

CURSUL 11: GRUPURI DE PERMUTĂRI

G. MINCU

1. GRUPURI DE PERMUTĂRI

Reamintim din cursul 8 faptul că, dată fiind o mulțime nevidă A , $S_A = \{f \in A^A : f \text{ este bijectivă}\}$ este grup în raport cu operația de compunere.

Noi vom face în acest curs referire la grupurile $S_n \stackrel{\text{not}}{=} S_{\{1,2,\dots,n\}}$, $n \in \mathbb{N}^*$.

Observația 1. Pentru orice $n \in \mathbb{N}^*$ avem $|S_n| = n!$.

Observația 2. S_n este ciclic pentru $n \in \{1, 2\}$.

S_n este necomutativ pentru orice $n \geq 3$.

2. DESCOMPUNERI ALE PERMUTĂRIILOR

Definiția 3. O permutare $\sigma \in S_n$ se numește *ciclu* dacă există $k \in \mathbb{N}^*$ și $\{i_1, i_2, \dots, i_k\} \subset \{1, 2, \dots, n\}$ astfel încât $\sigma(i_r) = i_{r+1}$ pentru orice $r \in \{1, 2, \dots, k-1\}$, $\sigma(i_k) = i_1$, iar $\sigma(j) = j$ pentru orice $j \in \{1, 2, \dots, n\} \setminus \{i_1, i_2, \dots, i_k\}$. Notăm un astfel de ciclu prin (i_1, i_2, \dots, i_k) , numărul k se numește *lungimea* ciclului, iar mulțimea $\{i_1, i_2, \dots, i_k\}$ poartă numele de *orbita* ciclului.

Observația 4. $(i_1, i_2, \dots, i_k)^{-1} = (i_k, i_{k-1}, \dots, i_1)$.

Observația 5. Permutarea inversă unui ciclu este tot un ciclu!

Definiția 6. Numim *transpoziție* orice ciclu de lungime doi.

Observația 7. $(i_1, i_2, \dots, i_k) = (i_1, i_2)(i_2, i_3) \dots (i_{k-1}, i_k)$, deci orice ciclu este produs de transpoziții.

Definiția 8. Două cicluri din S_n se numesc *disjuncte* dacă orbitele lor sunt disjuncte.

Propoziția 9. Orice două cicluri disjuncte comută.

Demonstrație: Fie $c_1, c_2 \in S_n$ două cicluri disjuncte și $i \in \{1, 2, \dots, n\}$. Întrucât orbitele ciclurilor considerate sunt disjuncte, i nu poate aparține ambelor orbite.

Dacă $c_1(i) = i$, atunci $(c_1 c_2)(i) = c_1(c_2(i)) = c_2(i) = c_2(c_1(i)) =$

$(c_2c_1)(i)$.

Dacă $c_2(i) = i$, atunci $(c_2c_1)(i) = c_2(c_1(i)) = c_1(i) = c_1(c_2(i)) = (c_1c_2)(i)$. \square

Observația 10. Calcule similare celor din demonstrația propoziției 9 conduc la concluzia că pentru orice cicluri disjuncte¹ c_1, c_2, \dots, c_r și pentru orice $k \in \{1, 2, \dots, n\}$ există $j \in \{1, 2, \dots, r\}$ astfel încât $(c_1c_2 \dots c_r)(k) = c_j(k)$.

Teorema 11. Orice permutare din S_n se poate scrie ca produs de cicluri disjuncte. Abstracție făcând de ordinea factorilor, această scriere este unică.

Demonstrație: Pentru $\sigma \in S_n$ notăm $\mathcal{M}_\sigma = \{k : \sigma(k) \neq k\}$. Vom demonstra prin inducție după $m = |\mathcal{M}_\sigma|$ că orice permutare σ se poate scrie în mod unic ca produs de cicluri disjuncte ale căror orbite sunt conținute în \mathcal{M}_σ .

Dacă $e = c_1c_2 \dots c_r$ cu factorii din membrul drept cicluri disjuncte, atunci, conform observației 10, $c_1 = c_2 = \dots = c_r = e$. Acest lucru probează afirmația teoremei pentru $m = 0$.

