

Σημειώσεις στην Βασική Άλγεβρα

Κωνσταντίνος Μπιζάνος

13 Ιανουαρίου 2025

Περιεχόμενα

1	Πρώτο Θεώρημα Ισομορφισμών	2
2	Κινέζικο Θεώρημα Υπολοίπων	2
3	Ασκήσεις στους Δακτυλίους Πηλίκου	4
4	Η έννοια της ομάδας	6
5	Η Συμμετρική Ομάδα S_n	7
6	Τάξη Στοιχείου Ομάδας	10
7	Ασκήσεις	12
8	Υποομάδες	14
9	Θεώρημα Lagrange	15
10	Κυκλικές Ομάδες	16
11	Άρτιες και Περιττές Μεταθέσεις	18
12	Ασκήσεις	19
13	Ομομορφισμοί Ομάδων	20
14	Ταξινόμηση Κυκλικών Ομάδων	23
15	Δομή Κυκλικών Ομάδων	23
16	Ασκήσεις στις Ομάδες	25

1 Πρώτο Θεώρημα Ισομορφισμών

Παράδειγμα 1. Δείξτε ότι $\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}$.

Λύση. Σκοπός είναι να εφαρμόσουμε το πρώτο θεώρημα ισομορφισμών. Συνεπώς, αναζητούμε $\varphi: \mathbb{R}[x] \rightarrow \mathbb{C}$ ώστε $\ker \varphi = \langle x^2 + 1 \rangle$. Ορίζουμε $\varphi: \mathbb{R}[x] \rightarrow \mathbb{C}$ με $\varphi(f(x)) = f(i)$. Είναι άμεσο ότι φ είναι ομομορφισμός δακτυλίων. Για το επί, έστω $a + bi \in \mathbb{C}$. Τότε, παρατηρούμε ότι

$$\varphi(bx + a) = a + bi.$$

Αρχικά, $x^2 + 1 \in \ker \varphi$ ($i^2 = -1$). Τότε, αφού $\ker \varphi$ είναι ιδεώδες, ισχύει ότι $f(x)(x^2 + 1) \in \ker \varphi$, για κάθε $f(x) \in \mathbb{R}[x]$. Άρα $\langle x^2 + 1 \rangle \subseteq \ker \varphi$.

Αντίστροφα, έστω $f(x) \in \ker \varphi$. Τότε $f(i) = 0$, δηλαδή i ρίζα του $f(x)$. Αφού $f(x) \in \mathbb{R}[x]$ και i ρίζα του, τότε και $\bar{i} = -i$ είναι επίσης ρίζα του. Επομένως, $x - i, x + i \mid f(x)$ και αφού $x - i, x + i$ είναι σχετικά πρώτα, τότε $x^2 + 1 = (x - i)(x + i) \mid f(x)$. Άρα, $f(x) = q(x)(x^2 + 1) \in \langle x^2 + 1 \rangle$ και έχουμε το ζητούμενο. ■

2 Κινέζικο Θεώρημα Υπολοίπων

Ορισμός 1. Έστω I, J ιδεώδη ενός δακτυλίου R . Τα I, J θα λέγονται **σχετικά πρώτα** αν

$$I + J = \{a + b \mid a \in I, b \in J\} = R$$

Αν ο R έχει μονάδα, ισοδύναμα υπάρχουν $a \in I$ και $b \in J$ ώστε $a + b = 1$.

Παρατήρηση 1. Ο παραπάνω ορισμός μπορεί να γενικευτεί, δηλαδή τα ιδεώδη $I_1, \dots, I_n$ ενός δακτυλίου R , θα λέγονται **σχετικά πρώτα** αν

$$I_1 + \dots + I_n = \{a_1 + \dots + a_n \mid a_j \in I_j\} = R.$$

Παράδειγμα 2 (Σημαντικό!). Έστω F σώμα, $f(x), g(x) \in F[x]$ **σχετικά πρώτα**, $I = \langle f(x) \rangle$ και $J = \langle g(x) \rangle$. Αφού $f(x)$ και $g(x)$ είναι σχετικά πρώτα, τότε υπάρχουν $a(x), b(x) \in F[x]$ ώστε

$$1 = \underbrace{a(x)f(x)}_{\in I} + \underbrace{b(x)g(x)}_{\in J} \in I + J.$$

Συνεπώς, τα ιδεώδη I, J είναι σχετικά πρώτα.

Παράδειγμα 3 (Σημαντικό!). Έστω $m, n \in \mathbb{Z}$ σχετικά πρώτοι μεταξύ τους. Αν $I = m\mathbb{Z}$ και $J = n\mathbb{Z}$, όμοιος με την προηγούμενη περίπτωση, τα I, J είναι σχετικά πρώτα.

Θέωρημα 1 (Κινέζικο Θεώρημα Υπολοίπων). Έστω R δακτύλιος και $I_1, \dots, I_n$ ιδεώδη του R .

(α) Η απεικόνιση

$$\psi: R/\bigcap_{j=1}^n I_j \rightarrow R/I_1 \times \cdots \times R/I_n, \quad \psi\left(r + \bigcap_{j=1}^n I_j\right) = (r + I_1, \dots, r + I_n).$$

είναι μονομορφισμός δακτυλίων.

(β) Αν $I_1, \dots, I_n$ είναι σχετικά πρώτα, τότε η ψ είναι ισομορφισμός δακτυλίων, δηλαδή

$$R/\bigcap_{j=1}^n I_j \cong R/I_1 \times \cdots \times R/I_n.$$

Απόδειξη. Βλέπε σημειώσεις Μ. Μαλιάκα. □

Παρατήρηση 2 (Ειδική Περίπτωση). Αν I, J σχετικά πρώτα ιδεώδη ενός δακτυλίου R , τότε

$$R/I \cap J \cong R/I \times R/J.$$

Σχόλιο 1. Γενικά όταν μας ζητείται να δείξουμε ένα ισομορφισμό μεταξύ δακτυλίων, όπου ο ένας είναι ευθύ γινόμενο δακτυλίων (καρτεσιανό γινόμενο), τότε είναι αρκετά πιθανό να πρέπει να εφαρμόσουμε Κ.Θ.Υ. (Κινέζικο Θεώρημα Υπολοίπων).

Παρατήρηση 3. Έστω I, J ιδεώδη ενός δακτυλίου R . Γνωρίζουμε ότι $IJ \subseteq I \cap J$. Αν I, J είναι σχετικά πρώτα, τότε $IJ = I \cap J$. Αυτό θα μπορούσε να είναι χρήσιμο στην περίπτωση, όπου $R = F[x]$, όπου γνωρίζουμε ότι $\langle f(x) \rangle \cdot \langle g(x) \rangle = \langle f(x)g(x) \rangle$.

Παράδειγμα 4. Δείξτε ότι $\mathbb{C}[x]/\langle (x-1)(x-2) \rangle \cong \mathbb{C} \times \mathbb{C}$.

Λύση. Έστω $I = \langle x-1 \rangle$ και $J = \langle x-2 \rangle$ τα οποία είναι σχετικά πρώτα ιδεώδη, αφού $x-1, x-2$ είναι σχετικά πρώτα. Επίσης, από την παραπάνω παρατήρηση,

$$\langle (x-1)(x-2) \rangle = IJ = I \cap J$$

Από το Κινέζικο Θεώρημα Υπολοίπων

$$\mathbb{C}[x]/\langle (x-1)(x-2) \rangle \cong \mathbb{C}[x]/I \cap J \cong \mathbb{C}[x]/I \times \mathbb{C}[x]/J.$$

Μέσω του συνήθη ομομορφισμού εκτίμησης γνωρίζουμε ότι $\mathbb{C}[x]/\langle x-a \rangle \cong \mathbb{C}$, για κάθε $a \in \mathbb{C}$, συνεπώς,

$$\mathbb{C}[x]/\langle (x-1)(x-2) \rangle \cong \mathbb{C}[x]/I \times \mathbb{C}[x]/J \cong \mathbb{C} \times \mathbb{C}.$$

■

Παράδειγμα 5. Δείξτε ότι $\mathbb{R}[x]/\langle f(x) \rangle \cong \mathbb{R} \times \mathbb{C}$, όπου $f(x) = (x+1)(x^2+1)$.

Λύση. Άσκηση.

■

3 Ασκήσεις στους Δακτυλίους Πηλίκου

Άσκηση 1. Πόσα στοιχεία έχουν οι παρακάτω δακτύλιοι ; Ποιοι είναι σώματα ;

(α) $R = \mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$

(β) $S = \mathbb{Z}_3[x]/\langle x^3 + x + 1 \rangle$

Λύση. (α) Αρχικά, αν F σώμα με m στοιχεία και $f(x)$ μη μηδενικό πολυώνυμο βαθμού n , τότε γνωρίζουμε ότι $|F[x]/\langle f(x) \rangle| = m^n$. Άρα, $|R| = 2^3 = 8$. Τώρα, γνωρίζουμε ότι R σώμα αν και μόνο αν $f(x)$ ανάγωγο. Αφού $f(x)$ είναι βαθμού 3 και δεν έχει ρίζα στο $\mathbb{Z}_2$, τότε είναι ανάγωγο. Συνεπώς R είναι σώμα.

(β) Όμοια με (α), $|S| = 3^3 = 27$. Ο S δεν είναι σώμα, αφού το $f(x) = x^3 + x + 1$ δεν είναι ανάγωγο ($f(1) = 3 = 0$).

■

Άσκηση 2. Έστω $p(x) = x^2 + 1 \in \mathbb{Z}_3[x]$ και $I = \langle p(x) \rangle$.

(α) Δείξτε ότι $\mathbb{Z}_3[x]/I$ είναι σώμα με 9 στοιχεία.

(β) Εξετάστε αν τα $x^4 + x + 1 + I$, $x^4 + 2 + I$ είναι αντιστρέψιμα στοιχεία στον $\mathbb{Z}_3[x]/I$ και αν είναι βρείτε τον αντίστροφό τους.

Λύση. (α) Βλέπε Άσκηση 4 (α).

(β) Θυμίζουμε ότι $g(x)+I$ είναι αντιστρέψιμο στον $\mathbb{Z}_3[x]/I$ αν και μόνο αν $\mu.κ.δ.(g(x), p(x)) = 1$.

- Το $x^4 + 2 + I$, δεν είναι αντιστρέψιμο αφού

$$x^4 + 2 = x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x^2 - 1)p(x).$$

- Εφαρμόζουμε ευκλείδειο αλγόριθμο για τα $g(x) = x^4 + x + 1$ και $p(x)$

$$g(x) = (x^2 - 1)p(x) + x + 2$$

$$p(x) = (x + 1)(x + 2) + 2$$

Συνεπώς, έχουμε ότι

$$2 = p(x) - (x + 1)(x + 2)$$

$$2 = p(x) - (x + 1)[g(x) - (x^2 - 1)p(x)]$$

$$2 = -(x + 1)g(x) + q(x)p(x)$$

$$1 = (x + 1)g(x) + h(x)p(x)$$

Από την τελευταία σχέση περνώντας σε κλάσεις mod I

$$1 + I = (x + 1 + I) \cdot (g(x) + I) + \underbrace{h(x)p(x) + I}_{=0} = (x + 1 + I) \cdot (g(x) + I).$$

Συνεπώς, έχουμε ότι $(g(x) + I)^{-1} = x + 1 + I$.

