Εισαγωγή στην Θεωρία Ομάδων

Πάρης Πάμφιλος
Πανεπιστήμιο Κρήτης

Δεκέμβριος 2002

Περιεχόμενα

Κεφάλαιο 1

Ομάδες, Ομομορφισμοί

1.1 Προέλευση της έννοιας

Στην ανάπτυξη των Μαθηματικών κεντρικό ρόλο παίζουν οι *αριθμοί* και οι **πράξεις** τους. Ιστορικά, ξεκινάμε από τους Φυσικούς αριθμούς, περνάμε στους ακέραιους, τους ρητούς , τους πραγματικούς, τους μιγαδικούς. Σε κάθε ένα απ΄ αυτά τα σύνολα έχουμε *πράξεις* που συνδιάζουν δύο αριθμούς και δίνουν σαν αποτέλεσμα έναν τρίτον αριθμό, το *αποτέλεσμα της πράξης*:

$$3+5=8, \quad (3/7)*(2/5)=6/35, \quad (3+5i)+(4+3i)=7+8i.$$

Το αποτέλεσμα είναι πάλι αριθμός του ιδίου *είδους* με τους δύο παράγοντες της πράξης. Στην γραμμική άλγεβρα μαθαίνομε γιά τους πίνακες και τις πράξεις μεταξύ πινάκων:

$$A+B=C, \quad A*B=D$$

(μπορούμε να θεωρήσουμε τους πίνακες σαν ένα είδος γενίκευσης των αριθμών) . Προσθέτομε *ομοειδείς* πίνακες, δηλαδή πίνακες που έχουν το ίδιο πλήθος γραμμών και το ίδιο πλήθος στηλών. Πολλαπλασιάζομε πίνακες A, B όταν οι στήλες του A είναι όσες οι γραμμές του B. Εδώ συναντάμε γιά πρώτη φορά μη-μεταθετικό πολλαπλασιασμό: $A*B \neq B*A$ (εφ΄ όσον ορίζεται το δεύτερο γινόμενο). Εύκολα βρίσκουμε τέτοια μη μεταθετικά γινόμενα π.χ.

$$\begin{pmatrix} 0 & 2 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Το κοινό στοιχείο σε όλα τα παραδείγματα είναι ότι: έχουμε *συστήματα αριθμών* και πράξεις που σε δύο *αριθμούς* α, β αντιστοιχούν έναν τρίτο, που γενικά θα μπορούσαμε να συμβολίσουμε με α*β. Το * δηλώνει άλλοτε την γνωστή μας πρόσθεση και άλλοτε τον πολλαπλασιασμό. Η ένοια της ομάδος τυποποιεί αυτό το φαινόμενο: **ενός συστήματος αριθμών και μιάς πράξης μεταξύ τους** .

1.2 Ορισμός Ομάδος

Ομάδα λέγεται ένα Σύνολο G μη κενό εφοδιασμένο με μια **πράξη** * η οποία σε κάθε ζεύγος $x, y \in G$, αντιστοιχεί ένα τρίτο στοιχείο $x*y \in G$, που ικανοποιεί τα εξής αξιώματα:

(1) Υπάρχει $e \in G : x*e = e*x = x$, γιά κάθε $x \in G$. (ύπαρξη μοναδιαίου)

(2) Ισχύει $(x*y)*z = x*(y*z)$, γιά κάθε x, y, $z \in G$. (προσεταιριστική ιδιότητα)

(3) Γιά κάθε $x \in G$ υπάρχει $x' \in G : x*x' = x'*x = e$. (ύπαρξη αντιστρόφου)

Το e λέγεται **μοναδιαίο** στοιχείο ή απλά **μονάδα**. Το x' λέγεται **αντίστροφο** του x και συμβολίζεται με x^{-1}.
Η ομάδα λέγεται **μεταθετική** ή **Αβελιανή** όταν επι πλέον ικανοποιεί το αξίωμα: $x * y = y * x, \forall\, x, y \in G$.
Αν η ομάδα είναι πεπερασμένη τότε ο ακέραιος $|G| = n > 1$ λέγεται **τάξη** της ομάδας.

Παρατηρήσεις
Από τα ίδια τα αξιώματα προκύπτουν ορισμένες άμεσες συνέπειες.
(1) Κάθε ομάδα περιέχει ένα τουλάχιστον ειδικό στοιχείο, την μονάδα της e.
(2) Υπάρχει μία και μόνον μονάδα. Δηλαδή δεν υπάρχει άλλο στοιχείο e' που να ικανοποιεί επίσης την (1) του ορισμού.
(3) Υπάρχει ένα και μόνο αντίστροφο x' γιά κάθε $x \in G$. Δηλαδή δεν υπάρχει άλλο στοιχείο x'' που να ικανοποιεί επίσης την (3) του ορισμού.
(4) Συμβολίζουμε πολλαπλά γινόμενα n παραγόντων $x*x*...*x = x^n$ και $x^{-1}*...*x^{-1} = x^{-n}$.

1.3 Παραδείγματα

Χρησιμοποιώ ζεύγη $(G, *)$ γιά να δηλώσω την ομάδα και την πράξη της. Όπου είναι σαφές από τα συμφραζόμενα ποιά είναι η πράξη, γράφω απλά G.
(1) Η **τετριμμένη** ομάδα που έχει το ένα και μόνο στοιχείο e που κάθε ομάδα υποχρεούται να έχει. $G = \{e\}$.
(2) Η μοναδική ομάδα με δύο στοιχεία $G = \{-1, +1\}$. Γιά την οποία αναγκαστικά θα ισχύει $(-1) * (-1) = +1$.
(3) Οι ακέραιοι $\mathbb{Z}$ με πράξη την πρόσθεση $(* = +)$ είναι ομάδα με $e = 0$, $x^{-1} = -x$.
(4) Αντιπαράδειγμα: $G = \mathbb{Z}_* = \{x \in \mathbb{Z} : x \neq 0\}$ με πράξη τον πολλαπλασιασμό ακεραίων. Υπάρχει μονάδα $e = 1, 1 * m = m = m * 1$, $\forall m \in G$, αλλά $1/m$ (το αντίστροφο) για $m \neq 0, \pm 1$ δεν περιέχεται στο σύνολο G.
(5) $G = \mathbb{Q}_* = \{x \in \mathbb{Q} : x \neq 0\}$ με πράξη τον πολλαπλασιασμό ρητών αριθμών . Την ομάδα αυτή ονομάζουμε **πολλαπλασιαστική** ομάδα των ρητών αριθμών.
(6) $G = \mathbb{R}_* = \{x \in \mathbb{R} : x \neq 0\}$ με πράξη τον πολλαπλασιασμό πραγματικών αριθμών . Την ομάδα αυτή ονομάζουμε **πολλαπλασιαστική** ομάδα των πραγματικών αριθμών.
(7) $G = \mathbb{Q}_+ = \{x \in \mathbb{Q} : x > 0\}$ με πράξη τον πολλαπλασιασμό ρητών αριθμών . Την ομάδα αυτή ονομάζουμε **πολλαπλασιαστική** ομάδα των θετικών ρητών αριθμών.
(8) $G = \mathbb{R}_* = \{x \in \mathbb{R} : x > 0\}$ με πράξη τον πολλαπλασιασμό πραγματικών αριθμών . Την ομάδα αυτή ονομάζουμε **πολλαπλασιαστική** ομάδα των θετικών πραγματικών αριθμών.
(9) $G = \mathbb{C}_* = \{x \in \mathbb{C} : x \neq 0\}$ με πράξη τον πολλαπλασιασμό μιγαδικών αριθμών . Την ομάδα αυτή ονομάζουμε **πολλαπλασιαστική** ομάδα των μιγαδικών αριθμών.
(10) $G = S^1 = \{x \in \mathbb{C} : |x| = 1\}$ με πράξη τον πολλαπλασιασμό μιγαδικών αριθμών . Την ομάδα αυτή ονομάζουμε **πολλαπλασιαστική** ομάδα των μοναδιαίων μιγαδικών αριθμών.
(11) $G = \mathbb{R}^n$, τον n-διάστατο πραγματικό διανυσματικό χώρο με πράξη την πρόσθεση διανυσμάτων.
(12) $G = \mathbb{R}^{nm}$, τον nm-διάστατο πραγματικό διανυσματικό χώρο των πινάκων $m \times n$ διαστάσεων με πράξη την πρόσθεση πινάκων.
(13) $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ = σύνολο των δυνατών υπολοίπων ως προς την διαίρεση με τον ακέραιο $n > 1$. Ως πράξη ορίζουμε την $x \dot{+} y =$ υπόλοιπο της διαίρεσης του $x+y$ ως προς

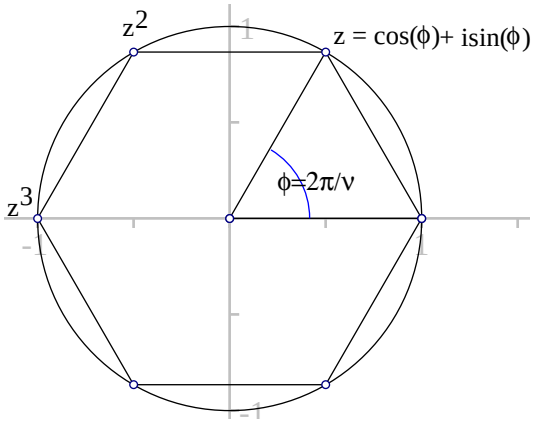
n. Εύκολα διαπιστώνουμε ότι το 0 είναι το μοναδιαίο αυτής της πράξης και ο αντίστροφος του x δίδεται από το $n - x$.

(14) $G = GL(n, \mathbb{R})$ = σύνολο των πραγματικών $n \times n$ πινάκων A με ορίζουσα $|A| \neq 0$, με πράξη τον πολλαπλασιασμό πινάκων.

(15) $G = GL(n, \mathbb{R})_+$ = σύνολο των πραγματικών $n \times n$ πινάκων A με ορίζουσα $|A| > 0$, με πράξη τον πολλαπλασιασμό πινάκων.

(16) $G = SL(n, \mathbb{R})$ = σύνολο των πραγματικών $n \times n$ πινάκων A με ορίζουσα $|A| = 1$, με πράξη τον πολλαπλασιασμό πινάκων.

(17) Γενικώτερα, ορίζονται ομάδες πινάκων με ορίζουσα 1, για τα διάφορα συστήματα αριθμών: $SL(n, \mathbb{Z})$ = σύνολο των $n \times n$ πινάκων A ακεραίων με ορίζουσα $|A| = 1$, με πράξη τον πολλαπλασιασμό πινάκων. Ανάλογα ορίζονται οι ομάδες $SL(n, \mathbb{Q})$, και $SL(n, \mathbb{C})$.



Σχήμα 1.1: Η ομάδα των $n-$στών ριζών της μονάδος

(18) $G = P_n = \{z \in \mathbb{C} : z^n = 1\}$, το σύνολο των $n-$στών μιγαδικών ριζών της μονάδος με πράξη τον πολλαπλασιασμό μιγαδικών αριθμών. Το P_n αποτελείται από τις κορυφές ενός κανονικού πολυγώνου με κέντρο το μηδέν και μία κορυφή στο $(1, 0)$, συνεπώς εγγεγραμμένου στον μοναδιαίο κύκλο του μιγαδικού επιπέδου .

ΠΡΟΒΛΗΜΑΤΑ 1.3

Πρόβλημα 1.3.1 *Δείξε ότι γιά κάθε ομάδα και δύο οποιαδήποτε στοιχεία αυτής ισχύει:*

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

Εξέτασε πότε ισχύει $a^{-1} * b^{-1} = b^{-1} * a^{-1}$, γιά κάθε ζεύγος στοιχείων.

Πρόβλημα 1.3.2 *Δείξε ότι μια ομάδα που ισχύει $x^2 = e$ γιά κάθε στοιχείο της, είναι αβελιανή.*

Πρόβλημα 1.3.3 *Δείξε ότι σε κάθε ομάδα υπάρχει ένα και μόνο μοναδιαίο.*

Πρόβλημα 1.3.4 *Δείξε ότι σε κάθε ομάδα $\forall\, x \in G$ υπάρχει ένα και μόνο αντίστροφο $x^{-1} \in G$.*

Πρόβλημα 1.3.5 *Δείξε ότι η απεικόνιση $z \mapsto z^{-1}$, της ομάδας G στον εαυτό της είναι 1 - 1 και επί.*

Πρόβλημα 1.3.6 *Εστω η ομάδα $G = \{t_1, ..., t_k\}$. Δείξε ότι γιά κάθε $t \in G$ ισχύει $G = \{t * t_1, ..., t * t_k\}$.*

Πρόβλημα 1.3.7 *Εστω η πεπερασμένη ομάδα $|G| = n$. Δείξε ότι γιά κάθε $g \in G$ υπάρχει ελάχιστο $k \in \mathbb{N}$ τέτοιο ώστε το σύνολο των δυνάμεων του g να είναι $G = \{g, g^2, ..., g^k = e\}$. Δείξε ότι $k \leq n$.*

Πρόβλημα 1.3.8 *Δείξε ότι εάν η ομάδα G έχει άρτια τάξη , τότε περιέχει ένα στοιχείο $z : z^2 = e$.*

Πρόβλημα 1.3.9 *Δείξε ότι σε κάθε ομάδα και γιά κάθε ακέραιο n, ισχύει $(xyx^{-1})^n = xy^n x^{-1}$.*

Πρόβλημα 1.3.10 *Δείξε ότι το σύνολο των πινάκων $\{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n = 0, \pm 1, \pm 2, ...\}$ είναι ομάδα ως προς τον πολλαπλασιασμό πινάκων . Δείξε το ίδιο και γιά τα επόμενα σύνολα πινάκων:*
α) Πραγματικοί τετραγωνικοί αντιστρέψιμοι πίνακες $n \times n$ διαστάσεων που έχουν όλα τα κάτω της κυρίας διαγωνίου στοιχεία τους μηδέν.
β) Πίνακες όπως στο α), που έχουν όμως μονάδες στην κύρια διαγώνιο.
γ) Το σύνολο πινάκων $D_4 = \{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \pm \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\}$.

Πρόβλημα 1.3.11 *Δείξε ότι σε κάθε ομάδα αν το στοιχείο $x \in G$, μετατίθεται με τα y^m και y^n όπου $(m, n) = 1$, τότε μετατίθεται και με το ίδιο το y.*

Πρόβλημα 1.3.12 *Δείξε ότι σε κάθε ομάδα, αν για τα στοιχεία $x, y \in G$, ισχύει $x^m = y^m$ και $x^n = y^n$ όπου $(m, n) = 1$, τότε ισχύει και $x = y$.*

1.4 Ευθύ γινόμενο ομάδων

Δοθέντων δύο ομάδων $(G_1, *_1), (G_2, *_2)$ το καρτεσιανό γινόμενο $G_1 \times G_2$ δέχεται την δομή ομάδος μέσω της πράξης $*$ που ορίζεται με τον εξής τρόπο:

$$(x, y) * (x', y') := (x *_1 x', y *_2 y').$$

Εύκολα διαπιστώνουμε ότι το ζεύγος $(G_1 \times G_2, *)$ ικανοποιεί τα αξιώματα της ομάδας. Το μοναδιαίο της είναι το $e = (e_1, e_2)$ το αντίστροφο του (x, y) είναι το (x^{-1}, y^{-1}).
Η νέα αυτή ομάδα συμβολίζεται συχνά με $G_1 \times G_2$ και αναφέρεται ως **Ευθύ γινόμενο των ομάδων** G_1, G_2.

Προφανώς ο προηγούμενος ορισμός επεκτείνεται και σε περισσότερες ομάδες: $G = G_1, ..., G_2$ και ορίζεται το ευθύ γινόμενο περισσοτέρων ομάδων:

$$G_1 \times G_2 \times G_3 ... \times G_n.$$

Με τον τρόπο αυτό, χρησιμοποιώντας δοθείσες ομάδες $G_1, ..., G_n$, μπορούμε να κατασκευάσουμε ομάδες κάπως πιό σύνθετες. Ιδιαίτερα ενδιαφέρον είναι το αντίστροφο ερώτημα που δημιουργήται αμέσως: *Δοθήσης ομάδος G, πότε υπάρχουν άλλες $G_1, ..., G_n$ έτσι ώστε $G = G_1 \times ... \times G_n$;*

Περισσότερα γιά το γινόμενο ομάδων θα δούμε στο κεφάλαιο 5. Όταν οι ομάδες είναι αβελιανές, γράφουμε $G_1 \oplus G_2 \oplus G_3 ... \oplus G_n$ και λέμε ότι τούτο είναι το **ευθύ άθροισμα** των ομάδων.

Παραδείγματα
$\mathbb{Z}^n, \mathbb{Q}^n, \mathbb{R}^n, \mathbb{C}^n$ είναι όλα παραδείγματα προσθετικών ομάδων, όπου η πρόσθεση ορίζεται συντεταγμένη προς συντεταγμένη, όπως στο ευθύ άθροισμα. Παρόμοια παραδείγματα αποτελούν τα σύνολα $n \times m$-διαστάτων πινάκων με πράξη την πρόσθεση πινάκων : $\mathbb{Z}^{nm}$, $\mathbb{Q}^{nm}$, $\mathbb{R}^{nm}$, $\mathbb{C}^{nm}$. Αναφέρω ακόμη τα παραδείγματα των πολλαπλασιαστικών ομάδων ${\mathbb{Q}_*}^n, {\mathbb{R}_*}^n, {\mathbb{C}_*}^n$ καθώς και των επίσης πολλαπλασιαστικών ${\mathbb{Q}_+}^n, {\mathbb{R}_+}^n, {\mathbb{C}_+}^n$.

Παρατήρηση
Ορισμένες φορές η δυνατότητα μιάς ομάδας να αναλυθεί σε ευθύ άθροισμα είναι κάπως κρυμμένη και δεν φαίνεται άμεσα. Π.χ. θα δούμε παρακάτω ότι (με μιά γενικώτερη αντίληψη για την έννοια της ισότητας) η ομάδα $(\mathbb{Z}_p, \dot{+})$, για ορισμένα p, μπορεί να θεωρηθεί η ίδια με μιά ομάδα της μορφής

$$G = \mathbb{Z}_{n_1} \oplus ... \oplus \mathbb{Z}_{n_k}.$$

ΠΡΟΒΛΗΜΑΤΑ 1.4

Πρόβλημα 1.4.1 *Δίδονται φυσικοί αριθμοί $k > 1, n > 1$. Κατασκεύασε ομάδα G αβελιανή τάξης k^n και για κάθε στοιχείο της οποίας να ισχύει $x^k = e$.*

Πρόβλημα 1.4.2 *Βρες μιά πράξη στο σύνολο $S^1 \times ... \times S^1$ (κ φορές), που το κάνει ομάδα.*

1.5 Ορισμός ομομορφισμού

Μιά απεικόνιση $F : (G_1, *_1) \longrightarrow (G_2, *_2)$ μεταξύ δύο ομάδων λέγεται **ομομορφισμός** ομάδων όταν ικανοποιεί την σχέση

$$F(x *_1 y) = F(x) *_2 F(y), \forall\, x, y \in G_1.$$

Παρατηρήσεις
Θα έλεγε κανείς ότι η προηγούμενη ιδιότητα εκφράζει το ότι η F *σέβεται* τις πράξεις : η εικόνα του γινομένου είναι το γινόμενο των εικόνων. Το κλασσικό παράδειγμα είναι αυτό της γραμμικής απεικόνισης

$$F : \mathbb{R}^m \longrightarrow \mathbb{R}^n,$$

όπου έχουμε $F(\vec{x} + \vec{y}) = F(\vec{x}) + F(\vec{y}), \forall\, \vec{x}, \vec{y} \in \mathbb{R}^m$. Η F περιγράφεται με έναν $m \times n$-διάστατο πίνακα A και χρησιμοποιεί τον πολλαπλασιασμό πίνακα με διάνυσμα: π.χ. γιά $m = n = 2$ μιά γραμμική απεικόνιση περιγράφεται από έναν πίνακα $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ και η απεικόνιση $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = F(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix})$ αντιστοιχεί:

$$\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} ax_1 + bx_2 \\ cx_1 + dx_2 \end{pmatrix}.$$

Η χαρακτηριστική ιδιότητα του ομομορφισμού ισοδυναμεί, σ' αυτήν την περίπτωση, με την ιδιότητα του πολλαπλασιασμού πίνακα επί διάνυσμα:

$$A(\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} x_1' \\ x_2' \end{pmatrix}) = A\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + A\begin{pmatrix} x_1' \\ x_2' \end{pmatrix}.$$

Παρατηρήσεις
(1) Το μοναδιαίο e_1 απεικονίζεται στο μοναδιαίο e_2. Πράγματι $F(e_1) = F(e_1 *_1 e_1) = F(e_1) *_2 F(e_1)$. Απλοποιώντας μεταξύ της πρώτου και τελευταίου μέλους των εξισώσεων, βρίσκουμε $F(e_1) = e_2$.
(2) Το αντίστροφο στοιχείου x^{-1} απεικονίζεται στο αντίστροφο της εικόνας $F(x^{-1}) = (F(x))^{-1}$. Πράγματι από την προηγούμενη παρατήρηση $e_2 = F(e_1) = F(x *_1 x^{-1}) = F(x) *_2 F(x^{-1})$. Και το συμπέρασμα προκύπτει από το μονοσήμαντο του αντιστρόφου.
(3) Η σύνθεση δύο ομομορφισμών $F : G_1 \to G_2\,, H : G_2 \to G_3$ είναι ομομορφισμός $H \circ F : G_1 \to G_3 : H \circ F(x *_1 y) = H(F(x) *_2 F(y)) = H(F(x)) *_3 H(F(y))$.

1.6 Παραδείγματα Ομομορφισμών

(1) Ο **ταυτοτικός** ομομορφισμός, δηλαδή η ταυτοτική απεικόνιση μιάς ομάδας στον εαυτό της.
(2) Ο **τετριμμένος** ομομορφισμός, δηλαδή η απεικόνιση μιάς ομάδας στον εαυτό της, γιά την οποία $F(x) = e$, $,\forall\, x \in G$.
(3) Η **εκθετική**, η γνωστή μας από τον απειροστικό λογισμό $F(x) = e^x$. Είναι ομομορφισμός της προσθετικής ομάδος $(\mathbb{R}, +)$ στην πολλαπλασιαστική $(\mathbb{R}_+\,, *)$. Η ιδιότητα του ομομορφισμού συμπίπτει με την γνωστή μας

$$e^{x+y} = e^x e^y.$$

(4) Ο **λογάριθμος**, η γνωστή μας από τον απειροστικό λογισμό $F(x) = log(x)$. Είναι ομομορφισμός της πολλαπλασιαστικής ομάδος $(\mathbb{R}_+\,, *)$ στην προσθετική $(\mathbb{R}, +)$. Η ιδιότητα του ομομορφισμού συμπίπτει με την γνωστή μας

$$logx * y = log(x) + log(y).$$

(5) Η απεικόνιση $F(A) = |A|$, που σε κάθε πραγματικό $n \times n$ πίνακα αντιστοιχεί την ορίζουσά του είναι ένας ομομορφισμός $F : GL(n,(R)) \longrightarrow \mathbb{R}_*$. Τούτο στηρίζεται στην ιδιότητα της ορίζουσας για γινόμενο πινάκων: $|AB| = |A||B|$.
(6) Η απεικόνιση $F(A) = sign(|A|)$, που σε κάθε πραγματικό $n \times n$ πίνακα αντιστοιχεί το πρόσημο της ορίζουσάς του, είναι ένας ομομορφισμός $F : GL(n, \mathbb{R}) \longrightarrow (\{-1, 1\}, *)$. Τούτο στηρίζεται πάλι στην ιδίοτητα: $|AB| = |A||B|$.
(7) Παίρνοντας το υπόλοιπο ενός ακεραίου $x \in \mathbb{Z}$ ως προς έναν σταθερό φυσικό $n > 1$, $F(x) = \overline{x} =$ υπόλοιπο διαίρεσης του x ως προς n, διαπιστώνουμε εύκολα ότι ορίζεται ομομορφισμός $F : \mathbb{Z} \longrightarrow \mathbb{Z}_n$.
(8) Η απεικόνιση της πολλαπλασιαστικής ομάδας $F : \mathbb{C}_* \longrightarrow S^1$, στον μοναδιαίο κύκλο, που σε κάθε μιγαδικό $z \in \mathbb{C}_*$ αντιστοιχεί το $F(z) = \frac{z}{|z|}$, βλέπουμε πάλι εύκολα ότι είναι ομομορφισμός.
(9) Για σταθερό φυσικό $n > 1$, η απεικόνιση $F : \mathbb{Z}_n \longrightarrow P_n$ που στο $k \in \{0, ..., n-1\}$ αντιστοιχεί το $z = e^{\frac{2\pi k}{n}} = cos(\frac{2\pi k}{n}) + isin(\frac{2\pi k}{n})$, είναι ομομορφισμός.

1.7 Μονο-, Επι-, Ισο-μορφισμοί

Ενας ομομορφισμός $F : (G_1 , *_1) \longrightarrow (G_2 , *_2)$ μεταξύ δύο ομάδων λέγεται **μονομορφισμός** ομάδων όταν είναι 1-1. Δηλ

$$F(x) = F(y) \Longrightarrow x = y.$$

Ο ομομορφισμός λέγεται **επιμορφισμός** ομάδων όταν είναι επί. Δηλ

$$\forall\, y \in G_2 , \exists\, x \in G_1 : F(x) = y.$$

Τέλος λέγεται **ισομορφισμός** όταν είναι ταυτόχρονα 1-1 και επί.

Παρατηρήσεις
(1) Αν η $F : (G_1 , *_1) \longrightarrow (G_2 , *_2)$ είναι ισομορφισμός, τότε ορίζεται αμέσως η $F^{-1} : (G_2 , *_2) \longrightarrow (G_1 , *_1)$ και είναι επίσης ισομορφισμός. Πράγματι, γιά να δείξουμε ότι $F^{-1}(x *_2 y) = F^{-1}(x) *_2 F^{-1}(y)$ αρκεί να δείξουμε ότι $F(F^{-1}(x *_2 y)) = F(F^{-1}(x) *_2 F^{-1}(y))$, που είναι προφανές.
(2) Δύο ομάδες $(G_1 , *_1), (G_2 , *_2)$ λέγονται ισόμορφες, όταν υπάρχει κάποιος ισομορφισμός που απεικονίζει την μιά στην άλλη.
(3) Δύο ισόμορφες ομάδες $(G_1 , *_1), (G_2 , *_2)$ έχουν τα ίδια δομικά χαρακτηριστικά και θεωρούνται κατά κάποιο τρόπο ταυτόσημες. Ένα από τα βασικά προβλήματα της θεωρίας ομάδων είναι η **ταξινόμηση** των ομάδων, δηλαδή η ανεύρεση όλων των δυνατών μη-ισομόρφων μεταξύ τους ομάδων. Το παράδειγμα (9) παραπάνω είναι παράδειγμα ισομορφισμού μεταξύ των ομάδων $(\mathbb{Z}_n , \dot{+})$, $(P_n , *)$. Οι ομάδες $\mathbb{Z}_m , \mathbb{Z}_n$ είναι εν τούτοις μη ισόμορφες γιά $m \neq n$, για τον απλούστατο λόγο, ότι έχουν διαφορετικό πλήθος στοιχείων.

Πρόταση 1.7.1 *Κάθε ομάδα G με $n = 1, 2, 3$ στοιχεία είναι ισόμορφη προς την $\{0\} , \mathbb{Z}_2 , \mathbb{Z}_3$ αντίστοιχα.*

Πράγματι, γιά $n = 1$ η πρόταση είναι προφανής. Γιά $n = 2$ η G θα είναι της μορφής $\{e, x\}$ με $x \neq e$. Πρέπει τότε $x^2 = e$, διότι αν ήταν $x^2 = x$, τότε πολ/ζοντας με x^{-1}, θα πέρναμε $x = e$. Αν λοιπόν αντιστοιχίσουμε $e \mapsto 0$ και $x \mapsto 1$, έχουμε έναν ισομορφισμό της G με την $\mathbb{Z}_2$. Ας έλθουμε τώρα στην περίπτωση που η G έχει τρία στοιχεία, άρα είναι της μορφής $\{e, x, y\}$. Πρέπει τότε να ισχύει $x * y = e$. Πράγματι, αν δεν ίσχυε τότε θα έπρεπε $x * y = x$ ή $x * y = y$ και στις δύο περίπτώσεις πολλάπλασιάζοντας με το στοιχείο x^{-1}, y^{-1} αντίστοιχα, πέρνουμε $x = e, y = e$ αντίστοιχα. Πράγμα άτοπο. Χρησιμοποιώντας αυτό συμεραίνουμε ότι $x^2 = y$. Πράγματι αν δεν ίσχυε αυτό, τότε θα έπρεπε $x^2 = x$ ή $x^2 = e$. Η πρώτη δυνατότητα απορρίπτεται διότι τότε θα είχαμε $x = e$. Η δεύτερη απορρίπτεται επίσης διότι πολ/ζοντας την $x^2 = e$ με y έχουμε $y * x^2 = y \Leftrightarrow (y * x) * x = y \Leftrightarrow x = y$ επίσης άτοπο. Συνολικά λοιπόν τα στοιχεία της ομάδας γράφονται $\{e, x, x^2\}$ και η αντιστοίχιση $e \mapsto 0, x \mapsto 1, x^2 \mapsto 2$ ορίζει έναν ισομορφισμό της G στην $\mathbb{Z}_3$.

Πρόταση 1.7.2 *Οι ομάδες $\mathbb{Z}_4$ και $\mathbb{Z}_2 \times \mathbb{Z}_2$ δεν είναι ισόμορφες.*

Κατ' αρχήν και οι δύο ομάδες έχουν 4 στοιχεία και θα μπορούσε κανείς να τις υποθέσει ισόμορφες. Όμως φαίνεται αμέσως ότι δεν είναι ισόμορφες από τον πολλαπλασιασμό μεταξύ των στοιχείων τους. Η $\mathbb{Z}_4$ γράφεται προφανώς στην μορφή $\{e, x, x^2, x^3\}$ με $x^4 = e$. Η $\mathbb{Z}_2 \times \mathbb{Z}_2$ από την άλλη μεριά έχει στοιχεία $e' = (0, 0), x' = (1, 0), y' = (0, 1), z' = (1, 1)$ και βλέπουμε αμέσως ότι ισχύει $t^2 = e'$ γιά κάθε στοιχείο της. Αν λοιπόν υπήρχε ισομορφισμός F μεταξύ

των δύο ομάδων τότε $F(x) \neq e'$ και έστω $F(x) = x'$. Τότε όμως $F(x^2) = F(x)F(x) = x'^2 = e'$, άρα $x^2 = e$, άτοπο.
Παρατήρηση Αργότερα θα δούμε ότι αυτές είναι , ουσιαστικά, οι μόνες ομάδες 4 στοιχείων. Κάθε άλλη ομάδα 4 στοιχείων είναι υποχρεωτικά ισόμορφη προς μίαν εκ των δύο.

1.8 Ο πίνακας της ομάδας

Ο πίνακας μιάς πεπερασμένης ομάδας G με n στοιχεία είναι ένας $n \times n$ πίνακας που προκύπτει απο τα στοιχεία $x_1, ..., x_n$ της ομάδας, βάζοντας στην $i-$γραμμή και $j-$στήλη το γινόμενο $y = x_i * x_j$. Γιά παράδειγμα οι πίνακες της $\mathbb{Z}_4$ και $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{0' = (0,0), 1' = (1,0), 2' = (0,1), 3' = (1,1)\}$, είναι αντίστοιχα:

$$\begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \\ 2 & 3 & 0 & 1 \\ 3 & 0 & 1 & 2 \end{pmatrix} \end{array} \quad , \quad \begin{array}{c} \\ 0' \\ 1' \\ 2' \\ 3' \end{array}\!\!\begin{array}{c} \begin{array}{cccc} 0' & 1' & 2' & 3' \end{array} \\ \begin{pmatrix} 0' & 1' & 2' & 3' \\ 1' & 0' & 3' & 2' \\ 2' & 3' & 0' & 1' \\ 3' & 2' & 1' & 0' \end{pmatrix} \end{array}.$$

Παρατηρήσεις
(1) Είναι προφανές ότι για ισομορφικές ομάδες θα μπορούσαμε να αντιστοιχίσουμε τον ίδιον αριθμό σε αντίστοιχα στοιχεία, έτσι ώστε οι πίνακες των δύο ομάδων να είναι οι ίδιοι.
(2) Η πρώτη γραμμή και η πρώτη στήλη είναι αντίστοιχα οι ίδιες με τις προηγούμενες, διότι αντιστοιχούν σε πολ/μό με το μοναδιαίο.
(3) Κάθε γραμμή περιέχει κάθε στοιχείο της ομάδας ακριβώς μιά φορά.
(4) Κάθε στήλη περιέχει κάθε στοιχείο της ομάδας ακριβώς μιά φορά.
(5) Αν διατάξουμε τα στοιχεία της ομάδας σε άλλη σειρά θα προκύψει, εν γένει, διαφορετικός πίνακας.

ΠΡΟΒΛΗΜΑΤΑ 1.8

Πρόβλημα 1.8.1 *Δείξε ότι γιά κάθε αβελιανή ομάδα και φυσικό αριθμό n η απεικόνιση $p_n : G \longrightarrow G, p_n(x) = x^n$, είναι ένας ομομορφισμός ομάδων.*

Πρόβλημα 1.8.2 *Δείξε ότι μια ομάδα G είναι αβελιανή, τότε και μόνον όταν η απεικόνιση $p_2 : G \longrightarrow G, p_2(x) = x^2$, είναι ένας ομομορφισμός ομάδων.*

Πρόβλημα 1.8.3 *Δείξε ότι γιά συγκεκριμένο στοιχείο της ομάδος $x \in G$, η απεικόνιση $I_x : G \longrightarrow G, I_x(y) = xyx^{-1}$, είναι ένας ομομορφισμός ομάδων. Ο ομομορφισμός αυτός λέγεται* **εσωτερικός**. *Δείξε ότι ο ομομορφισμός αυτός είναι ισομορφισμός και βρες τον αντίστροφό του. Πότε ο ισομορφισμός αυτός συμπίπτει με την ταυτοτική απεικόνιση της ομάδος;*

Πρόβλημα 1.8.4 *Δείξε ότι γιά κάθε ομάδα G, το σύνολο των ισομορφισμών $F : G \longrightarrow G$ (επειδή ο ισομορφισμός αυτός απεικονίζει την ομάδα στον εαυτό της λέγεται* **αυτομορφισμός**) *αποτελεί ομάδα με πράξη την σύνθεση απεικονίσεων. Η ομάδα αυτή συμβολίζεται με $Aut(G)$ και λέγεται ομάδα αυτομορφισμών της G.*

Κεφάλαιο 2

Υποομάδες , Σύμπλοκα

2.1 Ορισμός Υποομάδος

Υποομάδα ομάδος G λέγεται ένα μη κενό Σύνολο H **κλειστό** ως προς την πράξη $*$ της G. Με άλλα λόγια, ένα μη-κενό υποσύνολο που ικανοποιεί τα αξιώματα:
(1) $\forall x, y \in H \Longrightarrow x * y \in H$.
(2) $\forall x \in H \Longrightarrow x^{-1} \in H$.

Παρατηρήσεις
Από τα ίδια τα αξιώματα προκύπτουν ορισμένες άμεσες συνέπειες.
(1) Κάθε υποομάδα H της G περιέχει ένα τουλάχιστον στοιχείο, το μοναδιαίο e. Πράγματι γιά κάθε $x \in H$ το (2) συνεπάγεται ότι και το x^{-1} θα περιέχεται στην G. Αρα κατά το (1) και το $e = x * x^{-1}$ θα περιέχεται στο Η.
(2) Ολες οι υποομάδες της G έχουν κοινό με την H το μοναδιαίο e. Το μονοσύνολο $\{e\}$ ικανοποιεί κατά τετριμμένο τρόπο τα αξιώματα άρα είναι υποομάδα της G. Αυτή ονομάζεται **τετριμμένη** υποομάδα της G.
(3) Αν $F \subseteq H \subseteq G$ είναι, η κάθε μιά υποομάδα της επομένης, τότε και η F είναι κατ' ευθείαν υποομάδα της G.
(4) Εύκολα διαπιστώνουμε τα αξιώματα της υποομάδας και για την τομή $H_1 \cap H_2$ δύο υποομάδων ομάδας G. Στις ασκήσεις θα δούμε ότι η τομή οσωνδήποτε υποομάδων μιάς ομάδας G είναι πάλι υποομάδα της G. Αντίστοιχη ιδιότητα ωστόσο για την ένωση δεν ισχύει.

Πρόταση 2.1.1 *Τα δύο αξιώματα παραπάνω είναι ισοδύναμα με το αξίωμα:*
(1′) $\forall x, y \in H \Longrightarrow x * y^{-1} \in H$.

Το ότι τα δύο συνεπάγονται το (1′) είναι βέβαια προφανές. Το αντίστροφο είναι πάλι εύκολο. Παίρνοντας $x = y$ στην (1), βλέπουμε ότι το $e \in G$. Παίρνοντας κατόπιν $x = e$ στην (1′), βλέπουμε ότι $\forall y, \in H \Longrightarrow y^{-1} \in H$, δηλαδή το (2). Τέλος για κάθε $x, y \in H$, σύμφωνα με τα προηγούμενα, το $y^{-1} \in H$ άρα κατά το (1′) και το $x * (y^{-1})^{-1} = x * y \in H$. Άρα το (1′) συνεπάγεται και το (2).

2.2 Παραδείγματα Υποομάδων

(1) Έστω $n > 1$ ακέραιος θετικός. Το σύνολο $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\}$ όλων των πολλαπλασίων του n είναι προφανώς υποομάδα της $(\mathbb{Z}, +)$. Μάλιστα στις ασκήσεις δείχνουμε ότι κάθε

υποομάδα του $(\mathbb{Z},+)$ έχει αυτήν την μορφή.
(2) Οι ρητοί αριθμοί, θεωρούμενοι ως προσθετική ομάδα $(\mathbb{Q},+)$, είναι υποομάδα της προσθετικής ομάδας των πραγματικών αριθμών $(\mathbb{R},+)$.
(3) Αντίστοιχα προς τα προηγούμενα ισχύουν και για τις πολλαπλασιαστικές ομάδες: $(\mathbb{Q}_*,*)$, είναι υποομάδα της $(\mathbb{R}_*,*)$ και $(\mathbb{Q}_+,*)$, είναι υποομάδα της $(\mathbb{R}_+,*)$.
(4) Αντίστοιχα προς τα προηγούμενα ισχύουν και για τις μιγαδικές πολλαπλασιαστικές ομάδες: $(S^1,*)$, είναι υποομάδα της $(\mathbb{C}_*,*)$ και οι ομάδες $(P_n,*)$, είναι υποομάδες της $(S^1,*)$.
(5) Ως προς τον πολλαπλασιασμό πινάκων έχουμε την αλυσίδα υποομάδων (κάθε μιά της επομένης της): $SL(n,\mathbb{R}) \subset GL(n,\mathbb{R})_+ \subset GL(n,\mathbb{R})$.
(6) Στον $n-$διάστατο διανυσματικό χώρο $\mathbb{R}^n$ με πράξη την πρόσθεση διανυσμάτων, ορίζονται υποομάδες μέσω γραμμικών συνδυασμών. Πράγματι αν θεωρήσουμε k διανύσματα: $\overline{v}_1,...,\overline{v}_k$ του $\mathbb{R}^n$, τότε το σύνολο όλων των γραμμικών συνδυασμών τους $Span(\overline{v}_1,...,\overline{v}_k) = \{t_1\overline{v}_1+...+t_k\overline{v}_k : t_1,...,t_k \in \mathbb{R}\}$, διαπιστώνουμε εύκολα ότι ικανοποιεί τα αξιώματα της υποομάδος. Άρα οι διανυσματικοί υπόχωροι $(Span(\overline{v}_1,...,\overline{v}_k),+)$ είναι υποομάδες του $(\mathbb{R}^n,+)$.
(7) Από τις ποιό σημαντικές υποομάδες μιάς ομάδος είναι οι **παραγόμενες από ένα στοιχείο** x της ομάδος. $< x >= \{x^n : n \in \mathbb{Z}\}$. Μία ομάδα λέγεται **κυκλική** όταν υπάρχει κάποιο στοιχείο της x έτσι ώστε $G =< x >$.

