Curs VIII
ELEMENTE DE TEORIA GRUPURILOR

§ 7. GRUPURI DE PERMUTĂRI

Fie A o mulţime. Am observat că mulţimea S(A) a funcţiilor bijective de la A în A formează faţă de compunere un grup numit *grupul permutărilor* mulţimii A.

Propoziţia 7.1. Dacă A şi A' sunt două mulţimi echipotente (sau între care există o funcţie bijectivă), atunci grupurile de permutări S(A) şi S(A') sunt izomorfe.

Demonstraţie. Fie $f : A \to A'$ o funcţie bijectivă. Definim o funcţie $\varphi : S(A) \to S(A')$ care asociază oricărei funcţii bijective $u \in S(A)$ funcţia bijectivă $f \circ u \circ f^{-1} \in S(A')$, deci

$$\varphi(u) = f \circ u \circ f^{-1}.$$

Să demonstrăm că φ este un izomorfism de grupuri. Într-adevăr,

$$\varphi(u \circ v) = f \circ (u \circ v) \circ f^{-1} = f \circ u \circ (f^{-1} \circ f) \circ u \circ f^{-1} = (f \circ u \circ f^{-1}) \circ (f \circ v \circ f^{-1}) = \varphi(u) \circ \varphi(y),$$

adică φ este morfism de grupuri.

Să arătăm că φ este bijecţie. Dacă $\varphi(u) = \varphi(v)$, atunci

$$f \circ u \circ f^{-1} = f \circ v \circ f^{-1},$$

de unde compunând la stânga cu f^{-1} şi la dreapta cu f, rezultă $u = v$ şi deci φ este injectivă. Dacă $u' \in S(A')$, atunci $f^{-1} \circ u' \circ f \in S(A)$ şi

$$\varphi(f^{-1} \circ u' \circ f) = f \circ (f^{-1} \circ u' \circ f) \circ f^{-1} = (f \circ f^{-1}) \circ u' \circ (f \circ f^{-1}) = u',$$

deci φ este surjectivă.

Observaţie. În particular, dacă A este o mulţime finită cu n elemente, există o bijecţie între A şi mulţimea {1, 2, ... , n}, deci grupurile de permutări S(A) şi S({l, 2, ... , n}) sunt izomorfe. Atunci, pentru a studia grupul de permutări al unei mulţimi cu n elemente este suficient să studiem grupul $\mathbf{S}_n$ al permutărilor mulţimii {1, 2, ... , n}.

Definiţia 7.2. Grupul $\mathbf{S}_n$ se numeşte *grupul simetric de grad n* sau *grupul permutărilor de grad n*. Elementele lui $\mathbf{S}_n$ se numesc *permutări* de n elemente sau permutări de grad n. Elementul neutru e din $\mathbf{S}_n$ se numeşte *permutarea identică* de grad n.

Să considerăm $\sigma \in \mathbf{S}_n$ o permutare de n elemente, adică o funcţie bijectivă de la mulţimea {1, 2, ... , n} în ea însăşi. Punând în evidenţă valoarea $\sigma(i)$ a funcţiei σ pentru $i \in \{1, 2, ... , n\}$, vom nota permutarea astfel

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

unde $\sigma(l), \sigma(2), ... , \sigma(n)$ sunt numerele 1, 2, ... , n, eventual în altă ordine.

Vom arăta că $\mathbf{S}_n$ are n! elemente. Vom demonstra acest fapt folosind teorema lui Lagrange. Notăm $\overline{\mathbf{S}}_{n-1} = \{\sigma \in \mathbf{S}_n \mid \sigma(n) = n\}$, mulţimea permutărilor de n elemente care invariază pe n. Este clar că $\overline{\mathbf{S}}_{n-1}$ este un un subgrup al lui $\mathbf{S}_n$, izomorf cu grupul $\mathbf{S}_{n-1}$ al permutărilor de n – 1 elemente. Izomorfismul este dat de funcţia

$$\theta : \mathbf{S}_{n-1} \to \overline{\mathbf{S}}_{n-1},$$

definită prin

$$\theta(\sigma) = \overline{\sigma}, \text{ unde } \overline{\sigma}(i) = \sigma(i), \text{ pentru } 1 \le i \le n-1 \text{ şi } \overline{\sigma}(n) = n.$$

Deci $|\mathbf{S}_{n-1}| = |\overline{\mathbf{S}}_{n-1}|$.

