Permutációk véges halmazon

(előadásvázlat, 2012. szeptember 9.)

Maróti Miklós

Ennek az előadásnak a megértéséhez a következő fogalmakat kell tudni: ismétlés nélküli variáció, leképezés, indulási és érkezési halmaz, szürjektív, injektív, bijektív és identikus leképezés, leképezések szorzata és inverze, csoport, Abel-csoport, asszociatív, illetve kommutatív művelet, egységelem, csoportelem inverze és hatványa, determináns és tulajdonságai.

Az előadáshoz ajánlott jegyzet:

- Klukovits Lajos: *Klasszikus és lineáris algebra*, Polygon Kiadó, Szeged, 1999.
- Szendrei Ágnes: *Diszkrét matematika*, Polygon Kiadó, Szeged, 1994–2002.

1. Definíció. Az A halmaz permutációin a $\pi : A \to A$ bijektív leképezéseket értjük. Tetszőleges n pozitív egészre az $\{1, \dots, n\}$ halmaz összes permutációinak halmazát S_n-nel jelöljük.

2. Jelölés. A $\pi \in S_n$ permutációt megadhatjuk kétsoros írásmóddal

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1\pi & 2\pi & \cdots & n\pi \end{pmatrix},$$

vagy elempárok halmazaként:

$$\pi = \{(1, 1\pi),\ (2, 2\pi),\ \dots,\ (n, n\pi)\}.$$

3. Példa. Ha $\alpha \in S_3$ az a permutáció, amelyre $1\alpha = 2$, $2\alpha = 1$ és $3\alpha = 3$, akkor

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \{(1,2),\ (2,1),\ (3,3)\}.$$

4. Példa. Nem minden leképezés permutáció, például a

$$\varphi = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 3 \end{pmatrix} = \{(1,3),\ (2,1),\ (3,3)\}$$

leképezés se nem injektív (mert az 1 és 3 elemeknek ugyanaz a képe) se nem szürjektív (mert az érkezési halmaz 2 elmének nincsen őse).

5. Tétel. $|S_n| = n!$

6. Példa.

$$S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\},$$

$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\},$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

7. Tétel. $(S_n; \circ)$ *csoport.*

8. Példa. Számoljuk ki az

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \text{ és } \beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

permutációk szorzatát. Tudjuk, hogy minden x elemre $x(\alpha\beta) = (x\alpha)\beta$ (ez a leképezés szorzás definíciója). Tehát

$$\begin{aligned} 1(\alpha\beta) &= (1\alpha)\beta = 2\beta = 3, \\ 2(\alpha\beta) &= (2\alpha)\beta = 1\beta = 2, \\ 3(\alpha\beta) &= (3\alpha)\beta = 3\beta = 1, \end{aligned}$$

azaz

$$\alpha\beta = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Most kiszámoljuk a $\beta\alpha$ szorzatot is (a zárójelek elhagyásával):

$$\begin{aligned} 1\beta\alpha &= 2\alpha = 1, \\ 2\beta\alpha &= 3\alpha = 3, \\ 3\beta\alpha &= 1\alpha = 2, \end{aligned}$$

azaz

$$\beta\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}.$$

Vegyük észre, hogy $\alpha\beta \neq \beta\alpha$, azaz a permutációk szorzása nem kommutatív. Végezetül kiszámoljuk β inverzét. Mivel

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \{(1,2),\ (2,3),\ (3,1)\}$$

ezért

$$\beta^{-1} = \{(2,1),\ (3,2),\ (1,3)\} = \{(1,3),\ (2,1),\ (3,2)\} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Természetesen β és β^{-1} szorzata az identikus leképezés:

$$\beta\beta^{-1} = \beta^{-1}\beta = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

9. Definíció. A $\pi \in S_n$ permutáció az $x \in \{1, \ldots, n\}$ elemet mozgatja, ha $x\pi \neq x$. A $\pi \in S_n$ által mozgatott elemek halmazát M_π-vel jelöljük, azaz

$$M_\pi = \{\, x \in \{1, \ldots, n\} : x\pi \neq x \,\}.$$

10. Példa. Az

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

permutáció által mozgatott elemek halmaza $M_\alpha = \{1, 2\}$.

11. Kérdések. Hány olyan $\pi \in S_9$ permutáció van, amelyre

(1) $M_\pi = \{2, 3, 5\}$,
(2) $|M_\pi| = 1$,
(3) $|M_\pi| = 2$,
(4) $|M_\pi| = 3$?

12. Definíció. A $\pi, \sigma \in S_n$ permutációkat idegennek nevezzük, ha $M_\pi \cap M_\sigma = \emptyset$.

13. Kérdések.

(1) Az S_n halmazon az „idegenség” reláció reflexív, szimmetrikus, illetve tranzitív-e?
(2) Hány olyan permutációja van S_4-nek, amely az $\left(\begin{smallmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{smallmatrix}\right)$ permutációval idegen?
(3) Van-e olyan permutáció, amely idegen az inverzével?