2.3 $Kern(F), Im(F)$

Δοθέντος ομομορφισμού $F : (G_1\,,*_1) \longrightarrow (G_2\,,*_2)$ μεταξύ δύο ομάδων, ορίζονται αμέσως δύο υποομάδες που σχετίζονται μ' αυτόν. Η πρώτη είναι υποομάδα της $(G_1\,,*_1)$, λέγεται **πυρήνας του ομομορφισμού** $Kern(F) = \{x \in G_1 : F(x) = e_2\}$ και περιλαμβάνει όλα τα στοιχεία που απεικονίζονται μέσω της F στο ουδέτερο στοιχείο e_2 της δεύτερης ομάδος. Η δεύτερη υποομάδα που σχετίζεται με τον ομομορφισμό είναι υποομάδα της $(G_2\,,*_2)$ και λέγεται **εικόνα του ομομορφισμού** $Im(F) = \{y \in G_2 : \exists x \in G_1 : F(x) = y\}$.

Πρόταση 2.3.1 *Για κάθε ομομορφισμό $F : (G_1\,,*_1) \longrightarrow (G_2\,,*_2)$ τα σύνολα $Kern(F) \subseteq G_1$ και $Im(F) \subset G_2$ είναι υποομάδες των αντίστοιχων ομάδων. Επίσης $Kern(F) = \{e_1\}$ τότε καί μόνον όταν ο ομομορφισμός είναι 1-1.*

Πράγματι, γιά $x,y \in Kern(F) \Rightarrow F(x *_1 y) = F(x) *_2 F(y) = e_2 *_2 e_2 = e_2$. Αυτό δείχνει ότι και το $x *_1 y \in Kern(F)$ άρα το $Kern(F)$ είναι όντως υποομάδα. Εστω τώρα ότι $F(x) = F(y)$ τότε $F(x *_1 y^{-1}) = F(x) *_2 F(y^{-1}) = F(x) *_2 (F(y))^{-1} = e_2$ δηλαδή $x *_1 y^{-1} \in Kern(F)$. Προκύπτει αμέσως η ισοδυναμία των σχέσεων που αποδεικνύει τον ισχυρισμό: $F(x) = F(y) \Leftrightarrow x *_1 y^{-1} \in Kern(F)$. Το ότι η $Im(F)$ είναι υποομάδα της G_2 είναι εξίσου εύκολο.

Παρατηρήσεις
(1) Από την γραμμική άλγεβρα γνωρίζουμε ότι ένας πίνακας πραγματικών αριθμών A $m \times n$ διαστάσεων ορίζει μιά γραμμική απεικόνιση $F_A : \mathbb{R}^n \longrightarrow \mathbb{R}^m$. Η $F_A(x) = Ax$ είναι ένας ομομορφισμός ως προς την πρόσθεση διανυσμάτων. Το ομογενές σύστημα $Ax = 0$ προσδιορίζει ακριβώς τον πυρήνα αυτού του ομομορφισμού και είναι υποομάδα του $\mathbb{R}^n$. Ο κανόνας που μαθαίνουμε στην γραμμική άλγεβρα: η λύση του $Ax = c$ είναι $x = x_0 + x_1$ όπου x_0 η γενική λύση του ομογενούς $Ax = 0$ και x_1 μιά ειδική λύση του μη ομογενούς συστήματος $Ax = c$, μεταφέρεται στους ομομορφισμούς ομάδων: Η γενική λύση της $F(x) = y$ είναι άθροισμα $x = x_0 + x_1$ όπου το $x_0 \in Kern(F)$ και $F(x_1) = y$ μιά ειδική λύση.
(2) Δοθέντος υποσυνόλου $S \subseteq G$ το σύνολο των **λέξεων** $x_1^{n_1}...x_k^{n_k}$ όπου $n_1,...,n_k \in \mathbb{Z}$

και $x_1, ..., x_k \in S$ βλέπουμε εύκολα ότι αποτελεί υποομάδα της G. Η υποομάδα αυτή λέγεται **παραγόμενη** από το S και συμβολίζεται με $< S >$. Τα x_i λέγονται **γεννήτορες της** G. Ειδική περίπτωση είναι αυτή που παράγεται από τις δυνάμεις ενός στοιχείου $< x > \subseteq G$ η λεγόμενη **κυκλική** υποομάδα παραγόμενη από το x.
(4) Αν η ομάδα έχει πεπερασμένο πλήθος γεννητόρων, τότε λέγεται **πεπερασμένα παραγόμενη** διαφορετικά λέγεται **μη-πεπερασμένα παραγόμενη**.
(5) Μιά **σχέση** μεταξύ στοιχείων ομάδος είναι μιά εξίσωση ενός ορισμένου γινομένου στοιχείων της ομάδος με το ουδέτερο e της ομάδος. Μιά σχέση $f(x_1, ..., x_k) = e$ λέγεται ότι εξαρτάται από κάποιες άλλες f_1, f_2, ..., όταν μπορεί να εκφρασθεί σαν κάποιο γινόμενο (των αριστερών μελών) αυτών των σχέσεων. Διαφορετικά λέγεται ανεξάρτητη απ' αυτές.
(6) Μιά ομάδα μπορεί να έχει γεννήτορες οι οποίοι δεν είναι ανεξάρτητοι μεταξύ τους, αλλά ικανοποιούν ορισμένες σχέσεις. Ετσι λ.χ. η ομάδα που παράγεται από δύο στοιχεία της: s, t, που ικανοποιούν τις σχέσεις: $t^p = e$, $s^q = e$, $sts^{-1}t^{-1} = e$, (και, εννοήται, καμμία άλλη ανεξάρτητη απ' τις προηγούμενες) είναι ισόμορφη με την ομάδα $\mathbb{Z}_p \times \mathbb{Z}_q$. Για μιά τέτοια ομάδα γράφουμε $G =< s, t : s^p = e, t^q = e, st = ts >$.
(7) Αν $F : G_1 \longrightarrow G_2$, είναι ομομορφισμός ομάδων, μπορούμε να δούμε αμέσως ότι γιά κάθε υποομάδα $H \subset G_1$ η εικόνα $F(H) \subset G_2$, είναι υποομάδα της G_2.
(8) Το ίδιο συμβαίνει και με τις αντίστροφες εικόνες ομομορφισμών $F : G_1 \longrightarrow G_2$. Άν $H \subset G_2$ είναι υποομάδα τότε και η αντίστροφη εικόνα της μέσω της F που ορίζεται από την $F^{-1}(H) = \{g \in G_1 : F(g) \in H\}$, θα είναι υποομάδα της G_1.

2.4 Σύμπλοκα

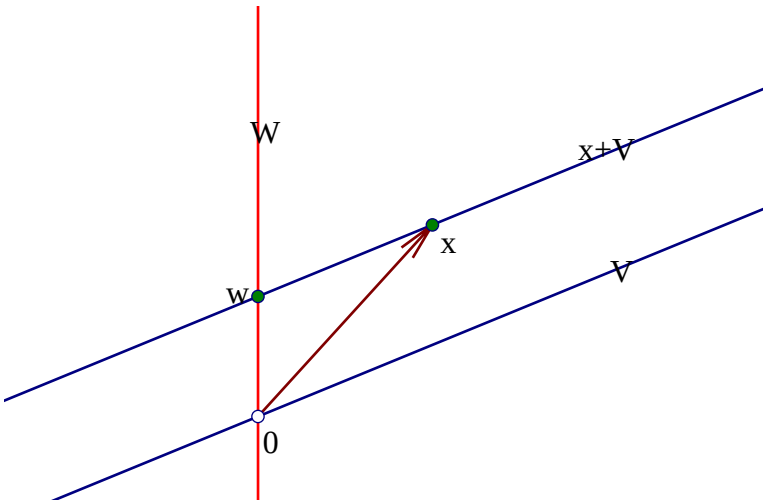
Έστω $H \subseteq G$ μιά υποομάδα της ομάδας G. Ορίζεται μιά σχέση ισοδυναμίας που διαμερίζει το G με την βοήθεια του H. Η σχέση ορίζεται ως εξής: $x \approx y \Leftrightarrow y^{-1} * x \in H$. Εύκολα βλέπουμε ότι η σχέση αυτή είναι πράγματι σχέση ισοδυναμίας, δηλαδή έχει τις ιδιότητες:
(1) $x \approx x$, $\forall x \in G$ (αυτοπαθής)
(2) $x \approx y \Rightarrow y \approx x$ (συμμετρική)
(3) $x \approx y, y \approx z \Rightarrow x \approx z$ (μεταβατική)
Τούτο σημαίνει ότι το σύνολο G διαμερίζεται σε ξένα μεταξύ τους υποσύνολα, τις κλάσεις ισοδυναμίας της σχέσης. Τις κλάσεις αυτές ονομάζουμε **σύμπλοκα** της υποομάδος.

Πρόταση 2.4.1 *Κάθε σύμπλοκο της ομάδας G ως προς την υποομάδα H γράφεται υπό μορφήν $xH = \{xh : h \in H\}$. Γιά δύο σύμπλοκα ισχύει $xH = yH$ ή $xH \cap yH = \emptyset$.*

Πράγματι, αν $xH \cap yH \neq \emptyset$, έστω $z \in xH \cap yH$. Τότε το z γράφεται με δύο τρόπους: $z = xh_1 = yh_2$ άρα $x = yh_2h_1^{-1} \in yH$. Τότε όμως και $xH \subseteq yH$. Ανάλογα δείχνουμε και την $yH \subseteq xH$.

Παρατηρήσεις
(1) Το σύνολο των συμπλόκων συμβολίζουμε με G/H. Το πλήθος των συμπλόκων συμβολίζουμε με $[G : H]$ και ονομάζουμε **δείκτη** της H στην G. Τούτο μπορεί να είναι άπειρο ή πεπερασμένο. Την απεικόνιση $p : G \longrightarrow G/H$ που σε κάθε $x \in G$ αντιστοιχεί το σύμπλοκο $p(x) = xH$, ονομάζουμε **κανονική προβολή** της ομάδος στο σύνολο πηλίκον.
(2) Ένα στοιχείο $x \in u$ ενός συμπλόκου u λέγεται **αντιπρόσωπος** του συμπλόκου. Προφανώς γιά κάθε αντιπρόσωπο $x \in u$ ισχύει $u = xH$. Συχνά μας ενδιαφέρει να προσδιορίσομε ενα σύνολο αντιπροσώπων, έναν γιά κάθε κλάση, με άλλα λόγια να περιγράψομε το σύνολο G/H των κλάσεων απεικονίζοντας το αμφιμονοσήμαντα σε ένα άλλο σύνολο. Τούτο

συμβαίνει για παράδειγμα στην επόμενη παρατήρηση.



Σχήμα 2.1: Τα σύμπλοκα ως προς υπόχωρο V του $\mathbb{R}^n$

(3) Στην περίπτωση ενός υποχώρου V του διανυσματικού χώρου $\mathbb{R}^n$, τα σύμπλοκα $x+V$ είναι υπερεπίπεδα παράλληλα του V. Αν W είναι συμπληρωματικός υπόχωρος του V, δηλαδή $V \oplus W = \mathbb{R}^n$, τότε κάθε σύμπλοκο τέμνει το W σε ένα ακριβώς σημείο $w \in (x+V) \cap W$. Το W λοιπόν είναι ένα σύνολο **αντιπροσώπων** των κλάσεων ισοδυναμίας ή συμπλόκων.

Πρόταση 2.4.2 *Κάθε υποομάδα G της πεπερασμένης ομάδος G ορίζει μιά διαμέριση της G σε $[G:H]$ υποσύνολα. Για τις τάξεις των ομάδων ισχύει $|G| = |H|[G:H]$ άρα η τάξη κάθε υποομάδος διαιρεί την τάξη της ομάδος.*

Πράγματι, υπάρχουν $[G:H]$ το πλήθος ξένα μεταξύ τους σύμπλοκα κάθε ένα από τα οποία περιέχει $|H|$ το πλήθος στοιχεία. Οι υπόλοιποι ισχυρισμοί προκύπτουν άμεσα. Άμεσα επίσης προκύπτουν και τα επόμενα πορίσματα.

Πρόταση 2.4.3 *Μιά πεπερασμένη ομάδα με πλήθος στοιχείων p πρώτο αριθμό, δεν περιέχει γνήσιες υποομάδες (διαφορετικές της $\{e\}$ και της ίδιας της G).*

Πρόταση 2.4.4 *Η τάξη $|< x >|$ ενός στοιχείου πεπερασμένης ομάδος $x \in G$ διαιρεί την τάξη της ομάδος $|G| = n$. Ισχύει πάντοτε $x^n = e$.*

Πρόταση 2.4.5 *Κάθε ομάδα G αποτελούμενη από 4 στοιχεία είναι ισόμορφη είτε προς την $\mathbb{Z}_2 \times \mathbb{Z}_2$ είτε προς την $\mathbb{Z}_4$.*

Πράγματι, αν η ομάδα έχει στοιχείο τάξης 4, $x \in G : x, x^2, x^3, x^4 = e$ είναι διαφορετικά μεταξύ τους άρα $G =< x >$ και η απεικόνιση $x^k \mapsto k$ δίνει έναν ομομορφισμό με την κυκλική ομάδα $\mathbb{Z}_4$.
Αν η ομάδα δεν έχει στοιχείο τάξης 4, τότε θα πρέπει κάθε στοιχείο της $x \neq e$ να έχει τάξη 2, δηλαδή να ικανοποιεί $x^2 = e$. Κατά το 1.3.2 είναι αβελιανή. Εστω ότι $x, y, z \in G$ είναι τα στοιχεία τα διαφορετικά του e. Διαπιστώνουμε αμέσως τα εξής:
α) $xy = z$
β) Οι $G_1 = \{e, x\}$, $G_2 = \{e, y\}$ είναι υποομάδες της G ισόμορφες της $\mathbb{Z}_2$.
γ) Η απεικόνιση F η οποία αντιστοιχεί: $\{(0,0) \mapsto e, (1,0) \mapsto x, (0,1) \mapsto y, (1,1) \mapsto z\}$ είναι ισομορφισμός $F : \mathbb{Z}_2 \times \mathbb{Z}_2 \longrightarrow G$.

Πρόταση 2.4.6 *Αν $H \subseteq G$ και $L \subseteq H$ είναι αντίστοιχα υποομάδες των G και H τότε η L είναι υποομάδα της G και ισχύει $[G : L] = [G : H][H : L]$.*

Πράγματι, το ότι η L είναι υποομάδα της G είναι προφανές. Για τον δεύτερο ισχυρισμό διαλέγουμε αντιπροσώπους $x_i, i \in G/H$ από τα $[G : H]$ το πλήθος σύμπλοκα της G ως προς H και αντιπροσώπους $y_j, j \in H/L$ από $[H : L]$ σύμπλοκα της H ως προς L. Τότε $G = \cup x_i H$ είναι η διαμέριση της G σε σύμπλοκα. Αντίστοιχα και $H = \cup y_j L$ είναι η διαμέριση της H σε σύμπλοκα. Αρα $G = \cup x_i y_j L$ είναι η διαμέριση της G σε σύμπλοκα ως προς την υποομάδα της L. Τούτο δείχνει ότι τα γινόμενα $x_i y_j$ είναι αντιπρόσωποι των συμπλόκων της G ως προς L και αποδεικνύει την ισότητα.

Πρόταση 2.4.7 *Για δύο πεπερασμένες υποομάδες H, H' ομάδος G αντιστοίχων τάξεων k, k' το σύνολο $HH' = \{hh' : h \in H, h' \in H'\}$ έχει kk'/m στοιχεία, όπου $m = |H \cap H'|$.*

Πράγματι η ένωση των συμπλόκων $xH', x \in H$ ισούται με το HH'. Τα σύμπλοκα όμως αυτά είναι διαφορετικά $xH' \neq yH'$ όταν το $y^{-1}x \notin H'$. Αρα το πλήθος των διαφορετικών συμπλόκων είναι $[H : H \cap H'] = k/m$. Η ισότητα προκύπτει από το ότι κάθε σύμπλοκο xH' έχει k' στοιχεία.

2.5 Κανονικές υποομάδες

Μιά υποομάδα $H \subseteq G$ της ομάδας G λέγεται κανονική όταν ισχύει $xH = Hx, \forall x \in G$. Πιό αναλυτικά τούτο σημαίνει ότι τα δύο σύνολα ταυτίζονται: $xH = \{xh : h \in G\} = Hx = \{h'x : h' \in G\}$.

Πρόταση 2.5.1 *Οι επόμενες προτάσεις είναι ισοδύναμες:*
(1) *Η υποομάδα $H \subseteq G$ είναι κανονική.*
(2) $\forall x \in G \Rightarrow xHx^{-1} \subseteq H$.
(3) $\forall x \in G \Rightarrow xHx^{-1} = H$.

Πράγματι, (1) $\Rightarrow$ (2) διότι αν $h \in H$ τότε $xh \in xH = Hx$, άρα θα υπάρχει $h' \in H : xh = h'x \Rightarrow xhx^{-1} = h' \in H$ που δείχνει ότι $xHx^{-1} \subseteq H$. (2) $\Rightarrow$ (3) διότι $xHx^{-1} \subseteq H$ γιά κάθε $x \in G$ συνεπάγεται και την $H \subseteq x^{-1}Hx$, $\forall x \in G$. Αρα και $xHx^{-1} = H$. Η (3) $\Rightarrow$ (1) είναι τετριμμένη.

Παρατηρήσεις
(1) Κάθε υποομάδα μιάς αβελιανής υποομάδας είναι κανονική. Άρα αν οι κανονικές υποομάδες έχουν κάποιο ενδιαφέρον αυτό θα φανεί στις μη-αβελιανές ομάδες.
(2) Κατ' αναλογίαν προς τα σύμπλοκα ορίζεται μέσω υποομάδος H μιά δεύτερη σχέση ισοδυναμίας, παρόμοια με την $\approx$ της προηγουμένης παραγράφου: $x \sim y \Leftrightarrow xy^{-1} \in H$. Οι κλάσεις ισοδυναμίας ως προς αυτήν την σχέση είναι τα σύνολα $Hx = \{hx : h \in H\}$ και το σύνολο των κλάσεων συμβολίζεται με $G \setminus H$. Η υποομάδα είναι κανονική τότε ακριβώς όταν $xH = Hx$ δηλαδή οι δύο σχέσεις ισοδυναμίας έχουν τις ίδιες κλάσεις ισοδυναμίας.
(3) Η ομάδα G λέγεται **απλή** όταν δεν έχει γνήσιες (δηλαδή δίαφορες του εαυτού της και της τετριμμένης $\{e\}$) κανονικές υποομάδες.

Πρόταση 2.5.2 *Γιά κάθε ομομορφισμό ομάδων $F : G_1 \longrightarrow G_2$ ο πυρήνας $Kern(F) \subseteq G_1$ είναι κανονική υποομάδα.*

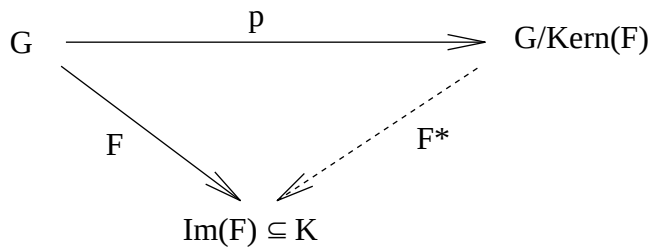
Πράγματι γιά τυχόν $x \in G_1$ και $h \in Kern(F)$ έχουμε $F(xhx^{-1}) = F(x)F(h)F(x^{-1}) = F(x)F(x^{-1}) = F(x)F(x)^{-1} = e$ άρα $xhx^{-1} \in Kern(F)$. Τούτο δείχνει ότι $xKern(F)x^{-1} \subseteq Kern(F)$.

Πρόταση 2.5.3 *Έστω G πεπερασμένη ομάδα τάξης $|G| = n$. Έστω $p|n$ ο ελάχιστος πρώτος αριθμός και διαιρέτης του n, διαφορετικός της μονάδος. Εάν $[G : H] = p$ τότε η H είναι κανονική.*

Παίρνουμε ένα στοιχείο $s \in G$ μη περιεχόμενο στο H. Δείχνουμε δύο πράγματα: (α) ότι τα σύμπλοκα $H, sH, s^2H, ... s^{p-1}H$ είναι διαφορετικά, και (β) ότι $t \in H \Rightarrow sts^{-1} \in H, \forall s \in G$ που αποδεικνύει την κανονικότητα. Για το (α): έστω ότι δύο συμπίπτουν: $s^iH = s^jH$, $i < j \Rightarrow s^{j-i} \in H$. Τότε, επειδή $j - i < p$ τα $(j - i)$ και n θα είναι πρώτα μεταξύ τους, άρα θα υπάρχουν $\mu, \nu : \mu \cdot (j - i) + \nu \cdot n = 1$. Τότε όμως $s = s^1 = s^{\mu\cdot(j-i)+\nu\cdot n} = (s^{j-i})^\mu \cdot (s^n)^\nu = (s^{j-i})^\mu \in H$ που είναι άτοπο. Γιά το (β): έστω ότι το $t \in H, b \notin H, s = btb^{-1} \notin H$. Το b θα περιέχεται σε κάποιο άλλο σύμπλοκο, έστω $b \in s^kH = bt^kb^{-1}H$, δηλαδή το b θα έχει την μορφή: $b = bt^kb^{-1}h, h \in H \Rightarrow t^kb^{-1} \in H \Rightarrow b^{-1} \in H$ που είναι άτοπο.

Πρόταση 2.5.4 *Γιά κάθε κανονική υποομάδα $H \subseteq G$ το σύνολο των κλάσεων G/H εφοδιάζεται με δομή ομάδος, έτσι ώστε η προβολή ενός στοιχείου $x \in G$ στην κλάση του $x' = xH$, να είναι ομομορφισμός ομάδων $F : G \longrightarrow G/H$. Ο πυρήνας $Kern(F) = H$. Η ομάδα G/H λέγεται* **ομάδα πηλίκον** *και η $F(x) = xH$* **κανονική προβολή**.

Την πράξη στο σύνολο των κλάσεων G/H ορίζουμε μέσω της πράξης στο G. Γιά δύο στοιχεία $u, v \in G/H$ διαλέγουμε αντιπροσώπους από τις κλάσεις $x \in u, y \in v$ και ορίζουμε $u*v = xyH$. Ο ορισμός αποδεικνύεται ανεξάρτητος των ειδικών αντιπροσώπων. Πράγματι αν $x' \in u, y' \in v$ είναι ισοδύναμα των x, y στοιχείων αντίστοιχα, τότε $x^{-1}x' \in H$ και $y^{-1}y' \in H$ και επομένως $(xy)^{-1}(x'y') = y^{-1}x^{-1}x'y' = y^{-1}hy' = y^{-1}y'h' = h''h' \in H$. Η πράξη λοιπόν αυτή στο G/H είναι καλώς ορισμένη, και βλέπουμε αμέσως ότι ικανοποιεί τα αξιώματα της ομάδος. Το ότι η κανονική προβολή είναι ομομορφισμός προκύπτει άμεσα από τον ορισμό της πράξης. Παρόμοια και το γεγονός ότι $Kern(F) = H$.



Σχήμα 2.2: Κανονική παραγοντοποίηση ομομορφισμού

Πρόταση 2.5.5 *Δοθέντος ομομορφισμού $F : G \longrightarrow K$ ομάδων, ορίζεται ομομορφισμός $F^* : G/Kern(F) \longrightarrow K$, έτσι ώστε $F = F^* \circ p$. Η παράσταση της F μ' αυτόν τον τρόπο λέγεται κανονική παραγοντοποίηση του ομομορφισμού. Η F^* είναι ισομορφισμός μεταξύ των ομάδων $G/Kern(F)$ και $Im(F) \subseteq K$ και φυσικά η p είναι επιμορφισμός ομάδων.*

Το διάγραμμα δηλώνει τον τρόπο που ορίζουμε την F^* : $F^*(xH) = F(x)$, όπου $H = Kern(F)$. Πρέπει να δούμε ότι η F^* είναι καλώς ορισμένη (ανεξάρτητη του αντιπροσώπου x) και ότι πληρούνται οι υπόλοιπες ιδιότητες του διαγράματος. Όλα αυτά όμως είναι τετριμμένα.

ΠΡΟΒΛΗΜΑΤΑ 2.5

Πρόβλημα 2.5.1 *Δείξε, χωρίς την χρήση της πρότασης 2.5.3, ότι μιά υποομάδα $H \subset G$ ομάδας G που έχει δείκτη $[G:H]=2$ είναι κανονική.*

Πρόβλημα 2.5.2 *Γιά $K=\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ με $SL(n,K)$ συμβολίζουμε το σύνολο των $n\times n$ πινάκων με στοιχεία από το K και ορίζουσα 1. Δείξε ότι σε κάθε περίπτωση η $SL(n,K)\subseteq GL(n,K)$ είναι κανονική υποομάδα της αντίστοιχης ομάδας των αντιστρεψίμων πινάκων.*

Πρόβλημα 2.5.3 *Εάν H και K είναι υποομάδες της ομάδος G και μία απ' αυτές είναι κανονική, τότε το γινόμενό τους $HK=\{hk : h\in H\ ,\ k\in K\}$, είναι υποομάδα της G. Εάν και οι δύο είναι κανονικές, τότε και το γινόμενό τους είναι κανονική υποομάδα. Εάν η G είναι πεπερασμένη τότε η τάξη της HK είναι $|HK|=|H||K|/|H\cap K|$.*

Πρόβλημα 2.5.4 *Έστω H κανονική υποομάδα της ομάδας G. Δείξε ότι κάθε υποομάδα $\bar{K}\subseteq \bar{G}=G/H$ της ομάδας-πηλίκον, ορίζει μιά υποομάδα $K\subseteq G$, περιέχουσα την H, $H\subseteq K$, έτσι ώστε οι ομάδες K/H και $\bar{K}$ να είναι ισόμορφες. (Υπόδειξη: Χρησιμοποίησε την πρόταση 2.5.5, γιά τον περιορισμό της κανονικής προβολής $p: G\longrightarrow \bar{G}$ στην K.)*

2.6 Κυκλικές Ομάδες

Η ομάδα G λέγεται **Κυκλική** , όταν υπάρχει στοιχείο της $a\in G$, με $G=<a>$. Κάθε πεπερασμένη κυκλική ομάδα είναι ισόμορφη με μιά $\mathbb{Z}_n$. Παρακάτω κάνουμε μιά σύντομη μελέτη αυτού του φαινομένου.

Πρόταση 2.6.1 *Κάθε υποομάδα G της $\mathbb{Z}$ είναι της μορφής $G=\{mk : k\in\mathbb{Z}\}=m\mathbb{Z}$, δηλαδή συμπίπτει με το σύνολο των πολλαπλασίων κάποιου μη-αρνητικού ακεραίου m. Κάθε υποομάδα της $m\mathbb{Z}$ είναι της μορφής $dm\mathbb{Z}$ γιά κάποιο μη-αρνητικό ακέραιο d.*

Πράγματι, αν η $G\neq\{0\}$, η ομάδα θα περίεχει θετικούς ακεραίους. Εστω λοιπόν m ο ελάχιστος θετικός ακέραιος που περιέχεται στην G. Ο m διαιρεί όλα τα στοιχεία της G. Πράγματι $x\in G$ διαιρούμενο με το m θα δίνει $x=rm+y$ με $0\leq y\leq m$. Αν το υπόλοιπο της διαίρεσης y ήταν διάφορο του μηδενός, τότε $y=x-rm\in G$ θα ήταν θετικό και μικρότερο από το m. Ατοπο, αφού το m είναι το μικρότερο μ' αυτήν την ιδιότητα. Ο δεύτερος ισχυρισμός αποδεικνύεται ανάλογα.

Πρόταση 2.6.2 *Γιά κάθε φυσικό n η ομάδα πηλίκον της $\mathbb{Z}$ ως προς την υποομάδα της $n\mathbb{Z}=\{nk : k\in\mathbb{Z}\}$ είναι ισόμορφη με την $\mathbb{Z}_n$.*

Βλέπουμε αμέσως ότι η απεικόνιση F που σε μία κλάση $v+\mathbb{Z}$ αντιστοιχεί τον ελάχιστο θετικό $\overline{v}$ περιεχόμενο σ' αυτήν την κλάση, ορίζει μέσω της κανονικής παραγοντοποίησης (πρόταση 2.5.5) ισομορφισμό $F': \mathbb{Z}/n\mathbb{Z}\longrightarrow\mathbb{Z}_n$.

Πρόταση 2.6.3 *Κάθε κυκλική ομάδα G είναι ισόμορφη προς την $\mathbb{Z}$ ή την $\mathbb{Z}_n$ γιά κάποιο θετικό n.*

Πράγματι, έστω η κυκλική ομάδα $G=<a>$ και ας ορίσουμε την απεικονιση $F:\mathbb{Z}\longrightarrow G$ με $F(k)=a^k$, $F(0)=e$. Βλέπουμε εύκολα ότι η F είναι επιμορφισμός ομάδων, άρα εισάγει μέσω της κανονικής παραγοντοποίησης (πρόταση 2.5.5) ισομορφισμό $F': \mathbb{Z}/Kern(F)\longrightarrow G$. Η πρόταση συνάγεται από την προηγούμενη, ανάλογα με το αν $Kern(F)=\{0\}$ ή

$Kern(F) \neq \{0\}$. Στην πρώτη περίπτωση η F είναι ισομορφισμός. Στην δεύτερη περίπτωση η $Kern(F)$ θα είναι της μορφής $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ και επομένως η F' ισομορφισμός της $\mathbb{Z}_n$ με την G.

Πρόταση 2.6.4 *Κάθε υποομάδα H μιάς κυκλικής ομάδος $G =< a >$ είναι κυκλική τάξης k , όπου k διαιρέτης της τάξεως $n = |G|$.*

Η απόδειξη είναι στην ουσία η ίδια με αυτήν της προηγουμένης πρότασης. Πρώτα σημειώνουμε ότι όλες οι υποομάδες της $m\mathbb{Z}$ είναι της μορφής $(km)\mathbb{Z}$ και ότι ισχύει $(m\mathbb{Z})/((km)\mathbb{Z}) = \mathbb{Z}/(k\mathbb{Z}) = \mathbb{Z}_k$. Γιά την απόδειξη της πρότασης θεωρούμε πάλι την $F : \mathbb{Z} \longrightarrow G$ με $F(x) = a^x$. Η αντίστροφη εικόνα της δοθήσης υποομάδος $H' = F^{-1}(H)$ είναι υποομάδα της $\mathbb{Z}$ άρα έχει την μορφή $m\mathbb{Z}$. Επίσης η H' περιέχει την $Kern(F) = n\mathbb{Z}$,άρα $n = km$ και η H θα είναι ισόμορφη προς την $m\mathbb{Z}/((km)\mathbb{Z}) = \mathbb{Z}_k$.

ΠΡΟΒΛΗΜΑΤΑ 2.6

Πρόβλημα 2.6.1 *Δείξε ότι οι ομάδες $m\mathbb{Z}/((km)\mathbb{Z})$ και $\mathbb{Z}_k$ είναι ισόμορφες.*

Πρόβλημα 2.6.2 *Δείξε ότι μιά απλή αβελιανή ομάδα είναι πεπερασμένη κυκλική με τάξη πρώτο αριθμό.*

Πρόβλημα 2.6.3 *Δείξε ότι η $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ έχει τρεις μη τετριμμένες υποομάδες. Δείξε επίσης ότι υπάρχουν τρεις διαφορετικοί μη-τετριμμένοι ομομορφισμοί $F : G \longrightarrow \mathbb{Z}_2$. Δείξε τέλος, ότι γιά κάθε δύο τέτοιους ομομορφισμούς F_1, F_2 υπάρχει αντιστρέψιμος ομομορφισμός $\Phi : G \longrightarrow G$, έτσι ώστε $F_2 = F_1 \circ \Phi$.*

Πρόβλημα 2.6.4 *Δείξε ότι γιά κάθε διαιρέτη $k|n$ της τάξης $n = |G|$ μιάς κυκλικής ομάδας G, υπάρχει μία ακριβώς υποομάδα της $H \subseteq G$, με αυτήν την τάξη: $|H| = k$. (Υπόδειξη: Αν $G =< a >$, $n = ks$, πάρε $H =< a^s >$. Γιά κάθε άλλη $H =< a^t >$, τάξης k, διαίρεσε $t = ms + v$ κτλ.).*

Πρόβλημα 2.6.5 *Δοθέντων δύο ακεραίων a, b, θεωρούμε το σύνολο $S = \{ua + vb : u, v \in \mathbb{Z}\}$. Δείξε ότι το σύνολο αυτό είναι υποομάδα της $\mathbb{Z}$, επομένως της μορφής $d\mathbb{Z}$. Δείξε ότι το d είναι ο ελάχιστος κοινός διαιρέτης των a, b, και γράφεται $d = ua + vb$ γιά κάποια u, $v \in \mathbb{Z}$. Συμπέρανε ότι a, b, είναι πρώτοι μεταξύ τους, τότε και μόνον τότε, όταν υπάρχουν u, $v \in \mathbb{Z}$ με $ua + vb = 1$.*

Πρόβλημα 2.6.6 *Δείξε ότι μιά ομάδα που παράγεται από δύο στοιχεία που ικανοποιούν τις σχέσεις $G =< s, t : s^p = e, t^q = e, st = ts >$, είναι ισόμορφη προς την $\mathbb{Z}_p \times \mathbb{Z}_q$.*

2.7 Μεταθέτρια υποομάδα

Μεταθέτη δύο στοιχείων ομάδος $a, b \in G$, ονομάζουμε το $[a\,, b] = a^{-1}b^{-1}ab$. Φυσικά τούτο έχει κάποιο νόημα μόνο στις μη-αβελιανές ομάδες. Την ομάδα που παράγεται από όλους τους δυνατούς μεταθέτες ονομάζουμε μεταθέτρια υποομάδα της ομάδος και συμβολίζουμε με $G' = [G\,, G]$. Τα στοιχεία της G' λοιπόν αποτελούνται, εξ' ορισμού, από γινόμενα μεταθετών $[a\,, b]$ της ομάδος.

Παρατηρήσεις
(1) Ο μεταθέτης $[a\,,b]=e$ γιά κάθε αβελιανή ομάδα. Συνεπώς η μεταθέτρια σ' αυτήν την περίπτωση είναι η τετριμμένη ομάδα.
(2) Γιά κάθε ομομορφισμό ομάδων $F: G_1 \longrightarrow G_2$, έχουμε $F([a\,,b])=F(a^{-1}b^{-1}ab)=F(a)^{-1}F(b)^{-1}F(a)F(b)=[F(a)\,,F(b)]$. Άρα η F σέβεται τον μεταθέτη και απεικονίζει την μεταθέτρια στην μεταθέτρια $F([G_1\,,G_1])\subseteq[G_2\,,G_2]$.
(3) Βλέπουμε αμέσως ότι $g[a\,,b]g^{-1}=[gag^{-1}\,,gbg^{-1}]$. Τούτο δείχνει αμέσως ότι η μεταθέτρια $[G\,,G]$ είναι κανονική υποομάδα της G.

Πρόταση 2.7.1 *Γιά την μεταθέτρια υποομάδα $H=[G\,,G]\subseteq G$ το σύνολο πηλίκον G/H είναι αβελιανή ομάδα.*

Πράγματι, σύμφωνα με τον ορισμό της πράξης στο σύνολο πηλίκον G/H, για δύο στοιχεία του $a'=aH\,,b'=bH\ \in G/H$, θα έχουμε $[a'\,,b']=a'^{-1}b'^{-1}a'b'=aH^{-1}bH^{-1}aHbH=a^{-1}b^{-1}abH=[a\,,b]H=H$. Αφού $[a\,,b]\in H$.

Πρόταση 2.7.2 *Εάν $H\,,K$ είναι κανονικές υποομάδες της ομάδος G, τότε η υποομάδα $[H\,,K]$ που παράγεται από τους μεταξύ τους μεταθέτες: $[h\,,k]=h^{-1}k^{-1}hk$ είναι κανονική.*

Τούτο στηρίζεται στην παρατήρηση πιο πάνω: $g[a\,,b]g^{-1}=[gag^{-1}\,,gbg^{-1}]$, που ισχύει ανεξάρτητα του που ανήκουν τα $a\,,b$. Συνέπεια αυτού είναι και η επόμενη πρόταση.

Πρόταση 2.7.3 *Η λεγόμενη* **παραγόμενη** *σειρά υποομάδων μιάς ομάδας $G: G'=[G\,,G]\,,$ $G''=[G\,,G]\,,\ldots,G^{(n)}=[G^{(n-1)}\,,G^{(n-1)}]\,,\ldots$ αποτελείται από κανονικές υποομάδες της G σε φθίνουσα διάταξη: $G\supseteq G'\supseteq G''\supseteq\ldots G^{(n)}\supseteq\ldots.$*

Πρόταση 2.7.4 *Κάθε υποομάδα H ομάδος G περιέχουσα την μεταθέτρια $[G\,,G]\subseteq H$ είναι κανονική.*

Τούτο στηρίζεται στην παρατήρηση: $axa^{-1}=[a^{-1}\,,x^{-1}]x\in Hx=H$ που ισχύει γιά κάθε $x\in H$ και κάθε $a\in G$.

2.8 Συζυγία

Συζυγία λέμε, σε μιά ομάδα G, μιά ειδική σχέση ισοδυναμίας μεταξύ των στοιχείων της: $x\sim y\ \Leftrightarrow\ \exists g\in G: y=gxg^{-1}$. Είναι εύκολο να δούμε ότι η σχέση αυτή είναι, πράγματι, σχέση ισοδυναμίας. Η ομάδα χωρίζεται λοιπόν σε ξένα μεταξύ τους υποσύνολα, τις κλάσεις ισοδυναμίας που λέγονται **κλάσεις συζυγίας**.

Παρατηρήσεις
(1) Συζυγή στοιχεία ομάδος έχουν σε πολλές περιπτώσεις παρόμοιες ιδιότητες. Π.χ. συζυγή στοιχεία έχουν την ίδια τάξη. Τούτο οφείλεται στην $(gxg^{-1})^n=g(x^n)g^{-1}$ που αποδεικνύεται εύκολα.
(2) Μιά κλάση συζυγίας που έχει ένα μόνο στοιχείο $\{x\}$ σημαίνει ότι $gxg^{-1}=x,\ \forall g\in G$. Άρα το x μετατίθεται με κάθε στοιχείο της ομάδας και ανήκει στο **κέντρο** της $Z(G)$. Το κέντρο $Z(G)\subseteq G$ αποτελείται ακριβώς απ' όλα τα στοιχεία x με την προηγούμενη ιδιότητα. Το κέντρο της ομάδας είναι μιά κανονική υποομάδα της.
(3) Μιά κανονική υποομάδα χαρακτηρίζεται από την $gHg^{-1}\subseteq H,\ \forall g\in G$. Τούτο σημαίνει ότι η H με κάθε x που περιέχει, περιέχει και ολόκληρη την κλάση συζυγίας του x.

Συνεπώς οι κανονικές υποομάδες είναι ενώσεις κλάσεων συζυγίας.
(4) Συζυγία ορίζεται και μεταξύ υποσυνόλων $A \subset G$ της ομάδος. Δύο υποσύνολά της A, A', λέγονται συζυγή, όταν υπάρχει στοιχείο $x \in G : xAx^{-1} = A'$. Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι υποομάδες της G που τυχαίνει να είναι συζυγείς. Οι κανονικές υποομάδες χαρακτηρίζονται απ' το ότι οι μόνες συζυγείς τους είναι ο εαυτός τους.

