ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΪΚΑ ΜΑΘΗΜΑΤΑ

Τίτλος Μαθήματος: Αλγεβρικές Δομές Ι

Ενότητα: Ομάδες μεταθέσεων (μετατάξεων)

Διδάσκων: Καθηγητής Νικόλαος Μαρμαρίδης, Καθηγητής Ιωάννης Μπεληγιάννης

Τμήμα: Μαθηματικών

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

7. **Ομάδες μεταθέσεων (μετατάξεων)**

7.1. **Οι πρώτες έννοιες.** Ας είναι A ένα μη κενό σύνολο και S_A το σύνολο των «ένα προς ένα» και «επί» απεικονίσεων από το σύνολο A στον εαυτό του.

Πρόταση 7.1. *Το σύνολο S_A μαζί με την πράξη της σύνθεσης απεικονίσεων*

$$\circ : S_A \times S_A \to S_A, (\sigma, \tau) \quad \mapsto \quad \sigma \circ \tau$$

αποτελεί μια ομάδα.

Απόδειξη. Επειδή το $A \neq \emptyset$, ορίζεται η ταυτοτική απεικόνιση:

$$\mathrm{Id}_A \to A, a \quad \mapsto \mathrm{Id}_A(a) := a,$$

η οποία ως «ένα προς ένα» και «επί» απεικόνιση ανήκει στο S_A.

Η σύνθεση απεικονίσεων ορίζει μια πράξη επί του S_A, αφού η σύνθεση δύο «ένα προς ένα» και «επί» απεικονίσεων είναι επίσης μια «ένα προς ένα» και «επί» απεικόνιση. Επίσης είναι γνωστό ότι η σύνθεση απεικονίσεων είναι προσεταιριστική.

Η ταυτοτική απεικόνιση Id_A έχει την ιδιότητα

$$\forall \sigma \in S_A, \quad \mathrm{Id}_A \circ \sigma = \sigma = \sigma \circ \mathrm{Id}_A$$

και γι' αυτό είναι το ταυτοτικό στοιχείο της υποψήφιας ομάδας $(S_A, \circ)$.
Τέλος για κάθε $\sigma \in S_A$, δηλαδή για κάθε απεικόνιση $\sigma : A \to A$ που είναι «ένα προς ένα» και «επί», ορίζεται απεικόνιση

$$\tau : A \to A, \quad a \mapsto b, \quad \text{όπου } b \text{ είναι εκείνο το στοιχείο του } A \text{ με } \sigma(b) = a.$$

(Υπενθυμίζουμε ότι για κάθε $a \in A$, υπάρχει πάντοτε ένα τέτοιο b με $\sigma(b) = a$, επειδή η σ είναι «επί» και κάθε τέτοιο b είναι μοναδικό επειδή η σ είναι «ένα προς ένα».)
Τώρα, για κάθε $b \in A$ είναι $\tau \circ \sigma(b) = b$ και επίσης για κάθε $a \in A$ είναι $\sigma \circ \tau(a) = a$. Επομένως,

$$\tau \circ \sigma = \mathrm{Id}_A \text{ και } \sigma \circ \tau = \mathrm{Id}_A.$$

Ώστε η απεικόνιση τ είναι το αντίστροφο[23] του στοιχείου σ στο σύνολο S_A και γι' αυτό το ζεύγος $A, \circ$ είναι μια ομάδα. ☐

Ορισμός 7.2. *Η ομάδα $(S_A, \circ)$ ονομάζεται η συμμετρική ομάδα του συνόλου A.*

Όταν το A έχει πεπερασμένο το πλήθος στοιχεία, ας πούμε ότι $\mid A \mid = n$, και επειδή το είδος των στοιχείων του A δεν έχει κανένα ουσιαστικό ρόλο στην κατασκευή της S_A, τότε δεχόμαστε ότι το σύνολο A έχει ως στοιχεία τους φυσικούς αριθμους $1, 2, \ldots, n$, δηλαδή ότι $A = \{1, 2, \ldots, n\}$, ονομάζουμε την ομάδα $(S_A, \circ)$ *συμμετρική ομάδα στα n στοιχεία* και τη συμβολίζουμε με $(S_n, \circ)$ ή απλώς S_n. Επιπλέον, ονομάζουμε τα στοιχεία της S_n *μεταθέσεις* ή *μετατάξεις*. Τέλος, παριστάνουμε με Id_n το ταυτοτικό στοιχείο της S_n.

Παρατήρηση 7.3. *Έστω ότι A είναι ένα **πεπερασμένο** σύνολο με n στοιχεία και ότι $\sigma : A \to A$ είναι μια απεικόνιση. Από τη Στοιχειώδη Θεωρία Συνόλων είναι γνωστό ότι τα επόμενα είναι ισοδύναμα:*

(1) *Η σ είναι μια «ένα προς ένα» απεικόνιση.*
(2) *Η σ είναι μια «ένα προς ένα» και «επί» απεικόνιση.*
(3) *Η σ είναι μια «επί» απεικόνιση.*

[23] Προσέξτε ότι όπως κατασκευάστηκε η $\tau = \sigma^{-1}$, είναι η απεικόνιση που είναι η αντίστροφη της σ όπως τη γνωρίζουμε απο τη Θεωρία Συνόλων και ταυτοχρόνως είναι το αντίστροφο στοιχείο της σ όπως αυτό ορίζεται στη Θεωρία Ομάδων.

Λήμμα 7.4. *Το πλήθος των στοιχείων της ομάδας $(S_n, \circ)$ ισούται με $n!$*

Απόδειξη. Ας είναι σ ένα στοιχείο της S_n. Η απεικόνιση σ προσδιορίζεται πλήρως από τις τιμές

$$\sigma(1), \sigma(2), \ldots, \sigma(i), \sigma(i+1), \ldots, \sigma(n).$$

Το στοιχείο $\sigma(1)$ μπορεί να πάρει οποιαδήποτε τιμή από το σύνολο $\{1, 2, \ldots, n\}$. Συνεπώς, για το $\sigma(1)$ υπάρχουν n το πλήθος επιλογές. Το στοιχείο $\sigma(2)$ μπορεί να πάρει οποιαδήποτε τιμή από το σύνολο $\{1, 2, \ldots, n\} \setminus \{\sigma(1)\}$, αφού η σ είναι μια «ένα προς ένα» απεικόνιση. Συνεπώς, για το $\sigma(2)$ υπάρχουν $(n-1)$ το πλήθος επιλογές. Τώρα, το στοιχείο $\sigma(3)$ μπορεί να πάρει οποιαδήποτε τιμή από το σύνολο $\{1, 2, \ldots, n\} \setminus \{\sigma(1), \sigma(2)\}$. Συνεπώς, για το $\sigma(2)$ υπάρχουν $(n-2)$ το πλήθος επιλογές. Συνεχίζοντας με τον τρόπο αυτό διαπιστώνουμε ότι για το στοιχείο $\sigma(i+1)$ υπάρχουν $(n-i)$ επιλογές, αφού το $\sigma(i+1)$ μπορεί να είναι οποιοδήποτε στοιχείο από το σύνολο $\{1, 2, \ldots, n\} \setminus \{\sigma(1), \sigma(2), \ldots, \sigma(i)\}$. Γι' αυτό το πλήθος των στοιχείων της S_n ισούται με $n \cdot (n-1) \cdot \ldots \cdot (n-i) \cdot \ldots \cdot 2 \cdot 1 = n!$ $\square$

Όπως παρατηρήσαμε στο προηγούμενο λήμμα, κάθε στοιχείο σ της $S_n, \circ$, δηλαδή κάθε μετάθεση (μετάταξη) περιγράφεται πλήρως από τις τιμές

$$\sigma(1),\ \ \sigma(2),\ \ \ldots, \sigma(i),\ \ \sigma(i+1),\ \ \ldots, \sigma(n-1),\ \ \sigma(n).$$

Έτσι ένας τρόπος για να παραστήσουμε μια $\sigma \in S_n$ είναι ο εξής:

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & i & i+1 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(i) & \sigma(i+1) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}$$

όπου στην πρώτη γραμμή του προηγούμενου σχήματος βρίσκονται τα στοιχεία του συνόλου A, δηλαδή τα $1, 2, \ldots, i, i+1, \ldots, n-1, n$ και στη δεύτερη γραμμή βρίσκονται οι αντίστοιχες εικόνες τους $\sigma(1), \sigma(2), \ldots, \sigma(i), \sigma(i+1), \ldots, \sigma(n-1), \sigma(n)$

Έτσι λοιπόν γράφοντας

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

δηλώνουμε τη μετάθεση σ της S_9, η οποία απεικονίζει τα στοιχεία του $A = \{1, 2, \ldots, 9\}$ ως εξής:

$$\begin{aligned} &1 \mapsto \sigma(1) = 9, \quad 2 \mapsto \sigma(2) = 3, \quad 3 \mapsto \sigma(3) = 2, \quad 4 \mapsto \sigma(4) = 5, \quad 5 \mapsto \sigma(5) = 7, \\ &6 \mapsto \sigma(6) = 6, \quad 7 \mapsto \sigma(7) = 1, \quad 8 \mapsto \sigma(8) = 4, \quad 9 \mapsto \sigma(9) = 8. \end{aligned}$$

Αν τώρα

$$\tau = \begin{pmatrix} 1 & 2 & \ldots & i & i+1 & \ldots & n-1 & n \\ \tau(1) & \tau(2) & \ldots & \tau(i) & \tau(i+1) & \ldots & \tau(n-1) & \tau(n) \end{pmatrix}$$

είναι ακόμα ένα στοιχείο της S_n, τότε η σύνθεση $\sigma \circ \tau$ ισούται με

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & \ldots & i & i+1 & \ldots & n-1 & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \ldots & \sigma(\tau(i)) & \sigma(\tau(i+1)) & \ldots & \sigma(\tau(n-1)) & \sigma(\tau(n)) \end{pmatrix}$$

Για παράδειγμα, αν τ είναι η μετάθεση της S_9:

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

τότε

$$\begin{aligned} \sigma \circ \tau &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \sigma(\tau(3)) & \sigma(\tau(4)) & \sigma(\tau(5)) & \sigma(\tau(6)) & \sigma(\tau(7)) & \sigma(\tau(8)) & \sigma(\tau(9)) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ \sigma(8) & \sigma(3) & \sigma(2) & \sigma(1) & \sigma(4) & \sigma(5) & \sigma(6) & \sigma(9) & \sigma(7) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 3 & 9 & 5 & 7 & 6 & 8 & 1 \end{pmatrix} \end{aligned}$$

και

$$\tau\circ\sigma=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\ \tau(\sigma(1))&\tau(\sigma(2))&\tau(\sigma(3))&\tau(\sigma(4))&\tau(\sigma(5))&\tau(\sigma(6))&\tau(\sigma(7))&\tau(\sigma(8))&\tau(\sigma(9))\end{pmatrix}$$
$$=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\ \tau(9)&\tau(3)&\tau(2)&\tau(5)&\tau(7)&\tau(6)&\tau(1)&\tau(4)&\tau(8)\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\ 7&2&3&4&6&5&8&1&9\end{pmatrix}$$

Παράδειγμα 7.5. ***Η συμμετρική ομάδα*** $(\mathbf{S_4},\circ)$ ***του συνόλου*** $\mathbf{A}=\{\mathbf{1},\mathbf{2},\mathbf{3},\mathbf{4}\}$.
Η S_4 αποτελείται τις «ένα προς ένα» και «επί» απεικονίσεις από το σύνολο A στον εαυτό του και η τάξη της $\circ(S_4)$ ισούται με $4!=24$.
Γράφουμε τα στοιχεία της S_4 χρησιμοποιώντας τη σημειογραφία που είδαμε προηγουμένως:

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

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

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

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

Ας εφαρμόσουμε την πράξη τής ομάδας, που εδώ είναι η σύνθεση των απεικονίσεων, πάνω σε κάποια ζεύγη στοιχείων:
Για να υπολογίσουμε τη σύνθεση $\tau_5\circ\sigma_2$ οφείλουμε να λογαριάσουμε τις τιμές της πάνω στα στοιχεία[24] *$1,2,3,4$ τού A. Έχουμε:*

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

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

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

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

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

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

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

Παρατηρούμε ότι αφού το στοιχείο σ_2^{-1} *είναι η αντίστροφη απεικόνιση τής* σ_2 *και αφού* $\sigma_2(1) = 1$, *θα πρέπει να ισχύει* $\sigma_2^{-1}(1) = 1$. *Ανάλογα, αφού* $\sigma_2(2) = 3$, *θα πρέπει να ισχύει* $\sigma_2^{-1}(3) = 2$, *αφού* $\sigma_2(3) = 4$, *θα πρέπει να ισχύει* $\sigma_2^{-1}(4) = 3$ *και τέλος αφού αφού* $\sigma_2(4) = 2$, *θα πρέπει να ισχύει* $\sigma_2^{-1}(2) = 4$. *Επομένως, το στοιχείο* σ_2^{-1} *ισούται με το στοιχείο* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$, *δηλαδή με το* $\sigma_2^{-1} = \sigma_1$.

