Descompunerea unei permutări în cicluri disjuncte

Lect.dr. M.Chiş
Universitatea de Vest din Timişoara

Viitori Olimpici ediţia a 9-a, etapa I, clasa a XI-a

Vom considera pentru un $n \in \mathbb{N}^*$ oarecare grupul simetric S_n al tuturor permutărilor mulţimii $\{1, 2, \ldots, n\}$, numite şi permutări de grad n, cu înmulţirea dată de compunerea permutărilor.

Definiţie 1. O permutare $\sigma \in S_n$ se numeşte *permutare ciclică* sau *ciclu* dacă există elemente $i_1, i_2, \ldots, i_l \in \{1, 2, \ldots, n\}$ cu proprietatea că $\sigma(i_k) = i_{k+1}$, $(\forall)k = \overline{1, l}$, unde $i_{l+1} = i_1$, iar $\sigma(j) = j$, $(\forall)j \notin \{i_1, i_2, \ldots, i_l\}$. Vom nota cu $(i_1, i_2, \ldots, i_l)$ această permutare ciclică, iar numărul l se va numi *lungimea ciclului*.

Observaţie 2. Evident, dacă $l = 1$, atunci $(i_1) = id$, permutarea identică. Scrierea unui ciclu de lungime $l \geq 2$ nu este unică, deoarece $(i_1, i_2, \ldots, i_l) = (i_j, i_{j+1}, \ldots, i_l, i_1, \ldots, i_{j-1})$, $(\forall)j \in \overline{2, l}$. Abstracţie făcând însă de alegerea primului element, ordinea succesivă a elementelor determină ciclul în mod unic.

Definiţie 3. *Ordinul unei permutări* $\sigma \in S_n$, pe care îl vom nota $ord(\sigma)$, este cel mai mic număr $m \in \mathbb{N}^*$, cu proprietatea că $\sigma^m = id$.

Observaţie 4. Are loc următoarea caracterizare a ordinului unei permutări:

$$ord(\sigma) = m \Longleftrightarrow [\sigma^t = id \Longleftrightarrow m|t].$$

Propoziţie 5. *Dacă $ord(\sigma) = m$, atunci $ord(\sigma^k) = \frac{m}{(m,k)}$, $(\forall)k \in \mathbb{Z}$.*

Demonstraţie. Avem echivalenţele $(\sigma^k)^t = id \Longleftrightarrow m|kt \Longleftrightarrow \frac{m}{(m,k)}|\frac{k}{(m,k)}t \Longleftrightarrow \frac{m}{(m,k)}|t$. De aici rezultă afirmaţia din enunţ. $\square$

Observaţie 6. Dacă $c = (i_1, i_2, \ldots, i_l)$ este un ciclu de lungime l, atunci $c^k(i_j) = i_{j+k}$, $(\forall)j = \overline{1, l}$(indicii fiind calculaţi modulo l). Obţinem că $c^l = id$, iar $c^k \neq id$, $(\forall)1 \leq k < l$. Astfel, $ord(c) = l$.

Notaţie 7. Pentru o permutare $\sigma \in S_n$ vom nota cu $F(\sigma) = \{i \in \{1, 2, \ldots, n\} | \, \sigma(i) = i\}$ mulţimea punctelor fixe ale lui σ, respectiv cu $M(\sigma) = \{i \in \{1, 2, \ldots, n\} | \, \sigma(i) \neq i\}$ mulţimea punctelor ”mişcate” de permutarea σ.

Observaţie 8. Pentru orice permutări $\alpha, \beta \in S_n$ avem că $F(\alpha) \cap F(\beta) \subseteq F(\alpha\beta)$.

Definiţie 9. Două permutări $\alpha, \beta \in S_n$ se numesc *disjuncte* dacă $M(\alpha) \cap M(\beta) = \emptyset$.

Observaţie 10. Condiţia ca două permutări $\alpha, \beta \in S_n$ să fie disjuncte se poate exprima echivalent şi prin $M(\alpha) \subseteq F(\beta)$(sau, prin simetrie, $M(\beta) \subseteq F(\alpha)$).