Πρόταση 2.8.1 *Για κάθε υποσύνολο $A \subseteq G$ ομάδας G, το σύνολο $N_G(A) = \{x \in G : xAx^{-1} \subseteq A\}$ αποτελεί υποομάδα και λέγεται* **κανονικοποιητής** *του A. Το σύνολο των συζυγών του A έχει $[G : N_G(A)]$ στοιχεία .*

Ο πρώτος ισχυρισμός, ότι η $N_G(A)$ είναι υποομάδα της G, αποδεικνύεται εύκολα. Για τον δεύτερο ισχυρισμό, ας συμβολίζουμε με $C(A)$ το σύνολο των συζυγών του A και ας ορίσουμε απεικόνιση $f : C(A) \longrightarrow G/N_G(A), f(gAg^{-1}) = gN_G(A)$ (το σύμπλοκο). Η f είναι 1-1. Πράγματι $gN_G(A) = g'N_G(A)$ συνεπάγεται $g' = gn$ γιά κάποι $n \in N_G(A)$ άρα $g'Ag'^{-1} = (gn)A(gn)^{-1} = g(nAn^{-1})g^{-1} = gAg^{-1}$. Προφανώς δε η f είναι και επί, αφου το $gN_G(A)$ προκύπτει σαν εικόνα μέσω της f του gAg^{-1}.

Παρατηρήσεις
(1) Οι κλάσεις συζυγίας αποτελούν μιά διαμέριση της ομάδας αλλά όχι τόσο νοικοκυρεμένη όσο η διαμέριση σε σύμπλοκα. Στην τελευταία οι κλάσεις έχουν όλες το ίδιο πλήθος στοιχείων, ενώ στις κλάσεις συζυγίας, οι κλάσεις έχουν διαφορετικό πλήθος στοιχείων.
(2) Τα στοιχεία του κέντρου της ομάδος έχουν ως συζυγή μόνο τον εαυτό τους, άρα ορίζουν μονοστοίχειες κλάσεις συζυγίας.
(3) Η προηγούμενη πρόταση δείχνει ότι οι κλάσεις συζυγίας, αν και δεν έχουν την κανονικότητα των συμπλόκων, εκφράζουν ωστόσο τους πληθικούς αριθμούς τους με την βοήθεια καταλλήλων συμπλόκων ($[G : N_G(A)]$). Άρα, στην περίπτωση πεπερασμένων ομάδων, το πλήθος των στοιχείων μιάς κλάσης συζυγίας διαιρεί την τάξη της ομάδος.

Πρόταση 2.8.2 *(***Εξίσωση των κλάσεων***) Γιά κάθε πεπερασμένη ομάδα G ισχύει*

$$|G| = |Z(G)| + [G : N_G(a_1)] + ... + [G : N_G(a_k)],$$

όπου $Z(G)$ είναι το κέντρο της G και $a_1, ... a_k$ είναι αντιπρόσωποι των κλάσεων συζυγίας της G που δεν ανήκουν στο κέντρο της G.

Η πρόταση είναι συνέπεια του ότι οι κλάσεις συζυγίας αποτελούν μιά διαμέριση του G σε ξένα μεταξύ τους σύνολα. Άρα η τάξη της G είναι το άθροισμα των πληθικών αριθμών αυτών των κλάσεων ισοδυναμίας. Κάθε $x \in Z(G)$ ορίζει ωστόσο μιά μονοστοίχειο κλάση, άρα υπάρχουν $|Z(G)|$ τέτοια στοιχεία. Διαλέγουμε κατόπιν έναν αντιπρόσωπο $a_i \in A_i$ από κάθε κλάση συζυγίας που δεν είναι μονοστοίχεια. Τα στοιχεία του A_i είναι ακριβώς τα συζυγή του a_i που σύμφωνα με την προηγούμενη πρόταση είναι $[G : N_G(a_i)]$ το πλήθος.

Πρόταση 2.8.3 *Κάθε πεπερασμένη ομάδα G της οποίας η τάξη είναι δύναμις p^n , $n \geq 1$ ενός πρώτου έχει μή τετριμμένο κέντρο $Z(G)$.*

Πράγματι, αν γράψουμε την εξίσωση των κλάσεων γι' αυτήν την ομάδα, τότε οι αριθμοί $[G : N_G(a_i)]$ θα διαιρούν το p^n άρα και $|Z(G)| = |G| - [G : N_G(a_1)] - ... - [G : N_G(a_k)]$ θα διαιρήται με το p και $|Z(G)| \geq 1$ (περιέχει το e), άρα $|Z(G)| \geq p$.

ΠΡΟΒΛΗΜΑΤΑ 2.8

Πρόβλημα 2.8.1 *Εστω p πρώτος φυσικός αριθμός. Προσδιόρισε όλες τις ομάδες με p το πλήθος στοιχεία.*

Πρόβλημα 2.8.2 *Δείξε ότι γιά κάθε $n \geq 2$ φυσικό, το σύνολο των αντιστρεψίμων στοιχείων της $\mathbb{Z}_n$ ως προς τον πολλαπλασιασμό των κλάσεων, αποτελεί ομάδα $\mathbb{Z}_n^*$ με $\phi(n)$ στοιχεία. Η συνάρτηση $\phi(n)$ (του Euler), δίνει το πλήθος των πρώτων προς το n και μικρότερων αυτού ακεραίων. Την συνάρτηση αυτή θα εξετάσουμε λεπτομερέστερα στο πέμπτο κεφάλαιο.*

Πρόβλημα 2.8.3 *Δείξε ότι γιά κάθε $n \geq 2$ φυσικό, το σύνολο $G_n \subset \mathbb{Z}_n$ των στοιχείων $x \in \mathbb{Z}_n$ που παράγουν την $\mathbb{Z}_n$, δηλαδή ισχύει $< x >= \mathbb{Z}_n$, έχει $\phi(n)$ το πλήθος στοιχεία. Αποτελεί το G_n υποομάδα της $\mathbb{Z}_n$; Ποιά ακριβώς στοιχεία του $\mathbb{Z}_n$ περιέχονται στο G_n;*

Πρόβλημα 2.8.4 *Δείξε ότι αν $d|n$ είναι διαιρέτης του n, τότε υπάρχουν $\phi(d)$ ακριβώς στοιχεία της $\mathbb{Z}_n$ τάξης d. (Υπόδειξη: Έστω $v = n/d$. Η υποομάδα $\{v, 2v, ..., dv = n\} \subset \mathbb{Z}_n$ είναι η μόνη που περιέχει στοιχεία τάξης d και έχει $\phi(d)$ γεννήτορες.)*

Πρόβλημα 2.8.5 *Βρες τις ομάδες $\mathbb{Z}_n^*$ γιά $n = 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20$.*

Πρόβλημα 2.8.6 *Δείξε ότι γιά δύο ακέραιους k, p, πρώτους μεταξύ τους ισχύει $k^{p-1} = 1 \bmod p$. (Υπόδειξη: το k παράγει το $\mathbb{Z}_p$ και $(1k)(2k)...((p-1)k) = (1)(2)...(p-1) \bmod p$.)*

Πρόβλημα 2.8.7 *(Θεώρημα Euler-Fermat) Δείξε ότι γιά δύο ακέραιους k, p πρώτους μεταξύ τους ισχύει $k^{\phi(p)} = 1 \bmod p$. Η συνάρτηση ϕ ορίζεται στην άσκηση 2.8.2. (Υπόδειξη: $\phi(p)$ είναι η τάξη της πολλαπλασιαστικής ομάδος $\mathbb{Z}_p^*$.)*

Πρόβλημα 2.8.8 *Δείξε ότι η ομάδα γινόμενο $G = G_1 \times G_2$ περιέχει δύο κανονικές υποομάδες G_1', G_2' που είναι ισόμορφες με τις G_1, G_2 αντίστοιχα. Δείξε επίσης ότι ισχύουν: (α) Κάθε στοιχείο $g \in G$ γράφεται $g = g_1 g_2$, όπου $g_1 \in G_1'$, $g_2 \in G_2'$. (β) τα προηγούμενα g_1, g_2, καθορίζονται μονοσήμαντα από το g. (γ) ισχύει $g_1 g_2 = g_2 g_1$ γιά κάθε $g_1 \in G_1'$, $g_2 \in G_2'$.*

Πρόβλημα 2.8.9 *Δείξε ότι η ομάδα γινόμενο $\mathbb{Z}_2 \times \mathbb{Z}_2$ δεν είναι ισόμορφη με την ομάδα $\mathbb{Z}_4$ αλλά είναι ισόμορφη με την ομάδα G_8 των αντιστρεψίμων στοιχείων της $\mathbb{Z}_8$ (δες 2.4.5).*

Πρόβλημα 2.8.10 *Δείξε ότι η τομή $G = \cap G_i$, μιάς οικογένειας (κανονικών) υποομάδων $G_i \subset G$ της ομάδας H, είναι (κανονική) υποομάδα της H. Δείξε ότι δεν ισχύει το ανάλογο γιά την* **ένωση** *μιάς οικογένειας υποομάδων της H. Γιά δοθέν στοιχείο $x \in H$ προσδιόρισε την τομή όλων των υποομάδων της H που περιέχουν το x. Δείξε ότι η τομή αυτή συμπίπτει με την κυκλική ομάδα που παράγεται από το x.*

Πρόβλημα 2.8.11 *Έστω το στοιχείο $z = (cos\phi, sin\phi)$, του μοναδιαίου κύκλου του μιγαδικού επιπέδου. Πότε η κυκλική ομάδα που παράγεται από τις δυνάμεις του z είναι πεπερασμένη και πότε άπειρη; Ποιά η σχέση αυτής της ομάδος με τις $\mathbb{Z}_n$ και $\mathbb{Z}$;*

Πρόβλημα 2.8.12 *Έστω η απεικόνιση $F([x]_{15}) = ([x]_3, [x]_5)$, $F : \mathbb{Z}_{15} \longrightarrow \mathbb{Z}_3 \times \mathbb{Z}_5$. Δείξε ότι η F είναι ομομορφισμός ομάδων. Βρες την υποομάδα-πυρήνα $H = Kern(F)$ της F. Συμπέρανε ότι απεικόνιση αυτή είναι ισομορφισμός ομάδων. Γενίκευσε το συμπέρασμα γιά μιά ανάλογη απεικόνιση $F : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$. Όπου m, n θετικοί ακέραιοι πρώτοι μεταξύ τους. Γενίκευσε ακόμη περισσότερο το συμπέρασμα γιά απεικόνιση της μορφής*

$$F : \mathbb{Z}_{m_1 ... m_k} \longrightarrow \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_k}.$$

Όπου οι ακέραιοι θετικοί $m_1, ..., m_k$ είναι ανά δύο πρώτοι μεταξύ τους.

Πρόβλημα 2.8.13 *Δείξε ότι αν οι υποομάδες H, K της ομάδος G είναι κανονικές και η τομή $K \cap H = \{e\}$, τότε κάθε στοιχείο της H μετατίθεται με κάθε στοιχείο της K.*

Πρόβλημα 2.8.14 *Εστω $\mathbb{C}_* = \{z \in \mathbb{C} \ : z \neq 0\}$ η πολλαπλασιαστική ομάδα των μιγαδικών αριθμών και S^1 η υποομάδα της των μοναδιαίων αριθμών. Περίγραψε τα σύμπλοκα της S^1 στην $\mathbb{C}_*$. Δείξε ότι η ομάδα πηλίκον $\mathbb{C}_*/S^1$ είναι ισόμορφη με την $\mathbb{R}_*$, πολλαπλασιαστική ομάδα των θετικών πραγματικών αριθμών.*

Πρόβλημα 2.8.15 *Δείξε ότι ο μόνος αυτομορφισμός της ομάδος $\mathbb{Z}$ είναι η ταυτοτική απεικόνιση.*

Πρόβλημα 2.8.16 *Δείξε ότι η ομάδα αυτομορφισμών της ομάδος $\mathbb{Z}_n$ είναι ισόμορφη με την πολλαπλασιαστική ομάδα $\mathbb{Z}_n^*$.*

Πρόβλημα 2.8.17 *Βρες τις ομάδες αυτομορφισμών της προσθετικής ομάδος $\mathbb{C}$ και των πολ/κών: $\mathbb{C}_*$ και S^1. (Υπόδειξη: Ταύτισε την $\mathbb{C}$ με το $\mathbb{R}^2$. Για τις πολλαπλασιαστικές συσχέτισε το $f(x)$ με το $f(1)$.)*

Πρόβλημα 2.8.18 *Δοθέντος υποσυνόλου $S \subseteq G$ δείξε ότι η παραγόμενη $< S >$ από το S υποομάδα της G ταυτίζεται με την τομή όλων των υποομάδων της G που περιέχουν το S.*

Πρόβλημα 2.8.19 *Δείξε ότι το κέντρο $Z(G) = \{g \in G : xgx^{-1} = g \ , \forall x \in G\}$ ομάδας G είναι κανονική υποομάδα της G.*

Πρόβλημα 2.8.20 *Δείξε ότι σε κάθε ομάδα τα ab και ba είναι συζυγή στοιχεία. Γενίκευσε γιά γινόμενα περισσοτέρων στοιχείων.*

Πρόβλημα 2.8.21 *Δείξε ότι το κέντρο της ομάδας $GL(n, \mathbb{R})$ είναι η ομάδα των διαγωνίων πινάκων με ίσα διαγώνια στοιχεία $c \neq 0$.*

Πρόβλημα 2.8.22 *Δείξε ότι ότι δεν υπάρχει πεπερασμένη απλή ομάδα G της οποίας η τάξη να είναι p^n , $n > 1$ με p πρώτο αριθμό.*

Πρόβλημα 2.8.23 *Δείξε ότι σε μιά πεπερασμένη ομάδα G και γιά κάθε γνήσια υποομάδα της H, η ένωση όλων των συζυγών της: gHg^{-1} δεν μπορεί να είναι ποτέ ίση με την G. (Υπόδειξη: Αν $d = [G : N_G(H)]$, τότε $G = \cup_{i=1}^{d} g_i N_G(H)$, όπου $\{g_i\}$ αντιπρόσωποι των κλάσεων $G/N_G(H)$. Αν ήταν και $G = \cup_{i=1}^{d} g_i H g_i^{-1}$, με $H \subset N_G(H)$, γνήσιο υποσύνολο, θα είχαμε αντίφαση.)*

Πρόβλημα 2.8.24 *Έστω ότι η ομάδα αυτομορφισμών $Aut(G)$ της ομάδας G, είναι κυκλική. Δείξε ότι τότε η ομάδα G είναι αβελιανή. Εάν επί πλέον η G είναι πεπερασμένη, τότε είναι και κυκλική. (Υπόδειξη: Αν δεν είναι αβελιανή, υπάρχουν στοιχεία x, $y \in G$ με $xy \neq yx$. Δείξε ότι αν οι εσωτερικοί αυτομορφισμοί $I_x = t^k$, $I_y = t^m$, όπου t γεννήτορας της $Aut(G)$, τότε $I_{xyx^{-1}y^{-1}} = e$, κτλ.)*

Κεφάλαιο 3

Ομάδες Μεταθέσεων

3.1 Ομάδες Μεταθέσεων γενικά

Δοθέντος συνόλου $X \neq \emptyset$, **μετάθεση** του X λέμε μιά αμφιμονοσήμαντη απεικόνιση f του X στον εαυτό του. Το σύνολο των μεταθέσεων του X αποτελεί μιά ομάδα ως προς την σύνθεση απεικονίσεων $g \circ f$. Αντίστροφο στοιχείο του f είναι η αντίστροφη απεικόνιση f^{-1} και ουδέτερο στοιχείο e είναι η ταυτοτική απεικόνιση του X στον εαυτό του. Την ομάδα αυτή συμβολίζουμε με $S(X)$.

Παρατηρήσεις
(1) Συνήθως μας ενδιαφέρουν υποομάδες της $S(X)$. Γιά παράδειγμα, για το $X = \mathbb{R}^n$ οι αμφιμονοσήμαντες γραμμικές απεικονίσεις (συνεχείς ομομορφισμοί ως προς την πρόσθεση διανυσμάτων) $f : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ αποτελούν υποοομάδα της $S(X)$ ισόμορφη προς την $GL(n, \mathbb{R})$.
(2) Ιδιαίτερο ενδιαφέρον παρουσιάζουν οι υποομάδες της $S(X)$ που προκύπτουν από γεωμετρικά σύνολα. Π.χ. αν το X είναι ένα τρίγωνο, ενδιαφέρον παρουσιάζει η υποομάδα του $S(X)$ που αποτελείται από ισομετρίες του επιπέδου που περιέχει το τρίγωνο και απεικονίζουν το τρίγωνο στον εαυτό του. Όσο πιο μεγάλη είναι αυτή η υποομάδα τόσο πιό συμμετρικό θα είναι το τρίγωνο. Έτσι το ισόπλευρο τρίγωνο θα έχει 6 ισομετρίες ενώ ένα τρίγωνο με τρεις διαφορετικές μεταξύ τους γωνίες θα έχει μία και μόνον ισομετρία (την ταυτοτική). Αργότερα θα εξετάσουμε λεπτομερώς την ομάδα ισομετριών ενός κανονικού $n-$γώνου.
(3) Χρειάζεται να προσέξουμε την ιδιαίτερη υφή των στοιχείων $f \in S(X)$. Τα στοιχεία της ομάδος είναι σχετικά περίπλοκα αντικείμενα, απεικονίσεις του X στον εαυτό του. Ετσι λ.χ. η ισότητα δύο στοιχείων f, g της ομάδος $S(X)$ σημαίνει μιά ολόκληρη διαδικασία, αφού πρέπει να δείξουμε ότι ισχύει $f(x) = g(x)$, $\forall x \in X$.
(4) Η επόμενη πρόταση δείχνει ότι οι υποομάδες των ομάδων μεταθέσεων $S(X)$ συμπεριλαμβάνουν όλες τις δυνατές περιπτώσεις ομάδων.

Πρόταση 3.1.1 *Για κάθε ομάδα G υπάρχει υποομάδα $G' \subseteq S(G)$ ισόμορφη της G.*

Πράγματι, γιά κάθε $g \in G$ ο πολλαπλασιασμός από αριστερά με το g $L_g : G \longrightarrow G$, $L_g(x) = gx$, είναι μιά αμφιμονοσήμαντη απεικόνιση του G στον εαυτό του με αντίστροφο την $L_{g^{-1}}$. Έτσι λοιπόν η απεικόνιση $L : G \longrightarrow S(G)$ με $L(g) = L_g$ μπορούμε να δούμε εύκολα ότι είναι ομομορφισμός ομάδων 1-1 και $G' = L(G) \subset S(G)$ είναι μιά υποομάδα της $S(G)$ ισόμορφη μέσω της L με την αρχική ομάδα G.
Η $G' = L(G) \subset S(G)$ λέγεται **κανονική παράσταση** της ομάδος G.

3.2 Η συμμετρική ομάδα S_n

Την προηγούμενη γενική έννοια περιορίζουμε εδώ στην περίπτωση του συνόλου $X = \underline{n} = \{1, 2, ..., n\}$. Την αντίστοιχη ομάδα μεταθέσεων $S(X) = S(\underline{n})$ ονομάζουμε συμμετρική ομάδα και συμβολίζουμε με S_n.

Παρατηρήσεις

(1) Τα στοιχεία της ομάδος αυτής είναι απεικονίσεις του $\underline{n}$ στον εαυτό του, άρα ταυτίζονται με αναδιατάξεις αυτού του συνόλου. Συνεπώς το πλήθος τους είναι όσο και το πλήθος των αναδιατάξεων του $\underline{n}$ δηλαδή $n!$.

(2) Συνηθίζεται ο συμβολισμός:

$$t = \begin{pmatrix} 1, 2, ..., n \\ i_1, ..., i_n \end{pmatrix},$$

ο οποίος περιγράφει αναλυτικά την μετάθεση $t \in S_n$, σημειώνοντας ότι το $i_k = t(k)$ ευρίσκεται κάτω από το k. Η αντίστροφη μετάθεση θα μπορούσε αντίστοιχα να συμβολισθεί με το

$$t^{-1} = \begin{pmatrix} i_1, ..., i_n \\ 1, ..., n \end{pmatrix}.$$

(3) Το $S_1 = e$ είναι η τετριμμένη ομάδα. Το S_2 περιλαμβάνει την ταυτοτική $e = \begin{pmatrix} 1\,2 \\ 1\,2 \end{pmatrix}$ και την $t = \begin{pmatrix} 1\,2 \\ 2\,1 \end{pmatrix}$, προφανώς με $t^2 = e$. Βλέπουμε αμέσως ότι η S_2 είναι ισόμορφη με την παλιά μας γνώριμο $\mathbb{Z}_2$.

(4) Ο αναλυτικός αυτός τρόπος γραφής διευκολύνει στο να βρούμε εύκολα το γινόμενο δύο μεταθέσεων $t, s \in S_n$. Πράγματι αν γράψουμε $t = \begin{pmatrix} 1 \dots n \\ i_1 \dots i_n \end{pmatrix}, s = \begin{pmatrix} 1 \dots n \\ j_1 \dots j_n \end{pmatrix}$ τότε το γινόμενο $st = \begin{pmatrix} 1 \dots n \\ k_1 \dots k_n \end{pmatrix}$ όπου $k_m = t(s(m)) = t(i_m) = j_{i_m}$ ευρίσκεται κάτω από το στοιχείο i_m στο σύμβολο της t. π.χ. $t = \begin{pmatrix} 1\,2\,3\,4 \\ 3\,2\,4\,1 \end{pmatrix}, s = \begin{pmatrix} 1\,2\,3\,4 \\ 2\,3\,1\,4 \end{pmatrix}$ δίδει $st = \begin{pmatrix} 1\,2\,3\,4 \\ 1\,3\,4\,2 \end{pmatrix}$.

Πρόταση 3.2.1 *Η ομάδα S_3 παράγεται από τις μεταθέσεις $s = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 3\ 1 \end{pmatrix}$ και $t = \begin{pmatrix} 1\ 2\ 3 \\ 1\ 3\ 2 \end{pmatrix}$. Τα στοιχεία της S_3 είναι τα e, s, t, s^2, ts και ts^2.*

Πράγματι, λογαριάζουμε αμέσως ότι $s^2 = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 1\ 2 \end{pmatrix}$ $ts = \begin{pmatrix} 1\ 2\ 3 \\ 3\ 2\ 1 \end{pmatrix}$ $ts^2 = \begin{pmatrix} 1\ 2\ 3 \\ 2\ 1\ 3 \end{pmatrix}$. Μαζί με την ταυτοτική αυτές είναι οι 6 δυνατές μεταθέσεις.

Παρατηρήσεις

(5) Με τους συμβολισμούς της προηγουμένης πρότασης, η S_3 περιλαμβάνει τις υποομάδες $\{e, t\}$ ισόμορφη της $\mathbb{Z}_2$ και την $\{e, s, s^2\}$ ισόμορφη της $\mathbb{Z}_3$. Ωστόσο η ομάδα δεν είναι ισόμορφη προς την $\mathbb{Z}_2 \times \mathbb{Z}_3$. Τούτο για τον απλούστατο λόγο ότι η τελευταία ομάδα είναι αβελιανή, ενώ η S_3 δεν είναι. Π.χ. $tst^{-1} = s^2 \Longrightarrow st \neq ts$.

(6) Γιά κάθε $m < n$ η S_m μπορεί να θεωρηθεί υποομάδα της S_n (ακριβέστερα, ισόμορφη προς υποομάδα της S_n). Πράγματι κάθε μετάθεση $t = \begin{pmatrix} 1\ 2\ \dots\ m \\ i_1\ \dots\ i_m \end{pmatrix} \in S_m$ μπορεί να

επεκταθεί με φυσιολογικό τρόπο σε μιά μετάθεση n στοιχείων, όπου τα τελευταία $n-m$ παραμένουν σταθερά: $t' = \begin{pmatrix} 1...m, m+1, ..., n \\ i_1...i_m, m+1, ..., n \end{pmatrix}$. Μπορούμε λοιπόν να ταυτίσουμε την S_m με την υποομάδα της S_n που αποτελείται από τις μεταθέσεις που αφήνουν τα $n-m$ τελευταία στοιχεία του $\underline{n}$ σταθερά.
(7) Κάθε μετάθεση $t \in S_n$ ορίζει την παραγόμενη υποομάδα $< t >= \{t, t^2, ...t^k\}$ ισόμορφη της $\mathbb{Z}_k$, όπου k η τάξη της t. Γιά κάθε στοιχείο $i \in \underline{n}$ προκύπτει το σύνολο $\{i, t(i), t^2(i), ..., t^{k-1}(i)\}$ που λέγεται **τροχιά** του i ως προς t. Οι τροχιές αυτές παίζουν ιδιαίτερο ρόλο στην ανάλυση μιάς μετάθεσης σε απλούστερες (τους κύκλους) που εξετάζουμε στην επόμενη παράγραφο.

Πρόταση 3.2.2 *Γιά δύο μεταθέσεις της* S_n $s = \begin{pmatrix} 1, 2, ..., n \\ i_1, ..., i_n \end{pmatrix}$ *και* $t \in S_n$, *ισχύει*

$$t' = tst^{-1} = \begin{pmatrix} t(1), ..., t(n) \\ t(i_1), ..., t(i_n) \end{pmatrix}.$$

.

Πράγματι, θεωρώντας τυχόν $x \in \underline{n}$ δείχνουμε ότι $t(x) = t'(x)$. Πράγματι έστω $u \in \underline{n} : x = t(u)$. Τότε $t'(x) = t'(t(u)) = tst^{-1}t(u) = ts(u) = t(i_u)$, που είναι ακριβώς το ζητούμενο.

ΠΡΟΒΛΗΜΑΤΑ 3.2

Πρόβλημα 3.2.1 *Δείξε ότι κάθε πεπερασμένη ομάδα* G, *τάξης* $|G| = n$, *είναι ισόμορφη με μιά υποομάδα της ομάδας* S_n. *(Υπόδειξη: Χρησιμοποίησε την 3.1.1.)*

Πρόβλημα 3.2.2 *Γράψε όλες τις μεταθέσεις των ομάδων* S_n, *γιά* $n = 2, 3, 4, 5, 6$.

Πρόβλημα 3.2.3 *Βρές το γινόμενο* ab, *όπου* $a, b \in S_4$ *οι μεταθέσεις:*

$$a = \begin{pmatrix} 1, 2, 3, 4 \\ 2, 4, 3, 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1, 2, 3, 4 \\ 3, 2, 1, 4 \end{pmatrix}.$$

Προσδιόρισε επίσης όλες τις δυνάμεις a^k, b^k, $\forall k \in \mathbb{Z}$.

Πρόβλημα 3.2.4 *Δείξε ότι οι υποομάδες της* S_4 , $A =< a >$, $B =< b >$, *που παράγονται από τα* a, b, *του προηγούμενου προβλήματος, δεν είναι ισόμορφες.*

Πρόβλημα 3.2.5 *Βρες όλες τις τροχιές των μεταθέσεων* a, b, *της άσκησης 3.2.3.*

3.3 Κύκλοι

Κύκλος ή κυκλική μετάθεση λέγεται μιά μετάθεση $t \in S_n$ που εναλλάσει κυκλικά k από τα στοιχεία του $\underline{n}$. $i_1 \mapsto i_2 \mapsto i_3 ... \mapsto i_k \mapsto i_1$. Γιά μιά τέτοια μετάθεση χρησιμοποιούμε τον συμβολισμό $t = (i_1, ..., i_k)$. Το k λέγεται **μήκος** του κύκλου

Παρατηρήσεις
(1) Τον ίδιο κύκλο μπορούμε να γράψουμε με πολλούς τρόπους $t = (i_1, ..., i_k) = (i_2, i_3, ..., i_k, i_1) = (i_3, i_4, ..., i_k, i_1, i_2) = ...$ χρησιμοποιώντας οποιαδήποτε κυκλική μετάθεση των στοιχείων

$(i_1, ..., i_k)$. Μπορούμε λοιπόν, κατά τον συμβολισμό του κύκλου, να φέρουμε στην πρώτη θέση ένα οποιοδήποτε στοιχείο του: $t = (i_s, i_{s+1}, ..., i_{s-1})$.
(2) Ο κύκλος $t = (i_1, ..., i_k)$ αφήνει σταθερά όλα τα άλλα στοιχεία του $\underline{n}$ που δεν συμμετέχουν σ' αυτόν. Τα στοιχεία αυτά λέγονται **αδρανή** στοιχεία του κύκλου. Τα $i_1, ..., i_k$ λέγονται ενεργά στοιχεία του κύκλου. Καθένα από τα ενεργά απεικονίζεται μέσω του κύκλου στο επόμενό του. Το τελευταίο απεικονίζεται στο πρώτο.
(3) Πρέπει να σημειώσουμε ότι ο συμβολισμός $t = (i_1, ..., i_k)$ αφήνει μιά ασάφεια ως προς το ποιό S_n θεωρούμε. Ο t θα μπορούσε να ανήκει σε οποιοδήποτε S_m αρκεί το m να είναι μεγαλύτερο ή ίσο όλων των i_s που συμμετέχουν στον κύκλο. Ετσι λ.χ. ο κύκλος $t = (3, 5, 2, 7)$ θα μπορούσε να ανήκει σε οποιαδήποτε απο τις ομάδες S_m με $m \geq 7$.
(4) Είναι προφανές ότι ο αντίστροφος του κύκλου $t = (i_1, ..., i_k)$ είναι πάλι κύκλος του ίδιου μήκους $t^{-1} = (i_k, ..., i_1)$.
(5) Οι δυνάμεις t^r ενός κύκλου δεν είναι εν γένει κύκλοι. Π.χ. γιά τον $t = (3, 5, 2, 7)$ έχουμε ότι $t^2 = (3, 2)(5, 7)$ που είναι γινόμενο δύο κύκλων. Πάντως γιά κάθε κύκλο t μήκους k θα έχουμε $t^k = e$. Επομένως ο αντίστροφος είναι $t^{-1} = t^{k-1}$.
(6) Συμπεραίνομε ότι γιά έναν κύκλο t μήκους k η κυκλική υποομάδα του S_n, $< t >= \{t, t^2, ..., t^k = e\}$ είναι ισόμορφη προς την $\mathbb{Z}_k$. Επίσης τα ενεργά στοιχεία του κύκλου $t = (i_1, ..., i_k)$ είναι $i_2 = t(i_1), i_3 = t^2(i_1), ..., i_k = t^{k-1}(i_1)$. Την ιδιότητα αυτή εκφράζουμε λέγοντας ότι η ομάδα $< t >$ **δρα απλά μεταβατικά** στο σύνολο $\{i_1, ..., i_k\}$ των ενεργών στοιχείων της. Στις ασκήσεις θα δούμε ότι αυτή η ιδιότητα χαρακτηρίζει τους κύκλους.

Πρόταση 3.3.1 *Δύο κύκλοι $t = (i_1, ..., i_k)$, $s = (j_1, ..., j_r)$ των οποίων τα σύνολα των ενεργών στοιχείων τους $\{i_1, ..., i_k\}$, $\{j_1, ..., j_r\}$ είναι ξένα μεταξύ τους, μετατίθενται: $ts = st$.*

Πράγματι, αρκεί να δείξουμε ότι $s(t(x)) = t(s(x))$ γιά κάθε $x \in \underline{n}$. Διακρίνουμε 3 περιπτώσεις. α) Αν το x είναι αδρανές και γιά τους δύο κύκλους, τότε $s(t(x)) = t(s(x)) = x$ αφού και οι δύο το αφήνουν σταθερό. β) Αν το x είναι αδρανές μόνο γιά τον t τότε $t(s(x)) = s(t(x)) = s(x)$ αφού τότε και το $s(x)$ θα είναι αδρανές του t. γ) Αν το x είναι αδρανές μόνο του s, τότε σκεφτόμενοι όπως στο β) βλέπουμε ότι $s(t(x)) = t(s(x)) = t(x)$. Κύκλους που πληρούν τις υποθέσεις της πρότασης τους λέμε **ξένους**.

Πρόταση 3.3.2 *Γιά δοθήσα μετάθεση $t = \begin{pmatrix} 1 & 2 & ... & n \\ i_1 & ... & & i_n \end{pmatrix}$ ορίζουμε την σχέση $\cong$ μεταξύ στοιχείων του $\underline{n}$: $x \cong y \Leftrightarrow \exists k \in \mathbb{Z} : t^k(x) = y$. Η σχέση αυτή είναι σχέση ισοδυναμίας και μιά κλάση $C = \{i_1, ..., i_r\}$ αυτής της σχέσης ισοδυναμίας γράφεται $C = \{t(i_1), t^2(i_1), ..., t^r(i_1) = i_1\}$.*

Κατ' αρχήν είναι εύκολο να δούμε ότι πράγματι αυτή η σχέση είναι σχέση ισοδυναμίας στο σύνολο $\underline{n}$. Εστω τώρα ότι $C = \{i_1, ..., i_r\}$ είναι μιά κλάση ισοδυναμίας ως προς αυτήν την σχέση. Θεωρούμε το σύνολο όλων των δυνάμεων $C' = \{t(i_1), ..., t^r(i_1)\}$ Τα στοιχεία του προηγουμένου συνόλου είναι ισοδύναμα του i_1 άρα μέσα στην ίδια μ' αυτό κλάση. Δηλαδή $C' \subseteq C$. Επίσης είναι διαφορετικά μεταξύ τους, διότι αν υπήρχε μιά επανάληψη $t^k(i_1) = t^m(i_1)$ με $k < m \leq r$ τότε θα είχαμε $t^{m-k}(i_1) = i_1$ και μόνον τα $t(i_1), ..., t^{m-k}(i_1)$ θα ήταν διαφορετικά , άρα η κλάση θα περιήχε μόνο $m - k < r$ στοιχεία. Άτοπο, αφού υποθέσαμε ότι το C περιέχει r στοιχεία. Γιά κάποιο εκθέτη s συνεπώς θα έχουμε $t^s(i_1) = i_1$. Και πάλι αν $s < r$ η κλάση θα περιήχε μόνο τα $t(i_1), ..., t^s(i_1)$ που είναι λιγώτερα από r. Άρα $t^r(i_1) = i_1$ και r είναι ο μικρότερος εκθέτης μ' αυτήν την ιδιότητα.

Πρόταση 3.3.3 *Κάθε μετάθεση $t \in S_n$ αναλύεται σε γινόμενο ξένων κύκλων $t = c_1 c_2 ... c_k$. Η ανάλυση αυτή είναι μοναδική, εκτός από αναδιάταξη των κύκλων.*

Σύμφωνα με την προηγούμενη πρόταση, κάθε κλάση $C = \{t(i_1), ..., t^r(i_1)\}$ ως προς την $\cong$ που ορίζει η t θα ορίζει και έναν κύκλο $c = (t(i_1), ..., t^r(i_1))$. Επειδή οι κλάσεις είναι ξένες μεταξύ τους και οι κύκλοι αυτοί θα είναι ξένοι μεταξύ τους. Αν λοιπόν $c_1, ..., c_k$ είναι οι κύκλοι που προκύπτουν μ' αυτήν την μέθοδο, αρκεί να δείξουμε ότι $t = c_1...c_k$ γράφεται σαν γινόμενο αυτών των κύκλων. Όμως το τυχόν $x \in \underline{n}$ ανήκει σε μία ακριβώς κλάση και χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε ότι το x είναι το t_1 του κύκλου c_1. Τότε το t_1 είναι αδρανές γιά όλους τους άλλους κύκλους και $c_1...c_k(x) = c_1(x) = t(x)$. Αυτό δείχνει ότι $c_1...c_k(x) = t(x)\ \forall\, x \in \underline{n}$ άρα $t = c_1...c_k$. Οι υπόλοιποι ισχυρισμοί είναι προφανείς (δες 3.3.1).

3.4 Παραδείγματα

(1) Έστω $t = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\,10 \\ 8\,2\,4\,3\,1\,5\,7\,6\,10\,9 \end{pmatrix}$. Ευρίσκουμε τους κύκλους της t παρακολουθώντας την τροχιά στοιχείων της. Ξεκινάμε από την τροχιά του $1 : t(1), t^2(1), t^3(1)...$ κ.ο.κ μέχρι να ξαναβρούμε το στοιχείο απ' το οποίο ξεκινήσαμε (το 1). Προκύπτει ο κύκλος: $(1\,8\,6\,5)$. Κατόπιν παίρνομε ένα στοιχείο που δεν ανήκει στον κύκλο αυτό και βρίσκομε την τροχιά του. Εδώ λ.χ. το μικρότερο στοιχείο που δεν ανήκει στον κύκλο είναι το 2, που δίδει τον κύκλο: (2). Κατόπιν το 3, που δίδει τον κύκλο: (3, 4). Κατόπιν το 7: (7). Κατόπιν τον 9, που δίδει τον κύκλο: (9, 10). Τελικά έχουμε $t = (1\,8\,6\,5)(2)(3,\,4)(7)(9,\,10)$.

(2) Συνήθως δεν γράφουμε τους μονοστοίχειους κύκλους που αντιστοιχούν σε αδρανή στοιχεία της αρχικής μετάθεσης. Έτσι γράφουμε $t = (1\,8\,6\,5)(3,\,4)(9,\,10)$. Ενοούμε ότι όποιο στοιχείο δεν εμφανίζεται σε κανένα κύκλο παραμένει σταθερό.

(3) Έστω $t = \begin{pmatrix} 1\,2\,3\,4\,5\,6\,7\,8\,9\,10 \\ 4\,2\,9\,5\,1\,8\,7\,6\,10\,3 \end{pmatrix}$. Προκύπτει $t = (1\,4\,5)(3\,9\,10)(6\,8)$.

(4) Στην αντίστροφη κατασκευή, της μετάθεσης από δοθέντες κύκλους, πρέπει να ξέρουμε το n γιά το οποίο $t \in S_n$. Έτσι η $t = (1\,3\,5)(7\,9\,6)$ μπορεί να θεωρηθεί ότι ανήκει στο S_n γιά οποιοδήποτε $n \geq 9$.

(5) Από την ανάλυση της t σε κύκλους συμπεραίνουμε αμέσως την τάξη της. Π.χ. γιά την προηγούμενη $t = (1\,3\,5)(7\,9\,6)$ η τάξη θα είναι 3, αφού $t^3 = (1\,3\,5)^3(7\,9\,6)^3 = ee = e$ και μάλιστα ανεξάρτητα του S_n στο οποίο θεωρούμε ότι περιέχεται η t. Ο κανόνας γενικεύεται στην επόμενη πρόταση. Προκύπτει επίσης το ενδιαφέρον ερώτημα: Ποιά είναι η μέγιστη δυνατή τάξη που μπορεί να έχει μιά μετάθεση $t \in S_n$;

Πρόταση 3.4.1 *Η τάξη μιάς μετάθεσης είναι το ελάχιστο κοινό πολλαπλάσιο των μηκών των κύκλων της.*

Πράγματι, αν $t = c_1...c_r$ είναι η ανάλυση σε κύκλους, τότε λόγω της μεταθετικότητας των ξένων κύκλων θα έχουμε $t^s = c_1^s...c_r^s$ γιά κάθε ακέραιο $s \in \mathbb{Z}$. Αν το s είναι το ελάχιστο κοινό πολλαπλάσιο των μηκών των κύκλων, τότε κάθε ένας από τους παράγοντες $c_i^s = e$. Προφανές επίσης και το αντίστροφο. Δηλαδή ότι αν $t^s = e$ τότε το s θα πρέπει να είναι πολλαπλάσιο κάθε ενός από τα μήκη των κύκλων, άρα να διαιρήται με το ελάχιστο κοινό πολλαπλάσιο αυτών.

Πρόταση 3.4.2 *Γιά κάθε κύκλο $s = (i_1, ..., i_k)$ και μετάθεση $t \in S_n$ και η συζυγής tst^{-1} είναι κύκλος και ισχύει $tst^{-1} = (t(i_1), ..., t(i_k))$. Αντίστροφα, γιά κάθε άλλο κύκλο $s' = (j_1, ..., j_k)$ του ιδίου μήκους με τον s υπάρχει $t \in S_n$ έτσι ώστε $s' = tst^{-1}$.*
Με άλλα λόγια, κάθε δύο κύκλοι του ιδίου μήκους είναι συζυγείς.

Πράγματι, κατά την 3.2.2 η $t' = tst^{-1}$ θα απεικονίζει το $t(i_1) \mapsto t(i_2) \mapsto t(i_2) \mapsto ...$ όπως ακριβώς ο κύκλος $(t(i_1), ..., t(i_k))$. Γιά το αντίστροφο αρκεί να πάρουμε την μετάθεση t που απεικονίζει $i_1 \mapsto j_1$ $i_2 \mapsto j_2 ...$ κ.τ.λ. και να εφαρμόσουμε το ευθύ.