■

Άσκηση 3. Θεωρούμε τα ιδεώδη $I = \langle x^2 + 2 \rangle$ και $J = \langle x^2 + 1 \rangle$ στο $\mathbb{Z}_5[x]$ και $R = \mathbb{Z}_5[x]/I$ και $S = \mathbb{Z}_5[x]/J$.

- (α) Δείξτε ότι R σώμα, αλλά S όχι περιοχή.
- (β) Αληθεύει ότι $R \cong \mathbb{Z}_5 \times \mathbb{Z}_5$; Αληθεύει ότι $S \cong \mathbb{Z}_5 \times \mathbb{Z}_5$;
- (γ) Πόσα στοιχεία έχει ο R ; Πόσα αντιστρέψιμα στοιχεία έχει ο S ;

Λύση. (α) Δείξτε ότι $x^2 + 2$ δεν έχει ρίζα στο $\mathbb{Z}_5$ και συμπεράνετε ότι είναι ανάγωγο. Συνεπώς, ο R είναι σώμα. Τώρα, το $f(x) = x^2 + 1$ έχει ρίζες το 2, 3 στο $\mathbb{Z}_5$, άρα $x^2 + 1 = (x - 2)(x - 3)$. Παρατηρούμε ότι

$$(x - 2) + I \cdot (x - 3) + I = x^2 + 1 + I = 0 + I.$$

με $x - 2 + I \neq 0 + I$ και $x - 3 + I \neq 0 + I$, άρα S δεν είναι περιοχή.

(β) Ο R είναι σώμα, ενώ $\mathbb{Z}_5 \times \mathbb{Z}_5$ δεν είναι περιοχή, άρα οι δακτύλιοι δεν μπορεί να είναι ισόμορφοι. Όμοια με το Παράδειγμα 4 έχουμε ότι

$$S = \mathbb{Z}_5[x]/\langle (x-2)(x-3) \rangle \cong \mathbb{Z}_5[x]/\langle (x-2) \rangle \times \mathbb{Z}_5[x]/\langle (x-3) \rangle \cong \mathbb{Z}_5 \times \mathbb{Z}_5.$$

(γ) Ομοίως με Άσκηση 4 ισχύει ότι $|R| = 5^2 = 25$. Για το δεύτερο σκέλος, δείξαμε ότι $S \cong \mathbb{Z}_5 \times \mathbb{Z}_5$. Άρα, $|U(S)| = |U(\mathbb{Z}_5 \times \mathbb{Z}_5)|$. Έχουμε δείξτε ότι

$$U(A \times B) = U(A) \times U(B)$$

όπου A, B τυχαίοι δακτύλιοι. Άρα,

$$|U(S)| = |U(\mathbb{Z}_5 \times \mathbb{Z}_5)| = |U(\mathbb{Z}_5) \times U(\mathbb{Z}_5)| = |U(\mathbb{Z}_5)|^2 = [\varphi(5)]^2 = 16.$$

■

4 Η έννοια της ομάδας

Ορισμός 2. Ένα σύνολο G εφοδιασμένο με μια πράξη $\cdot : G \times G \rightarrow G$ λέγεται **ομάδα** αν

- (α) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, για κάθε $a, b, c \in G$ (προσεταιριστική ιδιότητα)
- (β) υπάρχει $e \in G$ ώστε $a \cdot e = e \cdot a = a$, για κάθε $a \in G$ (ύπαρξη ουδέτερου στοιχείου)
- (γ) για κάθε $a \in G$, υπάρχει $b \in G$ ώστε $ab = ba = e$ (ύπαρξη αντιστρόφου).

Αν επιπλέον $a \cdot b = b \cdot a$, για κάθε $a, b \in G$, τότε η G λέγεται **αβελιανή**.

Παρατήρηση 4. Έστω $(G, \cdot)$ ομάδα και $a, b \in G$.

- (α) Το ουδέτερο στοιχείο $e \in G$ είναι μοναδικό. Αρκετές φορές συμβολίζεται με 1 ή 1_G .
- (β) Ο αντίστροφος του $a \in G$ είναι μοναδικός και συμβολίζεται με a^{-1} .
- (γ) Για $m \in \mathbb{Z} > 0$ ορίζουμε $a^m = \underbrace{a \cdot a \cdots a}_m \text{ φορές}$, ενώ $a^{-m} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_m \text{ φορές}$. Προφανώς, $a^0 = 1_G$.
- (δ) Για κάθε $m, n \in \mathbb{Z}$, τότε $a^m \cdot a^n = a^{m+n}$.
- (ε) Αν $ab = ba$, τότε $(ab)^n = a^n b^n$, για κάθε $n \in \mathbb{Z}$.

Παρατήρηση 5. Αν η G είναι αβελιανή, αρκετές φορές αντί για $\cdot$ χρησιμοποιούμε $+$ για τον συμβολισμό της πράξης της. Τότε, το ουδέτερο στοιχείο συμβολίζεται με 0_G και αντί για a^m γράφουμε ma .

Παράδειγμα 6. Τα ζεύγη $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ και $(\mathbb{C}, +)$ είναι αβελιανές ομάδες, όπου $+$ η συνήθης πρόσθεση. Εδώ το ουδέτερο στοιχείο είναι το 0 και ο αντίστροφος του a είναι το $-a$.

Παράδειγμα 7. Έστω R δακτύλιος. Το ζεύγος $(R, +)$ (πρόσθεση του δακτυλίου) είναι αβελιανή ομάδα (γιατί ;). Τώρα, έχουμε δείξει ότι αν $a, b \in U(R)$, τότε $ab \in U(R)$ και μάλιστα $(ab)^{-1} = b^{-1}a^{-1}$. Το σύνολο $U(R)$ μαζί με τον πολλαπλασιασμό του R είναι ομάδα (γιατί ;).

Παράδειγμα 8. Ένα σύνολο με ένα στοιχείο είναι ομάδα $G = \{1_G\}$ και λέγεται **τετριμμένη ομάδα**.

Ορισμός 3. Έστω $X \neq \emptyset$ σύνολο. Το **σύνολο συμμετριών** του X είναι το

$$S(X) = \{f: X \rightarrow X \mid f \text{ είναι } 1-1 \text{ και επί}\}.$$

Παράδειγμα 9. Έστω $X \neq \emptyset$ σύνολο. Το σύνολο συμμετριών $S(X)$ του X είναι ομάδα με πράξη την σύνθεση.

Απόδειξη. Προφανώς η σύνθεση συναρτήσεων είναι προσεταιριστική πράξη. Τώρα, η απεικόνιση $\text{id}_X: X \rightarrow X$ η συνήθης ταυτοτική απεικόνιση του X είναι του ουδέτερο στοιχείο της $S(X)$, αφού για κάθε $f \in S(X)$, τότε $f \circ \text{id}_X(x) = f(x)$, για κάθε $x \in X$. Τώρα, αν $f \in S(X)$, αφού f είναι 1-1 και επί, επιδέχεται αντίστροφη $g: X \rightarrow X \in S(X)$ με

$$f \circ g = g \circ f = \text{id}_X.$$

Άρα, κάθε $f \in S(X)$ έχει αντίστροφο. □

5 Η Συμμετρική Ομάδα S_n

Ορισμός 4. Η **συμμετρική ομάδα μεταθέσεων** S_n ($n \in \mathbb{Z}_{>0}$) είναι το σύνολο συμμετριών του συνόλου $\{1, \dots, n\}$ με πράξη την σύνθεση συναρτήσεων, δηλαδή

$$S_n = S(\{1, \dots, n\}) = \{f: \{1, \dots, n\} \rightarrow \{1, \dots, n\} \mid f \text{ είναι } 1-1 \text{ και επί}\}.$$

Τα στοιχεία $\sigma \in S_n$ θα συμβολίζονται με

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}.$$

Παράδειγμα 10. Στην S_3 η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ είναι η απεικόνιση όπου $\sigma(1) = 3$, $\sigma(2) = 2$ και $\sigma(3) = 1$.

Παρατήρηση 6. (α) Το ουδέτερο στοιχείο της S_n είναι η ταυτοτική απεικόνιση, δηλαδή

$$1_{S_n} = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 2 & 3 & \cdots & n \end{pmatrix}.$$

(β) Έχουμε ότι

- $S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}$
- $S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$.
- $S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}$

Πως συνθέτουμε δύο μεταθέσεις ;

Παράδειγμα 11. Στην S_3 θεωρούμε τις μεταθέσεις $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ και $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

Θέλουμε να υπολογίσουμε την σύνθεση $\sigma\tau$:

$$\begin{array}{ccc} 1 & 2 & 3 \\ \downarrow \tau & \downarrow \tau & \downarrow \tau \\ 3 & 2 & 1 \\ \downarrow \sigma & \downarrow \sigma & \downarrow \sigma \\ 3 & 1 & 2 \end{array}$$

Άρα, προκύπτει ότι $\sigma\tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

Παρατήρηση 7. Εξ' ορισμού γνωρίζου με ότι μια $\sigma \in S_n$ είναι 1-1 και επί. Συνεπώς, έχει αντίστροφη. Πως υπολογίζουμε την αντιστίστροφή της ;

Έστω $\sigma \in S_n$. Τότε, γνωρίζουμε ότι $\sigma^{-1}\sigma = 1_{S_n}$. Άρα, για $k \in \{1, \dots, k\}$ ισχύει ότι

$$k \xrightarrow{\sigma} \sigma(k) \xrightarrow{\sigma^{-1}} k$$

Άρα, η σ^{-1} στέλνει το $\sigma(k)$ στο k . Με καταχρηστικό συμβολισμό λοιπόν ισχύει ότι

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \cdots & \sigma(n) \\ 1 & \cdots & n \end{pmatrix}$$

Ταξινομώντας την πάνω γραμμή κατά αύξουσα σειρά παίρνουμε την σ^{-1} .

Παράδειγμα 12. Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$. Τότε ισχύει ότι

$$\sigma^{-1} = \begin{pmatrix} 3 & 4 & 5 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}.$$

Παρατήρηση 8. Ισχύει ότι S_n είναι αβελιανή για κάθε $n \geq 1$; Φυσικά και όχι! Για $n = 1, 2$ είναι προφανώς αβελιανή, αλλά για κάθε $n \geq 3$, η S_n δεν είναι αβελιανή. Θεωρούμε τις $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 2 & 1 & 3 & \cdots & n \end{pmatrix}$ και $\tau = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ 1 & 3 & 2 & \cdots & n \end{pmatrix}$. Τότε, $\sigma\tau(3) = \sigma(2) = 1$ ενώ $\tau\sigma(3) = \tau(3) = 2$, άρα $\sigma\tau \neq \tau\sigma$.