Propoziţie 11. *Oricare două permutări disjuncte $\alpha, \beta \in S_n$ comută, i.e. verifică egalitatea $\alpha\beta = \beta\alpha$.*

Demonstraţie. Dacă $\alpha, \beta \in S_n$ sunt disjuncte, atunci pentru orice $i \in M(\beta)$ rezultă că $\beta(i) \in M(\beta) \subseteq F(\alpha)$ şi obţinem că

$$\alpha\beta(i) = \begin{cases} i & , \text{ dacă } i \in F(\alpha) \cap F(\beta) \\ \beta(i) & , \text{ dacă } i \in M(\beta) \\ \alpha(i) & , \text{ dacă } i \in M(\alpha) \end{cases} = \beta\alpha(i), \ (\forall)i \in \{1, 2, \ldots, n\}.$$

$\square$

Corolar 12. Dacă permutările $\alpha_1, \alpha_2, \ldots, \alpha_k \in S_n$ sunt disjuncte două câte două, produsul lor nu depinde de ordinea factorilor.

Propoziţie 13. *Orice permutare se poate scrie în mod unic ca produs de cicluri disjuncte.*

Demonstraţie. Fie $\sigma \in S_n$ o permutare oarecare. Pentru orice $i \in \{1,2,\ldots,n\}$ există un cel mai mic $l_i \in \mathbb{N}^*$, astfel încât $\sigma^{l_i}(i) = i$. Pentru orice $i, j \in \{1,2,\ldots,n\}$ ciclurile (unic determinate) $(i, \sigma(i), \sigma^2(i), \ldots, \sigma^{l_i-1}(i))$ şi $(j, \sigma(j), \sigma^2(j), \ldots, \sigma^{l_j-1}(j))$ sunt atunci fie egale, fie disjuncte. Produsul tuturor acestor cicluri, considerat fiecare o singură dată, este atunci exact permutarea σ. $\square$

Propoziţie 14. *Dacă $\sigma = c_1c_2\ldots c_k$ este descompunerea unei permutări $\sigma \in S_n$ în cicluri disjuncte, ordinul său este dat de $ord(\sigma) = [l(c_1), l(c_2), \ldots, l(c_k)]$.*

Demonstraţie. Deoarece ciclurile disjuncte comută, avem că $\sigma^m = c_1^m c_2^m \ldots c_k^m$ şi obţinem că $\sigma^t = id \iff c_j^t = id, (\forall) j = \overline{1,k} \iff l(c_j)|t, (\forall) j = \overline{1,k} \iff [l(c_1), l(c_2), \ldots, l(c_k)]|t$. Echivalenţa arată că $ord(\sigma) = [l(c_1), l(c_2), \ldots, l(c_k)]$. $\square$

Propoziţie 15. *Dacă c este un ciclu de lungime l, iar $k \in \mathbb{Z}$ este prim cu l, atunci c^k este de asemenea un ciclu de lungime l.*

Demonstraţie. Fie $c = (i_1, i_2, \ldots, i_l)$. Cum $(k,l) = 1$, pentru orice $1 \le j < l$ există $u \in \mathbb{Z}$ astfel încât $ku \equiv j (\text{mod } l)$. Rezultă că $(c^k)^u(i_t) = i_{t+j}, (\forall) t = \overline{1,l}$, astfel că elementele $i_1, i_2, \ldots, i_l$ fac parte dintr-un acelaşi ciclu al permutării c^k. Cum $F(c) \subseteq F(c^k)$, rezultă afirmaţia din enunţ. $\square$

Propoziţie 16. *Dacă c este un ciclu de lungime l, iar $d \in \mathbb{N}$ este un divizor al lui l, atunci c^d se descompune într-un produs de d cicluri disjuncte de lungime $\frac{l}{d}$.*

Demonstraţie. Dacă $c = (i_1, i_2, \ldots, i_l)$, pentru orice $j = \overline{1,l}$ şi orice $1 \le k \le \frac{l}{d}$ avem că $(c^d)^k(i_j) = i_{j+kd}$. Rezultă că

$$c^d = \prod_{j=1}^{d} (i_j, i_{j+d}, i_{j+2d}, \ldots, i_{j+l-d}).$$

$\square$

Propoziţie 17. *Dacă c este un ciclu de lungime l, iar $k \in \mathbb{Z}$ are proprietatea că $(l,k) = d$, atunci c^k se decompune în d cicluri de lungime $\frac{l}{d}$.*

