες κυρίαρχες σειρές

$$\mathbb{Z}_2 \times \mathbb{Z}_2 > \mathbb{Z}_2 \times \{[0]_2\} > \{[0]_2\} \times \{[0]_2\},$$
$$\mathbb{Z}_4 > \langle [2]_4 \rangle > \{[0]_4\}.$$

Η οικογένεια των κυρίαρχων παραγόντων τής πρώτης είναι

$$(\ \mathbb{Z}_2 \times \mathbb{Z}_2 / \mathbb{Z}_2 \times \{[0]_2\} \cong \mathbb{Z}_2, \mathbb{Z}_2 \times \{[0]_2\} / \{[0]_2\} \times \{[0]_2\} \cong \mathbb{Z}_2\ )$$

και τής δεύτερης

$$(\mathbb{Z}_4/\langle[2]_4\rangle \cong \mathbb{Z}_2, \langle[2]_4\rangle/\{[0]_4\} \cong \mathbb{Z}_2)\,.$$

Συνεπώς, έχουν ισόμορφες κυρίαρχες σειρές.

Α 131. Να δοθεί παράδειγμα δύο πεπερασμένων ομάδων που να έχουν την ίδια τάξη, αλλά όπου τα μήκη των συνθετικών σειρών τους να είναι διαφορετικά.

Λύση. Θεωρούμε την εναλλάσσουσα ομάδα $\mathbb{A}_5$, η οποία είναι απλή, βλ. Θεώρημα 3.2.19, και έχει τάξη 60 και την κυκλική ομάδα $\mathbb{Z}_{60}$. Η συνθετική σειρά τής πρώτης είναι η

$$\mathbb{A}_5 > \{\mathrm{Id}_{S_5}\}$$

και τής δεύτερης είναι η

$$\mathbb{Z}_{60} > \langle[5]_{60}\rangle > \langle[10]_{60}\rangle > \langle[20]_{60}\rangle > \langle[0]_{60}\rangle.$$

Η οικογένεια των συνθετικών παραγόντων τής πρώτης είναι η $(\mathbb{A}_5)$ και τής δεύτερης η

$$(\mathbb{Z}_{60}/\langle[5]_{60} \cong \mathbb{Z}_5, \langle[5]_{60}\rangle/\langle[10]_{60}\rangle \cong \mathbb{Z}_2, \langle[10]_{60}\rangle/\langle[20]_{60}\rangle \cong \mathbb{Z}_2\langle[20]_{60}\rangle/\langle[0]_{60}\rangle \cong \mathbb{Z}_3)\,.$$

Α 132. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H, K είναι δύο υποομάδες της. Να δειχθεί ότι αν, η H είναι χαρακτηριστική υποομάδα τής G και η K είναι χαρακτηριστική υποομάδα τής H, τότε η K είναι χαρακτηριστική υποομάδα τής G.

Λύση. Έστω $\varphi : G \to G$ ένας αυτομορφισμός τής G. Θα δείξουμε ότι $\varphi(K) = K$. Παρατηρούμε ότι επειδή η H είναι χαρακτηριστική υποομάδα τής G, έχουμε $\varphi(H) = H$, δηλαδή ο φ περιορισμένος στην H είναι ένας αυτομορφισμός τής H. Επομένως, $\varphi(K) = K$, αφού η K είναι χαρακτηριστική υποομάδα τής H. Ώστε η K είναι χαρακτηριστική υποομάδα τής G.

Α 133. Να προσδιοριστούν όλες οι χαρακτηριστικές υποομάδες των εξής ομάδων:

(α′) τής συμμετρικής ομάδας $(S_3, \circ)$,

(β′) τής διεδρικής ομάδας $(D_4, \circ)$ και

(γ′) τής ομάδας των τετρανίων $(Q_8, \cdot)$.

Λύση. Θα αναζητήσουμε τις χαρακτηριστικές υποομάδες μεταξύ των ορθόθετων υποομάδων, αφού κάθε χαρακτηριστική είναι και ορθόθετη.
(α′) Οι μοναδικές ορθόθετες υποομάδες τής S_3 είναι οι $\{\mathrm{Id}_{S_3}\}, S_3$ και $\mathbb{A}_3$. Οι δύο πρώτες είναι προφανώς χαρακτηριστικές. Κάθε αυτομορφισμός χ τής S_3 διατηρεί τις τάξεις των υποομάδων. Επομένως, η εικόνα $\chi(\mathbb{A}_3)$ είναι μια υποομάδα τής S_3 τάξης 3. Η μοναδική υποομάδα τάξης 3 τής S_3 είναι η $\mathbb{A}_3$. Συνεπώς, η $\mathbb{A}_3$ είναι χαρακτηριστική υποομάδα τής S_3.
(β′) Υπενθυμίζουμε ότι η D_4 είναι η ομάδα των στερεών κινήσεων τού τετραγώνου και ότι

$$D_4 = \{\mathrm{Id}_4, \tau, \rho, \rho^2, \rho^3, \tau\circ\rho, \tau\circ\rho^2, \tau\circ\rho^3\},$$

όπου $\circ(\rho) = 4, \circ(\tau) = 2$ και $\rho \circ \tau = \tau \circ \rho^3$.

Αφού κάθε χαρακτηριστική υποομάδα μιας ομάδας είναι ορθόθετη, θα αναζητήσουμε τις χαρακτηριστικές υποομάδες τής D_4 μεταξύ των ορθόθετων υποομάδων τής D_4.

Σύμφωνα με το Θεώρημα 1.6.6, οι ορθόθετες υποομάδες τής D_4 είναι οι εξής:

$$\{\mathrm{Id}_4\}, \quad D_4, \quad \langle \rho^2 \rangle, \quad \langle \rho \rangle, \quad \langle \{\rho^2, \tau\} \rangle, \quad \langle \{\rho^2, \tau \circ \rho\} \rangle.$$

Προφανώς, οι τετριμμένες υποομάδες D_4 και $\{\mathrm{Id}_4\}$ είναι χαρακτηριστικές. Επίσης η $\langle \rho \rangle$ είναι χαρακτηριστική. Πράγματι, για κάθε $\chi \in \mathrm{Aut}(D_4)$ η εικόνα $\chi(\langle \rho \rangle)$ ισούται με τη $\langle \rho \rangle$, επειδή η $\langle \rho \rangle$ είναι η μοναδική κυκλική υποομάδα τάξης 4 που διαθέτει η D_4 και επειδή η εικόνα $\chi(\langle \rho \rangle)$ είναι επίσης κυκλική υποομάδα τάξης 4. Η $\langle \rho^2 \rangle$ είναι, σύμφωνα με την Άσκηση A132, επίσης χαρακτηριστική υποομάδα τής D_4, αφού προφανώς είναι[1] χαρακτηριστική υποομάδα τής $\langle \rho \rangle$.

Ισχυριζόμαστε ότι οι $\langle \{\rho^2, \tau\} \rangle$ και $\langle \{\rho^2, \tau \circ \rho\} \rangle$ δεν είναι χαρακτηριστικές υποομάδες τής D_4. Πράγματι από το Λήμμα 1.7.39, γνωρίζουμε ότι η απεικόνιση $\chi : D_4 \to D_4$ με $\chi(\rho^i) = \rho^i$ και $\chi(\tau \circ \rho^i) = \tau \circ \rho^{i+1}, i \in \mathbb{Z}$, είναι ένας αυτομορφισμός. Τώρα είναι $\chi(\langle \{\rho^2, \tau\} \rangle) = \langle \{\rho^2, \tau \circ \rho\} \rangle$ και $\chi(\langle \{\rho^2, \tau \circ \rho\} \rangle) = \langle \{\rho^2, \tau\} \rangle$. Επομένως, οι δύο αυτές υποομάδες τής D_4 δεν είναι χαρακτηριστικές.

(γ′) Οι υποομάδες τής τετρανιακής ομάδας $(\mathcal{Q}_8, \cdot)$, βλ. Άσκηση A58, είναι οι εξής:

$$\mathcal{Q}_8, \{E\}, \langle I \rangle = \langle -I \rangle, \langle J \rangle = \langle -J \rangle, \langle K \rangle = \langle -K \rangle, \langle -E \rangle.$$

Από την Άσκηση ΠΑ73, γνωρίζουμε ότι όλες οι υποομάδες είναι ορθόθετες. Προφανώς, οι τετριμμένες υποομάδες $\mathcal{Q}_8$ και $\{E\}$ είναι χαρακτηριστικές.

Η κυκλική υποομάδα $\langle -E \rangle$ είναι η μοναδική υποομάδα τάξης 2 και γι' αυτό[2] παραμένει σταθερή ως προς οποιονδήποτε αυτομορφισμό τής $\mathcal{Q}_8$. Ως εκ τούτου, η $\langle -E \rangle$ είναι χαρακτηριστική υποομάδα τής $\mathcal{Q}_8$.

Παρατηρούμε ότι η $\mathcal{Q}_8$ συμπίπτει με την υποομάδα της $\langle \{I, J\} \rangle$ που παράγεται από τα I, J καθώς και με την υποομάδα της $\langle \{J, K\} \rangle$ που παράγεται από τα J, K.

Η απεικόνιση $\chi : \mathcal{Q}_8 \to \mathcal{Q}_8$ με $\chi(I^\alpha J^\beta) = J^\alpha I^\beta, 1 \leq \alpha, \beta \leq 4$ είναι ένας αυτομορφισμός τής $\mathcal{Q}_8$ που δεν απεικονίζει ούτε την $\langle I \rangle$ ούτε την $\langle J \rangle$ στον εαυτό της. Συνεπώς, οι $\langle I \rangle$ και $\langle J \rangle$ δεν είναι χαρακτηριστικές υποομάδες τής $\mathcal{Q}_8$. Παρόμοια η απεικόνιση $\psi : \mathcal{Q}_8 \to \mathcal{Q}_8$ με $\psi(J^\alpha K^\beta) = K^\alpha J^\beta, 1 \leq \alpha, \beta \leq 4$ είναι ένας αυτομορφισμός τής $\mathcal{Q}_8$ που δεν απεικονίζει την $\langle K \rangle$ στον εαυτό της. Επομένως, ούτε η $\langle K \rangle$ είναι χαρακτηριστική υποομάδα τής $\mathcal{Q}_8$.

A 134. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης $p^r q^s$, όπου οι p, q είναι διαφορετικοί πρώτοι αριθμοί. Έστω ότι η G διαθέτει τις συνθετικές σειρές

$$G = H_0 > H_1 > H_2 > \cdots > H_{r+s} = \{e_G\}, \quad (*)$$
$$G = K_0 > K_1 > K_2 > \cdots > K_{r+s} = \{e_G\}, \quad (**)$$

όπου $[H_r : 1] = q^s$ και $[K_s : 1] = p^r$. Να δειχθεί ότι οι H_r και K_s είναι ορθόθετες υποομάδες τής G και κατόπιν να συμπεράνετε ότι η G είναι το εσωτερικό ευθύ γινόμενο αυτών των δύο υποομάδων.

[1] Οποιαδήποτε υποομάδα μιας πεπερασμένης κυκλικής ομάδας είναι χαρακτηριστική! (*γιατί;*)

[2] Ή επειδή είναι το κέντρο τής $\mathcal{Q}_8$.

Λύση. Παρατηρούμε ότι η H_r είναι μια q-Sylow υποομάδα τής G. Ισχυριζόμαστε ότι η H_r είναι ορθόθετη υποομάδα τής G από όπου προφανώς προκύπτει ότι η H_r είναι η μοναδική q-Sylow υποομάδα τής G. Συγκεκριμένα θα δείξουμε γενικότερα με τη βοήθεια επαγωγής ότι η H_r είναι ορθόθετη υποομάδα τής $H_{r-i}, \forall i, 1 \leq i \leq r$.

Για $r = 1$, είναι $H_r \trianglelefteq H_{r-1}$, διότι η $(*)$ είναι μια συνθετική (άρα και υποορθόθετη) σειρά. Όταν ο ισχυρισμός είναι αληθής για $i = j$, δηλαδή όταν $H_r \trianglelefteq H_{r-j}$, τότε θα δείξουμε ότι $H_r \trianglelefteq H_{r-(j+1)}$. Πράγματι, η H_r είναι η μοναδική υποομάδα τής H_{r-j} τάξης q^s, διότι είναι μια q-Sylow υποομάδα τής H_{r-j} με $H_r \trianglelefteq H_{r-j}$. Τώρα με τη βοήθεια τής Άσκησης Α72, συμπεραίνουμε ότι $H_r \trianglelefteq H_{r-(j+1)}$, αφού η $H_{r-j} \trianglelefteq H_{r-(j+1)}$. Έτσι ολοκληρώνεται η επαγωγική απόδειξη και τελικά έχουμε ότι $H_r \trianglelefteq G$.

Θεωρώντας τη συνθετική σειρά $(**)$, αποδεικνύεται με ακριβώς τον ίδιο τρόπο ότι $K_s \trianglelefteq G$.

Συνεπώς, η ομάδα G έχει μια μοναδική Sylow υποομάδα για κάθε πρώτο διαιρέτη τής τάξης της και σύμφωνα με το Λήμμα 4.1.11, ισούται με το εσωτερικό ευθύ γινόμενο $K_s H_r$.

Προτεινόμενες Ασκήσεις

ΠΑ 132. Να βρεθούν οι συνθετικοί παράγοντες

(α′) τής συμμετρικής ομάδας $(S_4, \circ)$,

(β′) τής διεδρικής ομάδας $(D_6, \circ)$.

ΠΑ 133. Να δειχθεί ότι κάθε πεπερασμένη ομάδα διαθέτει και συνθετικές και κυρίαρχες σειρές.

ΠΑ 134. Να δειχθεί ότι μια αβελιανή ομάδα διαθέτει κάποια συνθετική σειρά, αν και μόνο αν, είναι πεπερασμένη.

ΠΑ 135. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι $H \trianglelefteq G$ είναι μια ορθόθετη υποομάδα τής G. Αν η G διαθέτει συνθετικές σειρές, τότε να δειχθεί ότι υπάρχει μια συνθετική σειρά που έχει ως όρο την υποομάδα H.

ΠΑ 136. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = \{e_G\}, \tag{*}$$

είναι μια υποορθόθετη (αντιστοίχως ορθόθετη) ακολουθία υποομάδων για την G.

(α′) Αν $H \leq G$ είναι μια υποομάδα τής G, τότε να δειχθεί ότι η ακολουθία

$$H = H_0 \geq H_1 \geq \cdots \geq H_r = \{e_G\}, \text{ με } H_i = G_i \cap H, i = 0, 1, \ldots, r$$

είναι μια υποορθόθετη (αντιστοίχως ορθόθετη) ακολουθία υποομάδων για την H, όπου $\forall i, i = 0, 1, \ldots, r-1$, η πηλικοομάδα H_i/H_{i+1} είναι ισόμορφη με μια υποομάδα τής G_i/G_{i+1}.

(β′) Επιπλέον, αν η $H \trianglelefteq G$ είναι μια ορθόθετη υποομάδα τής G, τότε να δειχθεί ότι η ακολουθία

$$G/H = \hat{G}_0 \geq \hat{G}_1 \geq \cdots \geq \hat{G}_r = \{e_{G/H}\}, \text{ με } \hat{G}_i = G_iH/H, i = 0, 1, \ldots, r$$

είναι μια υποορθόθετη (αντιστοίχως ορθόθετη) ακολουθία υποομάδων για την G/H, όπου $\forall i, i = 0, 1, \ldots, r-1$, η $\hat{G}_i/\hat{G}_{i+1}$ είναι μια πηλικοομάδα τής G_i/G_{i+1}.

Κεφάλαιο 6

Επιλύσιμες Ομάδες

6.1 Προκαταρκτικές Έννοιες

Ορισμός 6.1.1. Μια ομάδα $(G, \star)$ ονομάζεται *επιλύσιμη*, αν διαθέτει μια ορθόθετη σειρά

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = \{e_G\}$$

με αβελιανούς παράγοντες.

Παράδειγμα 6.1.2. (α′) Κάθε αβελιανή ομάδα $(G, \star)$ είναι επιλύσιμη, αφού ο μοναδικός παράγοντας τής τετριμμένης ορθόθετης σειράς

$$G \geq \{e_G\}$$

είναι αβελιανή ομάδα.

(β′) Η εναλλάσσουσα υποομάδα $\mathbb{A}_4$ τής συμμετρικής ομάδας $(S_4, \circ)$ είναι επιλύσιμη, αφού η σειρά

$$\mathbb{A}_4 \geq V \geq \{\mathrm{Id}_4\},$$

όπου $V = \left\{\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}\right\}$ είναι ορθόθετη και οι παράγοντες $\mathbb{A}_4/V$ και $V/\{\mathrm{Id}_4\}$ είναι αβελιανοί, επειδή πρόκειται για ομάδες με πλήθος στοιχείων ≤ 4.

(γ′) Η συμμετρική ομάδα $(S_5, \circ)$ δεν είναι επιλύσιμη. Πράγματι, η σειρά

$$S_5 \geq \mathbb{A}_5 \geq \{\mathrm{Id}_5\}$$

είναι μια κυρίαρχη σειρά για την S_5. Αν λοιπόν υπήρχε μια ορθόθετη σειρά με αβελιανούς παράγοντες για την S_5, τότε αυτή θα εκλεπτύνονταν σε μια κυρίαρχη σειρά, τής οποίας οι κυρίαρχοι παράγοντες θα ήταν αβελιανοί, βλ. την αμέσως επόμενη Παρατήρηση 6.1.3. Αφού όμως δύο οποιεσδήποτε κυρίαρχες σειρές είναι ισόμορφες, θα υπήρχε μεταξύ αυτών των κυρίαρχων παραγόντων και ένας κυρίαρχος παράγοντας ισόμορφος προς την $\mathbb{A}_5$, η οποία όμως δεν είναι αβελιανή ομάδα.

(δ′) Η εναλλάσσουσα υποομάδα $\mathbb{A}_n$ τής συμμετρικής ομάδας $(S_n, \circ)$ δεν είναι επιλύσιμη όταν $n \geq 5$. Πράγματι, η $\mathbb{A}_n \geq \{\mathrm{Id}_n\}$ είναι η μόνη γνήσια ορθόθετη σειρά για την $\mathbb{A}_n$, αφού η $\mathbb{A}_n$ είναι απλή, για $n \geq 5$.

(ε′) Έστω ότι $(\mathrm{GL}_2(\mathbb{K}), \cdot)$ είναι η ομάδα των αντιστρέψιμων 2×2 πινάκων με συνιστώσες από ένα σώμα $\mathbb{K}$, ότι

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{K}, ad \neq 0 \right\}$$

είναι η υποομάδα τής $\mathrm{GL}_2(\mathbb{K})$ που αποτελείται από τους άνω τριγωνικούς πίνακες και ότι

$$G_1 = \left\{ \begin{pmatrix} 1_{\mathbb{K}} & b \\ 0 & 1_{\mathbb{K}} \end{pmatrix} \mid b \in \mathbb{K} \right\}$$

είναι η υποομάδα τής $\mathrm{GL}_2(\mathbb{K})$ που αποτελείται από τους πίνακες, οι οποίοι έχουν όλα τα διαγώνια στοιχεία ίσα με το μοναδιαίο στοιχείο $1_{\mathbb{K}}$ τού $\mathbb{K}$.
Η σειρά

$$G \geq G_1 \geq \{I_2\}\,,$$

όπου I_2 είναι ο ταυτοτικός 2×2 πίνακας, είναι μια ορθόθετη σειρά για την G. Επιπλέον η πηλικοομάδα G/G_1 είναι αβελιανή, επειδή είναι ισόμορφη προς το ευθύ γινόμενο $\mathbb{K}^\star \times \mathbb{K}^\star$, όπου $(\mathbb{K}^\star = \mathbb{K} \setminus \{0\}, \cdot)$ είναι η πολλαπλασιαστική ομάδα τού σώματος $\mathbb{K}$ και η πηλικοομάδα $G_1/\{I_2\}$ είναι αβελιανή, επειδή είναι ισόμορφη προς την προσθετική ομάδα $(\mathbb{K}, +)$ τού σώματος $\mathbb{K}$. Επομένως, η G είναι επιλύσιμη ομάδα.

Παρατήρηση 6.1.3. Έστω ότι $(G, \star)$ είναι μια επιλύσιμη ομάδα και ότι

$$G = G_0 \geq G_1 \geq \ldots G_i \geq G_{i+1} \geq \cdots \geq G_r = \{e_G\} \qquad (*)$$

είναι μια ορθόθετη σειρά για την G με αβελιανούς παράγοντες. Οι παράγοντες οποιασδήποτε ορθόθετης εκλέπτυνσης τής (*) είναι επίσης αβελιανοί.

Είναι αρκετό να εξετάσουμε τους παράγοντες που προκύπτουν εκλεπτύνοντας τη σειρά μεταξύ των όρων G_i και G_{i+1}. Ας υποθέσουμε ότι μεταξύ των G_i και G_{i+1} ενθέτουμε τις ορθόθετες υποομάδες $N_j, j = 1, 2, \ldots, \ell$:

$$G_i \geq N_1 \geq N_2 \geq \cdots \geq N_j \geq N_{j+1} \geq \cdots \geq N_\ell \geq G_{i+1}.$$

Οι παράγοντες $N_\ell/G_{i+1} \leq G_i/G_{i+1}$ και $G_i/N_1 \cong (G_i/G_{i+1})/(N_1/G_{i+1})$ είναι αβελιανοί, επειδή ο παράγοντας G_i/G_{i+1} είναι αβελιανός. Κάθε παράγοντας $N_j/N_{j+1}, j = 1, 2, \ldots, \ell - 1$ περιέχεται στην πηλικοομάδα G_i/N_{j+1}, η οποία είναι αβελιανή ως επιμορφική εικόνα τής G_i/G_{i+1}, αφού $G_i/N_{j+1} \cong (G_i/G_{i+1})/(N_{j+1}/G_{i+1})$. Ώστε ο παράγοντας N_j/N_{j+1} είναι αβελιανός $\forall j, 1 \leq j \leq \ell - 1$.

Πρόταση 6.1.4. *Έστω ότι $(G, \star)$ είναι μια επιλύσιμη ομάδα. Κάθε υποομάδα H τής G και κάθε πηλικοομάδα G/N, όπου $N \trianglelefteq G$, είναι επίσης επιλύσιμη ομάδα.*

Απόδειξη. Έστω ότι η

$$G = G_0 \geq G_1 \geq \cdots \geq G_i \geq G_{i+1} \geq \cdots \geq G_r = \{e_G\}$$

είναι μια ορθόθετη σειρά για τη G με αβελιανούς παράγοντες.

Αν $H \leq G$ είναι μια υποομάδα τής G, τότε θεωρούμε τη σειρά

$$\begin{aligned} H = H \bigcap G = H \bigcap G_0 \geq H \bigcap G_1 \geq \cdots \geq H \bigcap G_i \geq H \bigcap G_{i+1} \geq \dots \\ \cdots \geq H \bigcap G_r = H \bigcap \{e_G\} = \{e_G\}. \end{aligned} \qquad (**)$$

Προφανώς, $\forall i, 0 \leq i \leq r$, η $H \bigcap G_i$ είναι μια ορθόθετη υποομάδα τής H.
Επιπλέον,

$$H \bigcap G_i / H \bigcap G_{i+1} = H \bigcap G_i / (H \bigcap G_i) \bigcap G_{i+1} \cong (H \bigcap G_i) G_{i+1} / G_{i+1} \leq G_i / G_{i+1}$$

και έτσι προκύπτει ότι οι παράγοντες τής (**) είναι αβελιανοί.

Αν G/N είναι μια πηλικοομάδα τής G, όπου $N \trianglelefteq G$, τότε θεωρούμε τη σειρά

$$\begin{aligned} G/N = G_0/N \geq G_1N/N \geq \cdots \geq G_iN/N \geq G_{i+1}N/N \geq \dots \\ \cdots \geq G_rN/N = N/N = \{N\}. \end{aligned} \qquad (***)$$

Παρατηρούμε ότι

$$(G_iN/N)/(G_{i+1}N/N) \cong G_iN/G_{i+1}N = G_i(G_{i+1}N)/G_{i+1}N \cong G_i/G_i \bigcap (G_{i+1}N) \cong$$

$$(G_i/G_{i+1})/(G_i \bigcap (G_{i+1}N)/G_{i+1}).$$

(Προσέξτε ότι επιτρέπεται ο σχηματισμός τής πηλικοομάδας $(G_i \bigcap (G_{i+1}N)/G_{i+1})$, επειδή $G_{i+1} \leq G_i \bigcap (G_{i+1}N)$, αφού $G_{i+1} \leq G_i$.)
Ώστε $\forall i, 0 \leq i \leq r-1$, ο παράγοντας $(G_iN/N)/(G_{i+1}N/N)$ είναι ισόμορφος προς μια επιμορφική εικόνα τής αβελιανής ομάδας G_i/G_{i+1} και γι' αυτό είναι επίσης αβελιανός. Επομένως, η (***) είναι μια ορθόθετη σειρά με αβελιανούς παράγοντες για την πηλικοομάδα G/N. Συνεπώς, η G/N είναι μια επιλύσιμη ομάδα. □

Πόρισμα 6.1.5. *Η συμμετρική ομάδα $(S_n, \circ)$ δεν είναι επιλύσιμη όταν $n \geq 5$.*

Απόδειξη. Αν ήταν η S_n επιλύσιμη, τότε θα ήταν και η $\mathbb{A}_n$ επιλύσιμη. Αλλά όπως είδαμε αυτό είναι αδύνατο, αφού η $\mathbb{A}_n$ είναι απλή, για $n \geq 5$. □

Πρόταση 6.1.6. *Έστω ότι $(G, \star)$ είναι μια πεπερασμένη επιλύσιμη ομάδα.*

(α′) *Αν η G είναι απλή ομάδα, τότε είναι μια κυκλική ομάδα πρώτης τάξης.*

(β′) *Οποιοσδήποτε συνθετικός παράγοντας τής G είναι μια κυκλική ομάδα πρώτης τάξης.*

(γ′) *Οποιοσδήποτε κυρίαρχος παράγοντας τής G είναι μια στοιχειώδης αβελιανή p–ομάδα.*

Απόδειξη. (α′) Κάθε επιλύσιμη ομάδα G διαθέτει μια ορθόθετη σειρά με αβελιανούς παράγοντες. Αφού όμως η G είναι απλή, η μοναδική ορθόθετη σειρά για την G είναι η $G \geq \{e_G\}$ και ο παράγοντας $G/\{e_G\} \cong G$ οφείλει να είναι αβελιανός. Συνεπώς, η G είναι μια απλή αβελιανή ομάδα και από την Πρόταση 3.2.17, γνωρίζουμε ότι οι απλές κυκλικές ομάδες είναι κυκλικές πρώτης τάξης.
(β′) και (γ′) Οποιαδήποτε ορθόθετη σειρά με αβελιανούς παράγοντες για την G μπορεί να εκλεπτυνθεί σε μια συνθετική (αντιστοίχως κυρίαρχη) σειρά για την G. Με τρόπο ανάλογο τής Παρατήρησης 6.1.3 διαπιστώνουμε ότι οι συνθετικοί (αντιστοίχως κυρίαρχοι) παράγοντες είναι αβελιανοί. Συνεπώς, οι συνθετικοί (κυρίαρχοι) παράγοντες είναι απλές (αντιστοίχως χαρακτηριστικώς απλές) αβελιανές ομάδες που όπως γνωρίζουμε, βλ. Πρόταση 3.2.17 (αντιστοίχως βλ. Πόρισμα 5.3.8), είναι κυκλικές ομάδες πρώτης τάξης (αντιστοίχως στοιχειώδεις αβελιανές p–ομάδες). □

6.2 Μεταθέτες και παράγωγες Ομάδες

Ορισμός 6.2.1. Έστω $(G, \star)$ μια ομάδα. Το στοιχείο $xyx^{-1}y^{-1}$, όπου $x, y \in G$ ονομάζεται ο *μεταθέτης* των x, y και συμβολίζεται με $[x, y]$.

Ορισμός 6.2.2. Έστω $(G, \star)$ μια ομάδα. Ονομάζουμε *μεταθέτρια* ή *παράγωγη υποομάδα* τής G, την υποομάδα τής G που παράγεται από το σύνολο των μεταθετών τής G.

Με άλλα λόγια, η μεταθέτρια (παράγωγη) υποομάδα μιας ομάδας $(G, \star)$ είναι η

$$G' = \langle [x, y] \mid x, y \in G \rangle.$$

Συνήθως συμβολίζουμε τη μεταθέτρια (παράγωγη) υποομάδα τής G με G' ή με $[G, G]$. Πριν προχωρήσουμε σε παραδείγματα αποδεικνύουμε μια ιδιαιτέρως χρήσιμη πρόταση.

Πρόταση 6.2.3. *Έστω $(G, \star)$ μια ομάδα και G' η παράγωγη υποομάδα της. Τότε*

(α′) *Η G' είναι μια χαρακτηριστική υποομάδα τής G.*

(β′) *Η G' είναι η μικρότερη ορθόθετη υποομάδα τής G που έχει την ιδιότητα, η πηλικοομάδα G/G' να είναι αβελιανή.*
(Δηλαδή, αν N είναι ορθόθετη υποομάδα τής G με την ιδιότητα, η πηλικοομάδα G/N να είναι αβελιανή, τότε $G' \leq N$).

Απόδειξη. (α′) Σύμφωνα με την Παρατήρηση 3.2.11, αρκεί να δείξουμε ότι για κάθε αυτομορφισμό $\varphi \in \mathrm{Aut}(G)$, είναι $\varphi(G') \leq G'$. Αλλά η εικόνα $\varphi([x, y])$ οποιουδήποτε μεταθέτη $[x, y]$ είναι και πάλι ένας μεταθέτης, αφού $\varphi([x, y]) = [\varphi(x), \varphi(y)]$. Επομένως, $\varphi(G') \leq G'$.
(β′) Η πηλικοομάδα G/G' είναι αβελιανή, αφού

$$\forall x, y \in G, [x^{-1}, y^{-1}] \in G' \Rightarrow xyG = yxG.$$

Αν N είναι μια ορθόθετη υποομάδα τής G τέτοια, ώστε η G/N να είναι αβελιανή, τότε $\forall x, y \in G, xyN = yxN \Leftrightarrow \forall x, y \in G, [x^{-1}, y^{-1}] \in N$. Επομένως, κάθε γεννήτορας τής G' ανήκει στην N και γι' αυτό $G' \leq N$. □

Παρατήρηση 6.2.4. Μια ομάδα $(G,\star)$ είναι αβελιανή, αν και μόνο αν, η παράγωγη υποομάδα της G' ισούται με την τετριμμένη υποομάδα $\{e_G\}$. Πράγματι, η G είναι αβελιανή, αν και μόνο αν, η πηλικοομάδα $G/\{e_G\}$ είναι αβελιανή, αν και μόνο αν, $G' = \{e_G\}$.