Παρατηρήσεις
(1) Κάθε μετάθεση $t \in S_n$, με την διάσπαση σε κύκλους μηκών $k_1, ..., k_r$, καθορίζει και μία διαμέριση του n σε άθροισμα θετικών ακεραίων , αφού $n = k_1 + k_2 + ... + k_r$.
(2) Η προηγούμενη πρόταση δείχνει ότι δύο μεταθέσεις είναι συζυγείς τότε και μόνον τότε, όταν ορίζουν την ίδια διαμέριση του n.
(3) Από την διαμέριση επίσης μπορούμε να βρούμε την τάξη της μετάθεσης, ως το ελάχιστο κοινό πολλαπλάσιο των $k_1, ..., k_r$.
(4) Η προηγούμενη παρατήρηση έχει σαν συνέπεια κάποιους περιορισμούς για το ποιοι κύκλοι μπορούν να συμμετέχουν σε μιά μετάθεση δεδομένης τάξης. Έτσι λ.χ. στην S_4 τα στοιχεία τάξης 3, δεν μπορεί παρά να είναι αυτούσιοι 3-κύκλοι (διαμέριση 4=3+1). Παρόμοια στην S_5 στοιχείο τάξης 3 μπορεί να είναι μόνο αυτούσιος κύκλος (διαμέριση 5=3+1+1). Στην S_6 ωστόσο έχουμε στοιχείο τάξης 3 που είναι γινόμενο δύο κύκλων (διαμέριση 6=3+3).

3.5 Αντιμεταθέσεις

Αντιμετάθεση λέγεται ένας κύκλος μήκους δύο: $(i_i\ i_2)$. Με άλλα λόγια μιά μετάθεση που εναλλάσσει δύο και μόνον στοιχεία του $\underline{n}$, τα i_1, i_2 και αφήνει όλα τα υπόλοιπα $n-2$ σταθερά.

Παρατηρήσεις
(1) Προφανώς για μιά αντιμετάθεση $t \in S_n$ έχουμε $t^2 = e$. Ισοδύναμα $t^{-1} = t$.
(2) Αντίστροφα, αν γιά μιά μετάθεση ξέρουμε ότι $t^2 = e$, τότε δεν μπορεί παρά οι κύκλοι της να έχουν το πολύ μήκος 2. Άρα θα είναι γινόμενο ξένων αντιμεταθέσεων. Η επόμενη πρόταση δείχνει ότι και κάθε κύκλος είναι γινόμενο αντιμεταθέσεων, όχι όμως ξένων μεταξύ τους.

Πρόταση 3.5.1 *Κάθε κύκλος* $t = (i_1 ... i_k) = (i_2 ... i_k)(i_k\ i_1) = (i_k\ i_1)(i_1 ... i_{k-1})$. *Συνεπώς:*
(1) $t = (i_1 ... i_k) = (i_k\ i_{k-1}) ... (i_k\ i_3)(i_k\ i_2)(i_k\ i_1)$.
(2) $t = (i_1 ... i_k) = (i_k\ i_1)(i_{k-1}\ i_1)(i_{k-2}\ i_1) ... (i_2\ i_1)$.
Με άλλα λόγια, κάθε κύκλος μήκους μεγαλύτερου του 2 γράφεται σαν γινόμενο μη-ξένων αντιμεταθέσεων και μάλιστα με περισσότερους από έναν τρόπους.

Ο πρώτος ισχυρισμός αποδεικνύεται εφαρμόζοντας τις αντίστοιχες μεταθέσεις t και $t' = (i_2 ... i_k)(i_k\ i_1)$ σε ένα $x \in \underline{n}$. Προφανώς $t(x) = t'(x)$ γιά $x \in \{i_2, ..., i_{k-1}\}$. Βλέπουμε όμως αμέσως και ότι $t(x) = t'(x)$ γιά $x = i_1$ και $x = i_k$. Άρα $t(x) = t'(x)$ γιά κάθε $x \in \underline{n}$, άρα $t = t'$. Η δεύτερη ισότητα προκύπτει με ανάλογο συλλογισμό. Οι υπόλοιποι ισχυρισμοί προκύπτουν με απλή επαγωγή.

Πρόταση 3.5.2 *Κάθε μετάθεση* $t \in S_n$ *γράφεται σαν γινόμενο αντιμεταθέσεων.*

Τούτο είναι πάλι άμεση συνέπεια της προηγούμενης πρότασης και του γεγονότος ότι κάθε κύκλος γράφεται σαν γινόμενο αντιμεταθέσεων.

Πρόταση 3.5.3 *Οι αντιμεταθέσεις* $(12), ... (1n)$ *παράγουν την* S_n.

Αρκεί να παρατηρήσουμε ότι η τυχαία αντιμετάθεση $(ij) \in S_n$ γράφεται σαν γινόμενο:

$$(ij) = (1i)(1j)(1i),\ i \neq 1 \neq j,$$

και να εφαρμόσουμε την 3.5.2.

Πρόταση 3.5.4 *Οι μεταθέσεις $s = (12)$, $t = (1\,2\,....\,n)$ παράγουν την S_n.*

Τούτο αποδεικνύεται πάλι με μερικές απλές παρατηρήσεις: (α) το t^{j-1} απεικονίζει το $1 \mapsto j$, $2 \mapsto j+1$. Άρα (3.2.2) $(j\,,j+1) = t^{j-1}st^{1-j}$. Επομένως,

$$(\beta)\quad (1\,,j+1) = (j\,,j+1)(1j)(j\,,j+1) = t^{j-1}st^{1-j}(1j)t^{j-1}st^{1-j}.$$

Το (β) δείχνει ότι αν το $(1j)$ ανήκει στο σύνολο των στοιχείων που παράγονται από τα αρχικά s, t τότε και το $(1\,,j+1)$ ανήκει στο ίδιο σύνολο. Επομένως, επαγωγικά, οι μεταθέσεις $(12)\,,(13)\,,...\,(1n)$ παράγονται, όλες, από τα $s\,,t$, άρα (προηγούμενη πρόταση) και όλες οι μεταθέσεις παράγονται απ' αυτά τα δύο στοιχεία.

3.6 Πρόσημο μετάθεσης

Πρόσημο μετάθεσης $t \in S_n$ λέγεται ο αριθμός $sign(t) = \prod_{i<j} \frac{t(i)-t(j)}{i-j}$.
Σημείωσε ότι κάθε αριθμός που εμφανίζεται στον αριθμητή, εμφανίζεται και στον παρανομαστή, ενδεχομένως με διαφορετικό πρόσημο. Επομένως το πρόσημο είναι πάντοτε ίσο με ± 1.

Πρόταση 3.6.1 *Γιά δύο μεταθέσεις $t, s \in S_n$ ισχύει $sign(t) = \prod_{i<j} \frac{t(s(i))-t(s(j))}{s(i)-s(j)}$.*

Πράγματι στο τελευταίο γινόμενο, ο τυπικός όρος $\frac{t(s(i))-t(s(j))}{s(i)-s(j)}$ συμπίπτει με έναν τυπικό όρο του αρχικού ορισμού, αν $s(i) - s(j) < 0$. Αν $s(i) - s(j) > 0$ τότε αντιστρέφοντας τα πρόσημα σε παρανομαστή και αριθμητή έχουμε ότι $\frac{t(s(j))-t(s(i))}{s(j)-s(i)}$ συμπίπτει με κάποιον τυπικό όρο του αρχικού γινομένου. Σε κάθε περίπτωση λοιπόν το νέο γινόμενο θα αποτελείται από τους ίδιους παράγοντες με εκείνους του αρχικού ορισμού.

Πρόταση 3.6.2 *Γιά δύο μεταθέσεις $t, s \in S_n$ ισχύει $sign(ts) = sign(t)sign(s)$. Με άλλα λόγια η $sign$ είναι ένας ομομορφισμός ομάδων $sign : S_n \longrightarrow \{-1, +1\}$.*

Πράγματι, κατά τον ορισμό $sign(ts) = \prod_{i<j} \frac{ts(i)-ts(j)}{i-j} = \prod_{i<j} \frac{ts(i)-ts(j)}{i-j} \prod_{i<j} \frac{s(i)-s(j)}{s(i)-s(j)} = \prod_{i<j} \frac{ts(i)-ts(j)}{s(i)-s(j)} \prod_{i<j} \frac{s(i)-s(j)}{i-j}$. Σύμφωνα όμως με την προηγούμενη πρόταση, το πρώτο γινόμενο είναι το $sign(t)$ ενώ το δεύτερο το $sign(s)$.

Πρόταση 3.6.3 *Γιά μιά αντιμετάθεση $t = (k\,m)$ $k < m$ ισχύει $sign(t) = (-1)^{2(m-k-1)+1} = -1$.*

Δεν έχουμε παρά να παρατηρήσουμε στον ορισμό του $sign$ πόσα $s(i) - s(j)$ είναι θετικά, άρα συνισφέρουν ένα -1 στο συνολικό γινόμενο. Ομως στην διάταξη $1\ 2\ ...k\ ...\,m\ ...\,n$ η εναλλαγή των k, m: δημιουργεί την διάταξη $1\ 2\ ...k\ ...\,m\ ...\,n$ στην οποία τα μόνα ζεύγη με $s(i) - s(j) > 0$ είναι τα $(i, i+1)$, ..., $(i, j-1)$ καθώς και τα $(i+1, j)$, ..., $(j-1, j)$ και τέλος το (i, j).

Πρόταση 3.6.4 *Γιά μιά μετάθεση $t \in S_n$ ισχύει $sign(t) = \pm 1$ ανάλλογα με το αν η μετάθεση αναλύεται σε γινόμενο αρτίου πλήθους $(+1)$ ή περιττού πλήθους αντιμεταθέσεων (-1). Άρα με όσους τρόπους και αν γράψουμε την μετάθεση ως γινόμενο αντιμεταθέσεων θα χρησιμοποιούμε πάντοτε άρτιο ή περιττό πλήθος αντιμεταθέσεων, ανάλογα με το πρόσημό της. Μεταθέσεις με πρόσημο $+1$ τις λέμε* **άρτιες**. *Μεταθέσεις με πρόσημο -1 τις λέμε* **περιττές**.

Κατά την 3.5.2, κάθε μετάθεση $t \in S_n$ αναλύεται σε γινόμενο αντιμεταθέσεων $t = p_1 ... p_k$. Άρα $sign(t) = sign(p_1) ... sign(p_k)$. Κατά την προηγούμενη δε πρόταση κάθε αντιμετάθεση συνισφέρει ένα -1 στο προηγούμενο γινόμενο.

3.7 Η εναλλακτική ομάδα

Εναλλακτική ομάδα A_n λέγεται η υποομάδα $A_n \subset S_n$ των αρτίων μεταθέσεων. Το ότι το σύνολο των αρτίων μεταθέσεων είναι υποομάδα είναι προφανές. Η A_n είναι ο πυρήνας της $sign$, $A_n = Kern(sign) \subset S_n$. Γιά τυχούσα μετάθεση $t \in A_n$ το γινόμενο με την αντιμετάθεση $(1\,2)$ ορίζει μετάθεση $(1\,2)t$ αντιθέτου προσήμου απ' αυτό της t. Αυτό δείχνει ότι οι άρτιες μεταθέσεις είναι όσες και οι περιττές άρα $|A_n| = \frac{n!}{2}$.

Παραδείγματα
(1) A_3 είναι το πρώτο ενδιαφέρον παράδειγμα και αποτελείται από τις μεταθέσεις $a = (12)(23)$, $b = (12)(13) = (13)(23)$, e. Βλέπουμε αμέσως ότι $a^2 = b$ και ότι η ομάδα είναι ισόμορφη με την $\mathbb{Z}_3$.
(2) Το επόμενο παράδειγμα είναι η A_4 με 12 στοιχεία: e, (123), (132), (124), (142), (134) (143), (234) (243), $(12)(34)$, $(13)(24)$ και $(14)(23)$.

Πρόταση 3.7.1 *Γιά $n \geq 3$ οι 3-κύκλοι: (123), (124), ... $(12n)$ παράγουν την A_n. Με άλλα λόγια κάθε άρτια μετάθεση γράφεται σαν γινόμενο αυτών των κύκλων.*

Πράγματι, εξ' ορισμού στην ανάλυση μιάς άρτιας μετάθεσης $t = p_1 p_2 ... p_k$ σε αντιμεταθέσεις, σύμφωνα με την 3.5.3, το πλήθος k θα είναι άρτιος. Άρα μπορούμε να τις πάρουμε ανά δύο $p_1 p_2 = (1\,i_1)(1\,i_2)$, $p_3 p_4 = (1\,i_3)(1\,i_4)$, ..., κ.ο.κ. Ισχύει όμως

$$(1\,j)(1\,i) = (1ij)$$

$$(1ij) = (1j2)(12i)(12j) = (12j)^2(12i)(12j)$$

.

Πρόταση 3.7.2 *Για $n \geq 3$ αν η κανονική υποομάδα $N \subseteq A_n$ περιέχει έναν 3-κύκλο, τότε περιέχει όλους τους 3-κύκλους και συνεπώς $N = A_n$.*

Πράγματι, κατά την 3.4.2 όλοι οι 3-κύκλοι είναι μεταξύ τους συζυγείς. Άρα η ομάδα N ούσα κανονική και περιέχουσα έναν απ' αυτούς θα τους περιέχει όλους. Τότε όμως, κατά την προηγούμενη πρόταση θα περιέχει και ολόκληρη την A_n.

Πρόταση 3.7.3 *Γιά $n \geq 5$ η A_n είναι απλή, δηλαδή δεν έχει καμμία κανονική υποομάδα.*

Θεωρούμε μία κανονική υποομάδα $N \subseteq A_n$. Θα δείξουμε ότι η N ταυτίζεται με την A_n. Προς τούτο θεωρούμε ένα στοιχείο $t \in N$ που έχει το ελάχιστο δυνατόν πλήθος ενεργών στοιχείων d μεταξύ όλων των στοιχείων της N. Προφανώς $d \geq 3$. Αν ήταν $d = 3$, τότε η

N θα περιήχε έναν 3-κύκλο και κατά την προηγούμενη πρόταση θα είχαμε αμέσως $N = A_n$. Θα δείξουμε τώρα ότι $d > 3$ οδηγεί σε άτοπο. Προς τούτο αναλύουμε την t σε κύκλους:
(1) $t = (i_1\, i_2)(i_3\, i_4)...$ αν η t δεν περιέχει κύκλους μήκους > 2, ή
(2) $t = (i_1\, i_2, i_3\, ...)...$ αν η t περιέχει κύκλους μήκους > 2.
Στην δεύτερη περίπτωση, η t θα πρέπει να έχει δύο ακόμη τουλάχιστον ενεργά στοιχεία i_4, i_5. Τότε παίρνοντας τα συζυγή των προηγουμένων $t' = sts^{-1} \in N$ με $s = (i_3\, i_4\, i_5)$, έχουμε αντίστοιχα:
(1′) $t' = (i_1\, i_2)(i_4\, i_5)...$ στην περίπτωση (1),
(2′) $t' = (i_1\, i_2\, i_4\, ...)...$ στην περίπτωση (2).
Προφανώς $t' \neq t$ άρα $t'' = t^{-1}t' \neq e$. Στην t'', στην πρώτη περίπτωση προστίθεται το πολυ ένα ενεργό στοιχείο, το i_5, ενώ τα i_1, i_2 καθίστανται αδρανή. Άρα βρίσκουμε νέα μετάθεση $t'' \in N$ με $d-1$ ή λιγώτερα ενεργά στοιχεία, πράγμα που αντιφάσκει στην επιλογή του $t \in N$. Παρόμοια στην δεύτερη περίπτωση, ένα αδρανές στοιχείο της t θα είναι αδρανές και γιά την t''. Όμως η t'' έχει επιπρόσθετα το i_1 αδρανές ενώ η t το έχει ενεργό. Πάλι λοιπόν έχουμε αντίφαση προς την επιλογή του $t \in N$ να έχει ελάχιστο πλήθος ενεργών στοιχείων. Αυτό ολοκληρώνει την απόδειξη.

ΠΡΟΒΛΗΜΑΤΑ 3.7

Πρόβλημα 3.7.1 *Γιά κάθε μία από τις επόμενες μεταθέσεις προσδιόρισε τους κύκλους της και βρες αν είναι άρτια ή περιττή: α)* $\begin{pmatrix} 1234 \\ 3412 \end{pmatrix}$ *, β)* $\begin{pmatrix} 123456 \\ 621543 \end{pmatrix}$ *γ)* $\begin{pmatrix} 123456789 \\ 321458679 \end{pmatrix}$ *.*

Πρόβλημα 3.7.2 *Βρες τα στοιχεία $t \in S_5$, που μετατίθενται με τον κύκλο* (12345)*.*

Πρόβλημα 3.7.3 *Δείξε ότι οι μεταθέσεις* e, $(12)(34)$, $(13)(24)$, $(14)(23)$ *αποτελούν υποομάδα της A_4. Δείξε ότι η υποομάδα αυτή είναι κανονική. Η ομάδα αυτή συμβολίζεται συνήθως με V_4 και λέγεται* **4-ομάδα του Klein***. Δείξε ότι η ομάδα αυτή είναι ισόμορφη προς την $\mathbb{Z}_2 \times \mathbb{Z}_2$ που συναντήσαμε στην 2.4.5.*

Πρόβλημα 3.7.4 *Δείξε ότι γιά $n \geq 2$ οι $n-1$ μεταθέσεις* (12) (23) ... $(n-1\, ,n)$ *παράγουν την S_n.*

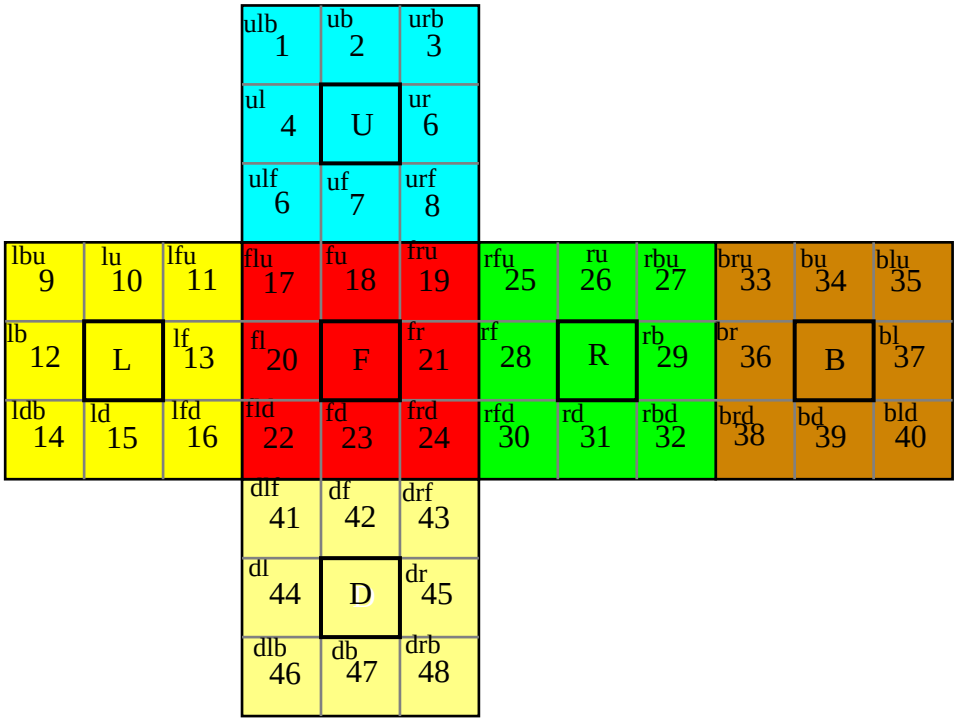
Πρόβλημα 3.7.5 *Δείξε ότι δύο μεταθέσεις $s, t \in S_n$ είναι συζυγείς τότε και μόνον όταν υπάρχει αμφιμονοσήμαντη αντιστοιχία μεταξύ των κύκλων τους, έτσι ώστε αντίστοιχοι κύκλοι να έχουν ίδιο μήκος.*

Πρόβλημα 3.7.6 *Δείξε ότι η A_4 δεν περιέχει καμμία υποομάδα τάξης 6 (παρόλο που το 6 διαιρεί το 12).*

Πρόβλημα 3.7.7 *Δείξε ότι τα στοιχεία $t = (1\, 2\, ...\, n)$ και $s = (1\, 2)$ ικανοποιούν $tst^{-1} = (2\, 3)\, , t^2st^{-2} = (3\, 4)\, , ... t^{n-2}st^{2-n} = ((n-1)\, n)$. Δείξε επίσης την $(1\, 2)(2\, 3)...((n-1)\, n) = (1\, 2\, ...\, n)$. Συμπέρανε ότι $(st)^{n-1} = e$.*

Πρόβλημα 3.7.8 *Δείξε ότι οι κύκλοι $s = (1\, 2)$, $t = (1\, 2\, 3)$, ικανοποιούν τις $s^2 = e$, $t^3 = e$, $sts^{-1} = t^2$. Συμπέρανε ότι μιά ομάδα που παράγεται από δύο στοιχεία και ικανοποιεί αυτές τις σχέσεις: $G =< s, t : \ s^2 = e,\ t^3 = e,\ sts^{-1} = t^2 >$, είναι ισόμορφη προς την S_3.*

3.8 Ο κύβος του Rubik



Σχήμα 3.1: Ο κύβος του Rubik

Ο κύβος του Rubik αποτελείται από $27 = 3 \times 9$ μικρότερους ίσους κύβους, συνδεδεμένους μεταξύ τους έτσι ώστε κάθε έδρα του να μπορεί να περιστρέφεται περί το κέντρο της. Τα κέντρα των εδρών μπορούν να θεωρηθούν ακίνητα. Στο σχήμα 3.1 παρίσταται ο κύβος με τις 6 έδρες του ανεπτυγμένες σ' ένα επίπεδο και τις έδρες των μικρότερων κύβων αριθμημένες. Οι επιτρεπόμενες κινήσεις είναι στροφές (κατά 90°) περί τα κέντρα U, L, F, R, B, D των εδρών του κύβου. Τα ονόματα προέρχονται από τις αντίστοιχες αγγλικές λέξεις (U = Up(πάνω), L = Left(αριστερά) κτλ.). Μετά από μιά σειρά επιτρεπομένων κινήσεων οι μικρές έδρες (τις ονομάζω **εδρίδια**) θα έχουν αναδιαταχθεί, συνεπώς θα δίνουν μιά μετάθεση του S_{48}. Το πρόβλημα είναι, ξεκινώντας από μιά οποιαδήποτε δυνατή θέση να καταλλήξουμε, μέσω επαλληλίας επιτρεπομένων κινήσεων, στην μορφή του σχήματος 3.1, που ονομάζουμε κανονική (αντιστοιχεί στην ταυτοτική μετάθεση $e \in S_{48}$) και στην οποία όλα τα εδρίδια του ιδίου χρώματος είναι στην ίδια έδρα του κύβου. Οι στροφές περί τα κέντρα των εδρών αντιστοιχούν σε μεταθέσεις της S_{48} που αναλύονται σε 4-κύκλους:

$$
\begin{aligned}
F &= (17,19,24,29)(18,21,23,20)(6,25,43,16)(7,28,4213)(8,30,41,11),\\
B &= (33,35,40,38)(34,37,39,36)(3,9,46,32)(2,12,47,29)(1,14,48,27),\\
L &= (9,11,16,14)(10,13,15,12)(1,17,41,40)(4,20,44,37)(6,22,46,35),\\
R &= (25,27,32,30)(26,29,31,28)(3,38,43,19)(5,36,45,21)(8,33,48,24),\\
U &= (1,3,8,6)(2,5,7,4)(9,33,25,17)(10,34,26,18)(11,35,27,19),\\
D &= (41,43,48,46)(42,45,47,44)(14,22,30,38)(15,23,31,39)(16,24,32,40).
\end{aligned}
$$

Η υποομάδα της S_{48} που παράγεται από τις 6 αυτές μεταθέσεις $G =< F, B, L, R, U, D > \subset S_{48}$, λέγεται **ομάδα του κύβου Rubik**. Οι στροφές F, B, ... κτλ. γίνονται κατά την φορά

του ρολογιού. Οι F^{-1}, B^{-1}... κτλ. γίνονται κατ' αντίθετη φορά.

Παρατηρήσεις

(1) Το πρώτο που πρέπει να παρατηρήσει ο παίκτης είναι η σταθερότητα των σχετικών θέσεων των κεντρικών εδριδίων. Το κόκκινο έχει αντίποδα πάντοτε το καφέ, το πράσινο έχει πάντοτε αντίποδα το κίτρινο κτλ. Κατά την διάρκεια του παιχνιδιού ο παίκτης, συνήθως, δεν προσέχει να διατηρεί την θέση των κέντρων των εδρών του κύβου σταθερή. π.χ. το κόκκινο εδρίδιο, $F = Front$ (μπροστά) να παραμένει πάντοτε μπροστά στα μάτια του. Αυτό σημαίνει ότι κάνει περιττές κινήσεις, στρέφοντας ολόκληρο τον κύβο με διάφορους τρόπους, ενδεχομένως απαραίτητες, για να διευκολύνει τα χέρια του να πραγματοποιήσουν τις απαραίτητες στροφές.

(2) Η προηγούμενη παρατήρηση οδηγεί σε μιά φυσική ονοματοθεσία των εδριδίων. Τα εδρίδια παίρνουν το πρώτο γράμμα του όνοματός τους από την έδρα του μεγάλου κύβου στην οποία περιέχονται. Τα υπόλοιπα γράμματα του εδριδίου αντιστοιχούν στις έδρες με τις οποίες συνορεύουν. Στην περίπτωση των τριών γραμμάτων, η τάξη των δύο τελευταίων δεν παίζει ρόλο.

(3) Το σύνολο των 48 εδριδίων χωρίζεται σε δύο ισοπληθικά σύνολα: V το σύνολο των εδριδίων σε κορυφές, που αποτελείται από $8 \times 3 = 24$, με ονόματα 3 γραμμάτων και το σύνολο E των εδριδίων σε ακμές, που αποτελείται από $12 \times 2 = 24$ εδρίδια και ονόματα δύο γραμμάτων. Έχει καθιερωθεί τα εδρίδια του V να λέγονται **κορυφές** και τα υπόλοιπα **ακμές**. Κύβοι που περιέχουν κορυφές λέγονται **κύβοι-κορυφών** και και κύβοι που περιέχουν ακμές λέγονται **κύβοι-ακμών**.

(4) Η επίλυση του προβλήματος, ξεκινώντας από μιά τυχαία θέση, και κάνοντας τυχαίες κινήσεις, φαίνεται μάλλον απίθανη, αφού η τάξη της ομάδος υπολογίζεται ότι είναι $|G| = 2^{37} * 3^{14} * 5^3 * 7^2 * 11 = 44.290.051.353.077.612.544.000$.

(5) Μιά θεμελιώδης παρατήρηση, στην οποία στηρίζονται όλες οι στρατηγικές επίλυσης, είναι ότι η ομάδα G έχει δύο τροχιές που συμπίπτουν ακριβώς με τα σύνολα V και E (για την έννοια της τροχιάς δες 6.3). Ο παίκτης το αντιλαμβάνεται βλέποντας ότι όποια κίνηση κι' αν κάνει, κορυφές θα πηγαίνουν σε κορυφές και ακμές σε ακμές. Μιά βασική λοιπόν στρατηγική είναι (α) να τοποθετηθούν πρώτα οι κύβοι-κορυφών στις σωστές θέσεις τους, (β) να τοποθετηθούν οι κύβοι-ακμών στις σωστές θέσεις, (γ) να διορθωθούν ενδεχόμενοι λανθασμένοι προσανατολισμοί των μικρών κύβων. Παρακάτω περιγράφεται λεπτομερώς αυτή η στρατηγική επίλυσης.

(6) **Σωστή θέση** ενός κύβου-κορυφής είναι αυτή κατά την οποία, τα χρωματά του είναι τα ίδια μ' αυτά των κέντρων των εδρών του, ενδεχομένως σε άλλη διάταξη. Ανάλογα ορίζεται και η σωστή θέση ενός κύβου-ακμής.

(7) Η συστηματική αντιμετώπιση του προβλήματος απαιτεί αρκετές γνώσεις της θεωρίας ομάδων και όχι μόνον. Μιά εισαγωγή στο θέμα και γενικώτερα τις σχέσεις ομάδων με διάφορα παιχνίδια, δίνει το βιβλίο του David Joyner, Adventures in Group Theory, Baltimore 2002. Στο βιβλίο αυτό στηρίζονται και οι σημειώσεις αυτής της παραγράφου, με μιά διαφορά στην διάταξη εφαρμογής λέξεων κινήσεων. Στο βιβλίο εφαρμόζονται οι κινήσεις μιάς λέξεως της ομάδας από αριστερά προς τα δεξιά, ενώ εδώ (για λόγους συνέπειας με τις άλλες παραγράφους) εφαρμόζονται από τα δεξιά προς τα αριστερά.

Στρατηγική επίλυσης

(1) Χρησιμοποιώντας μεταθέτες $[a, b] = aba^{-1}b^{-1}$ (εδώ λίγο διαφορετικός από τον ορισμό της 2.7), μετατοπίζουμε κύβο κορυφής A σε άλλο κύβο κορυφής B, προξενώντας μικρές

μόνον άλλαγές στους άλλους κύβους. Π.χ. ο μεταθέτης

$$K_1 = [D^{-1}, R] = D^{-1}RDR^{-1},$$

εναλλάσσει τους κύβους-κορυφών lfd και urf.
(2) Σε ορισμένες περιπτώσεις, χρησιμοποιώντας τέτοιες κινήσεις, τοποθετούνται όλοι οι κύβοι-κορυφών στις σωστές θέσεις τους. Σε γενικώτερες περιπτώσεις, με τέτοιες κινήσεις, τοποθετούνται όλοι οι κύβοι-κορυφών στις θέσεις τους, εκτός (α): δύο κύβων που πρέπει να αντιμετατεθούν , (β): τριών κύβων που πρέπει να μετατεθούν κυκλικά.
(3) Στην (α) περίπτωση, η κίνηση

$$K_2 = F^{-1}[U^{-1}, R^{-1}]^3FU = F^{-1}(U^{-1}R^{-1}UR)(U^{-1}R^{-1}UR)(U^{-1}R^{-1}UR)FU,$$

εναλλάσσει τους κύβους που περιέχουν τα urb, και ulf και μεταθέτει τις ακμές uf, ul, ub, ur, αφήνοντας τα υπόλοιπα εδρίδια αμετάβλητα.
(4) Στην (β) περίπτωση, κίνηση

$$K_3 = [U^{-1}, R^{-1}D^{-1}R] = U^{-1}R^{-1}D^{-1}RUR^{-1}DR,$$

μεταθέτει κυκλικά τους κύβους κορυφών brd, urb, ulb, αφήνοντας τους υπόλοιπους κύβους στην θέση τους.
(5) Μιά γενικώτερη εναλλαγή κύβων-κορυφών A, B, μπορούμε να την ανάγουμε στην προηγούμενη ειδική, μετατοπίζοντας πρώτα τον A στην θέση του urb, με κινήσεις $a = a_1a_2...$, τον B στην θέση του ulf, με κινήσεις $b = b_1b_2...$, κάνοντας την διαδικασία εναλλαγής των urb, ulf, όπως παραπάνω, με την K_2, και συμπληρώνοντας με τις αντίστροφες κινήσεις, με άλλα λόγια, χρησιμοποιώντας την συζυγή κίνηση $K' = a^{-1}b^{-1}Kba$. Το τέχνασμα αυτό ονομάζω **τέχνασμα αναγωγής**.
(6) Κύβοι-ακμών έρχονται στην σωστή θέση χρησιμοποιώντας κατ' επανάληψη την κίνηση:

$$K_4 = M_R^2U^{-1}M_RU^2M_R^{-1}U^{-1}M_R^2, \quad (K_4^{-1} = M_R^{-2}UM_RU^{-2}M_R^{-1}UM_R^{-2}),$$

όπου M_R συμβολίζει την στροφή, κατά 90°, με την φορά του ρολογιού, της μεσαίας φέτας, παράλληλης προς την R έδρα. Η κίνηση K_4 κάνει κυκλική μετάθεση των ακμών (uf, ul, ur) και αφήνει τα υπόλοιπα εδρίδια αμετάβλητα. Και εδώ σε γενικώτερες περιπτώσεις χρησιμοποιήται ανάλογο τέχνασμα αναγωγής γιά κύβους-ακμών.
(7) Η κίνηση που περιστρέφει ένα κύβο-κορυφής ωστε να τοποθετηθούν τα χρώματα στην σωστή θέση είναι του τύπου

$$K_5 = (BU^2B^{-1}RD^2R^{-1})^2, \quad (K_5^{-1} = (RD^{-2}R^{-1}BU^{-2}B^{-1})^2).$$

Η K_5 περιστρέφει το ufr κατά την φορά του ρολογιού και το bld κατά την αντίστροφη φορά, αφήνοντας τα υπόλοιπα εδρίδια αμετάβλητα. Το τέχνασμα αναγωγής (4) χρησιμοποιήται γιά τις υπόλοιπες περιπτώσεις.
(8) Οι κινήσεις που εναλλάσουν τα εδρίδια κύβων-ακμών, ώστε να τοποθετηθούν σωστά τα χρώματά τους είναι:

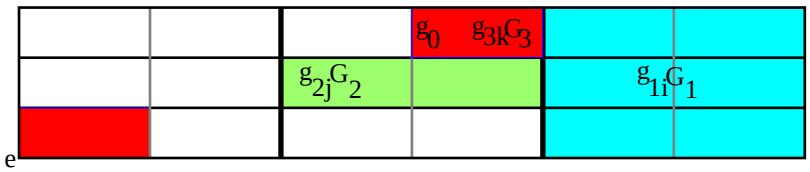
$$K_6 = U(UM_R^{-1})^3U(UM_R)^3, \qquad K_7 = (UM_R)^4.$$

Η K_6 εναλλάσσει τα uf, fu και ub, bu. Η K_7 εναλλάσσει τα εδρίδια των ub, ul και των df, db, αφήνοντας τα άλλα εδρίδια αμετάβλητα. Και εδώ σε γενικώτερες περιπτώσεις χρησιμοποιήται τέχνασμα αναγωγής γιά κύβους-ακμών.

(9) Τα ονόματα των θέσεων $ruf, ul, ...$ κτλ. έχουν συμβολική σημασία. Π.χ. το ruf σημαίνει το δεξιά-πάνω-εμπρός εδρίδιο (κορυφή), όποιο χρώμα κι' αν έχει σε δεδομένη στιγμή. Το M_R συμβολίζει την δεξιά κατά 90° στροφή της μεσαίας φέτας, παράλληλης προς την τρέχουσα δεξιά πλευρά του μεγάλου κύβου. Το ίδιο και τα U, L, ... στους προηγούμενους τύπους: έχουν συμβολική σημασία και αναφέρονται στην τρέχουσα θέση του μεγάλου κύβου.
(10) Ο παίκτης, χρησιμοποιώντας τις παραπάνω κινήσεις, μπορεί να φέρει τον κύβο στην κανονική του μορφή από οποιαδήποτε αρχική θέση. Χρειάζεται λίγη πρακτική εξάσκηση για την αναγνώριση των κινήσεων που πρέπει να γίνουν την δεδομένη στιγμή. Ο παίκτης κατ' αρχήν μπορεί να αποστηθήσει τις λίγες κινήσεις-κλειδιά, που περιγράφονται παραπάνω. Κατόπιν, με λίγη πρακτική, θα αναγνωρίζει αμέσως τα τεχνάσματα αναγωγής (4) που απαιτούν οι περιστάσεις. Οι κινήσεις που προτείνονται παραπάνω είναι λίγες και μέσω της αναγωγής των γενικωτέρων σ' αυτές, η απομνημόνευση ελαχιστοποιήται.

Το πλήθος των απαιτουμένων κινήσεων

Τίθεται ένα ερώτημα γιά το ποιό είναι το ελάχιστο πλήθος κινήσεων γιά την επίλυση του προβλήματος. Η επόμενη στρατηγική (του Thislethwaite), βασισμένη σε θεωρία και υπολογισμούς με τον υπολογιστή, οδηγεί στο συμπέρασμα ότι χρειάζονται το πολυ 52 κινήσεις. Ο αριθμός αυτός είναι ένα άνω φράγμα που μπορεί να μειωθεί. Δεν γνωρίζω αν έχει βρεθεί το ελάχιστο απαιτούμενο πλήθος κινήσεων, που λύνει το πρόβλημα για κάθε αρχική θέση.



Σχήμα 3.2: Πλήθος κινήσεων

(1) Η στρατηγική στηρίζεται στην διαμέριση της ομάδος G μέσω τριών υποομάδων της και των αντιστοίχων συμπλόκων τους:

$$G \supset G_1 \supset G_2 \supset G_3 \supset G_4 = \{e\}.$$

(2) Η θέση εκκίνησης του κύβου μπορεί να ταυτισθεί με ένα στοιχείο $g_0 \in G$, το οποίο θα περιέχεται σε κάποιο κιβωτισμό συμπλόκων:

$$\begin{aligned} g_0 \in g_{1i}G_1 \Rightarrow g_0 &= g_{1i}g_1,\ g_1 \in G_1 \\ g_1 \in g_{2j}G_2 \Rightarrow g_1 &= g_{2j}g_2,\ g_2 \in G_2 \\ g_2 \in g_{3j}G_3 \Rightarrow g_2 &= g_{3k}g_3,\ g_3 \in G_3 \\ \Rightarrow g_0 &= g_{1i}g_{2j}g_{3k}g_3. \end{aligned}$$

(3) Το κλειδί της στρατηγικής είναι ότι οι υποομάδες μπορούν να ορισθούν έτσι ώστε: (α) τα σύμπλοκα να αντιστοιχούν σε μιά μεθοδική διαδικασία, (β) το κάθε ένα από τα 4 βήματα (δηλαδή το κάθε ένα απο τα g_{1i}, g_{2j}, g_{3k}, g_3), να γράφεται ως ένα σχετικά μικρό γινόμενο απλών κινήσεων.
(4) Η πρώτη υποομάδα ορίζεται να είναι $G_1 =< R, L, F, B, U^2, D^2 >$. Αποδεικνύεται ότι $[G : G_1] = 2048$ και ότι υπάρχει σύστημα αντιπροσώπων $\{g_{1i}\}$ από τα σύμπλοκα G/G_1, κάθε ένας από τους οποίους γράφεται ως γινόμενο το πολύ 7 κινήσεων, που μετακινούν μόνον ακμές.
(5) Η δεύτερη υποομάδα ορίζεται να είναι $G_2 =< R, L, F^2, B^2, U^2, D^2 >$. Αποδεικνύεται ότι $[G_1 : G_2] = 1082565$ και ότι υπάρχει σύστημα αντιπροσώπων $\{g_{2j}\}$ από τα σύμπλοκα

G_1/G_2, κάθε ένας από τους οποίους γράφεται ως γινόμενο το πολύ 13 κινήσεων, που στρέφουν κορυφές περί τον εαυτό τους.
(6) Η τρίτη υποομάδα ορίζεται να είναι $G_3 =< R^2, L^2, F^2, B^2, U^2, D^2 >$. Αποδεικνύεται ότι $[G_2 : G_3] = 29400$ και ότι υπάρχει σύστημα αντιπροσώπων $\{g_{3k}\}$ από τα σύμπλοκα G_2/G_3, κάθε ένας από τους οποίους γράφεται ως γινόμενο το πολύ 15 κινήσεων, που τοποθετούν κύβους-ακμές και κύβους-κορυφές στις σωστές θέσεις τους, ενδεχομένως μεταθέτοντας τα χρώματα.
(7) Τέλος το στοιχείο $g_3 \in G_3$, με $|G_3| = 663552$, μπορεί να γραφεί σαν γινόμενο το πολύ 17 κινήσεων. Συνολικά λοιπόν χρειάζονται το πολύ $7 + 13 + 15 + 17 = 52$ κινήσεις γιά να λυθεί το πρόβλημα.