Demonstraţie. Fie $l_1 \in \mathbb{N}$ şi $k_1 \in \mathbb{Z}$, astfel încât $l = d \cdot l_1$ şi $k = d \cdot k_1$. Avem atunci că $(l_1, k_1) = 1$, c^d este un produs de d cicluri disjuncte de lungime l_1 şi rezultă că $c^k = (c^d)^{k_1}$ este un produs de d cicluri de lungime l_1. $\square$

Propoziţie 18. *Dacă $c = (i_1, i_2, \ldots, i_l)$ şi α sunt două permutări de grad n, atunci*

$$\alpha \cdot c \cdot \alpha^{-1} = (\alpha(i_1), \alpha(i_2), \ldots, \alpha(i_l)).$$

Demonstraţie. Pentru orice $k = \overline{1,l}$ avem că $(\alpha \cdot c \cdot \alpha^{-1})(\alpha(i_k)) = \alpha(c(i_k)) = \alpha(i_{k+1})$. De asemenea, pentru orice $j \in \{1,2,\ldots,n\} \setminus \{i_1, i_2, \ldots, i_l\}$ avem $(\alpha \cdot c \cdot \alpha^{-1})(\alpha(j)) = \alpha(c(j)) = \alpha(j)$. Deducem astfel egalitata din enunţul propoziţiei. $\square$

Observaţie 19. Dacă $\sigma, \alpha \in S_n$ sunt permutări de grad n, iar σ se descompune în produs de cicluri disjuncte sub forma $\sigma = c_1c_2\ldots c_k$, rezultă că $\alpha\sigma\alpha^{-1} = \alpha c_1 \alpha^{-1} \cdot \alpha c_2 \alpha^{-1} \cdot \ldots \alpha c_k \alpha^{-1}$. Astfel, formula din propoziţia de mai sus permite calculul conjugatei unei permutări σ printr-o permutare α(i.e., al produsului $\alpha\sigma\alpha^{-1}$).

Propoziţie 20. *Un ciclu $c = (i_1, i_2, \ldots, i_l)$ se poate descompune în produs de transpoziţii(=cicluri de lungime 2) sub forma $c = (i_1, i_l)(i_1, i_{l-1})\ldots(i_1, i_3)(i_1, i_2)$.*

Demonstraţie. Notând $t_k = (i_1, i_k)$ pentru $k = \overline{2,l}$, avem că

$$t_l t_{l-1} \ldots t_3 t_2(i_1) = t_l t_{l-1} \ldots t_3(i_2) = i_2,$$

$$t_l t_{l-1} \ldots t_3 t_2(i_k) = t_l t_{l-1} \ldots t_{k+1} t_k(i_k) = t_l t_{l-1} \ldots t_{k+1}(i_1) t_l t_{l-1} \ldots t_{k+2}(i_{k+1}) = i_{k+1} \quad, (\forall) k = \overline{2,l}, \text{ respectiv}$$

$$t_l t_{l-1} \ldots t_3 t_2(j) = j \quad, (\forall) j \in \{1,2,\ldots,n\} \setminus \{i_1, i_2, \ldots, i_l\}.$$

Rezultă că $t_l t_{l-1} \ldots t_3 t_2 = (i_1, i_2, \ldots, i_l) = c$.

$\square$

Corolar 21. Orice permutare se descompune în produs de transpoziţii.

Observaţie 22. Au loc identităţile:

$$(a, i_2, \ldots, i_k)(b, j_1, \ldots, j_l)(a, b) = (a, j_1, \ldots, j_l, b, i_1, \ldots, i_k)$$
$$(a, j_1, \ldots, j_l, b, i_1, \ldots, i_k)(a, b) = (a, i_2, \ldots, i_k)(b, j_1, \ldots, j_l)\,,$$

astfel că înmulţind o permutare σ cu o transpoziţie τ, numărul ciclurilor disjuncte ale lui $\sigma\tau$ diferă de cel al lui σ cu exact unul.