Vom demonstra prin inducţie după n că avem $|\mathbf{S}_n| = n!$. Pentru n = 1 este evident că $|\mathbf{S}_1| = 1 = 1!$. Să presupunem că $|\mathbf{S}_{n-1}| = (n-1)!$. Conform teoremei lui Lagrange avem că $|\mathbf{S}_n| = [\mathbf{S}_n : \overline{\mathbf{S}}_{n-1}]\,|\overline{\mathbf{S}}_{n-1}|$ adică, $|\mathbf{S}_n| = [\mathbf{S}_n : \overline{\mathbf{S}}_{n-1}]\,(n-1)!$.

Să calculăm indicele $[\mathbf{S}_n : \overline{\mathbf{S}}_{n-1}]$ al subgrupului $\overline{\mathbf{S}}_{n-1}$ în $\mathbf{S}_n$, adică numărul claselor de echivalenţă (la stânga) modulo $\overline{\mathbf{S}}_{n-1}$. Dacă $\sigma, \tau \in \mathbf{S}_n$, atunci $\sigma \equiv_s \tau \pmod{\overline{\mathbf{S}}_{n-1}}$ dacă şi numai dacă $\sigma^{-1}\tau \in \overline{\mathbf{S}}_{n-1}$, adică $\sigma^{-1}\tau(n) = n$ sau echivalent $\tau(n) = \sigma(n)$. Deci există n clase de echivalenţa (la stânga):

$$[\sigma_1], [\sigma_2], \dots, [\sigma_n],$$

unde $[\sigma_i] = \{\sigma \in \mathbf{S}_n \mid \sigma(n) = i\}$, oricare ar fi i = 1, 2, ... , n. Aşadar, $[\mathbf{S}_n : \overline{\mathbf{S}}_{n-1}] = n$ şi deci

$$|\mathbf{S}_n| = n\,(n-1)! = n!.$$

Definiţia 7.3. Fie $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$ o permutare de n elemente. O pereche (i, j) se numeşte *inversiune* a permutării σ dacă $i < j$ şi $\sigma(i) > \sigma(j)$. Notăm cu inv(σ) numărul inversiunilor permutării σ.

Dacă $\sigma \in \mathbf{S}_n$ este o permutare, definim numărul

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

care se numeşte *semnul* (*signatura*) permutării σ.

Observăm că orice diferenţă $\sigma(j) - \sigma(i)$, cu $i < j$, de la numărătorul produsului din formula care defineşte ε(σ), se simplifică cu una dintre diferenţele de la numitor, care apare eventual cu semn schimbat dacă (i, j) este o inversiune. Deci ε(σ) este un produs de +1 şi –1, factorul –1 apărând de atâtea ori câte inversiuni are permutarea σ. Deci $\varepsilon(\sigma) = (-1)^{\mathrm{inv}(\sigma)}$.

O permutare σ se numeşte *pară* dacă ε(σ) = l, adică are un număr par de inversiuni şi se numeşte *impară* dacă ε(σ) = –1, adică are un număr impar de inversiuni.

Există permutări pare ca, de exemplu, permutarea identică. Vom arăta că pentru orice $n \ge 2$ există şi permutări impare.

Fie $n \ge 2$ şi $k, l \in \{1, 2, \dots, n\}$ cu $k \ne l$. Permutarea τ_{kl} definită prin

$$\tau_{kl}(k) = l,\ \tau_{kl}(l) = k,\ \tau_{kl}(i) = i, \text{ dacă } i \ne k \text{ şi } i \ne l,$$

se numeşte *transpoziţie*. Transpoziţia τ_{kl} se mai notează (k l).

Propoziţia 7.4. Dacă $n \geq 2$ este un număr natural, atunci orice transpoziţie din $\mathbf{S}_n$ este permutare impară.

Demonstraţie. Fie transpoziţia (k l) şi să presupunem că $k < l$. Atunci

$$(k\ l) = \begin{pmatrix} 1 & 2 & \ldots & k-1 & k & \ldots & l-1 & l & \ldots & n \\ 1 & 2 & \ldots & k-1 & l & \ldots & l-1 & k & \ldots & n \end{pmatrix}$$

şi numărul de inversiuni este $(l - k) + (l - k - 1) = 2(l - k) - l$. Deci $\varepsilon((k, l)) = -1$.