Παράδειγμα 6.2.5. (α′) Η συμμετρική ομάδα $(S_3,\circ)$ δεν είναι αβελιανή. Επομένως, η παράγωγη υποομάδα $[S_3,S_3] = S_3'$ δεν ισούται με την $\{\mathrm{Id}_3\}$. Η S_3' είναι υποομάδα τής $\mathbb{A}_3$, αφού κάθε γεννήτοράς της, δηλαδή κάθε μεταθέτης $\sigma\circ\tau\circ\sigma^{-1}\circ\tau^{-1}$, $\sigma,\tau\in S_3$ είναι άρτια μετάταξη τής S_3. Αφού οι μοναδικές υποομάδες τής $\mathbb{A}_3$ είναι οι $\mathbb{A}_3$ και $\{\mathrm{Id}_3\}$, συμπεραίνουμε ότι $[S_3,S_3] = S_3' = \mathbb{A}_3$.

(β′) Η εναλλάσσουσα ομάδα $\mathbb{A}_4$ δεν είναι αβελιανή, επομένως η $[\mathbb{A}_4,\mathbb{A}_4] = \mathbb{A}_4' \neq \{e_{\mathbb{A}_4}\}$. Η υποομάδα $V = \left\{\mathrm{Id}_4, \begin{pmatrix}1 & 2\end{pmatrix}\circ\begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}\circ\begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix}\circ\begin{pmatrix}2 & 3\end{pmatrix}\right\}$ τής $\mathbb{A}_4$ είναι ορθόθετη και η πηλικοομάδα $\mathbb{A}_4/V$ είναι αβελιανή. Επομένως, η $\mathbb{A}_4' \leq V$. Αλλά η μοναδική ορθόθετη και $\neq \{e_{\mathbb{A}_4}\}$ υποομάδα τής $\mathbb{A}_4$ που περιέχεται στη V είναι η V. Συνεπώς, $[\mathbb{A}_4,\mathbb{A}_4] = \mathbb{A}_4' = V$.

(γ′) Θεωρούμε τη διεδρική ομάδα

$$D_4 = \{\mathrm{Id}_4, \tau, \rho, \rho^2, \rho^3, \tau\circ\rho, \tau\circ\rho^2, \tau\circ\rho^3\}.$$

Η D_4 δεν είναι αβελιανή και γι' αυτό $[D_4,D_4] = D_4' \neq \{\mathrm{Id}_4\}$. Το κέντρο $\mathcal{Z}(D_4)$ είναι ίσο με την κυκλική υποομάδα $\langle\rho^2\rangle$ και η πηλικοομάδα $D_4/\mathcal{Z}(D_4)$ είναι αβελιανή, επειδή $[D_4 : \mathcal{Z}(D_4)] = 4$. Οι μοναδικές υποομάδες τής $\mathcal{Z}(D_4)$ είναι οι $\mathcal{Z}(D_4)$ και $\{\mathrm{Id}_4\}$. Αφού $\{\mathrm{Id}_4\} \subsetneqq D_4' \leq \mathcal{Z}(D_4)$, συμπεραίνουμε ότι $[D_4,D_4] = D_4' = \mathcal{Z}(D_4)$.

(δ′) Θεωρούμε την εναλλάσσουσα υποομάδα $\mathbb{A}_5$ τής συμμετρικής ομάδας $(S_5,\circ)$. Η $\mathbb{A}_5$ δεν είναι αβελιανή, επομένως $\mathbb{A}_5' \neq \{e_{\mathbb{A}_5}\}$. Επειδή η $\mathbb{A}_5$ είναι απλή ομάδα και επειδή η παράγωγη υποομάδα της $\mathbb{A}_5'$ είναι ορθόθετη, η μοναδική επιλογή για την $\mathbb{A}_5'$ είναι η $\mathbb{A}_5' = \mathbb{A}_5$.

6.2.1 Η παράγωγη Σειρά μιας Ομάδας

Ορισμός 6.2.6. Έστω $(G,\star)$ μια ομάδα. Ορίζουμε επαγωγικά τις *ανώτερες παράγωγες υποομάδες* τής G, όπου $i \in \mathbb{N}\bigcup\{0\}$, ως $G^{(0)} = G$, $G^{(1)} = [G,G] = G'$ και $G^{(i+1)} = [G^{(i)}, G^{(i)}] = (G^{(i)})'$.

Δηλαδή, η $G^{(i+1)}$ είναι η παράγωγη υποομάδα τής $G^{(i)}$.

Ορισμός 6.2.7. Έστω $(G,\star)$ μια ομάδα. Η σειρά

$$G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(i)} \geq G^{(i+1)} \geq \ldots$$

ονομάζεται η *παράγωγη σειρά* για την ομάδα G.

Παράδειγμα 6.2.8. Από το Παράδειγμα 6.2.5 έχουμε ότι

(α′) Η παράγωγη σειρά για τη συμμετρική ομάδα $(S_3,\circ)$ είναι η

$$S_3 = S_3^{(0)} > S_3^{(1)} = \mathbb{A}_3 > S_3^{(2)} = \mathbb{A}_3' = \{\mathrm{Id}_3\}.$$

(β′) Η παράγωγη σειρά για την εναλλάσσουσα ομάδα $(\mathbb{A}_4, \circ)$ είναι η

$$\mathbb{A}_4 = \mathbb{A}_4^{(0)} > \mathbb{A}_4^{(1)} = V > \mathbb{A}_4^{(2)} = V' = \{e_{\mathbb{A}_4}\}.$$

(γ′) Η παράγωγη σειρά για τη διεδρική ομάδα $(D_4, \circ)$ είναι η

$$D_4 = D_4^{(0)} > D_4^{(1)} = \mathcal{Z}(D_4) > D_4^{(2)} = \mathcal{Z}(D_4)' = \{\mathrm{Id}_4\}.$$

(δ′) Η παράγωγη σειρά για την εναλλάσσουσα ομάδα $(\mathbb{A}_5, \circ)$ είναι η

$$\mathbb{A}_5 = \mathbb{A}_5 = \cdots = \mathbb{A}_5 = \cdots = \mathbb{A}_5 = \cdots,$$

αφού $\forall i \in \mathbb{N} \bigcup \{0\}, \mathbb{A}_5^{(i)} = \mathbb{A}_5$.

Πρόταση 6.2.9. *Έστω $(G, \star)$ μια ομάδα. Για κάθε $n \in \mathbb{N} \bigcup \{0\}$, η παράγωγη υποομάδα της $G^{(n)}$ είναι ορθόθετη.*

Απόδειξη. Θα εκτελέσουμε την απόδειξη με επαγωγή ως προς $n \in \mathbb{N} \bigcup \{0\}$.
Για $n = 0$ ο ισχυρισμός είναι αληθής, αφού $G^{(0)} = G$. Έστω ότι ο ισχυρισμός είναι αληθής για $n = r$, δηλαδή ότι $G^{(r)} \trianglelefteq G$. Για $n = r + 1$ γνωρίζουμε, βλ. Πρόταση 6.2.3, ότι η $G^{(r+1)}$ είναι χαρακτηριστική υποομάδα τής $G^{(r)}$ και αφού $G^{(r)} \trianglelefteq G$, έπεται, βλ. Παρατήρηση 3.2.13, ότι $G^{(r+1)} \trianglelefteq G$. Επομένως, $\forall n \in \mathbb{N} \bigcup \{0\}, G^{(n)} \trianglelefteq G$. □

Θεώρημα 6.2.10. *Έστω $(G, \star)$ μια ομάδα. Τα επόμενα είναι ισοδύναμα:*

(α′) *Η G είναι μια επιλύσιμη ομάδα.*

(β′) *Υπάρχει μια υποορθόθετη σειρά για τη G με όλους τους παράγοντές της αβελιανούς.*

(γ′) *Υπάρχει $r \in \mathbb{N} \bigcup \{0\}$ με την παράγωγη υποομάδα $G^{(r)}$ ίση με $\{e_G\}$.*

Απόδειξη. (α′) ⇒ (β′). Προφανές, αφού κάθε ορθόθετη σειρά για την G είναι επίσης υποορθόθετη σειρά για την G.
(β′) ⇒ (γ′). Θα δείξουμε ότι αν

$$G = G_0 \geq G_1 \geq \ldots G_i \geq G_{i+1} \geq \cdots \geq G_r = \{e_G\} \tag{*}$$

είναι μια υποορθόθετη σειρά για την G με αβελιανούς παράγοντες, τότε $\forall k \in \mathbb{N} \bigcup \{0\}$, η παράγωγη υποομάδα $G^{(k)}$ περιέχεται στον όρο G_k τής (*). (Δεχόμαστε ότι $G_s = G_r = \{e_G\}, \forall s \in \mathbb{N} \bigcup \{0\}, s \geq r$.) Θα εκτελέσουμε την απόδειξη με επαγωγή ως προς $k \in \mathbb{N} \bigcup \{0\}$.
Για $k = 0$, ο ισχυρισμός είναι αληθής, αφού $G^{(0)} = G$ και $G_0 = G$.
Έστω ότι ο ισχυρισμός είναι αληθής για $k = t$, δηλαδή ότι $G^{(t)} \leq G_t$. Θα δείξουμε ότι είναι αληθής για $k = t + 1$, δηλαδή ότι $G^{(t+1)} \leq G_{t+1}$.
Επειδή η πηλικοομάδα G_t/G_{t+1} είναι αβελιανή, συμπεραίνουμε, βλ. Πρόταση 6.2.3, ότι $(G_t)' = [G_t, G_t] \leq G_{t+1}$. Τώρα έχουμε:

$$G^{(t+1)} = (G^{(t)})' \leq (G_t)' \leq G_{t+1}.$$

Ώστε $\forall k \in \mathbb{N} \bigcup \{0\}$, είναι $G^{(k)} \leq G_k$.
Αφού λοιπόν $G_r = \{e_G\}$ και επειδή $G^{(r)} \leq G_r$, συμπεραίνουμε ότι $G^{(r)} = \{e_G\}$.
(γ′) ⇒ (α′). Λόγω τής υπόθεσης, η παράγωγη σειρά για την G εκφυλίζεται κατόπιν ενός πεπερασμένου αριθμού βημάτων, δηλαδή είναι τής μορφής

$$G = G^{(0)} \geq G^{(1)} \geq \cdots \geq G^{(i)} \geq G^{(i+1)} \geq \cdots \geq G_r = \{e_G\}. \tag{*}$$

Λόγω τής Πρότασης 6.2.9, $\forall i, 0 \leq i \leq r$, οι παράγωγες υποομάδες $G^{(i)}$ είναι ορθόθετες υποομάδες τής G. Επιπλέον, $\forall i, 0 \leq i \leq r-1$, οι παράγοντες $G^{(i)}/G^{(i+1)}$ είναι αβελιανοί. Επομένως, η (*) είναι μια ορθόθετη σειρά με αβελιανούς παράγοντες για την G. Ώστε η G είναι επιλύσιμη ομάδα. □

Πόρισμα 6.2.11. *Μια ομάδα $(G, \star)$ είναι επιλύσιμη, αν και μόνο αν, υπάρχει μια υποορθόθετη σειρά για τη G, τής οποίας όλοι οι παράγοντες είναι κυκλικές ομάδες πρώτης τάξης.*

Απόδειξη. «⇒» Σύμφωνα με το προηγούμενο θεώρημα, υπάρχει μια υποορθόθετη σειρά για τη G που έχει αβελιανούς παράγοντες. Η συγκεκριμένη σειρά εκλεπτύνεται σε μια συνθετική σειρά για την G. Η Πρόταση 6.1.6 μας πληροφορεί ότι όλοι οι συνθετικοί παράγοντες αυτής τής σειράς είναι κυκλικές ομάδες πρώτης τάξης.
«⇐» Η υποορθόθετη σειρά την ομάδα G έχει όλους τους παράγοντές της αβελιανούς. Σύμφωνα με το προηγούμενο θεώρημα η ομάδα G είναι επιλύσιμη. □

Προσέξτε ότι χάρη στο προηγούμενο θεώρημα, η αρχική ισχυρή συνθήκη για την επιλυσιμότητα μιας ομάδας, που απαιτούσε την ύπαρξη μια ορθόθετης σειράς με αβελιανούς παράγοντες, αντικαταστάθηκε από μια ασθενέστερη αλλά ισοδύναμη συνθήκη, η οποία απαιτεί την ύπαρξη μιας υποορθόθετης σειράς με αβελιανούς παράγοντες. Αυτή η ασθενέστερη συνθήκη επιτρέπει τη συμπλήρωση τής Πρότασης 6.1.4 στην εξής:

Πρόταση 6.2.12. *Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι $N \trianglelefteq G$ είναι μια ορθόθετη υποομάδα της. Αν η υποομάδα N και η πηλικοομάδα G/N είναι επιλύσιμες, τότε είναι και η G επιλύσιμη ομάδα.*

Απόδειξη. Αφού η G/N είναι επιλύσιμη, υπάρχει μια υποορθόθετη σειρά για τη G/N. Ας πούμε ότι η συγκεκριμένη υποορθόθετη σειρά είναι η:

$$G/N = \overline{G}_0 \geq \overline{G}_1 \geq \overline{G}_2 \geq \cdots \geq \overline{G}_i \geq \overline{G}_{i+1} \geq \cdots \geq \overline{G}_r = \{N\} \tag{*}$$

Συνεπώς, $\forall i, 0 \leq i \leq r-1$, η υποομάδα $\overline{G}_{i+1}$ είναι ορθόθετη υποομάδα τής $\overline{G}_i$ και το πηλίκο $\overline{G}_i/\overline{G}_{i+1}$ είναι αβελιανό. Για κάθε $i, 0 \leq i \leq r-1$, υπάρχει υποομάδα G_i τής G με $N \leq G_i$ και με $G_i/N = \overline{G}_i$, όπου επιπλέον η G_{i+1} ορθόθετη υποομάδα τής G_i.

Γι' αυτό από την (*) επάγεται η σειρά των υποομάδων

$$G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_i \geq G_{i+1} \geq \cdots \geq G_r = N, \tag{**}$$

όπου $\forall i, 0 \leq i \leq r-1$ η πηλικοομάδα G_i/G_{i+1} είναι αβελιανή, αφού $G_i/G_{i+1} \cong \overline{G}_i/\overline{G}_{i+1}$.
Θεωρούμε τώρα μια υποορθόθετη σειρά για την επιλύσιμη υποομάδα N, που έχει όλους τους παράγοντές της αβελιανούς:

$$N = N_0 \geq N_1 \geq N_2 \geq \cdots \geq N_j \geq N_{j+1} \geq \cdots \geq N_t = \{e_G\}. \tag{***}$$

Συνενώνοντας τις σειρές (**) και (***) προκύπτει η σειρά

$$G = G_0 \geq G_1 \geq \cdots \geq G_i \geq \cdots \geq G_r = N = N_0 \geq N_1 \geq N_j \geq \cdots \geq N_t = \{e_G\},$$

η οποία είναι μια υποορθόθετη σειρά για την G με όλους τους παράγοντές της αβελιανούς.

□

Παράδειγμα 6.2.13. Η συμμετρική ομάδα $(S_3, \circ)$ (αντιστοίχως $(S_4, \circ)$) είναι επιλύσιμη ομάδα, διότι η ορθόθετη υποομάδα της $\mathbb{A}_3$ (αντιστοίχως $\mathbb{A}_4$) είναι επιλύσιμη και η πηλικοομάδα $S_3/\mathbb{A}_3$ (αντιστοίχως $S_4/\mathbb{A}_4$) είναι επίσης επιλύσιμη, αφού έχει μόνο δύο στοιχεία και ως εκ τούτου, είναι αβελιανή, άρα και επιλύσιμη.

6.3 Μηδενοδύναμες Ομάδες

6.3.1 Τα ανώτερα Κέντρα μιας Ομάδας

Για οποιαδήποτε ομάδα $(G, \star)$ θα συμβολίζουμε με $\mathcal{Z}(G)$ το κέντρο της. Θέτουμε $\mathcal{Z}_1(G) = \mathcal{Z}(G)$. Θεωρούμε την πηλικοομάδα $G/\mathcal{Z}_1(G)$, τη φυσική προβολή $p_1 : G \to G/\mathcal{Z}_1(G)$ και ορίζουμε την υποομάδα $\mathcal{Z}_2(G)$ τής G ως την αντίστροφη εικόνα ως προς p_1, τού κέντρου τής $G/\mathcal{Z}_1(G)$, δηλαδή $\mathcal{Z}_2(G) = p_1^{-1}(\mathcal{Z}(G/\mathcal{Z}_1(G)))$. Συνεπώς, $\mathcal{Z}_2(G)/\mathcal{Z}_1(G) = \mathcal{Z}(G/\mathcal{Z}_1(G))$. Συνεχίζοντας με αυτόν τον τρόπο ορίζουμε επαγωγικώς την υποομάδα $\mathcal{Z}_{i+1}(G)$ τής G ως την αντίστροφη εικόνα, ως προς τη φυσική προβολή $p_i : G \to G/\mathcal{Z}_i(G)$, τού κέντρου τής $G/\mathcal{Z}_i(G)$, δηλαδή $\mathcal{Z}_{i+1}(G) = p_i^{-1}(\mathcal{Z}(G/\mathcal{Z}_i(G)))$. Συνεπώς, $\mathcal{Z}_{i+1}(G)/\mathcal{Z}_i(G) = \mathcal{Z}(G/\mathcal{Z}_i(G))$. Τέλος θέτουμε $\mathcal{Z}_0(G) = \{e_G\}$.

Ορισμός 6.3.1. Η σειρά

$$\{e_G\} = \mathcal{Z}_0(G) \leq \mathcal{Z}(G) = \mathcal{Z}_1(G) \leq \mathcal{Z}_2(G) \leq \cdots \leq \mathcal{Z}_i(G) \leq \ldots$$

ονομάζεται η *άνω κεντρική σειρά* για την ομάδα $(G, \star)$ και οι όροι τής σειράς ονομάζονται τα *ανώτερα κέντρα* τής G.

Παρατήρηση 6.3.2. Για κάθε $i \in \mathbb{N} \bigcup \{0\}$, οι υποομάδες $\mathcal{Z}_i(G)$ είναι χαρακτηριστικές (επομένως και ορθόθετες) υποομάδες τής G.
Για $i = 0$ αυτό είναι τετριμμένο. Θα δείξουμε με επαγωγή ότι $\forall i, i \in \mathbb{N}$ ο ισχυρισμός είναι αληθής.
Για $i = 1$, η $\mathcal{Z}_1(G)$ είναι το κέντρο τής G, το οποίο είναι γνωστό ότι είναι μια χαρακτηριστική υποομάδα τής G. Έστω ότι η $\mathcal{Z}_k(G)$ είναι μια χαρακτηριστική υποομάδα τής G. Θα δείξουμε ότι η $\mathcal{Z}_{k+1}(G)$ είναι επίσης μια χαρακτηριστική υποομάδα τής G, αποδεικνύοντας ότι αν $\varphi \in \mathrm{Aut}(G)$, τότε $\varphi(\mathcal{Z}_{k+1}(G)) \leq \mathcal{Z}_{k+1}(G)$.
Παρατηρούμε ότι ένα στοιχείο $x \in G$ ανήκει στην $\mathcal{Z}_{k+1}(G)$, αν και μόνο αν, $\forall g \in G$ είναι $xg\mathcal{Z}_k(G) = gx\mathcal{Z}_k(G)$ ή ισοδύναμα $\forall g \in G$ είναι $x^{-1}g^{-1}xg \in \mathcal{Z}_k(G)$. Θα δείξουμε ότι αν $x \in \mathcal{Z}_{k+1}(G)$, τότε $\varphi(x) \in \mathcal{Z}_{k+1}(G)$.
Επειδή ο φ είναι ένας αυτομορφισμός, κάθε $g \in G$ ισούται με κάποιο $\varphi(h), h \in G$. Έτσι έχουμε:

$$\varphi(x) \in \mathcal{Z}_{k+1}(G) \Leftrightarrow \forall \varphi(h) \in G, \varphi(x^{-1})\varphi(h)^{-1}\varphi(x)\varphi(h) = \varphi(x^{-1}h^{-1}xh) \in \mathcal{Z}_k(G).$$

Αλλά αφού το $x \in \mathcal{Z}_{k+1}(G)$, έπεται ότι $\forall h \in G$, το $x^{-1}h^{-1}xh$ ανήκει στην $\mathcal{Z}_k(G)$. Επομένως, το $\varphi(x^{-1}h^{-1}xh)$ ανήκει στη $\varphi(\mathcal{Z}_k(G))$, η οποία ισούται με την $\mathcal{Z}_k(G)$, αφού λόγω τής επαγωγικής υπόθεσης είναι χαρακτηριστική. Ώστε, αν $x \in \mathcal{Z}_{k+1}(G)$, τότε και $\varphi(x) \in \mathcal{Z}_{k+1}(G)$. Επομένως, $\varphi(\mathcal{Z}_{k+1}(G)) \leq \mathcal{Z}_{k+1}(G)$.

Παράδειγμα 6.3.3. (α′) Θεωρούμε τη συμμετρική ομάδα $(S_3, \circ)$. Η άνω κεντρική σειρά για την S_3 είναι η

$$\{\mathrm{Id}_3\} = \mathcal{Z}_0(S_3) = \{\mathrm{Id}_3\} = \mathcal{Z}_1(S_3) = \cdots = \{\mathrm{Id}_3\} = \mathcal{Z}_i(S_3) = \ldots$$

αφού η S_3 έχει τετριμμένο κέντρο.

(β′) Η άνω κεντρική σειρά για την $(S_4, \circ)$ είναι επίσης τετριμμένη, αφού

$$\{\mathrm{Id}_4\} = \mathcal{Z}_0(S_4) = \{\mathrm{Id}_4\} = \mathcal{Z}_1(S_4) = \cdots = \{\mathrm{Id}_4\} = \mathcal{Z}_i(S_4) = \ldots$$

επειδή το κέντρο $\mathcal{Z}(S_4)$ είναι η τετριμμένη υποομάδα $\{\mathrm{Id}_4\}$.

(γ′) Γενικά, η άνω κεντρική σειρά μιας ομάδας $(G, \star)$ με τετριμμένο κέντρο είναι η τετριμμένη σειρά

$$\{e_G\} = \mathcal{Z}_0(G) = \{e_G\} = \mathcal{Z}_1(G) = \cdots = \{e_G\} = \mathcal{Z}_i(G) = \ldots$$

Με τη βοήθεια τής έννοιας τής άνω κεντρικής σειράς μπορούμε να αποδείξουμε άμεσα ότι

Πρόταση 6.3.4. *Κάθε p–ομάδα $(G, \star)$ είναι επιλύσιμη και κάθε κυρίαρχος παράγοντάς της είναι κυκλική ομάδα τάξης p.*

Απόδειξη. Επειδή μια p–ομάδα έχει μη τετριμμένο κέντρο και επειδή οι μη τετριμμένες πηλικοομάδες μιας p–ομάδας είναι και αυτές p–ομάδες, διαπιστώνουμε ότι η άνω κεντρική σειρά μιας p–ομάδας έχει τη μορφή

$$\{e_G\} = \mathcal{Z}_0(G) < \mathcal{Z}(G) = \mathcal{Z}_1(G) < \cdots < \mathcal{Z}_r(G) = G,$$

αφού $\forall i, 0 \leq i \leq r$, η $\mathcal{Z}_i(G)$ είναι γνήσια υποομάδα τής $\mathcal{Z}_{i+1}(G)$ και γι' αυτό κατόπιν ενός πεπερασμένου αριθμού βημάτων κάποιος όρος τής σειράς θα γίνει ίσος με G. Τώρα όμως η άνω κεντρική σειρά είναι μια ορθόθετη σειρά για τη G με όλους τους παράγοντές της αβελιανούς. Επομένως η G είναι επιλύσιμη.

Εκλεπτύνοντας την άνω κεντρική σειρά, προκύπτει μια συνθετική σειρά με όλους τους συνθετικούς της παράγοντες απλές κυκλικές ομάδες. Αλλά αυτοί οι συνθετικοί παράγοντες είναι υποομάδες πηλικοομάδων p–ομάδων, όπου ο πρώτος p είναι σταθερός, γι' αυτό όλοι οι συνθετικοί παράγοντες είναι κυκλικές ομάδες με τάξη τον συγκεκριμένο πρώτο αριθμό p. Επιπλέον, οποιαδήποτε εκλέπτυνση τής άνω κεντρικής σειράς σε υποορθόθετη σειρά για την G είναι στην πραγματικότητα μια ορθόθετη σειρά (γιατί;) και γι' αυτό η προηγούμενη συνθετική σειρά είναι επίσης μια κυρίαρχη σειρά. Άρα κάθε κυρίαρχος παράγοντας τής G είναι κυκλική ομάδα τάξης p. $\square$

Ορισμός 6.3.5. Μια ομάδα $(G, \star)$ ονομάζεται *μηδενοδύναμη*, αν ο σχηματισμός τής άνω κεντρικής σειράς καταλήγει στην ομάδα G, κατόπιν ενός πεπερασμένου αριθμού βημάτων, δηλαδή υπάρχει κάποιος $r \in \mathbb{N} \bigcup \{0\}$ με $\mathcal{Z}_r(G) = G$.

Αν $r \in \mathbb{N} \bigcup \{0\}$ είναι ο ελάχιστος μη αρνητικός ακέραιος με $\mathcal{Z}_r(G) = G$, τότε η μηδενοδύναμη ομάδα G ονομάζεται *κλάσης* r.

Παρατήρηση 6.3.6. Προφανώς μια μηδενοδύναμη ομάδα $(G, \star)$ είναι επιλύσιμη, αφού η άνω κεντρική σειρά της είναι μια ορθόθετη σειρά για την G με όλους τους παράγοντές της αβελιανούς. Ωστόσο, κάθε επιλύσιμη ομάδα δεν είναι μηδενοδύναμη. Οι συμμετρικές ομάδες $(S_3, \circ)$ και $(S_4, \circ)$ είναι επιλύσιμες, βλ. Παράδειγμα 6.2.13, αλλά δεν είναι μηδενοδύναμες, αφού έχουν αμφότερες τετριμμένο κέντρο.

Σύμφωνα με τη απόδειξη τής Πρότασης 6.3.4 κάθε p–ομάδα είναι μηδενοδύναμη.

Θα δώσουμε μια πλήρη περιγραφή των μηδενοδύναμων ομάδων. Αρχίζουμε με την

Πρόταση 6.3.7. *Έστω $\mathcal{F} = (G_i, \star_i)_{i \in \{1,2,\ldots,n\}}$ μια πεπερασμένη οικογένεια μηδενοδύναμων ομάδων. Το εξωτερικό ευθύ γινόμενο $\prod_{i=1}^n G_i$ των ομάδων τής οικογένειας $\mathcal{F}$ είναι επίσης μια μηδενοδύναμη ομάδα.*

Απόδειξη. Θα αποδείξουμε ότι το εξωτερικό ευθύ γινόμενο $G = H \times K$ δύο μηδενοδύναμων ομάδων H και K είναι επίσης μια μηδενοδύναμη ομάδα, αφού κατόπιν με μια απλή επαγωγική απόδειξη μπορούμε άμεσα καταλήξουμε στο συμπέρασμα τού θεωρήματος.

Ισχυριζόμαστε ότι για κάθε $i \in \mathbb{N} \bigcup \{0\}$, το ανώτερο κέντρο $\mathcal{Z}_i(G)$ τού ευθέος γινομένου $G = H \times K$ οποιωνδήποτε δύο ομάδων $H \times K$ ισούται με το ευθύ γινόμενο $\mathcal{Z}_i(H) \times \mathcal{Z}_i(K)$ των ανώτερων κέντρων $\mathcal{Z}_i(H)$ και $\mathcal{Z}_i(K)$ των ομάδων H και K.
Θα εκτελέσουμε την απόδειξη με επαγωγή ως προς i:
Για $i = 0$, έχουμε $\mathcal{Z}_0(G) = \mathcal{Z}_0(H \times K) = \{(e_H, e_K)\} = \{e_H\} \times \{e_K\} = \mathcal{Z}_0(H) \times \mathcal{Z}_0(K)$. Αλλά και για $i = 1$, είναι επίσης άμεση η διαπίστωση ότι το κέντρο τού ευθέος γινομένου δύο ομάδων H, K, δηλαδή το $\mathcal{Z}_1(G) = \mathcal{Z}_1(H \times K)$, ισούται με το ευθύ γινόμενο $\mathcal{Z}_1(H) \times \mathcal{Z}_1(K)$ των κέντρων $\mathcal{Z}_1(H)$ και $\mathcal{Z}_1(K)$.
Έστω ότι ο ισχυρισμός είναι αληθής για $i = n$, δηλαδή ότι το $\mathcal{Z}_n(G) = \mathcal{Z}_n(H \times K)$, ισούται με το ευθύ γινόμενο $\mathcal{Z}_n(H) \times \mathcal{Z}_n(K)$. Θα αποδείξουμε τον ισχυρισμό για $i = n+1$, δηλαδή ότι το $\mathcal{Z}_{n+1}(G) = \mathcal{Z}_{n+1}(H \times K)$, ισούται με το ευθύ γινόμενο $\mathcal{Z}_{n+1}(H) \times \mathcal{Z}_{n+1}(K)$.
Θεωρούμε τους φυσικούς επιμορφισμούς ομάδων

$$\pi_H : H \to H/\mathcal{Z}_n(H) \text{ και } \pi_K : K \to K/\mathcal{Z}_n(K)$$

καθώς και τον επιμορφισμό

$$\pi : G = H \times K \to H/\mathcal{Z}_n(H) \times K/\mathcal{Z}_n(K), g = (h, k) \mapsto \pi(g) := (\pi_H(h), \pi_K(k)),$$

ο οποίος επάγεται από τους π_H, π_K. Θεωρούμε επίσης τον ισομορφισμό ομάδων

$$\begin{aligned} &\psi : H/\mathcal{Z}_n(H) \times K/\mathcal{Z}_n(K) \to (H \times K)/(\mathcal{Z}_n(H) \times \mathcal{Z}_n(K)), \\ &(h\mathcal{Z}_n(H), k\mathcal{Z}_n(K)) \mapsto \psi\left((h\mathcal{Z}_n(H), k\mathcal{Z}_n(K))\right) := (h, k)(\mathcal{Z}_n(H) \times \mathcal{Z}_n(K)). \end{aligned}$$

(Σημειώνουμε, ότι γενικώς, αν H, K είναι ομάδες και $A \trianglelefteq H$, $B \trianglelefteq K$ είναι ορθόθετες υποομάδες τους, τότε $A \times B \trianglelefteq H \times K$ και η απεικόνιση

$$H/A \times K/B \to (H \times K)/(A \times B), (hA, kB) \mapsto (h, k)(A \times B)$$

είναι ένας ισομορφισμός ομάδων, (*γιατί;*).)
Παρατηρούμε ότι, λόγω τής επαγωγικής υπόθεσης, η υποομάδα $\mathcal{Z}_n(H) \times \mathcal{Z}_n(K)$ ισούται με $\mathcal{Z}_n(H \times K)$ και γι΄αυτό η σύνθεση

$$\begin{aligned}\psi \circ \pi : G = H \times K \to& (H \times K)/\mathcal{Z}_n(H \times K),\\ g = (h, k) \mapsto& \psi \circ \pi((h, k)) = \psi \circ \pi(g) =\\ &\psi((\pi_H(h), \pi_K(k))) = (h, k)\mathcal{Z}_n(H \times K) = g\mathcal{Z}_n(H \times K) = g\mathcal{Z}_n(G)\end{aligned}$$

συμπίπτει με τον φυσικό επιμορφισμό ομάδων

$$\varphi : G \to G/\mathcal{Z}_n(G), g \mapsto g\mathcal{Z}_n(G).$$

Για το ανώτερο κέντρο $\mathcal{Z}_{n+1}(G)$ έχουμε:

$$\begin{aligned}&\mathcal{Z}_{n+1}(G) = \varphi^{-1}\left(\mathcal{Z}(G/\mathcal{Z}_n(G))\right) = \pi^{-1}\left(\psi^{-1}\left(\mathcal{Z}(G/\mathcal{Z}_n(G))\right)\right) =\\ &\pi^{-1}\left(\mathcal{Z}(H/\mathcal{Z}_n(H) \times K/\mathcal{Z}_n(K))\right),\end{aligned}$$

αφού ο ψ είναι ένας ισομορφισμός.
Επιπλέον,

$$\begin{aligned}&\pi^{-1}\left(\mathcal{Z}(H/\mathcal{Z}_n(H) \times K/\mathcal{Z}_n(K))\right) =\\ &\pi_H^{-1}\left(\mathcal{Z}(H/\mathcal{Z}_n(H))\right) \times \pi_K^{-1}\left(K/\mathcal{Z}_n(K)\right)) = \mathcal{Z}_{n+1}(H) \times \mathcal{Z}_{n+1}(K),\end{aligned}$$

αφού ο π επάγεται από τους επιμορφισμούς π_H και π_K.