Corolar 23. *Dacă $\sigma \in S_n$ se descompune în exact k cicluri disjuncte, atunci numărul minim de transpoziţii în care se descompune σ este $n - k$.*

Definiţie 24. O *inversiune a unei permutări* $\alpha \in S_n$ este o pereche $(i, j) \in \{1, 2, \ldots, n\}^2$ cu proprietatea că $i < j$ şi $\alpha(i) > \alpha(j)$. Notând cu $inv(\alpha)$ numărul inversiunii permuării α, *signatura permutării* α este

$$sgn(\alpha) = (-1)^{inv(\alpha)}.$$

O permutare se numeşte pară dacă are un număr par de inversiuni şi deci sinatura $+1$, respectiv impară dacă numărul inversiunilor sale este impar, iar signatura -1.

Observaţie 25. Orice transpoziţie are un număr impar de inversiuni. Într-adevăr, dacă $t = (i, j)$ este o transpoziţie, cu $i < j$, atunci inversiunile permutării t sunt date de perechea (i, j) şi toate perechile de forma (i, k) şi (k, j), unde $i < k < j$. Numărul acestora este $1 + 2(j - i - 1)$, deci impar. În consecinţă, orice transpoziţie este o permutare impară şi are signatura -1.

Observaţie 26. Direct din definiţie rezultă că

$$sgn(\alpha) = \prod_{\{i,j\} \subseteq \{1,2,\ldots,n\}} \frac{\alpha(i) - \alpha(j)}{i - j}.$$

Propoziţie 27. *Pentru orice $\alpha, \beta \in S_n$ are loc egalitatea $sgn(\alpha\beta) = sgn(\alpha) \cdot sgn(\beta)$.*

Demonstraţie. Ţinând cont de observaţia de mai sus, precum şi de faptul că pentru bijecţia β, atunci când submulţimile $\{i, j\}$ parcurg toate submulţimile cu 2 elemente ale lui $[1, n] \cap \mathbb{N}$ şi $\{\beta(i), \beta(j)\}$ vor parcurge toate aceste submulţimi, avem că

$$\begin{aligned} sgn(\alpha\beta) &= \prod_{\{i,j\} \subseteq \{1,2,\ldots,n\}} \frac{\alpha\beta(i) - \alpha\beta(j)}{i - j} = \prod_{\{i,j\} \subseteq \{1,2,\ldots,n\}} \frac{\alpha\beta(i) - \alpha\beta(j)}{\beta(i) - \beta(j)} \cdot \frac{\beta(i) - \beta(j)}{i - j} = \\ &= \prod_{\{i,j\} \subseteq \{1,2,\ldots,n\}} \frac{\alpha\beta(i) - \alpha\beta(j)}{\beta(i) - \beta(j)} \cdot \prod_{\{i,j\} \subseteq \{1,2,\ldots,n\}} \frac{\beta(i) - \beta(j)}{i - j} = \\ &= \prod_{\{k,l\} \subseteq \{1,2,\ldots,n\}} \frac{\alpha(k) - \alpha(l)}{k - l} \cdot \prod_{\{i,j\} \subseteq \{1,2,\ldots,n\}} \frac{\beta(i) - \beta(j)}{i - j} = sgn(\alpha) \cdot sgn(\beta). \end{aligned}$$

□

Corolar 28. Produsul a două permutări pare este o permutare pară.

Corolar 29. Paritatea unei permutări este dată de numărul de transpoziţii dintr-o descompunere a permutării în produs de transpoziţii.

Corolar 30. Un ciclu c de lungime $l(c) = l$ este permutare pară dacă şi numai dacă l este un număr impar.

Corolar 31. O permutare este pară dacă şi numai dacă în descompunerea sa în produs de cicluri disjuncte, numărul ciclurilor de lungime pară este par.

Propoziţie 32. *Fie $\sigma \in S_n$ o permutare de grad n având descompunerea în cicluri disjuncte(inclusiv ciclurile de lungime 1, corespunzătoare punctelor fixe ale lui σ) $\sigma = c_1c_2 \dots c_k$. Atunci:*
a) $sgn(\sigma) = (-1)^{n-k}$.
b) dacă σ conţine în descompunerea de mai sus k_1 cicluri netriviale(i.e., de lungime ≥ 2), iar $|M(\sigma)| = m$, atunci $sgn(\sigma) = (-1)^{m-k_1}$.