Propoziţia 7.5. Dacă $n \geq 2$ este un număr natural, funcţia

$$\varepsilon : \mathbf{S}_n \to \{-1, 1\},$$

de la grupul permutărilor $\mathbf{S}_n$ la grupul multiplicativ $\{-1, 1\}$, este un morfism surjectiv de grupuri.

Demonstraţie. Fie $\sigma, \tau \in \mathbf{S}_n$. Deoarece $\tau(1), \tau(2), \ldots, \tau(n)$ sunt numerele 1, 2, … , n, eventual într-o altă ordine şi cum în produsul care-l dă pe $\varepsilon(\sigma)$ diferenţele de la numitor se pot face şi în altă ordine decât cea din definiţie, rezultă că avem

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}.$$

Atunci:

$$\varepsilon(\sigma \circ \tau) = \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} = \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \frac{\tau(j) - \tau(i)}{j - i} =$$

$$= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \prod_{1 \leq i < j \leq n} \frac{\tau(j) - \tau(i)}{j - i} = \varepsilon(\sigma)\, \varepsilon(\tau),$$

deci ε este un morfism de grupuri. Deoarece orice transpoziţie este impară, iar permutarea identică este pară, rezultă că ε este surjectiv.

Definiţia 7.6. Să notăm cu $A_n = \{\sigma \in \mathbf{S}_n \mid \varepsilon(\sigma) = 1\}$, mulţimea permutărilor pare din $\mathbf{S}_n$. Este clar că A_n este un subgrup (normal) al lui $\mathbf{S}_n$, deci la rândul său este grup, numit *grupul altern de grad n*.

Evident $A_n = \mathrm{Ker}\ \varepsilon$ şi din teorema fundamentală de izomorfism pentru grupuri rezultă că grupul factor $\mathbf{S}_n/A_n$ este izomorf cu grupul multiplicativ $\{-1, 1\}$, deci indicele $[\mathbf{S}_n : A_n]$ este 2.

Corolarul 7.7. A_n are n!/2 elemente.

Definiţia 7.8. O permutare $\sigma \in \mathbf{S}_n$ se numeşte *ciclu de lungime m*, $2 \le m \le n$, dacă există m numere $i_1, i_2, \ldots, i_m \in \{1, 2, \ldots, n\}$ astfel încât să avem:

1° oricare ar fi $i \notin \{i_1, i_2, \ldots, i_m\}$, $\sigma(i) = i$,

2° $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3, \ldots, \sigma(i_{m-1}) = i_m$, $\sigma(i_m) = i_1$.

Acest ciclu

$$\sigma = \begin{pmatrix} 1 & \ldots & i_1 & \ldots & i_2 & \ldots & i_3 & \ldots & i_{m-1} & \ldots & i_m & \ldots & n \\ 1 & \ldots & i_2 & \ldots & i_3 & \ldots & i_4 & \ldots & i_m & \ldots & i_1 & \ldots & n \end{pmatrix}$$

îl vom nota $\sigma = (i_1\ i_2\ \ldots\ i_m)$.

Observăm că la orice sistem de m numere $i_1, i_2, \ldots, i_m$ cuprinse între 1 şi n putem să asociem cel puţin un ciclu de lungime m şi, mai mult,

$$(i_1\ i_2\ \ldots\ i_m) = (i_2\ i_3\ \ldots\ i_m\ i_1) = \ldots = (i_m\ i_1\ \ldots\ i_{m-1}).$$

Aşadar, numărul ciclilor de lungime m, $2 \le m \le n$, este $C_n^m\,(m-1)!$. De exemplu, orice transpoziţie este un ciclu de lungime 2. Prin urmare, rezultă că numărul transpoziţiilor din grupul $\mathbf{S}_n$ este C_n^2.

Propoziţia 7.9. Dacă $\sigma = (i_1\ i_2\ \ldots\ i_m) \in \mathbf{S}_n$ este un ciclu de lungime m, atunci

1) $\sigma^{-1} = (i_m\ i_{m-1}\ \ldots\ i_1)$,

2) $\mathrm{ord}(\sigma) = m$.

Demonstraţie. 1) Se verifică imediat.