14. Tétel. *Ha a $\pi, \sigma \in S_n$ permutációk idegenek, akkor*

(1) $\pi\sigma = \sigma\pi$, *és*
(2) $(\pi\sigma)^k = \pi^k\sigma^k$ *minden k egészre.*

15. Definíció. Legyen $n \geq k \geq 2$, és az $a_1, \dots, a_k \in \{1, \dots, n\}$ elemek páronként különbözőek. Ekkor azt a $\pi \in S_n$ permutációt, amelyre

$$\begin{aligned} a_1\pi &= a_2, \\ a_2\pi &= a_3, \\ &\vdots \\ a_{k-1}\pi &= a_k, \\ a_k\pi &= a_1, \end{aligned}$$

és $x\pi = x$ minden $x \in \{1, \dots, n\} \setminus \{a_1, \dots, a_k\}$ elemre, ciklusnak nevezzük és röviden így jelöljük:

$$\pi = (a_1 \ a_2 \ \cdots \ a_k).$$

A k számot a ciklus hosszának nevezzük. A 2 hosszúságú ciklusokat transzpozícióknak hívjuk.

16. Példa. Az

$$\alpha = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

permutáció ciklus, mivel a $k = 2$, $a_1 = 1$ és $a_2 = 2$ választással éppen ezt a permutációt kapjuk, azaz $\alpha = (1\ 2)$. Mivel α hossza éppen 2, ezért α transzpozíció is. A

$$\beta = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

permutáció szintén ciklus, és $\beta = (1\ 2\ 3)$.

17. Kérdések.

(1) Mi az $(a_1 \ a_2 \ \cdots \ a_k)$ ciklus által mozgatott elemek halmaza?
(2) Igaz-e, hogy ha $\pi, \sigma, \tau \in S_7$ páronként idegen permutációk, akkor $(\pi\sigma\tau)^5 = \pi^5\sigma^5\tau^5$?

18. Megjegyzés. Vegyük észre, hogy egy permutáció ciklusos alakban való megadása nem egyértelmű! Egyrészt ugyanazt a permutációt többféleképpen is felírhatjuk ciklusként:

$$(1\ 2\ 3) = (2\ 3\ 1) = (3\ 1\ 2).$$

A másik probléma pedig az, hogy az $(1\ 2\ 3)$ permutációról nem tudjuk eldönteni, hogy az S_3 vagy esetleg az S_4 csoport eleme-e. Természetesen ha S_3-beli permutációkról beszélünk, akkor

$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

viszont S_4-ben már

$$(1\ 2\ 3) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix},$$

és ez a két permutáció nem ugyanaz. Ugyan ez a probléma az identikus permutáció „id" jelölésével is, arról sem lehet eldönteni, hogy melyik permutációcsoportban használjuk.

19. Példa.

$$\begin{aligned} S_1 &= \{\mathrm{id}\}, \\ S_2 &= \{\mathrm{id}, (1\ 2)\}, \\ S_3 &= \{\mathrm{id}, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (3\ 2\ 1)\}. \end{aligned}$$

20. Kérdések.

(1) Hány transzpozíció van S_4-ben?
(2) Hány 3-hosszúságú ciklus van S_4-ben?
(3) Hány 4-hosszúságú ciklus van S_4-ben?
(4) Hány 1-hosszúságú ciklus van S_4-ben?

(5) Hány ciklus van S_4-ben?
(6) Hány olyan permutáció van S_4-ben amely nem ciklus?
(7) Hány n-hosszúságú ciklus van S_n-ben?

21. Példa. Természetesen nem minden permutáció ciklus, vegyük például a

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

permutációt. Tegyük fel, hogy π ciklus, és tekintsük azt az esetet, amikor $a_1 = 1$. Ekkor $a_1\pi = 2$, azaz $a_2 = 2$, továbbá $a_2\pi = 3$, azaz $a_3 = 3$. A következő lépésben azt kapjuk, hogy $a_3\pi = 1$ ami éppen egyenlő a_1-gyel, azaz $k = 3$ és az $(1\ 2\ 3)$ ciklust kaptuk. Viszont π több elemet mozgat mint 3, tehát π nem egyenlő $(1\ 2\ 3)$-mal, azaz $a_1 \neq 1$. Minden más esetben hasonló ellentmondásra jutunk.

Persze π előáll ciklusok szorzataként:

$$\pi = (1\ 2\ 3)(4\ 5).$$

22. Tétel. *Minden S_n-beli permutáció előáll páronként idegen ciklusok szorzataként, és ez az előállítás a tényezők sorrendjétől eltekintve egyértelműen meghatározott. (Az identikus permutációt ciklusok üres szorzatának tekintjük.)*

23. Példa. Adjuk meg a $\pi = (5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7)$ permutációt páronként idegen ciklusok szorzataként. Tekintsük azokat az elemeket, melyeket a szorzat valamely tagja mozgat: $\{1, 2, 3, 4, 5, 7\}$. Vegyünk ki ezek közül egyet, mondjuk az 1-gyet, és számoljuk ki, hogy ezt a π permutáció milyen elemekbe viszi át:

$$1\pi = 1(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 1(1\ 3\ 5)(4\ 3\ 7) = 3(4\ 3\ 7) = 7.$$