Αν τώρα οι H και K είναι μηδενοδύναμες ομάδες, τότε υπάρχουν $m, m' \in \mathbb{N}\bigcup\{0\}$ με $\mathcal{Z}_m(H) = H$ και $\mathcal{Z}_{m'}(K) = K$, και γι' αυτό επιλέγοντας το $\max\{m, m'\}$, έπεται ότι $\mathcal{Z}_{\max\{m,m'\}}(H \times K) = \mathcal{Z}_{\max\{m,m'\}}(H) \times \mathcal{Z}_{\max\{m,m'\}}(K) = H \times K$. Συνεπώς, το εξωτερικό ευθύ γινόμενο $H \times K$ είναι επίσης μια μηδενοδύναμη ομάδα. □

Πρόταση 6.3.8. *Έστω $(G, \star)$ είναι μια μηδενοδύναμη ομάδα. Αν $H \subsetneqq G$ είναι μια γνήσια υποομάδα της, τότε η H περιέχεται γνησίως στον ορθοθετοποιητή της $\mathcal{N}_G(H)$, δηλαδή $H \subsetneqq \mathcal{N}_G(H)$.*

Απόδειξη. Έστω ότι η G είναι μηδενοδύναμη κλάσης r και ότι $n \in \mathbb{N}\bigcup\{0\}$ είναι ο μεγαλύτερος μη αρνητικός ακέραιος με $\mathcal{Z}_n(G) \leq H$. Επειδή $H \subsetneqq G$, είναι προφανές ότι $n \leq r-1$. Αφού $\mathcal{Z}_{n+1}(G) \nleq H$, θα υπάρχει κάποιο $g \in \mathcal{Z}_{n+1}(G)$ με $g \notin H$. Θα αποδείξουμε ότι το συγκεκριμένο στοιχείο g περιέχεται στον ορθοθετοποιητή $\mathcal{N}_G(H)$, από όπου έπεται αμέσως ότι $H \subsetneqq \mathcal{N}_G(H)$.
Επειδή $\mathcal{Z}_{n+1}(G)/\mathcal{Z}_n(G) = \mathcal{Z}(G/\mathcal{Z}_n(G))$, το $g\mathcal{Z}_n(G)$ μετατίθεται με κάθε στοιχείο τής $G/\mathcal{Z}_n(G)$ και γι' αυτό μετατίθεται και με κάθε στοιχείο τής $H/\mathcal{Z}_n(G)$. Δηλαδή,

$$\forall h \in H, gh\mathcal{Z}_n(G) = hg\mathcal{Z}_n(G) \Leftrightarrow \forall h \in H, g^{-1}h^{-1}gh \in \mathcal{Z}_n(G).$$

Αφού όμως $\mathcal{Z}_n(G) \leq H$, συμπεραίνουμε ότι $\forall h \in H, g^{-1}h^{-1}g \in H \Leftrightarrow g \in \mathcal{N}_G(H)$. □

Θα εφαρμόσουμε αμέσως την προηγούμενη πρόταση κατά τη μελέτη των μηδενοδύναμων ομάδων, αλλά πρώτα είναι απαραίτητη η επόμενη έννοια:

Ορισμός 6.3.9. Έστω $(G, \star)$ μια ομάδα. Μια γνήσια υποομάδα τής G ονομάζεται *μεγιστοτική*, αν δεν περιέχεται σε καμιά άλλη γνήσια υποομάδα τής G.

Δηλαδή η υποομάδα $H \leq G$ είναι μεγιστοτική, αν $H \lneqq G$ και αν από $H \leq L$, όπου $L \leq G$ είναι οποιαδήποτε υποομάδα τής G, έπεται ή $H = L$ ή $L = G$.

Παράδειγμα 6.3.10. Οι μεγιστοτικές υποομάδες τής $(\mathbb{Z}, +)$ συμπίπτουν με τις υποομάδες $\langle p \rangle$, όπου ο p είναι ένας πρώτος αριθμός. Πράγματι, αν $\langle a \rangle, a \in \mathbb{N} \bigcup \{0\}$ είναι μια υποομάδα τής $\mathbb{Z}$ και ο a είναι ίσος με μηδέν ή είναι σύνθετος αριθμός, ας πούμε $a = \kappa\lambda$, με $1 < \kappa, \lambda < a$, τότε $\langle a \rangle \subsetneqq \langle \kappa \rangle \subsetneqq \mathbb{Z}$. Αν τώρα $\langle p \rangle$ είναι μια υποομάδα τής $\mathbb{Z}$, όπου ο p είναι ένας πρώτος αριθμός και αν $\langle p \rangle \subseteq \langle a \rangle, a \in \mathbb{N}$, τότε $p = \kappa a, \kappa \in \mathbb{N}$. Επομένως, $a = 1$ ή $a = p$ και γι' αυτό ή $\langle a \rangle = \langle p \rangle$ ή $\langle a \rangle = \mathbb{Z}$ και γι΄αυτό η $\langle p \rangle$ είναι μια μεγιστοτική υποομάδα τής $\mathbb{Z}$.

Πόρισμα 6.3.11. *Οι μεγιστοτικές υποομάδες μιας μηδενοδύναμης ομάδας είναι ορθόθετες.*

Απόδειξη. Έστω ότι H είναι μια μεγιστοτική υποομάδα μιας μηδενοδύναμης ομάδας $(G, \star)$ και ότι $\mathcal{N}_G(H)$ είναι ο ορθοθετοποιητής της. Επειδή η H είναι γνήσια υποομάδα τής G, συμπεραίνουμε από την Πρόταση 6.3.8 ότι ο ορθοθετοποιητής $\mathcal{N}_G(H)$ περιέχει γνησίως την H και αφού η H είναι μεγιστοτική καταλήγουμε στο ότι $\mathcal{N}_G(H) = G$. Επομένως, η H είναι ορθόθετη υποομάδα τής G. □

Πόρισμα 6.3.12. *Οι Sylow υποομάδες μιας πεπερασμένης μηδενοδύναμης ομάδας $(G, \star)$ είναι ορθόθετες.*

Απόδειξη. Αν η G είναι μια p–ομάδα, τότε δεν χρειάζεται να αποδείξουμε κάτι, αφού η G συμπίπτει με τη μοναδική p–Sylow υποομάδα της.
Έστω ότι η G δεν είναι μια p–ομάδα, ότι q είναι ένας πρώτος διαιρέτης τής τάξης τής G και ότι Q είναι μια αντίστοιχη q–Sylow υποομάδα τής G. Επειδή τώρα η Q είναι μια γνήσια υποομάδα τής G, συμπεραίνουμε από την Πρόταση 6.3.8 ότι η Q περιέχεται γνησίως εντός τού ορθοθετοποιητή της $\mathcal{N}_G(Q)$. Από την Πρόταση 3.1.9 γνωρίζουμε ότι ο ορθοθετοποιητής $\mathcal{N}_G(\mathcal{N}_G(Q))$ τής $\mathcal{N}_G(Q)$ συμπίπτει με την $\mathcal{N}_G(Q)$ και επειδή η G είναι μηδενοδύναμη, αυτό μπορεί να συμβαίνει, λόγω τής Πρότασης 6.3.8, μόνο, αν η $\mathcal{N}_G(Q)$ δεν είναι γνήσια υποομάδα τής G, δηλαδή μόνο, αν $\mathcal{N}_G(Q) = G$. Συνεπώς, η Q είναι μια ορθόθετη υποομάδα τής G. □

Θεώρημα 6.3.13. *Έστω $(G, \star)$ μια πεπερασμένη ομάδα. Η G είναι μηδενοδύναμη, αν και μόνο αν, είναι το εσωτερικό ευθύ γινόμενο των Sylow υποομάδων της.*

Απόδειξη. «$\Leftarrow$» Προφανώς, η G είναι ισόμορφη προς το εξωτερικό ευθύ γινόμενο των Sylow υποομάδων της. Αλλά κάθε Sylow υποομάδα είναι μια p–ομάδα για κάποιον κατάλληλο πρώτο αριθμό p και γι' αυτό κάθε Sylow υποομάδα είναι μηδενοδύναμη. Επομένως, η G είναι ισόμορφη προς ένα εξωτερικό ευθύ γινόμενο μια πεπερασμένης οικογένειας μηδενοδύναμων ομάδων και σύμφωνα με την Πρόταση 6.3.7 είναι και η ίδια μηδενοδύναμη.

«$\Rightarrow$» Έστω ότι η G είναι μια μηδενοδύναμη ομάδα. Αν η G είναι μια p–ομάδα, τότε δεν χρειάζεται να αποδείξουμε κάτι.
Έστω ότι η G δεν είναι p–ομάδα. Από το Πόρισμα 6.3.12 γνωρίζουμε ότι οποιαδήποτε Sylow υποομάδα τής G είναι ορθόθετη. Επομένως, σε κάθε πρώτο διαιρέτη τής τάξης τής G υπάρχει ακριβώς μία Sylow υποομάδα. Αφού λοιπόν ικανοποιούνται όλες οι υποθέσεις τού Λήμματος 4.1.11, συμπεραίνουμε ότι η G είναι το εσωτερικό ευθύ γινόμενο των Sylow υποομάδων της. □

Πόρισμα 6.3.14. *Κάθε υποομάδα και κάθε πηλικοομάδα μιας πεπερασμένης μηδενοδύναμης ομάδας $(G, \star)$ είναι επίσης μηδενοδύναμη.*

Απόδειξη. Από το Πόρισμα 6.3.12 γνωρίζουμε ότι όλες οι Sylow υποομάδες τής G είναι ορθόθετες και γι' αυτό σε κάθε πρώτο διαιρέτη p τής τάξης τής G υπάρχει ακριβώς μία p–Sylow υποομάδα. Ας είναι $P_1, P_2, \ldots, P_s$ οι Sylow υποομάδες που αντιστοιχούν στους διαφορετικούς πρώτους διαιρέτες $p_1, p_2, \ldots, p_s$ τής τάξης τής G.

Έστω ότι H είναι μια υποομάδα τής G. Για κάθε $i, 1 \leq i \leq s$, θεωρούμε την υποομάδα $H \bigcap P_i$ τής H. Προφανώς, η $H \bigcap P_i$ είναι ορθόθετη υποομάδα τής H, αφού η P_i είναι ορθόθετη υποομάδα τής G.
Αν δείξουμε ότι η $H \bigcap P_i$ είναι μια Sylow υποομάδα που αντιστοιχεί[1] στον πρώτο p_i και ότι κάθε Sylow υποομάδα τής H συμπίπτει με μια από τις $H \bigcap P_i$, τότε χρησιμοποιώντας το Λήμμα 4.1.11 συμπεραίνουμε ότι η H είναι το εσωτερικό ευθύ γινόμενο των Sylow υποομάδων της και λόγω τού Θεωρήματος 6.3.13 καταλήγουμε στο ότι η ομάδα H είναι μηδενοδύναμη.

Παρατηρούμε, ότι για κάθε $i, 1 \leq i \leq s$, η υποομάδα $H \bigcap P_i$ έχει ως τάξη μια δύναμη $p_i^{n_i}, n_i \in \mathbb{N} \bigcup \{0\}$ τού πρώτου p_i, αφού πρόκειται για μια υποομάδα τής P_i. Επιπλέον, ο δείκτης $[H : H \bigcap P_i] = [HP_i : P_i]$ δεν έχει ως παράγοντα τον πρώτο p_i, επειδή

$$[G : 1] = [G : P_i][P_i : 1] = [G : HP_i][HP_i : P_i][P_i : 1]$$

και επειδή η P_i έχει ως τάξη τη μεγαλύτερη δύναμη τού p_i που διαιρεί την τάξη τής G.
Επομένως, μεταξύ των υποομάδων τής H που έχουν ως τάξη μια δύναμη τού p_i, η υποομάδα $H \bigcap P_i$ έχει ως τάξη τη μεγαλύτερη δύναμη τού p_i και γι' αυτό είναι μια p_i–Sylow υποομάδα τής H. Επιπλέον, αν H_i είναι μια p_i–Sylow υποομάδα τής H, τότε από το Θεώρημα 3.1.5 (β′) συμπεραίνουμε ότι η H_i περιέχεται στην p_i–Sylow υποομάδα P_i τής G και γι' αυτό $H_i \leq H \bigcap P_i$ και αφού και οι δύο είναι p_i–Sylow υποομάδες συμπεραίνουμε ότι $H_i = H \bigcap P_i$.

Έστω ότι G/N είναι μια πηλικοομάδα τής G, όπου N είναι μια ορθόθετη υποομάδα τής G. Ακολουθούμε την ίδια μέθοδο όπως στην περίπτωση των υποομάδων. Για κάθε $i, 1 \leq i \leq s$, θεωρούμε την υποομάδα P_iN τής G και κατόπιν την υποομάδα P_iN/N τής G/N. Η P_iN είναι ορθόθετη υποομάδα τής G, αφού οι P_i και N είναι ορθόθετες υποομάδες τής G και η P_iN/N είναι επίσης ορθόθετη υποομάδα τής G/N.
Αν δείξουμε ότι η P_iN/N είναι μια Sylow υποομάδα που αντιστοιχεί στον πρώτο διαιρέτη p_i τής τάξης τής G/N, τότε κάθε Sylow υποομάδα τής G/N συμπίπτει με μια από τις

[1] Χωρίς βλάβη τής γενικότητας δεχόμαστε ότι αν ένας πρώτος p δεν διαιρεί την τάξη τής H, τότε η αντίστοιχη p–Sylow υποομάδα είναι η τετριμμένη υποομάδα $\{e_H\}$ τάξης $p^0 = 1$

P_iN/N, αφού οι τελευταίες είναι ορθόθετες υποομάδες τής G/N. Τότε χρησιμοποιώντας το Λήμμα 4.1.11 μπορούμε να συμπεράνουμε ότι η G/N είναι το εσωτερικό ευθύ γινόμενο των Sylow υποομάδων της και λόγω τού Θεωρήματος 6.3.13 να καταλήξουμε ότι η ομάδα G/N είναι μηδενοδύναμη.

Για κάθε πρώτο διαιρέτη p_i τής τάξης τής G, θεωρούμε την αντίστοιχη p_i–Sylow υποομάδα P_i και κατόπιν την πηλικοομάδα P_iN/N. Παρατηρούμε ότι η τάξη τής P_iN/N είναι μια δύναμη ≥ 0 τού p_i, αφού η P_iN/N είναι ισόμορφη προς την πηλικοομάδα $P_i/P_i \bigcap N$. Επιπλέον, η τάξη τής P_iN/N ισούται με 1, αν και μόνο αν, $P_i \leq N$.
Τέλος, η P_iN/N έχει ως τάξη τη μεγαλύτερη δύναμη τού p_i μεταξύ των υποομάδων τής G/N, που έχουν ως τάξη μια δύναμη τού p_i, αφού

$$[G/N : P_iN/N] = \frac{[G:1]}{[N:1]} \cdot \frac{[N:1]}{[P_iN:1]} = [G : P_iN].$$

και ο δείκτης $[G : P_iN]$ δεν έχει ως παράγοντα τον πρώτο p_i, ως διαιρέτης τού δείκτη $[G : P_i] = [G : P_iN][P_iN : P_i]$, ο οποίος δεν έχει ως παράγοντα τον πρώτο p_i. Συνεπώς, η P_iN/N είναι μια p_i–Sylow υποομάδα για κάθε πρώτο διαιρέτη p_i τής τάξης τής G/N. Η απόδειξη έχει ολοκληρωθεί. $\square$

Ολοκληρώνουμε τη στοιχειώδη μελέτη για τις μηδενοδύναμες ομάδες με την εξής αξιοσημείωτη

Πρόταση 6.3.15. *Έστω ότι $(G, \star)$ είναι μια μηδενοδύναμη πεπερασμένη ομάδα τάξης ≥ 2. Αν $N \neq \{e_G\}$ είναι μια οποιαδήποτε ορθόθετη υποομάδα τής G, τότε η τομή τής N με το κέντρο $\mathcal{Z}(G)$ τής G είναι πάντοτε μη τετριμμένη.*

Απόδειξη. Θεωρούμε πρώτα την ειδική περίπτωση, όπου η G είναι μια p–ομάδα. Παρατηρούμε ότι η N είναι μια αποσυνδετή ένωση από κλάσεις συζυγίας τής G, αφού πρόκειται για μια ορθόθετη υποομάδα τής G.
Έστω ότι $N = (\bigcup_{i=1}^{c} \mathcal{K}_i) \bigcup \mathcal{X}$, όπου $\mathcal{K}_i, 1 \leq i \leq c$, είναι οι κλάσεις συζυγίας που περιέχονται στην N και έχουν ακριβώς ένα στοιχείο και όπου $\mathcal{X} = \bigcup_{j=1}^{s} \mathcal{A}_j$ είναι η ένωση των κλάσεων συζυγίας $\mathcal{A}_j, 1 \leq j \leq s$ με περισσότερα τού ενός στοιχεία. Σημειώστε, ότι σε κάθε περίπτωση υπάρχει τουλάχιστον μια κλάση συζυγίας με ακριβώς ένα στοιχείο, ως εκ τούτου $c \geq 1$, ενώ το σύνολο $\mathcal{X}$ μπορεί να είναι το κενό σύνολο. Επιπλέον προσέξτε ότι αφού η G είναι μια p–ομάδα, το πλήθος των στοιχείων κάθε κλάσης $\mathcal{A}_j, 1 \leq j \leq s$ (όταν αυτή υπάρχει) ισούται με p^{α_j}, $\alpha_j \in \mathbb{N}$
Για το πλήθος των στοιχείων p^{λ}, $\lambda \in \mathbb{N}$, τής υποομάδας N ισχύει η ισότητα

$$p^{\lambda} = c + \varepsilon(p^{\alpha_1} + \cdots + p^{\alpha_s}),$$

όπου $\varepsilon = 0$, όταν το $\mathcal{X} = \emptyset$ και $\varepsilon = 1$, όταν το $\mathcal{X} \neq \emptyset$.
Όμως σε αμφότερες τις περιπτώσεις $\varepsilon = 0$ ή 1, το πλήθος c των κλάσεων συζυγίας $\mathcal{K}_i$ με ακριβώς ένα στοιχείο, οι οποίες περιέχονται στην N, είναι γνησίως μεγαλύτερο από 1, αφού ο πρώτος p διαιρεί πάντοτε τον c. Επειδή κάθε κλάση συζυγίας με ακριβώς ένα στοιχείο περιέχεται και στο κέντρο $\mathcal{Z}(G)$ τής G, συμπεραίνουμε ότι $\bigcup_{i=1}^{c} \mathcal{K}_i \leq \mathcal{Z}(G)$. Επομένως, $N \bigcap \mathcal{Z}(G) \neq \{e_G\}$.

Θεωρούμε τώρα τη γενική περίπτωση, όπου η G είναι οποιαδήποτε πεπερασμένη μηδενοδύναμη ομάδα. Σύμφωνα με το Θεώρημα 6.3.13, η G είναι το εσωτερικό ευθύ γινόμενο $P_1 \cdot P_2 \cdot \ldots \cdot P_s$ των Sylow υποομάδων της. Επειδή η ορθόθετη υποομάδα N έχει τάξη > 1, υπάρχει ένας πρώτος διαιρέτης p_i τής τάξης τής G, ο οποίος είναι και πρώτος διαιρέτης τής τάξης τής N. Γι' αυτό υπάρχει μια υποομάδα τής N τάξης p_i, η οποία οφείλει να περιέχεται στη μοναδική p_i–Sylow υποομάδα, ας πούμε την P_i τής G. Επομένως, $N \bigcap P_i \neq \{e_G\}$ και προφανώς η $N \bigcap P_i$ είναι μια ορθόθετη υποομάδα τής P_i. Αλλά η τάξη τής P_i είναι μια θετική δύναμη τού πρώτου p_i, δηλαδή η P_i είναι μια p–ομάδα. Γι' αυτό από το πρώτο μέρος τής απόδειξης, συμπεραίνουμε ότι $(N \bigcap P_i) \bigcap \mathcal{Z}(P_i) \neq \{e_G\}$. Δηλαδή υπάρχει τουλάχιστον ένα στοιχείο τής N που ανήκει στο κέντρο τής P_i. Αλλά κάθε στοιχείο τής P_i που ανήκει στο κέντρο της, ανήκει και στο κέντρο τής G, αφού η G είναι το εσωτερικό ευθύ γινόμενο των $P_1, P_2, \ldots, P_i, \ldots, P_s$. Συνεπώς, $N \bigcap \mathcal{Z}(G) \neq \{e_G\}$. □

Οι άνω κεντρική Σειρά τής διεδρικής Ομάδας $(D_n, \circ), n \geq 3$

Διακρίνουμε τις περιπτώσεις: (I) n περιττός ≥ 3, (II) $n = 2^k m$, $k \in \mathbb{N}$, m περιττός > 1 και (III) $n = 2^k, k \geq 2$.

Περίπτωση (I): Ως γνωστόν, εδώ το κέντρο $\mathcal{Z}(D_n)$ είναι τετριμμένο, δηλαδή $\mathcal{Z}(D_n) = \{\mathrm{Id}_n\}$ και γι' αυτό $\mathcal{Z}_i(D_n) = \{\mathrm{Id}_n\}, \forall i \in \mathbb{N} \cup \{0\}$.

Επομένως, η άνω κεντρική σειρά τής D_n είναι η

$$\{\mathrm{Id}_n\} = \mathcal{Z}_0(D_n) = \mathcal{Z}_1(D_n) = \cdots = \mathcal{Z}_i(D_n) = \mathcal{Z}_{i+1}(D_n) = \ldots$$

Προσέξτε ότι σύμφωνα με τον Ορισμό 6.3.5, η D_n δεν είναι μηδενοδύναμη, μολονότι είναι επιλύσιμη.

Περίπτωση (II): Εδώ, το κέντρο $\mathcal{Z}(D_{2^k m})$ ισούται με $\langle \rho^{2^{k-1}m} \rangle$, συνεπώς $\mathcal{Z}_1(D_{2^k m}) = \langle \rho^{2^{k-1}m} \rangle$.

Θα υπολογίσουμε τον όρο $\mathcal{Z}_2(D_{2^k m})$. Έχουμε: $D_{2^k m}/\mathcal{Z}_1(D_{2^k m}) = D_{2^k m}/\langle \rho^{2^{k-1}m} \rangle$. Από την Άσκηση ΠΑ82, γνωρίζουμε ότι $D_{2^k m}/\langle \rho^{2^{k-1}m} \rangle \cong D_{2^{k-1}m}$ και γι' αυτό το κέντρο τής $D_{2^k m}/\langle \rho^{2^{k-1}m} \rangle$ ισούται με $\{\langle \rho^{2^{k-1}m} \rangle, \rho^{2^{k-2}m} \langle \rho^{2^{k-1}m} \rangle\}$. Επομένως, $\mathcal{Z}_2(D_{2^k m}) = \langle \rho^{2^{k-2}m} \rangle$ και επαγωγικά συμπεραίνουμε ότι για $i, 1 \leq i \leq k$, είναι $\mathcal{Z}_i(D_{2^k m}) = \langle \rho^{2^{k-i}m} \rangle$.

Τώρα, παρατηρούμε ότι η πηλικοομάδα $D_{2^k m}/\mathcal{Z}_k(D_{2^k m}) = D_{2^k m}/\langle \rho^m \rangle$ είναι ισόμορφη προς την D_m τής οποίας το κέντρο είναι τετριμμένο, αφού ο m είναι περιττός. Ως εκ τούτου, $\mathcal{Z}_i(D_{2^k m}) = \{\mathrm{Id}_n\}, \forall i \in \mathbb{N}, i > k$.

Επομένως, η άνω κεντρική σειρά τής $D_{2^k m}$ είναι η

$$\begin{aligned}
&\{\mathrm{Id}_n\} = \mathcal{Z}_0(D_{2^k m}) < \mathcal{Z}_1(D_{2^k m}) = \langle \rho^{2^{k-1}m} \rangle < \mathcal{Z}_2(D_{2^k m}) = \langle \rho^{2^{k-2}m} \rangle < \ldots \\
&< \mathcal{Z}_i(D_{2^k m}) = \langle \rho^{2^{k-i}m} \rangle < \cdots < \mathcal{Z}_k(D_{2^k m}) = \langle \rho^m \rangle < \mathcal{Z}_{k+1}(D_{2^k m}) = \{\mathrm{Id}_n\} = \ldots
\end{aligned}$$

Προσέξτε ότι σύμφωνα με τον Ορισμό 6.3.5, η $D_{2^k m}$ δεν είναι μηδενοδύναμη, μολονότι είναι επιλύσιμη ομάδα.

Περίπτωση (III): Εδώ το κέντρο $\mathcal{Z}(D_{2^k}), k \geq 2$ ισούται με $\langle \rho^{2^{k-1}} \rangle$, συνεπώς $\mathcal{Z}_1(D_{2^k}) = \langle \rho^{2^{k-1}} \rangle$.

Ακριβώς όπως και προηγουμένως διαπιστώνουμε ότι για $i, 1 \leq i \leq k-1$, είναι $\mathcal{Z}_i(D_{2^k}) = \langle \rho^{2^{k-i}} \rangle$. Ιδιαιτέρως, $\mathcal{Z}_{k-1}(D_{2^k}) = \langle \rho^2 \rangle$. Θα υπολογίσουμε τώρα τον όρο $\mathcal{Z}_k(D_{2^k})$.

Από την Άσκηση ΠΑ82, γνωρίζουμε ότι η πηλικοομάδα $D_{2^k}/\mathcal{Z}_{k-1}(D_{2^k}) = D_{2^k}/\langle \rho^2 \rangle$ είναι ισόμορφη προς την $\mathbb{Z}_2 \times \mathbb{Z}_2$, η οποία είναι αβελιανή. Ως εκ τούτου, $\mathcal{Z}(D_{2^k}/\langle \rho^2 \rangle) = D_{2^k}/\langle \rho^2 \rangle$ και $\mathcal{Z}_k(D_{2^k}) = D_{2^k}$. Συνεπώς, $\mathcal{Z}_j(D_{2^k}) = D_{2^k}, \forall j \geq k, j \in \mathbb{N}$.

Επομένως, η άνω κεντρική σειρά τής $D_{2^k}, k \geq 2$, είναι η

$$\{\mathrm{Id}_n\} = \mathcal{Z}_0(D_{2^k}) < \mathcal{Z}_1(D_{2^k}) = \langle \rho^{2^{k-1}} \rangle < \mathcal{Z}_2(D_{2^k}) = \langle \rho^{2^{k-2}} \rangle < \dots$$
$$\dots < \mathcal{Z}_i(D_{2^k}) = \langle \rho^{2^{k-i}} \rangle < \dots < \mathcal{Z}_{k-1}(D_{2^k}) = \langle \rho^2 \rangle < \mathcal{Z}_k(D_{2^k}) = D_{2^k} = \mathcal{Z}_{k+1}(D_{2^k}) = \dots$$

Προσέξτε ότι στη συγκεκριμένη περίπτωση η επιλύσιμη ομάδα D_{2^k} είναι σύμφωνα με τον Ορισμό 6.3.5 μηδενοδύναμη. Αυτό όμως το γνωρίζαμε ήδη και από την απόδειξη τής Πρότασης 6.3.4, διότι η D_{2^k} είναι μια p- ομάδα, αφού η τάξη της είναι 2^{k+1}.

6.4 Οι Ομάδες τάξης <60 είναι επιλύσιμες

Συμπληρώνουμε τη στοιχειώδη μελέτη των επιλύσιμων ομάδων αποδεικνύοντας το

Θεώρημα 6.4.1. *Κάθε ομάδα τάξης < 60 είναι επιλύσιμη.*

Απόδειξη. Από την Πρόταση 6.3.4 γνωρίζουμε ότι κάθε ομάδα $(G, \star)$ με τάξη $p^i, i \in \mathbb{N}$, όπου ο p είναι πρώτος αριθμός είναι επιλύσιμη.

Από την Πρόταση 3.2.2 γνωρίζουμε ότι κάθε ομάδα $(G, \star)$ με τάξη pq, όπου p, q πρώτοι αριθμοί με $p < q$ είναι διαθέτει μια ορθόθετη υποομάδα N τάξης q, που προφανώς είναι επιλύσιμη. Η αντίστοιχη πηλικοομάδα G/N είναι μια ομάδα τάξης p και ως εκ τούτου επιλύσιμη. Αφού οι N και G/N είναι επιλύσιμες, συμπεραίνουμε ότι και η G είναι επιλύσιμη, λόγω τής Πρότασης 6.2.12.

Τέλος, από την Πρόταση 3.2.4 γνωρίζουμε ότι κάθε ομάδα με τάξη p^2q, όπου p, q πρώτοι αριθμοί με $p \neq q$, διαθέτει μια ορθόθετη υποομάδα N τάξης q, p ή p^2, που γνωρίζουμε ότι είναι επιλύσιμη. Η πηλικοομάδα G/N είναι μια ομάδα με τάξη αντιστοίχως p^2, pq ή q, η οποία σύμφωνα με όσα προείπαμε είναι επιλύσιμη. Αφού οι N και G/N είναι επιλύσιμες, συμπεραίνουμε, λόγω τής Πρότασης 6.2.12, ότι και η G είναι επιλύσιμη.

Οι μόνοι αριθμοί n με $1 \leq n \leq 59$ που δεν εμπίπτουν στις ανωτέρω περιπτώσεις είναι οι

(α′) $24 = 2^3 \cdot 3$, (β′) $30 = 2 \cdot 3 \cdot 5$, (γ′) $36 = 2^2 \cdot 3^2$, (δ′) $40 = 2^3 \cdot 5$,
(ε′) $42 = 2 \cdot 3 \cdot 7$, (στ′) $48 = 2^4 \cdot 3$, (ζ′) $54 = 2 \cdot 3^3$ και (η′) $56 = 2^3 \cdot 7$.

Η περίπτωση (α′), τάξη 24. Θα δείξουμε ότι μια ομάδα $(G, \star)$ τάξης 24 διαθέτει μια ορθόθετη υποομάδα N ή τάξης $4 = 2^2$ ή τάξης $8 = 2^3$. Η αντίστοιχη πηλικοομάδα G/N θα έχει ή τάξη $6 = 2 \cdot 3$ ή τάξη 3. Αφού οι N και G/N είναι επιλύσιμες, τότε θα είναι και η G επιλύσιμη.