Εργαζόμενοι με τον ίδιο τρόπο βλέπουμε ότι $\tau_5^{-1}(1) = 3$, $\tau_5^{-1}(2) = 2$, $\tau_5^{-1}(3) = 1$ *και* $\tau_5^{-1}(4) = 4$. *Επομένως, το στοιχείο* τ_5^{-1} *ισούται με το στοιχείο* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$, *δηλαδή με τον εαυτό του* τ_5*!* [25]

7.2. **Τροχιές και ανάλυση σε κύκλους.** Αρχίζουμε με το ακόλουθο:

Λήμμα 7.6. *Ας είναι* $\sigma \in S_n$ *μια μετάθεση (μετάταξη) του συνόλου* $A = \{1, 2, \ldots, n\}$ *και* ϕ_σ *το υποσύνολο του* $A \times A$ *που ορίζεται ως*

$$(a, b) \in \phi_\sigma \Longleftrightarrow \exists z \in \mathbb{Z}, \text{ με } \sigma^z(a) = b.$$

Η σχέση ϕ_σ *είναι μια σχέση ισοδυναμίας επί του συνόλου* A.

Απόδειξη. Πράγματι, $\forall a \in A$ είναι[26] $a\phi_\sigma a$, αφού $\sigma^0(a) = a$. Ώστε το σύνολο ϕ_σ διαθέτει την ανακλαστική ιδιότητα.

Αν $a, b \in A$ με $a\phi_\sigma b$, τότε $\exists z \in \mathbb{Z}$ με $\sigma^z(a) = b$. Συνεπώς, $\sigma^{-z}(b) = a$ και γι' αυτό $b\phi_\sigma a$. Ώστε το σύνολο ϕ_σ διαθέτει τη συμμετρική ιδιότητα.

Αν $a, b, c \in A$ με $a\phi_\sigma b$ και $b\phi_\sigma c$, τότε $\exists z_1, z_2 \in \mathbb{Z}$ με $\sigma^{z_1}(a) = b$ και $\sigma^{z_2}(b) = c$. Συνεπώς, $\sigma^{z_2+z_1}(a) = \sigma^{z_2} \circ \sigma^{z_1}(a) = \sigma^{z_2}(b) = c$ και γι' αυτό $a\phi_\sigma c$. Ώστε το σύνολο ϕ_σ διαθέτει τη μεταβατική ιδιότητα.

Επειδή λοιπόν ικανοποιούνται οι ανωτέρω τρεις ιδιότητες το ϕ_σ είναι μια σχέση ισοδυναμίας επί του συνόλου A. $\square$

Τώρα το σύνολο A διαμερίζεται στις κλάσεις ισοδυναμίας της ϕ_σ.

Ορισμός 7.7. *Ονομάζουμε* σ*-τροχιά του στοιχείου* $a \in A$ *την κλάση ισοδυναμίας του* a *ως προς τη σχέση ισοδυναμίας* ϕ_σ.

Συνήθως, η σ*-τροχιά* του στοιχείου $a \in A$ συμβολίζεται με $\mathcal{O}_{\sigma,a}$.

Παράδειγμα 7.8. *Θα προσδιορίσουμε τις τροχιές των στοιχείων του* $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ *για κάθε μια από τις επόμενες μεταθέσεις (μετατάξεις):*

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

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

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

[26] Όταν θέλουμε να δηλώσουμε ότι ένα ζεύγος $(a, b) \in A \times A$ ανήκει σε ένα υποσύνολο $\phi \subseteq A$, τότε γράφουμε $a\phi b$.

Παρατηρούμε ότι

$$1 \xrightarrow{\sigma} 9 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 1, \;\; 2 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 2, \;\; 6 \xrightarrow{\sigma} 6$$

Γι' αυτό η σ διαθέτει τρεις τροχιές τις:

$$\mathcal{O}_{\sigma,1} = \{1,9,8,4,5,7\}, \quad \mathcal{O}_{\sigma,2} = \{2,3\}, \quad \textit{και} \;\; \mathcal{O}_{\sigma,6} = \{6\}.$$

Παρατηρούμε ότι

$$1 \xrightarrow{\tau} 8 \xrightarrow{\tau} 9 \xrightarrow{\tau} 7 \xrightarrow{\tau} 6 \xrightarrow{\tau} 5 \xrightarrow{\tau} 4 \xrightarrow{\tau} 1, \;\; 2 \xrightarrow{\tau} 3 \xrightarrow{\tau} 2.$$

Γι' αυτό η τ διαθέτει δύο τροχιές τις:

$$\mathcal{O}_{\tau,1} = \{1,8,9,7,6,5,4\}, \quad \textit{και} \;\; \mathcal{O}_{\tau,2} = \{2,3\}.$$

Παρατηρούμε ότι

$$1 \xrightarrow{\rho} 9 \xrightarrow{\rho} 1, \;\; 2 \xrightarrow{\rho} 3 \xrightarrow{\rho} 2, \;\; 4 \xrightarrow{\rho} 4, \;\; 5 \xrightarrow{\rho} 5, \;\; 6 \xrightarrow{\rho} 6, \;\; 7 \xrightarrow{\rho} 7, \;\; 8 \xrightarrow{\rho} 8.$$

Γι' αυτό η ρ διαθέτει επτά τροχιές τις:

$$\mathcal{O}_{\rho,1} = \{1,9\}, \;\; \mathcal{O}_{\rho,2} = \{2,3\}, \;\; \mathcal{O}_{\rho,4} = \{4\}, \;\; \mathcal{O}_{\rho,5} = \{5\}, \;\; \mathcal{O}_{\rho,6} = \{6\}, \;\; \mathcal{O}_{\rho,7} = \{7\} \;\textit{και}\; \mathcal{O}_{\rho,8} = \{8\}.$$

Παρατήρηση 7.9. *Έστω ότι $\sigma \in S_n$, ότι $a \in A$ και ότι $\mathcal{O}_{\sigma,a} = \{\sigma^z(a) \mid z \in \mathbb{Z}\}$ είναι η σ-τροχιά του a. Επειδή $\mathcal{O}_{\sigma,a} \subseteq A$ και επειδή $\mid A \mid = n$, έπεται ότι το πλήθος των στοιχείων της $\mathcal{O}_{\sigma,a}$ είναι πεπερασμένο. Έτσι συμπεραίνουμε ότι δεν είναι δυνατόν όλες οι ακέραιες δυνάμεις $\sigma^z(a)$ να είναι διαφορετικές μεταξύ τους, αφού τότε το πλήθος των στοιχείων της $\mathcal{O}_{\sigma,a}$ θα ήταν άπειρο. Γι' αυτό υπάρχουν $z_1, z_2 \in \mathbb{Z}$ με $z_1 \neq z_2$, ας πούμε $z_1 > z_2$ και $\sigma^{z_1}(a) = \sigma^{z_2}(a)$. Επομένως, $\sigma^{z_1 - z_2}(a) = a$ με $z_1 - z_2 \in \mathbb{N}$. Έτσι συμπεραίνουμε ότι το σύνολο*

$$\mathcal{M}(\sigma, a) = \{m \in \mathbb{N} \mid \sigma^m(a) = a\}$$

είναι διαφορετικό από το κενό σύνολο και γι' αυτό διαθέτει ένα ελάχιστο στοιχείο $s := \min \mathcal{M}(\sigma, a)$.

Ώστε το s είναι ο ελάχιστος φυσικός αριθμός με $\sigma^s(a) = a$.

Ισχυριζόμαστε ότι

$$\mathcal{O}_{\sigma,a} = \{a, \sigma(a), \sigma^2(a), \ldots, \sigma^i(a), \sigma^{i+1}(a), \ldots, \sigma^{s-1}(a)\}.$$

Πράγματι, τα $\sigma^i(a), 0 \leq i \leq s-1$ είναι ανά δύο διαφορετικά, αφού αν, $\sigma^i(a) = \sigma^j(a), 0 \leq i, j \leq s-1$ με $i \neq j$, ας πούμε $i > j$, τότε $\sigma^{(i-j)}(a) = a$. Αυτό όμως αντίκειται στο ότι το s είναι το ελάχιστο του $\mathcal{M}(\sigma, a)$, αφού $i - j \in \mathbb{N}$, $i - j < s$ και $\sigma^{(i-j)}(a) = a$.

Επιπλέον, κάθε στοιχείο $\sigma^z(a) \in \mathcal{O}_{\sigma,a}$ ισούται με κάποιο από τα $\sigma^i(a), 0 \leq i \leq s-1$, αφού εκτελώντας την ευκλείδεια διαίρεση του z δια s έχουμε $z = \lambda s + \upsilon$, όπου $\upsilon = 0, 1, \ldots, s-1$ και γι' αυτό

$$\sigma^z(a) = \sigma^{(\lambda s + \upsilon)}(a) = \sigma^{\upsilon}(\sigma^{\lambda s}(a)) = \sigma^{\upsilon}(a)$$

Αφού $\forall \lambda \in \mathbb{Z}$, το $\sigma^{\lambda s}(a) = a$, όπως διαπιστώνουμε αμέσως παρακάτω:

Για $\lambda = 0$, $\sigma^{\lambda s}(a) = \sigma^0(a) = \mathrm{Id}_n(a) = a$

Για $\lambda > 0$ είναι

$$\sigma^{\lambda s}(a) = \underbrace{\sigma^n \circ \sigma^s \circ \cdots \circ \sigma^s}_{\lambda\text{ -φορές}}(a) = a, \quad \textit{αφού} \;\; \sigma^s(a) = a$$

και για $\lambda < 0$ είναι

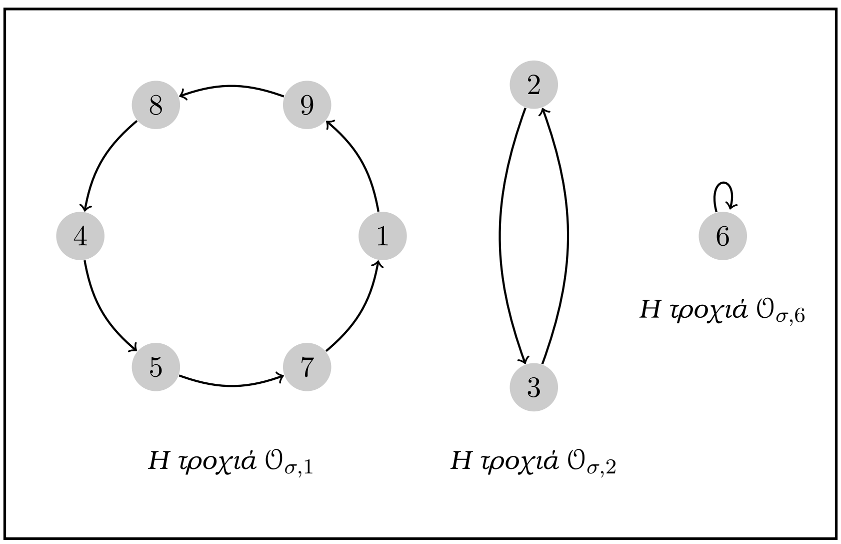
$$\sigma^{\lambda s}(a) = \underbrace{\sigma^{(-s)} \circ \sigma^{(-s)} \circ \cdots \circ \sigma^{(-s)}}_{|\lambda|\text{ -φορές}}(a) = a, \quad \textit{αφού} \;\; \sigma^{(-s)}(a) = a,$$

επειδή όταν $\sigma^s(a) = a$, τότε και $\sigma^{(-s)}(a) = a$.