Η παράγραφος αυτή περιγράφει τις βασικές ιδιότητες που συσχετίζουν την θεωρία ομάδων με ένα πραγματικό παιγνίδι. Ορισμένα από τα προβλήματα που συνδέονται με το παιγνίδι αυτό είναι εφικτά σε ένα εισαγωγικό μάθημα όπως αυτό. Π.χ. ότι η ομάδα δρα μεταβατικά στο σύνολο V των κορυφών καθώς και στο σύνολο E των ακμών, με την έννοια ότι γιά κάθε ζεύγος κορυφών (ακμών) υπάρχει ένα τουλάχιστον στοιχείο της ομάδος που απεικονίζει την μιά στην άλλη. Ωστόσο η θεωρία που εμπεριέχεται είναι αρκετά εκτεταμένη και περιέχει προβλήματα που παραμένουν ακόμη άλυτα. π.χ. δεν είναι ακόμη γνωστό πόσες είναι οι μη-ισόμορφες μεταξύ τους υποομάδες της ομάδας κύβου Rubik.

ΠΡΟΒΛΗΜΑΤΑ 3.8

Πρόβλημα 3.8.1 *Δείξε ότι η ομάδα του κύβου του Rubik περιέχει 6 διαφορετικές κυκλικές υποομάδες τάξης 4, ωστόσο δεν είναι ισόμορφη με το ευθύ γινόμενό τους.*

Πρόβλημα 3.8.2 *Γράψε το στοιχείο M_R (συμβολίζει την στροφή, κατά 90°, με την φορά του ρολογιού, της μεσέας φέτας, παράλληλης προς την δεξιά πλευρά του κύβου) της ομάδος σαν γινόμενο των γεννητόρων της F, B, ...*

Κεφάλαιο 4

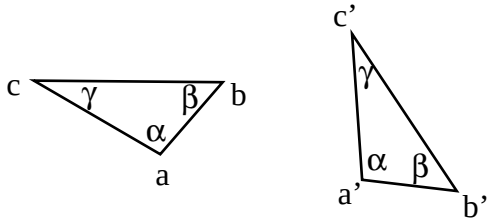
Διεδρικές Ομάδες

4.1 Ισομετρίες του επιπέδου

Ισομετρίες του επιπέδου λέμε τις αμφιμονοσήμαντες απεικονίσεις του επιπέδου στον εαυτό του $F : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ που διατηρούν την απόσταση δύο σημείων. Με άλλα λόγια ικανοποιούν

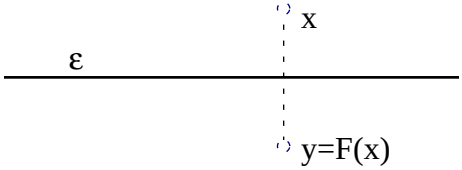
$$d(F(x),\, F(y)) = d(x,\, y),\ \forall\, x,\, y \in \mathbb{R}^2.$$

Παρατηρήσεις
(1) Υπενθυμίζω τον ορισμό της απόστασης: $d(x, y) = |y-x| = \sqrt{(y_1 - x_1)^2 + (y_2 - x_2)^2}$.
(2) Από τον ορισμό της ισομετρίας έπεται αμέσως ότι και η αντίστροφη απεικόνιση F^{-1} μιάς ισομετρίας είναι πάλι ισομετρία. Δύο σχήματα A, B (δηλ. υποσύνολα του επιπέδου) που συνδέονται με μιά ισομετρία: $B = F(A)$, λέγονται ισομετρικά.



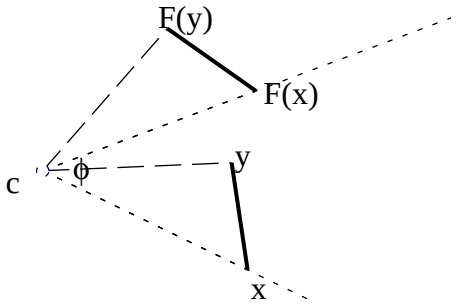
Σχήμα 4.1: Ισομετρικά τρίγωνα έχουν αντίστοιχες πλευρές και γωνίες ίσες

(3) Θα χρησιμοποιήσουμε συχνά το γεγονός ότι οι ισομετρίες, διατηρώντας τα μήκη, απεικονίζουν ένα τρίγωνο $(a,\, b,\, c)$ σε ένα $(a',\, b',\, c')$ ίσο προς το πρώτο, με την έννοια ότι τα δύο τρίγωνα έχουν αντίστοιχες πλευρές ίσες και απέναντι σε ίσες πλευρές κείνται ίσες γωνίες. Προφανώς επίσης ένας κύκλος απεικονίζεται μέσω ισομετρίας σε κύκλο, ακτίνας ίσης με αυτήν του αρχικού.
(4) Ειδικό παράδειγμα ισομετρίας είναι η **μεταφορά** $F(x) = x + v$, όπου $v \in \mathbb{R}^2$ σταθερό.



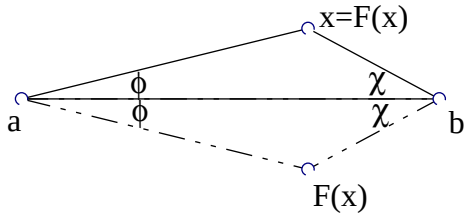
Σχήμα 4.2: Κατοπτρισμός ως προς ευθεία ε

(5) Ένα δεύτερο παράδειγμα ισομετρίας είναι η **ανάκλαση ή κατοπτρισμός** ως προς ευθεία ε. Σ' αυτήν την ισομετρία, στο τυχόν $x \in \mathbb{R}^2$ αντιστοιχούμε το $y = F(x)$, έτσι ώστε η ε να είναι η μεσοκάθετος του (xy). Η ε λέγεται **άξονας ή κάτοπτρο** του κατοπτρισμού.



Σχήμα 4.3: Στροφή με κέντρο c και γωνία φ

(6) Ένα τρίτο παράδειγμα ισομετρίας είναι η **στροφή** με κέντρο c και γωνία ϕ. Και στα τρία τελευταία παραδείγματα είναι πολύ εύκολο να δείξουμε την χαρακτηριστική ιδιότητα της ισομετρίας.
(7) Προφανώς η σύνθεση δύο ισομετριών $F \circ G$ είναι πάλι ισομετρία και το σύνολο των ισομετριών αποτελεί ομάδα ως προς την σύνθεση απεικονίσεων. Την ομάδα αυτή συμβολίζουμε με $Iso(\mathbb{R}^2)$).
(7) Ιδιαίτερο ρόλο στις ισομετρίες παίζουν τα σταθερά σημεία τους, δηλαδή τα σημεία γιά τα οποία $F(x) = x$. Μιά μεταφορά $F(x) = x + v$, με $v \neq 0$, δεν έχει κανένα σταθερό σημείο. Ένας κατοπτρισμός έχει όλα τα σημεία του άξονά του σταθερά. Μιά στροφή έχει μόνο το κέντρο της σταθερό.

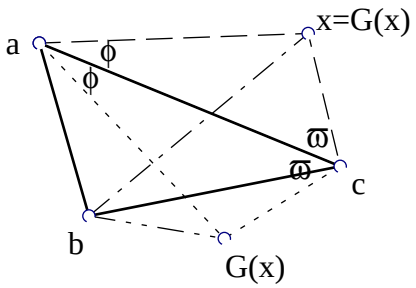


Σχήμα 4.4: Ισομετρία που αφήνει δύο σημεία σταθερά

Πρόταση 4.1.1 *Μία ισομετρία $F \in Iso(\mathbb{R}^2)$ που έχει δύο σταθερά σημεία a, b είναι ή η ταυτοτική ή ο κατοπτρισμός ως προς την ευθεία που ορίζουν αυτά τα δύο σημεία.*

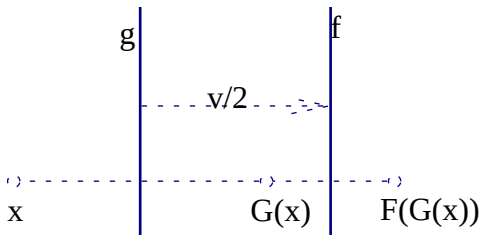
Πράγματι, τα τρίγωνα $(a,\ b,\ x)$ και $(a,\ b,\ F(x)) = (F(a),\ F(b),\ F(x))$ θα είναι ίσα, επομένως τα σημεία x, $F(x)$ ή συμπίπτουν ή είναι συμμετρικά ως προς την ευθεία των a, b. Στην περίπτωση που $F(x) = x$, η F έχει τρία σταθερά σημεία. Στην περίπτωση που $F(x)) \neq x$, η σύνθεση $G \circ F$ με την ανάκλαση G ως προς την ευθεία $(a,\ b)$, έχει τρία σταθερά σημεία. Το συμπέρασμα προκύπτει από την επόμενη πρόταση, συγκρίνοντας την F ή την $G \circ F$ (στην δεύτερη περίπτωση) με την ταυτοτική, που είναι μιά ειδική ισομετρία.

Πρόταση 4.1.2 *Δύο ισομετρίες F, F' που συμπίπτουν σε τρία σημεία σε γενική θέση a, b, c (δηλ. $F(a) = F'(a)$, $F(b) = F'(b)$, $F(c) = F'(c)$), συμπίπτουν σε όλα τα σημεία του επιπέδου (δηλ. $F = F'$, ή $F(x) = F'(x)\ \forall x \in \mathbb{R}^2$).*



Σχήμα 4.5: a, b, c σταθερά σημεία της G

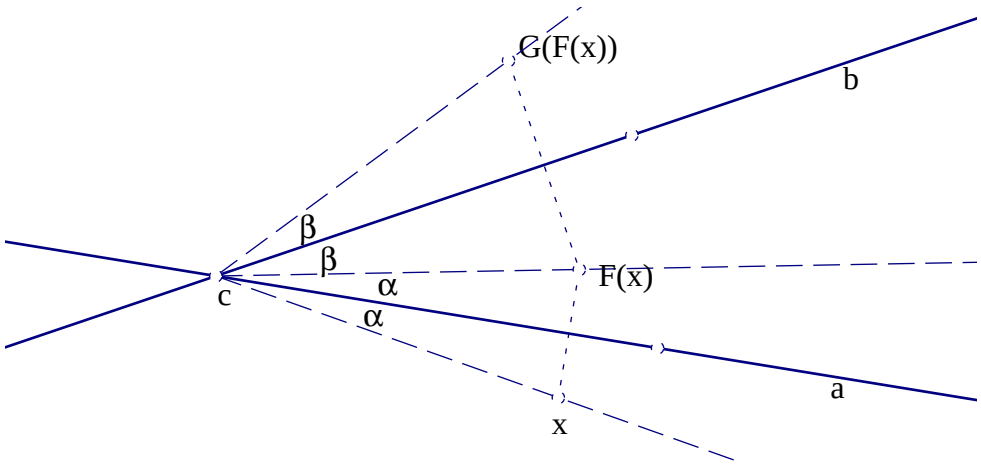
Δείχνουμε ότι υπό τις προϋποθέσεις της πρότασης, η $G = F' \circ F^{-1}$ είναι η ταυτοτική. Η G θα αφήνει εξ' υποθέσεως τα a, b, c σταθερά. Επίσης τα τρίγωνα $(a,\ c,\ x)$, $(G(a),\ G(c),\ G(x) = (a,\ c,\ G(x))$ θα είναι ίσα. Επομένως τα x, $G(x)$ ή θα ταυτίζονται ή θα είναι συμμετρικά ως προς την a, c. Η δεύτερη όμως περίπτωση αποκλείεται διότι $d(b, x) = d(G(b), G(x)) = d(b, G(x))$ που μπορεί να συμβαίνει μόνον όταν το b είναι επί της ευθείας των a, c, πράγμα που αποκλείσαμε.



Σχήμα 4.6: Σύνθεση παραλλήλων κατοπτρισμών είναι μεταφορά

Πρόταση 4.1.3 *Δύο κατοπτρισμοί F, G των οποίων οι άξονες είναι παράλληλοι έχουν ως σύνθεση $H = F \circ G$ μιά μεταφορά κατά $H(x) = x + v$, όπου v έχει μήκος το διπλάσιο της απόστασης των παραλλήλων αξόνων.*

Το συμπέρασμα προκύπτει άμεσα γεωμετρικά μετρώντας την απόσταση $x, F(G(x))$ γιά τυχόν σημείο του επιπέδου.



Σχήμα 4.7: Σύνθεση κατοπτρισμών με τεμνόμενους άξονες είναι στροφή

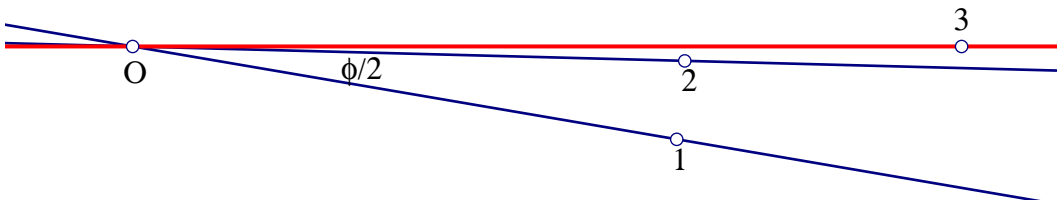
Πρόταση 4.1.4 *Δύο κατοπτρισμοί F, G των οποίων οι άξονες τέμνονται, έχουν ως σύνθεση $H = G \circ F$ μιά στροφή με κέντρο c την τομή των αξόνων τους και γωνία στροφής το διπλάσιο της γωνίας των αξόνων τους.*

Το συμπέρασμα προκύπτει άμεσα γεωμετρικά, μετρώντας την γωνία $\angle(x, c, G(F(x)))$ γιά τυχόν σημείο του επιπέδου.

4.2 Ομάδες που αφήνουν σταθερό σημείο

Θεωρούμε εδώ ένα σταθερό σημείο $O \in \mathbb{R}^2$ και το σύνολο των ισομετριών του επιπέδου που αφήνουν το σημείο αυτό σταθερό $F(O) = O$. Προφανώς το σύνολο αυτό αποτελεί μιά υποομάδα της $Iso(\mathbb{R}^2)$ που συμβολίζουμε με $Iso(\mathbb{R}^2)_O$.

Πρόταση 4.2.1 *Η σύνθεση $H = G \circ F$ μιάς στροφής $F \in Iso(\mathbb{R}^2)_O$ και ενός κατοπτρισμού $G \in Iso(\mathbb{R}^2)_O$ είναι κατοπτρισμός $H \in Iso(\mathbb{R}^2)_O$. Το ίδιο ισχύει και γιά την $H' = F \circ G$.*



Σχήμα 4.8: Σύνθεση κατοπτρισμού και στροφής στο $Iso(\mathbb{R}^2)_O$

Πράγματι, κατά το 4.1.4, την στροφή $F \in Iso(\mathbb{R}^2)_O$ μπορούμε να θεωρήσουμε σαν σύνθεση δύο ανακλάσεων $F = R_2 \circ R_1$ ως προς δύο άξονες που σχηματίζουν γωνία $\phi/2$ και τέμνονται στο O. Τους δε άξονες μπορούμε να πάρουμε σε αυθαίρετη κατεύθυνση, αρκεί η γωνία τους να είναι η αναφερθήσα. Τους παίρνουμε λοιπόν έτσι ώστε ο δεύτερος άξονας να συμπίπτει με τον άξονα του κατοπτρισμού G. Τότε $R_2 = G$ και $H = G \circ F = G \circ R_2 \circ R_1 = R_1$, που είναι το ζητούμενο. Ανάλογα προκύπτει και ο δεύτερος ισχυρισμός.

Πρόταση 4.2.2 *Κάθε μη-ταυτοτική ισομετρία της $F \in Iso(\mathbb{R}^2)_O$ είναι ή στροφή ή κατοπτρισμός.*

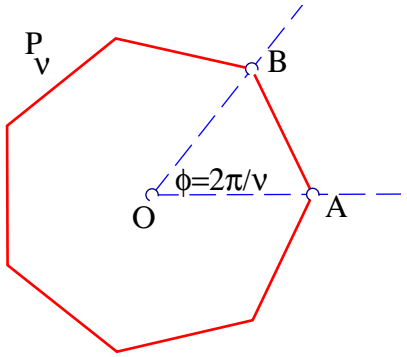
Πράγματι, αν έχει ένα ακόμη σταθερό σημείο, τότε κατά την 4.1.1, θα είναι κατοπτρισμός. Αν δεν έχει άλλο σταθερό σημείο εκτός του O, τότε παίρνουμε ένα τυχόν $x \neq O$ και την εικόνα του $y = F(x)$. Αφού η F είναι ισομετρία θα έχουμε $d(O, x) = d(O, F(x))$ και προφανώς υπάρχει μιά στροφή $G \in Iso(\mathbb{R}^2)_O$ που πάει το y πίσω στο x, $G(y) = x$. Έτσι η σύνθεση $H = G \circ F$ έχει δύο σταθερά σημεία: το O και το x. Συνεπώς, κατά την 4.1.1, θα είναι ή η ταυτοτική e ή ένας κατοπτρισμός R. Στην πρώτη περίπτωση $G \circ F = e \Rightarrow F = G^{-1}$ που είναι στροφή. Στην δεύτερη περίπτωση $G \circ F = R \Rightarrow F = G^{-1} \circ R$ που είναι σύνθεση κατοπτρισμού και στροφής, άρα, κατά την 4.2.1 κατοπτρισμός.

4.3 Διεδρικές ομάδες

Γιά ακέραιο $n \geq 2$ συμβολίζουμε με P_n ένα κανονικό πολύγωνο με n πλευρές και κέντρο στο σημείο O (στο πρώτο κεφάλαιο με το ίδιο σύμβολο συμβολίζαμε το κανονικό $n-$γωνο με κέντρο στο $O = (0, 0)$ και πρώτη κορυφή στο $(1, 0)$). Το σύνολο των ισομετριών του επιπέδου που απεικονίζουν το πολύγωνο στον εαυτό του το ονομάζουμε **διεδρική ομάδα**

του n-γώνου και συμβολίζουμε με D_n.

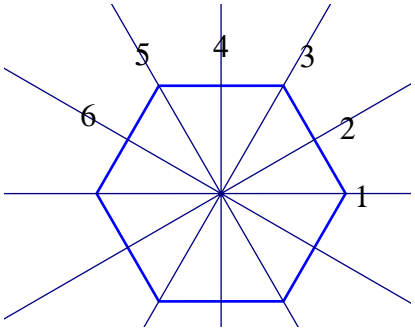
Παρατηρήσεις
(1) Προφανώς κάθε τέτοια ισομετρία απεικονίζει τον περιγεγραμμένο κύκλο του πολυγώνου στον εαυτό του, άρα και το κέντρο του O στον εαυτό του.
(2) Είναι προφανές ότι η αντίστροφη μιάς $F \in D_n$ απεικονίζει επίσης το πολύγωνο στον εαυτό του. Επίσης η σύνθεση δύο $F, G \in D_n$ είναι πάλι μιά ισομετρία $G \circ F \in D_n$. Άρα η D_n είναι υποομάδα της $Iso(\mathbb{R}^2)_O$.
(3) Κατά το 4.2.2, κάθε $F \in D_n$ θα είναι κατοπτρισμός ή στροφή. Μπορούμε λοιπόν να ξεκινήσουμε απ' αυτό το δεδομένο και να προσδιορίσουμε όλα τα στοιχεία της D_n.



Σχήμα 4.9: Γενήτορας στροφών του D_n

(4) Υπάρχει μιά ελάχιστη δυνατή στροφή $R \in D_n$ που απεικονίζει μιά κορυφή A, του πολυγώνου P_n, στην γειτονική της B, με φορά αντίθετη του ρολογιού. Η στροφή αυτή παράγει προφανώς μιά κυκλική ομάδα $< R >= \{e, R, R^2, ..., R^{n-1}\}$ ισόμορφη με την $\mathbb{Z}_n$. Την R ονομάζουμε **γεννήτορα** των στροφών της D_n. Από την γεωμετρία του σχήματος έχουμε την επόμενη πρόταση.

Πρόταση 4.3.1 *Κάθε στροφή $F \in D_n$ συμπίπτει με ένα στοιχείο της υποομάδας $< R > \subset D_n$.*

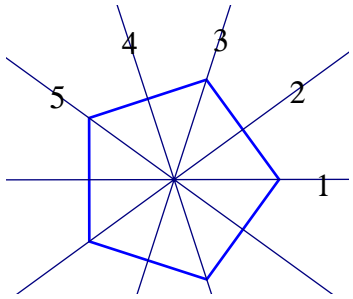


Σχήμα 4.10: Κατοπτρισμοί του D_n (n άρτιο)

Πρόταση 4.3.2 *Υπάρχουν n διαφορετικοί κατοπτρισμοί που απεικονίζουν το P_n στον εαυτό του.*

Πράγματι, οι κατοπτρισμοί ως προς τις ευθείες που ενώνουν το κέντρο με τις κορυφές και τις μεσοκάθετες των πλευρών του P_n είναι οι μοναδικές που απεικονίζουν το πολύγωνο αυτό

στον εαυτό του. Από την γεωμετρία του σχήματος συμπεραίνουμε ότι υπάρχουν n τέτοιοι διαφορετικοί κατοπτρισμοί, είτε το n είναι άρτιο είτε περιττό.



Σχήμα 4.11: Κατοπτρισμοί του D_n (n περιττό)

Πρόταση 4.3.3 *Η ομάδα D_n έχει $2n$ στοιχεία, από τα οποία τα n είναι κατοπτρισμοί και τα υπόλοιπα στροφές.*

Τούτο είναι συμπέρασμα των προηγουμένων.

ΠΡΟΒΛΗΜΑΤΑ 4.3

Πρόβλημα 4.3.1 *Δείξε ότι γιά κάθε διεδρική ομάδα D_n υπάρχει ισομορφισμός της $F : D_n \to S_n$ που ορίζει μιά υποομάδα $F(D_n) \subseteq S_n$, ισόμορφη της D_n. Βρές τις υποομάδες αυτές των S_3, S_4, S_5.*

Πρόβλημα 4.3.2 *Δείξε ότι η ομάδα V_4 του Klein (πρόβλημα 3.7.3), είναι ισόμορφη προς την ομάδα ισομετριών ενός ορθογωνίου παραλληλογράμμου στον εαυτό του.*

4.4 Δομή διεδρικών ομάδων

Μας ενδιαφέρει εδώ να δούμε τον τρόπο που παράγεται μιά διεδρική ομάδα από κάποια στοιχεία της και να την συνδέσουμε με άλλα παραδείγματα ομάδων.

Πρόταση 4.4.1 *Εστω $S \in D_n$ ένας κατοπτρισμός και $R \in D_n$ ο γεννήτορας στροφών της D_n. Τα στοιχεία της D_n, S, SR, SR^2, ..., SR^{n-1} είναι ακριβώς όλοι οι κατοπτρισμοί της D_n. Συνεπώς η D_n παράγεται από τα S και R.*

Το ότι αυτά τα στοιχεία είναι, όλα, κατοπτρισμοί προκύπτει από το 4.2.1. Προφανώς επίσης είναι διαφορετικά μεταξύ τους, άρα το συμπέρασμα, αφού η ομάδα αυτή περιέχει n ακριβώς κατοπτρισμούς.

Πρόταση 4.4.2 *Η D_n παράγεται από δύο οιεσδήποτε ανακλάσεις S_1, S_2 των οποίων οι άξονες σχηματίζουν γωνία π/n.*

Πράγματι, η στροφή $R' = S_1 \circ S_2$ θα συμπίπτει (δες 4.1.4) με τον γεννήτορα στροφών ή τον αντίστροφό του, άρα κατά το προηγούμενο, τα R' και S_1 θα παράγουν όλο το D_n.

Πρόταση 4.4.3 *Η D_n μπορεί να ταυτισθεί με την υποομάδα D'_n της συμμετρικής ομάδος S_n, που παράγεται από τον κύκλο $R' = (1 \ldots . n)$ και την μετάθεση $S' = (1n)(2, n-1)(3, n-2)$....*

Πράγματι, αν αριθμήσουμε τις διαδοχικές κορυφές του πολυγώνου P_n με τους αριθμούς του $\underline{n} = \{1, ..., n\}$, τότε σε κάθε ισομετρία $t \in D_n$ αντιστοιχεί μιά μετάθεση $P(t) \in S_n$. Η απεικόνιση αυτή είναι μονοσήμαντη, αφού η ισομετρία καθορίζεται πλήρως από την συμπεριφορά της στις κορυφές του πολυγώνου. Γιά τον ίδιο λόγο $P(ts) = P(t)P(s)$, άρα η P είναι μονομορφισμός και η εικόνα της $D'_n = Im(P) \subset S_n$ θα είναι υποομάδα της S_n. Το τελευταίο συμπέρασμα προκύπτει από το ότι οι μεταθέσεις R', S' είναι οι αντίστοιχες εικόνες των γεννητόρων της D_n.

Πρόταση 4.4.4 *Ο κατοπτρισμός S, και ο γεννήτορας στροφών R, που αναφέρονται στο 4.4.1, ικανοποιούν τις τρείς σχέσεις: $R^n = e$, $S^2 = e$, $(SR)^2 = e$. Κάθε ομάδα που παράγεται από δύο στοιχεία της R, S που ικανοποιούν τις προηγούμενες σχέσεις είναι ισόμορφη με την D_n.*

Κατ' αρχήν ότι ικανοποιούνται οι τρεις σχέσεις είναι προφανές. Οι δύο πρώτες από τον ορισμό των R, S και η τρίτη διότι η SR είναι κατοπτρισμός. Ο δεύτερος ισχυρισμός προκύπτει αποδεικνύοντας τα εξής εύκολα:
(1) Τα στοιχεία e, R, ..., R^{n-1}, S, SR, ..., SR^{n-1} είναι διαφορετικά μεταξύ τους.
(2) Το αντίστροφο, καθώς και οποιοδήποτε γινόμενο μεταξύ αυτών των $2n$ στοιχείων, είναι πάλι ένα απ' αυτά τα στοιχεία. Άρα η ομάδα που παράγεται απ' αυτά δεν περιέχει κανένα επιπλέον στοιχείο.
(3) Ο πίνακας πολλαπλασιασμού είναι ο ίδιος με αυτόν της D_n.
π.χ. Ας δείξουμε την κρίσιμη γιά το (2) σχέση: $R(SR^k) = RSRSSR^{k-1} = (RSRS)SR^{k-1} = SR^{k-1}$, άρα επαγωγικά , $R^m(SR^k) = SR^{k-m}$.

Πρόταση 4.4.5 *Η υποομάδα $< R > \subset D_n$, των στροφών της διεδρικής, είναι κανονική.*

Αρκεί να δείξουμε για τα εκτός της $< R >$ στοιχεία: $T = S$, SR, ..., SR^{n-1}, ότι ικανοποιούν την $T < R > T^{-1} \subset < R >$. Όμως γιά ένα τέτοιο $T = SR^k$ και ένα στοιχείο $R^m \in < R >$ έχουμε $TR^mT^{-1} = SR^kR^m(SR^k)^{-1} = SR^kR^mR^{-k}S^{-1} = SR^mS^{-1} = (SRS^{-1})^m = R^{-m} \in < R >$. Τούτο αποδεικνύει το ζητούμενο.

ΠΡΟΒΛΗΜΑΤΑ 4.4

Πρόβλημα 4.4.1 *Δείξε ότι η ομάδα $D_n/ < R >$ αποτελείται από δύο σύμπλοκα. Το ένα περιλαμβάνει όλες τις στροφές και το άλλο όλους τους κατοπτρισμούς.*

Πρόβλημα 4.4.2 *Δείξε ότι οι κατοπτρισμοί της D_n είναι όλοι συζυγείς μεταξύ τους όταν το n είναι περιττός. Οταν το n είναι άρτιος, δείξε ότι οι κατοπτρισμοί διαμερίζονται σε δύο κλάσεις συζυγίας με $n/2$ το πλήθος στοιχεία έκαστη.*

Πρόβλημα 4.4.3 *Δείξε ότι το κέντρο της D_n αποτελείται από δύο στοιχεία όταν το n είναι άρτιο και ένα στοιχείο αντίστοιχα όταν το n είναι περιττό. Δείξε επίσης ότι στην πρώτη περίπτωση, οι υπόλοιπες στροφές διαμερίζονται σε $(n/2) - 1$ κλάσεις συζυγίας και στην δεύτερη σε $(n-1)/2$ κλάσεις με δύο στοιχεία σε κάθε κλάση.*

Πρόβλημα 4.4.4 *Δείξε ότι η D_3 είναι ισόμορφη προς την συμμετρική ομάδα S_3. Εξήγησε τι σημαίνει τούτο γεωμετρικά. (Δες πρόβλημα 3.7.8.)*

Πρόβλημα 4.4.5 *Δείξε ότι η D_4 είναι ισόμορφη προς την ομάδα πινάκων του προβλήματος 1.3.10(γ). (Υπόδειξη: $R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, S = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.)*

Πρόβλημα 4.4.6 *Δείξε ότι μιά ομάδα που παράγεται από δύο στοιχεία και τις σχέσεις: $G =< s_1, s_2 : {s_1}^2 = {s_2}^2 = e, (s_1 \circ s_2)^n = e >$, είναι ισόμοφη προς την D_n.*

Κεφάλαιο 5

Πεπερασμένες αβελιανές ομάδες

Μετά την εξέταση των βασικών εννοιών και την ανάλυση διακεκριμένων παραδειγμάτων ομάδων, θα εξέτάσουμε μερικές απλές περιπτώσεις κατηγοριοποίησης ή ταξινόμησης ομάδων που σχετίζονται με πρώτους αριθμούς. Αυτό το κάνουμε για να εξασκηθούμε στην χρήση των γνώσεων που αποκτήσαμε και όχι γιά να καταλήξουμε σε κάποια ολοκληρωμένη ταξινόμηση. Μιά τέτοια πρόθεση είναι, με τα σημερινά δεδομένα, αδύνατον να πραγματοποιηθεί. Η ταξινόμηση των πεπερασμένων ομάδων και μόνον, ολοκληρώθηκε μόλις το 1983, με την εύρεση της τελευταίας σποραδικής απλής ομάδας. Η ομάδα αυτή, το λεγόμενο *τέρας*, έχει $2^{46} \times 3^{20} \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71$ στοιχεία. Για την ταξινόμηση αυτή υπολογίζεται ότι εργάστηκαν συνολικά εκατοντάδες μαθηματικών και οι λεπτομερείς επι μέρους αποδείξεις περιλαμβάνουν δεκάδες χιλιάδων τυπωμένων σελίδων. Το έργο της ταξινόμησης των πεπερασμένων ομάδων θεωρήται από τα μεγαλύτερα επιτεύγματα των Μαθηματικών. Από τα παραδείγματα που εξετάσαμε διαφαίνεται ότι υπάρχουν διάφορες κατηγορίες ομάδων: κυκλικές, αβελιανές, ομάδες πινάκων, ομάδες μεταθέσεων, ομάδες συμμετριών γεωμετρικών αντικειμένων, κ.ο.κ. Θα ξεκινήσουμε με μερικά θεωρήματα γιά την συνάρτηση $\phi(x)$ του Euler, που συναντήσαμε στο πρόβλημα 2.8.2. Θυμίζω ότι η συνάρτηση $\phi(n)$ δίνει το πλήθος των μικρότερων του n ακεραίων θετικών, που είναι πρώτοι προς το n. Στο προαναφερθέν πρόβλημα είδαμε ότι η $\phi(n)$ συμπίπτει με το πλήθος των στοιχείων της $\mathbb{Z}_n^*$. Εκεί επίσης είδαμε ότι η ίδια συνάρτηση συμπίπτει με το πλήθος των στοιχείων που παράγουν την Z_n. Θα καταλλήξουμε με την διάσπαση μιάς πεπερασμένης αβελιανής ομάδας σε γινόμενο αβελιανών ομάδων, των οποίων οι τάξεις είναι δυνάμεις πρώτων αριθμών.

5.1 Η συνάρτηση $\phi(x)$ του Euler

Πρόταση 5.1.1 *Γιά κάθε πρώτο θετικό ακέραιο p και φυσικό $n > 0$ ισχύει*

$$\phi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1).$$

Πράγματι, αφού ο p είναι πρώτος, οι μόνοι μη-πρώτοι προς το p^n, ανάμεσα στους αριθμούς $\{1, 2, ...p^n\}$, είναι τα πολλαπλάσια του p, που είναι $\{p \cdot 1, p \cdot 2, p \cdot 3, p \cdot 4, ..., p \cdot (p^{n-1} - 1), p \cdot p^{n-1}, \}$, δηλαδή p^{n-1} το πλήθος.

Πρόταση 5.1.2 *Γιά σχετικά πρώτους θετικούς ακέραιους a, b ισχύει*

$$\phi(ab) = \phi(a)\phi(b).$$

Ας δούμε μιάν απόδειξη που χρησιμοποιεί τις ομάδες που γνωρίζουμε (δες Πρόβλημα 2.8.12). Θεωρούμε την απεικόνιση $F : \mathbb{Z}_{ab} \longrightarrow \mathbb{Z}_a \times \mathbb{Z}_b$, με $F(x) = (x \bmod a, x \bmod b)$. Βλέπουμε εύκολα ότι η F είναι ισομορφισμός ομάδων. Ας συμβολίζουμε με G_n το σύνολο των μικρότερων του n και πρώτων προς αυτόν ακεραίων. Δείχνουμε ότι $F(G_{ab}) = G_a \times G_b$, το οποίο αποδεικνύει το ζητούμενο, αφού $\phi(n) = |G_n|$. Πράγματι, αν (x, ab) είναι πρώτοι μεταξύ τους, τότε αναγκαστικά και (x, a) , (x, b) θα είναι ζεύγη πρώτων μεταξύ τους. Αυτό δείχνει ότι $F(G_{ab}) \subseteq G_a \times G_b$. Αντίστροφα, αν (x_1, a) , (x_2, b) είναι ζεύγη πρώτων μεταξύ τους, οπότε $(x_1, x_2) \in G_a \times G_b$, τότε, λόγω της ισομορφικότητας της F θα υπάρχει $x \in \mathbb{Z}_{ab}$ με $F(x) = (x_1, x_2)$. Δείχνουμε ότι το x είναι πρώτος προς το ab άρα $x \in G_{ab}$ και επομένως $G_a \times G_b \subseteq F(G_{ab})$. Πράγματι αν το x δεν ήταν πρώτο προς το ab τότε θα υπήρχε πρώτος αριθμός και ταυτόχρονα κοινός διαιρέτης του x και του ab, έστω $d \neq 1$. Ο d θα έπρεπε να διαιρεί έναν από τα a, b έστω το a. Όμως $F(x) = (x \bmod a, x \bmod b) = (x_1, x_2) \Rightarrow x = x_1 + \lambda a$. Το d ως διαιρόν το a διαιρόν και το x θα έπρεπε τότε να διαιρεί και το x_1, που είναι άτοπο, διότι υπόθέσαμε ότι τα x_1, a είναι πρώτα μεταξύ τους.

Πρόταση 5.1.3 *Γιά κάθε ακέραιο θετικό n ισχύει:*

$$\phi(n) = n \prod_{p|n} (1 - (1/p)),$$

όπου $p|n$ συμβολίζει έναν πρώτο και διαιρέτη του n.

Η απόδειξη προκύπτει από την προηγούμενη πρόταση που εκφράζει μιά πολλαπλασιαστική ιδιότητα της συνάρτησης ϕ για πρώτους σχετικά αριθμούς. Η ιδιότητα αυτή επεκτείνεται επαγωγικά σε k το πλήθος παράγοντες: $\phi(a_1...a_k) = \phi(a_1)...\phi(a_k)$, εφόσον οι k αυτοί αριθμοί δεν έχουν κοινό παράγοντα. Την ιδιότητα αυτή εφαρμόζουμε στην ανάλυση του n σε πρώτους παράγοντες: $n = p_1^{d_1} ... p_k^{d_k}$.

Πρόταση 5.1.4 *Γιά κάθε ακέραιο θετικό n ισχύει:*

$$\sum_{d|n} \phi(d) = n$$

όπου $d|n$ συμβολίζει έναν διαιρέτη του n, συμπεριλαμβανομένου του 1 και του n.

Γιά την απόδειξη χρησιμοποιούμε πάλι την ομάδα $\mathbb{Z}_n$. Κάθε ένα στοιχείο x της ομάδας αυτής έχει τάξη d, κάποιο διαιρέτη του n. Γιά κάθε δε τέτοιο διαιρέτη υπάρχουν $\phi(d)$ στοιχεία μ' αυτήν την τάξη. Το συμπέρασμα προκύπτει άμεσα από το ότι η $\mathbb{Z}_n$ έχει n στοιχεία.

Πρόταση 5.1.5 *Έστω G πεπερασμένη ομάδα με $|G| = n$ και την ιδιότητα: σε κάθε διαιρέτη $d|n$ να αντιστοιχεί το πολύ μιά υποομάδα της G τάξης d. Τότε η G είναι κυκλική.*

Γιά την απόδειξη εισάγουμε την συνάρτηση $\psi(d)$ και την συγκρίνουμε με την συνάρτηση του Euler $\phi(d)$. Ορίζουμε λοιπόν την $\psi(d)$ να ισούται με το πλήθος των στοιχείων τάξης d της G. Εάν $\psi(d) \neq 0$ τότε υπάρχει, κατά την υπόθεση μία και μόνον υποομάδα τάξης d, η οποία συνεπώς θα περιέχει και όλα τα υπόλοιπα στοιχεία τάξης d, που είναι $\phi(d)$ το πλήθος. Άρα, με τις υποθέσεις της πρότασης, η $\psi(d)$ θα λαμβάνει ή την τιμή 0 ή την τιμή $\phi(d)$. Επειδή κάθε στοιχείο της ομάδας έχει τάξη d, έναν διαιρέτη του n, θα ισχύει:

$$\sum_{d|n} \psi(d) = n.$$

Ισχύει όμως και

$$\sum_{d|n} \psi(d) = n.$$

Πού λόγω της $\psi(d) \leq \phi(d)$, δεν είναι δυνατόν να ισχύουν ταυτόχρονα, παρά μόνον όταν $\psi(d) = \phi(d)$, $\forall d|n$. Ειδικά θα ισχύει και $\psi(n) = \phi(n) > 0$, που δίδει το ζητούμενο. Πράγματι ένα στοιχείο x τάξης n, θα δίδει $G =< x >$.

ΠΡΟΒΛΗΜΑΤΑ 5.1

Πρόβλημα 5.1.1 *Έστω G πεπερασμένη ομάδα με $|G| = n$ και την ιδιότητα: σε κάθε διαιρέτη $d|n$ να αντιστοιχούν το πολύ d στοιχεία της G με την ιδιότητα $x^d = e$. Δείξε ότι τότε η G είναι κυκλική. (Υπόδειξη: Αναγωγή στην τελευταία πρόταση και γεγονός ότι γιά κάθε στοιχείο x ομάδος τάξεως G με $|G| = k$, ισχύει $x^k = e$.)*

5.2 Ομάδες και πρώτοι αριθμοί

Πρόταση 5.2.1 *Έστω ότι η υποομάδα H της ομάδος G περιέχεται στο κέντρο της (τα στοιχεία της H μετατίθενται με κάθε στοιχείο της G) και η G/H είναι κυκλική. Τότε η G είναι αβελιανή.*

Πρέπει να δείξουμε ότι γιά κάθε $x, y \in G : xy = yx$. Προβάλουμε λοιπόν στο πηλίκον $x' = xH, y' = yH \in G/H$. Κατά την υπόθεση η τελευταία ομάδα είναι κυκλική και έστω ότι παράγεται από το $sH \in G/H$. Τότε $x' = xH = s^k H$ γιά κάποιον ακέραιο k και ανάλογα, $y' = yh = s^m H$. Τότε όμως τα x, y θα είναι της μορφής: $x = s^k h, y = s^m h'$ γιά κάποια $h, h' \in H$ άρα $xy = s^k h s^m h' = s^{k+m} hh' = s^m h' s^k h = yx$.

Πρόταση 5.2.2 *Μιά ομάδα της οποίας η τάξη $|G| = p^2$ είναι τετράγωνο πρώτου αριθμού, είναι αβελιανή.*

Πράγματι, κατά την πρόταση 2.8.3 το κέντρο H της G είναι μη-τετριμμένο, άρα $|H| = p$ ή p^2. Τότε η ομάδα G/H έχει τάξη 1 ή p, άρα είναι κυκλική. Το συμπέρασμα συνάγεται από την προηγούμενη πρόταση.