2) Din definiţia ciclului obţinem că $\sigma^k(i_1) = i_{k+1}$ pentru orice $1 \le k \le m-1$ şi $\sigma^m(i_1) = i_1$. Deoarece $i_1 \ne i_k$, pentru orice $2 \le k \le m$, avem că $\sigma^k \ne e$, pentru orice $1 \le k \le m-1$. Să arătăm că $\sigma^m = e$. Dacă $i \notin \{i_1, i_2, \ldots, i_m\}$, atunci $\sigma(i) = i$ şi deci $\sigma^m(i) = i$. Dacă $i = i_1$ am observat că $\sigma^m(i_1) = i_1$, iar dacă $i = i_{k+1}$, $1 \le k \le m-1$, atunci $\sigma^m(i) = \sigma^m(\sigma^k(i_1)) = \sigma^k(\sigma^m(i_1)) = \sigma^k(i_1) = i$. Deci oricare ar fi i, $1 \le i \le n$, avem că $\sigma^m(i) = i$, adică $\sigma^m = e$. Am demonstrat astfel că $\mathrm{ord}(\sigma) = m$.

Propoziţia 7.10. Fie $\sigma, \tau \in \mathbf{S}_n$, iar A, B două submulţimi nevide şi disjuncte ale mulţimii $\{1, 2, \ldots, n\}$ astfel încât:

1. Dacă $s \notin A$, atunci $\sigma(s) = s$, iar dacă $s \in A$, atunci $\sigma(s) \in A$;
2. Dacă $t \notin B$, atunci $\tau(t) = t$, iar dacă $t \in B$, atunci $\tau(t) \in B$.

Atunci $\sigma\tau = \tau\sigma$ şi $\mathrm{ord}(\sigma\tau) = \text{c.m.m.m.c.}(\mathrm{ord}(\sigma), \mathrm{ord}(\tau))$.

Demonstraţie. Fie $r \in \{1, 2, \ldots, n\}$ un element oarecare. Dacă $r \notin A \cup B$ atunci $\sigma(r) = r$ şi $\tau(r) = r$ şi deci $(\sigma\tau)(r) = (\tau\sigma)(r) = r$. Presupunem că $r \in A \cup B$. Dacă $r \notin A$, atunci $r \in B$ şi deci $\tau(r) = r$. Avem $(\sigma\tau)(r) = \sigma(\tau(r)) = \sigma(r)$, iar $(\tau\sigma)(r) = \tau(\sigma(r))$. Dar cum $\sigma(r) \in A$, atunci $\sigma(r) \notin B$ şi deci $\sigma(\tau(r)) = \sigma(r)$. Rezultă că şi în acest caz $(\sigma\tau)(r) = (\tau\sigma)(r)$. Analog, dacă $r \in B$, rezultă $(\sigma\tau)(r) = (\tau\sigma)(r)$. Deci $(\sigma\tau)(r) = (\tau\sigma)(r)$, oricare ar fi $r \in \{1, 2, \ldots, n\}$, adică $\sigma\tau = \tau\sigma$.

Fie acum $\mathrm{ord}(\sigma) = k$, $\mathrm{ord}(\tau) = l$, $\mathrm{ord}(\sigma\tau) = m$ şi să notăm $u = \text{c.m.m.m.c.}(k, l)$. Avem $(\sigma\tau)^m = e$ şi cum $\sigma\tau = \tau\sigma$, rezultă $\sigma^m\tau^m = e$ sau $\sigma^m = \tau^{-m}$. Vom arăta că $\sigma^m = e =$

τ^m. Într-adevăr, dacă $\sigma^m \neq e$, atunci există $r \in \{l, 2, \dots, n\}$ astfel încât $\sigma^m(r) \neq r$ şi deci neapărat $r \in A$. Din $\sigma^m(r) = \tau^{-m}(r)$, avem $\tau^{-m}(r) \neq r$, deci $\tau^m(r) \neq r$ şi deci neapărat $r \in B$. Aşadar $r \in A \cap B$, contradicţie cu faptul că $A \cap B = \emptyset$. Am obţinut astfel că $\sigma^m = e = \tau^m$.

Prin urmare, $k \mid m$ şi $l \mid m$ şi deci $u \mid m$. Fie $k', l' \in \mathbf{N}$ astfel încât $u = kk'$ şi $u = ll'$. Deci $(\sigma\tau)^u = \sigma^u\tau^u = (\sigma^l)^{l'}(\tau^k)^{k'} = e$, de unde obţinem că $m \mid u$. Din $u \mid m$ şi $m \mid u$ rezultă că $m = u$ şi propoziţia este demonstrată.