Πρόταση 1. Για κάθε $n \geq 1$ ισχύει ότι $|S_n| = n!$

Απόδειξη. Έστω $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$. Για το $\sigma(1)$ έχουμε n επιλογές. Για το $\sigma(2)$ έχουμε $n-1$ επιλογές (η σ είναι 1-1). Συνεχίζοντας για το $\sigma(n)$ έχουμε 1 επιλογή, άρα από την πολλαπλασιαστική αρχή, για την σ έχουμε $n \cdot (n-1) \cdots 2 \cdot 1 = n!$ επιλογές. $\square$

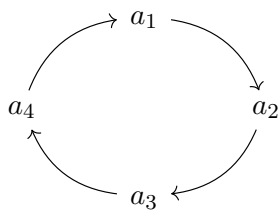
Ορισμός 5. Μια $\sigma \in S_n$ λέγεται **κυκλική μετάθεση** ή **κύκλος** μήκους m αν υπάρχουν διακεκριμένα $a_1, \dots, a_m \in \{1, \dots, n\}$ ώστε

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \dots, \sigma(a_{m-1}) = a_m, \sigma(a_m) = a_1$$

και $\sigma(i) = i$, για κάθε $i \notin \{a_1, \dots, a_m\}$. Στην περίπτωση αυτή συμβολίζουμε

$$\sigma = (a_1 \ a_2 \ \cdots \ a_m).$$

Το m λέγεται **μήκος του κύκλου**. Κάθε κύκλος μήκους 2 λέγεται **αντιμετάθεση**.



Κύκλος μήκους 4.

Παράδειγμα 13. Η $\sigma = (2\ 3\ 1) \in S_5$ είναι η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$.

Παρατήρηση 9. Αν $\sigma = (a_1 \ \cdots \ a_m)$, τότε $\sigma^{-1} = (a_m \ a_{m-1} \ \cdots \ a_2 \ a_1)$.

$$a_1 \xrightarrow{\sigma} a_2 \xrightarrow{\sigma} a_3 \xrightarrow{\sigma} \cdots \xrightarrow{\sigma} a_m$$

$$a_1 \xleftarrow{\sigma^{-1}} a_2 \xleftarrow{\sigma^{-1}} a_3 \xleftarrow{\sigma^{-1}} \cdots \xleftarrow{\sigma^{-1}} a_m$$

Πρόταση 2. Έστω $\sigma, \tau \in S_n$ ξένες. Τότε, $\sigma\tau = \tau\sigma$.

Πόρισμα 1. Έστω $\sigma, \tau \in S_n$ ξένες και $k \in \mathbb{Z}$. Τότε, ισχύει ότι $(\sigma\tau)^k = \sigma^k\tau^k$.

Θέωρημα 2 (Ανάλυση Μετάθεσης σε Ξένους Κύκλους). Έστω $\sigma \in S_n$ με $\sigma \neq 1$. Τότε, υπάρχουν $a_1, \dots, a_k \in S_n$ ξένοι κύκλοι ανά δύο ώστε $\sigma = a_1 \cdots a_k$. Η ανάλυση αυτή είναι μοναδική ως προς αναδιάταξη των προηγούμενων κύκλων.

Απόδειξη. Βλέπε σημειώσεις Μ. Μαλιάκα. □

Παράδειγμα 14. Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 2 & 9 & 8 & 6 & 7 & 1 \end{pmatrix} \in S_9$. Τότε, ισχύει ότι $\sigma = (1\ 3\ 5\ 9)(2\ 4)(6\ 8\ 7)$.

6 Τάξη Στοιχείου Ομάδας

Ορισμός 6. Έστω G ομάδα και $g \in G$. Αν υπάρχει $m \in \mathbb{Z}_{>0}$ ώστε $g^m = 1$, τότε ο ελάχιστος τέτοιος $m \in \mathbb{Z}_{>0}$ λέγεται **τάξη** του g και συμβολίζεται με $o(g)$ ή $|g|$. Αν δεν υπάρχει $m \in \mathbb{Z}_{>0}$ ώστε $g^m = 1$, τότε λέμε ότι η τάξη του g είναι **άπειρη**.

Παράδειγμα 15. Σε κάθε ομάδας G ισχύει ότι $o(g) = 1$ αν και μόνο αν $g = 1$.

Παράδειγμα 16. Έστω $\sigma = (a_1\ a_2\ \cdots\ a_m) \in S_n$ κύκλος μήκους m . Τότε, έχουμε ότι $o(\sigma) = m$, αφού έχουμε δείξει ότι $\sigma^m = 1$ και για κάθε $0 \leq k \leq m-1$ ισχύει ότι $\sigma^{k-1} \neq 1$.

Παράδειγμα 17. Θεωρούμε την ομάδα $(\mathbb{R} \setminus \{0\}, \cdot)$. Τότε, είναι άμεσο ότι $o(1) = 1$ και $o(-1) = 2$, αφού $(-1)^2 = 1$.

Παράδειγμα 18. Θεωρούμε την ομάδα $(\mathbb{Z}_8, +)$ και $[6] \in \mathbb{Z}_8$. Παρατηρούμε ότι

$$[6]^1 = [6] \neq 0, [6]^2 = [36] = [4] \neq [0] \text{ και } [6]^3 = [6][4] = [24] = [0].$$

Συνεπώς, έχουμε ότι $o([6]) = 3$.

Παράδειγμα 19. Στην $(\mathbb{Z}, +)$ κάθε μη μηδενικό στοιχείο έχει άπειρη τάξη, αφού για κάθε $n \neq 0$ και $m \in \mathbb{Z}_{>0}$ ισχύει ότι $mn \neq 0$.

Παρατήρηση 10. Αν G πεπερασμένη ομάδα, τότε κάθε στοιχείο της G έχει πεπερασμένη τάξη.

Απόδειξη. Έστω $g \in G$. Τότε, για κάθε $n \in \mathbb{N}$ ισχύει ότι $g^n \in G$. Αφού G πεπερασμένη, τότε υπάρχουν $m < k$ ώστε $g^m = g^k$, δηλαδή $g^{k-m} = 1$. Από την τελευταία σχέση συμπεραίνουμε ότι g έχει πεπερασμένη τάξη. $\square$

Θέωρημα 3. Έστω G ομάδα και $g \in G$ στοιχείο τάξης n . Ισχύει τα επόμενα :

(α) Για κάθε $m \in \mathbb{Z}_{>0}$, όπου $g^m = 1$ ισχύει ότι $n|m$.

(β) Για κάθε $k \geq 1$ ισχύει ότι

$$o(g^k) = \frac{n}{\mu.κ.δ.(k, n)}.$$

Απόδειξη. Θα δείξουμε το (α). Για το (β), βλέπε σημειώσεις Μ. Μαλιάκα. Έστω $m \in \mathbb{Z}_{>0}$ ώστε $g^m = 1$. Εφαρμόζουμε ευκλείδεια διαίρεση στα m, n ($n \leq m$). Συνεπώς, υπάρχει $q, r \in \mathbb{Z}$ ώστε $m = nq + r$ με $0 \leq r < n$. Αν $r \neq 0$, τότε ισχύει ότι $0 < r < n$ και

$$g^r = g^{m-nq} = g^m \cdot (g^n)^{-q} = 1.$$

Έτσι καταλήγουμε σε άτοπο, από τον ορισμό του n . $\square$

Πρόταση 3. Έστω $\sigma, \tau \in S_n$ ξένες μεταθέσεις με τάξεις m, n αντίστοιχα. Τότε, ισχύει ότι $o(\sigma\tau) = \epsilon.κ.π.(m, n)$.

Απόδειξη. Έστω $k = o(\sigma\tau)$ και $\ell = \text{ε.κ.π.}(m, n)$. Αφού k, ℓ θετικοί ακέραιοι, αρκεί να δείξουμε ότι $k|\ell$ και $\ell|k$.

- Από το Θεώρημα 3, για να δείξουμε ότι $k|\ell$ αρκεί να δείξουμε ότι $(\sigma\tau)^\ell = 1$. Αφού ℓ είναι πολλαπλάσιο των m, n αντίστοιχα, ισχύει ότι $\ell = mx = ny$, για $x, y \in \mathbb{Z}_{>0}$. Τότε, έχουμε ότι

$$(\sigma\tau)^\ell = \sigma^\ell \tau^\ell = (\sigma^m)^x (\tau^n)^y = 1.$$

όπου η πρώτη ισότητα ισχύει γιατί οι σ, τ είναι ξένες.

- Για να δείξουμε ότι $\ell|k$, από τον ορισμό του ε.κ.π. αρκεί να δείξουμε ότι k είναι πολλαπλάσιο των m, n αντίστοιχα, δηλαδή $m|k$ και $n|k$. Από το Θεώρημα 3, αρκεί να δείξουμε ότι $\sigma^k = 1$ και $\tau^k = 1$. Έχουμε ότι

$$(\sigma\tau)^k = \sigma^k \tau^k = 1 \Rightarrow \sigma^k = \tau^{-k}.$$

Αφού, σ, τ είναι ξένες, τότε και σ^k, τ^{-k} είναι ξένες, συνεπώς προκύπτει ότι $\sigma^k = \tau^{-k} = 1$, άρα έχουμε το ζητούμενο.

□

Πρόταση 4. Έστω $\sigma \in S_n$ με $\sigma = a_1 a_2 \cdots a_k \neq 1$ γινόμενο ξένων κύκλων μηκών $n_1, \dots, n_k$. Τότε, ισχύει ότι

$$o(\sigma) = \text{ε.κ.π.}(n_1, \dots, n_k).$$

Απόδειξη. Εφαρμόστε επαγωγή χρησιμοποιώντας το Παράδειγμα 16 και την Πρόταση 13. □

7 Ασκήσεις

Άσκηση 4. Έστω G ομάδα και $a, b \in G$. Δείξτε ότι :

- (α) $o(a) = o(a^{-1})$,
- (β) $o(b^{-1}ab) = o(a)$,
- (γ) $o(ab) = o(ba)$,
- (δ) αν $b^{-1}a^2b = a^3$ με $a \neq 1$, τότε $o(a) \geq 5$.

Λύση. (α) Έχουμε ότι $a^k = 1$ αν και μόνο αν $a^{-k} = 1$, για κάθε $k \in \mathbb{Z}_{>0}$.

(β) Παρατηρήστε ότι $(b^{-1}ab)^k = b^{-1}a^k b$, συνεπώς, $(b^{-1}ab)^k = 1$ αν και μόνο αν $a^k = 1$.

(γ) Έχουμε ότι $ab = b^{-1}(ba)b$, συνεπώς από το (β) έχουμε το ζητούμενο.

(δ) Το ζητούμενο προφανώς ισχύει αν $o(a) = \infty$. Αλλιώς, από το (β) έχουμε ότι $o(a^2) = o(a^3)$. Έχουμε ότι

$$o(a^2) = \frac{o(a)}{(o(a), 2)} = \frac{o(a)}{(o(a), 3)} = o(a^3).$$

Άρα, έχουμε ότι $(o(a), 2) = (o(a), 3)$, ενώ $(o(a), 2) = 1$ ή 2 και $(o(a), 2) = 1$ ή 3 . Συνεπώς, $(o(a), 2) = (o(a), 3) = 1$ και αφού $o(a) \neq 1$, υπάρχει p πρώτος $p \geq 5$ ώστε $p|o(a)$. Έτσι έχουμε το ζητούμενο. ■

Άσκηση 5. Έστω G ομάδα, η οποία έχει μοναδικό στοιχείο τάξης 2, έστω a . Δείξτε ότι $ab = ba$, για κάθε $b \in G$.