Πρόταση 5.2.3 **(Cauchy)** *Γιά κάθε πρώτο p που διαιρεί την τάξη $|G| = n$ μιάς ομάδος, υπάρχει στοιχείο της τάξης p.*

Η απόδειξη γίνεται με επαγωγή ως προς την τάξη n της ομάδος. Προφανώς ισχύει γιά $n = 1$, αφού τότε δεν υπάρχουν πρώτοι διαιρέτες του n. Υποθέτουμε τώρα ότι η πρόταση αληθεύει γιά κάθε $k < n$ και δείχνουμε ότι ισχύει και γιά n. Γράφουμε την εξίσωση (δες 2.8.2) των κλάσεων

$$n = c + h + h' + h'' + ...,$$

της ομάδας G, όπου $c = |Z(G)|$ είναι η τάξη του κέντρου της G και τα $h, h', ...$ είναι οι δείκτες ορισμένων γνήσιων υποομάδων της G:

$$h = [G : N], h' = [G : N'], h'' = [G : N''] ...$$

Αν κάποιο από τα $h, h', h'' ...$ δεν διαιρήται με το p, τότε το p πρέπει να δαιρεί την τάξη του αντιστοίχου N. Επειδή δε το N αυτό έχει τάξη μικρότερη του n, κατά την επαγωγική

απόδειξη, θα περιέχει στοιχείο τάξης p.
Ας υποθέσουμε τώρα ότι το p διαιρεί όλα τα $h, h', h''....$ Τότε, επειδή το p διαιρεί και το n, θα διαιρεί και το c. Έστω λοιπόν ένα τυχόν στοιχείο $a \in Z(G)$, $a \neq e$ τάξης k και $A =< a >$, η κυκλική υποομάδα που παράγεται από το a. Εάν το p διαιρεί το k, τότε το $a^{k/p}$ έχει τάξη p. Αν το p δεν διαιρεί το k, τότε το p θα διαιρεί την τάξη c/k της ομάδος Z/A. Άρα, κατά την επαγωγική υπόθεση (αφού $c/k < c \leq n$) το Z/A θα περιέχει στοιχείο $z' = zA$ τάξης p. Εάν m είναι η τάξη του $z \in Z$, τότε $z'^m = z^m A = A$, άρα το p διαιρεί το m. Τότε όμως το $z^{m/p}$ έχει τάξη p.

Πρόταση 5.2.4 *Έστω $p > 2$ πρώτος. Οι μόνες ομάδες τάξης $2p$ είναι η κυκλική $\mathbb{Z}_{2p}$ και η διεδρική D_p.*

Πράγματι, από το προηγούμενο θεώρημα έπεται ότι υπάρχουν δύο στοιχεία a, b τάξης p και 2 αντίστοιχα. Προφανώς η ομάδα αποτελείται τότε από τα στοιχεία:

$$e, a, a^2, ..., a^{p-1},\ b, a^2b, ..., a^{p-1}b.$$

Η υποομάδα $A =< a >$, τάξης p, έχει δείκτη 2 στο G, άρα η A είναι κανονική υποομάδα της G (δες 2.5.1). Κατά συνέπεια, $bab^{-1} = a^i$, γιά κάποιο $i : 0 \leq i \leq p-1$. Επειδή $b^2 = e$, έπεται $a = b(bab^{-1})b^{-1} = ba^ib^{-1} = (bab^{-1})^i = a^{i^2}$. Επειδή το a είναι τάξης p, έπεται $i^2 = 1 mod(p)$ και συνεπώς $i = \pm 1 mod(p)$, δηλαδή $i = 1$ ή $i = p-1$. Στην πρώτη περίπτωση $ba = ab$. Επειδή δε οι p, 2 είναι πρώτοι μεταξύ τους, το ab έχει τάξη $2p$. Έπεται ότι η $G =< ab >$ είναι κυκλική.
Στην δεύτερη περίπτωση, $bab^{-1} = a^{-1}$ και συνεπώς υπάρχει ομομορφισμός με την D_p (δες 4.4.4).

ΠΡΟΒΛΗΜΑΤΑ 5.2

Πρόβλημα 5.2.1 *Δείξε ότι οι ομάδες με 4, 9, 25, 49, 81, 121 και 169 στοιχεία είναι οπωσδήποτε αβελιανές.*

Πρόβλημα 5.2.2 *Βρες όλες τις μη-αβελιανές ομάδες τάξης 6, 10, 14, 22, 26, 34.*

5.3 Ευθύ γινόμενο ομάδων

Το ευθύ γινόμενο ομάδων ορίσαμε στην παράγραφο 1.4. Εδώ ερχόμαστε να εξετάσουμε τις συνθήκες κάτω από τις οποίες μπορεί να διασπασθεί μιά ομάδα σε ευθύ γινόμενο. Κατ' αρχήν τίθεται το ερώτημα πως εντοπίζονται, μέσα στην ομάδα που θέλουμε να διασπάσουμε, οι παράγοντες στους οποίους διασπάται η ομάδα. Την απάντηση δίδει η επόμενη πρόταση.

Πρόταση 5.3.1 *Μιά ομάδα G είναι ισόμορφη προς ένα ευθύ γινόμενο ομάδων $G_1 \times G_2$ τότε και μόνον τότε, όταν ικανοποιούνται οι επόμενες δύο συνθήκες:*
(1) Υπάρχουν δύο υποομάδες $A \subset G$ και $B \subset G$ της G με $ab = ba$, $\forall a \in A$, $\forall b \in B$.
(2) Κάθε στοιχείο $g \in G$ γράφεται με μοναδικό τρόπο $g = ab$, $a \in A$, $b \in B$.
Όταν ισχύουν αυτές οι συνθήκες, γράφουμε $G = AB$, τότε η G είναι ισόμορφη προς το $A \times B$ και αντίστροφα.

Η απόδειξη είναι πολύ απλή. Ξεκινάμε από το αντίστροφο με την εξής μορφή: Υποθέτουμε ότι υπάρχει ισομορφισμός $F : G_1 \times G_2 \longrightarrow G$ του γινομένου με την ομάδα G. Αμέσως ορίζονται δύο υποομάδες της $F(G_1 \times \{e_2\}) = A \subset G$, $F(\{e_1\} \times G_2) = B \subset G$ που θυμίζουν τους άξονες συντεταγμένων του $\mathbb{R}^2$. Διαπιστώνουμε εύκολα ότι οι υποομάδες αυτές ικανοποιούν τις παραπάνω συνθήκες. Γιά την (1): $ab = F(g_1, e_2)F(e_1, g_2) = F(g_1, g_2)$ και $ba = F(e_1, g_2)F(g_1, e_2) = F(g_1, g_2)$. Άρα $ab = ba$. Γιά την (2): $g = F(g_1, g_2) = F(g_1, e_2)F(e_1, g_2) = ab$, όπου $a = F(g_1, e_2)$ και $b = F(e_1, g_2)$. Η μοναδικότητα των a, b προκύπτει απλά: $ab = F(g_1, e_2)F(e_1, g_2) = F(g'_1, e_2)F(e_1, g'_2) = a'b'$ συνεπάγεται $F(g'^{-1}_1 g_1, g'^{-1}_2 g_2) = e$, άρα, λόγω της ισομορφικότητας της F, $g'^{-1}_1 g_1 = e_1$, $g'^{-1}_2 g_2 = e_2$.
Το αντίστροφο είναι εξ' ίσου απλό. Δοθέντων των υποομάδων $A \subset G$, $B \subset G$ που ικανοποιούν τις δύο συνθήκες, ορίζουμε αυτήν την φορά την απεικόνιση $F : A \times B \longrightarrow G$ με $F(a, b) = ab$. Το ότι η F είναι ομομορφισμός οφείλεται στην (1). Το ότι η F είναι ισομορφισμός προκύπτει αμέσως από το (2). Πράγματι, $F((a, b)*(a', b')) = F(aa', bb') = aa'bb'$. επίσης $F(a, b) = ab$, $F(a', b') = a'b' \Rightarrow F(a, b) * F(a', b') = aba'b' = aa'bb'$. Το τελευταίο λόγω της μεταθετικότητας. Αυτό δείχνει ότι η F είναι ομομορφισμος. Κατά το (2), κάθε $g \in G$ θα γράφεται μονοσήμαντα $g = ab = F(a, b)$. Αυτό δείχνει ότι η F είναι 1-1 και επί και ολοκληρώνει την απόδειξη.

Πρόταση 5.3.2 *Οι υποομάδες $A \subset G$ και $B \subset G$ της προηγούμενης πρότασης είναι κανονικές. Επίσης $A \cap B = \{e\}$.*

Προφανώς, αφού $bab^{-1} = bb^{-1}a = a$, που δείχνει την κανονικότητα της A. Ανάλογα και η κανονικότητα της B. Γιά τον δεύτερο ισχυρισμό $a \in A \cap B \Rightarrow e = a * a^{-1} = e * e \Rightarrow a = e$, $a^{-1} = e$, βάσει του μονοσήμαντου και θεωρώντας το $a \in A$ και το $a^{-1} \in B$.

Πρόταση 5.3.3 *Αν η πεπερασμένη ομάδα G έχει τάξη $|G| = n = kl$, όπου k, l πρώτοι μεταξύ τους και υπάρχουν κανονικές υποομάδες H, K, αντιστοίχων τάξεων k, l, τότε η G είναι ισόμορφη με το $H \times K$.*

Κατ' αρχήν το τυχόν $g \in H \cap K$ θα έχει τάξη r που διαιρεί και τους δύο ακέραιους k, l. Επειδή αυτοί είναι πρώτοι μεταξύ τους, θα είναι συνεπώς $r = 1$, άρα $x = e$. Επειδή επίσης $|HK| = |H||K|/|H \cap K|$ (2.5.3) έπεται το ζητούμενο.

Πρόταση 5.3.4 *Αν το στοιχείο της ομάδος $x \in G$, έχει τάξη $n = kl$, όπου $(k, l) = 1$, πρώτοι μεταξύ τους, τότε υπάρχει μοναδικό ζεύγος μετατιθεμένων στοιχείων, (a, b), αντιστοίχων τάξεων (k, l), με την ιδιότητα $x = ab$. Επιπλέον τα a, b, είναι ακέραιες δυνάμεις του x.*

Κατ' αρχήν, $(k, l) = 1$ συνεπάγεται ότι $ku + lv = 1$ για κάποιους ακέραιους (u, v). Προφανώς τότε θα ισχυει και $(k, lv) = 1 = (l, ku)$. Ορίζουμε λοιπόν $a = x^{lv}$, $b = x^{ku}$, τα οποία μετατίθενται μεταξύ τους και είναι και ακέραιες δυνάμεις του x, όπως τα θέλει ο τελευταίος ισχυρισμός. Επειδή $(k, lv) = 1$, το $a = x^{lv}$ έχει τάξη k και αντίστοιχα το b έχει τάξη l (δες 2.8.3).
Έστω τώρα ότι υπάρχει μιά δεύτερη ανάλυση σε γινόμενο $x = a'b' = b'a'$, με τις ίδιες τάξεις (k, l) για τα (a', b') αντιστοίχως. Υψώνοντας στην δύναμη lv και λαμβάνοντας υπόψιν ότι $(k, lv) = 1$, παίρνουμε $a = x^{lv} = (a'b')^{lv} = a'^{lv} = a'^{(lv+ku)} = a'$ και ανάλογα $b = b'$.

ΠΡΟΒΛΗΜΑΤΑ 5.3

Πρόβλημα 5.3.1 *Δείξε ότι η συνθήκη (2) της 5.3.1 είναι ισοδύναμη με τις εξής δύο:*
(1′) Κάθε στοιχείο $g \in G$ γράφεται σαν γινόμενο $g = ab,\ a \in A,\ b \in B$.
(2′) Η ισότητα $e = ab$ $a \in A,\ b \in B$, συνεπάγεται, $a = b = e$.

Πρόβλημα 5.3.2 *Δείξε ότι κάθε ομάδα τάξης p^2, όπου p πρώτος, είναι ισομορφική προς την $\mathbb{Z}_p^2$ ή την $\mathbb{Z}_p \times \mathbb{Z}_p$. (Υπόδειξη: Σκέψη ανάλογη της πρότασης 2.4.5).*

Πρόβλημα 5.3.3 *Γενίκευσε την τελευταία πρόταση 5.3.4 γιά γινόμενο περισσοτέρων παραγόντων $n = k_1...k_r$, όπου $(k_i,\ k_j) = 1,\ $ γιά $i \neq j$.*

5.4 Αδιάσπαστες ομάδες

Αδιάσπαστη λέγεται μιά ομάδα G όταν δεν υπάρχουν υποομάδες της $A \subset G$ και $B \subset G$ με τις δύο ιδιότητες του ευθέως γινομένου (πρόταση 5.3.1). Στον αντίποδα αυτών είναι οι **διασπώμενες** ομάδες, γιά τις οποίες υπάρχουν υποομάδες σαν τις A, B. Πως όμως αναγνωρίζεται η ύπαρξη τέτοιων υποομάδων όπως οι A, B;

Πρόταση 5.4.1 *Μιά ομάδα G είναι διασπώμενη, τότε και μόνον τότε, αν υπάρχει ενδομορφισμός $F : G \longrightarrow G$ με τις ιδιότητες:*
(1) $F^2 = F$.
(2) Γιά κάθε στοιχείο $g \in G$ ισχύει: $gF(x)g^{-1} = F(gxg^{-1})$.
Αν υπάρχει τέτοια απεικόνιση τότε η ομάδα είναι το ευθύ γινόμενο των $A = Im(F)$ και $B = Kern(F)$.

Ας αρχίσουμε αντίστροφα, υποθέτωντας ότι υπάρχουν δύο υποομάδες με τις ιδιότητες της (πρότασης 5.3.1). Ορίζουμε τότε την απεικόνιση F μέσω της δυνατότητας που έχουμε να γράψουμε κάθε $x \in G$ μονοσήμαντα σαν γινόμενο $x = ab$. Ορίζουμε λοιπόν $F(x) = a$. Κατ' αρχήν η F είναι ομομορφισμός αφού γιά $x = ab,\ x' = a'b'$ έχουμε $F(xx') = F(aba'b') = F(aa'bb') = aa' = F(x)F(x')$. Επίσης $F^2 = F$, διότι $F(F(x)) = F(a) = F(a * e) = a = F(x),\ \forall x \in G$. Τέλος $gF(x)g^{-1} = gag^{-1}$ και αν γράψουμε $g = a'b'$, τότε $gag^{-1} = (a'b')a(a'b')^{-1} = a'b'ab'^{-1}a'^{-1} = a'aa'^{-1}$, λόγω της μεταθετικότητας των a, b'. Το ίδιο αποτέλεσμα βρίσκουμε επίσης γιά το $F(gxg^{-1})$, και τούτο αποδεικνύει το (2).
Ας υποθέσουμε τώρα ότι έχουμε μιά F με τις δύο παραπάνω ιδιότητες. Ορίζουμε τότε τις υποομάδες $A = Im(F)$ και $B = Kern(F)$ και αποδεικνύουμε ότι ικανοποιούν τις δύο συνθήκες της (πρότασης 5.3.1). Κατ' αρχήν ισχύει $A \cap B = \{e\}$. Πράγματι, αν $x \in A \cap B$ τότε ταυτόχρονα $x = F(y)$ και $F(x) = e$. Τότε όμως $e = F(x) = F(F(y)) = F(y)$, άρα $y \in B = Kern(F) \Rightarrow x = F(y) = e$. Γιά τυχόν $x \in G$, έστω $a = F(x)$ και $b = a^{-1}x$. Προφανώς $a \in A = Im(F)$, $b \in B = Kern(F)$ και $x = ab$. Το μονοσήμαντο της παράστασης σαν γινόμενο προκύπτει από το ότι $A \cap B = \{e\}$. Πράγματι $ab = a'b' \Rightarrow a'^{-1}a = b'b^{-1} = x$ και το $x \in A \cap B$, άρα $x = e$. Μένει να δείξουμε ότι $ab = ba$. Όμως $bab^{-1} \in A$, αφού αν $a = F(y)$ τότε και $bab^{-1} = bF(y)b^{-1} = F(byb^{-1})$. Επίσης γιά κάθε $a = F(x) \in A \Rightarrow F(a) = F(F(x)) = F(x) = a$, δηλαδή η F αφήνει σταθερά τα στοιχεία του A. Τότε όμως τα $bab^{-1} \in A$ και $a \in A$ ταυτίζονται αφού $F(bab^{-1}) = F(b)F(a)F(b^{-1}) = F(a)$.

Παρατηρήσεις
(1) Από την προηγούμενη απόδειξη προκύπτει ότι η υποομάδα $A = Im(F)$ αποτελείται από σταθερά σημεία της F.
(2) Μιά γνήσια υποομάδα $A \subset G$ γιά την οποία υπάρχει άλλη υποομάδα $B \subset G$ με τις

ιδιότητες της (πρότασης 5.3.1), λέγεται **ευθύς παράγων** της G.
(3) Στην προηγούμενη παράγραφο είδαμε ότι κάθε ευθύς παράγων είναι κανονική υποομάδα της G. Άρα μιά ομάδα G που έχει έναν ευθύ παράγοντα δεν μπορεί να είναι απλή. Απλές ομάδες, συνεπώς, είναι μη-διασπώμενες ή αδιάσπαστες.
(4) Παράδειγμα αδιάσπαστης ομάδος είναι η $\mathbb{Z}$. Σ' αυτήν κάθε υποομάδα είναι της μορφής $m\mathbb{Z} = \{m \cdot t : t \in \mathbb{Z}\}$, δηλαδή αποτελείται από τα πολλαπλάσια ενός σταθερού μη-αρνητικού $m \in \mathbb{Z}$. Η τομή δύο τέτοιων υποομάδων είναι πάντοτε μη τετριμμένη, άρα η $\mathbb{Z}$ δεν έχει ευθείς παράγοντες.
(5) Το προηγούμενο παράδειγμα δείχνει ότι υπάρχουν ομάδες αδιάσπαστες και ταυτόχρονα μη-απλές.
(6) Άλλο παράδειγμα αδιάσπαστης και ταυτόχρονα μη-απλής ομάδας είναι η $G = \mathbb{Z}_p^a$, όπου p είναι πρώτος αριθμός και $a > 1$. Οι μόνες υποομάδες αυτής είναι οι $\mathbb{Z}_p^b$ με $b < a$. Προφανώς δε δύο τέτοιες υποομάδες A, B περιέχονται η μιά στην άλλη. Αν ήταν λοιπόν η $A \subset B$ ευθύς παράγων, θα έπρεπε $A = A \cap B = 0$ και συνεπώς $B = G$.

Πρόταση 5.4.2 *Μιά πεπερασμένη κυκλική ομάδα είναι αδιάσπαστη, τότε και μόνον τότε, αν η τάξη της είναι $|G| = p^a$, όπου p πρώτος και $a \geq 1$ φυσικός.*

Το ότι είναι αδιάσπαστη όταν η τάξη της είναι όπως αναφέρεται, το δείξαμε προηγουμένως. Έστω τώρα ότι $n = kl$ με k, l, πρώτους μεταξύ τους. Κατά το 2.6.2, υπάρχουν (κανονικές) υποομάδες H, K, αντιστοίχων τάξεων k, l και κατά το 5.3.3, η G είναι ισόμορφη με το $H \times K$.

5.5 Ευθύ γινόμενο περισσοτέρων παραγόντων

Στην παράγραφο αυτή γενικεύουμε την έννοια του ευθέως γινομένου για περισσότερους των δύο παράγοντες.

Πρόταση 5.5.1 *Η ομάδα G λέγεται ότι είναι το ευθύ γινόμενο των υποομάδων της $A_i \subset G$, $i = 1, ..., n$ όταν ισχύουν οι δύο επόμενες συνθήκες:*
(1) Για κάθε ζεύγος $A_i \subset G$ και $A_j \subset G$, ισχύει $ab = ba$, $\forall\, a \in A_i$, $\forall b \in A_j$.
(2) Κάθε στοιχείο $g \in G$ γράφεται με μοναδικό τρόπο $g = a_1...a_n$.
Όταν ισχύουν αυτές οι συνθήκες, γράφουμε $G = A_1...A_n$, τότε η G είναι ισόμορφη προς το $A_1 \times ... \times A_n$.

Η απόδειξη της πρότασης είναι στην ουσία η ίδια με αυτήν της 5.3.1. Το ίδιο ισχύει και γιά τις αποδείξεις των επομένων προτάσεων. Είναι εντελώς ανάλογες προς τις αποδείξεις των προτάσεων που έπονται της 5.3.1. Τις αφήνω λοιπόν σαν ασκήσεις γιά τον αναγνώστη.

Πρόταση 5.5.2 *Οι υποομάδες $A_i \subset G$, $i = 1, ..., n$, της προηγούμενης πρότασης είναι κανονικές. Επίσης $A_i \cap A_j = \{e\}$, $\forall i \neq j$.*

Πρόταση 5.5.3 *Με τις προϋποθέσεις της 5.5.1, οι απεικονίσεις $p_i : G \longrightarrow A_i$ με $p_i(g) = a_i$ (γιά $g = a_1...a_n$), είναι ομομορφισμοί, λέγονται **κανονικές προβολές** και ικανοποιούν τις συνθήκες:*
(1) Μετατίθενται με τους εσωτερικούς αυτομορφισμούς της G, δηλαδή $p_i(xgx^{-1}) = xp_i(g)x^{-1}$, $\forall g, x \in G$.
(2) Ικανοποιούν $p_i^2 = p_i$ και $p_i(G) = A_i$.
(3) Ικανοποιούν $p_i(p_j(x)) = p_j(p_i(x)) = e$, $\forall x \in G$ και γιά κάθε $i \neq j$.

Αντίστροφα, δοθέντων n ομομορφισμών με τις προηγούμενες τρεις ιδιότητες, η G διασπάται στο ευθύ γινόμενο $G = A_1...A_n$, όπου $A_i = p_i(G) = Im(p_i)$.

5.6 Πεπερασμένες αβελιανές ομάδες

Στην παράγραφο αυτή κάνουμε μιά πλήρη ταξινόμηση των πεπερασμένων αβελιανών ομάδων. Ξεκινάμε με μιά χρήσιμη απλή πρόταση που σχετίζεται με την πρόταση 2.4.5 καθώς και το πρόβλημα 5.3.2, αλλά με την προϋπόθεση ότι η ομάδα G είναι αβελιανή.

Πρόταση 5.6.1 *Έστω η αβελιανή ομάδα G, τάξεως $|G| = p^k$, όπου p πρώτος, $k \geq 1$, με την ιδιότητα $x^p = e$, $\forall x \in G$. Τότε η G είναι ευθύ άθροισμα $G = A_1...A_k$ κυκλικών ομάδων τάξεως p.*

Η απόδειξη της πρότασης είναι πολύ απλή και γίνεται επαγωγικά. Θεωρούμε πρώτα ένα στοιχείο $a_1 \neq e$ και την υποομάδα $A_1 =< a_1 >$. Υποθέτουμε κατόπιν (επαγωγική υπόθεση) ότι βρήκαμε n κυκλικές υποομάδες $A_1, ..., A_n$, τάξης p των οποίων το γινόμενο $A_1A_2...A_n$ είναι ευθύ (δηλ. το $G' = A_1A_2...A_n$ ικανοποιεί τις συνθήκες του 5.5.1). Προφανώς το $G' = A_1A_2...A_n$ έχει τάξη p^n. Αν $n < k$, θεωρούμε στοιχείο $a_{n+1} \in G$ που δεν ανήκει στο G'. Έστω $A_{n+1} =< a_{n+1} >$. Η A_{n+1} είναι τάξης p και $A_{n+1} \cap G' = \{e\}$. Διαφορετικά θα είχαμε $x \in A_{n+1} \cap G'$, $x \neq e$ και συνεπώς $a_{n+1} \in < x >= A_{n+1} \subset G'$, αντίθετα με την υπόθεση. Άρα το $A_1A_2...A_nA_{n+1}$ είναι ευθύ. Κατ' αυτόν τον τρόπο ορίζουμε επαγωγικά k κυκλικές υποομάδες A_i των οποίων το γινόμενο είναι ευθύ. Επειδή δε το $A_1A_2...A_k$ έχει τάξη p^k θα έχουμε $G = A_1...A_k$.

Πρόταση 5.6.2 *Έστω η αβελιανή ομάδα G, τάξεως $|G| = {p_1}^{k_1}...{p_r}^{k_r}$, όπου p_i πρώτοι διαφορετικοί μεταξύ τους και k_i φυσικοί αριθμοι. Έστω P_i η υποομάδα της G που αποτελείται από όλα τα στοιχεία της τάξεως ${p_i}^{k_i}$. Τότε η $|P_i| = {p_i}^{k_i}$ και η G είναι ευθύ άθροισμα $G = P_1...P_r$. Επίσης αυτή είναι η μόνη ανάλυση της G σε ευθύ άθροισμα υποομάδων με τάξεις δυνάμεις διαφορετικών πρώτων.*

Κατ' αρχήν, επειδή κάθε στοιχείο $x \in P_i$ έχει τάξη δύναμη του p_i, κατά την 5.2.3, το P_i θα έχει τάξη δύναμη του p_i. Επίσης $P_j \cap \prod_{i \neq j} P_i = \{e\}$, διότι κάθε στοιχείο του $x \in \prod_{i \neq j} P_i$ θα έχει τάξη έναν διαιρέτη του $\prod_{i \neq j} {p_i}^{k_i}$. Άρα το γινόμενο $G' = P_1...P_n$, είναι ευθύ. Κάθε $x \in G$ θα έχει τάξη s που διαιρεί το ${p_1}^{k_1}...{p_r}^{k_r}$ άρα της μορφής ${p_1}^{l_1}...{p_r}^{l_r}$, $l_i \leq k_i$. Χρησιμοποιώντας την 5.3.4, βλέπουμε ότι το x γράφεται $x = x_1...x_r$, όπου το x_i έχει τάξη ${p_i}^{l_i}$ άρα περιέχεται στο P_i. Αναλύεται λοιπόν η G σε ευθύ άθροισμα $G = P_1...P_r$. Τότε ${p_1}^{k_1}...{p_r}^{k_r} = |G| = |P_1||P_2|...|P_r|$, και επειδή η $|P_i|$ είναι δύναμις του p_i βλέπουμε ότι $|P_i| = {p_i}^{k_i}$.
Ας υποθέσουμε τώρα ότι η G γράφεται με άλλον τρόπο σαν ευθύ άθροισμα υποομάδων που πληρούν τις συνθήκες της πρότασης $G = Q_1...Q_s$. Τότε ${p_1}^{k_1}...{p_r}^{k_r} = |G| = |Q_1||P_2|...|Q_s|$ συνεπάγεται $s = r$ και , ενδεχομένως αναδιατάσσοντας τα Q_i , βρίσκουμε ότι αυτά έχουν τάξεις ${p_i}^{k_i}$ αντίστοιχα. Λόγω του ορισμού των P_i, έχουμε $Q_i \subset P_i$. Άρα $Q_i = P_i$.

Πρόταση 5.6.3 *Έστω η αβελιανή ομάδα G, τάξης $|G| = p^k$, p πρώτο και $k > 0$ ακέραιο. Έστω και $s \in G$, στοιχείο της μέγιστης δυνατής τάξης στην G. Τότε η κυκλική ομάδα που παράγεται από το s, $S =< s >$, είναι ευθύς παράγων της G.*

Έστω q η μέγιστη αυτή δυνατή τάξη. Αφού κάθε στοιχείο $x \in G$ θα έχει τάξη $q' \leq q \Rightarrow x^q = e$. Έστω T μιά υποομάδα μέγιστης τάξης της S που έχει τομή $S \cap T = \{e\}$. Ισχύει $G = S \oplus T$.

Πράγματι, ας υποθέσουμε ότι $S \oplus T \neq G$. Θα δείξουμε ότι αυτό οδηγεί σε άτοπο. Πράγματι, η τάξη της $G/(S \oplus T)$ είναι δύναμις του p, άρα η ομάδα αυτή (Cauchy) περιέχει στοιχείο τάξης p. Τούτο σημαίνει ότι υπάρχει $x \in G$, $x \notin S \oplus T$ και $x^p \in S \oplus T$, άρα $x^p = s^n t$, $t \in T$. (*) Τότε το $(x^p)^{\frac{q}{p}} = (s^n t)^{\frac{q}{p}} \Rightarrow e = x^q = (s^n)^{\frac{q}{p}} t^{\frac{q}{p}} \Rightarrow s^{\frac{nq}{p}} = t^{-\frac{q}{p}} \in S \cap T \Rightarrow s^{nq/p} = t^{q/p} = e$. Έπεται ότι το p διαιρεί το n (το nq/p πρέπει να είναι πολ/σιο του q). Έστω $n = pn'$ και $y = xs^{-n'}$. Από την (*) έχουμε $y^p = x^p s^{-n'p} = x^p s^{-n} = t \in T$. Επίσης $y \notin (S \oplus T)$, αφού διαφορετικά θα έπρεπε και το x να περιέχεται στο $(S \oplus T)$. Η υποομάδα $T' =< T, y >$, περιέχει την T ως γνήσια υποομάδα, άρα πρέπει να τέμνει το S. Ισχύει λοιπόν μιά σχέση της μορφής:

$$s^m = ty^k,\ t \in T, \quad k, m \in \mathbb{Z},\ m \neq 0 \bmod q.$$

Εάν το p διαιρούσε το k, τότε το $y^k \in T$ (αφού $y^p \in T$), άρα και το μη τετριμμένο στοιχείο s^m του S θα ήταν $s^m \in T$. Πράγμα που αντιφάσκει στην $S \cap T = \{e\}$. Συνεπώς το p δεν διαιρεί το k. Επειδή δε $y^p, y^k,$ είναι και τα δύο στην $S \oplus T,$ και $(p,\ k) = 1,$ έπεται ότι και το $y \in S \oplus T,$ πράγμα άτοπον. Συνεπώς $G = S \oplus T$.

Πρόταση 5.6.4 *Κάθε αβελιανή ομάδα αναλύεται σε ευθύ γινόμενο ορισμένων κυκλικών ομάδων που τάξεις τους είναι δυνάμεις πρώτων αριθμών. Οι παράγοντες του γινομένου, εκτός της διάταξής τους, είναι μονοσήμαντα ορισμένοι.*

Γιά την ανάλυση σε τέτοιους παράγοντες εφαρμόζουμε πρώτα την πρόταση 5.6.2 και διασπάμε μονοσήμαντα σε παράγοντες των οποίων οι τάξεις είναι δυνάμεις πρώτων διαφορετικών μεταξύ τους. Κατόπιν, εφαρμόζοντας την προηγούμενη πρόταση διασπάμε επαγωγικά κάθε έναν από τους παράγοντες με $|G| = p^k$ σε ευθύ γινόμενο κυκλικών ομάδων. Το μόνο που χρειάζεται να δείξουμε είναι το μονοσήμαντο των παραγόντων, όταν η τάξη της $|G| = p^k$. Γιά μιά τέτοια ανάλυση γράφουμε

$$G = a_1\mathbb{Z}_p \oplus a_2\mathbb{Z}_{p^2} \oplus ... \tag{5.1}$$

και πρέπει να δείξουμε ότι οι μη-αρνητικοί ακέραιοι a_1, a_2, ... προσδιορίζονται πλήρως από την δομή της G. Πράγματι, θα ισχύει

$$pG = a_2(p\mathbb{Z}_{p^2}) \oplus a_3(p\mathbb{Z}_{p^3})... \tag{5.2}$$

$p\mathbb{Z}_p = \{0\}$ αφού όλα τα στοιχεία της $\mathbb{Z}_p$ είναι τάξης p.

$$G/pG = a_1\mathbb{Z}_p/(p\mathbb{Z}_p) \oplus a_2\mathbb{Z}_{p^2}/(p\mathbb{Z}_{p^2}) \oplus ..., \tag{5.3}$$

όπου όλοι οι παράγοντες είναι ομάδες τάξης p. Έπεται ότι η $G/(pG)$ είναι τάξης p^{n_1}, όπου

$$n_1 = a_1 + a_2 + ... \tag{5.4}$$

Αντικαθιστώντας στα προηγούμενα την G με την pG και την pG με την p^2G κτλ. βλέπουμε ότι οι ομάδες $G/pG,\ \ pG/p^2G,\ \ p^2G/p^3G,\ \ ...$ που καθορίζονται όλες πλήρως από την G, και έχουν αντίστοιχες τάξεις $p^{n_1}, p^{n_2}, ... : n_1 = a_1 + a_2 + ...,\ \ n_2 = a_2 + a_3 + ...,\ \ n_3 = a_3 + a_4 + ...$ κτλ. Τα $a_1 = n_1 - n_2,\ \ a_2 = n_2 - n_3,\ \ $ κτλ. καθορίζονται συνεπώς μονοσήμαντα από την G.

Παρατηρήσεις

(1) Γιά κάθε δύναμη πρώτου αριθμού $q = p^k$, και κάθε διαμέριση του k σε ένα άθροισμα μη-αρνητικών ακεραίων $k = a_1 + ... + a_r,\ r \leq k$ αντιστοιχεί ένα γινόμενο κυκλικών ομάδων

$G = \mathbb{Z}_{p^{a_1}} \oplus ... \oplus \mathbb{Z}_{p^{a_k}}$ τάξης q και αντίστροφα. Το πλήθος των αβελιανών ομάδων τάξης $q = p^k$, ευρίσκεται λοιπόν σε αμφιμονόσημαντο αντιστοιχεία με το πλήθος των διαμερίσεων του k σε μη αρνητικούς προσθεταίους.

(2) Γιά παράδειγμα, το $q = p^4$, δίδει 5 διαφορετικές ομάδες, διότι τόσες είναι οι διαμερίσεις του 4:

$$4, \;\; 3+1, \;\; 2+2, \;\; 2+1+1, \;\; 1+1+1+1,$$

που αντιστοιχούν στις αβελιανές ομάδες:

$$\mathbb{Z}_{p^4}, \;\; \mathbb{Z}_{p^3} \oplus \mathbb{Z}_p, \;\; \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}, \;\; \mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p, \;\; \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p.$$

ΠΡΟΒΛΗΜΑΤΑ 5.6

Πρόβλημα 5.6.1 *Βρές τα $a_1, a_2, ...$ και $n_1, n_2, ...$ που αναφέρονται στην πρόταση 5.6.4, γιά τις αβελιανές ομάδες τάξης p^4 της τελευταίας παρατήρησης.*

Πρόβλημα 5.6.2 *Προσδιόρισε όλες τις διαμερίσεις του 5 και βρες όλες τις αβελιανές ομάδες τάξης p^5, όπου p πρώτος.*

Πρόβλημα 5.6.3 *Προσδιόρισε όλες τις αβελιανές ομάδες τάξεων 6, 12, 27 , 108.*

Κεφάλαιο 6

Ημιευθύ γινόμενο ομάδων

Είναι λίγο πιό πολύπλοκο από το ευθύ αλλά περιλαμβάνει πολλές σημαντικές ομάδες που ενώ δεν διασπώνται σε ευθύ, διασπώνται σε ημιευθύ γινόμενο. Τα απλούστερα παραδείγματα είναι οι διεδρικές ομάδες, οι ομάδες ισομετριών των ευκλειδείων χώρων και ειδικώτερα του τρισδιάστατου χώρου ($\mathbb{R}^3$) καθώς και πεπερασμένες ομάδες των οποίων η τάξη γράφεται σαν γινόμενο ορισμένων πρώτων αριθμών. Τα τελευταία παραδείγματα συμπεριλαμβάνουν ομάδες όπως αυτές με τάξεις αντίστοιχα: $|G| = pq$ και $|G| = p^3$, όπου p, q, πρώτοι αριθμοί. Ξεκινώ με την ανάλυση των ισομετριών του χώρου. Τα περί των ομάδων $O(3)$ και $Iso(\mathbb{R}^3)$, που συζητούνται παρακάτω, θα μπορούσαν να μεταφερθούν, σχεδόν αυτολεξί, στις n διαστάσεις και τις αντίστοιχες ομάδες $O(n)$ και $Iso(\mathbb{R}^n)$. Ωστόσο, γιά την απλότητα της συζήτησης, περιορίζομαι στις 3 διαστάσεις.

6.1 Η ομάδα O(3)

Η ομάδα αυτή είναι υποομάδα της $GL(3, \mathbb{R})$, ομάδας των αντιστρεψίμων 3×3 πραγματικών πινάκων. Οι πίνακες $A \in O(3)$, που την αποτελούν, ονομάζονται **ορθογώνιοι** και χαρακτηρίζονται από το γεγονός ότι έχουν ως αντίστροφο $A^{-1} = A^t$, τον λεγόμενο **ανάστροφο** A^t που προκύπτει από τον A εναλλάσσοντας τον ρόλο γραμμών και στηλών. Αν με $(A)_{ij}$ συμβολίζουμε το στοιχείο στην $i-$ γραμμή και $j-$ στήλη της A, τότε $(A^t)_{ij} = (A)_{ji}$. Π.χ.

$$A = \begin{pmatrix} 1\ 2\ 3 \\ 4\ 5\ 6 \\ 7\ 8\ 9 \end{pmatrix} \Rightarrow A^t = \begin{pmatrix} 1\ 4\ 7 \\ 2\ 5\ 8 \\ 3\ 6\ 9 \end{pmatrix}.$$

Λαμβάνοντας υπόψιν τον ορισμό του γινομένου πινάκων, βλέπουμε αμέσως ότι $(AB)^t = B^t A^t$, που έχει σαν συνέπεια ότι το γινόμενο ορθογωνίων πινάκων είναι πάλι ορθογώνιος πίνακας. $A^{-1} = A^t$, $B^{-1} = B^t$, $\Rightarrow (AB)^{-1} = B^{-1}A^{-1} = B^t A^t = (AB)^t$. Η $O(3)$ λοιπόν είναι υποομάδα της $GL(n, \mathbb{R})$ και σχετίζεται άμεσα με τον χώρο $\mathbb{R}^3$ και το εσωτερικό γινόμενο $(x, y) = x_1y_1 + x_2y_2 + x_3y_3$, $\forall x = (x_1, x_2, x_3)$, $\forall y = (y_1, y_2, y_3) \in \mathbb{R}^3$, που ορίζεται σ' αυτόν.

Γενικά, κάθε πίνακας $A \in GL(n, \mathbb{R})$, ορίζει απεικόνιση που συμβολίζουμε με το ίδιο γράμμα $A : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ με $Ax = y = (y_1, \ldots, y_n)$ και $y_i = \sum_{j=1}^n a_{ij}x_j$, γιά κάθε $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$. Η απεικόνιση αυτή χρησιμοποιεί τον πολλαπλασιασμό πινάκων (πίνακα επί διάνυσμα-στήλη για την ακρίβεια) και στην σύνθεση απεικονίσεων αντιστοιχεί το γινόμενο πινάκων AB. Η απεικόνιση είναι γραμμική:

$$A(x + y) = Ax + Ay, \quad \forall x, y \in \mathbb{R}^n. \tag{6.1}$$

Ενδιαφέρουσα είναι και η σχέση που συνδέει τον ανάστροφο με το εσωτερικό γινόμενο:

$$(Ax,\, y) = (x,\, A^t y),\ \ \forall x,\, y \in \mathbb{R}^n. \tag{6.2}$$

Η οποία για τον ορθογώνιο πίνακα $A \in O(3)$ συνεπάγεται:

$$(Ax,\, Ay) = (x,\, A^t Ay) = (x,\, A^{-1} Ay) = (x,\, y),\ \ \forall x,\, y \in \mathbb{R}^3. \tag{6.3}$$

Θυμίζω ότι το **μέτρο** διανύσματος εκφράζεται μέσω του εσωτερικού γινομένου:

$$|x| = \sqrt{x_1^2 + x_2^2 + x_3^2} = \sqrt{(x,\, x)}\ \ \Rightarrow |x|^2 = (x,\, x). \tag{6.4}$$

Το ίδιο δε και η **απόσταση**:

$$d(x,\, y) = |x - y| = \sqrt{(x - y, x - y)},\ \ \forall x,\, y \in \mathbb{R}^3. \tag{6.5}$$

Από αυτές προκύπτει αμέσως η

$$d(Ax,\, Ay) = d(x,\, y),\ \ \forall x,\, y \in \mathbb{R}^3,\ \forall A \in O(3). \tag{6.6}$$

Με άλλα λόγια, οι απεικονίσεις που ορίζονται από ορθογώνιους πίνακες διατηρούν την απόσταση μεταξύ δύο σημείων του χώρου, είναι λοιπόν, όπως λέμε **ισομετρίες** του χώρου.