Για το πλήθος n_2 των 2–Sylow υποομάδων έχουμε: $n_2 \equiv 1 \mathrm{mod} 2$ και $n_2/3$. Επομένως, $n_2 = 1$ ή 3.

Αν $n_2 = 1$, τότε υπάρχει μια ορθόθετη υποομάδα τάξης $8 = 2^3$. Αν $n_2 = 3$, τότε θα δείξουμε ότι υπάρχει μια ορθόθετη υποομάδα τάξης 4. Πράγματι, αφού $n_2 = 3$, υπάρχουν ακριβώς τρεις υποομάδες P, Q, R τάξης 8. Θεωρούμε δύο εξ αυτών, ας πούμε τις P, Q. Για το πλήθος των στοιχείων τού συνόλου PQ έχουμε:

$$|PQ| = \frac{|P||Q|}{|P \bigcap Q|} = \frac{2^3 \cdot 2^3}{|P \bigcap Q|}.$$

Παρατηρούμε ότι η τάξη τής υποομάδας $P \bigcap Q$ είναι ένας διαιρέτης τού 2^3. Η τάξη τής $P \bigcap Q$ δεν μπορεί να είναι 2^3 διότι $P \neq Q$, αλλά επίσης δεν είναι ούτε 1 ούτε 2, αφού τότε το πλήθος τού συνόλου PQ είναι αντιστοίχως $2^3 \cdot 2^3 = 64$ και $(2^3 \cdot 2^3)/2 = 32$, πράγμα άτοπο αφού $|PQ| \leq |G| = 24$. Επομένως, η τάξη τής υποομάδας $P \bigcap Q$ είναι $2^2 = 4$. Επειδή οι δείκτες $[P : P \bigcap Q] = 2$ και $[Q : P \bigcap Q] = 2$, καταλήγουμε στο ότι η $P \bigcap Q$ είναι ορθόθετη υποομάδα και τής P και τής Q. Συνεπώς, η $P \bigcap Q$ είναι ορθόθετη υποομάδα και τής $\langle P \bigcup Q \rangle$, δηλαδή τής υποομάδας που παράγεται από το $P \bigcup Q$. Αλλά, η $\langle P \bigcup Q \rangle$ περιέχει το σύνολο PQ, το οποίο έχει 16 στοιχεία, αφού $|P \bigcap Q| = 4$. Όμως η μοναδική υποομάδα τής G που έχει τουλάχιστον 16 στοιχεία είναι η ίδια η G, αφού $|G| = 24$. Γι' αυτό $\langle P \bigcup Q \rangle = G$ και η $P \bigcap Q$ είναι μια ορθόθετη υποομάδα τής G τάξης 4.

$\boxed{\text{Η περίπτωση (β′), τάξη 30.}}$ Από την Πρόταση 3.2.14 γνωρίζουμε ότι κάθε ομάδα $(G, \star)$ τάξης 30 διαθέτει μια ορθόθετη υποομάδα N τάξης 5. Η πηλικοομάδα G/N έχει τάξη $6 = 2 \cdot 3$. Αφού οι N και G/N είναι επιλύσιμες, συμπεραίνουμε ότι και η G είναι επιλύσιμη.

$\boxed{\text{Η περίπτωση (γ′), τάξη 36.}}$ Θα δείξουμε ότι μια ομάδα $(G, \star)$ τάξης 36 διαθέτει μια ορθόθετη υποομάδα N ή τάξης $9 = 3^2$ ή τάξης 3. Η αντίστοιχη πηλικοομάδα G/N θα έχει ή τάξη $4 = 2^2$ ή τάξη $12 = 2^2 \cdot 3$. Αφού οι N και G/N είναι επιλύσιμες, τότε θα είναι και η G επιλύσιμη.

Για το πλήθος n_3 των 3–Sylow υποομάδων έχουμε: $n_3 \equiv 1 \bmod 3$ και $n_3/4$. Επομένως, $n_3 = 1$ ή 4.

Αν $n_3 = 1$, τότε υπάρχει μια ορθόθετη υποομάδα τάξης $9 = 3^2$. Αν $n_3 = 4$, τότε θα δείξουμε ότι υπάρχει μια ορθόθετη υποομάδα τάξης 3. Πράγματι, αφού $n_3 = 4$, υπάρχουν ακριβώς τέσσερεις υποομάδες P, Q, R, S τάξης 9. Θεωρούμε δύο εξ αυτών, ας πούμε τις P, Q. Για το πλήθος των στοιχείων τού συνόλου PQ έχουμε:

$$|PQ| = \frac{|P||Q|}{|P \bigcap Q|} = \frac{3^2 \cdot 3^2}{|P \bigcap Q|}.$$

Παρατηρούμε ότι η τάξη τής υποομάδας $P \bigcap Q$ είναι ένας διαιρέτης τού 3^2. Η τάξη τής $P \bigcap Q$ δεν μπορεί να είναι 3^2 διότι $P \neq Q$, αλλά επίσης δεν είναι 1, αφού τότε το πλήθος τού συνόλου PQ είναι $3^2 \cdot 3^2 = 81$, πράγμα άτοπο αφού $|PQ| \leq |G| = 36$. Επομένως, η τάξη τής υποομάδας $P \bigcap Q$ είναι 3. Οι P, Q είναι αβελιανές ομάδες, αφού έχουν ως τάξη το τετράγωνο ενός πρώτου αριθμού, δηλαδή το 3^2. Τώρα η $P \bigcap Q$ είναι ορθόθετη υποομάδα και τής P και τής Q. Συνεπώς, η $P \bigcap Q$ είναι ορθόθετη υποομάδα και τής $\langle P \bigcup Q \rangle$, δηλαδή τής υποομάδας που παράγεται από το $P \bigcup Q$. Αλλά, η $\langle P \bigcup Q \rangle$ περιέχει το σύνολο PQ, το οποίο έχει 27 στοιχεία, αφού $|P \bigcap Q| = 3$. Όμως η μοναδική υποομάδα τής G που έχει τουλάχιστον 27 στοιχεία είναι η ίδια η G, αφού $|G| = 36$. Γι' αυτό $\langle P \bigcup Q \rangle = G$ και η $P \bigcap Q$ είναι μια ορθόθετη υποομάδα τής G τάξης 3.

Η περίπτωση (δ′), τάξη 40. Θα δείξουμε ότι μια ομάδα $(G, \star)$ τάξης $40 = 2^3 \cdot 5$ διαθέτει μια ορθόθετη υποομάδα N τάξης 5. Η αντίστοιχη πηλικοομάδα G/N θα έχει τάξη $8 = 2^3$. Αφού οι N και G/N είναι επιλύσιμες, τότε θα είναι και η G επιλύσιμη.
Για το πλήθος n_5 των 5–Sylow υποομάδων έχουμε: $n_5 \equiv 1 \bmod 5$ και $n_5/8$. Επομένως, $n_5 = 1$ και γι' αυτό υπάρχει μια ορθόθετη υποομάδα N τάξης 5.

Η περίπτωση (ε′), τάξη 42. Θα δείξουμε ότι μια ομάδα $(G, \star)$ τάξης $42 = 2 \cdot 3 \cdot 7$ διαθέτει μια ορθόθετη υποομάδα N τάξης 7. Η αντίστοιχη πηλικοομάδα G/N θα έχει τάξη $6 = 2 \cdot 3$. Αφού οι N και G/N είναι επιλύσιμες, τότε θα είναι και η G επιλύσιμη.
Για το πλήθος n_7 των 7–Sylow υποομάδων έχουμε: $n_7 \equiv 1 \bmod 7$ και $n_7/6$. Επομένως, $n_7 = 1$ και γι' αυτό υπάρχει μια ορθόθετη υποομάδα N τάξης 7.

Η περίπτωση (στ′, τάξη 48). Θα δείξουμε ότι μια ομάδα $(G, \star)$ τάξης $48 = 2^4 \cdot 3$ διαθέτει μια ορθόθετη υποομάδα N ή τάξης $16 = 2^3$ ή τάξης 8. Η αντίστοιχη πηλικοομάδα G/N θα έχει ή τάξη 3 ή τάξη $6 = 2 \cdot 3$. Αφού οι N και G/N είναι επιλύσιμες, τότε θα είναι και η G επιλύσιμη.
Για το πλήθος n_2 των 2–Sylow υποομάδων έχουμε: $n_2 \equiv 1 \bmod 2$ και $n_2/3$. Επομένως, $n_2 = 1$ ή 3.
Αν $n_2 = 1$, τότε υπάρχει μια ορθόθετη υποομάδα τάξης $16 = 2^3$. Αν $n_2 = 3$, τότε θα δείξουμε ότι υπάρχει μια ορθόθετη υποομάδα τάξης 8. Πράγματι, αφού $n_2 = 3$, υπάρχουν ακριβώς τρεις υποομάδες P, Q, R τάξης 16. Θεωρούμε δύο εξ αυτών, ας πούμε τις P, Q. Για το πλήθος των στοιχείων τού συνόλου PQ έχουμε:

$$|PQ| = \frac{|P||Q|}{|P \bigcap Q|} = \frac{2^4 \cdot 2^4}{|P \bigcap Q|}.$$

Παρατηρούμε ότι η τάξη τής υποομάδας $P \bigcap Q$ είναι ένας διαιρέτης τού 2^4. Η τάξη τής $P \bigcap Q$ δεν μπορεί να είναι 2^4 διότι $P \neq Q$, αλλά επίσης δεν είναι ούτε 1 ούτε 2 ούτε 4, αφού τότε το πλήθος τού συνόλου PQ είναι αντιστοίχως $2^8 = 256, 2^7 = 128, 2^6 = 64$, πράγμα άτοπο αφού $|PQ| \leq |G| = 48$. Επομένως, η τάξη τής υποομάδας $P \bigcap Q$ είναι 8. Επειδή οι δείκτες $[P : P \bigcap Q] = 2$ και $[Q : P \bigcap Q] = 2$, καταλήγουμε στο ότι η $P \bigcap Q$ είναι ορθόθετη υποομάδα και τής P και τής Q. Συνεπώς, η $P \bigcap Q$ είναι ορθόθετη υποομάδα και τής $\langle P \bigcup Q \rangle$, δηλαδή τής υποομάδας που παράγεται από το $P \bigcup Q$. Αλλά, η $\langle P \bigcup Q \rangle$ περιέχει το σύνολο PQ, το οποίο έχει 32 στοιχεία, αφού $|P \bigcap Q| = 8$. Όμως η μοναδική υποομάδα τής G που έχει τουλάχιστον 32 στοιχεία είναι η ίδια η G, αφού $|G| = 48$. Γι' αυτό $\langle P \bigcup Q \rangle = G$ και η $P \bigcap Q$ είναι μια ορθόθετη υποομάδα τής G τάξης 8.

Η περίπτωση (ζ′), τάξη 54. Έστω $(G, \star)$ είναι μια ομάδα τάξης $54 = 2 \cdot 3^3$. Από τη Θεωρία Sylow γνωρίζουμε ότι η υπάρχει μια υποομάδα N τάξης 2^3. Ο δείκτης $[G : N]$ ισούται με 2. Επομένως, η N είναι μια ορθόθετη υποομάδα τής G με τάξη 3^3, δηλαδή δύναμη πρώτου αριθμού και γι' αυτό είναι μια επιλύσιμη ομάδα. Η πηλικοομάδα G/N είναι προφανώς επιλύσιμη. Συνεπώς, η G είναι μια επιλύσιμη ομάδα.

Η περίπτωση (η′), τάξη 56. Θα δείξουμε ότι μια ομάδα $(G, \star)$ τάξης $56 = 2^3 \cdot 7$ διαθέτει μια ορθόθετη υποομάδα N ή τάξης 7 ή τάξης $2^3 = 8$. Η αντίστοιχη πηλικοομάδα G/N θα έχει ή τάξη 8 ή τάξη 7. Αφού οι N και G/N είναι επιλύσιμες, τότε θα είναι και η G

επιλύσιμη.
Για το πλήθος n_7 των 7–Sylow υποομάδων έχουμε: $n_7 \equiv 1 \bmod 7$ και $n_7/2^3$. Επομένως, $n_7 = 1$ ή 8.
Αν $n_7 = 1$, τότε υπάρχει μια ορθόθετη υποομάδα τάξης 7. Αν $n_7 = 8$, τότε οι οκτώ στο πλήθος 7–Sylow υποομάδες χορηγούν $8 \times 6 = 48$ στοιχεία τάξης 7. θα δείξουμε ότι υπάρχει μια ορθόθετη υποομάδα τάξης 8. Από τη Θεωρία Sylow γνωρίζουμε ότι η υπάρχει τουλάχιστον μια υποομάδα H τάξης $2^3 = 8$. Έτσι συνολικά έχουμε $8 \times 6 + 8 = 56$ στοιχεία στην G, συμπεριλαμβάνοντας σε αυτά και το ουδέτερο στοιχείο τής G. Αν η H δεν ήταν ορθόθετη θα υπήρχε μια συζυγής K τής H, η οποία θα είχε επίσης οκτώ στοιχεία και σίγουρα ένα στοιχείο που δεν θα ανήκε στην H. Αυτό το στοιχείο θα ήταν τάξης ή 2 ή 4 ή 8. Συνεπώς, θα ήταν διαφορετικό από 48 στοιχεία τάξης 7. Έτσι συνολικά διαπιστώνουμε ότι η G έχει τουλάχιστον $56 + 1 = 57$ στοιχεία. Αυτό είναι αδύνατο, αφού $|G| = 56$. Επομένως, υπάρχει ακριβώς μία Sylow υποομάδα τάξης $2^3 = 8$, η οποία τώρα είναι προφανώς ορθόθετη. □

Ολοκληρώνουμε την παρούσα ενότητα με δύο πολύ σημαντικά θεωρήματα που η απόδειξή τους δεν μπορεί να γίνει εδώ αφού δεν έχουμε απαραίτητα εργαλεία:

Θεώρημα 6.4.2 (Το $p^\alpha q^\beta$ Θεώρημα Burnside). *Για οποιουσδήποτε πρώτους αριθμούς p και q, κάθε ομάδα $(G, \star)$ τάξης $p^\alpha q^\beta$ είναι επιλύσιμη.*

Το θεώρημα αυτό αποδείχθηκε από τον Burnside το 1904 με τη βοήθεια τής Θεωρίας Χαρακτήρων. Μια απόδειξη με καθαρά μεθόδους Θεωρίας Ομάδων δόθηκε στις αρχές τού 1970.

Το επόμενο θεώρημα είναι το πλέον σημαντικό για τις επιλύσιμες ομάδες.

Θεώρημα 6.4.3 (Feit-Thompson, 1963). *Κάθε ομάδα $(G, \star)$ περιττής τάξης είναι επιλύσιμη.*

Η απόδειξη τού θεωρήματος είναι 255 σελίδες και καταλαμβάνει ένα ολόκληρο τεύχος τού Pacific Journal of Mathematics.

Ασκήσεις στις επιλύσιμες Ομάδες

Λυμένες Ασκήσεις

A 135. (α′) Να υπολογίσετε την παράγωγη ομάδα $\mathbb{A}_3'$ τής εναλλάσσουσας ομάδας $\mathbb{A}_3$.

Χωρίς να χρησιμοποιήσετε το ότι για $n \geq 5$, η $\mathbb{A}_n$ είναι απλή, να δειχθούν τα εξής:

(β′) Για $n \geq 5$, η παράγωγη υποομάδα $\mathbb{A}_n'$ τής $\mathbb{A}_n$ είναι η $\mathbb{A}_n$.

(γ′) Για $n \geq 5$, η παράγωγη υποομάδα S_n' τής συμμετρικής ομάδας S_n είναι η $\mathbb{A}_n$.

Λύση. (α′) Η $\mathbb{A}_3$ είναι αβελιανή, αφού είναι μια ομάδα τάξης 3. Γι' αυτό $\mathbb{A}_3' = \{\mathrm{Id}_{S_3}\}$.
(β′) Επειδή η παράγωγη υποομάδα $\mathbb{A}_n'$ είναι ορθόθετη υποομάδα τής $\mathbb{A}_n$ και $n \geq 5$, για να δείξουμε ότι $\mathbb{A}_n' = \mathbb{A}_n$, αρκεί να δείξουμε ότι η $\mathbb{A}_n'$ περιέχει έναν κύκλο μήκους 3, βλ.

Πόρισμα 3.2.21. Θεωρούμε τα στοιχεία $\sigma = \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}$ και $\tau = \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 5\end{pmatrix}$. Υπολογίζουμε τον μεταθέτη:

$$\begin{aligned}[\tau, \sigma] =& \tau \circ \sigma \circ \tau^{-1} \circ \sigma^{-1} = \\ & \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 5\end{pmatrix} \circ \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix} \circ \begin{pmatrix}3 & 5\end{pmatrix} \circ \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 2\end{pmatrix} = \\ & \begin{pmatrix}3 & 5 & 4\end{pmatrix} \in \mathbb{A}'_n.\end{aligned}$$

(γ′) Θεωρούμε τα στοιχεία $\sigma = \begin{pmatrix}2 & 3 & 4\end{pmatrix}$ και $\tau = \begin{pmatrix}1 & 2 & 3\end{pmatrix}$ τής S_n. Το $\sigma^{-1} \circ \tau^{-1} \circ \sigma \circ \tau$ είναι στοιχείο τής παράγωγης υποομάδας S'_n και ισούται με $\begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}$ που είναι στοιχείο τής $\mathbb{A}_n$. Συνεπώς, $S'_n \cap \mathbb{A}_n \neq \{\mathrm{Id}_{S_n}\}$. Αφού όμως η $S'_n \cap \mathbb{A}_n$ είναι μια ορθόθετη υποομάδα τής $\mathbb{A}_n$ που περιέχει το γινόμενο $\begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}$, το οποίο είναι γινόμενο δύο αποσυνδετών αντιμεταθέσεων, συμπεραίνουμε από την Άσκηση 121, ότι $S'_n \cap \mathbb{A}_n = \mathbb{A}_n$ και ως εκ τούτου $S'_n = \mathbb{A}_n$.

Α 136. Να δειχθεί ότι το κέντρο $Z(\mathbb{A}_n)$ τής $\mathbb{A}_n$ είναι η τετριμμένη υποομάδα $\{\mathrm{Id}_{S_n}\}$, όταν $n \geq 5$.

Λύση. Εδώ θα χρησιμοποιήσουμε ότι η $\mathbb{A}_n$, $n \geq 5$ είναι απλή. Επειδή το κέντρο οποιασδήποτε ομάδας είναι πάντοτε μια ορθόθετη υποομάδα, συμπεραίνουμε ότι $Z(\mathbb{A}_n) = \{\mathrm{Id}_{S_n}\}$.

Α 137. Να δειχθεί ότι όλοι οι κυρίαρχοι παράγοντες μιας μη τετριμμένης p–ομάδας είναι κυκλικές ομάδες τάξης p.

Λύση. Στην Πρόταση 6.3.4 έχουμε ήδη αποδείξει ότι κάθε p–ομάδα είναι επιλύσιμη και ότι κάθε κυρίαρχος παράγοντάς της είναι κυκλική ομάδα τάξης p. Εδώ θα παρουσιάσουμε μια διαφορετική απόδειξη με επαγωγή ως προς n, όπου p^n είναι η τάξη τής p–ομάδας και p είναι ένας σταθερός πρώτος αριθμός.
Για $n = 1$, η G είναι μια ομάδα τάξης p και η σειρά

$$\{e_G\} \leq G$$

είναι μια κυρίαρχη σειρά, αφού η G είναι κυκλική πρώτης τάξης p. Επιπλέον, $G/\{e_G\} \cong \mathbb{Z}_p$ και στη συγκεκριμένη περίπτωση ο ισχυρισμός τής άσκησης είναι αληθής.

Έστω ότι ο ισχυρισμός είναι αληθής για κάθε ομάδα τάξης p^j, όπου $j \leq k$. Θα αποδείξουμε ότι ο ισχυρισμός είναι αληθής και για $k+1$, δηλαδή για μια ομάδα G τάξης p^{k+1}.
Από το Θεώρημα 2.4.13, γνωρίζουμε ότι κάθε μη τετριμμένη p–ομάδα έχει μη τετριμμένο κέντρο. Συνεπώς, υπάρχει κάποιο $x \neq e_G$ με $x \in Z(G)$.
Αν $\langle x \rangle = G$, τότε η G είναι κυκλική τάξης p^{k+1} και η σειρά

$$\langle x \rangle > \langle x^p \rangle > \cdots > \langle x^{p^i} \rangle > \langle x^{p^{i+1}} \rangle > \cdots > \langle x^{p^k} \rangle > \langle x^{p^{k+1}} \rangle = \{e_G\}, \qquad (*)$$

είναι κυρίαρχη με κυρίαρχους παράγοντες $\forall i, 0 \leq i \leq k$, $\langle x^{p^i} \rangle / \langle x^{p^{i+1}} \rangle$ κυκλικές ομάδες τάξης p.
Αν $\langle x \rangle \lneqq G$ και επειδή η $\langle x \rangle$ είναι ορθόθετη υποομάδα τής G, μπορούμε να σχηματίσουμε την πηλικοομάδα $G/\langle x \rangle$, τής οποίας η τάξη είναι p^r με $k+1 \gneqq r \gneqq 1$, διότι $[G/\langle x \rangle : 1] =$

$\frac{[G:1]}{[\langle x\rangle:1]} = \frac{p^{k+1}}{[\langle x\rangle:1]}$ και $p^{k+1} \gneqq [\langle x\rangle : 1] \gneqq 1$.
Λόγω τής επαγωγικής υπόθεσης, η $G/\langle x\rangle$ διαθέτει μια κυρίαρχη σειρά

$$G/\langle x\rangle = H_0 > H_1 > \dots H_i > H_{i+1} \dots > H_t = \langle x\rangle/\langle x\rangle, \qquad (**)$$

όπου $\forall i, 0 \leq i \leq t-1$ οι κυρίαρχοι παράγοντες H_i/H_{i+1} είναι κυκλικές ομάδες τάξης p.
Θεωρούμε τον φυσικό επιμορφισμό $\pi : G \to G/\langle x\rangle, g \mapsto g\langle x\rangle$ και για κάθε ορθόθετη υποομάδα H_i τής κυρίαρχης σειράς (**) σχηματίζουμε την προεικόνα της $G_i := \pi^{-1}(H_i) \leq G$.
Παρατηρούμε ότι $\forall i, 0 \leq i \leq t$ είναι $\langle x\rangle < G_i$, ότι οι G_i είναι ορθόθετες υποομάδες τής G, ότι $\forall i, 0 \leq i \leq t-1$ η G_i περιέχει γνησίως την G_{i+1} και ότι $\forall i, 0 \leq i \leq t$ είναι $H_i = G_i/\langle x\rangle$.
Τέλος από τα θεωρήματα ισομορφίας έχουμε $\forall i, 0 \leq i \leq t-1, G_i/G_{i+1} \cong H_i/H_{i+1}$.
Συνεπώς, όλες οι πηλικοομάδες G_i/G_{i+1} είναι κυκλικές ομάδες τάξης p. Θεωρούμε την ακολουθία υποομάδων:

$$G = G_0 > G_1 > \dots > G_i > G_{i+1} \dots > G_t = \langle x\rangle. \qquad (***)$$

Παρατηρούμε ότι η (***) δεν επιδέχεται μη τετριμμένη εκλέπτυνση, αφού τα πηλίκα G_i/G_{i+1} είναι κυκλικές ομάδες πρώτης τάξης p. Τώρα συμπληρώνουμε την (***) με την κυρίαρχη σειρά που προκύπτει από την κυκλική υποομάδα $\langle x\rangle$. Αν η τάξη τού x είναι $p^s, 1 < s < k+1$, τότε πρόκειται για την ανάλογη τής κυρίαρχης σειράς που είδαμε στην (*):

$$\langle x\rangle > \langle x^p\rangle > \dots > \langle x^{p^i}\rangle > \langle x^{p^{i+1}}\rangle > \dots > \langle x^{p^{s-1}}\rangle > \langle x^{p^s}\rangle = \{e_G\}.$$

Σχηματίζουμε τη σειρά

$$G = G_0 > \dots > G_i > \dots > G_t = \langle x\rangle > \dots > \langle x^{p^i}\rangle > \dots > \langle x^{p^{s-1}}\rangle > \langle x^{p^s}\rangle = \{e_G\}.$$

και παρατηρούμε ότι είναι κυρίαρχη, όπου όλοι οι κυρίαρχοι παράγοντές της είναι κυκλικές ομάδες τάξης p.

Α 138. Θεωρούμε την ομάδα $(G, \cdot)$ των πραγματικών 4×4 πινάκων τής μορφής

$$\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

με πράξη «·» τον συνηθισμένο πολλαπλασιασμό πινάκων. Έστω H υποσύνολο τής G που απαρτίζεται από τους πίνακες τής μορφής

$$\begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Να δειχθούν τα εξής:

(α′) Το H είναι μια ορθόθετη αβελιανή υποομάδα τής G.

(β′) Η παράγωγη υποομάδα G' περιέχεται στην H.

(γ′) Η G είναι μια επιλύσιμη ομάδα.

Λύση. (α′) Θεωρούμε την προσθετική ομάδα $(\mathbb{R}^4, +)$ και την απεικόνιση

$$\varphi : G \to \mathbb{R}^4, A = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix} \mapsto \varphi(A) := (a, b, d, e)$$

Η φ είναι ένας ομομορφισμός ομάδων, διότι όταν

$$A = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & d \\ 0 & 0 & 1 & e \\ 0 & 0 & 0 & 1 \end{pmatrix} \text{ και } B = \begin{pmatrix} 1 & s & t & x \\ 0 & 1 & 0 & y \\ 0 & 0 & 1 & w \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

τότε

$$AB = \begin{pmatrix} 1 & a+s & b+t & c+bw+x+ay \\ 0 & 1 & 0 & d+y \\ 0 & 0 & 1 & e+w \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Επομένως,

$$\varphi(AB) = (a+s, b+t, d+y, e+w) = (a, b, d, e) + (s, t, y, w) = \varphi(A) + \varphi(B).$$

Επιπλέον, ο φ είναι προφανώς επιμορφισμός με πυρήνα $\ker \varphi$ την υποομάδα H που δίνεται στην εκφώνηση τής άσκησης. Επομένως, $H \trianglelefteq G$.

(β′) Αφού $G/H \cong \mathbb{R}^4$, έχουμε ότι η G/H είναι αβελιανή ομάδα. Γι' αυτό με τη βοήθεια τής Πρότασης 6.2.3 συμπεραίνουμε ότι η παράγωγη υποομάδα G' τής G περιέχεται στην H.

(γ′) Ισχυριζόμαστε ότι $H \subseteq G'$, διότι κάθε στοιχείο $\begin{pmatrix} 1 & 0 & 0 & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ τής H ισούται με τον μεταθέτη

$$\left[\begin{pmatrix}1&1&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix},\begin{pmatrix}1&0&0&0\\0&1&0&c\\0&0&1&0\\0&0&0&1\end{pmatrix}\right]=$$

$$\begin{pmatrix}1&1&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&c\\0&0&1&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1&1&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}^{-1}\begin{pmatrix}1&0&0&0\\0&1&0&c\\0&0&1&0\\0&0&0&1\end{pmatrix}^{-1}=$$

$$\begin{pmatrix}1&1&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&c\\0&0&1&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1&-1&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&0\\0&1&0&-c\\0&0&1&0\\0&0&0&1\end{pmatrix}=$$

$$\begin{pmatrix}1&0&0&c\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

Ώστε $H=G'$. Τώρα θεωρούμε τη σειρά

$$G\geq G'=H\geq\{e_G\}.$$

Η πηλικοομάδα $G/G'\cong\mathbb{R}^4$ είναι αβελιανή. Η πηλικοομάδα $G'/\{e_G\}\cong G'=H$ είναι επίσης αβελιανή, αφού

$$\begin{pmatrix}1&0&0&c\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}\begin{pmatrix}1&0&0&d\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}=\begin{pmatrix}1&0&0&c+d\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

Ώστε η G είναι επιλύσιμη ομάδα.

Α 139. Να βρεθεί η παράγωγη σειρά τής διεδρικής ομάδας $(D_n,\circ)$, $n\geq 3$ και να συμπεράνετε ότι για κάθε $n\geq 3$, η D_n είναι επιλύσιμη.

Λύση. Υπενθυμίζουμε ότι

$$D_n=\{\mathrm{Id}_n,\tau,\rho,\rho^2,\ldots,\rho^{n-1},\tau\circ\rho,\tau\circ\rho^2,\ldots,\tau\circ\rho^{n-1}\},$$

όπου $\circ(\rho)=n$, $\circ(\tau)=2$ και $\forall i\in\mathbb{Z}$, $\rho^i\circ\tau=\tau\circ\rho^{-i}$.

Υπολογίζουμε τους μεταθέτες:

$[\rho^i, \rho^j] = \rho^i \circ \rho^j \circ \rho^{-i} \circ \rho^{-j} = \mathrm{Id}_n,$
$[\tau \circ \rho^i, \rho^j] = \tau \circ \rho^i \circ \rho^j \circ \rho^{-i} \circ \tau^{-1} \circ \rho^{-j} = \tau \circ \rho^j \circ \tau \circ \rho^{-j} = \rho^{-j} \circ \tau \circ \tau \circ \rho^{-j} = \rho^{-2j}$
$[\rho^i, \tau \circ \rho^j] = \rho^i \circ \tau \circ \rho^j \circ \rho^{-i} \circ \rho^{-j} \circ \tau^{-1} = \rho^i \circ \tau \circ \rho^{-i} \circ \tau = \tau \circ \rho^{-2i} \circ \tau = \rho^{2i},$
$[\tau \circ \rho^i, \tau \circ \rho^j] = \tau \circ \rho^i \circ \tau \circ \rho^j \circ \rho^{-i} \circ \tau^{-1} \circ \rho^{-j} \circ \tau^{-1} = \rho^{-i} \circ \rho^j \circ \rho^{-i} \circ \rho^j =$
$\rho^{-2i} \circ \rho^{2j} = \rho^{2(j-i)}.$

Επιλέγοντας $j = i+1$, διαπιστώνουμε ότι $D_n^{(1)} = \langle \rho^2 \rangle$. Επειδή η $\langle \rho^2 \rangle$ είναι αβελιανή ομάδα, συμπεραίνουμε ότι $\{\mathrm{Id}_n\} = \langle \rho^2 \rangle^{(1)} = D_n^{(2)}$. Ως εκ τούτου, η παράγωγη σειρά τής D_n είναι η

$$D_n = D_n^{(0)} > D_n^{(1)} = \langle \rho^2 \rangle > D_n^{(2)} = \{\mathrm{Id}_n\}.$$

Από το Θεώρημα 6.2.10, συμπεραίνουμε ότι η D_n είναι επιλύσιμη.

Α 140. Έστω ότι $(G, \star)$ είναι μια ομάδα και $A, B \neq \emptyset$, δύο μη κενά υποσύνολα τής G. Συμβολίζουμε με $[A, B]$ την υποομάδα τής G που παράγεται από το σύνολο των μεταθετών $\{[a, b] \mid a \in A, b \in B\}$.
Να δειχθεί ότι όταν η G παράγεται από ένα σύνολο K, τότε η μικρότερη ορθόθετη υποομάδα τής G που περιέχει την $[K, K]$ είναι η παράγωγη υποομάδα G'.