Παρατηρούμε ότι κάθε τροχιά $\mathcal{O}_{\sigma,a}$ μιας μετάθεσης (μετάταξης) σ μπορεί να αναπαρασταθεί με τη βοήθεια ενός προσανατολισμένου γραφήματος. Το γράφημα αυτό αποτελείται από κορυφές και προσανατολισμένες ακμές[27]. Κορυφές του γραφήματος είναι τα στοιχεία της τροχιάς $\mathcal{O}_{\sigma,a}$. Υπάρχει μια προσανατολισμένη ακμή με αρχή την κορυφή i και τέλος την κορυφή j, ακριβώς όταν $j = \sigma(i)$.

Σύμφωνα με την αμέσως προηγούμενη παρατήρησή μας οι κορυφές του γραφήματος της τροχιάς $\mathcal{O}_{\sigma,a}$ είναι τα $a, \sigma(a), \sigma^{n-1}(a)$. Κάθε κορυφή $\sigma^i(a)$ συνδέεται με μια προσανατολισμένη ακμή με την κορυφή $\sigma^{i+1}(a)$, όταν $0 \leq i \leq \ n-2$ και επιπλέον η κορυφή $\sigma^{(n-1)}(a)$ συνδέεται με την κορυφή $\sigma^n(a) = a$. Συνεπώς, το γράφημα είναι κυκλικό.

Παράδειγμα 7.10. *Ας δούμε τα γραφήματα των τροχιών των μεταθέσεων σ, τ και ρ του Παραδείγματος 7.8.*



Σχήμα 4. Τα γραφήματα των τροχιών του σ, Παράδειγμα 7.8

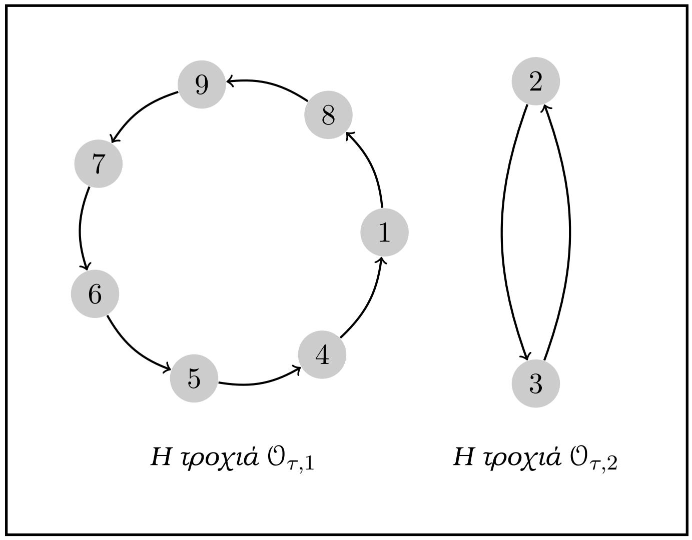
Ορισμός 7.11. *Μια μετάθεση (μετάταξη) της $(S_n, \circ)$ ονομάζεται κύκλος της S_n, αν διαθέτει **το πολύ** μια τροχιά με περισσότερα του ενός στοιχεία.*

Ορισμός 7.12. *Μήκος ενός κύκλου ονομάζουμε το πλήθος των στοιχείων εκείνης της τροχιάς του, που έχει το μεγαλύτερο πλήθος στοιχείων.*

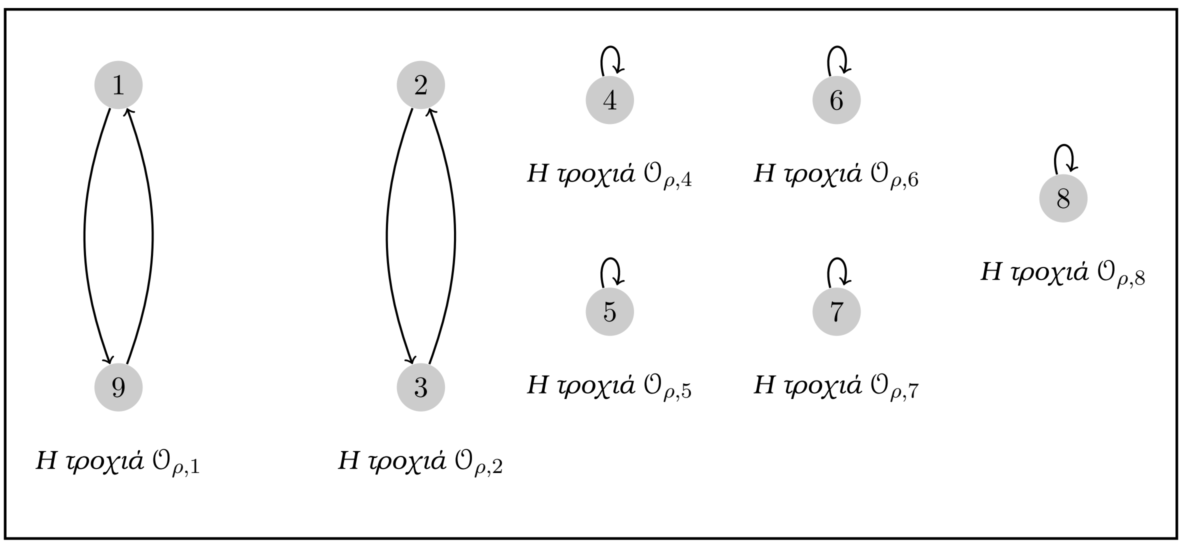
Για παράδειγμα η μετάθεση

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 1 \end{pmatrix} \in S_8$$

[27]Δηλαδή, τμήματα γραμμών που το ένα σημείο τους θεωρείται η αρχή και το άλλο το τέλος.



Σχήμα 5. Τα γραφήματα των τροχιών του τ, Παράδειγμα 7.8



Σχήμα 6. Τα γραφήματα των τροχιών του ρ, Παράδειγμα 7.8

είναι ένας κύκλος της S_8 αφού $\mathcal{O}_{\mu,1} = \{1,2,3,4,5,6,7,8\}$. Το μήκος του μ είναι 8.
Αλλά και η

$$\nu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 8 & 2 & 4 & 5 & 6 & 7 & 3 \end{pmatrix} \in S_8$$

είναι επίσης ένας κύκλος της S_8 αφού $\mathcal{O}_{\nu,1} = \{1\}$, $\mathcal{O}_{\nu,2} = \{2,8,3\}$, $\mathcal{O}_{\nu,4} = \{4\}$, $\mathcal{O}_{\nu,5} = \{5\}$, $\mathcal{O}_{\nu,6} = \{6\}$ και $\mathcal{O}_{\nu,7} = \{7\}$. Το μήκος του ν είναι 3.
Αντίθετα, η μετάθεση

$$\xi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 5 & 6 & 7 & 8 \end{pmatrix} \in S_8$$

δεν είναι ένας κύκλος της S_8, αφού έχει περισσότερες από μία τροχιές με περισσότερα του ενός στοιχεία. Πράγματι, $\mathcal{O}_{\xi,1} = \{1,2\}$ και $\mathcal{O}_{\xi,3} = \{3,4\}$. Εδώ δεν ορίζεται το μήκος της ξ, αφού η ξ δεν είναι κύκλος.

Παρατήρηση 7.13. (1) *Το ταυτοτικό στοιχείο της S_n, δηλαδή το*

$$\mathrm{Id}_n = \begin{pmatrix} 1 & 2 & \dots & i & i+1 & \dots & n \\ 1 & 2 & \dots & i & i+1 & \dots & n \end{pmatrix}$$

είναι ένας κύκλος αφού κάθε τροχιά του αποτελείται από ακριβώς ένα στοιχείο. Αλλά και αντίστροφα αν, κάθε τροχιά μιας μεταθεσης $\sigma \in S_n$ αποτελείται από ακριβώς ένα στοιχείο, τότε η σ ισούται με το Id_n.

(2) *Αν μια μετάθεση $\sigma \in S_n$ είναι ένας κύκλος, ο οποίος δεν ισούται με το ταυτοτικό στοιχείο Id_n, τότε υπάρχει κάποιο $a \in A = \{1, 2, \dots, n\}$ με $\sigma(a) \neq a$. Γι' αυτό ο σ διαθέτει ακριβώς μια τροχιά, την $\mathcal{O}_{\sigma,a}$, η οποία αποτελείται από περισσότερα του ενός στοιχεία και μάλιστα*

$$\mathcal{O}_{\sigma,a} = \{a, \sigma(a), \sigma^2(a), \dots, \sigma^i(a), \sigma^{i+1}(a), \dots, \sigma^{s-1}(a)\},$$

όπου, σύμφωνα με την Παρατήρηση 7.9, ο s είναι ο μικρότερος φυσικός με $\sigma^s(a) = a$.

Συνεπώς,

Το μήκος ενός κύκλου $\sigma \neq \mathrm{Id}_n$ ισούται με τον μικρότερο φυσικό s με $\sigma^s(a) = a$, όπου a είναι ένα οποιοδήποτε στοιχείο της τροχιάς του σ που έχει περισσότερα από ένα στοιχεία.

Χαρη σε αυτήν την παρατήρηση μπορούμε να παραστήσουμε έναν κύκλο σ που διαθέτει μια τροχιά με περισσότερα από ένα στοιχεία, ας πούμε την

$$\mathcal{O}_{\sigma,a} = \{a, \sigma(a), \sigma^2(a), \dots, \sigma^i(a), \sigma^{i+1}(a), \dots, \sigma^{s-1}(a)\}, s \geq 2, \text{ για κάποιο } a \in A = \{1, 2, \dots, n\}$$

ως εξής:

$$\sigma = \begin{pmatrix} a & \sigma(a) & \sigma^2(a) & \dots & \sigma^i(a) & \sigma^{i+1}(a) & \dots & \sigma^{s-1}(a) \end{pmatrix},$$

ερμηνεύοντας την ανωτέρω σημειογραφία κατά τον εξής τρόπο:

Έστω $x \in A = \{1, 2, \dots, n\}$, τότε

$$\sigma(x) = \begin{cases} x, & \text{αν } x \neq \sigma^i(a), 1 \leq i \leq s-1, \text{ δηλαδή όταν } x \notin \mathcal{O}_{\sigma,a} \\ \sigma^{i+1}(a), & \text{αν } x = \sigma^i(a), 1 \leq i \leq s-2 \\ a, & \text{αν } x = \sigma^{s-1}(a) \end{cases} \tag{*}$$

Παράδειγμα 7.14. (1) *Θεωρούμε τη μετάθεση*

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

Η σ είναι κύκλος, αφού έχει ακριβώς μια τροχιά με περισσότερα του ενός στοιχεία, πρόκειται για την τροχιά

$$\mathcal{O}_{\sigma,2} = \{2, \sigma^1(2) = 4, \sigma^2(2) = 6, \sigma^3(2) = 8, \sigma^4(2) = 10, \sigma^5(2) = 12\}$$

Το μήκος του κύκλου σ είναι 6 και χρησιμοποιώντας τη νέα σημειογραφία που εισαγάγαμε προηγουμένως έχουμε:

$$\sigma = \begin{pmatrix} 2 & 4 & 6 & 8 & 10 & 12 \end{pmatrix}$$

Προσέξτε ότι θα μπορούσαμε να είχαμε κατασκευάσει την προηγούμενη τροχιά αρχίζοντας από κάποιο άλλο στοιχείο της, ας πούμε το 10. Τώρα έχουμε:

$$\mathcal{O}_{\sigma,10} = \{10, \sigma^1(10) = 12, \sigma^2(10) = 2, \sigma^3(10) = 4, \sigma^4(10) = 6, \sigma^5(10) = 8\}$$

και ο κύκλος γράφεται

$$\sigma = \begin{pmatrix} 10 & 12 & 2 & 4 & 6 & 8 \end{pmatrix}$$

Η σειρά εμφάνισης των στοιχείων στις δύο προηγούμενες παραστάσεις είναι διαφορετική, ωστόσο αυτές ορίζουν το ίδιο στοιχείο της S_{12}, δηλαδή το σ.