Λύση. Έστω $b \in G$. Θέλουμε να δείξουμε ότι $ab = ba$ ισοδύναμα αρκεί να δείξουμε ότι $b^{-1}ab = a$. Από την Άσκηση 4 (β), έχουμε ότι $o(b^{-1}ab) = o(a) = 2$ και από την υπόθεση έχουμε ότι $b^{-1}ab = a$. ■

Άσκηση 6. Έστω G ομάδα, όπου για κάθε $g \in G$ με $g \neq 1$ ισχύει ότι $o(g) = 2$. Δείξτε ότι η G είναι αβελιανή.

Λύση. Έστω $a, b \in G$. Θέλουμε να δείξουμε ότι $ab = ba$. Από την υπόθεση, για κάθε $g \in G$, ισχύει ότι $g^2 = 1$, δηλαδή $g = g^{-1}$. Έχουμε ότι

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

■

Άσκηση 7. Έστω $\sigma = (1\ 2\ 3\ 4)(3\ 4\ 5\ 6) \in S_6$.

(α) Βρείτε την τάξη της σ^{100} .

(β) Εξετάστε αν υπάρχει $\tau \in S_6$ ώστε $\tau^3 = \sigma$.

Λύση. Παρατηρούμε ότι η δοσμένη σ είναι η

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix} = (1\ 2\ 3)(4\ 5\ 6).$$

Συνεπώς, από την Πρόταση 4, $o(\sigma) = \text{ε.κ.π.}(3, 3) = 3$. Άρα, προκύπτει ότι

$$o(\sigma^{100}) = \frac{3}{(3, 100)} = 3.$$

(β) Έστω, προς άτοπο, ότι υπάρχει $\tau \in S_6$ με $\tau^3 = \sigma$. Αφού $o(\sigma) = 3$ έχουμε ότι

$$o(\tau^3) = \frac{o(\tau)}{(o(\tau), 3)} = 3.$$

Έχουμε ότι $(o(\tau), 3) = 1$ ή 3 . Αν, $(o(\tau), 3) = 3$, άρα $o(\tau^3) = 1 = o(\sigma)$ το οποίο είναι άτοπο. Αν $(o(\tau), 3) = 1$, τότε από την παραπάνω σχέση έχουμε ότι $o(\tau) = 3$ και καταλήγουμε σε άτοπο. ■

8 Υποομάδες

Ορισμός 7. Έστω A σύνολο και $*$: $A \times A \rightarrow A$ μια πράξη στο A . Ένα $B \subseteq A$ λέγεται **κλειστό** υποσύνολο του A ως προς την πράξη $*$ αν $x * y \in B$, για κάθε $x, y \in B$. Ισοδύναμα, ο περιορισμός της πράξης $*$ στο $B \times B$ δίνει μια πράξη στο B : $*$: $B \times B \rightarrow B$.

Ορισμός 8. Έστω G ομάδα και $H \subseteq G$ κλειστό. Η H λέγεται **υποομάδα** της G αν είναι ομάδα με την πράξη της G περιορισμένη στο H . Στην περίπτωση αυτή συμβολίζουμε $H \leq G$.

Παράδειγμα 20. Είναι σαφές ότι $(\mathbb{Z}, +) \leq (\mathbb{Q}, +)$, $(\mathbb{Q}, +) \leq (\mathbb{R}, +)$ και $(\mathbb{R}, +) \leq (\mathbb{C}, +)$. Επίσης, $(\mathbb{R} \setminus \{0\}, \cdot) \leq (\mathbb{C} \setminus \{0\}, \cdot)$.

Παράδειγμα 21. Το $\mathbb{N}$ δεν είναι κλειστό υποσύνολο του $(\mathbb{Z}, +)$, αφού για κάθε $n \neq 0$ στο $\mathbb{N}$, τότε $-n \notin \mathbb{N}$.

Πρόταση 5. Έστω $(G, \cdot)$ ομάδα και $H \subseteq G$ μη κενό. Τα ακόλουθα είναι ισοδύναμα.

- (α) Η H είναι υποομάδα της G .
- (β) Για κάθε $a, b \in H$ ισχύει ότι $a \cdot b, a^{-1} \in H$.
- (γ) Για κάθε $a, b \in H$ ισχύει ότι $a \cdot b^{-1} \in H$.

Απόδειξη. Αποδείξτε την παραπάνω πρόταση. □

Παράδειγμα 22. Έστω $G = S_n$ και $H = \{\sigma \in S_n \mid \sigma(n) = n\}$. Θα δείξουμε ότι $H \leq G$. Πράγματι, έστω $\sigma, \tau \in H$. Τότε, $\sigma \circ \tau(n) = \sigma(n) = n$, συνεπώς $\sigma\tau \in H$. Επίσης, αφού $\sigma(n) = n$, τότε $\sigma^{-1}(n) = n$, άρα $\sigma^{-1} \in H$.

Παράδειγμα 23. Έστω G αβελιανή ομάδα και $H = \{g \in G \mid g^2 = 1\}$. Θα δείξουμε ότι $H \leq G$. Προφανώς, $H \neq \emptyset$, αφού $1 \in H$. Τώρα, έστω $a, b \in H$, δηλαδή $a^2 = b^2 = 1$. Τότε, αφού G αβελιανή, $(ab)^2 = a^2b^2 = 1$, συνεπώς $ab \in H$. Τέλος, αν $a^2 = 1$, τότε προφανώς $a^{-2} = 1$, άρα $a^{-1} \in H$.

Πρόταση 6. Έστω G ομάδα και $\{H_i\}_{i \in I}$ οικογένεια υποομάδων της G . Τότε, $\bigcap_{i \in I} H_i$ είναι υποομάδα της G .

Απόδειξη. Αποδείξτε την παραπάνω πρόταση. □

9 Θεώρημα Lagrange

Θέωρημα 4 (Lagrange). Έστω G πεπερασμένη ομάδα και $H \leq G$. Τότε, ισχύει ότι $|H| \mid |G|$.

Απόδειξη. Βλέπε σημειώσεις Μ. Μαλιάκα. □

Παράδειγμα 24. Έστω G ομάδα τάξης $n \leq 200$ και υποομάδες της H, K με τάξεις 10 και 11 αντίστοιχα.

- (α) Βρείτε την τάξη της G .
- (β) Δείξτε ότι για κάθε $g \in G$, υπάρχουν $h \in H$ και $k \in K$ ώστε $g = hk$.

Λύση. (α) Από το θεώρημα Lagrange, αφού $H, K \leq G$, τότε ισχύει ότι $10, 11 \mid |G|$ και αφού $(10, 11) = 1$, προκύπτει ότι $110 \mid |G|$. Αφού $1 \leq |G| \leq 200$ έχουμε ότι $|G| = 110$.

- (β) Έστω $HK = \{hk \mid h \in H, k \in K\} \subseteq G$. Αν δείξουμε ότι $|HK| = 110$, τότε θα έχουμε ότι $G = HK$ και το ζητούμενο έπεται άμεσα. Για κάθε $h \in H$ έχουμε 10 επιλογές και για κάθε $k \in K$ έχουμε 11 επιλογές.

Αν ξέραμε ότι για κάθε h, h' και $k, k' \in K$ με $hk = h'k' \Rightarrow h = h'$ και $k = k'$, τότε από την πολλαπλασιαστική αρχή για είχαμε ακριβώς 110 επιλογές για το hk . Έστω h, h' και $k, k' \in K$ με $hk = h'k'$, δηλαδή $(h')^{-1}h = k(k')^{-1} \in H \cap K$.

Πόσα στοιχεία έχει το $H \cap K$; Αφού $H \cap K \leq H, K$ από το Θεώρημα Lagrange ισχύει ότι $|H \cap K| \mid 10$ και $|H \cap K| \mid 11$. Συνεπώς, ισχύει ότι $|H \cap K| \mid (10, 11) = 1$, άρα $H \cap K = \{1\}$. Συνεπώς, αφού $(h')^{-1}h = k(k')^{-1} \in H \cap K = \{1\}$ έχουμε ότι $(h')^{-1}h = 1$ και $k(k')^{-1} = 1$, δηλαδή $h = h'$ και $k = k'$. ■

10 Κυκλικές Ομάδες

Ορισμός 9. Έστω G ομάδα και $g \in G$. Η **κυκλική υποομάδα** που παράγεται από το g είναι το σύνολο $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Παρατήρηση 11. Δείξτε ότι το σύνολο $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ είναι πράγματι ομάδα.

Παρατήρηση 12. Αν η πράξη της G είναι προσθετική, τότε έχουμε ότι $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$

Ορισμός 10. Μια ομάδα G θα λέγεται **κυκλική** αν υπάρχει $g \in G$ ώστε $G = \langle g \rangle$. Στην περίπτωση αυτή το g λέγεται **γεννήτορας** της G .

Παράδειγμα 25. Στην $(\mathbb{Z}, +)$, για κάθε $m \in \mathbb{Z}$, έχουμε ότι $m\mathbb{Z} = \{km \mid k \in \mathbb{Z}\} = \langle m \rangle$ είναι κυκλική.

Παράδειγμα 26. Η $\mathbb{Z}$ είναι κυκλική και μάλιστα $\mathbb{Z} = \langle 1 \rangle$, αφού κάθε $n \in \mathbb{Z}$ γράφεται $n = n \cdot 1$. Όμοια, η ομάδα $(\mathbb{Z}_n, +)$ είναι κυκλική τάξης n , αφού $\mathbb{Z}_n = \langle [1] \rangle$.

Παρατήρηση 13. Κάθε κυκλική ομάδα είναι αβελιανή.

Απόδειξη. Αποδείξτε την παραπάνω Παρατήρηση. □

Πρόταση 7. Κάθε ομάδα G με τάξη p πρώτο είναι κυκλική.

Απόδειξη. Αφού $|G| = p \neq 1$, τότε υπάρχει $g \in G$ με $g \neq 1$. Συνεπώς, $\langle g \rangle \neq \{1\}$ και από το Θεώρημα Lagrange ισχύει ότι $|\langle g \rangle| \mid |G| = p$. Συνεπώς, $|\langle g \rangle| = 1$ ή p και αφού $|\langle g \rangle| = p = |G|$ έχουμε ότι $G = \langle g \rangle$. □

Κίνητρο 1. Έχουμε δει ότι $(\mathbb{Z}_n, +)$ είναι κυκλική με $\mathbb{Z}_n = \langle [1] \rangle = \{[0], \dots, [n-1]\}$. Μήπως, αυτή η ιδιότητα μπορεί να μεταφερθεί σε οποιαδήποτε πεπερασμένη κυκλική ομάδα ;

Πρόταση 8. Έστω $G = \langle g \rangle$ κυκλική με $o(g) = n$. Τότε, $G = \{1, g, \dots, g^{n-1}\}$

Απόδειξη. Γνωρίζουμε ότι $G = \langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$. Έστω $g^k \in G$. Από ευκλείδεια διαίρεση του k με το n , υπάρχουν $q, r \in \mathbb{Z}$ με $0 \leq r \leq n-1$ ώστε $k = qn + r$. Τότε,

$$g^k = g^{qn+r} = \underbrace{(g^n)^q}_1 \cdot g^r = g^r \in \{1, g, \dots, g^{n-1}\}.$$

Άρα, $G \subseteq \{1, g, \dots, g^{n-1}\}$. Η αντίστροφη σχέση περιέχεται προφανώς ισχύει, άρα έχουμε ισότητα. $\square$

Πρόταση 9. Έστω G πεπερασμένη ομάδα με $|G| = n$. Τότε, αν $g \in G$ με $o(g) = k$, τότε $k|n$.