Λύση. Είναι προφανές ότι η $[K, K]$ περιέχεται στην $[G, G] = G'$, η οποία ως γνωστόν είναι μια ορθόθετη υποομάδα τής G.
Τώρα θα δείξουμε ότι αν $N \trianglelefteq G$ είναι μια ορθόθετη υποομάδα τής G με $[K, K] \leq N$, τότε η G' περιέχεται επίσης στην N και προς τούτο αρκεί να δείξουμε ότι $\forall x, y \in G$, ο γεννήτορας $[x, y]$ τής G' ανήκει στην N.

Αφού $\langle K \rangle = G$, κάθε $x \in G$ ισούται με ένα γινόμενο τής μορφής $x = a_1 a_2 \ldots a_n$, όπου $\forall i, 1 \leq i \leq n$, είτε το a_i είτε το a_i^{-1} είναι στοιχείο τού K. Αυτό το εκφράζουμε εν συντομία γράφοντας $\forall i, 1 \leq i \leq n, a_i \in K \cup K^{-1}$, όπου βέβαια $K^{-1} = \{k^{-1} \mid k \in K\}$.

Έστω ότι $x = a_1 a_2 \ldots a_n$ και $y = b_1 b_2 \ldots b_m$ είναι στοιχεία τής G, όπου $\forall i, 1 \leq i \leq n, a_i \in K \cup K^{-1}$ και $\forall j, 1 \leq i \leq m, b_j \in K \cup K^{-1}$. Θα δείξουμε με τη βοήθεια τής επαγωγής ως προς $n + m$ ότι $\forall x, y \in G$, ο μεταθέτης $[x, y]$ ανήκει στην N.

Παρατηρούμε γενικώς, ότι ο μεταθέτης $[x, y] = xyx^{-1}y^{-1}$ ανήκει στην N, αν και μόνο αν το $x^{-1}[x, y]x = [y, x^{-1}]$ ανήκει στο N, αφού η N είναι ορθόθετη υποομάδα. Επομένως,

$$[x, y] \in N \Leftrightarrow [y, x^{-1}] \in N \Leftrightarrow [x^{-1}, y^{-1}] \in N \Leftrightarrow [y^{-1}, x] \in N. \qquad (*)$$

Επιπλέον, επειδή η N υποομάδα ο μεταθέτης $[x, y]$ ανήκει στην N, αν και μόνο αν, το $[x, y]^{-1} = [y, x]$ ανήκει στην $N1$

$$[x, y] \in N \Leftrightarrow [y, x] \in N \Leftrightarrow [x, y^{-1}] \in N \Leftrightarrow [y^{-1}, x^{-1}] \in N \Leftrightarrow [x^{-1}, y] \in N. \qquad (**)$$

Αν λοιπόν $n + m = 2$, τότε τα x, y ανήκουν στο $K \cup K^{-1}$ τότε, λόγω των (*) και (**), ο μεταθέτης $yx^{-1}y^{-1} = [x, y]$ ανήκει στην N.

Έστω ότι για κάθε n, m με $n + m \leq \ell$, ο μεταθέτης $[x, y]$ με $x = a_1a_2 \dots a_n$ και $y = b_1b_2 \dots b_m$ ανήκει στην N. Θα δείξουμε ότι κάθε μεταθέτης με $n+m = \ell+1$ ανήκει επίσης στην N.

Αφού $n + m = \ell + 1$, θα είναι ή $x = a_1a_2 \dots a_{n+1}$ και $y = b_1b_2 \dots b_m$ ή $x = a_1a_2 \dots a_n$ και $y = b_1b_2 \dots b_{m+1}$, όπου $a_i, b_j \in K \cup K^{-1}$.
Στην πρώτη περίπτωση, εφαρμόζοντας τον τύπο (α′), βλ. Άσκηση ΠΑ147, έχουμε

$$[x, y] = [a_1(a_2 \dots a_{n+1}), y] = a_1[a_2 \dots a_{n+1}, y]a_1^{-1}[a_1, y].$$

Λόγω τής επαγωγικής υπόθεσης, οι μεταθέτες $[a_2 \dots a_{n+1}, y]$ και $[a_1, y]$ ανήκουν στην N. Επιπλέον, επειδή η N είναι ορθόθετη το $a_1[a_2 \dots a_{n+1}, y]a_1^{-1}$ ανήκει επίσης στην N. Έτσι τελικώς ο $[x, y] \in N$.
Στη δεύτερη περίπτωση, εφαρμόζοντας τον τύπο (β′), βλ. Άσκηση ΠΑ147, έχουμε

$$[x, y] = [x, b_1(b_2 \dots b_{m+1})] = [x, b_1]b_1[x, b_2 \dots b_{m+1}]b_1^{-1}.$$

και όπως προηγουμένως συμπεραίνουμε ότι ο $[x, y] \in N$.

Α 141. Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι οι H, K και L είναι ορθόθετες υποομάδες τής G. Να δειχθεί ότι

(α′) $[[H, K], L] \subseteq [[K, L], H]\,[[L, H], K]$,

(β′) $[HK, L] = [H, L]]\,[K, L]$,

Λύση. Αρχίζουμε με ορισμένες γενικές παρατηρήσεις:
Αν A, B είναι υποομάδες μιας ομάδας $(G, \star)$, τότε η υποομάδα $[A, B]$ ισούται με την υποομάδα $[B, A]$. Πράγματι, το αντίστροφο κάθε γεννήτορα $[a, b]$ τής $[A, B]$ ισούται με $[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a]$ και συνεπώς είναι ένας γεννήτορας τής $[B, A]$. Επομένως, $[A, B] \supseteq [B, A]$. Όμοια, $[B, A] \supseteq [A, B]$.
Αν A, B είναι ορθόθετες υποομάδες μιας ομάδας $(G, \star)$, τότε και η $[A, B]$ είναι επίσης ορθόθετη υποομάδα τής G. Για την απόδειξη τού ισχυρισμού είναι αρκετό να αποδείξουμε ότι $\forall g \in G, a \in A, b \in B$, το $g[a, b]g^{-1}$ ανήκει στην $[A, B]$. Το τελευταίο είναι αληθές, αφού ένας απλός υπολογισμός δίνει
$g[a, b]g^{-1} = [gag^{-1}, gbg^{-1}] \in [A, B]$, αφού $A \trianglelefteq G$ και $B \trianglelefteq G$.
(α′) Σύμφωνα με τα παραπάνω η υποομάδα $[[K, L], H]\,[[L, H], K]$ είναι μια ορθόθετη υποομάδα τής G ως γινόμενο των ορθόθετων υποομάδων $[[K, L], H]$ και $[[L, H], K]$.

Ο τύπος (γ′) τής Άσκησης ΠΑ147 μπορεί να γραφεί και ως

$$\begin{aligned}
&\forall x, y, z \in G : \\
&x^{-1}\left[[x, y^{-1}], z^{-1}\right]x = \left(y^{-1}\left[[y, z^{-1}], x^{-1}\right]^{-1} y\right)\left(z^{-1}\left[[z, x^{-1}], y^{-1}\right]^{-1} z\right)
\end{aligned}$$

και εκτελώντας τις αντικαταστάσεις

$$y \mapsto y^{-1}, y^{-1} \mapsto y, z \mapsto z^{-1}, z^{-1} \mapsto z,$$

παίρνουμε

$$\begin{aligned}&\forall x, y, z \in G :\\ &x^{-1}\,[[x,y],z]\,x = \left(y\left[[y^{-1},z],x^{-1}\right]^{-1}y^{-1}\right)\left(z\left[[z^{-1},x^{-1}],y\right]^{-1}z^{-1}\right)\end{aligned}$$

από όπου έπεται

$$\begin{aligned}&\forall x, y, z \in G :\\ &[[x,y],z] = \left((x^{-1}y)\left[[y^{-1},z],x^{-1}\right]^{-1}(x^{-1}y)^{-1}\right)\left((x^{-1}z)\left[[z^{-1},x^{-1}],y\right]^{-1}(x^{-1}z)^{-1}\right).\end{aligned}$$

Χρησιμοποιώντας τον αμέσως παραπάνω τύπο, παρατηρούμε ότι $\forall x \in H$, $\forall y \in K$ και $\forall z \in L$, κάθε γεννήτορας $[[x,y],z]$ τής $[[H,K],L]$ ανήκει στην $[[K,L],H]\,[[L,H],K]$, αφού το $(x^{-1}y)\left[[y^{-1},z],x^{-1}\right]^{-1}(x^{-1}y)^{-1}$ ανήκει στην $[[K,L],H]$, επειδή το $\left[[y^{-1},z],x^{-1}\right]^{-1} \in [[K,L],H]$ και η $[[K,L],H]$ είναι ορθόθετη υποομάδα τής G και αντίστοιχα το $(x^{-1}z)\left[[z^{-1},x^{-1}],y\right]^{-1}(x^{-1}z)^{-1}$ ανήκει στην $[[L,H],K]$, επειδή το $\left[[z^{-1},x^{-1}],y\right]^{-1} \in [[L,H],K]$ και η $[[L,H],K]$ είναι ορθόθετη υποομάδα τής G.

Επομένως, $[[H,K],L] \subseteq [[K,L],H]\,[[L,H],K]$.

(β′) Παρατηρούμε ότι $[HK,L] \supseteq [H,L]]\,[K,L]$, αφού $[HK,L] \supseteq [H,L]]$ και $[HK,L] \supseteq [K,L]$. Υπολείπεται η απόδειξη τής σχέσης $[HK,L] \subseteq [H,L]\,[K,L]$.

Έστω $[xy,z], x \in H, y \in K, z \in L$ ένας γεννήτορας τής $[HK,L]$. Θα δείξουμε ότι το στοιχείο $[xy,z]^{-1} = [z,xy]$ ανήκει στην $[H,L][K,L]$ από όπου έπεται ότι και ο $[xy,z] \in [H,L][K,L]$ και συνεπώς $[HK,L] \subseteq [H,L]\,[K,L]$.

Εφαρμόζοντας στο $[z,xy]$ τον τύπο (γ′) τής Άσκησης ΠΑ147, παίρνουμε:

$$[z,xy] = [z,x](x[z,y]x^{-1}).$$

Το στοιχείο $[z,x]$ ανήκει στην υποομάδα $[L,H] = [H,L]$ και το στοιχείο $x[z,y]x^{-1}$ ανήκει στην $[L,K] = [K,L]$, διότι το $[z,y] \in [L,K]$ και η $[L,K]$ είναι ορθόθετη υποομάδα τής G. Επομένως, $[z,xy] \in [H,L][K,L]$.

Α 142. Έστω ότι $(G,\star)$ είναι μια ομάδα και ότι οι H,K είναι υποομάδες τής G. Να δειχθεί ότι η $[H,K]$ είναι ορθόθετη υποομάδα τής $\langle H,K\rangle$.
(*Συμβολίζουμε με* $\langle H,K\rangle$ *την υποομάδα τής* G *που παράγεται από το σύνολο* $H \cup K$.)

Λύση. Παρατηρούμε ότι προφανώς η $[H,K]$ είναι υποομάδα τής $\langle H,K\rangle$.
Για να δείξουμε ότι $[H,K] \trianglelefteq \langle H,K\rangle$, αρκεί να δείξουμε ότι για κάθε γεννήτορα $[h,k]$ τής $[H,K]$ και κάθε γεννήτορα α τής $\langle H,K\rangle$, το $\alpha^{-1}[h,k]\alpha$ είναι στοιχείο τής $[H,K]$.
Διακρίνουμε δύο περιπτώσεις $\alpha = \chi \in H$ και $\alpha = \kappa \in K$.
Θα δείξουμε ότι $\forall \chi \in H$, το $\chi^{-1}[h,k]\chi$ είναι στοιχείο τής $[H,K]$ και προτρέπουμε τον αναγνώστη να ασχοληθεί με την άλλη περίπτωση που είναι παρεμφερής.

Έχουμε:

$$\chi^{-1}[h,k]\chi = \chi^{-1}hkh^{-1}k^{-1}\chi = [\chi^{-1}h,k][\chi^{-1},k]^{-1} \in [H,K].$$

Α 143. Έστω ένας ομομορφισμός ομάδων $\varphi : G \to H$. Να δειχθεί ότι

(α′) $\varphi(G)' = \varphi(G')$.

(β′) Αν η H είναι επιλύσιμη ομάδα και ο φ είναι μονομορφισμός, τότε και η G είναι επιλύσιμη.

(γ′) Αν η G είναι επιλύσιμη ομάδα και ο φ είναι επιμορφισμός, τότε και η H είναι επιλύσιμη.

Λύση. (α′) Αν $[x, y]$ είναι ένας γεννήτορας τής παράγωγης ομάδας G' τής G, τότε το $\varphi([x, y]) = [\varphi(x), \varphi(y)]$ ανήκει στη $\varphi(G)'$. Επομένως, $\varphi(G') \subseteq \varphi(G)'$. Αλλά και αντίστροφα κάθε γεννήτορας τής $\varphi(G)'$ είναι τής μορφής $[\varphi(x), \varphi(y)] = \varphi([x, y])$, όπου $x, y \in G$. Συνεπώς, $\varphi(G)' \subseteq \varphi(G')$. Ώστε, $\varphi(G)' = \varphi(G')$.
(β′) Από τη θεωρία γνωρίζουμε ότι κάθε υποομάδα τής επιλύσιμης ομάδας H είναι επιλύσιμη. Επομένως, η $\varphi(G)$ είναι επιλύσιμη και επειδή ο φ είναι ένας μονομορφισμός, συμπεραίνουμε ότι και η $G \cong \varphi(G)$ είναι επιλύσιμη.
(γ′) Επειδή ο φ είναι ένας επιμορφισμός, είναι $H \cong G/\mathrm{Ker}(\varphi)$. Αλλά κάθε πηλικοομάδα τής επιλύσιμης ομάδας G είναι επιλύσιμη. Επομένως η H είναι επιλύσιμη ομάδα.

Προτεινόμενες Ασκήσεις

ΠΑ 137. Να δειχθεί ότι κάθε ομάδα τάξης $2 \cdot 3^2 \cdot 5 = 90$ και κάθε ομάδα τάξης $2 \cdot 3 \cdot 5^2 = 150$ είναι επιλύσιμη. (Ενώ όπως γνωρίζουμε, η εναλλάσσουσα ομάδα $\mathbb{A}_5$, τάξης $2^2 \cdot 3 \cdot 5 = 60$ είναι απλή!)

ΠΑ 138. Να δειχθεί ότι κάθε ομάδα τάξης 1000 είναι επιλύσιμη.

ΠΑ 139. Να βρεθούν όλες οι δυνατές συνθετικές σειρές τής κυκλικής ομάδας $\langle a \rangle$ τάξης 24 και να προσδιοριστούν οι συνθετικοί παράγοντες.

ΠΑ 140. Να βρεθεί μια συνθετική σειρά τής ομάδας $(\mathbb{Z}_{p^k}, +)$, όπου ο p είναι πρώτος και ο k φυσικός. Να προσδιοριστούν κατόπιν οι συνθετικοί παράγοντες τής σειράς.

ΠΑ 141. Έστω $(G, \star)$ μια ομάδα. Να δειχθούν τα εξής:

(α′) Όταν το κέντρο τής G είναι τετριμμένο, δηλαδή $\mathcal{Z}(G) = \{e_G\}$, τότε όλοι οι όροι $\mathcal{Z}_i(G), i \in \mathbb{N} \cup \{0\}$ είναι τετριμμένοι.

(β′) Όταν η ομάδα G είναι αβελιανή, τότε όλοι οι όροι $\mathcal{Z}_i(G), i \in \mathbb{N} \cup \{0\}$ είναι ίσοι με την ομάδα G.

ΠΑ 142. Ποιό είναι το κέντρο και ποιά η μεταθέτρια υποομάδα μιας απλής ομάδας;

ΠΑ 143. Να δειχθεί ότι η ομάδα $(\mathrm{Iso}(\mathbb{R}), \circ)$ των ισομετριών τού $\mathbb{R}$, βλ. Παράδειγμα 1.2.6, είναι επιλύσιμη ομάδα.

ΠΑ 144. Να δειχθεί ότι για κάθε $n \geq 3$, η διεδρική ομάδα $(D_n, \circ)$ είναι επιλύσιμη και να προσδιοριστεί το σύνολο των κλάσεων ισομορφίας των συνθετικών και των κυρίαρχων παραγόντων της.

ΠΑ 145. Να δειχθεί με δύο διαφορετικούς τρόπους ότι η τετρανιακή ομάδα $(\mathcal{Q}_8, \circ)$ είναι επιλύσιμη.

ΠΑ 146. Έστω $(G, \cdot)$ η ομάδα των αντιστρέψιμων 2×2 άνω τριγωνικών πινάκων με συνιστώσες από ένα σώμα $\mathbb{K}$. Να δειχθεί ότι η G είναι επιλύσιμη ομάδα.

ΠΑ 147. Να αποδειχθούν οι επόμενοι τύποι που αναφέρονται στους μεταθέτες μιας ομάδας $(G, \star)$:

(α′) $\forall x, y, z \in G : [xy, z] = x[y, z]x^{-1}[x, z]$,

(β′) $\forall x, y, z \in G : [x, yz] = [x, y]y[x, z]y^{-1}$,

(γ′) $\forall x, y, z \in G : x^{-1}[[x, y^{-1}], z^{-1}]xz^{-1}[[z, x^{-1}], y^{-1}]zy^{-1}[[y, z^{-1}], x^{-1}]y = e_G$.

ΠΑ 148. Έστω $(G, \star)$ μια μηδενοδύναμη ομάδα και H μια μεγιστοτική υποομάδα της. Να δειχθεί ότι η μεταθέτρια υποομάδα G' τής G περιέχεται στην H.

ΠΑ 149. Να δειχθεί ότι κάθε μη αβελιανή ομάδα $(G, \star)$ τάξης p^3, όπου p πρώτος, είναι μηδενοδύναμη κλάσης 3.

ΠΑ 150. Να δειχθεί ότι κάθε ομάδα τάξης 135 είναι μηδενοδύναμη.

Κεφάλαιο 7

Επεκτάσεις Ομάδων

7.1 Προκαταρκτικές Έννοιες

Σύμφωνα με το Θεώρημα 5.2.8 των Jordan–Hölder, αν μια ομάδα $(G, \star)$ διαθέτει συνθετικές σειρές, τότε αυτές είναι ισόμορφες, δηλαδή το πλήθος και οι τύποι ισομορφίας των συνθετικών παραγόντων είναι μοναδικά καθορισμένοι. Ιδιαιτέρως, μια πεπερασμένη ομάδα G διαθέτει πάντοτε συνθετικές σειρές, οι οποίες προκύπτουν προσδιορίζοντας πρώτα μια μεγιστοτική ορθόθετη υποομάδα G_1 τής $G = G_0$, ακολούθως μια μεγιστοτική 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

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

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 ισομορφίας) συνθετικούς παράγοντες. Οι προηγούμενες παρατηρήσεις οδηγούν στο λεγόμενο

Πρόγραμμα Hölder

(α′) Να προσδιοριστούν (με ακρίβεια ισομορφίας) 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 συγκεκριμένων 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.

7.2 Το Πρόβλημα τής Επέκτασης και το ημιευθύ Γινόμενο

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

Ορισμός 7.2.1. Έστω ότι $(N, \star_N)$ και $(H, \star_H)$ είναι δύο ομάδες. Μια ομάδα $(G, \star)$ ονομάζεται *επέκταση* τής N με την H, αν υπάρχει μια ορθόθετη υποομάδα N_1 τής G, όπου η πηλικοομάδα G/N_1 είναι ισόμορφη προς την ομάδα H.

Παράδειγμα 7.2.2. (α′) Οι $(S_3, \circ)$ 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 $(S_3, \circ)$ δεν είναι.

(β′) Αν $(N, \star_N)$ και $(H, \star_H)$ είναι δύο ομάδες, τότε το ευθύ γινόμενό τους $G = N \times H$ είναι επέκταση τής N με την H (καθώς και επέκταση τής H με την N).

7.2.1 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 7.2.3. Έστω $(G, \star)$ μια ομάδα και N, H δύο υποομάδες της. Η ομάδα G ονομάζεται το *εσωτερικό ημιευθύ γινόμενο* τής N με την H, αν

(α′) $N \trianglelefteq G$, δηλαδή η N είναι ορθόθετη υποομάδα τής G,

(β′) $G = NH$ και

(γ′) $N \bigcap H = \{e_G\}$.

Προσέξτε ότι αν επιπλέον είναι $H \trianglelefteq G$, 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 $G = N \rtimes H$.

Παρατήρηση 7.2.4. (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 $n_1h_1 = n_2h_2$, όπου $n_1, n_2 \in N, h_1, h_2 \in H$, τότε $n_2^{-1}n_1 = h_2h_1^{-1} \in N \bigcap H = \{e_G\}$. Συνεπώς, $n_2^{-1}n_1 = e_G = h_2h_1^{-1}$ 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 $g_1 = n_1h_1, g_2 = n_2h_2, n_1, n_2 \in N, h_1, h_2 \in H$, έχουμε

$$g_1g_2 = n_1h_1n_2h_2 = n_1(h_1n_2h_1^{-1})h_1h_2 = n_1n'h_1h_2, \text{ όπου } h_1n_2h_1^{-1} = n' \in N.$$

Ώστε, το «H–τμήμα» τού γινομένου g_1g_2 ισούται με το γινόμενο h_1h_2 των «H–τμημάτων» των g_1 και g_2 αντιστοίχως. Επομένως, η καλά ορισμένη απεικόνιση

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

είναι ένας ομομορφισμός ομάδων, αφού

$$\varphi(g_1g_2) = \varphi(n_1h_1n_2h_2) = \varphi(n_1n'h_1h_2) = h_1h_2 = \varphi(g_1)\varphi_(g_2).$$

Επιπλέον, είναι ολοφάνερο ότι ο φ είναι ένας επιμορφισμός με $\ker\varphi = N$ 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 τη γενική περίπτωση, που θα εκθέσουμε στην Πρόταση 7.2.5.

(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

$$\theta_h(n_1n_2) = h(n_1n_2)h^{-1} = (hn_1h^{-1})(hn_2h^{-1}) = \theta_h(n_1)\theta_h(n_2).$$

Συνεπώς, η απεικόνιση

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

είναι ένας ομομορφισμός ομάδων, αφού

$$\forall h_1, h_2 \in H, n \in N : \theta(h_1h_2)(n) = \theta_{h_1h_2}(n) = (h_1h_2)n(h_1h_2)^{-1} = h_1(h_2nh_2^{-1})h_1^{-1} =$$
$$h_1(\theta_{h_2}(n))h_1^{-1} = \theta_{h_1}(\theta_{h_2}(n)) = \theta_{h_1} \circ \theta_{h_2}(n) = \theta(h_1) \circ \theta(h_2)(n).$$

Επομένως,

$$\forall h_1, h_2 \in H : \theta(h_1h_2) = \theta(h_1) \circ \theta(h_2).$$

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 7.2.5. *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 προς την N και η υποομάδα $\overline{H}$ είναι ισόμορφη προς 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

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

Αλλά

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

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:

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

και

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

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:

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

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 $\overline{N} \bigcap \overline{H} = \{(e_N, e_H)\}$. Ώστε, $G = \overline{N} \rtimes \overline{H}$. □

Ορισμός 7.2.6. 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 7.2.5 ονομάζεται το *εξωτερικό ημιευθύ γινόμενο* των ομάδων N και H και παριστάνεται ως $N \rtimes_\theta H$.

Παρατήρηση 7.2.7. (α′) Λαμβάνοντας υπ' όψιν την Παρατήρηση 7.2.4 (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»:

Παράδειγμα 7.2.8. (α′) Θεωρούμε την ομάδα τετρανίων:

$$\mathcal{Q}_8 = \{\pm E, \pm I, \pm J, \pm K\}, \text{ με } (-E)^2 = E, I^2 = J^2 = K^2 = IJK = -E,$$

όπου το E είναι το ταυτοτικό στοιχείο τής $\mathcal{Q}_8$ και όπου το $-E$ μετατίθεται με οποιοδήποτε άλλο στοιχείο.
Ισχυριζόμαστε ότι
*η $\mathcal{Q}_8$ **δεν είναι** το (εσωτερικό) ημιευθύ γινόμενο δύο μη τετριμμένων υποομάδων της. Θα αποδείξουμε μάλιστα ότι δεν υπάρχουν μη τετριμμένες υποομάδες N, H τής $\mathcal{Q}_8$, τέτοιες ώστε $\mathcal{Q}_8 = NH$ και $N \bigcap H = \{1\}$.*

Πράγματι, παρατηρούμε ότι αν $Q_8 = NH$ και $N \bigcap H = \{1\}$, όπου $N \neq \{1\}, \mathcal{Q}_8$ και $H \neq \{1\}, \mathcal{Q}_8$, τότε η τάξη τής μίας από τις δύο υποομάδες ισούται με 4 και η άλλη ισούται με 2, αφού

$$8 = [\mathcal{Q}_8 : 1] = |NH| = \frac{[N:1][H:1]}{[N \bigcap H : 1]} = [N:1][H:1].$$

Αλλά η $\mathcal{Q}_8$ διαθέτει μόνο μία υποομάδα τάξης 2, την $\langle -E \rangle$, αφού υπάρχει ακριβώς ένα στοιχείο τάξης 2. Λόγω αυτής τής παρατήρησης, συμπεραίνουμε τώρα ότι κάθε υποομάδα τής $\mathcal{Q}_8$ τάξης 4 οφείλει να είναι κυκλική, αφού αν δεν ήταν κυκλική, τότε θα είχε δύο διαφορετικές υποομάδες τάξης 2, (επειδή θα ήταν ισόμορφη προς 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 $\mathcal{Q}_8$ τάξης 4, περιέχει την $\langle -E \rangle$ και γι' αυτό η τομή μιας υποομάδας τάξης 4 με τη μοναδική υποομάδα τάξης 2, δηλαδή την $\langle -E \rangle$, ισούται με $\langle -E \rangle$. Ώστε, πάντοτε η τομή μιας υποομάδας τάξης 2 με μια υποομάδα τάξης 4 είναι διαφορετική από την $\{E\}$.

Εν τούτοις, η $\mathcal{Q}_8$ είναι επέκταση τής $\mathbb{Z}_4$ με την $\mathbb{Z}_2$, επειδή η $\mathcal{Q}_8$ διαθέτει ορθόθετες κυκλικές υποομάδες τάξης 4, παραδείγματος χάριν την $N = \langle I \rangle \cong \mathbb{Z}_4$ και όπου $\mathcal{Q}_8/N \cong \mathbb{Z}_2$.

(**Σημείωση**: Στην Άσκηση Α58 προσδιορίσαμε όλες τις υποομάδες τής $\mathcal{Q}_8$. Παρατηρούμε ότι η τομή δύο οποιωνδήποτε υποομάδων $\neq \{E\}$ τής $\mathcal{Q}_8$ περιέχει πάντοτε την $\langle -E \rangle$. Επομένως, η συνθήκη $N \bigcap H$ δεν μπορεί να ικανοποιηθεί όταν οι N και H είναι $\neq \{E\}$.)

(β′) Η διεδρική ομάδα $D_n = \{\mathrm{Id}_n, \tau, \rho, \rho^2, \ldots, \rho^{n-1}, \tau \circ \rho, \tau \circ \rho^2, \ldots, \tau \circ \rho^{n-1}\}$, $n \geq 3$, βλ. σελ. 18, ισούται με το εσωτερικό ημιευθύ γινόμενο τής ορθόθετης υποομάδας $\langle \rho \rangle$ με την υποομάδα $\langle \tau \rangle$, δηλαδή $D_n = \langle \rho \rangle \rtimes \langle \tau \rangle$.

Πράγματι, ήδη γνωρίζουμε ότι η $\langle \rho \rangle$ είναι ορθόθετη υποομάδα τής D_n. Η τομή $\langle \rho \rangle \bigcap \langle \tau \rangle$ ισούται με $\{\mathrm{Id}_n\}$. Η υποομάδα $\langle \rho \rangle \langle \tau \rangle$ ισούται με την D_n, αφού το πλήθος των στοιχείων τής $\langle \rho \rangle \langle \sigma \rangle$ είναι

$$[\langle \rho \rangle \langle \tau \rangle : 1] = \frac{[\langle \rho \rangle : 1][\langle \tau \rangle : 1]}{[\langle \rho \rangle \bigcap \langle \tau \rangle : 1]} = 2n.$$

Τέλος, ο ομομορφισμός $\theta : \langle \tau \rangle \to \mathrm{Aut}(\langle \rho \rangle)$, που είδαμε στην Παρατήρηση 7.2.4 (γ′), προσδιορίζεται πολύ εύκολα: Η $\langle \tau \rangle$ είναι κυκλική ομάδα τάξης 2 και γι' αυτό κάθε ομομορφισμός με πεδίο ορισμού την $\langle \tau \rangle$ προσδιορίζεται πλήρως από την τιμή της στον γεννήτορα τ. Επομένως, για να υπολογίσουμε τον ομομορφισμό $\theta : \langle \tau \rangle \to \mathrm{Aut}(\langle \rho \rangle)$ είναι αρκετό να υπολογίσουμε τον αυτομορφισμό $\theta_\tau : \langle \rho \rangle \to \langle \rho \rangle$. Όμως αφού η $\langle \rho \rangle$ είναι κυκλική, ο θ_τ προσδιορίζεται μοναδικά από την τιμή $\theta_\tau(\rho)$. Σύμφωνα με την Παρατήρηση 7.2.4 (γ′), έχουμε $\theta_\tau(\rho) = \tau \rho \tau^{-1} = \tau \rho \tau = \tau \tau \rho^{n-1} = \rho^{n-1} = \rho^{-1}$. (Προσέξτε, ότι το ρ^{-1} είναι πάντοτε γεννήτορας τής κυκλικής ομάδας $\langle \rho \rangle$)!.)

Συνεπώς, η D_n είναι ισόμορφη προς το εξωτερικό ημιευθύ 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 $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(A)$ ορίζεται από τις τιμές $\theta_{[1]_2}(a) = -a, \forall a \in A$.

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

Παράδειγμα 7.2.9. (α′) Η συμμετρική ομάδα $(S_4, \circ)$ είναι το εσωτερικό ημιευθύ γινόμενο τής ορθόθετης υποομάδας

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

με την υποομάδα $H = \{\sigma \in S_4 \mid \sigma(4) = 4\}$, δηλαδή $S_4 = V \rtimes H$.

Ήδη γνωρίζουμε, βλ. Άσκηση ΠΑ94, ότι η V είναι ορθόθετη υποομάδα τής S_4

Επιπλέον,

$$[VH : 1] = \frac{[V : 1][H : 1]}{[V \bigcap H : 1]} = 4 \cdot 6 = 24,$$

αφού $V \bigcap H = \{\mathrm{Id}\}$ και συνεπώς, $S_4 = VH$.
Θα προσπαθήσουμε να προσδιορίσουμε τον ομομορφισμό $\theta : H \to \mathrm{Aut}(V)$, βλ. Παρατήρηση 7.2.4 (γ′).

