

Descompunerea unei permutări în cicluri disjuncte

Lect.dr. M.Chis
Universitatea de Vest din Timișoara

Viitori Olimpici ediția a 8-a, etapa I, clasa a XI-a

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

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

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

Definiție 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 $\sigma^m = id$.

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

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

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

Demonstrație. Avem echivalențele $(\sigma^k)^t = id \iff m|kt \iff \frac{m}{(m,k)} | \frac{k}{(m,k)} t \iff \frac{m}{(m,k)} | t$. De aici rezultă afirmația din enunț. \square

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

Notație 7. Pentru o permutare $\sigma \in S_n$ vom nota cu $F(\sigma) = \{i \in \{1, 2, \dots, n\} | \sigma(i) = i\}$ mulțimea punctelor fixe ale lui σ , respectiv cu $M(\sigma) = \{i \in \{1, 2, \dots, n\} | \sigma(i) \neq i\}$ mulțimea punctelor "mișcate" de permutarea σ .

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

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

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

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

Demonstrație. Dacă $\alpha, \beta \in S_n$ sunt disjuncte, atunci pentru orice $i \in M(\beta)$ rezultă că $\beta(i) \in M(\beta) \subseteq F(\alpha)$ și obținem că

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

\square

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

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

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

Propoziție 14. Dacă $\sigma = c_1 c_2 \dots c_k$ este descompunerea unei permutări $\sigma \in S_n$ în cicluri disjuncte, ordinul său este dat de $\text{ord}(\sigma) = [l(c_1), l(c_2), \dots, l(c_k)]$.

Demonstrație. Deoarece ciclurile disjuncte comută, avem că $\sigma^m = c_1^m c_2^m \dots c_k^m$ și obținem că $\sigma^t = id \iff c_j^t = id, (\forall) j = \overline{1, k} \iff l(c_j) | t, (\forall) j = \overline{1, k} \iff [l(c_1), l(c_2), \dots, l(c_k)] | t$. Echivalența arată că $\text{ord}(\sigma) = [l(c_1), l(c_2), \dots, l(c_k)]$. \square

Propoziție 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 .

Demonstrație. Fie $c = (i_1, i_2, \dots, i_l)$. Cum $(k, l) = 1$, pentru orice $1 \leq j < l$ există $u \in \mathbb{Z}$ astfel încât $ku \equiv j \pmod{l}$. Rezultă că $(c^k)^u(i_t) = i_{t+j}, (\forall) t = \overline{1, l}$, astfel că elementele i_1, i_2, \dots, i_l fac parte dintr-un același ciclu al permutării c^k . Cum $F(c) \subseteq F(c^k)$, rezultă afirmația din enunț. \square

Propoziție 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 $\frac{l}{d}$.

Demonstrație. Dacă $c = (i_1, i_2, \dots, i_l)$, pentru orice $j = \overline{1, l}$ și orice $1 \leq k \leq \frac{l}{d}$ avem că $(c^d)^k(i_j) = i_{j+kd}$. Rezultă că

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

\square

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

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

Propoziție 18. Dacă $c = (i_1, i_2, \dots, i_l)$ și α sunt două permutări de grad n , atunci

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

Demonstrație. 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 $j \in \{1, 2, \dots, n\} \setminus \{i_1, i_2, \dots, i_l\}$ avem $(\alpha \cdot c \cdot \alpha^{-1})(\alpha(j)) = \alpha(c(j)) = \alpha(j)$. Deducem astfel egalitatea din enunțul propoziției. \square

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

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

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

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

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

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

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

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

Observație 22. Au loc identitățile:

$$\begin{aligned} (a, i_2, \dots, i_k)(b, j_1, \dots, j_l)(a, b) &= (a, j_1, \dots, j_l, b, i_1, \dots, i_k) \\ (a, j_1, \dots, j_l, b, i_1, \dots, i_k)(a, b) &= (a, i_2, \dots, i_k)(b, j_1, \dots, j_l), \end{aligned}$$

astfel că înmulțind o permutare σ cu o transpoziție 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 transpoziții în care se descompune σ este $n - k$.

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

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

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

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

Observație 26. Direct din definiție rezultă că

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

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

Demonstrație. Ținând cont de observația de mai sus, precum și de faptul că pentru bijecția β , atunci când submulțimile $\{i, j\}$ parcurg toate submulțimile cu 2 elemente ale lui $[1, n] \cap \mathbb{N}$ și $\{\beta(i), \beta(j)\}$ vor parcurge toate aceste submulțimi, avem că

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

□

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

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

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

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

Propoziție 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) $\sigma = c_1 c_2 \dots c_k$. Atunci:

a) $\text{sgn}(\sigma) = (-1)^{n-k}$.

b) dacă σ conține în descompunerea de mai sus k_1 cicluri netriviiale (i.e., de lungime ≥ 2), iar $|M(\sigma)| = m$, atunci $\text{sgn}(\sigma) = (-1)^{m-k_1}$.

Demonstrație. a) $\text{sgn}(\sigma) = \text{sgn}(c_1 c_2 \dots c_k) = \text{sgn}(c_1) \cdot \text{sgn}(c_2) \cdot \dots \cdot \text{sgn}(c_k) = (-1)^{l(c_1)-1} \cdot (-1)^{l(c_2)-1} \cdot \dots \cdot (-1)^{l(c_k)-1} = (-1)^{l(c_1)+l(c_2)+\dots+l(c_k)-k} = (-1)^{n-k}$.

b) Evident, $|F(\sigma)| = n - m = k - k_1$, astfel că $n - k = m - k_1$ și deci $\text{sgn}(\sigma) = (-1)^{m-k_1}$. □

Observație 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 $\sigma = c_1 c_2 \dots c_k$, atunci $\sigma^{-1} = c_1^{-1} c_2^{-1} \dots c_k^{-1}$.

c) Dacă $\sigma \in S_n$ se descompune în produs de transpoziții sub forma $\sigma = t_1 t_2 \dots t_m$, atunci $\sigma^{-1} = t_m t_{m-1} \dots t_2 t_1$.

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

Notăție 35. $A_n = \{\sigma \in S_n \mid \text{sgn}(\sigma) = 1\}$ este mulțimea tuturor permutărilor pare de grad n (grupul altern de grad n).

Observație 36. Se pot verifica ușor următoarele identități:

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 transpoziții de forma $(1, i)$, cu $2 \leq i \leq n$. Spunem că S_n este generat de transpozițiile $(1, i)$, $2 \leq i \leq n$.

b) Orice permutare de grad n se poate scrie ca produs de transpoziții de forma $(i, i+1)$, cu $1 \leq i \leq n-1$.

Notăție 38. Proprietățile din corolarul de mai sus se pot scrie sub forma:

a) $S_n = \langle (1, i) \mid 2 \leq i \leq n \rangle$.

b) $S_n = \langle (i, i+1) \mid 1 \leq i \leq n-1 \rangle$.

Observație 39. Au loc identitățile:

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

Observație 41. Au loc identitățile:

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