(2) *Ας δούμε ποιο στοιχείο σ της S_{12} παριστάνει το*

$$\begin{pmatrix}8 & 5 & 11 & 3\end{pmatrix}.$$

Σύμφωνα με την ερμηνεία της σημειογραφίας που δόθηκε στην Παρατήρηση 7.13,(2)(*) έχουμε:

$$\sigma(i) = i, \forall i \in \{1, 2, \ldots, 11, 12\} \setminus \{8, 5, 11, 3\},$$
$$\sigma(8) = 5, \;\; \sigma^2(8) = \sigma(5) = 11, \;\; \sigma^3(8) = \sigma(11) = 3, \;\; \sigma^4(8) = \sigma(3) = 8.$$

Συνεπώς, η συγκεκριμένη μετάθεση σ είναι η

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

Ορισμός 7.15. *Οι κύκλοι της $(S_n, \circ)$ μήκους s ονομάζονται s-κύκλοι.*
Οι κύκλοι της $(S_n, \circ)$ μήκους 2, δηλαδή οι 2-κύκλοι, ονομάζονται αντιμεταθέσεις.

Παρατήρηση 7.16. (1) *Κάθε 1-κύκλος της S_n παριστάνει το ταυτοτικό στοιχείο Id_n. Πράγματι, ας είναι $a \in A = \{1, 2, \ldots, n\}$ και ας θεωρήσουμε τον 1-κύκλο $\tau = (a)$.*
Σύμφωνα με την Παρατήρηση 7.13.(2)(*) έχουμε,

$$\tau(x) = \begin{cases} x, & \text{αν } x \in A \setminus \{a\} \\ a, & \text{αν } x = a. \end{cases}$$

Ώστε στην S_n όλοι οι 1-κύκλοι είναι ίσοι μεταξύ τους αφού είναι όλοι ίσοι με το ταυτοτικό στοιχείο Id_n.

(2) *Ένας κύκλος μήκους 2 ονομάζεται αντιμετάθεση επειδή εναλλάσσει δύο διαφορετικά στοιχεία του συνόλου $A = \{1, 2, \ldots, n\}$.*
Πράγματι, αν $\tau = (a\;\; b)$, όπου $a, b \in A = \{1, 2, \ldots, n\}, a \neq b$, τότε

$$\tau(x) = \begin{cases} x, & \text{αν } x \in A \setminus \{a, b\} \\ b, & \text{αν } x = a \\ a, & \text{αν } x = b \end{cases}$$

Ορισμός 7.17. *Δύο κύκλοι της $(Sn, \circ)$ ονομάζονται αποσυνδετοί (ή ξένοι), αν οι τροχιές τους με το μεγαλύτερο πλήθος στοιχείων δεν έχουν κοινά στοιχεία.*

Παρατήρηση 7.18. *Από τον προηγούμενο ορισμό προκύπτει ότι για να είναι δύο κύκλοι της S_n αποσυνδετοί πρέπει να έχουν και οι δύο μήκος ≥ 2, αφού αν ένας από τους δύο έχει μήκος 1, τότε αυτός είναι το ταυτοτικό στοιχείο Id_n της S_n. Αλλά τώρα κάθε τροχιά του Id_n έχει μήκος 1, δηλαδή είναι μια τροχιά που έχει το μεγαλύτερο πλήθος στοιχείων, και είναι σαφές ότι όποιος και αν είναι ο άλλος κύκλος, η τροχιά του με το μεγαλύτερο πλήθος στοιχείων έχει μη κενή τομή με κάποια από τις τροχιές του Id_n.*

Παράδειγμα 7.19. *Οι κύκλοι $\sigma = \begin{pmatrix}1 & 9 & 8\end{pmatrix}$ και $\tau = \begin{pmatrix}11 & 1 & 12\end{pmatrix}$ της S_{12} δεν είναι αποσυνδετοί. Η μοναδική τροχιά του σ με μήκος > 1 είναι η $\mathcal{O}_{\sigma,1} = \{1, 9, 8\}$. Η μοναδική τροχιά του τ με μήκος > 1 είναι η $\mathcal{O}_{\tau,11} = \{11, 1, 12\}$ και $\mathcal{O}_{\sigma,1} \cap \mathcal{O}_{\tau,11} = \{1\} \neq \emptyset$.*
Αντίθετα οι κύκλοι $\sigma = \begin{pmatrix}1 & 9 & 8\end{pmatrix}$ και $\rho = \begin{pmatrix}6 & 3 & 7\end{pmatrix}$ της S_{12} είναι αποσυνδετοί, αφού $\mathcal{O}_{\rho,6} = \{6, 3, 7\}$ και $\mathcal{O}_{\sigma,1} \cap \mathcal{O}_{\rho,6} = \emptyset$.

Πρόταση 7.20. *Κάθε στοιχείο της $(S_n, \circ)$ ή είναι ένας κύκλος ή είναι μια σύνθεση κύκλων αποσυνδετών ανά δύο, όπου το μήκος εκάστου είναι ≥ 2.*

Απόδειξη. Έστω μια μετάθεση (μετάταξη) σ της S_n.

Εάν η σ είναι ένας κύκλος δεν χρειάζεται να αποδειχθεί τίποτα.

Ας υποθέσουμε ότι η σ δεν είναι κύκλος. Τότε η σ διαθέτει τουλάχιστον δύο τροχιές με περισσότερα του ενός στοιχεία. Έστω ότι οι τροχιές της σ με περισσότερα του ενός στοιχεία είναι οι

$$\mathcal{O}_1 = \mathcal{O}_{\sigma,a_{11}} = \{a_{11}, a_{12}, \ldots, a_{1t_1}\}, \mathcal{O}_2 = \mathcal{O}_{\sigma,a_{21}} = \{a_{21}, a_{22}, \ldots, a_{2t_2}\}, \ldots,$$
$$\mathcal{O}_i = \mathcal{O}_{\sigma,a_{i1}} = \{a_{i1}, a_{i2}, \ldots, a_{it_i}\}, \ldots, \mathcal{O}_s = \mathcal{O}_{\sigma,a_{s1}} = \{a_{s1}, a_{s2}, \ldots a_{st_s}\}.$$

Για κάθε $i, 1 \leq i \leq s$ ορίζουμε τη μετάθεση γ_i ως εξής

$$\gamma_i(a) = \begin{cases} \sigma(a), & \text{αν } a \in \mathcal{O}_i, \\ a, & \text{αν } a \notin \mathcal{O}_i \end{cases}$$

Συνεπώς για κάθε $i, 1 \leq i \leq s$, η γ_i ισούται με τον κύκλο $\begin{pmatrix} a_{i1} & a_{i2} & \ldots & a_{it_i} \end{pmatrix}$. Προσέξτε ότι το μήκος του γ_i είναι ≥ 2, αφού ισούται με το πλήθος t_i των στοιχείων της τροχιάς $\mathcal{O}_i$.

Ισχυριζόμαστε ότι $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s$.

Αν το a είναι ένα στοιχείο του $\{1, 2, \ldots, n\} \setminus (\mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_s)$, τότε $\sigma(a) = a$ και $\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s(a) = a$, αφού το a δεν εμφανίζεται σε κανέναν από τους κύκλους γ_i.

Αν το a είναι ένα στοιχείο από το σύνολο $(\mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_s)$, τότε το a ανήκει σε ακριβώς μία τροχιά, ας πούμε την $\mathcal{O}_i$, αφού τα σύνολα $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_s$ είναι ανά δύο αποσυνδετά (ξένα).

Έτσι έχουμε

$$\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_{i-1} \circ \gamma_i \circ \cdots \circ \gamma_s(a) = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_{i-1} \circ \gamma_i \circ \cdots \circ \gamma_{s-1}(a) = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_{i-1} \circ \gamma_i(a),$$

αφού $\gamma_s(a) = a, \gamma_{s-1}(a) = a, \ldots, \gamma_{i+1}(a) = a$.

Τώρα παρατηρούμε ότι από τον ορισμό του γ_i και επειδή το στοιχείο a ανήκει στην τροχιά $\mathcal{O}_i$, έπεται ότι το στοιχείο $\gamma_i(a)$ ισούται με $\sigma(a)$, που επίσης ανήκει στην τροχιά $\mathcal{O}_i$ και γι' αυτό το $\sigma(a)$ δεν ανήκει σε καμιά από τις τροχιές $\mathcal{O}_{i-1}, \ldots, \mathcal{O}_2, \mathcal{O}_1$. Συνεπώς, $\gamma_{i-1}(\sigma(a)) = \sigma(a), \gamma_{i-2}(\sigma(a)) = \sigma(a), \ldots \gamma_2(\sigma(a)) = \sigma(a), \gamma_1(\sigma(a)) = \sigma(a)$.

Έτσι παίρνουμε

$$\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_{i-1} \circ \gamma_i(a) = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_{i-1}(\sigma(a)) = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_{i-2}(\sigma(a)) = \gamma_1(\sigma(a)) = \sigma(a).$$

Ώστε τελικώς,

$$\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_{i-1} \circ \gamma_i \circ \cdots \circ \gamma_s(a) = \sigma(a).$$

Αποδείξαμε λοιπόν ότι $\forall a \in \{1, 2, \ldots, n\}, \sigma(a) = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s(a)$. Συνεπώς, $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s$, όπου $\forall i, 1 \leq i \leq s$ το μήκος του γ_i είναι ≥ 2, όπως ακριβώς ισχυριστήκαμε. □

Λήμμα 7.21. *Έστω ότι γ και δ είναι δύο αποσυνδετοί κύκλοι της $(S_n, \circ)$, τότε οι κύκλοι μετατίθενται μεταξύ τους, δηλαδή*

$$\gamma \circ \delta = \delta \circ \gamma.$$

Απόδειξη. Σύμφωνα με την Παρατήρηση 7.18 αμφότεροι οι γ και δ έχουν μήκος ≥ 2. Έστω ότι

$$\gamma = \begin{pmatrix} c_1 & c_2 & \ldots & c_r \end{pmatrix}, \delta = \begin{pmatrix} d_1 & d_2 & \ldots & d_t \end{pmatrix}, \text{ όπου } r, t \geq 2.$$

Για κάθε $a \in \{1, 2, \ldots, n\} \setminus (\{c_1, c_2, \ldots, c_r\} \cup \{d_1, d_2, \ldots, d_t\})$ είναι

$$\gamma \circ \delta(a) = a = \delta \circ \gamma(a).$$

Για κάθε $a \in \{c_1, c_2, \ldots, c_r\}$ είναι

$$\gamma \circ \delta(a) = \gamma(\delta(a)) = \gamma(a) = \delta(\gamma(a)) = \delta \circ \gamma(a),$$

αφού $a \in \{c_1, c_2, \ldots, c_r\}$ συνεπάγεται ότι επίσης $\gamma(a) \in \{c_1, c_2, \ldots, c_r\}$ και γι' αυτό a και $\gamma(a) \notin \{d_1, d_2, \ldots, d_t\}$, επειδή οι γ, δ είναι αποσυνδετοί κύκλοι. Έτσι $\delta(a) = a$ και $\delta(\gamma(a)) = \gamma(a)$. Ακριβώς ανάλογα αποδεικνύεται ότι, για κάθε $a \in \{d_1, d_2, \ldots, d_t\}$ είναι

$$\gamma \circ \delta(a) = \gamma(\delta(a)) = \delta(a) = \delta(\gamma(a)) = \delta \circ \gamma(a),$$

αφού $a = \gamma(a)$ και $\delta(a) = \gamma(\delta(a))$. □

Πόρισμα 7.22. *Αν $\gamma_1, \gamma_2, \ldots, \gamma_s$ είναι κύκλοι της $(S_n, \circ)$ ανά δύο αποσυνδετοί, τότε*

$$\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s = \gamma_{i_1} \circ \gamma_{i_2} \circ \cdots \circ \gamma_{i_s},$$

όπου $i_1, i_2, \ldots, i_s$ είναι μια οποιαδήποτε αναδιάταξη των $1, 2, \ldots, s$.