Απόδειξη. Έστω $H = \langle g \rangle \leq G$ υποομάδα, όπου από την Πρόταση 12, έχουμε ότι $|H| = o(g) = k$. Από το Θεώρημα Lagrange ισχύει ότι $k = |H| \mid |G| = n$. $\square$

Παράδειγμα 27. Έστω $G = \langle g \rangle$ ομάδα τάξης 12. Βρείτε την τάξη της ομάδας $\langle g^{26} \rangle \cap \langle g^{99} \rangle$.

Λύση. Αρχικά, από Πρόταση 12, έχουμε ότι $o(g) = 12$. Παρατηρούμε ότι $g^{26} = g^{2 \cdot 12 + 2} = g^2$ και ομοίως $g^{99} = g^{8 \cdot 12 + 3} = g^3$. Άρα, αναζητούμε την τάξη της ομάδας $\langle g^2 \rangle \cap \langle g^3 \rangle$. Έχουμε ότι

$$o(g^2) = \frac{12}{(2, 12)} = 6 \quad \text{και} \quad o(g^3) = \frac{12}{(3, 12)} = 4.$$

Α' Τρόπος

Από την Πρόταση 12, έχουμε ότι

$$\langle g^2 \rangle = \{1, g^2, g^4, g^6, g^8, g^{10}\}$$

και

$$\langle g^3 \rangle = \{1, g^3, g^6, g^9\}.$$

Άρα, έχουμε ότι $\langle g^2 \rangle \cap \langle g^3 \rangle = \{1, g^6\}$. Άρα, η τάξη της αντίστοιχης ομάδας είναι 2.

Β' Τρόπος

Αν $H = \langle g^2 \rangle \cap \langle g^3 \rangle$, τότε αφού $H \leq \langle g^2 \rangle, \langle g^3 \rangle$, από το Θεώρημα Lagrange, έχουμε ότι $|H| \mid 6$ και $|H| \mid 4$, άρα $|H| \mid (4, 6) = 2$. Συνεπώς, ισχύει ότι $|H| = 1$ ή 2. Αφού $g^6 \in \langle g^2 \rangle \cap \langle g^3 \rangle$ με $g^6 \neq 1$, άρα $|H| = 2$. $\blacksquare$

11 Άρτιες και Περιττές Μεταθέσεις

Ορισμός 11. Μια $\sigma \in S_n$ λέγεται **αντιμετάθεση** αν είναι κύκλος μήκους 2, δηλαδή της μορφής $\sigma = (a_1 a_2)$.

Πρόταση 10. Κάθε $\sigma \in S_n$ γράφεται ως γινόμενο αντιμεταθέσεων.

Απόδειξη. Γνωρίζουμε ότι κάθε μη τετριμμένη μετάθεση γράφεται ως γινόμενο ξένων κύκλων ανά δύο. Συνεπώς, αρκεί να δείξουμε το ζητούμενο υποθέτοντας ότι $\sigma = (a_1 \cdots a_m)$ κύκλος μήκους m . Παρατηρήστε ότι

$$\sigma = (a_1 \cdots a_m) = (a_1 a_m)(a_1 a_{m-1}) \cdots (a_1 a_2).$$

Μπορεί η παραπάνω ιδέα για γραφή σε γινόμενο αντιμεταθέσεων να φαίνεται αναπάντεχη και μη προφανής, αλλά περιγράφεται πλήρως από το παρακάτω σχήμα. $\square$

Κίνητρο 2. Μπορούμε να ισχυριστούμε ότι η γραφή σε γινόμενο αντιμεταθέσεων είναι μοναδική ; Φυσική και όχι ! Για παράδειγμα, αν $\sigma = (12) \in S_3$, τότε $\sigma = (12)(13)(13)$. Άρα, μπορεί κάποιο χαρακτηριστικό να παραμένει σταθερό ως προς αυτή την ιδιότητα ; Φυσικά ! Αυτό είναι το πρόσημο του πλήθους των αντιμεταθέσεων. Δεν μπορεί να μετάθεση να γράφεται ταυτόχρονα ως γινόμενο άρτιου και περιττού πλήθους αντιμεταθέσεων. Για την απόδειξη αυτού του ισχυρισμού βλέπε σημειώσεις Μ. Μαλιάκα. Θεωρώντας δεδομένο αυτό δίνουμε τους ακόλουθους ορισμούς.

Ορισμός 12. Έστω $\sigma \in S_n$. Η σ λέγεται **άρτια** αν μπορεί να γραφτεί ως άρτιο πλήθος αντιμεταθέσεων. Σε αντίθετη περίπτωση η σ λέγεται **περιττή**. Επίσης, ορίζουμε

$$A_n = \{\sigma \in S_n \mid \sigma \text{ είναι άρτια}\}$$

η οποία λέγεται **εναλλάσσουσα υποομάδα** της S_n .

Πρόταση 11. Η A_n είναι πράγματι υποομάδα της S_n και μάλιστα $|A_n| = |S_n|/2 = n!/2$.

Παρατήρηση 14. Μπορεί να ορισθεί συνάρτηση $\text{sign}: S_n \rightarrow \{0, 1\}$ με

$$\text{sign}(\sigma) = \begin{cases} 0, & \sigma \text{ είναι άρτια} \\ 1, & \sigma \text{ είναι περιττή} \end{cases}.$$

Παράδειγμα 28. Στην S_{10} θεωρούμε την μετάθεση $\sigma = (1 \ 3 \ 5 \ 9 \ 8)$. Τότε, έχουμε ότι $\sigma = (18)(19)(15)(13)$, δηλαδή συμπεραίνουμε ότι σ είναι άρτια.

12 Ασκήσεις

Άσκηση 8. Έστω G ομάδα και H, K υποομάδες της G με τάξεις m, n αντίστοιχα, ώστε $(m, n) = 1$. Δείξτε ότι $H \cap K = \{1\}$.

Λύση. Έχουμε ότι $H \cap K \leq H$ και $H \cap K \leq K$, άρα από το Θεώρημα Lagrange $|H \cap K| \mid m$ και $|H \cap K| \mid n$, άρα ισχύει ότι $|H \cap K| \mid (m, n) = 1$, συνεπώς έχουμε άμεσα ότι $H \cap K = \{1\}$. ■

Άσκηση 9. Έστω G ομάδα τάξης pq , όπου p, q πρώτοι. Δείξτε ότι κάθε γνήσια υποομάδα της G είναι κυκλική.

Λύση. Έστω $H \subsetneq G$, δηλαδή $|H| < |G| = pq$. Από το Θεώρημα Lagrange, έχουμε ότι $|H| \mid |G| = pq$ και αφού $|H| < |G| = pq$, τότε $|H| = 1$ ή p ή q . Προφανώς, αν $H = \{1\} = \langle 1 \rangle$, ενώ αν $|H| = p$ ή q , έχουμε δείξει ότι ομάδες με τάξη πρώτο αριθμό είναι κυκλικές. ■

Άσκηση 10. Δίνεται η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 5 & 2 & 6 & 3 & 1 \end{pmatrix} \in S_7$.

- (α) Εξετάσθε αν η σ είναι περιττή.
- (β) Βρείτε τους $m \in \mathbb{Z}$ ώστε $\langle \sigma^m \rangle \leq A_7$.
- (γ) Εξετάσθε αν υπάρχει $\tau \in S_7$ ώστε $\sigma = \tau^{2020}$.

Λύση. (α) Έχουμε ότι $\sigma = (1\ 4\ 2\ 7)(3\ 5\ 6)$, συνεπώς ισχύει ότι $\sigma = (17)(12)(14)(36)(35)$, άρα η σ είναι περιττή.

- (β) Παρατηρούμε ότι $\langle \sigma^m \rangle \leq A_7$ αν και μόνο αν κάθε στοιχείο της $\langle \sigma^m \rangle$ είναι άρτια μετάθεση, δηλαδή σ^{mk} είναι άρτια, για κάθε $k \in \mathbb{Z}$. Τα προηγούμενα είναι ισοδύναμα με το σ^m να είναι άρτια. Όμως, από (α), ισχύει ότι

$$\sigma^m = \underbrace{(17)(12)(14)(36)(35)}_{5 - \text{αντ.}} \underbrace{(17)(12)(14)(36)(35)}_{5 - \text{αντ.}} \cdots \underbrace{(17)(12)(14)(36)(35)}_{5 - \text{αντ.}}.$$

$5m - \text{αντιμεταθέσεις}$

(γ) Είναι εύκολο να παρατηρήσει κανείς ότι για κάθε $\tau \in S_7$, όπου τ είναι γινόμενο k αντιμεταθέσεων, ισχύει ότι τ^{2020} είναι γινόμενο $2020k$ αντιμεταθέσεων, άρα τ^{2020} είναι άρτια. Αφού σ είναι περιττή, συμπεραίνουμε ότι δεν υπάρχει $\tau \in S_7$ ώστε $\sigma = \tau^{2020}$. ■

Άσκηση 11. Έστω G ομάδα τάξης 105.

- (α) Αν $H \leq G$ με $|H| > 35$, δείξτε ότι $H = G$.
- (β) Αν $g \in G$ με $g^{39} = 1$, δείξτε ότι $g^3 = 1$.

Άσκηση 12. Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & a & 1 & b & 6 & 7 & 3 \end{pmatrix} \in S_7$.

- (α) Βρείτε a, b ώστε σ να είναι άρτια.
- (β) Αν σ είναι άρτια, αληθεύει ότι $(13)(56)(67) \in \langle \sigma \rangle$;

Άσκηση 13. Έστω $\sigma = (2\ 3\ 4\ 5)(4\ 5\ 1\ 6\ 7) \in S_7$.

- (α) Βρείτε την τάξη της σ και εξετάστε αν σ είναι άρτια.
- (β) Βρείτε την τάξη της ομάδας $\langle \sigma^{33} \rangle \cap \langle \sigma^{50} \rangle$.

13 Ομομορφισμοί Ομάδων

Ορισμός 13. Έστω $(G, \cdot), (H, *)$ ομάδες. Μια $\varphi: G \rightarrow H$ θα λέγεται **ομομορφισμός ομάδων** αν $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$, για κάθε $a, b \in G$.

- Αν φ είναι ομομορφισμός και 1-1 θα λέγεται **μονομορφισμός**.
- Αν φ είναι ομομορφισμός και επί θα λέγεται **επιμορφισμός**.
- Αν φ είναι ομομορφισμός και 1-1 και επί θα λέγεται **ισομορφισμός**.

Σημειώνουμε ότι δύο ομάδες G και H λέγονται **ισόμορφες**, αν υπάρχει $\varphi: G \rightarrow H$ ισομορφισμός ομάδων. Συμβολίζουμε με $G \cong H$.

Παρατήρηση 15. Έστω $\varphi: G \rightarrow H$ ομομορφισμός ομάδων. Τότε,

- (α) $\varphi(1_G) = 1_H$

(β) $\varphi(g^{-1}) = [\varphi(g)]^{-1}$, για κάθε $g \in G$.