Să considerăm acum o permutare $\sigma \in S_n$ cu $m = |\mathcal{M}_\sigma| > 0$. Există atunci $k \in \{1, 2, \dots, n\}$ cu $\sigma(k) \neq k$. Cum $k_\sigma \stackrel{\text{def}}{=} \{\sigma(k), \sigma^2(k), \dots\} \subset \{1, 2, \dots, n\}$, k_σ este finită, deci există $i < j$ astfel încât $\sigma^i(k) = \sigma^j(k)$, de unde $\sigma^{j-i}(k) = k$. Prin urmare, $\{t \in \mathbb{N}^* : \sigma^t(k) = k\} \neq \emptyset$; fie s cel mai mic element al acestei mulțimi. Este ușor de probat (temă!) relația $k_\sigma = \{k, \sigma(k), \dots, \sigma^{s-1}(k)\}$; punând $c \stackrel{\text{not}}{=} (k, \sigma(k), \dots, \sigma^{s-1}(k))$, constatăm că avem $\mathcal{M}_{c^{-1}\sigma} \subset \mathcal{M}_\sigma \setminus \{k\}$, deci $|\mathcal{M}_{c^{-1}\sigma}| < |\mathcal{M}_\sigma|$. Conform ipotezei de inducție, $c^{-1}\sigma$ se scrie ca un produs $c_1c_2 \dots c_r$ de cicluri disjuncte cu orbitele conținute în $\mathcal{M}_{c^{-1}\sigma}$; drept urmare, $cc_1c_2 \dots c_r$ este o descompunere a lui σ în produs de cicluri disjuncte cu orbitele incluse în \mathcal{M}_σ .

Pentru partea de unicitate, păstrând semnificațiile de mai sus pentru k și c, c_1, \dots, c_r , considerăm și scrierea $\sigma = \gamma_1\gamma_2 \dots \gamma_t$ ca produs de cicluri disjuncte. Având în vedere observația 10, există $j \in \{1, 2, \dots, n\}$ pentru care $\sigma(k) = \gamma_j(k)$. După o eventuală renumerotare, putem considera că $j = 1$. Ciclurile $\gamma_1, \gamma_2, \dots, \gamma_t$ fiind disjuncte, $c^u(k) = \sigma^u(k) = \gamma_1^u(k)$ pentru orice $u \in \mathbb{Z}$, de unde $\gamma_1 = c$. Compunând acum relația $cc_1c_2 \dots c_r = \gamma_1\gamma_2 \dots \gamma_t$ cu c^{-1} , obținem $c_1c_2 \dots c_r = \gamma_2\gamma_3 \dots \gamma_t$. În virtutea ipotezei de inducție, $\{c_1, c_2, \dots, c_r\} = \{\gamma_2, \gamma_3, \dots, \gamma_t\}$. Ținând cont și de unicitatea deja probată a scrierii lui e , demonstrația se încheie. \square

¹ sau chiar permutări arbitrare disjuncte, noțiunea definindu-se ca și în cazul ciclurilor

Corolarul 12. Orice permutare din S_n se poate scrie ca produs de transpoziții.

Observația 13. Spre deosebire de descompunerea în produs de cicluri disjuncte, descompunerea unei permutări în produs de transpoziții nu este unică.

Observația 14. $S_n = \langle \{(i, j) : 1 \leq i < j \leq n\} \rangle$.

Temă: Demonstrați că:

- i) $S_n = \langle (1, 2), (1, 3), \dots, (1, n) \rangle$.
- ii) $S_n = \langle (1, 2), (2, 3), \dots, (n-1, n) \rangle$.
- iii) $S_n = \langle (1, 2), (1, 2, \dots, n) \rangle$.

3. PERMUTĂRI PARE ȘI IMPARE. SIGNATURĂ

Definiția 15. Fie $\sigma \in S_n$, $n \geq 2$. O pereche (i, j) , unde $1 \leq i < j \leq n$ se numește *inversiune* a lui σ dacă $\sigma(i) > \sigma(j)$.

Definiția 16. Permutarea $\sigma \in S_n$ se numește *pară* dacă are un număr par de inversiuni; σ se numește *impară* dacă are un număr impar de inversiuni.

Propoziția 17. Orice transpoziție este permutare impară.

Demonstrație: Inversiunile transpoziției (i, j) , unde $1 \leq i < j \leq n$, sunt (i, k) , $k \in \{i+1, i+2, \dots, j\}$ și (l, j) , $l \in \{i+1, i+2, \dots, j-1\}$; numărul acestora este $(j-i) + (j-1-i) = 2(j-i) - 1$, care este impar. \square

Definiția 18. Prin *signatura* permutării $\sigma \in S_n$, $n \geq 2$, înțelegem numărul

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

Observația 19. În produsul din definiția 18 se simplifică de fapt toți numitorii și toți numărătorii, la numărători rămânând câte un -1 de fiecare dată când $\sigma(j) - \sigma(i) < 0$. Prin urmare,

$$\varepsilon(\sigma) = (-1)^{\text{Numărul inversiunilor lui } \sigma}$$

Corolarul 20. a) $\sigma \in S_n$ este pară dacă și numai dacă $\varepsilon(\sigma) = 1$.

b) $\sigma \in S_n$ este impară dacă și numai dacă $\varepsilon(\sigma) = -1$.