Πρόταση 7.23. *Έστω ότι σ είναι ένα στοιχείο της $(S_n, \circ)$.*

(1) *Αν το σ είναι ένας κύκλος της S_n με μήκος $\ell(\sigma)$, τότε η τάξη $\circ(\sigma)$ ισούται με $\ell(\sigma)$.*
(2) *Αν το σ ισούται με μια σύνθεση $\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s$ κύκλων με πλήθος $s \geq 2$, αποσυνδετών ανά δύο και μήκους $\ell(\gamma_i) \geq 2, \forall i, 1 \leq i \leq s$, τότε η τάξη $\circ(\sigma)$ ισούται με το ελάχιστο κοινό πολλαπλάσιο των μηκών $\ell(\gamma_i), 1 \leq i \leq s$.*

Απόδειξη. (1) Αν ο σ είναι ένας κύκλος μήκους $\ell(\sigma) = 1$, τότε $\sigma = \mathrm{Id}_n$ και συνεπώς, $\circ(\sigma) = 1 = \ell(\sigma)$. Έστω ότι ο $\sigma = \begin{pmatrix} a_1 & a_2 & \ldots & a_t \end{pmatrix}$ είναι ένας κύκλος μήκους $\ell(\sigma) = t \geq 2$.
Παρατηρούμε ότι

$$\forall i, 1 \leq i \leq t-1, \sigma^i(a_1) = a_{i+1} \text{ και ότι } \sigma^t(a_1) = a_1. \tag{*}$$

Συνεπώς, $\nexists i \in \mathbb{N}, 1 \leq i \leq t-1$ με $\sigma^i = \mathrm{Id}_n$, αφού $\sigma^i(a_1) \neq a_1$. Θα δείξουμε τώρα ότι $\sigma^t = \mathrm{Id}_n$ και τότε επειδή ο $t = \ell(\sigma)$ είναι ο μικρότερος φυσικός με αυτήν την ιδιότητα, συμπεραίνουμε ότι $t = \circ(\sigma)$.
Ήδη γνωρίζουμε από την $(*)$ ότι $\sigma^t(a_1) = a_1$. Θα δείξουμε ότι $\forall i, 2 \leq i \leq t$ είναι $\sigma^t(a_i) = a_i$. Επειδή $i \geq 2$ έχουμε, λόγω της $(*)$, ότι $a_i = \sigma^{i-1}(a_1)$. Επομένως, $\sigma^t(a_i) = \sigma^t(\sigma^{i-1}(a_1)) = \sigma^{i-1}(\sigma^t(a_1)) = \sigma^{i-1}(a_1) = a_i$. Ώστε, $\sigma^t = \mathrm{Id}_n$.
(2) Θα αποδείξουμε πρώτα ότι αν, για κάποιο $r \in \mathbb{N}$ είναι $(\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s)^r = \mathrm{Id}_n (**)$, τότε $\forall i, 1 \leq i \leq s$, είναι $\gamma_i^r = \mathrm{Id}_n$.

Παρατηρούμε ότι από το Πόρισμα 7.22 προκύπτει ότι

$$(\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s)^r = \gamma_1^r \circ \gamma_2^r \circ \cdots \circ \gamma_i^r \circ \cdots \circ \gamma_{s-1}^r \circ \gamma_s^r = \mathrm{Id}_n. \tag{**}$$

αφού οι $\gamma_1, \gamma_2, \ldots, \gamma_{s-1}, \gamma_s$ είναι ανά δύο αποσυνδετοί κύκλοι,

Ας είναι $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_{s-1}, \mathcal{O}_s$ οι αντίστοιχες, ανά δύο αποσυνδετές, τροχιές των $\gamma_1, \gamma_2, \ldots, \gamma_{s-1}, \gamma_s$. Θεωρούμε την ένωσή τους $U = (\mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_{s-1} \cup \mathcal{O}_s)$

Αν $a \in \{1, 2, \ldots, n\} \setminus U$, τότε

$$\forall i, 1 \leq i \leq s, \gamma_i^r(a) = a.$$

Υπολείπεται να δείξουμε ότι αν, $a \in U$, τότε και πάλι $\forall i, 1 \leq i \leq s$, είναι $\gamma_i^r(a) = a$. Αλλά όταν $a \in U$, τότε υπάρχει ακριβώς ένας δείκτης $j, 1 \leq j \leq s$ με $a \in \mathcal{O}_j$, αφού οι τροχιές είναι ανά δύο αποσυνδετές.

Αν $j = 1$, τότε έχουμε $\gamma_2(a) = a, \ldots, \gamma_s(a) = a$ και γι' αυτό και $\gamma_2^r(a) = a, \ldots, \gamma_s^r(a) = a$. Συνεπώς, από την $(**)$ παίρνουμε

$$\forall a \in U, \gamma_1^r \circ \gamma_2^r \circ \cdots \circ \gamma_i^r \circ \cdots \circ \gamma_{s-1}^r \circ \gamma_s^r(a) = \gamma_1^r(a) = \mathrm{Id}_n(a) = a.$$

Αν $j > 1$, τότε έχουμε $\forall i \neq j, 1 \leq i \leq s, \gamma_i(a) = a$ και γι' αυτό και $\forall i \neq j, 1 \leq i \leq s, \gamma_i^r(a) = a$. Τώρα από την $(**)$ παίρνουμε

$$\forall a \in U, \gamma_1^r \circ \gamma_2^r \circ \cdots \circ \gamma_j^r \circ \cdots \circ \gamma_{s-1}^r \circ \gamma_s^r(a) = \gamma_1^r \circ \gamma_2^r \circ \cdots \circ \gamma_j^r(a) = \mathrm{Id}_n(a) = a$$

και κατόπιν

$$\forall a \in U, \gamma_j^r(a) = \gamma_{j-1}^{(-r)} \circ \gamma_{j-2}^{(-r)} \circ \cdots \circ \gamma_1^{(-r)}(a). \tag{***}$$

Όμως, επειδή, $\forall i \neq j, 1 \leq i \leq s$ είναι $\gamma_i(a) = a$ και κατόπιν $\gamma_i^r(a) = a$, έπεται ότι $\forall i \neq j, 1 \leq i \leq s$ είναι επίσης $\gamma_i^{(-r)}(a) = a$.

Γι' αυτό η $(***)$ δίνει

$$\forall a \in U, \gamma_j^r(a) = \gamma_{j-1}^{(-r)} \circ \gamma_{j-2}^{(-r)} \circ \cdots \circ \gamma_1^{(-r)}(a) = \gamma_{j-1}^{(-r)} \circ \gamma_{j-2}^{(-r)} \circ \cdots \circ \gamma_2^{(-r)}(a) = \cdots = \gamma_{j-1}^{(-r)}(a) = a.$$

Αποδείξαμε λοιπόν ότι $\forall a \in \{1, 2, \ldots, n\}$ και $\forall i, 1 \leq i \leq n$ έχουμε $\gamma_i^r(a) = a$, δηλαδή $\gamma_i^r = \mathrm{Id}_n$.
Ώστε, όταν $\sigma = (\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s)$ και $\sigma^r = (\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s)^r = \mathrm{Id}_n, r \in \mathbb{N}$, όπου οι γ_i είναι αποσυνδετοί κύκλοι, τότε

$$\forall i, 1 \leq i \leq s, \gamma_i^r = \mathrm{Id}_n.$$

Επιπλέον, αν για κάποιο $r \in \mathbb{N}$ είναι $(\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s)^r = \mathrm{Id}_n$, τότε η τάξη $\circ(\gamma_i) = \ell(\gamma_i)$ είναι διαιρέτης του r, αφού $\forall i, 1 \leq i \leq s, \gamma_i^r = \mathrm{Id}_n$. Συνεπώς, και το ελάχιστο κοινό πολλαπλάσιο ϵ των τάξεων $\circ(\gamma_i) = \ell(\gamma_i), 1 \leq i \leq s$ είναι επίσης διαιρέτης του r. Γι' αυτό αν, κατορθώσουμε να αποδείξουμε ότι

$$\sigma^\epsilon = (\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s)^\epsilon = \mathrm{Id}_n,$$

τότε το ελάχιστο κοινό πολλαπλάσιο ϵ είναι η τάξη του σ, αφού για κάθε άλλο $r \in \mathbb{N}$ με $\sigma^r = \mathrm{Id}_n$, έπεται ότι το ϵ διαιρεί το r, δηλαδή το ϵ είναι ο μικρότερος φυσικός αριθμός με την ιδιότητα αυτή. Αλλά

$$\sigma^\epsilon = (\gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_i \circ \cdots \circ \gamma_s)^\epsilon = \gamma_1^\epsilon \circ \gamma_2^\epsilon \circ \cdots \circ \gamma_i^\epsilon \circ \cdots \circ \gamma_s^\epsilon = \mathrm{Id}_n,$$

αφού το ϵ ως πολλαπλάσιο οποιασδήποτε τάξης $\circ(\gamma_i) = \ell(\gamma_i)$ έχει την ιδιότητα $\gamma_i^\epsilon = \mathrm{Id}_n$.

Ώστε, όταν $\sigma = \gamma_1 \circ \cdots \circ \gamma_s$, όπου οι γ_i είναι κύκλοι μήκους ≥ 2 και αποσυνδετοί ανά δύο, τότε η τάξη $\circ(\sigma)$ ισούται με το ελάχιστο κοινό πολλαπλάσιο ϵ των τάξεων των κύκλων γ_i. □

Παράδειγμα 7.24. *Η τάξη του*

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

είναι 7 *αφού*

$$\sigma = \begin{pmatrix} 1 & 7 & 10 & 8 & 9 & 2 & 6 \end{pmatrix},$$

δηλαδή είναι ένας κύκλος μήκους 7.

Η τάξη του

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

είναι το ελάχιστο κοινό πολλαπλάσιο των τάξεων των κύκλων $\begin{pmatrix} 1 & 9 & 2 \end{pmatrix}$, $\begin{pmatrix} 3 & 4 & 5 \end{pmatrix}$, $\begin{pmatrix} 6 & 7 \end{pmatrix}$ *και* $\begin{pmatrix} 8 & 10 \end{pmatrix}$, *αφού*

$$\tau = \begin{pmatrix} 1 & 9 & 2 \end{pmatrix} \circ \begin{pmatrix} 3 & 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 6 & 7 \end{pmatrix} \circ \begin{pmatrix} 8 & 10 \end{pmatrix}.$$

Επομένως $\circ(\tau) = 6$.

Η τάξη του $\sigma \circ \tau$ ***δεν είναι*** $\circ(\sigma) \cdot \circ(\tau) = 7 \cdot 6 = 42$. *Για να υπολογίσουμε τη συγκεκριμένη τάξη πρέπει να εκφράσουμε το* $\sigma \circ \tau$ *ως σύνθεση αποσυνδετών κύκλων.*

Έχουμε

$$\begin{array}{llll} \sigma \circ \tau(1) = \sigma(9) = 2 & \sigma \circ \tau(2) = \sigma(1) = 7 & \sigma \circ \tau(3) = \sigma(4) = 4 & \sigma \circ \tau(4) = \sigma(5) = 5 \\ \sigma \circ \tau(5) = \sigma(3) = 3 & \sigma \circ \tau(6) = \sigma(7) = 10 & \sigma \circ \tau(7) = \sigma(6) = 1 & \sigma \circ \tau(8) = \sigma(10) = 8 \\ \sigma \circ \tau(9) = \sigma(2) = 6 & \sigma \circ \tau(10) = \sigma(8) = 9. & & \end{array}$$

Επομένως,

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

Γι' αυτό, η τάξη του $\sigma \circ \tau$ *είναι το ελάχιστο κοινό πολλαπλάσιο των τάξεων* $\circ\left(\begin{pmatrix} 1 & 2 & 7 \end{pmatrix}\right) = 3$, $\circ\left(\begin{pmatrix} 3 & 4 & 5 \end{pmatrix}\right) = 3$ *και* $\circ\left(\begin{pmatrix} 6 & 10 & 9 \end{pmatrix}\right) = 3$, *δηλαδή* $\circ(\sigma \circ \tau) = 3$.