Corolarul 7.11. Fie $\sigma \in \mathbf{S}_n$, $n \geq 2$, o permutare astfel încât $\sigma = \tau_1 \tau_2 \dots \tau_t$, unde $\tau_1, \tau_2, \dots, \tau_t$ sunt cicli disjuncţi. Atunci $\mathrm{ord}(\sigma) = \text{c.m.m.m.c.}(\mathrm{ord}(\tau_1), \mathrm{ord}(\tau_2), \dots, \mathrm{ord}(\tau_t))$.

Demonstraţie. Rezultă imediat prin generalizarea punctului 2 al propoziţiei de mai sus.

Definiţia 7.12. Ciclurile $\sigma = (i_1\ i_2\ \dots\ i_m)$ şi $\tau = (j_1\ j_2\ \dots\ j_k)$ se numesc *disjuncte* dacă

$$\{i_1, i_2, \dots, i_m\} \cap \{j_1, j_2, \dots, j_k\} = \emptyset.$$

Propoziţia precedentă aplicată în cazul ciclurilor disjuncte σ şi τ ne spune că

$$\sigma\tau = \tau\sigma \text{ şi } \mathrm{ord}(\sigma\tau) = \text{c.m.m.m.c.}(m, k).$$

Teorema 7.13. Orice permutare $\sigma \in \mathbf{S}_n$, $\sigma \neq e$, se descompune ca un produs finit de cicli disjuncţi. Mai mult, această descompunere este unică, abstracţie făcând de ordinea factorilor.

Demonstraţie. Fie n_σ numărul de elemente ale mulţimii $\{1, 2, \dots, n\}$ permutate efectiv de către σ, adică

$$n_\sigma = |\{i \mid \sigma(i) \neq i\}|.$$

Deoarece $\sigma \neq e$, există i astfel încât $\sigma(i) \neq i$ şi cum σ este injectivă avem $\sigma(\sigma(i)) \neq \sigma(i)$ şi deci $n_\sigma \geq 2$. Vom face demonstraţia prin inducţie după acest număr.

Dacă $\sigma \in \mathbf{S}_n$, astfel încât $n_\sigma = 2$, atunci există $i \neq j$, astfel încât $\sigma(i) = j$, $\sigma(j) = i$ şi $\sigma(k) = k$ oricare ar fi $k \neq i$ şi $k \neq j$. În acest caz σ este transpoziţia $(i\ j)$.

Presupunem teorema adevărată pentru toate permutările τ care permută efectiv mai puţin de n_σ elemente, adică $n_\tau < n_\sigma$, şi să arătăm că ea este adevărată şi pentru σ.

Dacă $i_1 \in \{1, 2, \dots, n\}$ astfel încât $\sigma(i_1) \neq i_1$, notăm $i_2 = \sigma(i_1), \dots, i_{k+1} = \sigma(i_k), \dots$. Este clar că $i_{k+1} = \sigma^k(i_1)$, oricare ar fi $k \geq 1$. Dacă $t = \mathrm{ord}(\sigma)$, atunci $\sigma^t = e$ şi deci $\sigma^t(i_1) = i_1$, adică $i_{t+1} = i_1$. Din proprietatea de bună ordonare a mulţimii $\mathbf{N}$ a numerelor naturale, există un cel mai mic număr natural nenul m cu proprietatea că $i_{m+1} = i_1$.

Numerele $i_1, i_2, \dots, i_m$ sunt distincte. Într-adevăr, dacă $i_r = i_s$, cu $r \neq s$, şi $1 \leq r, s \leq m$, atunci $\sigma^{r-1}(i_1) = \sigma^{s-1}(i_1)$. Să presupunem că $r > s$ şi fie $p = r - s$. Atunci $\sigma^{r-s}(i_1) = i_1$, adică $\sigma^p(i_1) = i_1$ sau $i_{p+1} = i_1$. Dar egalitatea $i_{p+1} = i_1$, unde $0 < p < m$, este în contradicţie cu alegerea numărului m.