(γ) $\varphi(g^n) = [\varphi(g)]^n$, για κάθε $g \in G$ και $n \in \mathbb{Z}$.

Παράδειγμα 29. Έστω R, S δακτύλιοι και $\varphi: R \rightarrow S$ ομομορφισμός δακτυλίων.

(α) Τότε, $(R, +), (S, +)$ αβελιανές ομάδες και $\varphi: (R, +) \rightarrow (S, +)$ είναι ομομορφισμός ομάδων.

(β) Έχουμε δει ότι $(U(R), \cdot), (U(S), \cdot)$ ομάδες και εύκολα αποδεικνύεται ότι $\varphi|_{U(R)}: (U(R), \cdot) \rightarrow (U(S), \cdot)$ είναι ομομορφισμός ομάδων.

Παράδειγμα 30. Έστω $\varphi: S_n \rightarrow \mathbb{Z}_2$, η οποία ορίζεται ως εξής

$$\varphi(\sigma) = \begin{cases} [0], & \sigma \text{ είναι άρτια} \\ [1], & \sigma \text{ είναι περιττή} \end{cases}.$$

Δείξτε ότι φ είναι επιμορφισμός ομάδων.

Πρόταση 12. Έστω $\varphi: G \rightarrow H$ και $\psi: H \rightarrow K$ ομομορφισμοί ομάδων.

(α) Η $\psi \circ \varphi$ είναι ομομορφισμός ομάδων.

(β) Αν φ είναι ισομορφισμός ομάδων, τότε φ^{-1} είναι ισομορφισμός ομάδων.

Απόδειξη. Άσκηση. Συγκρίνετε με την αντίστοιχη Πρόταση στους δακτυλίους. □

Πρόταση 13. Έστω $\varphi: G \rightarrow H$ ισομορφισμός ομάδων. Ισχύουν τα ακόλουθα :

(α) G είναι πεπερασμένη αν και μόνο αν H είναι πεπερασμένη.

(β) G είναι αβελιανή αν και μόνο αν H είναι αβελιανή.

(γ) G είναι κυκλική αν και μόνο αν H είναι κυκλική.

(δ) Για κάθε $g \in G$ ισχύει ότι $o(g) = o(\varphi(g))$.

Απόδειξη. Σημειώνουμε ότι αρκεί να δείξουμε τους ευθύς ισχυρισμούς, καθώς από την Πρόταση 12 (β), έχουμε ότι $\varphi^{-1}: H \rightarrow G$ είναι ισομορφισμός.

- (α) Προφανώς, αφού φ είναι 1-1 και επί, έχουμε ότι $|G| = |H|$ και το ζητούμενο έπεται άμεσα.
- (β) Έστω ότι G είναι αβελιανή. Θ.δ.ο. H είναι αβελιανή. Έστω $h_1, h_2 \in H$, τότε υπάρχουν g_1, g_2 ώστε $h_1 = \varphi(g_1)$ και $h_2 = \varphi(g_2)$. Τότε,

$$h_1 h_2 = \varphi(g_1) \varphi(g_2) = \underbrace{\varphi(g_1 g_2) = \varphi(g_2 g_1)}_{G \text{ αβελιανή}} = \varphi(g_2) \varphi(g_1) = h_2 h_1.$$

Συνεπώς, έχουμε ότι H είναι αβελιανή.

- (γ) Υποθέτουμε ότι $G = \langle g \rangle$ κυκλική. Θα δείξουμε ότι H αβελιανή και μάλιστα $H = \langle \varphi(g) \rangle$. Έστω $h \in H$. Αφού φ είναι επί, υπάρχει $x \in G$ ώστε $h = \varphi(x)$. Όμως, $x \in G = \langle g \rangle$, άρα υπάρχει k ώστε $x = g^k$. Συνεπώς, έχουμε ότι

$$h = \varphi(x) = \varphi(g^k) = [\varphi(g)]^k \in \langle \varphi(g) \rangle.$$

- (δ) Αφού η φ είναι ισομορφισμός, παρατηρήστε ότι για κάθε $g \in G$ ισχύει ότι $g^k = 1$ αν και μόνο αν $[\varphi(g)]^k = 1$. $\square$

Παρατήρηση 16. Αν θεωρήσουμε ομάδες $(G_1, \cdot), (G_2, *)$ μπορούμε να θεωρήσουμε το καρτεσιανό τους γινόμενο $G_1 \times G_2 = \{(g_1, g_2) \mid g_i \in G_i\}$, το οποίο αποκτά δομή ομάδας με τον προφανή τρόπο

$$(g_1, g_2) \cdot (g'_1, g'_2) := (g_1 \cdot g'_1, g_2 * g'_2).$$

Παρατήρηση 17. Για κάθε $[k] \in (\mathbb{Z}_n, +)$ έχουμε ότι $o(k) \leq n$, αφού $n[k] = [kn] = [0]$.

Παράδειγμα 31. Θα εξετάσουμε αν οι ομάδες $(\mathbb{Z}_4, +)$ και $\mathbb{Z}_2 \times \mathbb{Z}_2$ (όπως ορίσθηκε σε παραπάνω παρατήρηση) είναι ισόμορφες. Αρχικά $\mathbb{Z}_4$ έχουμε δει ότι είναι κυκλική. Αφού, $|\mathbb{Z}_2 \times \mathbb{Z}_2| = 4$, για να είναι κυκλική θα πρέπει να περιέχει στοιχείο τάξης 4. Όμως, για κάθε $([a], [b]) \in \mathbb{Z}_2 \times \mathbb{Z}_2$ έχουμε ότι $2([a], [b]) = ([0], [0])$, άρα $o(([a], [b])) \leq 2$. Συνεπώς, $\mathbb{Z}_2 \times \mathbb{Z}_2$ δεν περιέχει στοιχείο τάξης 4 και ειδικότερα δεν είναι κυκλική. Από την Πρόταση 13 προκύπτει ότι οι παραπάνω ομάδες δεν είναι ισόμορφες.

Ορισμός 14. Έστω $\varphi: G \rightarrow H$ ομομορφισμός ομάδων. Ορίζουμε ως **πυρήνα** της φ το σύνολο $\ker \varphi = \{g \in G \mid \varphi(g) = 1_H\}$.

Παρατήρηση 18. Δείξτε ότι για $\varphi: G \rightarrow H$ ομομορφισμό ομάδων, ισχύει ότι $\ker \varphi \leq G$ και $\text{Im} \varphi = \{\varphi(g) \mid g \in G\} \leq H$ και ότι φ είναι 1-1 αν και μόνο αν $\ker \varphi = \{1_G\}$.

Απόδειξη. Άσκηση. Συγκρίνετε την παραπάνω παρατήρηση με το αντίστοιχο αποτέλεσμα στους δακτύλιους. $\square$

14 Ταξινόμηση Κυκλικών Ομάδων

Κίνητρο 3. Γενικότερα, υπάρχουν άπειρες διακεκριμένες κυκλικές ομάδες οι οποίες δεν ξέρουμε καν ποια είναι ως σύνολα ούτε πως μπορούν να μοιάζουν. Παρόλα αυτά αν επικεντρωθούμε απλώς στην δομή τους ως ομάδες, όπως προδίδει και η Πρόταση 13, δύο ισόμορφες ομάδες πρακτικά είναι δύο διαφορετικές όψεις του ίδιου νομίσματος. Δηλαδή, αν τις εξετάσουμε ως προς τα ομοδοθεωρητικά τους χαρακτηριστικά είναι το ίδιο. Έτσι το παρακάτω θεώρημα, παρότι δεν γνωρίζουμε ακριβώς ποιες είναι όλες οι κυκλικές ομάδες με τα ακριβή σύνολα και τις πράξεις τους, ως προς ισομορφισμό μπορούμε να τις ταυτίσουμε με δύο περιπτώσεις : αν η G είναι άπειρη κυκλική είναι ισόμορφη με την $(\mathbb{Z}, +)$, ενώ αν είναι κυκλική τάξης n η G είναι ισόμορφη με την $(\mathbb{Z}_n, +)$. Συνεπώς, ως προς ισομορφισμό, έχουμε ταξινομήσει πλήρως τις κυκλικές ομάδες.

Θέωρημα 5. Έστω $G = \langle g \rangle$ κυκλική ομάδα.

- (α) Αν $|G| = \infty$, τότε $G \cong \mathbb{Z}$.
- (β) Αν $|G| = n < \infty$, τότε $G \cong \mathbb{Z}_n$.

Απόδειξη.

- (α) Έστω ότι $|G| = \infty$, δηλαδή $o(g) = \infty$. Θεωρούμε $\varphi: G \rightarrow \mathbb{Z}$ με $\varphi(g^k) = k$. Δείξτε ότι φ είναι ισομορφισμός ομάδων.
- (β) Έστω ότι $|G| = n < \infty$, δηλαδή $o(g) = n < \infty$. Θεωρούμε $\varphi: G \rightarrow \mathbb{Z}_n$ με $\varphi(g^k) = [k]$. Δείξτε ότι φ είναι ισομορφισμός ομάδων. $\square$

15 Δομή Κυκλικών Ομάδων

Κίνητρο 4. Μελετώντας ομάδες φυσιολογικά μπορούν να προκύψουν κάποια ερωτήματα.

- (α) Προφανώς υποομάδας πεπερασμένες ομάδας είναι πεπερασμένη. Επίσης, εύκολα αποδεικνύει κανείς ότι υποομάδα αβελιανής ομάδας είναι αβελιανή. Αν μας δώσουν μια κυκλική ομάδα παρόλα αυτά μπορούμε να ισχυριστούμε ότι ισχύει κάτι αντίστοιχο ; Δηλαδή ότι υποομάδα κυκλικής είναι κυκλική ; Η απάντηση είναι καταφατική !
- (β) Επίσης, το θεώρημα Lagrange μας λέει ότι για κάθε G πεπερασμένη και $H \leq G$, τότε $|H| \mid |G|$. Ισχύει για κάθε πεπερασμένη ομάδα το αντίστροφο ; Δηλαδή αν $d \mid |G|$, όπου G πεπερασμένη ομάδα και $d > 0$, ισχύει ότι υπάρχει $H \leq G$ ώστε $|H| = d$; Γενικά όχι ! Για παράδειγμα, δεν υπάρχει υποομάδα της A_4 (έχει τάξη 12) τάξης 2. Αν είχε αποδεικνύεται ότι αυτή η H θα περιείχε στοιχείο τάξης 2, το οποίο θα ήταν μια περιττή μετάθεση. Όμως, το αντίστροφο ισχύει στην ειδική περίπτωση όπου G είναι κυκλική. Μάλιστα, αυτή η H είναι και μοναδική !

Θέωρημα 6 (Δομή Κυκλικών Ομάδων). Έστω $G = \langle g \rangle$ κυκλική.

- (α) Αν $H \leq G$, τότε H είναι κυκλική.
(β) Υποθέτουμε ότι $|G| = n < \infty$ και έστω $d > 0$ ώστε $d|n$. Τότε, υπάρχει μοναδική κυκλική υποομάδα της G τάξης n .