Πρόταση 6.1.1 *Οι στήλες ενός ορθογώνιου πίνακα $A \in O(3)$ αποτελούν ορθοκανονική βάση. Αντίστροφα, αν $a_1,\, a_2,\, a_3 \in \mathbb{R}^3$ είναι τρία ορθοκανονικά διανύσματα, τότε ο πίνακας που έχει αυτά τα διανύσματα ως στήλες είναι ορθογώνιος.*

Η απόδειξη είναι ένας τυπικός λογαριασμός που χρησιμοποιούμε τις ιδιότητες του εσωτερικού γινομένου και τους ορισμούς. Ένα σύνολο διανυσμάτων $\{a_1,\, a_2,\, ...\}$, λέγεται ορθοκανονικό, όταν $(a_i,\, a_j) = 0$ γιά $i \neq j$ και $(a_i,\, a_i) = 1$ γιά $i = 1,\, 2,\, ...$ Το πιό απλό σύστημα ορθοκανονικών διανυσμάτων είναι το γνωστό $e_1 = (1,\, 0,\, 0)^t$, $e_2 = (0,\, 1,\, 0)^t$, $e_3 = (0,\, 0,\, 1)^t$. Ο εκθέτης t δηλώνει ότι θεωρούμε το ανάστροφο του διανύσματος-γραμμή δηλαδή το διάνυσμα στήλη. Τότε ο πολλαπλασιασμός $Ae_i = a_i$ δίνει την $i-$στή στήλη του πίνακα A. Η δε σχέση $(a_i,\, a_j) = (Ae_i,\, Ae_j) = (e_i, e_j)$ φανερώνει ότι οι στήλες ενός ορθογώνιου πίνακα είναι ορθοκανονικά διανύσματα. Και αντίστροφα, η ίδια σχέση φανερώνει ότι ο πίνακας που προκύπτει από ορθοκανονικά $\{a_1,\, a_2,\, a_3\}$ είναι ορθογώνιος.

6.2 Η ομάδα $Iso(\mathbb{R}^3)$

Γενικώτερα **ισομετρία** του χώρου ονομάζουμε κάθε απεικόνιση F του χώρου στον εαυτό του που διατηρεί την απόσταση:

$$F : \mathbb{R}^3 \longrightarrow \mathbb{R}^3,\ \ d(F(x),\, F(y)) = d(x,\, y)\ \ \forall x,\, y \in \mathbb{R}^3. \tag{6.7}$$

Κατ' αναλογίαν με τις ισομετρίες του επιπέδου που εξετάσαμε στο κεφάλαιο για τις διεδρικές ομάδες, το σύνολο των ισομετριών του χώρου αποτελεί ομάδα που συμβολίζουμε με $Iso(\mathbb{R}^3)$. Η ομάδα $O(3)$ των ορθογωνίων πινάκων είναι ισόμορφη προς μία υποομάδα αυτής της ομάδας. Ο ισομορφισμός αντιστοιχεί στο πίνακα $A \in O(3)$ την αντίστοιχη γραμμική απεικόνιση $y = Ax$ του $\mathbb{R}^3$ στον εαυτό του. Μέσω αυτού του ισομορφισμού ταυτίζομε την $O(3)$ με την αντίστοιχη υποομάδα του $Iso(\mathbb{R}^3)$ και γράφουμε πλέον $O(3) \subset Iso(\mathbb{R}^3)$. Η υποομάδα αυτή έχει μιά χαρακτηριστική ιδιότητα, ανάμεσα στο πλήθος των γενικών ισομετριών. Αφηνει το $0 \in \mathbb{R}^3$ σταθερό. Εύλογα λοιπόν τις ισομετρίες αυτές τις ονομάζουμε **ορθογώνιες**.

Πρόταση 6.2.1 *Κάθε ισομετρία $F \in Iso(\mathbb{R}^3)$, με την ιδιότητα $F(0) = 0$ είναι της μορφής $F(x) = Ax$, με $A \in O(3)$.*

Εφαρμόζω την ταυτότητα που εκφράζει το εσωτερικό γινόμενο συναρτήσει του μέτρου:

$$-2(x,\, y) = (x - y,\, x - y) - (x,\, x) - (y,\, y),\ \forall x,\, y \in \mathbb{R}^3.$$

Εφαρμόζοντας την προηγούμενη παίρνουμε: $-2(F(x),\, F(y)) = (F(x) - F(y), F(x) - F(y)) - (F(x), F(x)) - (F(y), F(y)) = d(F(x),\, F(y))^2 - d(F(x),\, 0)^2 - d(F(y),\, 0)^2 = d(x,\, y)^2 - d(x,\, 0)^2 - d(y,\, 0)^2 = -2(x,\, y)$ και τούτο $\forall x,\, y \in \mathbb{R}^3$. Με άλλα λόγια η F διατηρεί το εσωτερικό γινόμενο. Τότε όμως ορθοκανονικά διανύσματα θα απεικονίζονται σε ορθοκανονικά. Ειδικά τα $a_1 = F(e_1),\, a_2 = F(e_2),\, a_3 = F(e_3)$, θα είναι ορθοκανονικά και κατά συνέπεια θα ορίζεται ορθογώνιος πίνακας A με στήλες τα $\{a_1,\, a_2,\, a_3\}$. Ας συμβολίζουμε με $G(x) = Ax$ την ισομετρία που ορίζεται από τον ορθογώνιο πίνακα A. Τότε η απεικόνιση $H = G^{-1} \circ F$, είναι ισομετρία, διατηρεί κι' αυτή το εσωτερικό γινόμενο και ικανοποιεί $H(e_i) = G^{-1}(a_i) = A^t a_i = e_i$. Συνεπώς κάθε $x = (x_1,\, x_2,\, x_3)$ απεικονίζεται στο $y = H(x)$ και ισχύει $y_i = (y,\, e_i) = (H(x), H(e_i)) = (x,\, e_i) = x_i$. Με άλλα λόγια η H απεικονίζει κάθε διάνυσμα στον εαυτό του, άρα είναι η ταυτοτική $G^{-1} \circ F = I \Rightarrow F(x) = G(x) = Ax,\ \forall x \in \mathbb{R}^3$.

Μεταφορά λέμε μιά απεικόνιση της μορφής $T(x) = x + v$, όπου $v \in \mathbb{R}^3$ είναι ένα σταθερό διάνυσμα. Το v λέγεται διάνυσμα μεταφοράς. Προφανώς η μεταφορά είναι ισομετρία και η αντίστροφή της είναι μεταφορά κατά το αντίθετο διάνυσμα $-v$.

Πρόταση 6.2.2 *Το σύνολο των μεταφορών αποτελεί υποομάδα του $Iso(\mathbb{R}^3)$, ισόμορφη προς την $\mathbb{R}^3$ (θεωρούμενη ομάδα με την πρόσθεση διανυσμάτων).*

Η απόδειξη είναι προφανής. Το γινόμενο δύο μεταφορών $T_1(x) = x + v_1$ και $T_2(x) = x + v_2$, είναι η μεταφορά $T_2 \circ T_1(x) = x + (v_1 + v_2)$. Και ο ισομορφισμός είναι η απεικόνιση που αντιστοιχεί στην $T(x) = x + v$ το διάνυσμα μεταφοράς $v \in \mathbb{R}^3$. Στο εξής θα ταυτίζουμε λοιπόν το $\mathbb{R}^3$ με μιά υποομάδα του $Iso(\mathbb{R}^3)$ και θα γράφουμε $\mathbb{R}^3 \subset Iso(\mathbb{R}^3)$.

Πρόταση 6.2.3 *Κάθε ισομετρία $F \in Iso(\mathbb{R}^3)$, γράφεται $F(x) = Ax + v$, με $A \in O(3)$ και $v \in \mathbb{R}^3$. Με άλλα λόγια κάθε ισομετρία είναι σύνθεση μιάς ορθογώνιας ισομετρίας και μιάς μεταφοράς.*

Η απόδειξη είναι πολύ εύκολη. Θεωρούμε το διάνυσμα $v = F(0)$ και την μεταφορά $T(x) = x - v$. Τότε η ισομετρία $G = T \circ F \in Iso(\mathbb{R}^3)$, αφήνει το 0 σταθερό: $G(0) = T(F(0)) = F(0) - v = 0$. Κατά την 6.2.1 λοιπόν, θα υπάρχει ορθογώνιος πίνακας $A \in O(3)$, έτσι ώστε $G(x) = Ax$, $\forall x \in \mathbb{R}^3$, που αποδεικνύει το ζητούμενο.

Έχουμε λοιπόν την $Iso(\mathbb{R}^3)$ και δύο διακεκριμένες υποομάδες της, την υποομάδα των στροφών $O(3)$ και την υποομάδα των μεταφορών $\mathbb{R}^3$. Από την τελευταία επίσης πρόταση βλέπουμε ότι σε κάθε ισομετρία F αντιστοιχεί μονοσήμαντα ένα ζεύγος $(A,\, v) \in O(3) \times \mathbb{R}^3$. Είναι λοιπόν η ομάδα ισόμορφη με το $O(3) \times \mathbb{R}^3$; Η απάντηση είναι *σχεδόν* αλλά όχι ακριβώς. Σαν σύνολο είναι, αλλά η δομή ομάδος δεν είναι αυτή του γινομένου των ομάδων. Αν ταυτίσουμε την F με το ζεύγος $(A,\, v)$, τότε στην σύνθεση δύο ισομετριών $F_1(x) = A_1 x + v_1$ και $F_2(x) = A_2 x + v_2$, $G = F_2 \circ F_1$, έχουμε $G(x) = F_2(F_1(x)) = F_2(A_1 x + v_1) = A_2(A_1 x + v_1) + v_2 = A_2 A_1 x + (A_2 v_1 + v_2)$. Άρα στην $F_2 \circ F_1$ αντιστοιχεί το ζεύγος $(A_2 A_1,\, A_2 v_1 + v_2)$ και όχι το $(A_2 A_1,\, v_1 + v_2)$ που αντιστοιχεί στο γινόμενο των ομάδων. Αυτό που χρειάζεται είναι να τροποποιήσουμε την πράξη στο $O(3) \times \mathbb{R}^3$ και αυτό οδηγεί στο ημιευθύ γινόμενο.

6.3 Δράση ομάδος

Δράση ομάδας G σε ένα σύνολο $X \neq \emptyset$, λέμε έναν ομομορφισμό$F : G \longrightarrow S(X)$, της ομάδας στην ομάδα μεταθέσεων $S(X)$, του X. Η δράση λέγεται **πιστή**, όταν είναι 1-1, ή ισοδύναμα, ο πυρήνας του ομομορφισμού είναι τετριμμένος $Kern(F) = \{e\}$.

Από τον ορισμό έχουμε ότι κάθε $F(g)$ είναι μία αντιστρέψιμη απεικόνιση $F(g) : X \longrightarrow X$. Συχνά παραλείπουμε το σύμβολο F και γράφουμε gx αντί του $F(g)x$. Από την ιδιότητα του ομορφισμού έχουμε ότι τα στοιχεία g, g^{-1}, ορίζουν αντίστροφες μεταθέσεις του X, $g^{-1}gx = x$.

Παραδείγματα δράσεων Δράσεις έχουμε ήδη συναντήσει χωρίς να το αναφέρουμε. Κατ' αρχήν μιά ομάδα δρα στον εαυτό της με πολλούς τρόπους.
(1) $X = G$ και $L : G \longrightarrow S(X)$ η απεικόνιση που σε κάθε $g \in G$ αντιστοιχεί τον πολλαπλασιασμό από αριστερά με το g, $L(g)x = gx$, $\forall x \in G$.
(2) $X = G$ και $R : G \longrightarrow S(X)$ η απεικόνιση που σε κάθε $g \in G$ αντιστοιχεί τον πολλαπλασιασμό από τα δεξιά με το g^{-1}, $R(g)x = xg^{-1}$. Τον εκθέτη -1 χρειαζόμαστε για να έχουμε πραγματικό ομομορφισμό $R : G \longrightarrow S(G)$, $R(gh)x = x(gh)^{-1} = xh^{-1}g^{-1} = R(g)R(h)x$.
(3) $X = G$ και $I : G \longrightarrow S(X)$, η απεικόνιση που σε κάθε $g \in G$ αντιστοιχεί την συζυγία με το στοιχείο g, $I(g)x = gxg^{-1}$. Οι δύο πρώτες δράσεις είναι πιστές. Η τελευταία μπορεί να είναι πιστή ή όχι, ανάλογα με το αν η G έχει κέντρο ή όχι. Το κέντρο $Z(G)$ της ομάδας είναι ακριβώς ο πυρήνας της I.
(4) Η ομάδα $GL(n, \mathbb{R})$ δρα φυσιολογικά στον χώρο $\mathbb{R}^n$, μέσω του πολλαπλασιασμού διανύσματος-στήλη με πίνακα. Πράγματι, σε κάθε $A \in GL(n, \mathbb{R})$ αντιστοιχούμε την γραμμική απεικόνιση $L(A) : \mathbb{R}^n \longrightarrow \mathbb{R}^n$, $L(A)x = Ax$.

Τροχιά ενός σημείου $x \in X$, ως προς την δράση της ομάδος G στο X, λέμε το σύνολο των σημείων $\{gx : g \in G\}$ που συχνά συμβολίζουμε με Gx. Δύο σημεία x, $y \in X$ είναι στην ίδια τροχιά, τότε και μόνον, όταν υπάρχει $g \in G$ με την ιδιότητα $gx = y$. Εύκολα βλέπουμε ότι, γιά τα σημεία του X, η σχέση του ανήκειν στην ίδια τροχιά, είναι μιά σχέση ισοδυναμίας, της οποίας οι κλάσεις ισοδυναμίας είναι ακριβώς οι τροχιές. Κάθε δράση λοιπόν επάγεται μιά διαμέριση του X σε υποσύνολα, τις τροχιές της δράσης. Ειδικές περιπτώσεις τροχιών μιάς δράσης πάνω σε μιά ομάδα είναι τα σύμπλοκά της ως προς κάποια ομάδα (αριστερά και δεξιά) και οι κλάσεις συζυγίας. Η δράση λέγεται **μεταβατική** όταν έχει μία και μόνον τροχιά. **Απλά** μεταβατική λέγεται η μεταβατική δράση, γιά την οποία η $gx = x$, γιά ένα σημείο $x \in X$ συνεπάγεται $g = e$. Με άλλα λόγια, η μεταβατική δράση της οποίας η μόνη απεικόνιση $F(g) \in S(X)$, που έχει σταθερά σημεία είναι η ταυτοτική. **Σταθεροποιητής** ενός σημείου $x \in X$ ως προς μιά δράση της ομάδας G στο X , λέγεται η υποομάδα $H \subseteq G$ της G που αποτελείται από όλα εκείνα τα $g \in G$ που αφήνουν το x σταθερό: $gx = x$. Τον σταθεροποιητή του $x \in X$ συμβολίζουμε συχνά με G_x. Στην περίπτωση της απλά μεταβατικής δράσης, όλοι οι σταθεροποιητές ταυτίζονται με την τετριμμένη ομάδα.

Πρόταση 6.3.1 *Οι σταθεροποιητές G_x και G_y δύο σημείων στην ίδια τροχιά μιάς δράσης είναι ισόμορφες υποομάδες της G και μάλιστα συζυγείς.*

Δείχνουμε ότι $gG_xg^{-1} \subseteq G_y$, εφόσον τα σημεία $y = gx$ είναι στην ίδια τροχιά. Πράγματι, αν $h \in G_x$, τότε $ghg^{-1}y = ghg^{-1}gx = ghx = gx = y$, άρα $ghg^{-1} \in G_y$.

Πρόταση 6.3.2 *Υπάρχει αμφιμονοσήμαντη αντιστοιχεία μεταξύ των σημείων της τροχιάς Gx και του συνόλου πηλίκου G/G_x. Γιά πεπερασμένα σύνολα: $|Gx| = [G : G_x]$.*

Αρκεί να θεωρήσουμε την απεικόνιση $T : G/G_x \longrightarrow Gx$, με $T(gG_x) = gx$. Προφανώς η T είναι επί και $T(gG_x) = gx = g'x = T(g'G_x)$, συνεπάγεται ότι $g^{-1}g' \in G_x \Rightarrow gG_x = g'G_x$, που δείχνει το 1-1.

Πρόταση 6.3.3 *Γιά κάθε δράση πεπερασμένης ομάδος G σε πεπερασμένο σύνολο X, ας συμβολίζομε με $N(G,X)$ το πλήθος των τροχιών και με n_g το πλήθος των σταθερών σημείων της $g : X \to X$. Τότε ισχύει:*

$$N(G,X)|G| = \sum_{g\in G} n_g.$$

Ορίζουμε την συνάρτηση $\delta_{g,x} = 1$, όταν $gx = x$ και $\delta_{g,x} = 0$, όταν $gx \neq x$. Με την βοήθεια αυτής της συνάρτησης μπορούμε να γράψουμε το δεξί μέλος της ισότητας σαν διπλό άθροισμα:

$$\sum_{g\in G} n_g = \sum_{g\in G}(\sum_{x\in X} \delta_{g,x}) = \sum_{x\in X}(\sum_{g\in G} \delta_{g,x}) = \sum_{x\in X}(|G_x|) = \sum_{N(G,X)} (\sum_{y\in Gx} |G_y|).$$

Στο τελευταίο διπλό άθροισμα, η εξωτερική άθροιση γίνεται ως προς τις διαφορετικές τροχιές και η εσωτερική ως προς τα σημεία μιάς συγκεκριμένης τροχιάς. Επειδή όλες οι G_y για τα $y \in Gx$ είναι ισόμορφες, άρα έχουν το ίδιο πλήθος στοιχείων, το εσωτερικό άθροισμα είναι $|G_x| \sum_{y\in Gx} 1 = |G_x||Gx| = |G|$. Τούτο αποδεικνύει την πρόταση.

ΠΡΟΒΛΗΜΑΤΑ 6.3

Πρόβλημα 6.3.1 *Ξαναδές την ανάλυση μιάς μετάθεσης $t \in S_n$ σε κύκλους και βρες την δράση, της οποίας οι τροχιές είναι ακριβώς οι κύκλοι στους οποίους αναλύεται η μετάθεση. (Υπόδειξη: Η ομάδα $< t >$ δρα στο $\underline{n}$.)*

Πρόβλημα 6.3.2 *Δείξε ότι τα σύμπλοκα gH μιάς ομάδας G ως προς υποομάδα της H είναι τροχιές μιάς δράσης της H στην G. (Υπόδειξη: $R : H \to S(G)$, $R(h)(g) = gh^{-1}$.)*

Πρόβλημα 6.3.3 *Δείξε ότι γιά την δράση της προηγούμενης άσκησης, η πρόταση 6.3.3 είναι ισοδύναμη με την $|G| = |H|[G : H]$.*

Πρόβλημα 6.3.4 *Θεώρησε την δράση της ομάδας των μοναδιαίων μιγαδικών αριθμών στο μιγαδικό επίπεδο: $F : S^1 \longrightarrow S(\mathbb{C})$, $F(s)(z) = sz$. Βρες τις τροχιές αυτής της δράσης.*

Πρόβλημα 6.3.5 *Θεώρησε την δράση της ομάδας των αντιστρεψίμων πινάκων στον εαυτό της: $F : GL(n,\mathbb{R}) \longrightarrow S(GL(n,\mathbb{R}))$, $F(g)(x) = gx$ (πολλαπλασιασμός πίνακα επί πίνακα). Βρες τις τροχιές αυτής της δράσης. Είναι η δράση μεταβατική ή απλά-μεταβατική;*

Πρόβλημα 6.3.6 *Θεώρησε την δράση της ομάδας των αντιστρεψίμων πινάκων στον $n-$διάστατο χώρο: $F : GL(n,\mathbb{R}) \longrightarrow S(\mathbb{R}^n)$, $F(g)(x) = gx$ (πολλαπλασιασμός πίνακα επί διάνυσμα στήλη). Βρες τις τροχιές αυτής της δράσης.*

Πρόβλημα 6.3.7 *Έστω G ομάδα και $H \subset G$ υποομάδα. Θεώρησε την δράση της G στο σύνολο πηλίκον $\bar{H} = G/H$, $F(g)(xH) = (gx)H$. Δείξε ότι ο πυρήνας της F είναι μιά κανονική υποομάδα της G που περιέχεται στην H. Συμπέρανε ότι αν η H είναι απλή τότε η δράση F είναι 1-1 και η ομάδα $F(G) \subset S(\bar{H})$ είναι ισόμορφη με την G.*

6.4 Ημιευθύ γινόμενο

Πρόταση 6.4.1 *Δοθέντων δύο ομάδων A, B και μιάς δράσης $F : A \to Aut(B)$, με $F(A) \subseteq Aut(B)$, δηλαδή δράσης γιά την οποία τα $F(a) : B \to B$ είναι αυτομορφισμοί της ομάδος B, ορίζεται δομή ομάδος στο σύνολο $B \times A$ μέσω του τύπου:*

$$(b,\, a)(b',\, a') = (b(F(a)b', aa')),\ \ \forall (b,\, a),\, (b',\, a') \in B \times A.$$

Την ομάδα αυτή συμβολίζουμε με $B \times_F A$. Η ισόμορφη της B, υποομάδα $B' = B \times \{e_A\}$ της $B \times_F A$, είναι κανονική.

Παραλείποντας την F γράφω $(b,\, a)(b',\, a') = (ba(b'),\, aa')$ και εννοώ φυσικά το σωστό $(b(F(a)b'), aa')$. Το $(e_B,\, e_A)$ είναι το μοναδιαίο. Το αντίστροφο του $(b,\, a)$ είναι:

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

Πράγματι $(e_B,\, e_A)(b,\, a) = (e_B e_A(b), e_A a) = (b,\, a)$, αφού $e_A(b) = b$. Παρόμοια δείχνουμε ότι $(b,\, a)(e_B,\, e_A) = (b,\, a)$. Γιά το αντίστροφο $(b,\, a)(a^{-1}(b^{-1}), a^{-1}) = (ba(a^{-1}(b^{-1})), aa^{-1}) = (bb^{-1},\, e_A) = (e_A,\, e_B)$. Η τελευταία διότι η $a(a^{-1}(b)) = b$, (δηλ. η $F(a)F(a^{-1})(b) = F(aa^{-1})(b) = F(e_A)(b) = b$) αφού η F είναι ομομορφισμός. Ανάλογα αποδεικνύονται και οι υπόλοιπες ιδιότητες της ομάδος.
Γιά την κανονικότητα εξετάζουμε το $(e_B, a)(b, e_A)(e_B, a)^{-1}$. Σύμφωνα με τα προηγούμενα τούτο είναι ίσον με το $(b, a) = (a(b), a)(e_B, a^{-1}) = (a(b), e_A) \in B'$.

Παρατηρήσεις Την ομάδα $B \times_F A$ ονομάζουμε **ημιευθύ** γινόμενο των ομάδων B, και A, ως προς την δράση $F : A \to Aut(B)$.
(1) Οι ομάδες A, B που ορίζουν το ημιευθύ γινόμενο είναι ισόμορφες με τις αντίστοιχες υποομάδες $A' = \{e_B\} \times A$ και $B' = B \times \{e_A\}$ του $B \times_F A$.
(2) Σαν σύνολο, το $B \times_F A$ συμπίπτει με το $B \times A$, όμως η πράξη ομάδος διαφέρει από την πράξη-γινόμενο που ορίζεται συνήθως στο καρτεσιανό γινόμενο ομάδων.
(3) Κάθε στοιχείο της ομάδος $G = B \times_F A$ γράφεται μονοσήμαντα σαν γινόμενο $g = b'a'$ με $a' \in A'$ και $b' \in B'$. Επίσης το γινόμενο δύο τέτοιων στοιχείων $g_1 = {b'}_1{a'}_1,\ g_2 = {b'}_2{a'}_2$ γράφεται $g_1 g_2 = {b'}_1{a'}_1{b'}_2{a'}_2 = {b'}_1{a'}_1{b'}_2{a'}_1{}^{-1}{a'}_1{a'}_2 = ({b'}_1({a'}_1{b'}_2{a'}_1{}^{-1}))({a'}_1{a'}_2)$
(4) Στην προηγούμενη ισότητα θεωρώντας ότι $a' = (e_B,\, a),\ b' = (b,\, e_A)$ και παρατηρώντας τις πράξεις στην προηγούμενη απόδειξη βλέπουμε ότι το γινόμενο των ${a'}_1{a'}_2$ είναι το $(a_1a_2)'$, ενώ μέσα στην πρώτη παρένθεση είναι το $(b_1(F(a_1)(b_2)))'$.
(5) Η τελευταία παρατήρηση φανερώνει ότι στην ομάδα G που δημιουργήται σαν ημιευθύ γινόμενο των A, B, η πράξη προσδιορίζεται από τις πράξεις αντίστοιχα στα A' και B' (ισόμορφα των A, B) καθώς και από την δράση της A' μέσω συζυγίας στην B' που είναι κανονική υποομάδα της G. Έτσι ακριβώς αναγνωρίζονται οι ομάδες που διασπώνται σε ευθύ γινόμενο.

Πρόταση 6.4.2 *Οι επόμενες προτάσεις είναι ισοδύναμες:*
α) Η ομάδα G είναι ισόμορφη προς το ημιευθύ γινόμενο δύο υποομάδων της A, B.
β) Οι υποομάδες A, B της G ικανοποιούν τις συνθήκες:
(β1) Κάθε $g \in G$ γράφεται μονοσήμαντα $g = ba$ με $b \in B$ και $a \in A$.
(β2) Η υποομάδα B είναι κανονική.

Το ότι το (α) συνεπάγεται το (β), το είδαμε προηγουμένως. Το αντίστροφο είναι εύκολο, αρκεί να χρησιμοποιήσουμε την συζυγία, η οποία εξ' υποθέσεως αφήνει αναλλοίωτο

το Β, άρα ορίζει μιά δράση του A στο B. Πράγματι ορίζουμε την δράση $F : A \to Aut(B)$, $F(a)b = aba^{-1}$. Γιά δύο στοιχεία $g = ba$, $g' = b'a'$, έχουμε $gg' = bab'a' = bab'a^{-1}aa' = b((F(a)b'))aa'$. Βλέπουμε αμέσως ότι η απεικόνιση $T : G \to B \times_F A$ με $T(g) = (b, a)$ είναι ισομορφισμός.

Πρόταση 6.4.3 *Η ομάδα $Iso(\mathbb{R}^3)$ είναι ημιευθύ γινόμενο των $A = O(3)$ και $B = \mathbb{R}^3$, όπου η τελευταία ταυτίζεται με την ομάδα των μεταφορών.*

Κατά την 6.2.3 κάθε ισομετρία γράφεται $F(x) = Ax + v$, ως σύνθεση μιάς ορθογώνιας ισομετρίας και μιάς μεταφοράς: $F = V \circ A$. Εδώ, με το ίδιο γράμμα A συμβολίζω την ισομετρία $x \mapsto Ax$ και με V συμβολίζω την μεταφορά $x \mapsto x + v$. Η ανάλυση αυτή είναι μονοσήμαντη. Πράγματι, αν $F = V \circ A = V' \circ A'$, είχε μιά δεύτερη ανάλυση, τότε $V \circ A = V' \circ A' \Rightarrow V'^{-1} \circ V = A' \circ A^{-1}$. Τότε $V'^{-1} \circ V(0) = A' \circ A^{-1}(0) = 0$. Άρα η μεταφορά $V'^{-1} \circ V$, θα άφηνε σταθερό το 0. Τούτο είναι δυνατόν μόνο γιά την ταυτοτική, άρα $V'^{-1} \circ V = e$, από την οποία παίρνουμε και $A' \circ A^{-1} = e$. Επίσης η υποομάδα B των μεταφορών είναι κανονική. Πράγματι, $(A \circ V \circ A^{-1})(x) = (A \circ V)(A^{-1}x) = A(A^{-1}x + v) = x + A(v)$. Που σημαίνει ότι $A \circ V \circ A^{-1} = V'$, όπου V' συμβολίζει την μεταφορά $x \mapsto x + A(v)$. Εφαρμόζοντας την προηγούμενη πρόταση παίρνουμε την απόδειξη της πρότασης.

ΠΡΟΒΛΗΜΑΤΑ 6.4

Πρόβλημα 6.4.1 *Δείξε ότι η ομάδα S_3 είναι ημιευθύ γινόμενο των $\mathbb{Z}_3$ και $\mathbb{Z}_2$.*

6.5 Ημιευθύ γινόμενο και αυτομορφισμοί

Από τον ορισμό του, το ημιευθύ γινόμενο περιλαμβάνει τρία στοιχεία: (A, B, F), τις δύο ομάδες A, B, καθώς και τον ομομορφισμό της A στην ομάδα $Aut(B)$ μέσω της δράσης F. Μέσω της δράσης ορίζεται μιά υποομάδα $F(A) \subseteq Aut(B)$. Προκύπτει λοιπόν το πρόβλημα: Πότε δύο δράσεις F, F', δίνουν ισόμορφες ομάδες $B \times_F A \approx B \times_{F'} A$; Οι επόμενες προτάσεις απαντούν σε ορισμένες απλές περιπτώσεις.

Πρόταση 6.5.1 *Έστωσαν δύο δράσεις $F : A \to Aut(B)$, $F' : A \to Aut(B)$, συζυγείς στην $Aut(B)$, δηλαδή δράσεις γιά τις οποίες υπάρχει $\beta \in Aut(B)$, με $F'(a) = \beta \circ F(a) \circ \beta^{-1}$, γιά κάθε $a \in A$. Τότε οι αντίστοιχες ομάδες $B \times_F A$, $B \times_{F'} A$, είναι ισόμορφες.*

Πράγματι, ορίζεται αμέσως η απεικόνιση $f_\beta : B \times_F A \longrightarrow B \times'_F A$, με $f_\beta(b, a) = (\beta(b), a)$, που λόγω των ιδιοτήτων της β, είναι 1-1 και επί. Αρκεί λοιπόν να δείξουμε ότι είναι ομομορφισμός. Προς τούτο υπολογίζουμε τα (α): $f_\beta(b, a) *_2 f_\beta(b', a')$ και (β): $f_\beta((b, a) *_1 (b', a'))$ και δείχνουμε ότι είναι ίσα. (α): $f_\beta(b, a) *_2 f_\beta(b', a') = (\beta(b), a) *_2 (\beta(b'), a') = (\beta(b)a(\beta(b')), aa') = (\beta(b)(F'(a) \circ \beta)(b'), aa') = (\beta(b)(\beta \circ F(a))(b'), aa') = \beta(bF(a)(b')), aa')$, η τελευταία διότι η β είναι ομομορφισμός. (β): $f_\beta((b, a) *_1 (b', a')) = f_\beta(ba(b'), aa') = \beta(bF(a)(b')), aa')$.

Πρόταση 6.5.2 *Έστωσαν δύο δράσεις $F : A \to Aut(B)$, $F' : A \to Aut(B)$, και έστω ότι υπάρχει $\alpha \in Aut(A)$, με $F' = F \circ \alpha$. Τότε οι αντίστοιχες ομάδες $B \times_F A$, $B \times_{F'} A$, είναι ισόμορφες.*

Πάλι διαπιστώνουμε αμέσως ότι η απεικόνιση $f_\alpha : B \times_F A \longrightarrow B \times'_F A$, με $f_\alpha(b, a) = (b, \alpha(a))$, είναι ισομορφισμός.

Πρόταση 6.5.3 *Έστωσαν δύο δράσεις* $F : A \to Aut(B)$, $F' : A \to Aut(B)$, *και έστω ότι η ομάδα* A *είναι κυκλική και οι* $F(A)$, $F'(A)$ *είναι συζυγείς υποομάδες της* $Aut(B)$. *Τότε οι αντίστοιχες ομάδες* $B \times_F A$, $B \times_{F'} A$, *είναι ισόμορφες.*

Πράγματι, από την συζυγία των υποομάδων $A_1 = F(A)$, $A_2 = F'(A)$ συμπεραίνομε ότι υπάρχει $\beta \in Aut(B)$, έτσι ώστε $A_2 = \beta A_1 \beta^{-1}$. Αν $a \in A$, είναι γεννήτορας της A, τούτη συνεπάγεται ότι υπάρχει ακέραιος k, έτσι ώστε $F'(a^k) = \beta \circ F(a) \circ \beta^{-1}$. Τότε η απεικόνιση $\Phi(b, a) = (\beta(b), a^k)$, ορίζει τον απαιτούμενο ισομορφισμό. Και πάλι προφανώς η Φ είναι 1-1 και επί και αρκεί να δείξουμε ότι είναι ομομορφισμός. Τούτο όμως επαληθεύεται αμέσως και επαφίεται στον αναγνώστη.

6.6 Ομάδες τάξης pq

Πρίν προχωρήσουμε στην ανάλυση των ομάδων των οποίων η τάξη είναι της μορφής $|G| = pq$, με $p > q$ πρώτους, εξετάζουμε μιάν ειδική περίπτωση μη-αβελιανής ομάδας με τέτοια τάξη.

Πρόταση 6.6.1 *Έστω ότι οι πρώτοι αριθμοί* $p > q$, *ικανοποιούν* $p = 1 \bmod q$ *και έστω ότι* a *είναι ακέραιος με* $a^q = 1 \bmod p$, $a \neq 1 \bmod p$. *Τότε η ομάδα* G, *που παράγεται από δύο στοιχεία της:* s, $t \in G$, *που ικανοποιούν τις σχέσεις:*

$$s^p = e,\ t^q = e,\ tst^{-1} = s^a,$$

είναι ημιευθύ γινόμενο των υποομάδων της $< s >$ *και* $< t >$ *και έχει* pq *στοιχεία.*

Από τις σχέσεις της υπόθεσης συμπεραίνομε ότι η κυκλική ομάδα $< s > \subset G$ τάξης p, είναι κανονική. Ορίζουμε λοιπόν μιά δράση $F :< t > \to Aut(< s >)$, αντιστοιχώντας $F(t) = (s \mapsto s^a)$. Επειδή η t είναι γεννήτορας της $< t >$, αυτό αρκεί για να ορίσει πλήρως τον ομομορφισμό F. Πράγματι, γιά ένα οποιοδήποτε άλλο στοιχείο t' της $< t >$, θα έχουμε $t' = t^k$ και συνεπώς θα πρέπει $F(t') = F(t^k) = F(t)^k$, που λόγω της μορφής του $F(t)$ θα είναι $F(t') = (s \mapsto s^{a^k})$. Από την υπόθεση προκύπτει ότι: $F(t^q) = (s \mapsto s^{a^q} = s)$, είναι η ταυτοτική. Αποδεικνύουμε ότι η G είναι ισόμορφη με την $G' =< s > \times_F < t >$. Ορίζουμε την $H : G' \to G$, μέσω της $H(s_1, t_1) = s_1 t_1 \in G$, $\forall s_1 \in < s >$, $t_1 \in < t >$. Ισχύει $H((s_1, t_1) * (s_2, t_2)) = H(s_1 t_1(s_2), t_1 t_2) = H(s_1(F(t_1)(s_2)), t_1 t_2)$, σύμφωνα με τον ορισμό της πράξης στο ημιευθύ άθροισμα. Αν $t_1 = t^k$ τότε, πάλι σύμφωνα με τον ορισμό: $H(s_1(F(t_1)(s_2)), t_1 t_2) = H(s_1(s_2)^{a^k}, t_1 t_2) = s_1 s_2^{a^k} t_1 t_2$. Από την άλλη μεριά $H(s_1, t_1)H(s_2, t_2) = s_1 t_1 s_2 t_2 = s_1(t_1 s_2 {t_1}^{-1}) t_1 t_2 = s_1(t^k s_2 t^{-k}) t_1 t_2 = s_1 {s_2}^{a^k} t_1 t_2$, σύμφωνα με την τελευταία σχέση που ισχύει στην ομάδα G εξ' υποθέσεως. Η H λοιπόν είναι ομομορφισμός. Εύκολα βλέπουμε ότι είναι 1-1, διότι $s_1 t_1 = e$, συνεπάγεται προφανώς $s_1 = t_1 = e$. Επίσης είναι και επί, αφού, βάσει των σχέσεων της G, κάθε στοιχείο της θα γράφεται στην μορφή $g = s^m t^n$, άρα $g = H(s^m, t^n)$. Η H συνεπώς δίνει τον ομομορφισμό που ζητάμε.

Παρατηρήσεις

(1) Σημειώνω ότι, στην προηγούμενη απόδειξη, την ύπαρξη της H την εξασφαλίζει θεωρητικά η γενική πρόταση 6.4.2. Αρκεί να δείξουμε ότι στην παρούσα περίπτωση πληρούνται οι προϋποθέσεις εφαρμογής αυτής της γενικής πρότασης, πράγμα εύκολο. Προτίμησα ωστόσο την λεπτομερή αυτή ανάλυση για να δούμε άλλη μιά φορά την δομή του ημιευθέως γινομένου.

(2) Στην προηγούμενη πρόταση η ομάδα G φαίνεται να εξαρτάται από την επιλογή του ακεραίου a που ικανοποιεί τις συνθήκες που αναφέρονται εκεί. Η εξάρτηση υλοποιήται μέσω

της δράσης $F :< t >\to Aut(< s >)$ που ορίζει το ημιευθύ γινόμενο. Η δράση αυτή εξαρτάται από το a, που είναι στοιχείο τάξης q της πολλαπλασιαστικής ομάδος $\mathbb{Z}_p^* = Aut(< s >)$ (δες πρόβλημα 2.8.16). Η ομάδα αυτή είναι κυκλική τάξεως $p-1$ (διότι ο p πρώτος). Εξ' υποθέσεως δε το q ικανοποιεί $p = 1 \bmod q$, άρα διαιρεί το $p-1$. Συνεπώς τα στοιχεία τάξης q αυτής της ομάδος, αποτελούν την μία και μοναδική κυκλική υποομάδα $C_{p,q}$ τάξης q της $Aut(< s >)$. Τούτο σημαίνει ότι και γιά κάθε άλλο a' που πληροί τις συνθήκες της πρότασης, η αντίστοιχη υποομάδα $F'(< t >) \subset Aut(< s >)$ ισούται με την $F(< t >)$, άρα εφαρμόζεται η πρόταση 6.5.3 και τα αντίστοιχα ημιευθέα γινόμενα είναι ισόμορφα.
(3) Η επόμενη πρόταση δείχνει ότι, εκτός από τις προηγούμενες ομάδες και τις κυκλικές τάξης pq, ουσιαστικά δεν υπάρχουν άλλες ομάδες μ' αυτήν την τάξη.

Πρόταση 6.6.2 *Δοθέντων δύο πρώτων αριθμών $p > q$ υπάρχουν μία ή δύο μόνον μη-ισόμορφες ομάδες τάξης pq, ανάλογα με τις δύο δυνατότητες γιά τα p, q:*
(1) Αν το $p \neq 1 \bmod q$, τότε κάθε ομάδα τάξης pq είναι ισόμορφη προς την $\mathbb{Z}_{pq}$.
(2) Αν το $p = 1 \bmod q$, τότε κάθε ομάδα τάξης pq είναι ισόμορφη είτε προς την κυκλική $\mathbb{Z}_{pq}$, είτε προς μίαν ομάδα G που παράγεται από δύο στοιχεία s, $t \in G$, που ικανοποιούν τις σχέσεις:

$$s^p = e,\ t^q = e,\ tst^{-1} = s^a,$$

όπου a είναι ακέραια λύση των $a^q = 1 \bmod p$, $a \neq 1 \bmod p$.