Fie acum ciclul $\tau = (i_1\ i_2\ \dots\ i_m)$ şi să considerăm permutarea $\sigma' = \tau^{-1}\sigma$. Dacă $\sigma(i) = i$, atunci $i \notin \{i_1, i_2, \dots, i_m\}$ şi deci $\tau^{-1}(i) = i$, de unde $\sigma'(i) = i$. Mai mult, dacă $i_k \in \{i_1, \dots, i_m\}$ este clar că $\sigma'(i_k) = (\tau^{-1}\sigma)(i_k) = \tau^{-1}(\sigma(i_k)) = i_k$ şi deci, în plus, elementele $i_1, i_2, \dots,$

i_m rămân neschimbate dacă le aplicăm permutarea σ'. Aşadar $n_{\sigma'} < n_\sigma$ şi conform ipotezei de inducţie există ciclurile disjuncte $\tau_2, \tau_3, \ldots, \tau_t$ astfel încât $\sigma' = \tau_2 \tau_3 \ldots \tau_t$ sau $\tau^{-1}\sigma = \tau_2 \tau_3 \ldots \tau_t$, de unde $\sigma = \tau\ \tau_2\ \tau_3 \ldots \tau_t$. Mai mult, din demonstraţie rezultă că ciclul τ este disjunct de fiecare din ciclurile disjuncte $\tau_2, \tau_3, \ldots, \tau_t$. Notând $\tau_1 = \tau$ obţinem descompunerea $\sigma = \tau_1\ \tau_2\ \tau_3 \ldots \tau_t$ în produs de cicli disjuncţi. Tot din demonstraţie se observă că această descompunere este unică, abstracţie făcând de ordinea factorilor.

Propoziţia 7.14. Orice ciclu din $\mathbf{S}_n$ este un produs de transpoziţii.

Demonstraţie. Dacă $\sigma = (i_1\ i_2 \ldots i_m)$ este un ciclu de lungime m, atunci prin calcul direct rezultă

$$\sigma = (i_1 i_m)(i_1\ i_{m-1}) \ldots (i_1\ i_2) = (i_1\ i_2)(i_2\ i_3) \ldots (i_{m-1}\ i_m).$$

Corolarul 7.15. Orice permutare $\sigma \in \mathbf{S}_n$, $n \geq 2$, este produs de transpoziţii.

Demonstraţie. Dacă $\sigma = e$, atunci $\sigma = e = (1, 2)(1, 2)$. Dacă $\sigma \neq e$, afirmaţia rezultă din teorema şi propoziţia de mai sus.

Observaţie. Din cele de mai sus se observă că descompunerea unei permutări în produs de transpoziţii nu este unică, în schimb paritatea numărului de transpoziţii care apar în orice descompunere a unei permutări este aceeaşi. Într-adevăr, fie $\sigma = \tau_1\ \tau_2 \ldots \tau_t = \sigma_1\ \sigma_2 \ldots \sigma_s$, unde $\tau_1, \tau_2, \ldots, \tau_t$ şi $\sigma_1, \sigma_2, \ldots, \sigma_s$ sunt transpoziţii. Ţinând cont că semnul unei transpoziţii este -1, obţinem $\varepsilon(\sigma) = (-1)^t = (-1)^s$, de unde rezultă că r şi s sunt în acelaşi timp pare sau impare.

Aplicaţie. Fie permutarea $\sigma \in \mathbf{S}_{10}$, unde

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

Să scriem permutarea σ ca produs de cicli disjuncţi şi ca produs de transpoziţii. De asemenea, să determinăm ordinul permutării σ.

Considerăm numărul 1 care este permutat efectiv de σ, deoarece $\sigma(1) = 3$. Cum $\sigma(3) = 1$ obţinem $\tau_1 = (1\ 3)$. Considerăm acum următorul număr care este permutat efectiv de σ şi care nu aparţine mulţimii $\{1, 3\}$. Acesta este 2. Cum $\sigma(2) = 5$, $\sigma(5) = 7$, $\sigma(7) = 8$, $\sigma(8) = 2$ obţinem ciclul $\tau_2 = (2\ 5\ 7\ 8)$. Fie acum numărul 6 care este permutat efectiv de σ. Avem $\sigma(6) = 10$, $\sigma(10) = 9$, $\sigma(9) = 6$ şi astfel obţinem ciclul $(6\ 10\ 9)$. Deci σ se scrie ca produs de cicluri disjuncte astfel: $\sigma = (1\ 3)\ (2\ 5\ 7\ 8)\ (6\ 10\ 9)$.

Din ultima propoziţie a acestui paragraf rezultă că σ se poate scrie ca produs de transpoziţii astfel: $\sigma = (1\ 3)\ (2\ 8)\ (2\ 7)\ (2\ 5)\ (6\ 9)\ (6\ 10)$.

În final avem $\text{ord}(\sigma) = \text{c.m.m.m.c.}(2, 4, 3) = 12$.