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

Η απεικόνιση

$$\begin{aligned} \chi : & V \to \mathbb{Z}_2 \times \mathbb{Z}_2, \\ & \mathrm{Id}_4 \mapsto ([0]_2, [0]_2), \\ & u = \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix} \mapsto ([1]_2, [0]_2) \\ & v = \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix} \mapsto ([0]_2, [1]_2), \\ & u \circ v = \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix} \mapsto ([1]_2, [1]_2), \end{aligned}$$

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, επιλέγοντας μια $\mathbb{Z}_2$–βάση τής $\mathbb{Z}_2 \times \mathbb{Z}_2$, οι αυτομορφισμοί τής $\mathbb{Z}_2 \times \mathbb{Z}_2$ μπορούν, 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:

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

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

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 $\begin{pmatrix}1 & 2 & 3\end{pmatrix}$ και $\begin{pmatrix}1 & 2\end{pmatrix} \in H$, αφού $H = \langle \begin{pmatrix}1 & 2 & 3\end{pmatrix}, \begin{pmatrix}1 & 2\end{pmatrix} \rangle = S_3$.

Έχουμε:

$$\begin{aligned} \theta_{(1\,2\,3)}(u) &= \begin{pmatrix}1 & 2 & 3\end{pmatrix} \circ u \circ \begin{pmatrix}1 & 2 & 3\end{pmatrix}^{-1} = \begin{pmatrix}2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 4\end{pmatrix} = u \circ v \\ \theta_{(1\,2\,3)}(v) &= \begin{pmatrix}1 & 2 & 3\end{pmatrix} \circ v \circ \begin{pmatrix}1 & 2 & 3\end{pmatrix}^{-1} = \begin{pmatrix}2 & 1\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix} = u. \end{aligned}$$

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.

$$\begin{aligned} \theta_{(1\,2)}(u) &= \begin{pmatrix}1 & 2\end{pmatrix} \circ u \circ \begin{pmatrix}1 & 2\end{pmatrix}^{-1} = \begin{pmatrix}2 & 1\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix} = u \\ \theta_{(1\,2)}(v) &= \begin{pmatrix}1 & 2\end{pmatrix} \circ v \circ \begin{pmatrix}1 & 2\end{pmatrix}^{-1} = \begin{pmatrix}2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 4\end{pmatrix} = u \circ v. \end{aligned}$$

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 2.

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[1].

Επομένως, $S_4 \cong V \rtimes_\theta H$ και αφού η $H \cong S_3$ συμπεραίνουμε ότι $S_4 \cong V \rtimes_\theta S_3$.

(β′) Η εναλλάσσουσα ομάδα $(\mathbb{A}_4, \circ)$ 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 κυκλική υποομάδα $K = \langle \begin{pmatrix}1 & 2 & 3\end{pmatrix} \rangle$, δηλαδή $\mathbb{A}_4 = V \rtimes K$.
Κατ' αρχάς, η V είναι ορθόθετη υποομάδα τής $\mathbb{A}_4$, αφού $V \trianglelefteq S_4$.
Επιπλέον,

$$[VK : 1] = \frac{[V:1][K:1]}{[V \bigcap K : 1]} = 4 \cdot 3 = 12,$$

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

Προς ποιό εξωτερικό ημιευθύ γινόμενο τής V με την K είναι ισόμορφη η $\mathbb{A}_4$; Θα προσδιορίσουμε και πάλι τον ομομορφισμό $\theta : K \to \mathrm{Aut}(V)$, βλ. Παρατήρηση 7.2.4 (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 μόνο ο υπολογισμός τής τιμής $\theta_{(1\ 2\ 3)}$.

Έχουμε:

$$\theta_{(1\ 2\ 3)}(\mathrm{Id}_4) = \begin{pmatrix}1 & 2 & 3\end{pmatrix} \circ \mathrm{Id}_4 \circ \begin{pmatrix}1 & 2 & 3\end{pmatrix}^{-1} = \mathrm{Id}_4,$$
$$\theta_{(1\ 2\ 3)}\left(\begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix}\right) = \begin{pmatrix}1 & 2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\end{pmatrix}^{-1} = \begin{pmatrix}2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 4\end{pmatrix},$$
$$\theta_{(1\ 2\ 3)}\left(\begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix}\right) = \begin{pmatrix}1 & 2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 3\end{pmatrix} \circ \begin{pmatrix}2 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\end{pmatrix}^{-1} = \begin{pmatrix}2 & 1\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix},$$
$$\theta_{(1\ 2\ 3)}\left(\begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix}\right) = \begin{pmatrix}1 & 2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 4\end{pmatrix} \circ \begin{pmatrix}2 & 3\end{pmatrix} \circ \begin{pmatrix}1 & 2 & 3\end{pmatrix}^{-1} = \begin{pmatrix}2 & 4\end{pmatrix} \circ \begin{pmatrix}1 & 3\end{pmatrix}.$$

Επομένως, $\mathbb{A}_4 \cong V \rtimes_\theta K$ και αφού η $K \cong \mathbb{Z}_3$ συμπεραίνουμε ότι $\mathbb{A}_4 \cong V \rtimes_\theta \mathbb{Z}_3$.

[1]Στην Άσκηση A86 προσδιορίσαμε την ομάδα αυτομορφισμών τής ομάδας $(V, \star)$ των τεσσάρων στοιχείων, η οποία βέβαια είναι ισόμορφη προς την υποομάδα V τής S_4.

(γ′) Θεωρούμε τις κυκλικές ομάδες $C_3 = \langle a \rangle$ και $C_4 = \langle b \rangle$ τάξεων 3 και 4 αντιστοίχως. Η αντιστοιχία

$$\begin{aligned} \theta : & C_4 \to \mathrm{Aut}(C_3) \cong \mathbb{Z}_2 \\ b^s \to \ & \theta_{b^s} : C_3 \to C_3, \begin{cases} \forall x \in C_3, \theta_{b^s}(x) := x & \text{όταν } s \equiv 0 \bmod 2 \\ \forall x \in C_3, \theta_{b^s}(x) := x^{-1} & \text{όταν } s \equiv 1 \bmod 2. \end{cases} \end{aligned}$$

είναι μια καλά ορισμένη απεικόνιση, η οποία είναι ομομορφισμός.

Το εξωτερικό ημιευθύ γινόμενο $G = C_3 \rtimes_\theta C_4$ 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 $\{e_{C_3}\} \times C_4$ θα ήταν μια ορθόθετη υποομάδα τής G και τότε η G θα ήταν ισόμορφη προς το ευθύ γινόμενο $C_3 \times C_4$ που είναι μια αβελιανή ομάδα.

Με την ίδια επιχειρηματολογία συμπεραίνουμε ότι η μη αβελιανή ομάδα $G = C_3 \rtimes_\theta C_4$ ***δεν είναι ισόμορφη*** ούτε προς την εναλλάσσουσα ομάδα $\mathbb{A}_4$, η οποία είναι μη αβελιανή τάξης 12, διότι η υποομάδα

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

είναι μια ορθόθετη 2–Sylow υποομάδα τής $\mathbb{A}_4$, που είναι 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 7.2.10. *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:

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

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. $\square$

Η επόμενη πρόταση συμπληρώνει την Πρόταση 3.2.2.

Πρόταση 7.2.11. *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 3.2.2, γνωρίζουμε ότι η G διαθέτει μια ορθόθετη κυκλική υποομάδα C_q πρώτης τάξης q και μια κυκλική υποομάδα C_p πρώτης τάξης p. Επειδή $C_q \bigcap C_p = \{e_G\}$ 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 προς 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 προς την πολλαπλασιαστική ομάδα $\mathbb{Z}_q^\star$ των αντιστρέψιμων στοιχείων τού πεπερασμένου σώματος $\mathbb{Z}_q$, βλ. Παράδειγμα 1.7. Από το Θεώρημα 3.2.29 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

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

ένας οποιοσδήποτε ομομορφισμός ομάδων. Η εικόνα $\mathrm{im}\,\theta$ τού ομομορφισμού θ είναι ισόμορφη προς 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 $\mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$ είναι ο τετριμμένος και γι' αυτό στη συγκεκριμένη περίπτωση το εσωτερικό ημιευθύ γινόμενο $G = C_q \rtimes C_p$ είναι ισόμορφο προς το εξωτερικό ευθύ γινόμενο $\mathbb{Z}_q \times \mathbb{Z}_p$.

(β′). Αν $p \mid q-1$, τότε από τα προηγούμενα συμπεραίνουμε ότι εκτός τού τετριμμένου ομομορφισμού $\tau : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q), \forall [z]_p \in \mathbb{Z}_p, \tau([z]_p) = \mathrm{Id}_{\mathbb{Z}_q}$ 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 εμφυτεύσουμε την $\mathbb{Z}_p$, μέσω ενός μονομορφισμού $\theta : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$, εντός τής ομάδας αυτομορφισμών 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 $\theta : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$ είναι ένας μονομορφισμός.

Έστω ότι $\theta : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$ και $\varphi : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$ 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 $\mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$ είναι ισόμορφα. Παρατηρούμε ότι οι μη τετριμμένες υποομάδες $\mathrm{im}\,\theta$ και $\mathrm{im}\,\varphi$ τής $\mathrm{Aut}(\mathbb{Z}_q)$ είναι και οι δύο τάξης p, αφού είναι και οι δύο ισόμορφες προς την $\mathbb{Z}_p$. Συνεπώς, $\mathrm{im}\,\theta = \mathrm{im}\,\varphi$, 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

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

η οποία είναι ένας αυτομορφισμός τής $\mathbb{Z}_p$.
Από το Λήμμα 7.2.10 γνωρίζουμε ότι τα εξωτερικά ημιευθέα γινόμενα $\mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ και $\mathbb{Z}_p \rtimes_{\varphi\circ(\varphi^{-1}\circ\theta)} \mathbb{Z}_q$ είναι ισόμορφες ομάδες. Έτσι, αφού $\varphi \circ (\varphi^{-1} \circ \theta) = \theta$, καταλήγουμε ότι $\mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p \cong \mathbb{Z}_q \rtimes_\varphi \mathbb{Z}_p$. □

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

Πρόταση 7.2.12. *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′) ⇒ (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:

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

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

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

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

Γι΄αυτό

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

Ώστε $\forall \overline{h} \in H, n \in N$, $\theta_{\overline{h}}(n) = n$, δηλαδή $\forall \overline{h} \in H$, $\theta_{\overline{h}} = \mathrm{Id}_N$. 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 7.2.13. *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. «⇐» 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.
«⇒» 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 τού 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 7.2.14. *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 ομάδα, αν και μόνο αν, ο ομομορφισμός $\theta : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$ είναι τετριμμένος. Στην περίπτωση αυτή $\mathbb{Z}_q \rtimes_\theta \mathbb{Z}_p = \mathbb{Z}_q \times \mathbb{Z}_p$.*

Η ομάδα αυτομορφισμών $\mathrm{Aut}(D_n)$ της διεδρικής ομάδας $(D_n, \circ), n \geq 3$

Κατ’ αρχάς παρουσιάζουμε μια πολύ απλή μορφή τής έννοιας τής διασπάσιμης σύντομης ακριβούς ακολουθίας[2], προσαρμοσμένη στους σκοπούς τής παρούσας ενότητας.

Έστω ότι οι $(G', \star')$, $(G, \star)$ και $(G'', \star'')$ είναι ομάδες και ότι οι $G' \xrightarrow{\chi} G \xrightarrow{\psi} G''$ είναι μια ακολουθία δύο ομομορφισμών.

[2]Πρόκειται για μια ιδιαιτέρως σημαντική έννοια στα Σύγχρονα Μαθηματικά.

Ορισμός 7.2.15. Η ακολουθία των ομομορφισμών $\chi : G' \to G$ και $\psi : G \to G''$ ονομάζεται μια *σύντομη ακριβής ακολουθία ομομορφισμών*, αν ο χ είναι μονομορφισμός, ο ψ είναι επιμορφισμός και ισχύει ότι η εικόνα $\operatorname{im} \chi$ ισούται με τον πυρήνα $\ker \psi$.

Παράδειγμα 7.2.16. Όταν $(G, \star)$ είναι μια ομάδα και $N \trianglelefteq G$ είναι μια ορθόθετη υποομάδα της, τότε η ακολουθία $N \xrightarrow{\iota_N} G \xrightarrow{\pi_N} G/N$, όπου $\iota_N : N \to G, n \mapsto i_N(n) := n$ είναι η εμφύτευση τής N στη G και $\pi_N : G \to G/N, g \mapsto \pi_N(g) := gN$ είναι η φυσική προβολή τής G στην πηλικοομάδα G/N αποτελεί προφανώς μια σύντομη ακριβή ακολουθία.

Ορισμός 7.2.17. Η σύντομη ακριβής ακολουθία ονομάζεται *διασπάσιμη*, αν υπάρχει ομομορφισμός $\varphi : G'' \to G$ με τη σύνθεση $\psi \circ \varphi : G'' \to G''$ ίση με τον ταυτοτικό αυτομορφισμό $\mathrm{Id}_{G''}$ τής G''.

Παράδειγμα 7.2.18. Έστω ότι $G_1 \times G_2$ είναι το εξωτερικό ευθύ γινόμενο των ομάδων $(G_1, \star_1)$ και $(G_2, \star_2)$. Θεωρούμε τον ομομορφισμό $\iota_1 : G_1 \to G_1 \times G_2, g_1 \mapsto \iota_1(g_1) := (g_1, e_{G_2})$ και τον ομομορφισμό $\pi_2 : G_1 \times G_2 \to G_2, (g_1, g_2) \mapsto \pi_2((g_1, g_2)) := g_2$.
Η ακολουθία $G_1 \xrightarrow{\iota_1} G_1 \times G_2 \xrightarrow{\pi_2} G_2$ είναι σύντομη ακριβής, διότι προφανώς ο ι_1 είναι μονομορφισμός, ο π_2 είναι επιμορφισμός και $\operatorname{im} \iota_1 = \{(g_1, e_{G_2}) \mid g_1 \in G_1\} = \ker \pi_2$. Επιπλέον, η συγκεκριμένη σύντομη ακριβής ακολουθία είναι διασπάσιμη, αφού ο ομομορφισμός $\pi_2 \circ \iota_2 : G_2 \to G_2$ ισούται με τον ταυτοτικό αυτομορφισμό Id_{G_2}, όπου $\iota_2 : G_2 \to G_1 \times G_2, g_2 \mapsto \iota_2(g_2) := (e_{G_1}, g_2)$.

Λήμμα 7.2.19. *Έστω ότι η ακολουθία των ομομορφισμών $N \xrightarrow{\iota} G \xrightarrow{\psi} H$ είναι μια σύντομη ακριβής ακολουθία. Αν υπάρχει ομομορφισμός $\chi : H \to G$ με $\psi \circ \chi = \mathrm{Id}_H$, δηλαδή αν η ακολουθία είναι διασπάσιμη, τότε η ομάδα G είναι το εσωτερικό ημιευθύ γινόμενο τής ορθόθετης υποομάδας $\operatorname{im} \iota \trianglelefteq G$ με την υποομάδα $\operatorname{im} \chi \leq G$. Με άλλα λόγια $G = \operatorname{im} \iota \rtimes \operatorname{im} \chi$.*

Απόδειξη. Θα επιβεβαιώσουμε τις απαιτήσεις τού Ορισμού 7.2.3. Κατ' αρχάς $\operatorname{im} \iota \trianglelefteq G$, διότι $\operatorname{im} \iota = \ker \psi$. Όταν $g \in \operatorname{im} \iota \bigcap \operatorname{im} \chi$, τότε $g = \chi(h) = \iota(n)$, για κάποια $h \in H$ και $n \in N$. Παρατηρούμε ότι $\psi(g) = \psi(\chi(h)) = \psi(\iota(n)) = e_H$, αφού $\operatorname{im} \iota = \ker \psi$ και ότι $\psi(\chi(h)) = h$, αφού $\psi \circ \chi = \mathrm{Id}_H$. Επομένως $h = e_H$ και ως εκ τούτου, $g = \chi(h) = \chi(e_H) = e_H$.

Κάθε $g \in G$ εκφράζεται ως $g = g[\chi(\psi(g^{-1}g))] = [g\chi(\psi(g^{-1}))]\chi(\psi(g))$. Προφανώς, το $\chi(\psi(g))$ ανήκει στο $\operatorname{im} \chi$. Ισχυριζόμαστε ότι το $g\chi(\psi(g^{-1}))$ ανήκει στο $\operatorname{im} \iota = \ker \psi$. Πράγματι, $\psi(g\chi(\psi(g^{-1}))) = \psi(g)(\psi \circ \chi \circ \psi(g^{-1})) = \psi(g)\psi(g^{-1}) = e_H$, διότι $\psi \circ \chi = \mathrm{Id}_H$. Επομένως, $G = (\operatorname{im} \iota)(\operatorname{im} \chi)$ και τελικώς $G = \operatorname{im} \iota \rtimes \operatorname{im} \chi$. □

Θεώρημα 7.2.20. *Η ομάδα $\mathrm{Aut}(D_n)$ αυτομορφισμών τής διεδρικής ομάδας $(D_n, \circ)$ είναι ισόμορφη με το εξωτερικό ημιευθύ γινόμενο $\mathbb{Z}_n \rtimes_\theta \mathbb{U}_n$, όπου $\theta : \mathbb{U}_n \to \mathrm{Aut}(\mathbb{Z}_n)$ είναι ο ισομορφισμός με την τιμή $\theta_{[s]_n} : \mathbb{Z}_n \to \mathbb{Z}_n, [i]_n \mapsto \theta_{[s]_n}([i]_n) := [si]_n$, για κάθε $[s]_n \in \mathbb{U}_n$.*

(Στις επόμενες γραμμές για να αποφύγουμε τυχόν παρανοήσεις συμβολίζουμε την πράξη τής D_n με «$\cdot$» και την πράξη τής σύνθεσης των στοιχείων τής $\mathrm{Aut}(D_n)$ με «$\circ$».)

Απόδειξη. Θεωρούμε τη σύντομη ακριβή ακολουθία $\ker \Psi \xrightarrow{\iota} \mathrm{Aut}(D_n) \xrightarrow{\Psi} \mathrm{Aut}(\langle \rho \rangle)$, $(*)$, βλ. στην απόδειξη τού Θεωρήματος 1.7.40, όπου ι είναι η εμφύτευση τού $\ker \Psi$ στην $\mathrm{Aut}(D_n)$

και $\Psi : \mathrm{Aut}(D_n) \to \mathrm{Aut}(\langle\rho\rangle)$ είναι ο επιμορφισμός με $\Psi(\chi) := \chi_{|\langle\rho\rangle}, \forall \chi \in \mathrm{Aut}(D_n)$. Υπενθυμίζουμε ότι ο $\ker\Psi$ ισούται με την κυκλική ομάδα $\langle\psi\rangle$, όπου ψ είναι ο αυτομορφισμός τής D_n με $\psi(\rho) = \rho$ και $\psi(\tau) = \tau\cdot\rho$, βλ. Παρατήρηση 1.7.41.

Ισχυριζόμαστε ότι η σύντομη ακριβής ακολουθία $(*)$ είναι διασπάσιμη. Πράγματι, κάθε αυτομορφισμός $\sigma \in \mathrm{Aut}(\rho)$, επεκτείνεται σε έναν αυτομορφισμό $\hat{\sigma} \in \mathrm{Aut}(D_n)$, ορίζοντας $\forall i \in \mathbb{Z}, \hat{\sigma}(\rho^i) = \sigma(\rho^i)$ και $\hat{\sigma}(\tau\cdot\rho^i) = \tau\cdot\sigma(\rho^i)$, βλ. το πρώτο τμήμα τού Λήμματος 1.7.39. Θα δείξουμε ότι η απεικόνιση $\Sigma : \mathrm{Aut}(\langle\rho\rangle) \to \mathrm{Aut}(D_n), \sigma \mapsto \Sigma(\sigma) := \hat{\sigma}$ είναι ένας ομομορφισμός.

Προς τούτο, αρκεί να ισχύει $\Sigma(\sigma_1\circ\sigma_2) = \Sigma(\sigma_1)\circ\Sigma(\sigma_2)$.

Για κάθε $\rho^i, i \in \mathbb{Z}$, είναι $\Sigma(\sigma_1\circ\sigma_2)(\rho^i) = (\sigma_1\circ\sigma_2)(\rho^i)$ και $\Sigma(\sigma_1)\circ\Sigma(\sigma_2)(\rho^i) = \Sigma(\sigma_1)(\Sigma(\sigma_2)(\rho^i)) = \Sigma(\sigma_1)(\hat{\sigma}_2(\rho^i)) == \Sigma(\sigma_1)(\sigma_2(\rho^i)) = \hat{\sigma}_1(\sigma_2(\rho^i)) \overset{(\dagger)}{=} \sigma_1(\sigma_2(\rho^i)) = (\sigma_1\circ\sigma_2)(\rho^i)$. Η ισότητα $(\dagger)$ ισχύει επειδή το $\sigma_2(\rho^i)$ ανήκει στην $\langle\rho\rangle$.

Για κάθε $\tau\cdot\rho^i, i \in \mathbb{Z}$, είναι $\Sigma(\sigma_1\circ\sigma_2)(\tau\cdot\rho^i) = \tau\cdot((\sigma_1\circ\sigma_2)(\rho^i))$ και $\Sigma(\sigma_1)\circ\Sigma(\sigma_2)(\tau\cdot\rho^i) = \Sigma(\sigma_1)(\Sigma(\sigma_2)(\tau\cdot\rho^i)) = \Sigma(\sigma_1)(\hat{\sigma_2}(\tau\cdot\rho^i)) = \Sigma(\sigma_1)(\tau\cdot\sigma_2(\rho^i)) = \hat{\sigma_1}(\tau\cdot\sigma_2(\rho^i)) \overset{(\ddagger)}{=} \tau\cdot\sigma_1(\sigma_2(\rho^i)) = \tau\cdot((\sigma_1\circ\sigma_2)(\rho^i))$. Η ισότητα $(\ddagger)$ ισχύει επειδή το $\sigma_2(\rho^i)$ ανήκει στην $\langle\rho\rangle$. Άρα η απεικόνιση Σ είναι ομομορφισμός.

Ισχυριζόμαστε ότι η σύνθεση $\Psi\circ\ \Sigma$ ισούται με την ταυτοτική απεικόνιση $\mathrm{Aut}(\rho) \to \mathrm{Aut}(\langle\rho\rangle)$. Πράγματι $\forall\sigma \in \mathrm{Aut}(\rho)$, είναι $\Psi\circ\ \Sigma(\sigma) = \Psi(\hat{\sigma}) = \hat{\sigma}_{|\langle\rho\rangle} = \sigma$

Αφού η $(*)$ είναι μια διασπάσιμη σύντομη ακριβής ακολουθία, συμπεραίνουμε από το Λήμμα 7.2.19 ότι $\mathrm{Aut}(D_n) = \mathrm{im}\,\iota \rtimes \mathrm{im}\,\Sigma$.

Τώρα θα κατασκευάσουμε τον ομομορφισμό $\Theta : \mathrm{im}\,\Sigma \to \mathrm{Aut}(\mathrm{im}\,\iota)$. Όταν $\sigma \in \mathrm{Aut}(\langle\rho\rangle)$ με $\sigma(\rho) = \rho^s$, όπου $s \in \mathbb{N}, 1 \le s \le n$ με $\mathrm{MK\Delta}(s,n) = 1$, τότε ο αυτομορφισμός $\Theta_{\Sigma(\sigma)} : \mathrm{im}\,\iota \to \mathrm{im}\,\iota$ ορίζεται πλήρως από την τιμή επί τού γεννήτορα ψ τής $\mathrm{im}\,\iota = \ker\Psi$. Υπενθυμίζουμε ότι ο $\Theta_{\Sigma(\sigma)}(\psi)$ ορίζεται ως $\Theta_{\Sigma(\sigma)}(\psi) := \Sigma(\sigma)\circ\psi\circ\Sigma(\sigma)^{-1} = \hat{\sigma}\circ\psi\circ\hat{\sigma}^{-1}$, βλ. Παρατήρηση 7.2.4. Ας προσδιορίσουμε αυτόν τον αυτομορφισμό. Είναι $\hat{\sigma}\circ\psi\circ\hat{\sigma}^{-1}(\rho) = \rho$, διότι η $\mathrm{im}\,\iota = \ker\Psi$ είναι ορθόθετη υποομάδα τής $\mathrm{Aut}(D_n)$. Επιπλέον είναι $\hat{\sigma}\circ\psi\circ\hat{\sigma}^{-1}(\tau) = \hat{\sigma}\circ\psi(\tau) = \hat{\sigma}(\tau\cdot\rho) = \tau\cdot\sigma(\rho) = \tau\cdot\rho^s$. Άρα, ο αυτομορφισμός $\Theta_{\Sigma(\sigma)} : \mathrm{im}\,\iota \to \mathrm{im}\,\iota$ ισούται με τον αυτομορφισμό τής $\mathrm{im}\,\iota$, ο οποίος απεικονίζει τον γεννήτορα ψ στο ψ^s, διότι $\psi^s(\rho) = \rho$ και $\psi^s(\tau) = \tau\cdot\rho^s$. Προσέξτε ότι ο Θ είναι ισομορφισμός, αφού κάθε αυτομορφισμός τής $\mathrm{im}\,\iota = \ker\Psi$ είναι τής μορφής $\psi \mapsto \psi^s$, όπου $s \in \mathbb{N}, 1 \le s \le n$ με $\mathrm{MK\Delta}(s,n) = 1$, διότι η $\mathrm{im}\,\iota = \ker\Psi$ είναι μια κυκλική ομάδα τάξης n.

Παρατηρούμε ότι $\mathrm{im}\,\Sigma \cong \mathrm{Aut}(\langle\rho\rangle) \cong \mathbb{U}_n$ και ότι $\mathrm{im}\,\iota = \ker\Psi \cong \mathbb{Z}_n$, όπου $(\mathbb{U}_n,\cdot)$ η ομάδα των αντιστρέψιμων στοιχείων τού $\mathbb{Z}_n$. Μέσω αυτών των ισομορφισμών, ο ομομορφισμός $\Theta : \mathrm{im}\,\Sigma \to \mathrm{Aut}(\mathrm{im}\,\iota)$ αντιστοιχεί στον ομομορφισμό $\theta : \mathbb{U}_n \to \mathrm{Aut}(\mathbb{Z}_n), [s]_n \mapsto \theta_{[s]_n}$, όπου $\theta_{[s]_n} : \mathbb{Z}_n \to \mathbb{Z}_n, [i]_n \mapsto [si]_n$. Επομένως η ομάδα $\mathrm{Aut}(D_n)$ των αυτομορφισμών τής D_n είναι ισόμορφη προς το εξωτερικό ημιευθύ γινόμενο $\mathbb{Z}_n \rtimes_\theta \mathbb{U}_n$. □

7.3 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 οποιονδήποτε έχει παρακολουθήσει 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 3.2.2 και 7.2.11.

Ας δούμε το γενικό αποτέλεσμα που θα αποδείξουμε:

Θεώρημα 7.3.1. *Έστω n ένας πάγιος φυσικός. Κάθε ομάδα τάξης n είναι κυκλική, αν και μόνο αν, οι αριθμοί n και $\varphi(n)$ είναι σχετικώς πρώτοι, όπου φ είναι η φ-συνάρτηση Euler.*

Παρατήρηση 7.3.2. Υπενθυμίζουμε τα εξής:

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

(β′) Αν $n = n'n''$ με $\text{ΜΚΔ}(n', n'') = 1$, τότε $\varphi(n) = \varphi(n')\varphi(n'')$.

(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

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

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

Επιπλέον, παρατηρούμε τα εξής:

(ε′) Έστω ότι $n > 1$ είναι ένας φυσικός με $\text{ΜΚΔ}(n, \varphi(n)) = 1$, 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 $\text{ΜΚΔ}(p, n') = 1$ και $\alpha \geq 2$. Αλλά τότε $\varphi(n) = (p^\alpha - p^{\alpha-1})\varphi(n')$ και συνεπώς ο p θα διαιρούσε και τον n και τον $\varphi(n)$, άρα και τον $\text{ΜΚΔ}(n, \varphi(n)) = 1$, 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 $n = p^\alpha n'$, $\alpha \geq 2$ με $\text{ΜΚΔ}(p, n') = 1$.

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 τάξης 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 $\varphi(n')$ είναι διαιρέτης τού $\varphi(n)$.

(η′) Αν $(G, \star)$ είναι μια ομάδα με τάξη n με τον ΜΚΔ$(n, \varphi(n)) = 1$ και αν $H = \langle a \rangle$ είναι μια κυκλική υποομάδα της, τότε ο ορθοθετοποιητής $\mathcal{N}_G(H) = \{g \in G \mid gHg^{-1} = H\}$ τής H συμπίπτει με τον κεντροποιητή $\mathcal{C}_G(a) = \{g \in G \mid ga = ag\}$ τού γεννήτορα a τής H.

Κατ' αρχάς, $\forall h \in H$, έχουμε $\mathcal{C}_G(a) \leq \mathcal{C}_G(h)$. Πράγματι, όταν $g \in \mathcal{C}_G(a)$ και $h \in H$, τότε υπάρχει $s \in \mathbb{N} \bigcup \{0\}$ με $h = a^s$ και

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

Επομένως, $\mathcal{C}_G(a) \leq \mathcal{N}_G(H)$.
Τώρα θα δείξουμε ότι $\mathcal{N}_G(H) \leq \mathcal{C}_G(a)$. Πράγματι, αν $g \in \mathcal{N}_G(H)$, 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 1.7, γνωρίζουμε ότι η τάξη τής ομάδας $\mathrm{Aut}(H)$ ισούται με $\varphi(n')$, όπου n' είναι η τάξη τής κυκλικής ομάδας H. Επομένως, η τάξη $\circ(\sigma_g)$ τού σ_g είναι ένας διαιρέτης τής τάξης $\varphi(n')$ τής H. Από το (ε′) γνωρίζουμε ότι ο n είναι ελεύθερος τετραγώνων και από το (ζ′) γνωρίζουμε ότι $\varphi(n') \mid \varphi(n)$. Ως εκ τούτου, $\circ(\sigma_g) \mid \varphi(n)$.

Αφού για κάθε $s \in \mathbb{N}$, η συζυγία $\sigma_{g^s} : H \to H, h \to g^shg^{-s}$ 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 $g \in \mathcal{N}_G(H) \leq G$ διαιρεί την τάξη n τής G, συμπεραίνουμε ότι $\circ(\sigma_g) \mid n$.

Αφού όμως ΜΚΔ$(n, \varphi(n)) = 1$ και επειδή όπως διαπιστώσαμε $\circ(\sigma_g) \mid \varphi(n)$ 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 $g \in \mathcal{N}_G(H)$, τότε $g \in \mathcal{C}_G(a)$ και συνεπώς $\mathcal{N}_G(H) \leq \mathcal{C}_G(a)$.

Έτσι αποδείξαμε ότι $\mathcal{N}_G(H) = \mathcal{C}_G(a)$, για κάθε κυκλική υποομάδα $H = \langle a \rangle$ τής G.