Συμπληρώνουμε την παρούσα υποενότητα με τα ακόλουθα:

Πρόταση 7.25. *Ο k-κύκλος $\gamma = \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix}, k \geq 2$ της $(S_n, \circ), n \geq 2$ έχει ως αντίστροφο στοιχείο τον k-κύκλο $\delta = \begin{pmatrix} a_k & a_{k-1} & \dots & a_1 \end{pmatrix}$.*

Απόδειξη. Είναι αρκετό να αποδείξουμε ότι $\delta \circ \gamma = \mathrm{Id}_n, (*)$, αφού τότε έχουμε

$$(\delta \circ \gamma) \circ \gamma^{-1} = \mathrm{Id}_n \circ \gamma^{-1} \Leftrightarrow \delta \circ \mathrm{Id}_n = \gamma^{-1} \Leftrightarrow \delta = \gamma^{-1}.$$

Για να αποδείξουμε την $(*)$, πρέπει να διαπιστώσουμε ότι $\forall x \in \{1, 2, \dots, n\}$ ισχύει $\delta \circ \gamma(x) = x$.

Αν $x \in \{1, 2, \dots, n\} \setminus \{a_1, a_2, \dots, a_k\}$, τότε

$$\delta \circ \gamma(x) = \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix} \circ \begin{pmatrix} a_k & a_{k-1} & \dots & a_1 \end{pmatrix}(x) = \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix}(x) = x.$$

Αν $x \in \{a_1, a_2, \dots, a_k\}$, τότε

$$\delta \circ \gamma(x) = \begin{cases} \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix} \circ \begin{pmatrix} a_k & a_{k-1} & \dots & a_1 \end{pmatrix}(a_i) = \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix}(a_{i-1}) = a_i \quad \text{αν, } i \neq 1 \\ \text{και για } i = 1 \\ \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix} \circ \begin{pmatrix} a_k & a_{k-1} & \dots & a_1 \end{pmatrix}(a_1) = \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix}(a_k) = a_1. \end{cases}$$

Έτσι διαπιστώνουμε ότι η $(*)$ είναι αληθής και συνεπώς $\delta = \begin{pmatrix} a_k & a_{k-1} & \dots & a_1 \end{pmatrix} = \gamma^{-1}$. □

Πρόταση 7.26. *Έστω ότι σ είναι μια μετάθεση (μετάταξη) της $(S_n, \circ), n \geq 2$ και ότι $\gamma = \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix}$ είναι ένας k-κύκλος, $k \geq 1$. Τότε*

$$\sigma \circ \gamma \circ \sigma^{-1} = \sigma \circ \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix} \circ \sigma^{-1} = \begin{pmatrix} \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_k) \end{pmatrix}.$$

Απόδειξη. Θα δείξουμε ότι $\forall x \in \{1, 2, \dots, n\}$ είναι

$$\sigma \circ \gamma \circ \sigma^{-1}(x) = \begin{pmatrix} \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_k) \end{pmatrix}(x). \qquad \textbf{(*)}$$

Διακρίνουμε δύο περιπτώσεις:

(I) Αν, $x \in \{1, 2, \dots, n\} \setminus \{\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k)\}$, τότε

$$\begin{pmatrix} \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_k) \end{pmatrix}(x) = x.$$

Αφού $x \notin \{\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k)\}$ και σ^{-1} είναι η αντίστροφη της σ, έχουμε ότι $\sigma^{-1}(x) \notin \{a_1, a_2, \dots, a_k\}$ και γι' αυτό

$$\sigma \circ \gamma \circ \sigma^{-1}(x) = \sigma \circ \begin{pmatrix} \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_k) \end{pmatrix} \circ \sigma^{-1}(x) =$$
$$\sigma\left[\begin{pmatrix} \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_k) \end{pmatrix}(\sigma^{-1}(x))\right] = \sigma(\sigma^{-1}(x)) = x.$$

Ώστε, όταν $x \in \{1, 2, \dots, n\} \setminus \{\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k)\}$, τότε η $(*)$ είναι αληθής.

(II) Αν, $x \in \{\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k)\}$, ας πούμε $x = \sigma(a_i), 1 \leq i \leq k$, τότε

$$\begin{pmatrix} \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_k) \end{pmatrix}(x) = \begin{pmatrix} \sigma(a_1) & \sigma(a_2) & \dots & \sigma(a_k) \end{pmatrix}(\sigma(a_i)) =$$
$$\begin{cases} \sigma(a_{i+1}), & \text{αν, } 1 \leq i \leq k-1 \\ \sigma(a_1), & \text{αν, } i = k \end{cases}$$

και

$$\sigma \circ \gamma \circ \sigma^{-1}(x) = \sigma \circ \begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix} \circ \sigma^{-1}(\sigma(a_i)) = \sigma\left[\begin{pmatrix} a_1 & a_2 & \dots & a_k \end{pmatrix}(a_i)\right] =$$
$$\begin{cases} \sigma(a_{i+1}), & \text{αν, } 1 \leq i \leq k-1 \\ \sigma(a_1), & \text{αν, } i = k \end{cases}.$$

Ώστε, όταν $x \in \{\sigma(a_1), \sigma(a_2), \dots, \sigma(a_k)\}$, τότε η $(*)$ είναι και πάλι αληθής. Επομένως, $\forall x \in \{1, 2, \dots, n\}$ η $(*)$ είναι αληθής. Η απόδειξη της πρότασης έχει ολοκληρωθεί. □

7.3. **Εκτιμώντας τις τάξεις των μεταθέσεων (μετατάξεων) της $(\mathbf{S_n}, \circ)$. Διαμερίσεις του $\mathbf{n}$.**
Προκειμένου να υπολογίσουμε την τάξη μιας μετάθεσης $\sigma \in S_n$, πρέπει σύμφωνα με Προτάσεις 7.20 και 7.23, να εκφράσουμε τη σ ως σύνθεση αποσυνδετών κύκλων και κατόπιν να υπολογίσουμε το ελάχιστο κοινό πολλαπλάσιο από τα μήκη των κύκλων.

Έστω ότι σ είναι ένα στοιχείο της $\in S_n$ και ότι $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$ είναι μια ανάλυση της σ ως σύνθεση αποσυνδετών κύκλων. Παρατηρούμε ότι μπορούμε να συμπληρώσουμε την ανάλυση με κύκλους (αν υπάρχουν) μήκους 1, οι οποίοι αντιστοιχούν ακριβως στις τροχιές της σ που αποτελούνται από ένα και μόνο στοιχείο.
Για παράδειγμα αν,

$$\sigma = \begin{pmatrix} 4 & 12 & 8 \end{pmatrix} \circ \begin{pmatrix} 2 & 7 & 9 & 11 \end{pmatrix} \in S_{12},$$

τότε η σ εκφράζεται και ως

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

Γενικά αν, $\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$ είναι μια ανάλυση της $\sigma \in S_n$ ως σύνθεση αποσυνδετών κύκλων $\gamma_i = \begin{pmatrix} a_{i1} & a_{i2} & \ldots & a_{it_i} \end{pmatrix}, 1 \leq i \leq s$ με αντίστοιχα μήκη $\ell(\gamma_i) = t_i$, τότε μπορούμε να συμπληρώσουμε την ανάλυση με $m = [n - (t_1 + t_2 + \cdots + t_s)]$ το πλήθος 1–κύκλους $\begin{pmatrix} b_1 \end{pmatrix}, \begin{pmatrix} b_2 \end{pmatrix}, \ldots, \begin{pmatrix} b_m \end{pmatrix}$, όπου

$$\forall j, 1 \leq j \leq m, b_j \in \{1, 2, \ldots, n\} \setminus \bigcup_{i=1}^{s} \{a_{i1}, a_{i2}, \ldots, a_{it_i}\}.$$

και συνεπώς

$$\sigma = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s = \begin{pmatrix} b_1 \end{pmatrix} \circ \begin{pmatrix} b_2 \end{pmatrix} \circ \cdots \circ \begin{pmatrix} b_m \end{pmatrix} \circ \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s.$$

Παρατηρούμε τώρα ότι το άθροισμα όλων των μηκών των κύκλων της προηγούμενης ανάλυσης ισούται με n. Επειδή αποσυνδετοί κύκλοι μετατίθενται, βλ. Πόρισμα 7.22, μπορούμε επιπλέον να δεχθούμε ότι οι κύκλοι $\gamma_i, 1 \leq i \leq s$ είναι διατεταγμένοι με αύξουσα σειρά ως προς τα μήκη τους, δηλαδή αν $i < j$, τότε $\ell(\gamma_i) = t_i \leq t_j = \ell(\gamma_j)$.
Έτσι έχουμε

$$n = \underbrace{1 + 1 + \cdots + 1}_{m-\text{φορές}} + t_1 + t_2 + \cdots + t_s$$

Ορισμός 7.27. *Κάθε ακολουθία φυσικών αριθμών $(n_1, n_2, \ldots, n_r)$ με $n_1 \leq n_2 \leq \cdots \leq n_r$ και $n_1 + n_2 + \cdots + n_r = n$ ονομάζεται μια διαμέριση του φυσικού αριθμού $n \in \mathbb{N}$.*

Ώστε, κάθε $\sigma \in S_n$ χορηγεί μια διαμέριση του n, αλλά και αντίστροφα κάθε διαμέριση $(n_1, n_2, \ldots, n_r)$ του n χορηγεί μια μετάθεση (όχι απαραίτητα μοναδική) της S_n, αφού μπορούμε να προσδιορίσουμε r κύκλους μήκους n_i, οι οποίοι μάλιστα μπορεί να είναι αποσυνδετοί ανά δύο για κάθε $n_i \geq 2$.

Για παράδειγμα, η διαμέριση $(1, 2, 3, 3, 3)$ του 12 δίνει τη μετάθεση

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

καθώς επίσης και τη μετάθεση

$$\tau = \begin{pmatrix} 5 \end{pmatrix} \circ \begin{pmatrix} 2 & 7 \end{pmatrix} \circ \begin{pmatrix} 4 & 8 & 10 \end{pmatrix} \circ \begin{pmatrix} 3 & 6 & 9 \end{pmatrix} \circ \begin{pmatrix} 1 & 11 & 12 \end{pmatrix}$$

Οι σ και τ επειδή προκύπτουν από την ίδια διαμέριση του 12, δηλαδή την $(1, 1, 3, 3, 4)$, έχουν την ίδια ταξη, αφού το ελάχιστο κοινό πολλαπλάσιο των μηκών των αποσυνδετών κύκλων τους είναι το ίδιο, δηλαδή ισούται με $2 \cdot 3 = 6$.

Ορισμός 7.28. *Ονομάζουμε κυκλικό τύπο μιας μετάθεσης $\sigma \in S_n$, την αντίστοιχη διαμέριση του n, που προκύπτει αναλύοντας την σ σε γινόμενο αποσυνδετών κύκλων $\gamma_i, 1 \leq i \leq s$ διατεταγμένων με αύξουσα σειρά, συμπληρώνοντας (αν είναι απαραίτητο) την αρχή της ακολουθίας με τόσες μονάδες, όση είναι η διαφορά $n - \sum_{i=1}^{s} \ell(\gamma_i)$.*

Για παράδειγμα ο κυκλικός τύπος της

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 4 & 5 \end{pmatrix} \in S_5$$

είναι $(1, 2, 2)$ ενώ της

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 3 & 5 & 4 & 6 & 7 & 8 & 9 \end{pmatrix} = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 4 & 5 \end{pmatrix} \in S_9$$

είναι $(1, 1, 1, 1, 1, 2, 2)$.