Απόδειξη. (α) Αν $H = \{1\}$ προφανώς είναι κυκλική. Αν $H \neq \{1\}$, τότε υπάρχει $k \neq 0$ ώστε $g^k \in H$. Μάλιστα, αφού για κάθε $h \in H$, τότε h^{-1} , μπορούμε να υποθέσουμε ότι $k > 0$. Διαλέγουμε τον ελάχιστο $k > 0$ ώστε $g^k \in H$. Θα δείξουμε ότι $H = \langle g^k \rangle$. Προφανώς, $\langle g^k \rangle \subseteq H$. Έστω $g^\lambda \in H$. Από ευκλείδεια διαίρεση των λ, k , τότε υπάρχουν μοναδικά q, r ώστε $\lambda = qk + r$ με $0 \leq r < k$. Αν $r \neq 0$, τότε

$$g^r = (g^k)^{-q} \cdot g^\lambda \in H \quad 0 < r < k$$

Από τη επιλογή του k , τότε καταλήγουμε σε άτοπο, συνεπώς $r = 0$ και $g^\lambda = (g^k)^q \in \langle g^k \rangle$.

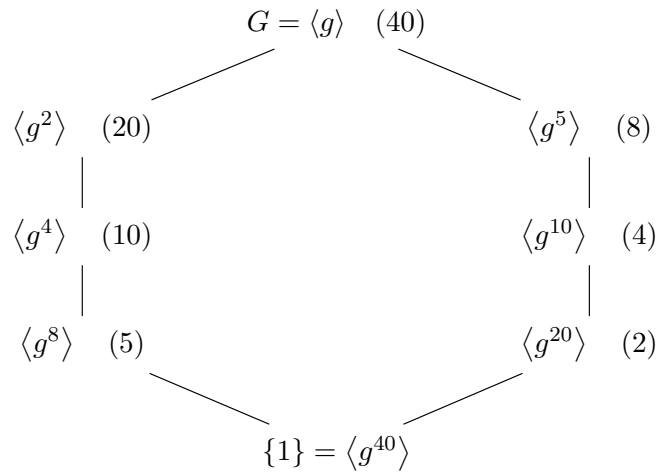
- (β) • Για την ύπαρξη, αν $k = n/d$ θα δείξουμε ότι $H = \langle g^k \rangle$ είναι η ζητούμενη υποομάδα τάξης d . Έχουμε ότι $|H| = o(g^k) = \frac{n}{(n,k)} = \frac{n}{k} = d$.
• Για την μοναδικότητα, έστω $K = \langle \sigma^\lambda \rangle$ μια άλλη υποομάδα της G τάξης d . Θ.δ.ο. $H = K$. Αφού $d = o(\sigma^\lambda) = \frac{n}{(\lambda, n)}$, τότε $(\lambda, n) = \frac{n}{d} = k$. Υπάρχουν x, y με $(\lambda, n) = x\lambda + yn = k$. Έτσι, $\sigma^k = \sigma^{x\lambda} \in K$. Αφού $H \subseteq K$ και έχουν την ίδια τάξη, συμπεραίνουμε ότι $H = K$.

□

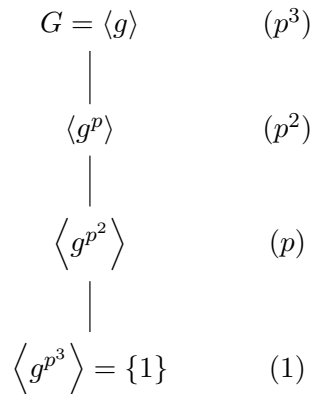
Πόρισμα 2. Αν μας δοθεί πεπερασμένη κυκλική $G = \langle g \rangle$ τάξης n , για κάθε $d|n$ με $d > 0$, τότε υπάρχει μοναδική H κυκλική υποομάδα της G με $H = \langle g^{n/d} \rangle$. Άρα, υποομάδα της G ίδιας τάξης ταυτίζονται.

Παράδειγμα 32. Δίνεται κυκλική $G = \langle g \rangle$ τάξης 40. Οι θετικοί διαιρέτες του 40 είναι οι

1, 2, 4, 5, 8, 10, 20, 40. Άρα, το διάγραμμα υποομάδων της G είναι το εξής



Παράδειγμα 33. Έστω Δίνεται κυκλική $G = \langle g \rangle$ τάξης p^3 , όπου p πρώτος. Οι θετικοί διαιρέτες του p^3 είναι οι $1, p, p^2, p^3$. Άρα, το διάγραμμα υποομάδων της G είναι το εξής



16 Ασκήσεις στις Ομάδες

Άσκηση 14. Έστω $G = \langle g \rangle$ κυκλική τάξης 120 και $H = \langle g^{636} \rangle$.

- (α) Βρείτε τον ελάχιστο θετικό ακέραιο m ώστε $g^m \in H$.
- (β) Βρείτε τους γεννήτορες της H .

Λύση. (α) Αρχικά εύκολα παρατηρούμε ότι $H = \langle g^{636} \rangle = \langle g^{36} \rangle$ και $o(g^{36}) = 120/(36, 120) = 12$. Συνεπώς, $|H| = 10$ και από το θεώρημα δομής κυκλικών ομάδων $H = \langle g^{120/10} \rangle = \langle g^{12} \rangle = \{1, g^{12}, g^{24}, \dots, g^{12 \cdot 9}\}$. Έτσι, το ζητούμενο m είναι το 12.

(β) Τα στοιχεία της H είναι της μορφής αν $h = g^{12}$ έχουμε ότι $H = \langle h \rangle$. Ένα h^k είναι γεννήτορας της H αν $H = \langle h^k \rangle$ αν $o(h^k) = o(h)/(o(h), k) = 10$ αν $(10, k) = 1$ με $0 \leq k \leq 9$. Άρα, $k = 1, 3, 5, 7, 9$ και οι ζητούμενοι γεννήτορες είναι οι h, h^3, h^5, h^9 . ■

Άσκηση 15. Έστω G κυκλική ομάδα τάξης $n^5 - n$, για $n > 1$. Δείξτε ότι υπάρχει υποομάδα της G τάξης 30.

Λύση. Από το θεώρημα δομής κυκλικών ομάδων, αρκεί να δείξουμε ότι $2 \cdot 3 \cdot 5 = 30 | n^5 - 5$, για κάθε $n > 1$. Αφού 2, 3, 5 είναι σχετικά πρώτοι, αρκεί να δείξουμε ότι $2 | n^5 - 5$, $3 | n^5 - 5$ και $5 | n^5 - 5$ το οποίο προκύπτει εφαρμόζοντας 3 φορές το Θεώρημα Fermat (για $p = 2, 3, 5$), το οποίο αφήνεται ως άσκηση. ■

Άσκηση 16. Δίνεται η μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 10 & 11 & 9 & 3 & 12 & 1 & 2 & 7 & 6 & 5 & 8 \end{pmatrix} \in S_{12}.$$

Συμβολίζουμε με $\langle x \rangle$ την κυκλική υποομάδα της S_{12} που παράγεται από τη $x \in S_{12}$.

(α) Δείξτε ότι $\langle \sigma^{2019} \rangle = \langle \sigma^{1821} \rangle$.

(β) Πόσους γεννήτορες έχει η $\langle \sigma \rangle$; Πόσοι από αυτούς είναι άρτιες μεταθέσεις;

(γ) Βρείτε τις υποομάδες τάξης 2 και 3 της $\langle \sigma \rangle$ και γράψτε τα στοιχεία τους ως γινόμενα ξένων κύκλων.

Λύση. (α) Έχουμε ότι $\sigma = (1497)(2 \ 10 \ 6 \ 12 \ 8)(3 \ 11 \ 5)$. Έτσι έχουμε ότι $o(\sigma) = \text{ε.κ.π.}(3, 4, 5) = 60$ με $o(\sigma^{1821}) = \frac{60}{(60, 1821)} = 20$ και όμοια $o(\sigma^{2019}) = \frac{60}{(60, 2019)} = 20$. Από θεώρημα δομής κυκλικών ομάδων, αφού $\langle \sigma^{2019} \rangle, \langle \sigma^{1821} \rangle$ είναι κυκλικές υποομάδες της $\langle \sigma \rangle$ ίδιας τάξης, τότε είναι ίσες.

(β) Έχουμε ότι $\langle \sigma \rangle = \{1, \sigma, \dots, \sigma^{59}\}$ και σ^k (με $0 \leq k \leq 59$) είναι γεννήτορας της $\langle \sigma \rangle$ αν και μόνο αν $\langle \sigma \rangle = \langle \sigma^k \rangle$ αν και μόνο αν $o(\sigma^k) = 60$ αν και μόνο αν $0 \leq k \leq 59$ και $(k, 60) = 1$. Άρα, έχουμε ότι το ζητούμενο πλήθος είναι $\varphi(60) = 8$. Τώρα, έχουμε ότι σ είναι περιττή (μπορεί να γραφτεί ως 9 αντιμεταθέσεις), άρα σ^k άρτια αν k είναι άρτιος. Όμως, σ^k είναι γεννήτορας αν $(k, 60)$ ειδικότερα αν k περιττός. Συνεπώς, κανέναν από τους γεννήτορες δεν είναι άρτια μετάθεση.

- (γ) Έστω H και K οι αντίστοιχες υποομάδες τάξεις 2 και 3. Από το θεώρημα δομής κυκλικών ομάδων έχουμε ότι $H = \langle \sigma^{60/2} \rangle = \langle \sigma^{30} \rangle = \{1, \sigma^{30}\}$ και όμοιας $K = \langle \sigma^{60/3} \rangle = \langle \sigma^{20} \rangle = \{1, \sigma^{20}, \sigma^{40}\}$. Ενδεικτικά θα γράψουμε ως γινόμενο ξένων κύκλων την σ^{20} . Έχουμε ότι

$$\begin{aligned}\sigma^{20} &= (1497)^{20} (2 \ 10 \ 6 \ 12 \ 8)^{20} (3 \ 11 \ 5)^{20} \\ &= [(1497)^4]^5 [(2 \ 10 \ 6 \ 12 \ 8)^5]^4 (3 \ 11 \ 5)^{18} (3 \ 11 \ 5)^2 \\ &= (3 \ 11 \ 5)(3 \ 11 \ 5) = (3 \ 5 \ 11)\end{aligned}$$

■

Άσκηση 17. Έστω $\sigma = (1 \ 2 \ 5 \ 7)(1 \ 2 \ 4 \ 6 \ 8) \in S_8$

- (α) Βρείτε μια παράσταση της σ^{10} ως γινόμενο κύκλων ξένων ανά δύο.
 (β) Βρείτε τον ελάχιστο θετικό ακέραιο n ώστε $\langle \sigma^{7n} \rangle = \langle \sigma^{100} \rangle$.
 (γ) Αληθεύει ότι υπάρχει $\tau \in S_8$ ώστε $\tau^{-1}\sigma\tau = \sigma^2$;

Λύση. (α) Έχουμε ότι $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 3 & 6 & 7 & 8 & 1 & 2 \end{pmatrix} = (1 \ 5 \ 7)(2 \ 4 \ 6 \ 8)$. Συνεπώς, έχουμε ότι

$$\sigma^{10} = (1 \ 5 \ 7)^{10} (2 \ 4 \ 6 \ 8)^{10} = (1 \ 5 \ 7)(2 \ 4 \ 6 \ 8)^2.$$

Συνεπώς, έχουμε ότι $\sigma^{10} = (1 \ 5 \ 7)(2 \ 6)(4 \ 8)$ γινόμενο ξένων κύκλων.