Κατά το θεώρημα του Cauchy (5.2.3), υπάρχουν στοιχεία s, $t \in G$, αντιστοίχων τάξεων p, q. Η υποομάδα $S =< s >$, με δείκτη $[G : S] = q$ τον ελάχιστο διαιρέτη της τάξης, θα είναι, κατα την 2.5.3, κανονική. Συνεπώς περιέχει το $tst^{-1} = s^a \in S$. Τότε θα έχουμε $s = t^q s t^{-q} = s^{a^q}$. Συνεπώς $a^q = 1 \bmod p$. Διακρίνουμε δύο περιπτώσεις:
(1) $a = 1 \bmod p$, οπότε $tst^{-1} = s^a = s \Rightarrow ts = st$. Σ' αυτήν την περίπτωση το st έχει τάξη pq και παράγει την G, η οποία συνεπώς είναι ισόμορφη με την $\mathbb{Z}_{pq}$.
(2) Αν $a \neq 1 \bmod p$, τότε το a, θεωρούμενο ως στοιχείο της πολλαπλασιαστικής ομάδος $\mathbb{Z}_p^*$ είναι τάξης q και συνεπώς το q διαιρεί την τάξη $p-1$ αυτής της ομάδος. Άρα $p = 1 \bmod q$. Επειδή η $|G| = pq$, η ομάδα παράγεται από τα s, t, και ικανοποιούνται όλες οι σχέσεις της περίπτωσης (2) της πρότασης.

6.7 Ομάδες τάξης p^3

Υποθέτουμε ότι p είναι πρώτος αριθμός και εξετάζουμε τις ομάδες με $|G| = p^3$. Διακρίνουμε τρεις περιπτώσεις: (α) Η ομάδα είναι αβελιανή, (β) Μη-αβελιανή τάξης 8 ($p = 2$) και τέλος (γ) Μη-αβελιανή τάξης p^3, $p > 2$.

Πρόταση 6.7.1 *Κάθε αβελιανή ομάδα τάξης p^3 είναι ισόμορφη προς μιάν εκ των:*

$$\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p, \quad \mathbb{Z}_{p^2} \times \mathbb{Z}_p, \quad \mathbb{Z}_{p^3}.$$

Αν η ομάδα G έχει στοιχείο τάξης p^3, τότε προφανώς θα είναι ισόμορφη με την $\mathbb{Z}_{p^3}$. Αν όλα τα στοιχεία της έχουν τάξη p, τότε κατά την πρόταση 5.6.1, θα είναι ισόμορφη προς το γινόμενο $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$. Η περίπτωση που απομένει είναι να υπάρχει κάποιο στοιχείο $s \in G$, τάξης p^2. Έστω τότε $t \in G$, $t \notin < s >$. Έστω $S =< s >$, $q = p^2$. Επειδή κάθε στοιχείο της G έχει τάξη, που διαιρεί το p^3, θα πρέπει $t^q = e$. Επειδή το G/S έχει τάξη p, θα πρέπει $t^p \in S$, άρα $t^p = s^i$. Τότε $s^{ip} = t^q = e$, άρα το i είναι πολλαπλάσιο του p, έστω $i = jp$. Τότε το $u = s^{-j}t$, $u^p = s^{-jp}t^p = e$, $u \notin S$. Το u είναι λοιπόν τάξης p

και εκτός του S. Η υποομάδα $T =< u >$ ικανοποιεί $T \cap S = \{e\}$, $TS = G$, άρα (5.3.1) η G είναι το ευθύ γινόμενο των S και T, τα οποία είναι αντίστοιχα ισόμορφα προς τα $\mathbb{Z}_{p^2}$ και $\mathbb{Z}_p$.

Παρατήρηση
Σημειώνω ότι, η προηγούμενη πρόταση είναι, στην ουσία, ειδική περίπτωση ($|G| = p^3$), των γενικωτέρων θεωρημάτων γιά πεπερασμένες αβελιανές ομάδες. Δες ειδικά τις παρατηρήσεις που ακολουθούν την πρόταση 5.6.4.

Πρόταση 6.7.2 *Κάθε μη-αβελιανή ομάδα με 8 στοιχεία είναι ισόμορφη προς μία από τις επόμενες δύο ομάδες που παράγονται από δύο στοιχεία s, $t \in G$:*

$$D_4 =< s,\ t : s^4 = e,\ t^2 = e,\ tst^{-1} = s^{-1} > \tag{6.8}$$

$$Q_8 =< s,\ t : s^4 = e,\ t^2 = s^2,\ tst^{-1} = s^{-1} > \tag{6.9}$$

Η πρώτη είναι η διεδρική ομάδα των ισομετριών του τετραγώνου και η δεύτερη είναι η λεγόμενη **ομάδα των βασικών τετρανίων**.

Έστω G τάξης 8. Προφανώς η G δεν μπορεί να έχει στοιχείο τάξης 8 και επίσης δεν είναι δυνατόν όλα τα στοιχεία της να έχουν τάξη 1 ή 2. Σ' όλες αυτές τις περιπτώσεις η G θα ήταν αβελιανή. Υπάρχει λοιπόν στοιχειο s τάξης 4. Η υποομάδα $S =< s >$, ως έχουσα δείκτη 2 θα είναι κανονική. Έστω $t \in G$ μη περιεχόμενο στο S. Το στοιχείο tst^{-1} έχει τάξη 4, άρα ισούται με το s ή το s^3. Αν ήταν $tst^{-1} = s$, τότε η G θα ήταν αβελιανή. Άρα $tst^{-1} = s^3 = s^{-1}$. Σημείωσε ότι τα δύο σύμπλοκα S και tS είναι όλο το G, άρα τα s, t παράγουν το G. Εξετάζουμε τώρα την τάξη του t.
α) Αν υπάρχει $t \notin S$ τάξης 2, τότε το G παράγεται από τα s, t και ισχύουν οι σχέσεις της 6.8. Άρα η ομάδα είναι ισόμορφη προς την διεδρική D_4.
β) Αν κάθε $t \notin S$ έχει τάξη 4, τότε, επειδή το G/S είναι τάξης 2, το $t^2 \in S$. Ως έχον τάξη 2 θα πρέπει λοιπόν $t^2 = s^2$ και ικανοποιούνται οι σχέσεις της 6.9. Η ομάδα συνεπώς είναι ισόμορφη προς την αντίστοιχη Q_8.

Παρατηρήσεις
(1) Σημειώνω ότι οι δύο ομάδες είναι ημιευθέα γινόμενα των υποομάδων τους S, T, που παράγονται αντίστοιχα από τα s, t. Αυτό προκύπτει αμέσως εφαρμόζοντας την πρόταση 6.4.2.
(2) Το ότι δύο ομάδες που ικανοποιούν το ίδιο σύστημα σχέσεων, λ.χ. το 6.8 είναι ισόμορφες, προκύπτει άμεσα ορίζοντας τον ισομορφισμό μέσω αντιστοίχισης των γεννητόρων.
(3) Το ότι οι δύο ομάδες που ορίζονται από τις 6.8 και 6.9 είναι μη-ισόμορφες αποδεικνύεται π.χ. από το γεγονός ότι η πρώτη δεν έχει στοιχείο τάξης 4 εκτός της S ενώ η δεύτερη έχει.
(4) Σημειώνω ότι η D_4 είναι ισόμορφη προς την ομάδα πινάκων που αναφέρεται στο πρόβλημα 1.3.10(γ). (Δες πρόβλημα 4.4.6.)

Πρόταση 6.7.3 *Γιά κάθε πρώτο $p > 2$, ορίζονται οι δύο μη αβελιανές ομάδες που παράγονται από δύο και τρία στοιχεία τους αντίστοιχα και έχουν p^3 στοιχεία:*

$$< s,\ t :\ s^{p^2} = e,\ t^p = e,\ tst^{-1} = s^{1+p} > \tag{6.10}$$

$$< s,\ t,\ u :\ s^p = e,\ t^p = e,\ u^p = e,\ tst^{-1} = s,\ usu^{-1} = s,\ utu^{-1} = st > \tag{6.11}$$

Και οι δύο είναι ημιευθέα γινόμενα υποομάδων τους και έχουν p^3 στοιχεία.

Πράγματι, στην πρώτη περίπτωση, οι σχέσεις δείχνουν ότι η υποομάδα $S =< s >$ είναι κανονική τάξης p^2 και κάθε στοιχείο της ομάδας γράφεται μονοσήμαντα ως γινόμενο $g = s^m t^n$. Γιά το τελευταίο, αρκεί να θεωρήσουμε τα σύμπλοκα της G ως προς την S.
Ανάλογα και στην δεύτερη περίπτωση, η ομάδα S που παράγεται από τα s, t είναι κανονική αβελιανή τάξης p^2 και κάθε στοιχείο της ομάδος γράφεται μονοσήμαντα σαν γινόμενο στοιχείων της S και της $U =< u >$. Εφαρμόζεται λοιπόν και πάλι η γενική πρόταση 6.4.2.

Παρατηρήσεις
Έστω G η δεύτερη ομάδα που ορίζεται από την 6.11.
(1) Η υποομάδα $S =< s, t > \subset G$ και η $U =< u >$ έχουν στοιχεία τάξης p.
(2) Αποδεικνύεται εύκολα ότι γιά το τυχόν στοιχείο $s' = s^k t^r \in S$ ισχύει $us' = s^k s' u$. Επαγωγικά, επίσης αποδεικνύεται ότι $(us')^p = s^{k(1+2+...+p)} s'^p u^p$.
(3) Οι προηγούμενες σχέσεις συνεπάγονται ότι κάθε στοιχείο της G έχει τάξη p, άρα η ομάδα δεν είναι ισόμορφη προς την 6.10, η οποία έχει στοιχεία τάξης p^2.

Πρόταση 6.7.4 *Κάθε μη-αβελιανή ομάδα με $|G| = p^3$ στοιχεία, όπου p πρώτος, $p > 2$, είναι ισόμορφη προς μίαν εκ των 6.10, 6.11.*

Πράγματι, κατά την πρόταση 2.8.3, το κέντρο Z της G θα είναι μη-τετριμμένη υποομάδα της G, άρα τάξεως p ή p^2. Επειδή όμως η G/Z δεν είναι κυκλική (διαφορετικά, κατά την 5.2.1, η G θα ήταν αβελιανή), η τάξη του Z πρέπει να είναι p και συνεπώς κάθε στοιχείο $\overline{x} \in G/Z$ ικανοποιεί $\overline{x}^p = \overline{e}$, δηλαδή $x^p \in Z$, $\forall x \in G$. Διακρίνουμε πάλι δύο περιπτώσεις, που αντιστοιχούν στις δύο αναφερθήσες ομάδες: (α) η ομάδα περιέχει στοιχείο τάξης p^2 και (β) κάθε στοιχείο της ομάδος είναι τάξης p.
(α) Έστω $s \in G$ τάξης p^2 και $S =< s > \subset G$. Κατά την 2.5.3, η S θα είναι κανονική. Έστω t στοιχείο της ομάδος $t \notin S$. Τότε $tst^{-1} = s^a$ λόγω κανονικότητας της S. Τότε επίσης $t^p s t^{-p} = s^{a^p}$ και επειδή το $t^p \in Z \Rightarrow s = s^{a^p} \Rightarrow a^p = 1 \bmod p^2$. Απ' αυτήν προκύπτει αμέσως (π.χ. θέτοντας $a = k + rp$ και κάνοντας τις πράξεις) ότι $a = 1 \bmod p$ και $a^p = 1 \bmod p$. Επειδή $tst^{-1} \neq s$, (διαφορετικά η $G =< s, t >$ θα ήταν αβελιανή), έπεται ότι $a \neq 1 \bmod p^2$. Τότε θα πρέπει $a = 1 + jp$, με $j \neq 0 \bmod p$. Τούτο συνεπάγεται ότι υπάρχει $k : jk = 1 \bmod p$. Τότε θα ισχύει $a^k = (1+jp)^k = 1 + kjp + p^2(...) = 1 + (1+mp)p + p^2(...) = (1+p) \bmod p^2$. Κατά συνέπειαν, $t^k s t^{-k} = s^{a^k} = s^{1+p}$. Αντικαθιστώντας λοιπόν το t με το t^k αποδεικνύουμε την σχέση $tst^{-1} = s^{1+p}$ $(*)$.
Γιά να δείξουμε την δεύτερη σχέση, $t^p = e$, ξεκινάμε από το στοιχείο $s^p \in S$, το οποίο περιέχεται στο κέντρο και το παράγει $Z =< s^p >$. Τούτο διότι, όπως δείξαμε στην αρχή, κάθε $t^p \in Z$ και το κέντρο είναι τάξης p. Επειδή και $t^p \in Z$, έπεται ότι $t^p = s^{ip}$, γιά κάποιον ακέραιο $i < p$ και συνεπώς:

$$(ts^{-i})^2 = ts^{-i}ts^{-i} = (ts^{-i}t^{-1})(t^2 s^{-i} t^{-2})t^2 = s^{-i(a+a^2)} t^2.$$

Η τελευταία διότι $ts^{-i}t^{-1} = s^a$ ισχύει, με a αντίστοιχο προς το αρχικό (πρίν την αντικατάσταση του αρχικού t). Επαγωγικά αποδεικνύουμε εύκολα ότι:

$$(ts^{-i})^k = s^{-i(a+a^2+...+a^k)} t^k.$$

Τούτη γιά $k = p$ δίνει $(ts^{-i})^p = s^{-i(a+a^2+...+a^p)} t^p = s^{-ip} t^p = e$. Η τελευταία, βάσει της $a^p = 1 \bmod p^2$ (και της συνέπειάς της $a = 1 \bmod p$). Έτσι, αντικαθιστώντας το t με το ts^{-i}, πετυχαίνουμε, εκτός της $(*)$, το t να ικανοποιεί και την $t^p = e$. Αυτό ολοκληρώνει την πρώτη περίπτωση (α) και δείχνει ότι η G είναι ισόμορφη προς την 6.10.

(β) Υποθέτουμε τώρα ότι κάθε στοιχείο της ομάδος είναι τάξης p. Έστω t στοιχείο της ομάδος $t \notin Z$ και u στοιχείο εκτός της ομάδος $W =< Z, t >$. Η W είναι τάξης p^2, αφου το t μετατίθεται με το Z και είναι τάξης p. Η G/Z είναι επίσης τάξης p^2, άρα κατά την πρόταση 5.2.2, είναι αβελιανή. Συνεπώς, το στοιχείο $s = utu^{-1}t^{-1} \in Z$. Επειδή η $G =< Z, t, u >$ δεν είναι αβελιανή, το t δεν μετατίθεται με το u. Συνεπώς, $s \neq e$ και $Z =< s > \Rightarrow G =< s, t, u >$. Επειδή ισχύουν όλες οι σχέσεις:

$$s^p = t^p = u^p = e, \quad tst^{-1} = t, \quad usu^{-1} = s, \quad utu^{-1} = st,$$

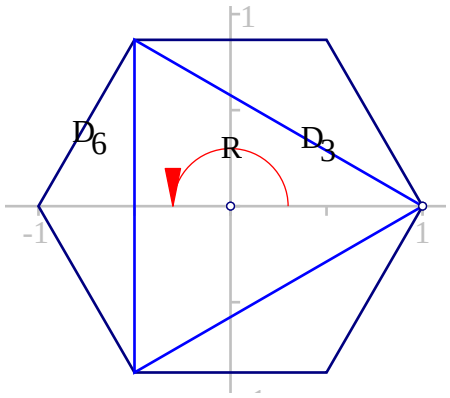
η ομάδα είναι ισόμορφη με την 6.11.

ΠΡΟΒΛΗΜΑΤΑ 6.7

Πρόβλημα 6.7.1 *Δείξε ότι η ομάδα Q_8 είναι ισόμορφη με την ομάδα πινάκων:*

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

(Υπόδειξη: $s = \begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}, t = \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$*.)*



Σχήμα 6.1: $D_6 \approx D_3 \times \mathbb{Z}_2$

Πρόβλημα 6.7.2 *Δείξε ότι η διεδρική ομάδα D_{2n} είναι ευθύ γινόμενο των υποομάδων της D_n και $< R >$, όπου R η στροφή κατά γωνία π ή συμμετρία ως προς κέντρο. (Υπόδειξη: $D_{2n} =< s, t : s^{2n} = t^2 = e, (st)^2 = e >$, περιέχει τις υποομάδες $A =< s^2, t >$ και $B =< s^n >$. Δείξε ότι τούτες ικανοποιούν τις προϋποθέσεις της πρότασης 5.3.1, καθώς και ότι η A είναι ισόμορφη της D_n.)*

Πρόβλημα 6.7.3 *Δείξε ότι η διεδρική ομάδα D_{2n} είναι ημιευθύ γινόμενο των υποομάδων της D_n και $< R >$, όπου R μιά ανάκλαση που δεν περιέχεται στην D_n. Γιατί αυτό δεν αποτελεί αντίφαση στο προηγούμενο πρόβλημα ;*

Κεφάλαιο 7

Θεωρήματα του Sylow

Τα τρία θεωρήματα του Sylow (1832-1918) είναι σημαντικά για την μελέτη των πεπερασμένων ομάδων. Αποφαίνονται γιά την ύπαρξη και δομή υποομάδων, ανάλογα με το μέγεθος της τάξης της ομάδος και συχνά αποτελούν το σημείο εκκίνησης γιά την διάσπαση ομάδος σε απλούστερες ή γενικώτερα την διερεύνηση της δομής της.

7.1 Πρώτο θεώρημα του Sylow

Πρόταση 7.1.1 *Εάν p είναι πρώτος αριθμός και η δύναμις p^k διαιρεί την τάξη $n = |G|$ της ομάδος G, τότε υπάρχει υποομάδα τάξης p^k της G.*

Η απόδειξη μοιάζει με την απόδειξη της θεωρήματος Cauchy (5.2.3) και γίνεται με επαγωγή ως προς την τάξη n της ομάδος. Προφανώς ισχύει γιά $n = 1$, αφού τότε δεν υπάρχουν πρώτοι διαιρέτες του n. Υποθέτουμε τώρα ότι η πρόταση αληθεύει γιά κάθε τάξη ομάδος $m < n$ και δείχνουμε ότι ισχύει και γιά $m = n$. Γράφουμε την εξίσωση (δες 2.8.2) των κλάσεων

$$n = c + h + h' + h'' + ...,$$

της ομάδας G, όπου $c = |Z(G)|$ είναι η τάξη του κέντρου της G και τα $h, h', ...$ είναι οι δείκτες ορισμένων γνήσιων υποομάδων της G:

$$h = [G : N], h' = [G : N'], h'' = [G : N''] ...$$

Αν το p διαιρεί το c, τότε κατά το θεώρημα Cauchy, το κέντρο $Z(G)$ θα περιέχει υποομάδα A τάξης p. Επειδή η A περιέχεται στο κέντρο, θα είναι κανονική στην G. Τότε η τάξη n/p της G/A θα διαιρήται με το p^{k-1}. Κατά την επαγωγική υπόθεση, τότε η G/A θα περιέχει υποομάδα H/A, όπου H υποομάδα της G περιέχουσα την A, τάξης p^{k-1}. Τότε η υποομάδα H της G θα έχει τάξη p^k και η πρόταση θα ισχύει.
Έστω τώρα ότι το p δεν διαιρεί το c. Επειδή το p διαιρεί το n, θα πρέπει κάποιο από τα $h, h', ...$ να μην διαιρήται με το p. Διαφορετικά, αν όλα διαιρούνταν με το p και το $c = n - h - h' - ...$, θα διαιρήτο με το p. Έστω λοιπόν ότι το h δεν διαιρήται με το p. Επειδή $h = [G : N]$, το p θα πρέπει να διαιρεί την τάξη του N. Επειδή το N είναι γνήσια υποομάδα της G, έχει τάξη μικρότερη του n, άρα, κατά την επαγωγική υπόθεση περιέχει υποομάδα τάξης p^k. Και σ' αυτήν λοιπόν την περίπτωση, η πρόταση ισχύει.

Παρατηρήσεις
(1) Υποομάδες $H \subseteq G$ των οποίων η τάξη ισούται με την μέγιστη δύναμη πρώτου p^k που

διαιρεί την τάξη της ομάδος $n = |G|$, λέγονται **υποομάδες- Sylow** της G.
(2) Γενικώτερα υποομάδες $H \subseteq G$ των οποίων η τάξη ισούται με μιά δύναμη πρώτου p^r που διαιρεί την τάξη της ομάδος $n = |G|$, λέγονται **p-υποομάδες** της G.
(3) Το πρώτο θεώρημα του Sylow εξασφαλίζει τόσο την ύπαρξη υποομάδων- Sylow όσο και p-υποομάδων. Τα επόμενα δύο θεωρήματα του Sylow συσχετίζουν τις διάφορες υποομάδες- Sylow μεταξύ τους καθώς και την σχέση των υποομάδων- Sylow με τις p-υποομάδες.

7.2 Δεύτερο θεώρημα του Sylow

Κατ' αρχήν μιά χρήσιμη ιδιότητα των λεγομένων **p-στοιχείων** μιάς ομάδος. Έτσι ονομάζονται τα στοιχεία $x \in G$ της ομάδος, των οποίων η τάξη είναι δύναμις ενός πρώτου p^r, διαιρέτη της τάξης της ομάδος $n = |G|$.

Πρόταση 7.2.1 *Δοθήσης p-υποομάδος Sylow H της ομάδος G, τα μόνα p-στοιχεία $x \in G$ γιά τα οποία $xHx^{-1} = H$, είναι τα ίδια τα στοίχεία της H.*

Πράγματι, έστω $N = N_G(H)$ ο κανονικοποιητής της H στην G. Επειδή η $H \subseteq N$, είναι κανονική υποομάδα της N και, προφανώς, η H είναι p-υποομάδα Sylow της N, η ομάδα-πηλίκον N/H έχει τάξη q, αριθμό πρώτο προς το p, συνεπώς δεν περιέχει p-στοιχείο διαφορετικό της μονάδος e. Τούτο αποδεικνύει τον ισχυρισμό, αφού το x με τις ιδιότητες της πρότασης θα ήταν $x \in N$ και xH θα ήταν p-στοιχείο της N/H.

Πρόταση 7.2.2 *(Δεύτερο Θεώρημα του Sylow) Γιά κάθε πρώτο p που διαιρεί την τάξη $n = |G|$, της ομάδος, οι p-υποομάδες Sylow της G είναι συζυγείς μεταξύ τους. Γιά το πλήθος τους ν_p ισχύει $\nu_p = 1 \bmod p$.*

Γιά την απόδειξη θεωρούμε την δράση μιάς οποιασδήποτε p-υποομάδας Sylow H σε μιά κλάση συζυγίας Ω των p-υποομάδων Sylow. Υποθέτουμε ότι το $x \in H$ δρά μέσω συζυγίας στο Ω, απεικονίζοντας μιά ομάδα $K \in \Omega$ στην $xKx^{-1} \in \Omega$. Ο σταθεροποιητής H_K της δράσης στο $K \in \Omega$ θα είναι $H_K = \{x \in H : xKx^{-1} = K\}$ και επειδή όλα τα στοιχεία $x \in H$ είναι p-στοιχεία, κατά την προηγούμενη πρόταση, $H_K = H \cap K$. Άρα η τροχιά του K θα έχει πλήθος στοιχείων: $|H(K)| = [H : H \cap K]$. Εάν το $H = K$, τότε ο αριθμός αυτός είναι 1, εάν $H \neq K$, ο αριθμός αυτός είναι πολλαπλάσιο του p. Συνεπώς, επειδή το Ω είναι ένωση τέτοιων τροχιών, το πλήθος των στοιχείων του θα είναι $|\Omega| = 1 \bmod p$.
Αν υπήρχε $H \notin \Omega$, τότε θεωρώντας την δράση αυτής της ομάδας στο Ω, θα βρίσκαμε γιά το $|\Omega| = 0 \bmod p$. Πράγμα που αντιφάσκει στην προηγούμενη ισότητα. Συμπεραίνουμε ότι η Ω είναι η μοναδική κλάση συζυγίας και έχει $1 \bmod p$ στοιχεία. Αυτό αποδεικνύει και τους δύο ισχυρισμούς της πρότασης.

Παρατηρήσεις
(1) Η προηγούμενη πρόταση συνεπάγεται ότι το πλήθος των p-υποομάδων Sylow της ομάδας G ισούται με το πλήθος των στοιχείων της μοναδικής κλάσης συζυγίας της που είναι $[G : N_G(H)]$, όπου H μιά οποιαδήποτε p-υποομάδα Sylow .
(2) Μιά άλλη συνέπεια είναι ότι μιά p-υποομάδα Sylow είναι κανονική, όταν ακριβώς δεν υπάρχει άλλη p-υποομάδα Sylow.
(3) Επειδή μιά p-υποομάδα Sylow $H \subset G$ είναι κανονική υποομάδα του κανονικοποιητή της $H \subseteq N_G(H)$, και ταυτόχρονα είναι p-υποομάδα Sylow του $N_G(H)$, συνάγεται ότι η H είναι η μοναδική p-υποομάδα Sylow της $N_G(H)$.

(4) Έστω ότι η τάξη της ομάδος $|G| = n = p^r q$, όπου p πρώτος και p, q, αριθμοί πρώτοι μεταξύ τους. Από την $[G : H] = [G : N_G(H)][N_G(H) : H]$, έπεται ότι το πλήθος $\nu_p = [G : N_G(H)]$ των p-υποομάδων Sylow της G διαιρεί τον δείκτη $[G : H] = q$. Συνεπώς γιά το πλήθος ν_p των συζυγών p-υποομάδων Sylow έχουμε τις δύο συνθήκες:

$$\nu_p = 1 \bmod p, \qquad \nu_p | q.$$

(5) Η προηγούμενη πρόταση και η προηγούμενη παρατήρηση αποτελούν, σε ορισμένες περιπτώσεις, ισχυρούς περιορισμούς, που οδηγούν στην $\nu_p = 1$, που σημαίνει ότι η αντίστοιχη p-υποομάδα Sylow είναι κανονική. Συχνά τούτο είναι το πρώτο βήμα γιά την διάσπαση σε ημιευθύ ή ευθύ γινόμενο. Γιά παράδειγμα, αν $|G| = p^a q^b$, όπου p, q πρώτοι, και κανένα από τα $q, q^2, ..., q^b$, δεν είναι ίσο με $1 \bmod p$ ($\pi.\chi$ $175 = 7 \cdot 5^2$), τότε η G είναι ημιευθύ γινόμενο των αντιστοίχων p-και q-υποομάδων Sylow. Αναλυτικώτερα παραδείγματα αυτού του τύπου θα δούμε στις εφαρμογές, στο τέλος του κεφαλαίου.

7.3 Τρίτο θεώρημα του Sylow

Το θεώρημα αυτό βάζει τάξη στις p-υποομάδες της ομάδας G, δείχνοντας ότι κάθε τέτοια είναι υποομάδα μιάς p-υποομάδας Sylow.

Πρόταση 7.3.1 *Κάθε p-υποομάδα H μιάς ομάδος G είναι υποομάδα μιάς p-υποομάδος Sylow K της G.*

Θεωρούμε, όπως και προηγουμένως, την δράση (μέσω συζυγίας) της υποομάδος H στην κλάση συζυγίας Ω των p-υποομάδων Sylow. Ο σταθεροποιητής H_K της δράσης στο $K \in \Omega$ θα είναι $H_K = \{x \in H : xKx^{-1} = K\}$ και επειδή όλα τα στοιχεία $x \in H$ είναι p-στοιχεία, κατά την πρόταση 7.2.1, $H_K = H \cap K$. Άρα η τροχιά του K θα έχει πλήθος στοιχείων: $|H(K)| = [H : H \cap K]$. Εάν το $H = K$, τότε ο αριθμός αυτός είναι 1, εάν $H \neq K$, ο αριθμός αυτός είναι πολλαπλάσιο του p. Συνεπώς, επειδή το Ω έχει πλήθος στοιχείων $|\Omega| = 1 \bmod p$, θα υπάρχει τροχιά $H(K)$ κάποιας $K \in \Omega$, που το πλήθος στοιχείων της $|H(K)| = |H|/|H_K|$ δεν είναι πολλαπλάσιο του p, άρα ισούται με 1. Τότε $H \cap K = H$, άρα $H \subset K$.

7.4 Εφαρμογές

Πρόταση 7.4.1 *Κάθε ομάδα τάξης 45 είναι αβελιανή.*

Πράγματι κατά το πρώτο θεώρημα Sylow, η ομάδα θα έχει 3-υποομάδα Sylow H, τάξης 9. Τούτη, κατά την πρόταση 5.2.2, θα είναι αβελιανή το δε πλήθος των συζυγών αυτής της ομάδος θα είναι $\nu_3 = 1 \bmod 3 = 1, 4, ...$ Ταυτόχρονα το ν_3 θα πρέπει να διαιρεί το 5, άρα $\nu_3 = 1$ και η H είναι κανονική. Έστω τώρα 5-υποομάδα Sylow K, τάξης 5. Προφανώς αυτή θα είναι αβελιανή και $\nu_5 = 1 \bmod 5 = 1, 6, 11, ...$ πρέπει να διαιρεί το 9. Έπεται ότι $\nu_5 = 1$ και η K είναι κανονική. Ο ισχυρισμός έπεται από την πρόταση 5.3.3.

Είναι προφανές ότι παρόμοιο επιχείρημα μπορεί να εφαρμοστεί σε διάφορες περιπτώσεις που η τάξη $n = |G|$ της ομάδος γράφεται σαν γινόμενο δυνάμεων πρώτων $n = p^k q^m$ και οι πρώτοι είναι τέτοιοι ώστε να υποχρεώνουν τα $\nu_q = \nu_p = 1$. Τότε, όταν επί πλέον τα k, $m \leq 2$, η ομάδα, ως ευθύ γινόμενο δύο αβελιανών θα είναι αβελιανή. Γιά παράδειγμα:

Πρόταση 7.4.2 *Κάθε ομάδα τάξης $99 = 3^2 11$ είναι αβελιανή.*

Πράγματι, πάλι πρέπει $\nu_3 = 1 \bmod 3 = 1, 4, ...$ και το ν_3 να διαιρεί το 11 που συνεπάγεται $\nu_3 = 1$. $\nu_5 = 1 \bmod 5 = 1, 6, ...$ και το ν_5 να διαιρεί το 9 που συνεπάγεται $\nu_5 = 1$. Παρόμοια λ.χ. κάθε ομάδα τάξης $156 = 3^2 17$ ή $175 = 5^2 7$ είναι αβελιανή.

Πρόταση 7.4.3 *Υπάρχουν 5 μη-ισόμορφες ομάδες τάξης 12.*

Το υπόλοιπο της παραγράφου είναι αφιερωμένο στην απόδειξη αυτής της πρότασης. Κατ' αρχήν υπάρχουν δύο αβελιανές ομάδες μ' αυτήν την τάξη: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$ και $\mathbb{Z}_4 \times \mathbb{Z}_3$. Υποθέτουμε τώρα ότι η ομάδα G είναι μη-αβελιανή. Ξεκινάμε με το πρώτο θεώρημα Sylow, που εξασφαλίζει 3-υποομάδα Sylow B, τάξης 3 και 2-υποομάδα Sylow A τάξης $4{=}2^2$. Υπάρχουν δύο δυνατότητες γιά την B (α): Να μην είναι κανονική, οπότε δείχνουμε ότι η G πρέπει να είναι ισόμορφη με την εναλλακτική A_4, και (β): Η B να είναι κανονική και η A να μην είναι κανονική (διότι αν ήταν κι αυτή κανονική, τότε η G θα ήταν ευθύ γινόμενο αβελιανών).

(α): Αν η 3-υποομάδα Sylow B δεν είναι κανονική, τότε έχει $\nu_3 = 4$ συζυγείς υποομάδες. Επίσης η δράση της G στο σύνολο-πηλίκον G/B, $F(g)(hB) = (gh)B$ είναι 1-1 (δες πρόβλημα 6.3.7). Συνεπώς η υποομάδα $F(G) \subset S(G/B) \approx S_4$, είναι τάξης 12 και περιέχει 8 στοιχεία τάξης 3 (δύο από κάθε συζυγή υποομάδα της B). Όλα όμως τα στοιχεία τάξης 3 της S_4 περιέχονται στην εναλλακτική υποομάδα A_4 (δες παρατήρηση (4) μετά την πρόταση 3.4.2). Άρα η $F(G) \cap A_4$ είναι τάξης τουλάχιστον 8, και επειδή η τάξη της πρέπει να διαιρεί την τάξη της A_4 που είναι 12, έπεται ότι $F(G) = A_4$. Τούτο ολοκληρώνει την απόδειξη ότι $G \approx A_4$.

(β): Αν η B είναι κανονική τότε η ομάδα G θα είναι ήμιευθύ γινόμενο $G = B \times_F A$, όπου $F : A \longrightarrow Aut(B)$, μιά δράση. Το πρόβλημα λοιπόν σ' αυτήν την περίπτωση είναι να βρούμε όλες τις δυνατές δράσεις που δίνουν διαφορετικά ημιευθέα γινόμενα. Τούτο εξαρτάται από την μορφή της A. Η A θα είναι ισόμορφη είτε προς την $\mathbb{Z}_4$ είτε προς την $\mathbb{Z}_2 \times \mathbb{Z}_2$. Οδηγεί τούτο στις περιπτώσεις (β1) και (β2).
Κατ' αρχήν $Aut(B) \approx Aut(\mathbb{Z}_3) \approx \mathbb{Z}_2$ (δες πρόβλημα 2.8.16).

(β1): Αν $A \approx \mathbb{Z}_4$, τότε υπάρχει ένας μη τετριμμένος ομομορφισμός $F : A \longrightarrow Aut(B)$, αυτός που στον γεννήτορα a της A αντιστοιχεί τον αυτομορφισμό $b \mapsto b^2$ της B. Επομένως σ' αυτήν την περίπτωση έχουμε ένα μόνο ημιευθύ γινόμενο $B \times_F A \approx \mathbb{Z}_3 \times_F \mathbb{Z}_4$. Η ομάδα αυτή λέγεται **δικυκλική** και η δομή της περιγράφεται από τις σχέσεις:

$$Q_6 =< a, b : a^4 = e, b^3 = e, aba^{-1} = b^2 > .$$

(β2): Αν $A \approx \mathbb{Z}_2 \times \mathbb{Z}_2$, τότε υπάρχουν τρεις διαφορετικοί μη-τετριμμένοι ομομορφισμοί $F : A \longrightarrow Aut(B)$, που αντιστοιχούν στους τρεις διαφορετικούς ομομορφισμούς της ομάδος $\mathbb{Z}_2 \times \mathbb{Z}_2$ στην $\mathbb{Z}_2$ (δες πρόβλημα 2.6.3). Στην περίπτωση αυτή οι ομομορφισμοί ικανοποιούν τις προϋποθέσεις της πρότασης 6.5.2 και κατά συνέπειαν ορίζουν ισόμορφα ημιευθέα γινόμενα. Αν παραστήσουμε τις ομάδες A, B, μέσω των γεννητόρων τους $A =< s, t \ : s^2 = t^2 = e, \ st = ts >$, $B =< b : b^3 = e >$, τότε μία από τις δράσεις είναι η αντιστοιχούσα στο s τον μοναδικό μη-τετριμμένο ομομορφισμό $b \mapsto b^2$ και στο t τον ταυτοτικό. Ως προς αυτήν την δράση το ημιευθύ γινόμενο περιγράφεται με τις σχέσεις:

$$G =< s, \, t, \, b : \ s^2 = t^2 = b^3 = e, \ st = ts, \ sbs^{-1} = b^2, \ tbt^{-1} = b > .$$

Η ομάδα αυτή περιέχει τις υποομάδες $H =< s, b : \ s^2 = b^3 = e, \ sbs^{-1} = b^2 >$, και $T =< t : t^2 = e >$. Η σχέσεις $tb = bt$, $ts = st$, δείχνουν ότι οι δύο ομάδες μετατίθενται. Η τομή τους είναι το $\{e\}$ και συνεπώς η G είναι το ευθύ άθροισμα αυτών των δύο υποομάδων της. Η ομάδα H είναι όμως ισόμορφη με την $S_3 \approx D_3$ (δες πρόβλημα 3.7.8). Επίσης η T συμπίπτει με τον πυρήνα της δράσης F και είναι ισόμορφη της $\mathbb{Z}_2$. Άρα σ' αυτήν την περίπτωση η ομάδα G είναι ισόμορφη του ευθέως γινομένου : $D_3 \times \mathbb{Z}_2 \approx D_6$. Γιά τον τελευταίο ισομορφισμό δές το πρόβλημα 6.7.2.

7.5 Ομάδες μικρής τάξεως (≤ 15)

Επισκοπώντας τα πεπραγμένα ας συμπληρώσουμε την λίστα των μη-ισομορφικών μεταξύ τους ομάδων γιά τις ομάδες μικρής τάξεως (≤ 15). Ο πίνακας παρακάτω συνοψίζει τα συμπεράσματα και παραπέμπει στις παραγράφους που αποδεικνύονται τα αντίστοιχα αποτελέσματα.

Τάξη	**Ομάδα**	**Σχόλια**
1	$\{e\}$	Η τετριμμένη ομάδα
2	$\mathbb{Z}_2$	πρόταση 1.7.1
3	$\mathbb{Z}_3$	
4	$\mathbb{Z}_4$	ελάχιστη τάξη με δύο μη-ισόμορφες
4	$V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$	2.4.5 και 3.7.3
5	$\mathbb{Z}_5$	κυκλική, 2.6
6	$\mathbb{Z}_6 \approx \mathbb{Z}_2 \times \mathbb{Z}_3$	ευθύ γινόμενο κυκλικών 2.8.12
6	$D_3 \approx S_3$	μη-αβελιανή ελάχιστης τάξης 3.7.8 και 4.4.4
7	$\mathbb{Z}_7$	κυκλική
8	$\mathbb{Z}_8$	κυκλική
8	$\mathbb{Z}_4 \times \mathbb{Z}_2$	αβελιανή, γινόμενο κυκλικών
8	$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	διάσπαση αβελιανών: 5.6.4
8	D_4	Διεδρική, 6.7.2
8	Q_8	Μοναδιαία τετράνια
9	$\mathbb{Z}_9$	κυκλική
9	$\mathbb{Z}_3 \times \mathbb{Z}_3$	αβελιανή
10	$\mathbb{Z}_{10} \approx \mathbb{Z}_5 \times \mathbb{Z}_2$	κυκλική
10	D_5	διεδρική
11	$\mathbb{Z}_{11}$	κυκλική
12	$\mathbb{Z}_{12} \approx \mathbb{Z}_4 \times \mathbb{Z}_3$	κυκλική
12	$\mathbb{Z}_2 \times \mathbb{Z}_6 \approx \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$	αβελιανή
12	A_4	εναλλακτική 7.4.3
12	$D_6 \approx D_3 \times \mathbb{Z}_2$	διεδρική
12	Q_6	δικυκλική
13	$\mathbb{Z}_{13}$	κυκλική
14	$\mathbb{Z}_{14} \approx \mathbb{Z}_7 \times \mathbb{Z}_2$	κυκλική
14	D_7	διεδρική 5.2.4
15	$\mathbb{Z}_{15} \approx \mathbb{Z}_5 \times \mathbb{Z}_3$	κυκλική 6.6.2

Ο πίνακας θα μπορούσε να συνεχιστεί. Ωστόσο οι λογαριασμοί γίνονται γρήγορα υπερβολικά περίπλοκοι. Ήδη στην επόμενη τάξη $16 = 2^4$ έχουμε 14 μη-ισόμορφες ομάδες (γενικά, οι δυνάμεις του 2 παρουσιάζουν μεγάλη ποικιλία) και χρειάζεται επι πλέον ανάπτυξη της θεωρίας για να αντιμετωπιστούν με οργανωμένο τρόπο. Η ταξινόμηση των πεπερασμένων ομάδων τάξης ≤ 200 έγινε από τον Otto Hoelder (1859-1937). Το 2001, με την ευκαιρία της αλλαγής της χιλιετίας, οι Besche, Eick, O,Brien κ.α. (Electronic Res. Announc. AMS 7(2001)) δημοσίευσαν μιά λίστα με τις μη-ισόμορφες πεπερασμένες ομάδες γιά όλες τις τάξεις ≤ 2000. Το πλήθος τους ανέρχεται σε 49.910.529.484. Απ' αυτές οι 49.487.365.422 είναι ομάδες τάξεως $2^{10} = 1024$ και μόνον οι υπόλοιπες 423.164.062 είναι ομάδες άλλων τάξεων. Προφανώς οι αντίστοιχοι υπολογισμοί απαιτούν την χρήση υπολογιστή και ειδικών προγραμμάτων. Για το παραπάνω αποτέλεσμα χρησιμοποιήθηκαν διάφορα

προγράμματα, οπως λ.χ. το GAP, διατιθέμενο ελεύθερα στο διαδίκτυο στην διεύθυνση http://www.gap-system.org/ gap/Info4/distrib.html.