Πρόταση 7.29. *Αν ο κυκλικός τύπος μια μετάθεσης (μετάταξης) $\sigma \in S_n$ είναι $(n_1, n_2, \ldots, n_t)$, τότε η τάξη $\circ(\sigma)$ ισούται με το ελάχιστο κοινό πολλαπλάσιο των αριθμών $n_1, n_2, \ldots, n_t$.*

Απόδειξη. Ήδη γνωρίζουμε ότι η τάξη της σ ισούται με το ελάχιστο κοινό πολαπλάσιο των μηκών των αποσυνδετών κύκλων μήκους ≥ 2 που εμφανίζονται σε μια ανάλυσή της. Αν συμβεί και κάποιοι από τους φυσικούς αριθμούς που εμφανίζονται στην αρχή της $(n_1, n_2, \ldots, n_t)$ είναι ίσοι με 1, αυτό δεν επηρρεάζει τον υπολογισμό του ελάχιστου κοινού πολλαπλασίου. □

Μέγιστη Τάξη Αν λοιπόν θέλουμε να υπολογίσουμε ποια είναι η μέγιστη τάξη των στοιχείων της S_n, οφείλουμε να υπολογίσουμε όλες τις διαμερίσεις $(n_1, n_2, \ldots, n_t)$ του συγκεκριμένου n και κατόπιν να προσδιορίσουμε για κάθε μια το ελάχιστο κοινό πολλαπλάσιο των αριθμών του συνόλου $\{n_1, n_2, \ldots, n_t\}$. Το μεγαλύτερο ελάχιστο κοινό πολλαπλασιο δίνει και τη μέγιστη τάξη των στοιχείων της S_n, πρόκειται δηλαδή για τον αριθμό

$$m = \max\{\text{ελάχιστο κοινό πολλαπλάσιο}(n_1, n_2, \ldots, n_t) \mid (n_1, n_2, \ldots, n_t) \text{ διαμέριση του } n\}$$

Για παράδειγμα οι διαμερίσεις του φυσικού αριθμού 5 είναι οι:

1	1	1	1	1
1	1	1	2	
1	2	2		
1	1	3		
2	3			
1	4			
5				

Συνεπώς, η μέγιστη τάξη ενός στοιχείου της S_5 είναι το ελάχιστο κοινό πολλαπλάσιο των 2 και 3, δηλαδή το 6. Τα στοιχεία της S_5 που έχουν τάξη 6 είναι ακριβώς τα στοιχεία που είναι συνθέσεις δύο αποσυνδετών κύκλων μήκους 2 και 3 αντιστοίχως.
Έτσι τα $\sigma_1 = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 3 & 4 & 5 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 3 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 5 \end{pmatrix}$, $\sigma_3 = \begin{pmatrix} 4 & 5 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$ είναι στοιχεία της S_5 τάξης 6.
Φυσικά, γνωρίζοντας όλες τις διαμερίσεις του n γνωρίζουμε και όλες τις τάξεις των στοιχείων της S_n. Γι' αυτό οι τάξεις των στοιχείων της S_5 είναι οι $1, 2, 3, 6, 4, 5$ αφού αυτοί οι αριθμοί είναι ακριβώς τα διαφορετικά ελάχιστα κοινά πολλαπλάσια που προκύπτουν από τις διαμερίσεις του 5.

Συνεπώς ο προσδιορισμός όλων των τάξεων των στοιχείων της S_n ανάγεται στον υπολογισμό όλων των δυνατών διαμερίσεων του n. Αυτό δεν είναι καθόλου απλό, επειδή δεν υπάρχει τύπος που να δίνει το

Φυσικός n	1	2	3	4	5	6	7	8	9	10
Πλήθος Διαμερίσεων $P(n)$	1	2	3	5	7	11	15	22	30	42

Πίνακας 1. Οι διαμερίσεις του $n = 1, 2, \ldots, 10$

πλήθος $P(n)$ των διαμερίσεων ενός φυσικού n, το οποίο σημειωτέον ότι αυξάνει πολύ γρήγορα, όπως διαπιστώνει κανείς και από τους επόμενους δύο πίνακες:

Φυσικός n	100	200	300	400
Πλήθος Διαμερίσεων $P(n)$	190569292	3972999029388	9253082936723602	6727090051741041926

Πίνακας 2. Οι διαμερίσεις του $n = 100, 200, 300$

7.4. **Άρτιες και περιττές μεταθέσεις (μετατάξεις).**

Λήμμα 7.30. *Κάθε k-κύκλος $\gamma = \begin{pmatrix} a_1 & a_2 & \ldots & a_k \end{pmatrix}$ της $(S_n, \circ), n \geq 2$ είναι σύνθεση αντιμεταθέσεων. Αν $k \geq 2$, τότε ο γ είναι σύνθεση $(k-1)$ το πλήθος αντιμεταδέσων.*

Απόδειξη. Αν ο κύκλος γ έχει μήκος $k = 1$, τότε ισούται με την ταυτοτική απεικόνιση Id_n, και $\gamma = \mathrm{Id}_n = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}$.

Αν ο κύκλος γ έχει μήκος $k \geq 2$, τότε ισχύει ότι

$$\gamma = \begin{pmatrix} a_1 & a_2 & \ldots & a_k \end{pmatrix} = \begin{pmatrix} a_1 & a_k \end{pmatrix} \circ \begin{pmatrix} a_1 & a_{k-1} \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_{i+1} \end{pmatrix} \circ \begin{pmatrix} a_1 & a_i \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 \end{pmatrix}. \quad \textbf{(*)}$$

Αφού όταν, $x \in \{1, 2, \ldots, n\} \setminus \{a_1, a_2 \ldots, a_k\}$, τότε $\gamma(x) = x$ και

$$\begin{pmatrix} a_1 & a_k \end{pmatrix} \begin{pmatrix} a_1 & a_{k-1} \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_{i+1} \end{pmatrix} \circ \begin{pmatrix} a_1 & a_i \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 \end{pmatrix} (x) = x.$$

Όταν $x \in \{a_1, a_2 \ldots, a_k\}, x \neq a_k$, ας πούμε $x = a_i$ με $i \neq k$, τότε $\gamma(a_i) = a_{i+1}$ και

$$\begin{pmatrix} a_1 & a_k \end{pmatrix} \circ \begin{pmatrix} a_1 & a_{k-1} \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_{i+1} \end{pmatrix} \circ \begin{pmatrix} a_1 & a_i \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 \end{pmatrix} (a_i) =$$
$$\begin{pmatrix} a_1 & a_k \end{pmatrix} \circ \begin{pmatrix} a_1 & a_{k-1} \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_{i+1} \end{pmatrix} \circ \begin{pmatrix} a_1 & a_i \end{pmatrix} (a_i) =$$
$$\begin{pmatrix} a_1 & a_k \end{pmatrix} \circ \begin{pmatrix} a_1 & a_{k-1} \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_{i+1} \end{pmatrix} (a_1) = \begin{pmatrix} a_1 & a_k \end{pmatrix} \circ \begin{pmatrix} a_1 & a_{k-1} \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_{i+2} \end{pmatrix} (a_{i+1}) = a_{i+1}.$$

Τέλος, όταν $x = a_k$, τότε $\gamma(a_k) = a_1$ και

$$\begin{pmatrix} a_1 & a_k \end{pmatrix} \circ \begin{pmatrix} a_1 & a_{k-1} \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_{i+1} \end{pmatrix} \circ \begin{pmatrix} a_1 & a_i \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 \end{pmatrix} (a_k) =$$
$$\begin{pmatrix} a_1 & a_k \end{pmatrix} (a_k) = a_1.$$

Επομένως,

$$\forall a \in \{1, 2, \ldots, n\}, \gamma(a) = \begin{pmatrix} a_1 & a_k \end{pmatrix} \circ \begin{pmatrix} a_1 & a_{k-1} \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_{i+1} \end{pmatrix} \circ \begin{pmatrix} a_1 & a_i \end{pmatrix} \circ \cdots \circ \begin{pmatrix} a_1 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 \end{pmatrix} (a)$$

και συνεπώς η $(*)$ είναι αληθής.

Προφανώς, το πλήθος των αντιμεταθέσεων είναι $(k-1)$. ☐

Πρόταση 7.31. *Κάθε στοιχείο $\sigma \in S_n, n \geq 2$ είναι σύνθεση αντιμεταδέσεων.*

Απόδειξη. Σύμφωνα με την Πρόταση 7.23 κάθε μετάθεση (μετάταξη) είναι σύνθεση κύκλων και σύμφωνα με το προηγούμενο Λήμμα κάθε κύκλος είναι σύνθεση αντιμεταθέσεων. Επομένως, κάθε μετάθεση είναι σύνθεση αντιμεταθέσεων. ☐

Για την απόδειξη του επόμενου θεωρήματος είναι απαραίτητο να ανακαλέσει ο αναγνώστης στη μνήμη του την έννοια της ορίζουσας $\det(A)$ ενός $n \times n$ πίνακα A, καθώς και ότι η ορίζουσα ενός πίνακα A αλλάζει πρόσημο όταν εναλλάξουμε δύο γραμμές της.

Επιπλέον, χρειάζεται να οριστεί το πως δρουν τα στοιχεία της ομάδας $(S_n, \circ)$ πάνω στο σύνολο $\mathcal{M}_n(\mathbb{R})$ των $n \times n$ πινάκων.
Αν σ είναι ένα στοιχείο της S_n και $A \in \mathcal{M}_n(\mathbb{R})$ είναι ένας πίνακας με γραμμές τις $A_1, A_2, \dots, A_n$, τότε ορίζουμε ως $\sigma(A)$ τον $n \times n$ πίνακα με i–οστή γραμμή την $A_{\sigma(i)}, \forall i, 1 \leq i \leq n$.

Για παράδειγμα, αν

$$\sigma = \begin{pmatrix} 1 & 3 & 5 \end{pmatrix} \circ \begin{pmatrix} 2 & 4 \end{pmatrix} \quad \text{και} \quad A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 \end{pmatrix}, \text{ τότε } \sigma(A) = \begin{pmatrix} 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 \\ 6 & 7 & 8 & 9 & 10 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}.$$

Παρατηρούμε ότι

Αν σ, τ είναι δύο στοιχεία της S_n και A είναι ένας $n \times n$ πίνακας, τότε $\sigma \circ \tau(A) = \sigma(\tau(A))$.

Αυτό είναι αληθές, αφού για κάθε $i, 1 \leq i \leq n$, η i–οστή γραμμή του $\sigma \circ \tau(A)$ είναι η $A_{\sigma \circ \tau(i)}$ και η i–οστή γραμμή του $\sigma(\tau(A))$ είναι η $A_{\sigma(\tau(i))}$. Επειδή όμως $\forall i, 1 \leq i \leq n$, $\sigma \circ \tau(i) = \sigma(\tau(i))$, οι δύο αυτές γραμμές είναι για κάθε i, ίσες και γι'αυτό $\sigma \circ \tau(A) = \sigma(\tau(A))$.

Θεώρημα 7.32. *Δεν υπάρχει στοιχείο $\sigma \in S_n, n \geq 2$, το οποίο να είναι σύνθεση ταυτοχρόνως και αρτίου και περιττού πλήθους αντιμεταθέσεων.*

Απόδειξη. Έστω ένα $\sigma \in S_n$, το οποίο είναι σύνθεση $2\kappa, \kappa \in \mathbb{N}$ αντιμεταθέσεων $\mu_i, 1 \leq i \leq 2\kappa$ και σύνθεση $2\lambda + 1, \lambda \in \mathbb{N}$ αντιμεταθέσεων $\nu_j, 1 \leq j \leq 2\lambda + 1$.

Θεωρούμε τον ταυτοτικό $n \times n$ πίνακα $\mathrm{I}_n = (\delta_{ij})$, όπου $\delta_{ij}, 1 \leq i, j \leq n$ είναι το σύμβολο του Kronecker[28]. Παρατηρούμε ότι για οποιαδήποτε αντιμετάθεση $\tau = \begin{pmatrix} s & t \end{pmatrix}, 1 \leq s, t \leq n, s \neq t$, η ορίζουσα $\det(\tau(\mathrm{I}_n))$ του πίνακα $\tau(\mathrm{I}_n)$ ισούται με $-\det(\mathrm{I}_n) = -1$, αφού ο $\tau(\mathrm{I}_n)$ προκύπτει από τον ταυτοτικό πίνακα I_n κατόπιν εναλλαγής της s–οστής με την t–οστή γραμμή.

Συνεπώς αν, $\sigma = \mu_1 \circ \cdots \circ \mu_{2\kappa}$, τότε $\det(\sigma(\mathrm{I}_n)) = \det((\mu_1 \circ \cdots \circ \mu_{2\kappa})(\mathrm{I}_n)) = (-1)^{2\kappa} = 1$. Ενώ αν, $\sigma = \nu_1 \circ \cdots \circ \nu_{2\lambda+1}$, τότε $\det(\sigma(\mathrm{I}_n)) = \det((\nu_1 \circ \cdots \circ \nu_{2\lambda+1})(\mathrm{I}_n)) = (-1)^{2\lambda+1} = -1$. Έτσι καταλήγουμε στο ότι $\det(\sigma(\mathrm{I}_n)) = 1$ και $\det(\sigma(\mathrm{I}_n)) = -1$. Πράγμα, άτοπο.