Απόδειξη. **(Η απόδειξη τού Θεωρήματος 7.3.1)**
«$\Rightarrow$» Έστω ότι για κάποιον φυσικό n, κάθε ομάδα τάξης n είναι κυκλική. Θα δείξουμε ότι ο ΜΚΔ$(n, \varphi(n)) = 1$. Σύμφωνα με το (στ′) των Παρατηρήσεων 7.3.2, ο n είναι ελεύθερος τετραγώνων, δηλαδή ισούται με $p_1p_2 \ldots p_s$, όπου οι $p_i, 1 \leq i \leq s$ είναι πρώτοι αριθμοί διαφορετικοί ανά δύο και ως εκ τούτου ο $\varphi(n)$ ισούται με $(p_1 - 1)(p_2 - 1) \ldots (p_s - 1)$.

Αν ήταν ο ΜΚΔ$(n, \varphi(n)) \neq 1$, 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 7.2.11, 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_ip_j. Θεωρούμε την κυκλική ομάδα $\mathbb{Z}_{n'}$, όπου $n = p_ip_jn'$ 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 ΜΚΔ$(n, \varphi(n)) = 1$.

«$\Leftarrow$» Θα δείξουμε ότι, για κάθε φυσικό n με ΜΚΔ$(n, \varphi(n)) = 1$, κάθε ομάδα τάξης n είναι κυκλική.

Έστω ότι υπάρχουν φυσικοί n με ΜΚΔ$(n, \varphi(n)) = 1$, 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 ΜΚΔ$(m, \varphi(m)) = 1$, συμπεραίνουμε από το (ε′) των Παρατηρήσεων 7.3.2, ότι ο m είναι ελεύθερος τετραγώνων,

Ας υποθέσουμε ότι $(G, \star)$ μια ομάδα τάξης m, η οποία δεν είναι κυκλική. Θα δείξουμε ότι είναι αδύνατο να υπάρχει μια τέτοια ομάδα. Κατ' αρχάς, παρατηρούμε ότι η G δεν είναι ούτε αβελιανή, αφού αν ήταν, τότε θα ήταν και κυκλική, διότι ο m είναι ελεύθερος τετραγώνων, βλ. Πόρισμα 4.2.10.

Αν m' είναι ένας διαιρέτης τού m, τότε ΜΚΔ$(m', \varphi(m')) = 1$. Αφού αν δ είναι ένας κοινός διαιρέτης των m' και $\varphi(m')$, τότε ο δ είναι επίσης κοινός διαιρέτης των m και $\varphi(m)$, επειδή $m' \mid m$ και $\varphi(m') \mid \varphi(m)$, βλ. το (ζ′) των Παρατηρήσεων 7.3.2.

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 $\mathcal{Z}(G)$ τής G είναι γνήσια υποομάδα της G επειδή, όπως είδαμε, η G δεν είναι αβελιανή. Ισχυριζόμαστε ότι $\mathcal{Z}(G) = \{e_G\}$. Πράγματι, αν ήταν $\mathcal{Z}(G) \neq \{e_G\}$, τότε λόγω τού (*), η πηλικοομάδα $G/\mathcal{Z}(G)$ θα ήταν κυκλική (αφού θα είχε τάξη έναν διαιρέτη τού m γνήσια μικρότερο από τον m) και τότε η G θα ήταν αβελιανή, βλ. Άσκηση Α78. Αυτό όμως είναι άτοπο. Ώστε, $\mathcal{Z}(G) = \{e_G\}$.

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

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 αφού για κάθε πρώτο διαιρέτη p τού m υπάρχει στοιχείο αντίστοιχης τάξης, βλ. Θεώρημα Cauchy (Θεώρημα 2.3.11). Λόγω τού (*), η $\mathcal{M}$ είναι μια κυκλική υποομάδα τής G και γι΄αυτό $\mathcal{M} \leq \mathcal{C}_G(g)$, όπου g είναι οποιοδήποτε στοιχείο τής $\mathcal{M}$. Επειδή η $\mathcal{M}$ είναι μεγιστοτική και η $\mathcal{C}_G(g)$ είναι γνήσια υποομάδα τής G, συμπεραίνουμε ότι $\forall g \in \mathcal{M}, g \neq e_G$ είναι $\mathcal{C}_G(g) = \mathcal{M}$.

Ισχυριζόμαστε ότι

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

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

Ερχόμαστε τώρα στο κύριο επιχείρημα τής απόδειξης:

Έστω $\mathcal{M}$ μια μεγιστοτική υποομάδα τής G. Ισχυριζόμαστε ότι κάθε υποομάδα τής G, η οποία είναι συζυγής προς την $\mathcal{M}$, είναι επίσης μεγιστοτική. Πράγματι, όταν η $g\mathcal{M}g^{-1}$ περιέχεται γνήσια σε μια υποομάδα $A \leq G$, τότε η $\mathcal{M}$ περιέχεται γνήσια στην $g^{-1}Ag$ και γι' αυτό $g^{-1}Ag = G$. Συνεπώς, $A = G$ και ως εκ τούτου, η $g\mathcal{M}g^{-1}$ είναι μεγιστοτική. Ώστε κάθε υποομάδα που είναι συζυγής προς την $\mathcal{M}$, είναι επίσης μεγιστοτική υποομάδα τής G. Λόγω τού (**), συμπεραίνουμε ότι η τομή δύο οποιωνδήποτε διαφορετικών υποομάδων τής G, οι οποίες είναι συζυγείς προς την $\mathcal{M}$, ισούται με $\{e_G\}$.

Το πλήθος τού συνόλου[3] $\{g\mathcal{M}g^{-1} \mid g \in G\}$, δηλαδή τού συνόλου των υποομάδων τής G οι οποίες είναι συζυγείς προς την $\mathcal{M}$, ισούται με τον δείκτη

$$[G : \mathcal{N}_G(\mathcal{M})] = [G:1]/[\mathcal{N}_G(\mathcal{M}):1],$$

όπου $\mathcal{N}_G(\mathcal{M})$ είναι ο ορθοθετοποιητής τής $\mathcal{M}$, βλ. το (γ′) των Παρατηρήσεων 2.4.7. Η $\mathcal{M}$ είναι κυκλική, διότι είναι μια γνήσια υποομάδα τής G και λόγω τής παραδοχής που κάναμε για την τάξη m τής G. Ας πούμε ότι $\mathcal{M} = \langle a \rangle$. Σύμφωνα με το (ζ′) των Παρατηρήσεων 7.3.2, έχουμε ότι $\mathcal{N}_G(\mathcal{M}) = \mathcal{C}_G(a)$. Αλλά όπως είδαμε προηγουμένως, για κάθε $g \in \mathcal{M}, g \neq e_G$, είναι $\mathcal{M} = \mathcal{C}_G(g)$. Ιδιαιτέρως, $\mathcal{M} = \mathcal{C}_G(a)$ και συνεπώς ο ορθοθετοποιητής $\mathcal{N}_G(\mathcal{M})$ τής $\mathcal{M}$ ισούται με την ίδια την $\mathcal{M}$.

Επομένως, το πλήθος τού συνόλου $\{g\mathcal{M}g^{-1} \mid g \in G\}$ ισούται με $[G:1]/[\mathcal{M}:1]$.

Τώρα, το πλήθος των στοιχείων $\neq e_G$ που περιέχει η ένωση $\bigcup_{g\in G} g\mathcal{M}g^{-1}$ ισούται με

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

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

Όπως και προηγουμένως, διαπιστώνουμε ότι το πλήθος των στοιχείων $\neq e_G$ που περιέχει η ένωση $\bigcup_{g\in G} g\mathcal{N}g^{-1}$ ισούται με

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

Το μόνο κοινό στοιχείο όλων αυτών των μεγιστοτικών υποομάδων, οι οποίες είναι συζυγείς ή προς την $\mathcal{M}$ ή 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 $\neq e_G$, που περιέχει η ένωση $(\bigcup_{g\in G} g\mathcal{M}g^{-1}) \bigcup (\bigcup_{g\in G} g\mathcal{N}g^{-1})$.

[3]Η τροχιά τής $\mathcal{M}$, καθώς η G δρα μέσω συζυγίας επί τού συνόλου των υποομάδων της.

Δηλαδή,

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

Επειδή $[\mathcal{M}:1] \geq 2$ και $[\mathcal{N}:1] \geq 2$, η τελευταία **γνήσια!** ανισότητα δεν είναι αληθής και έτσι οδηγούμαστε σε άτοπο. Ώστε, δεν υπάρχει καμιά κυκλική ομάδα G τάξης m που να ικανοποιεί τη συνθήκη $\text{ΜΚΔ}(m, \varphi(m)) = 1$. Η απόδειξη τού θεωρήματος έχει πλέον ολοκληρωθεί. □

Πόρισμα 7.3.3. *Για $n \in \mathbb{N}$, ο ΜΚΔ$(\ \varphi(n), \varphi(\varphi(n))\ )$ ισούται με 1, αν και μόνο αν, $n = 1, 2, 3, 4, 6$.*

Απόδειξη. «$\Leftarrow$» Επειδή $\varphi(1) = 1, \varphi(2) = 1, \varphi(3) = 2, \varphi(4) = 2, \varphi(6) = 2$ είναι προφανές ότι ο ΜΚΔ$(\ \varphi(n), \varphi(\varphi(n))\ ) = 1$.
«$\Rightarrow$» Επειδή ο ΜΚΔ$(\ \varphi(n), \varphi(\varphi(n))\ ) = 1$, συμπεραίνουμε από το Θεώρημα 7.3.1 ότι κάθε ομάδα τάξης $\varphi(n)$ είναι κυκλική. Ιδιαιτέρως, η ομάδα $(\mathbb{U}_n, \cdot)$ των αντιστρέψιμων στοιχείων τού $\mathbb{Z}_n$ είναι κυκλική, διότι η τάξη της ισούται με $\varphi(n)$. Από την Άσκηση A95, γνωρίζουμε ότι στην περίπτωση αυτή, η τάξη n ισούται με $1, 2, 4, p^k, 2p^k$ με $k \in \mathbb{N}$, όπου ο p είναι ένας περιττός πρώτος. Επειδή $\varphi(p^k) = p^{(k-1)}(p-1)$, συμπεραίνουμε ότι $\varphi(p^k) \geq 4$, για κάθε $k \in \mathbb{N}$ και κάθε περιττό πρώτο ≥ 5. Επομένως, ο 2 είναι διαιρέτης των $\varphi(p^k)$ και $\varphi(\varphi(p^k))$, αφού γενικά ο $\varphi(s)$ είναι άρτιος αριθμός, όταν ο $s \geq 3$. Ως εκ τούτου οι $\text{ΜΚΔ}(\varphi(p^k), \varphi(\varphi(p^k)))$ και $\text{ΜΚΔ}(\varphi(2p^k), \varphi(\varphi(2p^k)))$ είναι $\neq 1$, για κάθε περιττό πρώτο αριθμό $p \geq 5$.
Με τον ίδιο ακριβώς τρόπο συμπεραίνουμε ότι για $k \geq 2$, οι $\text{ΜΚΔ}(\varphi(3^k), \varphi(\varphi(3^k)))$ και $\text{ΜΚΔ}(\varphi(2 \cdot 3^k), \varphi(\varphi(2 \cdot 3^k)))$ είναι $\neq 1$. Έτσι μένουν μόνο οι περιπτώσεις 3 και $2 \cdot 3 = 6$, όπου προφανώς $\text{ΜΚΔ}(\varphi(3), \varphi(\varphi(3))) = 1$ και $\text{ΜΚΔ}(\varphi(6), \varphi(\varphi(6))) = 1$. □

Ασκήσεις στα ημιευθέα Γινόμενα

Λυμένες Ασκήσεις

A 144. Να βρεθούν (με ακρίβεια ισομορφίας) όλα τα εξωτερικά ημιευθέα γινόμενα τής κυκλικής ομάδας C_3 με τον εαυτό της, όπου $[C_3 : 1] = 3$.

Λύση. Κάθε εξωτερικό ημιευθύ γινόμενο τής C_3 με τον εαυτό της είναι τής μορφής $C_3 \rtimes_\theta C_3$, όπου $\theta : C_3 \to \text{Aut}(C_3)$ είναι ένας ομομορφισμός από τη C_3 στην ομάδα αυτομορφισμών της $\text{Aut}(C_3)$. Επειδή $\text{Aut}(C_3) \cong \mathbb{U}_3 \cong \mathbb{Z}_2$, συμπεραίνουμε ότι ο μοναδικός ομομορφισμός θ είναι ο τετριμμένος, διότι ο $\text{ΜΚΔ}[3, 2] = 1$. Από την Πρόταση 7.2.12, συμπεραίνουμε ότι κάθε εξωτερικό ημιευθύ γινόμενο είναι ισόμορφο με το εξωτερικό ευθύ γινόμενο $C_3 \times C_3$. Με ακρίβεια ισομορφίας, υπάρχει μόνο ένα εξωτερικό ευθύ γινόμενο τής C_3 με τον εαυτό της, το οποίο φυσικά είναι το $C_3 \times C_3$.
(Μια διαφορετική επιχειρηματολογία: Η ομάδα $C_3 \rtimes_\theta C_3$ είναι τάξης 3^2 και ως εκ τούτου είναι αβελιανή. Τώρα συμπεραίνουμε και πάλι με τη βοήθεια τού Πορίσματος 7.2.13, ότι $C_3 \rtimes_\theta C_3 \cong C_3 \times C_3$.)

Α 145. Να δειχθεί ότι για κάθε περιττό φυσικό $n \geq 3$, υπάρχει μια μη αβελιανή ομάδα τάξης $2n$.

Λύση. Φυσικά μπορούμε να απαντήσουμε αμέσως λέγοντας ότι η διεδρική ομάδα $(D_n, \circ)$ δεν είναι αβελιανή και η τάξη της ισούται με $2n$. Όμως εδώ θα επιχειρηματολογήσουμε με τη βοήθεια τής έννοιας τού ημιευθέος γινομένου. Θεωρούμε την ομάδα $(\mathbb{Z}_2, +)$ και την κυκλική ομάδα C_n τάξης n. Η απεικόνιση $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(C_n)$ με $\theta([0]_2) = \mathrm{Id}_{C_n}$ και $\theta([1]_2) : C_n \to C_n, x \mapsto x^{-1}$ είναι ένας ομομορφισμός ομάδων, ο οποίος μάλιστα δεν είναι ο τετριμμένος, αφού υπάρχει πάντοτε κάποιο $x \in C_n$ με $x \neq x^{-1}$, διότι ο n είναι περιττός ≥ 3. Συνεπώς, το εξωτερικό ημιευθύ γινόμενο $C_n \rtimes_\theta C_2$ είναι μια μη αβελιανή ομάδα τάξης $2n$.

Α 146. Έστω $C_{p^2} = \langle a \rangle$ μια κυκλική ομάδα τάξης p^2 και $N = \langle a^p \rangle$ η μοναδική υποομάδα τής C_{p^2} τάξης p. Θεωρούμε τη σύντομη ακριβή ακολουθία $\mathrm{N} \xrightarrow{\iota_N} C_{p^2} \xrightarrow{\pi_N} C_{p^2}/N, \ \ (*)$, όπου ι_N είναι η εμφύτευση τής N στην C_{p^2} και π_N είναι η φυσική προβολή. Να δειχθεί ότι η σύντομη ακριβής ακολουθία $(*)$ δεν είναι διασπάσιμη.

Λύση. Αν η $(*)$ ήταν διασπάσιμη, τότε η C_{p^2} θα ήταν ισόμορφη με ένα ημιευθές γινόμενο τής N με την C_{p^2}/N. Επειδή η C_{p^2} είναι αβελιανή, τότε αυτή θα ήταν ισόμορφη με το εξωτερικό ευθύ γινόμενο δύο ομάδων τάξης p και τότε δεν θα διέθετε ένα στοιχείο τάξης p^2. Αυτό όμως είναι άτοπο. Άρα η $(*)$ είναι μια σύντομη ακριβής ακολουθία που δεν διασπάται.

Α 147. Έστω ότι $(\mathrm{GL}_n(\mathbb{K}), \cdot)$ είναι η ομάδα των αντιστρέψιμων $n \times n$ πινάκων με συνιστώσες από ένα σώμα $\mathbb{K}$, ότι $\mathrm{SL}_n(\mathbb{K}) \trianglelefteq \mathrm{GL}_n(\mathbb{K})$ είναι η υποομάδα που αποτελείται από τους πίνακες A με $\det A = 1$ και ότι $(\mathbb{K}^\star, \cdot)$ είναι η πολλαπλασιαστική ομάδα τού σώματος $\mathbb{K}$. Να δειχθεί ότι η $\mathrm{GL}_n(\mathbb{K})$ είναι το εξωτερικό ημιευθύ γινόμενο τής $\mathrm{SL}_n(\mathbb{K})$ με την $\mathbb{K}^\star$. Επιπλέον για $n \geq 2$, να δειχθεί ότι το συγκεκριμένο ημιευθύ γινόμενο δεν είναι ευθύ.

Λύση. Θεωρούμε την ακολουθία $\mathrm{SL}_n(\mathbb{K}) \xrightarrow{\iota} \mathrm{GL}_n(\mathbb{K}) \xrightarrow{\det} \mathbb{K}^\star, \ \ (*)$, όπου $\iota : \mathrm{SL}_n(\mathbb{K}) \to \mathrm{GL}_n(\mathbb{K}), A \mapsto i(A) := A$ είναι η εμφύτευση τής $\mathrm{SL}_n(\mathbb{K})$ στη $\mathrm{GL}_n(\mathbb{K})$ και $\det : \mathrm{GL}_n(\mathbb{K}) \to \mathbb{K}^\star, A \mapsto \det A$ είναι ομομορφισμός που ορίζεται από την ορίζουσα det. Η συγκεκριμένη ακολουθία είναι προφανώς μια σύντομη ακριβή ακολουθία.
Ισχυριζόμαστε ότι η $(*)$ είναι διασπάσιμη. Πράγματι, θεωρούμε την απεικόνιση

$$\chi : \mathbb{K}^\star \to \mathrm{GL}_n(\mathbb{K}), k \mapsto \chi(k) := \begin{pmatrix} k & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & 0 \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Είναι εύκολη η διαπίστωση ότι ο χ είναι ένας ομομορφισμός ομάδων με την ιδιότητα $\det \circ \chi = \mathrm{Id}_{\mathbb{K}^\star}$. Από το Λήμμα 7.2.19, συμπεραίνουμε ότι η $\mathrm{GL}_n(\mathbb{K})$ είναι το εξωτερικό ημιευθύ γινόμενο $\mathrm{SL}_n(\mathbb{K}) \rtimes_\theta \mathbb{K}^\star$.
Παρατηρούμε ότι ο ομομορφισμός

$$\theta : \mathbb{K}^\star \to \mathrm{Aut}(\mathrm{SL}_n(\mathbb{K})), k \mapsto \theta_k : \begin{array}{l} \mathrm{SL}_n(\mathbb{K}) \to \mathrm{SL}_n(\mathbb{K}) \\ \qquad A \mapsto \chi(k) A \chi(k)^{-1} \end{array}$$

δεν είναι ο ταυτοτικός, όταν ο $n \geq 2$.

Πράγματι, θεωρούμε τον άνω τριγωνικό πίνακα $A = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}$

και διαπιστώνουμε ότι

$$\chi(k)A = \begin{pmatrix} k & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} k & k & k & \dots & k \\ 0 & 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

ενώ

$$A\chi(k) = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \begin{pmatrix} k & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} k & 1 & 1 & \dots & 1 \\ 0 & 1 & 1 & \dots & 1 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

Επομένως, όταν $k \neq 1$, τότε $\chi(k)A\chi(k)^{-1} \neq A$.

Α 148. Έστω ότι $(\mathrm{GL}_2(\mathbb{C}), \cdot)$ είναι η ομάδα των αντιστρέψιμων 2×2 πινάκων με συνιστώσες από το σώμα $\mathbb{C}$ των μιγαδικών αριθμών και ότι G είναι η υποομάδα που παράγεται από τους πίνακες

$$A = \begin{pmatrix} \omega & 0 \\ 0 & \omega^2 \end{pmatrix} \text{ και } B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

όπου $\omega = e^{2\pi i/3}$ είναι μια πρωταρχική κυβική ρίζα τής μονάδας. Να δειχθεί ότι η G είναι μια ομάδα τάξης 12, η οποία δεν είναι ισόμορφη ούτε με την εναλλάσσουσα ομάδα $\mathbb{A}_6$ ούτε με τη διεδρική D_6.

Λύση. Η υποομάδα $H = \langle A \rangle$ που παράγεται από τον πίνακα A είναι μια κυκλική ορθόθετη υποομάδα τής $\mathrm{GL}_2(\mathbb{C})$ που έχει τάξη 3. Η υποομάδα $\mathrm{K} = \langle \mathrm{B} \rangle$ που παράγεται από τον πίνακα B είναι μια κυκλική υποομάδα τής $\mathrm{GL}_2(\mathbb{C})$ που έχει τάξη 4. Το σύνολο HK είναι υποομάδα τής $\mathrm{GL}_2(\mathbb{C})$, διότι η $H \trianglelefteq \mathrm{GL}_2(\mathbb{C})$. Προφανώς η HK περιέχεται στην υποομάδα $\langle \{A, B\} \rangle$ που παράγεται από τούς πίνακες A, B και επειδή $A, B \in HK$, συμπεραίνουμε ότι ηHK ισούται με την $\langle \{A, B\} \rangle$. Η τάξη τής HK ισούται με $[HK : 1] = \frac{[H:1][K:1]}{[H \bigcap K:1]} = \frac{3 \cdot 4}{1} = 12$.

Η HK είναι το εσωτερικό ημιευθύ γινόμενο τής H με την K. Αφού $H \cong \mathbb{Z}_3$ και $K \cong \mathbb{Z}_4$ συμπεραίνουμε ότι $HK \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_4$.

Η HK δεν είναι ισόμορφη με τη διεδρική D_6, διότι η HK έχει στοιχείο τάξης 4, ενώ η D_6 δεν έχει. Η HK δεν είναι ισόμορφη με την εναλλάσσουσα ομάδα $\mathbb{A}_6$, διότι η HK έχει στοιχείο τάξης 6, ενώ η $\mathbb{A}_6$ δεν έχει.

Α 149. Να προσδιοριστούν με ακρίβεια ισομορφίας όλες οι ομάδες $(G, \star)$ τάξης $18 = 2 \cdot 3^2$.

Λύση. Κατ' αρχάς από τη Θεωρία Sylow προκύπτει ότι το πλήθος n_3 των 3-Sylow υποομάδων τής G, ισούται με 1, αφού $n_3 \equiv 1 \bmod 3$ και $n_3 \mid 2$. Επομένως, η G διαθέτει ακριβώς μία ορθόθετη υποομάδα H τάξης 9 και μια υποομάδα K τάξης 2 και ως εκ τούτου, η G ισούται με το εσωτερικό ημιευθύ γινόμενο $G = H \rtimes K$. Άρα, η G είναι ισόμορφη με ένα εξωτερικό ημιευθύ γινόμενο $\overline{H} \rtimes_\theta \overline{K}$, όπου $\theta : \overline{K} \to \mathrm{Aut}(\overline{H})$ είναι ένας ομομορφισμός. Θα προσδιορίσουμε τον ομομορφισμό θ για όλες τις δυνατές τιμές των $\overline{H}$ και $\overline{K}$.

Αφού η $\overline{H}$ είναι μια ομάδα τάξης $9 = 3^2$, συμπεραίνουμε ότι η $\overline{H}$ είναι αβελιανή και από το Θεώρημα Ταξινόμησης των πεπερασμένων αβελιανών Ομάδων, βλ. Θεώρημα 4.2.12, συμπεραίνουμε ή ότι $\overline{H} \cong \mathbb{Z}_9$ ή ότι $\overline{H} \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

Αφού η $\overline{K}$ είναι μια ομάδα τάξης 2, συμπεραίνουμε ότι η $\overline{K}$ είναι ισόμορφη με την $\mathbb{Z}_2$.

Ως εκ τούτου, θα προσδιορίσουμε όλες τους δυνατούς ομομορφισμούς θ στις περιπτώσεις (Ι) $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_9)$ και (ΙΙ) $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3)$.

Περίπτωση (Ι): Όταν ο $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_9)$ είναι ο τετριμμένος ομομορφισμός με $\theta_{[1]_2} = \mathrm{Id}_{\mathbb{Z}_9} : \mathbb{Z}_9 \to \mathbb{Z}_9, [z]_9 \mapsto [z]_9$, τότε το εξωτερικό ημιευθύ γινόμενο $\mathbb{Z}_9 \rtimes_\theta \mathbb{Z}_2$ είναι ισόμορφο με το εξωτερικό ευθύ γινόμενο $\mathbb{Z}_9 \times \mathbb{Z}_2$ και έτσι $G \cong \mathbb{Z}_9 \times \mathbb{Z}_2$.

Όταν ο $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_9)$ δεν είναι ο τετριμμένος ομομορφισμός, τότε η τάξη τής εικόνας $\theta_{[1]_2}$ ισούται με 2. Στην ομάδα $\mathrm{Aut}(\mathbb{Z}_9) \cong \mathbb{U}_9 = \{[1]_9, [2]_9, [4]_9, [5]_9, [7]_9, [8]_9\}$, το μοναδικό στοιχείο τάξης 2 είναι ο αυτομορφισμός $\chi : \mathbb{Z}_9 \to \mathbb{Z}_9, [z]_9 \mapsto [8z]_9$. Επομένως, $\theta_{[1]_2} = \chi$ και ιδιαιτέρως $\theta_{[1]_2}([1]_9) = \chi([1]_9) = [8]_9 = [9-1]_9$.

Από το Παράδειγμα 7.2.8(β'), γνωρίζουμε ότι στην περίπτωση αυτή το ημιευθύ γινόμενο $\mathbb{Z}_9 \rtimes_\theta \mathbb{Z}_2$ είναι ισόμορφο προς τη διεδρική ομάδα D_9. Άρα, $G \cong D_9$.

Περίπτωση (ΙΙ): Όταν ο $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3)$ είναι ο τετριμμένος ομομορφισμός με $\theta_{[1]_2} = \mathrm{Id}_{\mathbb{Z}_3 \times \mathbb{Z}_3} : \mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3 \times \mathbb{Z}_3, ([z]_3, [z']_3) \mapsto ([z]_3, [z']_3)$, τότε το εξωτερικό ημιευθύ γινόμενο $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\theta \mathbb{Z}_2$ είναι ισόμορφο με το εξωτερικό ευθύ γινόμενο $(\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_2$ και έτσι $G \cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \times \mathbb{Z}_2$.

Ας δούμε τώρα τι συμβαίνει, όταν ο $\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3)$ δεν είναι τετριμμένος. Τότε βέβαια η τάξη τής εικόνας $\theta_{[1]_2} := \sigma$ ισούται με 2 και έτσι ισχύει ότι $\sigma \neq \mathrm{Id}_{\mathbb{Z}_3}$ και $\sigma^2 = \mathrm{Id}_{\mathbb{Z}_3}$. Παρατηρώντας ότι οι ενδομορφισμοί τής αβελιανής ομάδας $\mathbb{Z}_3 \times \mathbb{Z}_3$ συμπίπτουν με τους γραμμικούς ενδομορφισμούς τού $\mathbb{Z}_3$-διανυσματικού χώρου $\mathbb{Z}_3 \times \mathbb{Z}_3$, θεωρούμε τον σ ως γραμμικό αυτομορφισμό και διαπιστώνουμε ότι ο $f(\sigma)$ είναι ο μηδενικός ενδομορφισμός, όπου $f(x)$ είναι το πολυώνυμο $x^2 - 1 \in \mathbb{Z}_3[x]$, αφού $\sigma^2 = \mathrm{Id}_{\mathbb{Z}_3}$. Επομένως το ελάχιστο πολυώνυμο $m_\sigma(x)$ τού σ είναι ή το $x-1$ ή το $x+1$ ή το x^2-1. Όμως αφού η τάξη τού σ δεν ισούται με 1, δηλαδή ο σ δεν είναι η ταυτοτική απεικόνιση, συμπεραίνουμε ότι $m_\sigma(x) \neq x - 1$. Όταν $m_\sigma(x) = x + 1$, τότε ο σ ισούται με $-\mathrm{Id}_{\mathbb{Z}_3 \times \mathbb{Z}_3}$. Όταν $m_\sigma(x) = x^2 - 1$, τότε ο σ έχει δύο διαφορετικές μη μηδενικές ιδιοτιμές, οι οποίες είναι ακριβώς τα δύο μη μηδενικά στοιχεία $[1]_3$ και $[2]_3$ τού $\mathbb{Z}_3$, άρα ο σ είναι διαγωνοποιήσιμος και μπορούμε χωρίς περιορισμό τής γενικότητας[4] να δεχθούμε ότι $\sigma(([1]_3,[0]_3)) = [1]_3([1]_3,[0]_3) = ([1]_3,[0]_3)$ και $\sigma(([0]_3,[1]_3)) = [2]_3([0]_3,[1]_3) = ([0]_3,[2]_3)$.

Κατ' αυτόν τον τρόπο διαπιστώνουμε ότι υπάρχουν ακριβώς δύο μη τετριμμένοι ομομορφισμοί από την $\mathbb{Z}_2$ στην $\mathbb{Z}_3 \times \mathbb{Z}_3$:

$$\theta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3) \text{ με } \theta_{[1]_2} : \begin{aligned}[t] &\mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3 \times \mathbb{Z}_3 \\ &([z]_3,[z']_3) \mapsto (-[z]_3,-[z']_3)\end{aligned}$$

και

$$\overline{\theta} : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3 \times \mathbb{Z}_3) \text{ με } \overline{\theta}_{[1]_2} : \begin{aligned}[t] &\mathbb{Z}_3 \times \mathbb{Z}_3 \to \mathbb{Z}_3 \times \mathbb{Z}_3 \\ &([z]_3,[z']_3) \mapsto ([z]_3,-[z']_3)\end{aligned}$$

Έτσι προκύπτει ή ότι $G \cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_\theta \mathbb{Z}_2$ ή ότι $G \cong (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes_{\overline{\theta}} \mathbb{Z}_2$.

Οι δύο αυτές ομάδες δεν είναι ισόμορφες, διότι το κέντρο τής πρώτης είναι τετριμμένο, ενώ το κέντρο τής δεύτερης δεν είναι (*άσκηση για τον αναγνώστη*).

Προτεινόμενες Ασκήσεις

ΠΑ 151. Να κατασκευαστεί ένα εξωτερικό ημιευθύ γινόμενο που να είναι μια μη αβελιανή ομάδα τάξης 6.

ΠΑ 152. Για ποιές τιμές τού $n \geq 3$, ισχύει ότι $\mathrm{Aut}(D_n) \cong D_n$, όπου $(D_n, \circ)$ είναι η διεδρική ομάδα των ισομετριών τού κανονικού n-γώνου;

ΠΑ 153. Έστω $(V, \star)$ η ομάδα των τεσσάρων στοιχείων και $\mathrm{Aut}(V)$ η ομάδα των αυτομορφισμών της. Θεωρούμε την ταυτοτική απεικόνιση $\iota : \mathrm{Aut}(V) \to \mathrm{Aut}(V)$ και σχηματίζουμε το εξωτερικό ημιευθύ γινόμενο $V \rtimes_\iota \mathrm{Aut}(V)$. Να δειχθεί ότι $V \rtimes_\iota \mathrm{Aut}(V) \cong S_4$.