Demonstraţie. a) $sgn(\sigma) = sgn(c_1c_2 \dots c_k) = sgn(c_1) \cdot sgn(c_2) \cdot \dots \cdot sgn(c_k) = (-1)^{l(c_1)-1} \cdot (-1)^{l(c_2)-1} \cdot \dots \cdot (-1)^{l(c_k)-1} = (-1)^{l(c_1)+l(c_2)+\dots+l(c_k)-k} = (-1)^{n-k}$.
b) Evident, $|F(\sigma)| = n - m = k - k_1$, astfel că $n - k = m - k_1$ şi deci $sgn(\sigma) = (-1)^{m-k_1}$. □

Observaţie 33. a) Dacă $c = (i_1, i_2, \dots, i_l)$ este o permutare ciclică, inversa sa este $c^{-1} = (i_l, i_{l-1}, \dots, i_2, i_1)$.
b) Dacă $\sigma \in S_n$ are descompunerea în cicluri disjuncte $\sigma = c_1c_2 \dots c_k$, atunci $\sigma^{-1} = c_1^{-1}c_2^{-1} \dots c_k^{-1}$.
c) Dacă $\sigma \in S_n$ se descompune în produs de transpoziţii sub forma $\sigma = t_1t_2 \dots t_m$, atunci $\sigma^{-1} = t_mt_{m-1} \dots t_2t_1$.

Corolar 34. Inversa unei permutări pare este o permutare pară.

Notaţie 35. $A_n = \{\sigma \in S_n | sgn(\sigma) = 1\}$ este mulţimea tuturor permutărilor pare de grad n(*grupul altern de grad* n).

Observaţie 36. Se pot verifica uşor următoarele identităţi:
a) $(i, j) = (1, i)(1, j)(1, i)$, $(\forall)i, j \geq 2, i \neq j$.
b) $(i, j) = (i, i+1)(i+1, i+2)(i+2, i+3) \dots (j-2, j-1)(j-1, j)(j-2, j-1) \dots (i+1, i+2)(i, i+1)$, $(\forall)1 \leq i < j \leq n$.

Corolar 37. a) Orice permutare de grad n se poate scrie ca produs de transpoziţii de forma $(1, i)$, cu $2 \leq i \leq n$. Spunem că S_n este generat de transpoziţiile $(1, i)$, $2 \leq i \leq n$.
b) Orice permutare de grad n se poate scrie ca produs de transpoziţii de forma $(i, i+1)$, cu $1 \leq i \leq n-1$.

Notaţie 38. Proprietăţile din corolarul de mai sus se pot scrie sub forma:
a) $S_n = \langle (1, i) | 2 \leq i \leq n \rangle$.
b) $S_n = \langle (i, i+1) | 1 \leq i \leq n-1 \rangle$.

Observaţie 39. Au loc identităţile:
a) $(i, j)(i, j) = id$.
b) $(i, j)(i, k) = (i, k, j)$.
c) $(i, j)(k, l) = (i, k, j)(i, k, l)$.

Corolar 40. $A_n = \langle (i, j, k) | i, j, k = \overline{1, n}, i \neq j \neq k \neq i \rangle$.

Observaţie 41. Au loc identităţile:
a) $(1, i, j) = (1, 2, j)(1, 2, j)(1, 2, i)(1, 2, j)$, $(\forall)i, j \geq 3, i \neq j$.
b) $(2, i, j) = (1, 2, i)(1, 2, j)(1, 2, i)(1, 2, i))$, $(\forall)i, j \geq 3, i \neq j$.
c) $(i, j, k) = (1, 2, k)(1, 2, i)(1, 2, j)(1, 2, k)(1, 2, i)$, $(\forall)i, j, k \geq 3, i \neq j \neq k \neq i$.

Corolar 42. $A_n = \langle (1, 2, i) | 3 \leq i \leq n \rangle$.