Propoziția 21. Pentru orice $\sigma, \tau \in S_n$ are loc relația $\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$.

Corolarul 22. ε este morfism de grupuri de la S_n la $(\{-1, 1\}, \cdot)$.

Corolarul 23. i) $\varepsilon(e) = 1$.
 ii) Pentru orice $\sigma \in S_n$ avem $\varepsilon(\sigma^{-1}) = \varepsilon(\sigma)$.

Observația 24. $\ker \varepsilon$ constă în permutările pare din S_n .

Corolarul 25. Permutările pare din S_n constituie un subgrup normal al lui S_n .

Notăm subgrupul permutărilor pare din S_n cu A_n .

Definiția 26. A_n se numește *grupul altern* de grad n .

Corolarul 27. $\frac{S_n}{A_n} \simeq \{-1, 1\}$.

Demonstrație: Aplicăm corolarul 22, observația 24 și teorema fundamentală de izomorfism pentru grupuri. \square

Corolarul 28. Pentru orice $n \geq 2$ avem $|A_n| = \frac{n!}{2}$.

Corolarul 29. i) Orice ciclu de lungime pară este impar.
 ii) Orice ciclu de lungime impară este par.

Demonstrație: Aplicăm observația 7 și propozițiile 17 și 21. \square

4. ORDINUL UNEI PERMUTĂRI

Observația 30. Ordinul oricărui ciclu este egal cu lungimea sa.

Demonstrație: Considerând un ciclu $\sigma = (i_1, i_2, \dots, i_k) \in S_n$, constatăm că $\sigma^j(i_1) = i_{j+1}$, deci $\sigma^j \neq e$, pentru orice $j < k$. Demonstrația se încheie observând că $\sigma^k = e$. \square

Corolarul 31. Orice transpoziție are ordinul 2.

Propoziția 32. Ordinul unei permutări $\sigma \in S_n$ este egal cu cel mai mic multiplu comun al ordinelor ciclurilor disjuncte din descompunerea sa standard.

Demonstrație: Fie $\sigma \in S_n$ și $\sigma = c_1 c_2 \dots c_r$ descompunerea acesteia în produs de cicluri disjuncte. Notăm $t_j = \text{ord } c_j$, $j \in \{1, 2, \dots, r\}$, și $m = [t_1, t_2, \dots, t_r]$. Conform propoziției 9, avem $\sigma^t = c_1^t c_2^t \dots c_r^t$ pentru orice $t \in \mathbb{Z}$. Prin urmare, $\sigma^m = e$, iar $\sigma^t = e$ dacă și numai dacă $c_j^t = e$ pentru orice $j \in \{1, 2, \dots, r\}$ dacă și numai dacă $\text{ord } c_j | t$ pentru orice $j \in \{1, 2, \dots, r\}$ dacă și numai dacă $m | t$. Afirmatia este acum consecință a propoziției 30 din cursul 10. \square

5. ORICE GRUP SE SCUFUNDĂ ÎNTR-UN GRUP DE PERMUTĂRI

Așa cum arată și titlul paragrafului, orice grup poate fi regăsit ca subgrup al unui grup de permutări. Acest lucru este consecință a următoarei teoreme a lui Cayley:

Teorema 33. Orice grup G este izomorf cu un subgrup al lui S_G .

Demonstrație: Considerăm funcția $\varphi : G \rightarrow S_G$, $\varphi(g) = h_g$, unde $h_g : G \rightarrow G$, $h_g(x) = gx$. Întrucât $h_{g^{-1}} = h_g^{-1}$, h_g este într-adevăr un element al lui S_G , deci φ este corect definită.

Pentru $g, g', x \in G$ avem $h_{gg'}(x) = (gg')x = g(g'x) = h_g(h_{g'}(x)) = (h_g h_{g'})(x)$, de unde $h_{gg'} = h_g \circ h_{g'}$. De aici obținem faptul că φ este morfism de grupuri.

Dacă $g, g' \in G$ sunt astfel încât $h_g = h_{g'}$, atunci $g = h_g(e) = h_{g'}(e) = g'$, deci morfismul φ este injectiv. \square

Corolarul 34. Orice grup cu n elemente este izomorf cu un subgrup al lui S_n .

BIBLIOGRAFIE

- [1] T. Dumitrescu, *Algebra*, Ed. Universității din București, 2006.
- [2] I. D. Ion, N. Radu, *Algebră*, Ed. Didactică și Pedagogică, București, 1981.
- [3] C. Năstăsescu, C. Niță, C. Vraciu, *Bazele algebrei*, Ed. Academiei, București, 1986.