Ώστε, οποιοδήποτε στοιχείο $\sigma \in S_n$ είναι σύνθεση ή μόνο από άρτιου πλήθους ή μόνο από περιττού πλήθους αντιμεταθέσεις. ☐

Ορισμός 7.33. *Μια μετάθεση (μετάταξη) σ της συμμετρικής ομάδας $(S_n, \circ), n \geq 2$ ονομάζεται άρτια (αντιστοίχως περιττή) αν, είναι σύνθεση άρτιου (αντιστοίχως περιττού) πλήθους αντιμεταθέσεων.*

Παράδειγμα 7.34. *Η μετάθεση (μετάταξη)*

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

είναι άρτια, αφού

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

Η μετάθεση (μετάταξη)

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

[28] $\delta_{ij} = 1$, όταν $i = j$ και $\delta_{ij} = 0$, όταν $i \neq j$

είναι περιττή, αφού

$$\tau = \begin{pmatrix}1 & 2 & 7\end{pmatrix} \circ \begin{pmatrix}3 & 4 & 5\end{pmatrix} \circ \begin{pmatrix}6 & 10\end{pmatrix} = \begin{pmatrix}1 & 7\end{pmatrix} \circ \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}3 & 5\end{pmatrix} \circ \begin{pmatrix}3 & 4\end{pmatrix} \circ \begin{pmatrix}6 & 10\end{pmatrix}$$

Παρατήρηση 7.35. *Ένας k-κύκλος $\gamma = \begin{pmatrix}a_1 & a_2 & \dots & a_k\end{pmatrix}$ μήκους $k \geq 2$ είναι άρτια (αντιστοίχως περιττή) μετάθεση, όταν το μήκος του k είναι περιττό (αντιστοίχως άρτιο), αφού από το Λήμμα 7.30 γνωρίζουμε ότι ένας k-κύκλος είναι σύνθεση $(k-1)$ το πλήθος αντιμεταθέσων.*

Αλλά και κάθε 1-κύκλος της $S_n, n \geq 2$ είναι μια άρτια μετάθεση, αφού κάθε 1-κύκλος ισούται με το ταυτοτικό στοιχείο Id_n της S_n και $\mathrm{Id}_n = \begin{pmatrix}1 & 2\end{pmatrix} \circ \begin{pmatrix}1 & 2\end{pmatrix}$.

Πρόταση 7.36. *Το υποσύνολο*

$$\mathbb{A}_n = \{\sigma \in S_n \mid \sigma \text{ άρτια μετάθεση } \}$$

της $(S_n, \circ), n \geq 2$ αποτελεί μια υποομάδα της S_n.

Απόδειξη. Λόγω του Λήμματος **;;**, για να αποδείξουμε ότι το $\mathbb{A}_n$ είναι μια υποομάδα της S_n, είναι επαρκές να δείξουμε ότι το $\mathbb{A}_n$ είναι κλειστό ως προς τη πράξη της S_n, δηλαδή είναι κλειστό ως προς τη σύνθεση των απεικονίσεων, αφού πρόκειται για ένα πεπερασμένο σύνολο. Αλλά όταν τα σ, τ είναι στοιχεία του $\mathbb{A}_n$, τότε και η σύνθεσή τους $\sigma \circ \tau$ ανήκει επίσης στο $\mathbb{A}_n$, αφού όταν δύο μεταθέσεις (μετατάξεις) σ, τ είναι σύνθεση άρτιου πλήθους αντιμεταθέσεων, ας πούμε αντίστοιχα 2κ και 2λ, τότε η μετάθεση $\sigma \circ \tau$ είναι σύνθεση $2\kappa + 2\lambda = 2(\kappa + \lambda)$ πλήθους αντιμεταθέσεων, δηλαδή είναι επίσης μια άρτια μετάθεση. Επομένως, η $\mathbb{A}_n$ είναι μια υποομάδα της S_n. ☐

Ορισμός 7.37. *Η υποομάδα $\mathbb{A}_n$ της $(S_n, \circ)$ ονομάζεται η εναλλάσσουσα υποομάδα της S_n.*

Παρατήρηση 7.38. *Στην προηγούμενη απόδειξη διαπιστώσαμε πολύ εύκολα ότι η σύνθεση δύο άρτιων μεταθέσεων (μετατάξεων) είναι μια άρτια μετάταξη. Διαπιστώνεται επίσης πολύ εύκολα, μετρώντας το πλήθος των αντιμεταθέσεων, ότι η σύνθεση μια περιττής μετάθεσης (μετάταξης) με μια άρτια καθώς και η σύνθεση μιας άρτιας με μια περιττή δίνει μια περιττή μετάθεση. Τέλος η σύνθεση μια περιττής μετάθεσης με μια περιττή, δίνει μια άρτια μετάθεση.*

Τα προηγούμενα εκφράζονται συνοπτικά αντιστοιχώντας σε κάθε μετάθεση $\sigma \in S_n$ το λεγόμενο πρόσημο $\epsilon(\sigma) \in \{1, -1\} \subset \mathbb{Z}$ της σ ως εξής:

$$\epsilon(\sigma) = \begin{cases} 1 & \text{αν, η } \sigma \text{ είναι άρτια} \\ -1 & \text{αν, η } \sigma \text{ είναι περιττή} . \end{cases}$$

Τώρα γνωρίζουμε ότι, για οποιαδήποτε δύο στοιχεία $\sigma, \tau \in S_n$ είναι:

$$\epsilon(\sigma \circ \tau) = \epsilon(\sigma) \cdot \epsilon(\tau).$$

Πρόταση 7.39. *Η τάξη της υποομάδας $\mathbb{A}_n$ της $(S_n, \circ), n \geq 2$ ισούται με $\frac{n!}{2}$.*

Απόδειξη. Από το Λήμμα 7.4 γνωρίζουμε ότι η τάξη της S_n ισούται με $n!$. Επιπλέον γνωρίζουμε ότι η S_n ισούται με την αποσυνδετή ένωση $S_n = \mathbb{A}_n \cup (S_n \setminus \mathbb{A}_n)$, αφού κάθε μετάθεση της S_n είναι ή άρτια, δηλαδή ανήκει στην $\mathbb{A}_n$, ή περιττή, δηλαδή ανήκει στο $S_n \setminus \mathbb{A}_n$. Γι' αυτό

$$\mid S_n \mid = \mid \mathbb{A}_n \mid + \mid (S_n \setminus \mathbb{A}_n) \mid . \tag{*}$$

Θα δείξουμε ότι το πλήθος $\mid \mathbb{A}_n \mid$ της υποομάδας $\mathbb{A}_n$ ισούται με το πλήθος $\mid (S_n \setminus \mathbb{A}_n) \mid$ του συνόλου $(S_n \setminus \mathbb{A}_n)$.

Θεωρούμε την αντιμετάθεση $\mu = \begin{pmatrix}1 & 2\end{pmatrix}$. Επειδή η σύνθεση μιας περιττής μετάθεσης με μια άρτια δίνει μια περιττή μετάθεση, ορίζεται με τη βοήθεια της μ η απεικόνιση

$$\phi : \ \mathbb{A}_n \longrightarrow (S_n \setminus \mathbb{A}_n), \ \ \sigma \mapsto \ \ \mu \circ \sigma.$$

Επειδή η σύνθεση μιας περιττής μετάθεσης με μια περιττή δίνει μια άρτια μετάθεση, ορίζεται με τη βοήθεια της μ και η απεικόνιση

$$\psi : \ (S_n \setminus \mathbb{A}_n) \longrightarrow \mathbb{A}_n, \ \ \tau \mapsto \ \ \mu \circ \tau.$$

Αλλά οι $\phi \circ \psi$ και $\psi \circ \phi$ είναι οι ταυτοτικές απεικονίσεις των συνόλων $(S_n \setminus \mathbb{A}_n)$ και $\mathbb{A}_n$, αφού

$$\forall \tau \in S_n \setminus \mathbb{A}_n) : \ \phi \circ \psi(\tau) = \phi(\mu \circ \tau) = \mu \circ (\mu \circ \tau) = \mu^2 \circ \tau = \begin{pmatrix}1 & 2\end{pmatrix}^2 \circ \tau = \mathrm{Id}_n \circ \tau = \tau$$

και

$$\forall \sigma \in \mathbb{A}_n : \ \psi \circ \phi(\sigma) = \psi(\mu \circ \sigma) = \mu \circ (\mu \circ \sigma) = \mu^2 \circ \sigma = \begin{pmatrix}1 & 2\end{pmatrix}^2 \circ \sigma = \mathrm{Id}_n \circ \sigma = \sigma.$$

Επομένως, η ϕ είναι μια «1–1» και «επί» απεικόνιση και γι' αυτό $\mid \mathbb{A}_n \mid = \mid (S_n \setminus \mathbb{A}_n) \mid$.

Τώρα η $(*)$ δίνει

$$\mid S_n \mid = 2 \cdot \mid \mathbb{A}_n \mid \ \ \Rightarrow \ \ \mid \mathbb{A}_n \mid = \frac{\mid S_n \mid}{2} = \frac{n!}{2}.$$

□

Με τη βοήθεια της έννοιας της διαμέρισης ενός φυσικού n, βλ. Υποενότητα 7.3, μπορούμε να περιγράψουμε τον κυκλικό τύπο των στοιχείων της S_n που ανήκουν στην υποομάδα $\mathbb{A}_n$.

Έστω σ μια μετάθεση (μετάταξη) $\in S_n$ και η ανάλυσή του

$$\sigma = \gamma_1 \circ \gamma_2 \circ \ldots \gamma_s$$

σε γινόμενο αποσυνδετών κύκλων. Αφού

$$\epsilon(\sigma) = \epsilon(\gamma_1 \circ \gamma_2 \circ \ldots \gamma_s) = \epsilon(\gamma_1) \cdot \epsilon(\gamma_2) \cdot \cdots \cdot \epsilon(\gamma_s),$$

μπορεί κανείς να υπολογίσει το αν η σ είναι άρτια η περιττή, υπολογίζοντας τα $\epsilon(\gamma_i), 1 \leq i \leq s$, όπου υπενθυμίζουμε ότι ένας κύκλος με άρτιο μήκος (αντίστοιχα περιττό) είναι περιττή (άρτια) μετάθεση!

Παράδειγμα 7.40. *Θα προσδιορίσουμε τον κυκλικό τύπο και τις τάξεις των στοιχείων της* $\mathbb{A}_7$.

Οι διαμερίσεις του 7 είναι οι:

1	1	1	1	1	1	1
1	1	1	1	1	2	
1	1	1	2	2		
1	2	2	2			
1	1	1	1	3		
1	1	2	3			
1	3	3				
1	1	1	4			
1	1	5				
1	6					
1	2	4				
2	2	3				
2	5					
3	4					
7						

Παρατηρούμε ότι οι μεταθέσεις της S_7 *που ανήκουν στην* $\mathbb{A}_7$ *έχουν κυκλικό τύπο*

$$(1,1,1,1,1,1,1,1),(1,1,1,2,2),(1,1,1,1,3),(1,3,3),(1,1,5),(1,2,4),(2,2,3),(3,4),(7).$$

Γι᾽ αυτό οι αντίστοιχες τάξεις των στοιχείων της $\mathbb{A}_7$ *είναι:*

$$\varepsilon.\kappa.\pi.(1,1,1,1,1,1,1,1)=1, \varepsilon.\kappa.\pi.(1,1,1,2,2)=2, \varepsilon.\kappa.\pi.(1,1,1,1,3)=3,$$
$$\varepsilon.\kappa.\pi.(1,3,3)=3, \varepsilon.\kappa.\pi.(1,1,5)=5, \varepsilon.\kappa.\pi.(1,2,4)=4, \varepsilon.\kappa.\pi.(2,2,3)=6, \varepsilon.\kappa.\pi.(7)=7.$$

Ανοικτά Ακαδημαϊκά Μαθήματα

Πανεπιστήμιο Ιωαννίνων

Τέλος Ενότητας

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Ιωαννίνων**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Σημειώματα

Σημείωμα Αναφοράς

Σημείωμα Αδειοδότησης