ΠΑ 154. Έστω η κυκλική ομάδα $(\mathbb{Z}_n, +), n \geq 3$ και $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{U}_n$ η ομάδα των αυτομορφισμών της. Θεωρούμε τον ισομορφισμό

$$\begin{aligned} \chi : &\mathbb{U}_n \to \mathrm{Aut}(\mathbb{Z}_n), \\ &[s]_n \mapsto \chi_{[s_n]} : \mathbb{Z}_n \to \mathbb{Z}_n, [z]_n \mapsto \chi_{[s_n]}([z]_n) := [sz]_n \end{aligned}$$

και σχηματίζουμε το εξωτερικό ημιευθύ γινόμενο $\mathbb{Z}_n \rtimes_\chi \mathbb{U}_n$.
Να δειχθεί ότι η ομάδα $\mathbb{Z}_n \rtimes_\chi \mathbb{U}_n$ είναι επιλύσιμη, αλλά δεν είναι μηδενοδύναμη.

ΠΑ 155. Να προσδιοριστούν με ακρίβεια ισομορφίας όλες οι ομάδες τάξης 12.
(Υπόδειξη: Πρόταση 3.2.3 και ημιευθύ γινόμενο.)

ΠΑ 156. Να προσδιοριστούν με ακρίβεια ισομορφίας όλες οι ομάδες τάξης 20.

[4]λόγω ομοιότητας

Παράρτημα

Μια συνοπτική ιστορία τής ταξινόμησης των απλών πεπερασμένων ομάδων, βλ. [35]

1832	Ο Galois εισαγάγει την έννοια «ορθόθετη υποομάδα» και προσδιορίζει τις απλές ομάδες $\mathbb{A}_n$, $n \geq 5$ και $\mathrm{PSL}_2(\mathbb{F}_p)$, $p \geq 5$.
1854	Ο Cayley ορίζει τις αφηρημένες ομάδες.
1861	Ο Mathieu περιγράφει τις πρώτες δύο Mathieu ομάδες M_{11}, M_{12}, τις πρώτες σποραδικές απλές ομάδες και ανακοινώνει την ύπαρξη τής M_{24}.
1870	Ο Jordan απαριθμεί ορισμένες απλές ομάδες: την εναλλάσσουσα και τις ειδικές γραμμικές προβολικές. Τονίζει τη σημασία των απλών ομάδων.
1872	Ο Sylow αποδεικνύει τα Θεωρήματα Sylow.
1873	Ο Mathieu παρουσιάζει τις Mathieu ομάδες M_{22}, M_{23}, M_{24}.
1892	Ο Otto Hölder αποδεικνύει ότι η τάξη οποιασδήποτε μη αβελιανής απλής ομάδας πρέπει να είναι γινόμενο τουλάχιστον τεσσάρων πρώτων αριθμών και προτείνει την ταξινόμηση των πεπερασμένων απλών ομάδων.
1893	Ο Cole ταξινομεί όλες τις απλές ομάδες με τάξη ≤ 660.
1896	Οι Frobenius και Burnside αρχίζουν τη μελέτη τής θεωρίας χαρακτήρων για τις πεπερασμένες ομάδες.
1899	Ο Burnside ταξινομεί τις απλές ομάδες των οποίων ο κεντροποιητής οποιασδήποτε ενέλιξης είναι μια μη τετριμμένη στοιχειώδης αβελιανή 2–ομάδα.
1901	Ο Frobenius αποδεικνύει ότι μια Frobenius ομάδα διαθέτει έναν Frobenius πυρήνα, και ως εκ τούτου δεν είναι απλή.
1901	Ο Dickson ορίζει τις κλασικές ομάδες υπεράνω πεπερασμένων σωμάτων, και τις ασυνήθιστες ομάδες τύπου G_2 υπεράνω σωμάτων περιττής χαρακτηριστικής.
1901	Ο Dickson ορίζει τις ασυνήθιστες πεπερασμένες απλές ομάδες τύπου E_6.
1904	Ο Burnside χρησιμοποιώντας τη θεωρία χαρακτήρων αποδεικνύει το Θεώρημα Burnside: Η τάξη οποιασδήποτε πεπερασμένης, μη αβελιανής απλής ομάδας οφείλει να διαιρείται από τουλάχιστον τρεις διαφορετικούς πρώτους.
1905	Ο Dickson ορίζει τις απλές ομάδες τύπου G_2 υπεράνω σωμάτων χαρακτηριστικής 2.
1911	Ο Burnside εικάζει ότι οποιαδήποτε πεπερασμένη, μη αβελιανή απλή ομάδα έχει άρτια τάξη.
1928	Ο Hall αποδεικνύει την ύπαρξη των Hall υποομάδων των επιλύσιμων ομάδων.
1933	Ο Hall αρχίζει τη μελέτη του για τις p–ομάδες.

1935	Ο Brauer αρχίζει τη μελέτη των μοδιακών χαρακτήρων.
1936	Ο Zassenhaus ταξινομεί τις πεπερασμένες αυστηρώς 3-μεταβατικές μετατακτικές ομάδες.
1938	Ο Fitting εισάγει την έννοια τής Fitting υποομάδας και αποδεικνύει το Θεώρημα Fitting ότι η Fitting υποομάδα μιας επιλύσιμης ομάδας περιέχει τον κεντροποιητή της.
1942	Ο Brauer περιγράφει τους μοδιακούς χαρακτήρες μιας ομάδας η τάξη τής οποίας ισούται με pn, όπου p πρώτος και n φυσικός με ΜΚΔ$(p, n) = 1$.
1954	Ο Brauer ταξινομεί τις απλές ομάδες που διαθέτουν την $\mathrm{GL}_2(\mathbb{F}_q)$ ως κεντροποιητή μιας ενέλιξης.
1955	Το Θεώρημα Brauer–Fowler συνεπάγει ότι το πλήθος των απλών πεπερασμένων ομάδων με δοθέντα κεντροποιητή μιας ενέλιξης είναι πεπερασμένο, υποδεικνύοντας μια μέθοδο ταξινόμησης με τη βοήθεια κεντροποιητών ενελίξεων.
1955	Ο Chevalley ορίζει τις Chevalley ομάδες, ιδιαιτέρως παρουσιάζει τις εξαιρετικές απλές ομάδες των τύπων F_4, E_7 και E_8.
1956	Το Θεώρημα των Hall–Higman.
1957	Ο Suzuki αποδεικνύει ότι όλες οι πεπερασμένες απλές CA ομάδες περιττής τάξης είναι κυκλικές.
1958	Το Θεώρημα Brauer–Suzuki–Wall χαρακτηρίζει τις προβολικές ειδικές γραμμικές ομάδες βαθμίδας 1 και ταξινομεί τις απλές CA ομάδες.
1959	Ο Steinberg ορίζει τις ομάδες Steinberg, που δίνουν κάποιες νέες πεπερασμένες απλές ομάδες μεταξύ των οποίων τις $3D_4$ και $2E_6$ (οι τελευταίες προσδιορίστηκαν επίσης και από τον Jacques Tits περίπου την ίδια εποχή).
1959	Το Θεώρημα Brauer–Suzuki που αναφέρεται σε ομάδες με γενικευμένες 2–Sylow τετρανιακές υποομάδες αποδεικνύει ιδιαιτέρως ότι καμιά από αυτές δεν είναι απλή.
1960	Ο Thompson αποδεικνύει ότι μια ομάδα με έναν αυτομορφισμό πρώτης τάξης και ελεύθερο από σταθερά σημεία, είναι μηδενοδύναμη.
1960	Οι Feit, Hall και Thompson αποδεικνύουν ότι όλες οι πεπερασμένες απλές CN ομάδες περιττής τάξης είναι κυκλικές.
1960	Ο Suzuki εισαγάγει τις ομάδες Suzuki των τύπων 2B2.
1961	Ο Ree εισαγάγει τις ομάδες Ree των τύπων 2F4 και 2G2.
1963	Οι Feit και Thompson αποδεικνύουν το θεώρημα περιττής τάξης.
1964	Ο Tits εισαγάγει τα BN ζεύγη για τις ομάδες τύπου Lie και ορίζει την Tits ομάδα.
1965	Το Θεώρημα Gorenstein–Walter ταξινομεί τις ομάδες που διαθέτουν μια διεδρική 2-Sylow υποομάδα.
1966	Ο Glauberman αποδεικνύει το $Z^{\star}$-Θεώρημα.
1966	Ο Janko εισαγάγει την Janko-ομάδα J1, την πρώτη νέα σποραδική ομάδα μετά από έναν αιώνα.
1968	Ο Glauberman αποδεικνύει το ZJ-Θεώρημα.
1968	Οι Higman και Sims εισαγάγουν τη Higman-Sims ομάδα.
1968	Ο Conway εισαγάγει τις Conway ομάδες.
1969	Το Θεώρημα Walter ταξινομεί τις ομάδες με αβελιανές 2-Sylow υποομάδες.
1969	Εισαγωγή τής σποραδικής Suzuki ομάδας , τής Janko ομάδας J2, τής Janko ομάδας J3, τής McLaughlin ομάδας και τής Held ομάδας.
1969	Στηριγμένος σε ιδέες τού Thompson ο Gorenstein εισαγάγει τους ενδεικτικούς συναρτητές.
1970	Ο Bender εισαγάγει τη γενικευμένη Fitting υποομάδα.

1970	Το Θεώρημα Alperin–Brauer–Gorenstein ταξινομεί τις ομάδες με ημιδιεδρικές ή στεφανιαίες 2-Sylow υποομάδες ολοκληρώνοντας την ταξινόμηση των απλών ομάδων με 2-βαθμίδα το πολύ 2.
1971	Ο Fischer εισαγάγει τις τρεις Fischer ομάδες.
1971	Ο Thompson ταξινομεί τα τετραγωνικά ζεύγη.
1971	Ο Bender ταξινομεί ομάδα με ισχυρά εμφυτευμένη υποομάδα.
1972	Ο Gorenstein προτείνει ένα πρόγραμμα 16 βημάτων για την ταξινόμηση των απλών ομάδων. Η διαδικασία τής τελικής ταξινόμησης είναι αρκετά κοντά στην πρότασή του.
1972	Ο Lyons εισαγάγει τη Lyons ομάδα.
1973	Ο Rudvalis εισαγάγει τη Rudvalis ομάδα.
1973	Ο Fischer ανακαλύπτει την «baby monster» ομάδα (αδημοσίευτο), με τη βοήθεια τής οποίας οι Fischer και Griess ανακαλύπτουν τη «monster» ομάδα, η οποία εν συνεχεία οδηγεί τον Thompson στην Thompson σποραδική ομάδα και τον Norton στη Harada-Norton ομάδα (η οποία ανακαλύφθηκε με διαφορετικό τρόπο και από τον Harada).
1974	Ο Thompson ταξινομεί τις N-ομάδες, πρόκειται για ομάδες που όλες τους οι τοπικές υποομάδες είναι επιλύσιμες.
1974	Το Θεώρημα Gorenstein–Harada ταξινομεί τις απλές ομάδες με τμηματική 2-βαθμίδα το πολύ 4 διαμερίζοντας τις υπόλοιπες απλές ομάδες σε δύο τύπους.
1974	Ο Tits αποδεικνύει ότι οι ομάδες με BN-ζεύγη βαθμίδας το πολύ 3 είναι ομάδες τύπου Lie.
1974	Ο Aschbacher ταξινομεί τις ομάδες με έναν 2-γνησίως παραγόμενο πυρήνα.
1975	Οι Gorenstein και Walter αποδεικνύουν το L-ισόρροπο θεώρημα.
1976	Ο Glauberman αποδεικνύει το θεώρημα ενδεικτικού συναρτητή.
1976	Ο Aschbacher αποδεικνύει το θεώρημα συνιστώσας, δείχνοντας ότι οι ομάδες περιττού τύπου που ικανοποιούν ορισμένες συνθήκες διαθέτουν μία συνιστώσα σε στάνταρ μορφή. Οι ομάδες με μια συνιστώσα στάνταρ μορφής είχαν ταξινομηθεί σε μια μεγάλη συλλογή άρθρων από διαφορετικούς συγγραφείς.
1976	Ο O'Nan εισαγάγει την O'Nan ομάδα.
1976	Ο Janko εισαγάγει τη Janko ομάδα J4, την τελευταία σποραδική ομάδα που ανακαλύφθηκε.
1977	Ο Aschbacher χαρακτηρίζει τις ομάδες Lie τύπου περιττής χαρακτηριστικής στο κλασικό θεώρημά του τής ενέλιξης. Κατόπιν αυτού τού θεωρήματος, που κατά κάποιο τρόπο αναφέρεται σε «σχεδόν όλες» τις απλές ομάδες, υπήρχε γενικώς η αίσθηση ότι η ολοκλήρωση τής ταξινόμησης ήταν πολύ κοντά.
1978	Ο Timmesfeld αποδεικνύει το υπερεξειδικευμένο O2 θεώρημά του, διασπώντας την ταξινόμηση των GF(2)-τύπου ομάδων σε πολλά μικρότερα προβλήματα.
1978	Ο Aschbacher ταξινομεί τις λεπτές πεπερασμένες ομάδες, που ως επί το πλείστον είναι ομάδες βαθμίδας 1 Lie-τύπου υπεράνω σωμάτων χαρακτηριστικής 2.
1981	Ο Bombieri εφαρμόζοντας τη θεωρία εξάλειψης συμπληρώνει το έργο τού Thompson για τον χαρακτηρισμό των ομάδων Ree, το οποίο αποτελεί ένα από τα δυσκολότερα βήματα τής ταξινόμησης.
1982	Ο McBride αποδεικνύει το θεώρημα ενδεικτικού συναρτητή για όλες τις πεπερασμένες ομάδες.
1982	Ο Grees κατασκευάζει εξ υπαρχής τη «monster» ομάδα.
1983	Το θεώρημα των Gilman–Griess ταξινομεί τις ομάδες χαρακτηριστικού 2-τύπου και βαθμίδας τουλάχιστον 4 με στάνταρ συνιστώσες, που είναι μία από τις τρεις περιπτώσεις τού θεωρήματος τριχοτομίας.
1983	Ο Aschbacher αποδεικνύει ότι δεν υπάρχει πεπερασμένη ομάδα, η οποία να ικανοποιεί την περίπτωση τής μοναδικότητας, που είναι μία από τις τρεις περιπτώσεις τού θεωρήματος τριχοτομίας για ομάδες χαρακτηριστικού 2-τύπου.

1983	Οι Gorenstein και Lyons αποδεικνύουν το θεώρημα τριχοτομίας για ομάδες χαρακτηριστικού 2-τύπου και βαθμίδας τουλάχιστον 4, ενώ ο Aschbacher το αποδεικνύει για την περίπτωση τής βαθμίδας 3. Κατ' αυτόν τον τρόπο οι συγκεκριμένες ομάδες διαχωρίζονται σε τρεις υποπεριπτώσεις: τις ομάδες που ικανοποιούν την περίπτωση τής μοναδικότητας, τις ομάδες GF(2)-τύπου και τις ομάδες με μια στάνταρ συνιστώσα.
1983	Ο Gorenstein ανακοινώνει την ολοκλήρωση τής ταξινόμησης, κάπως πρόωρα αφού η απόδειξη τής ημιλεπτής περίπτωσης δεν ήταν ακόμα ολοκληρωμένη.
1994	Οι Gorenstein, Lyons και Solomon ξεκινούν τη δημοσίευση μιας αναθεωρημένης ταξινόμησης.
2004	Οι Aschbacher και Smith δημοσιεύουν το έργο τους για τις ημιλεπτές ομάδες (οι οποίες ως επί το πλείστον είναι ομάδες Lie-τύπου βαθμίδας το πολύ 2 υπεράνω σωμάτων χαρακτηριστικής 2) συμπληρώνοντας έτσι το τελευταίο κενό τής ταξινόμησης που ήταν γνωστό εκείνο τον καιρό.
2008	Οι Harada και Solomon συμπληρώνουν ένα μικρό κενό τής ταξινόμησης περιγράφοντας εκείνες τις ομάδες με στάνταρ συνιστώσα, οι οποίες αποτελούν κάλυμμα τής Mathieu ομάδας M22.
2012	Οι Georges Gonthier και οι συνεργάτες του ανακοινώνουν μια εκδοχή τού θεωρήματος Feit-Thompson, η απόδειξη τής οποίας έχει ελεγχθεί με ηλεκτρονικό υπολογιστή με τη βοήθεια τού λογισμικού Coq.

Βιβλιογραφία

[1] Σ. Ανδρεαδάκης. *Μαθήματα επί τής Θεωρίας Ομάδων*, 1976.

[2] Σ. Ανδρεαδάκης. *Ασκήσεις στη Θεωρία Ομάδων*, 1981.

[3] Δ. Βάρσος, Δ. Δεριζιώτης, Μ. Μαλιάκας, Στ.. Παπασταυρίδης, Ευ. Ράπτης, Ολ. Ταλέλλη. *Μια Εισαγωγή στην Άλγεβρα*. Εκδόσεις Σοφία, 2003.

[4] B. Baumslag and B. Chandler. *Schaum's outline of theory and problems of group theory*. Schaum's outline series. McGraw-Hill, New York, 1968.

[5] D. Bayer. *Notes on semidirect products*. http://www.math.columbia.edu/~bayer/S09/ModernAlgebra/semidirect.pdf.

[6] J. A. Beachy and W. D. Blair. *Abstract algebra*. Waveland Press, Long Grove, Ill., 3rd ed edition, 2006.

[7] T. S. Blyth and E. F. Robertson. *Algebra through practice: a collection of problems in algebra with solutions, Book 5, Groups*. Cambridge University Press, Cambridge, 1985.

[8] S. Bosch. *Algebra*. Springer-Lehrbuch. Springer, Berlin, 8. (διορθωμένη έκδοση) 2013.

[9] K. Conrad. *Expository Papers*. http://www.math.uconn.edu/~kconrad/blurbs/

[10] J. D. Dixon. *Problems in group theory*. A Blaisdell book in pure and applied mathematics. Blaisdell Pub. Co, Waltham, Mass., 1967.

[11] D. S. Dummit and R. M. Foote. *Abstract algebra*. Wiley, Hoboken, NJ, 3rd ed edition, 2004.

[12] C. Fuchs and G. Wüstholz. *Übungen zur Algebra: Aufgaben - Lösungen - Probeklausuren*. Springer Spektrum. Springer, Wiesbaden, 2014.

[13] Θ. Θεοχάρη-Αποστολίδη. *Εισαγωγή στη Θεωρία Ομάδων*. Υπηρεσία Δημοσιευμάτων Α.Π.Θ., Θεσσαλονίκη, 1991.

[14] J. A. Gallian. *Contemporary abstract Algebra*. Brooks/Cole Cengage Learning, Boston, MA, 8th ed edition, 2012.

[15] C. F. Gardiner. *A first course in group theory.* Universitext. Springer-Verlag, New York, 1980.

[16] D. Guichard. *When is* $\mathbb{U}(n)$ *cyclic? An algebraic approach*. Mathematics Magazine, 72(2):139–142, 1999.

[17] I. N. Herstein. *Topics in algebra.* Xerox College Pub., Lexington, Mass., 2d ed edition, 1975.

[18] M. Holz. *Repetitorium Algebra*. Binomi, 2010. Μετάφραση: Ν. Μαρμαρίδης. Εκδόσεις Συμμετρία, 2015.

[19] J. F. Humphreys. *A course in group theory.* Oxford University Press, Oxford, 1996.

[20] T. W. Hungerford. *Abstract algebra: an introduction.* Springer (Graduate Texts in Mathematics 73), 1974.

[21] D. Jungnickel. *On the uniqueness of the cyclic group of order n.* American Mathematical Monthly, 99 (6) (1992), 545 - 547.

[22] C. Karpfinger and K. Meyberg. *Algebra: Gruppen - Ringe - Körper.* Spektrum Akademischer Verlag, Heidelberg, 2009.

[23] C. Karpfinger. *Arbeitsbuch Algebra.* Springer Spektrum, Berlin Heidelberg, 2015.

[24] E. S. Lyapin, A. I. Aĭzenshtat, and M. M. Lesokhin. *Exercises in group theory.* Plenum Press, New York, 1972.

[25] P. Morandi. *Semidirect products.* http://sierra.nmsu.edu/morandi/notes/semidirect.pdf.

[26] Δ. Νταής. *Θεωρία Ομάδων*. Πανεπιστήμιο Κρήτης, Ηράκλειο 2015.

[27] D. J. S. Robinson. *A course in the theory of groups*, volume 80. Springer-Verlag, New York, 2nd ed edition, 1996.

[28] S. Roman. *Fundamentals of group theory: an advanced approach.* Birkhäuser, New York, 2012.

[29] J. S. Rose. *A course on group theory.* Cambridge University Press, Cambridge, 1978.

[30] H. E. Rose. *A course on finite groups.* Universitext. Springer, London, 2009.

[31] J. J. Rotman. *Advanced modern algebra*, volume v. 114 of *Graduate studies in mathematics.* American Mathematical Society, Providence, R.I., 2nd ed edition, 2010.

[32] J. J. Rotman. *An introduction to the theory of groups*, volume 148. Springer-Verlag, New York, 4th ed edition, 1995.

[33] G. Smith and O. Tabachnikova. *Topics in group theory.* Springer, London, 2000.

[34] J. Sullivan. *Classification of fininite abelian groups.* http://torus.math.uiuc.edu/jms/m317/handouts/finabel.pdf

[35] Wikipedia. *Classification of finite simple groups.* https://en.wikipedia.org/wiki/Classification_of_finite_simple_groups.

Ευρετήριο Εννοιών και Ονομάτων

n–οστή
    ρίζα μονάδας, 58
p–Sylow υποομάδα, 198
p–ομάδα, 197
p–ομάδες στοιχειώδεις
    αβελιανές, 225

Burnside Θεώρημα, 172

Cauchy Θεώρημα, 184
Cayley Θεώρημα, 177

Euler
    φ–συνάρτηση, 27

Klein
    ομάδα, 25

Sylow Θεώρημα, 198

Wilson Θεώρημα, 44

Zassenhaus Λήμμα, 246

Εξίσωση Κλάσεων, 188
Θεώρημα Burnside, 172
Θεώρημα Cauchy, 184
Θεώρημα Cayley, 177
Θεώρημα Sylow, 198
Θεώρημα Wilson, 44
Θεώρημα ταξινόμησης
    πεπερασμένων
        αβελιανών ομάδων, 237
Λήμμα Zassenhaus, 246
Λήμμα Πεταλούδας, 246
Πεταλούδας Λήμμα, 246
άνω κεντρική σειρά, 266
άπειρη ομάδα, 11
άρτια
    μετάταξη, 158
αβελιανή ομάδα, 11
ακέραια
    δύναμη, 27
ακέραιο
    πολλαπλάσιο, 27
αλγεβρική δομή, 1
αμφιρριπτική απεικόνιση, 2
αντιμετάθεση, 147
ανώτερα κέντρα, 266
ανώτερη παράγωγη υποομάδα, 263
απεικόνιση
    αμφιρριπτική, 2
    ενριπτική, 2
    επιρριπτική, 2
απλή ομάδα, 213
απόσταση διανυσμάτων, 15
αυτομορφισμός
    εξωτερικός, 128
    εσωτερικός, 128
    ομάδας, 123
αυτομορφισμών
    ομάδα, 124
γενική γραμμική ομάδα, 14
γινόμενο
    εξωτερικό ευθύ, 224
    εξωτερικό ημιευθύ, 291
    εσωτερικό ευθύ, 226

εσωτερικό ημιευθύ, 288
ευθύ, 41, 100
γνήσια υποομάδα, 52
δείκτης υποομάδας, 72
διαμέριση συνόλου, 67
διαμέριση φυσικού, 235
διανυσμάτων
απόσταση, 15
διεδρική ομάδα, 18
διμελής πράξη, 1
δομή
αλγεβρική, 1
δράση
φυσιολογική, 180
δράση μεταβατική, 170
δράση ομάδας, 164
δράση πιστή, 168
δράση συζυγίας, 185
δύναμη ακέραια, 27
εκλέπτυνση ορθόθετη, 244
εκλέπτυνση υποορθόθετη , 244
εναλλάσσουσα ομάδα, 160
ενδομορφισμός
ομάδας, 123
ενριπτική απεικόνιση, 2
εξωτερικό γινόμενο
ευθύ, 224
ημιευθύ, 291
εξωτερικός
αυτομορφισμός, 128
επέκταση ομάδων, 288
επιλύσιμη ομάδα, 259
επιμορφισμός, 115
επιρριπτική απεικόνιση, 2
εσωτερικό
γινόμενο ευθύ, 226
γινόμενο ημιευθύ, 288
εσωτερικός
αυτομορφισμός, 128
ευθύ
εξωτερικό γινόμενο, 224
εσωτερικό γινόμενο, 226
ευθύ γινόμενο, 41, 100
ημιευθύ
εξωτερικό γινόμενο, 291
εσωτερικό γινόμενο, 288
ισομετρία, 15
ισομορφισμός, 115
ισόμορφες
ορθόθετες σειρές, 245
υποορθόθετες σειρές, 245
ισόμορφη
ομάδα, 118
κέντρο ομάδας, 63, 185
κανονική υποομάδα, 101
κατοπτρισμός, 17
κεντροποιητής, 187
κεντροποιητής στοιχείου, 65
κεντροποιητής υποομάδας, 65
κεντροποιούσα υποομάδα, 65
κλάση
διπλή πλευρική, 78
πλευρική, 104
κλάση ισοτιμίας, 12
κλάση συζυγίας, 185
κυκλική ομάδα, 81
κυκλική υποομάδα, 53, 59
κυρίαρχη σειρά, 249
κυρίαρχοι παράγοντες, 249
μήκος
κυρίαρχης σειράς, 250
συνθετικής σειράς, 250
μεγιστοτική υποομάδα, 270
μετάθεση, 2, 30
μετάταξη, 2, 30
άρτια, 158
περιττή, 158
μετάταξης
πρόσημο, 158
μεταβατική δράση, 170
μεταθέτης στοιχείων, 262
μεταθέτρια υποομάδα, 262
μεταθετική ομάδα, 11
μεταθετική πράξη, 3
μετατακτική αναπαράσταση, 168
μηδενοδύναμη ομάδα, 268
μονομορφισμός, 114
ομάδα, 10

  n-οστών ριζών μονάδας, 57
  Klein, 25
  άπειρη, 11
  αβελιανή, 11
  απλή, 213
  αυτομορφισμών, 124
  γενική γραμμική, 14
  διεδρική, 18
  εναλλάσσουσα, 160
  επιλύσιμη, 259
  ισόμορφη, 118
  κυκλική, 81
  μεταθετική, 11
  μηδενοδύναμη, 268
    κλάσης r, 268
  πεπερασμένη, 11
  πεπερασμένως παραγόμενη, 59
  συμμετρίας, 2, 29
    κανονικού n-γώνου, 18
  τεσσάρων στοιχείων, 25
  χαρακτηριστικώς απλή, 252
ομάδα πηλίκο, 104
ομάδας
  αυτομορφισμός, 123
  δράση, 164
  ενδομορφισμός, 123
  κέντρο, 63, 185
  παράγωγη σειρά, 263
  τάξη, 11
ομάδας κυκλικής
  γεννήτορας, 81
ομάδων
  εξωτερικό ευθύ γινόμενο, 224
  επέκταση, 288
  ομομορφισμός, 112
ομομορφισμού
  πυρήνας, 116
ομομορφισμός
  τετριμμένος, 115
ομομορφισμός ομάδων, 112
ορθοθετοποιητής υποομάδας, 63, 188
ορθοθετοποιούσα υποομάδα, 63
ορθόθετες
  ισόμορφες σειρές, 245
ορθόθετη εκλέπτυνση, 244
ορθόθετη σειρά, 243
  με επαναλήψεις, 243
ορθόθετη υποομάδα, 101
ορθόθετης σειράς
  παράγοντες, 243

παράγοντες
  κυρίαρχοι, 249
  ορθόθετης σειράς, 243
  συνθετικοί, 249
  υποορθόθετης σειράς, 243
παράγωγη ανώτερη υποομάδα, 263
παράγωγη σειρά ομάδας, 263
παράγωγη υποομάδα, 262
παραγόμενη υποομάδα, 59
πεπερασμένη ομάδα, 11
πεπερασμένων αβελιανών ομάδων
  θεώρημα ταξινόμησης, 237
πεπερασμένως παραγόμενη
  ομάδα, 59
  υποομάδα, 59
περιττή
  μετάταξη, 158
πηλικοομάδα, 104
πίνακας Young, 235
πίνακας πράξης, 4
πιστή δράση, 168
πλευρική κλάση, 104
  αριστερή, 69
  δεξιά, 69
πολλαπλάσιο ακέραιο, 27
πράξη
  διμελής, 1
  μεταθετική, 3
  προσεταιριστική, 2
προβολή
  φυσική, 113
προσεταιριστική πράξη, 2
πρωταρχικές ρίζες, 219
πρόσημο
  μετάταξης, 158
πυρήνας δράσης, 168
πυρήνας ομομορφισμού, 116

ρίζα
    πρωταρχική τής μονάδας, 81
ρίζα μονάδας
    n–οστή, 58
ρίζες πρωταρχικές, 219
σειρά
    κυρίαρχη, 249
    ομάδας παράγωγη, 263
    ορθόθετη , 243
        με επαναλήψεις, 243
    συνθετική, 249
    υποορθόθετη , 243
        με επαναλήψεις, 243
σειράς
    κυρίαρχης
        μήκος, 250
    συνθετικής
        μήκος, 250
σειράς όροι, 243
σταθεροποιητής, 170
σταθερό στοιχείο, 170
στερεά κίνηση, 15
στοιχεία συζυγή, 185
στοιχείο
    σταθερό, 170
στοιχείου
    κεντροποιητής, 65
στοιχείου τάξη, 82
στοιχειώδεις αβελιανές
    p–ομάδες, 225
στροφή, 17
συζυγή στοιχεία, 185
συζυγής υποομάδα, 65
συμμετρική
    ομάδα, 29
συμμετρική ομάδα, 2
συνθετική σειρά, 249
συνθετικοί παράγοντες, 249
συνόλου
    διαμέριση, 67
σύνολο
    γεννητόρων, 59
τάξη ομάδας, 11
τάξη στοιχείου, 82
τετριμμένη υποομάδα, 52
τετριμμένος ομομορφισμός, 115
τροχιά, 169
υποομάδα, 52
    Sylow, 198
    γνήσια, 52
    κανονική, 101
    κεντροποιούσα, 65
    κυκλική, 53, 59
    μεγιστοτική, 270
    μεταθέτρια, 262
    ορθοθετοποιούσα, 63, 188
    ορθόθετη, 101
    παράγωγη, 262
        ανώτερη, 263
    παραγόμενη, 59
    πεπερασμένως παραγόμενη, 59
    συζυγής, 65
    τετριμμένη, 52
    χαρακτηριστική, 210
υποομάδας
    δείκτης, 72
    κεντροποιητής, 65
    ορθοθετοποιητής, 63, 188
υποομάδων
    εσωτερικό ευθύ γινόμενο, 226
υποορθόθετες
    ισόμορφες σειρές, 245
υποορθόθετη εκλέπτυνση, 244
υποορθόθετη σειρά, 243
    με επαναλήψεις, 243
υποορθόθετης σειράς
    παράγοντες, 243
φ–συνάρτηση
    Euler, 27
φυσική
    προβολή, 113
φυσιολογική δράση, 180
χαρακτηριστική υποομάδα, 210
χαρακτηριστικώς απλή
    ομάδα, 252
όροι σειράς, 243