- (β) Αρχικά $o(\sigma) = \text{ε.κ.π.}(3, 4) = 12$, έτσι $o(\sigma^{100}) = 3$. Έχουμε ότι $\langle \sigma^{7n} \rangle = \langle \sigma^{100} \rangle$, από το θεώρημα δομής κυκλικών ομάδων, αν και μόνο αν $o(\sigma^{7n}) = |\langle \sigma^{7n} \rangle| = 3$. Ισοδύναμα ψάχνουμε n ώστε $(7n, 12) = 4$. Ο ελάχιστος τέτοιος n είναι $n = 4$.
 (γ) Είναι μια εύκολη άσκηση να δείξει κανείς ότι αν τ είναι γινόμενο k αντιμεταθέσεων, τότε τ^{-1} είναι επίσης γινόμενο k αντιμεταθέσεων. Αφού σ γράφεται ως γινόμενο 5 αντιμεταθέσεων, για κάθε $\tau \in S_8$, έχουμε ότι $\tau^{-1}\sigma\tau$ περιττή, ενώ σ^2 είναι άρτια. Άρα, δεν υπάρχει $\tau \in S_8$ ώστε $\tau^{-1}\sigma\tau = \sigma^2$.

■

Άσκηση 18. Θεωρούμε τη συμμετρική ομάδα S_n , όπου n περιττός ακέραιος με $n \geq 5$, το στοιχείο αυτής $\sigma = (1 \ 2 \ 3)(2 \ 3 \ \dots \ n)$ και την κυκλική υποομάδα $H = \langle \sigma \rangle$ της S_n .

- (α) Βρείτε την τάξη του σ (συναρτήσει του n) και εξετάστε αν η H έχει υποομάδα τάξης 4.
 (β) Δείξτε ότι $(1 \ 2) \in H$. Αληθεύει ότι $(1 \ 3) \in H$;

(γ) Δείξτε ότι δεν υπάρχει $\tau \in S_n$ με $\sigma = \tau^{2022}$.

Λύση. (α) Παρατηρούμε ότι

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots & n \\ 2 & 1 & 4 & 5 & 6 & \cdots & 3 \end{pmatrix} = (12)(3 \ 4 \ 5 \ \cdots \ n).$$

Το μήκος του κύκλου $(3 \ 4 \ 5 \ \cdots \ n)$ είναι $n - 2$ περιττός, αφού n περιττός, άρα $o(\sigma) = \text{ε.κ.π.}(2, n-2) = 2(n-2)$. Αν H είχε υποομάδα τάξης 4, από το θεώρημα Lagrange, θα έπρεπε $4|2(n-2)$, δηλαδή $2|n-2$, το οποίο δεν μπορεί να συμβαίνει αφού $n-2$ περιττός.

(β) Το $n-2$ είναι περιττός, άρα είναι της μορφής $n-2 = 2k+1 \geq 3$ ($n \geq 5$). Συνεπώς, $\sigma^{n-2} \in H$ και μάλιστα

$$\sigma^{n-2} = (12)^{n-2}(3 \ 4 \ 5 \ \cdots \ n)^{n-2} = (12) \in H.$$

Τώρα, αν $\sigma^m \in H$ έχουμε ότι $\sigma^m(1) \in \{1, 2\}$, συνεπώς $(13) \notin H$.

(γ) Παρατηρήστε ότι

$$\sigma = (1 \ 2)(3 \ n)(3 \ n-1) \cdots (3 \ 4).$$

δηλαδή είναι γινόμενο $n-2$ αντιμεταθέσεων, άρα είναι περιττή. Τώρα, αν $\tau \in S_n$, αυτή είναι ένα γινόμενο k αντιμεταθέσεων (το k εξαρτάται από την τ), συνεπώς τ^{2022} είναι γινόμενο $2022k$ αντιμεταθέσεων, δηλαδή τ^{2022} είναι άρτια. Επομένως, δεν υπάρχει $\tau \in S_n$, ώστε $\sigma = \tau^{2022}$. ■

Άσκηση 19. Θεωρούμε την μετάθεση $\sigma = (12)(345678) \in S_8$ και την κυκλική ομάδα $G = \langle \sigma \rangle$ που παράγεται από την σ .

(α) Περιέχει η G στοιχείο τάξεως 3 ;

(β) Η μετάθεση (178) ανήκει στην υποομάδα G ;

Λύση. (α) Έχουμε ότι $o(\sigma) = \text{ε.κ.π.}(2, 8) = 8$, άρα G είναι κυκλική τάξης 8. Αφού $3|8$, από το θεώρημα δομής κυκλικών ομάδων, υπάρχει μοναδική κυκλική υποομάδα H της G τάξης 3 και μάλιστα $H = \langle \sigma^{8/3} \rangle = \langle \sigma^2 \rangle$. Άρα, έχουμε ότι $o(\sigma^2) = |H| = 3$.

(β) Έχουμε ότι $\tau = (178) \in G$ αν και μόνο αν υπάρχει k ώστε $\tau = \sigma^k = (12)^k(345678)^k$. Όμως, για κάθε k έχουμε ότι $\sigma^k(1) \in \{1, 2\}$ ενώ $\tau(1) = 7$, άρα $(178) \notin G$. ■

Άσκηση 20. Έστω $\sigma = (1\ 2\ 5\ 7)(1\ 2\ 4\ 6\ 8) \in S_8$.

- (α) Βρείτε μια παράσταση της σ^{10} ως γινόμενο κύκλων ξένων ανά δύο.
- (β) Βρείτε τον ελάχιστο θετικό ακέραιο n ώστε $\langle \sigma^{7n} \rangle = \langle \sigma^{100} \rangle$.
- (γ) Αληθεύει ότι υπάρχει $\tau \in S_8$ ώστε $\tau^{-1}\sigma\tau = \sigma^2$;

Λύση. (α) Έχουμε ότι $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 4 & 3 & 6 & 7 & 8 & 1 & 2 \end{pmatrix} = (1\ 5\ 7)(2\ 4\ 6\ 8)$. Συνεπώς, έχουμε ότι

$$\sigma^{10} = (1\ 5\ 7)^{10}(2\ 4\ 6\ 8)^{10} = (1\ 5\ 7)(2\ 4\ 6\ 8)^2.$$

Συνεπώς, έχουμε ότι $\sigma^{10} = (1\ 5\ 7)(2\ 6)(4\ 8)$ γινόμενο ξένων κύκλων.

- (β) Αρχικά έχουμε ότι $o(\sigma) = \text{ε.κ.π.}(3, 4) = 12$. Συνεπώς, ισχύει ότι $o(\sigma^{100}) = 3$. Έχουμε ότι $\langle \sigma^{7n} \rangle = \langle \sigma^{100} \rangle$, από το θεώρημα δομής κυκλικών ομάδων, αν και μόνο αν $o(\sigma^{7n}) = |\langle \sigma^{7n} \rangle| = 3$. Ισοδύναμα ψάχνουμε n ώστε $(7n, 12) = 4$. Ο ελάχιστος τέτοιος n είναι $n = 4$.
- (γ) Είναι μια εύκολη άσκηση να δείξει κανείς ότι αν τ είναι γινόμενο k αντιμεταθέσεων, τότε τ^{-1} είναι επίσης γινόμενο k αντιμεταθέσεων. Αφού σ γράφεται ως γινόμενο 5 αντιμεταθέσεων, για κάθε $\tau \in S_8$, έχουμε ότι $\tau^{-1}\sigma\tau$ περιττή, ενώ σ^2 είναι άρτια. Άρα, δεν υπάρχει $\tau \in S_8$ ώστε $\tau^{-1}\sigma\tau = \sigma^2$. ■

Άσκηση 21. Θεωρούμε τις μεταθέσεις $\sigma, \tau \in S_9$ με

$$\sigma = (1\ 4\ 9\ 3\ 8\ 6)(2\ 7\ 5) \quad \text{και} \quad \tau = (1\ 7\ 4\ 9)(2\ 6)(3\ 8\ 5).$$

Επίσης θεωρούμε τις ομάδες $G = \langle \sigma \rangle$ και $H = \langle \tau \rangle$.

- (α) Να εξετάσετε αν οι ομάδες G και H είναι ισόμορφες.
- (β) Για ποιους πρώτους αριθμούς p είναι η μετάθεση σ^p γεννήτορας της ομάδας G ;

Λύση. (α) Παρατηρήστε ότι $|G| = o(\sigma) = \text{ε.κ.π.}(3, 6) = 6$ και $|H| = o(\tau) = \text{ε.κ.π.}(2, 3, 4) = 12$. Εφόσον G, H είναι πεπερασμένες κυκλικές διαφορετικής τάξης, από το θεώρημα ταξινόμησης κυκλικών ομάδων, δεν είναι ισόμορφες.

- (β) Έχουμε ότι σ^p είναι γεννήτορας της G αν και μόνο αν $G = \langle \sigma^p \rangle$ αν και μόνο αν $|G| = o(\sigma^p)$ αν και μόνο αν $o(\sigma^p) = \frac{6}{(p, 6)} = 6$. Για κάθε p πρώτο με $p \neq 2, 3$ έχουμε ότι σ^p είναι γεννήτορας της G . ■

Άσκηση 22. Έστω $\sigma = (1\ 6\ 2\ 3) \in S_6$.

- (α) Αν $\varphi: S_6 \rightarrow \mathbb{Z}_9$ ομομορφισμός ομάδων, δείξτε ότι $\sigma \in \ker \varphi$.
- (β) Βρείτε την τάξη της ομάδας $\langle \sigma^{2010} \rangle \cap \langle \sigma^{2011} \rangle$.
- (γ) Εξετάσθε αν υπάρχει $\tau \in S_6$ τέτοια ώστε $\sigma = \tau^4$.

Λύση. (α) Θέλουμε να δείξουμε ότι $\sigma \in \ker \varphi$, ισοδύναμα $\varphi(\sigma) = [0]$, δηλαδή $o(\varphi(\sigma)) = 1$.
Αφού $o(\sigma) = 4$, τότε $\sigma^4 = 1$, συνεπώς $(\varphi(\sigma))^4 = 1$. Επομένως, έχουμε ότι $o(\varphi(\sigma)) | 4$.
Επιπλέον, $o(\varphi(\sigma)) | 9 = |\mathbb{Z}_9|$, άρα $o(\varphi(\sigma)) | (4, 9) = 1$.

(β) Αφού $o(\sigma^{2010}) = 2$, τότε, από το θεώρημα δομής κυκλικών ομάδων, $\langle \sigma^{2010} \rangle = \langle \sigma^2 \rangle$ και ομοίως δείχνουμε ότι $\langle \sigma^{2011} \rangle = \langle \sigma \rangle$. Άρα, η δοσμένη τομή είναι η $\langle \sigma^2 \rangle \cap \langle \sigma \rangle = \langle \sigma^2 \rangle$, η οποία έχει τάξη 2.

(γ) Έχουμε ότι σ είναι περιττή (γιατί ;), ενώ για κάθε $\tau \in S_6$ έχουμε ότι τ^4 άρτια. Συνεπώς, δεν μπορεί να υπάρχει τέτοια τ ώστε $\sigma = \tau^4$.

■