Folytassuk a kapott elemekkel, azaz

$$\begin{aligned} 7\pi &= 7(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 7(1\ 3\ 5)(4\ 3\ 7) = 7(4\ 3\ 7) = 4, \\ 4\pi &= 4(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 5(1\ 3\ 5)(4\ 3\ 7) = 1(4\ 3\ 7) = 1. \end{aligned}$$

Visszaértünk ahhoz az elemhez, amiből kiindultunk, tehát megvan az első ciklusunk: $(1\ 7\ 4)$. A maradék elemekből vegyük a következőt, mondjuk a 2-től, és számoljuk ki hogy ezt π milyen elemekbe viszi át:

$$\begin{aligned} 2\pi &= 2(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 3(1\ 3\ 5)(4\ 3\ 7) = 5(4\ 3\ 7) = 5, \\ 5\pi &= 5(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 2(1\ 3\ 5)(4\ 3\ 7) = 2(4\ 3\ 7) = 2, \end{aligned}$$

azaz a második ciklus a $(2\ 5)$ transzpozíció. Kimaradt még a 3, amelyre elvégezve a számolást azt kapjuk, hogy

$$3\pi = 3(5\ 2\ 3\ 4)(1\ 3\ 5)(4\ 3\ 7) = 4(1\ 3\ 5)(4\ 3\ 7) = 4(4\ 3\ 7) = 3,$$

azaz π a 3-mat nem mozgatja, tehát ezt az elemet figyelmen kívül hagyhatjuk. Tehát π páronként idegen ciklusok szorzatára bontott alakja $\pi = (1\ 7\ 4)(2\ 5)$. Ezt a számolást nem írjuk le általában, hanem fejben végezzük el!

24. Kérdések. Hány olyan permutáció van G-ben, amelynek páronként idegen ciklusok szorzatára bontott alakja P alakú:

(1) $G = S_4$, $P = (\cdot\ \cdot)(\cdot\ \cdot)$,
(2) $G = S_5$, $P = (\cdot\ \cdot)(\cdot\ \cdot)$,
(3) $G = S_5$, $P = (\cdot\ \cdot)(\cdot\ \cdot\ \cdot)$?

25. Tétel. *Tetszőleges $\pi = (a_1\ a_2\ \cdots\ a_k) \in S_n$ ciklusra*

(1) $\pi^{-1} = (a_k\ a_{k-1}\ \cdots\ a_1)$,
(2) $\pi^k = \mathrm{id}$,
(3) *Ha* $i \equiv j \pmod{k}$, *akkor* $\pi^i = \pi^j$.

26. Példa. Kiszámoljuk az $((1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9))^{-22}$ permutációt páronként idegen ciklusok szorzataként. Mivel az $(1\ 2\ 3\ 4)$, $(5\ 6\ 7)$ és $(8\ 9)$ ciklusok páronként idegenek, ezért

$$((1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9))^{-22} = (1\ 2\ 3\ 4)^{-22}(5\ 6\ 7)^{-22}(8\ 9)^{-22}.$$

Az $(1\ 2\ 3\ 4)$ ciklus hossza 4 és a -22-edik hatványát keressük. Mivel $-22 \equiv 2 \pmod 4$, ezért

$$(1\ 2\ 3\ 4)^{-22} = (1\ 2\ 3\ 4)^2 = (1\ 3)(2\ 4).$$

Hasonlóan $-22 \equiv -1 \pmod 3$, illetve $-22 \equiv 0 \pmod 2$, azaz

$$(5\ 6\ 7)^{-22} = (5\ 6\ 7)^{-1} = (7\ 6\ 5), \text{ és}$$
$$(8\ 9)^{-22} = (8\ 9)^0 = \mathrm{id}.$$

Tehát

$$((1\ 2\ 3\ 4)(5\ 6\ 7))^{-22} = (1\ 3)(2\ 4)(7\ 6\ 5).$$

27. Példa. Oldjuk meg az

$$(1\ 3\ 2)(2\ 5)\pi(4\ 5\ 7) = (2\ 6)$$

egyenletet. Az egyenlet mindkét oldalát ugyanazzal a permutációval ugyanarról az oldalról beszorozhatjuk. Először balról szorzunk $(1\ 3\ 2)$ inverzével:

$$(1\ 3\ 2)^{-1}(1\ 3\ 2)(2\ 5)\pi(4\ 5\ 7) = (1\ 3\ 2)^{-1}(2\ 6),$$

azaz

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

Ezt folytatva azt kapjuk, hogy

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

amit a szokásos módon páronként idegen ciklusok szorzatára bontunk: $\pi = (5\ 3\ 1\ 6\ 2\ 4\ 7)$.

28. Tétel. *Tetszőleges ciklus felírható transzpozíciók szorzataként, mégpedig*

$$(a_1\ a_2\ a_3\ \cdots\ a_k) = (a_1\ a_2)(a_1\ a_3)\cdots(a_1\ a_k).$$

Következésképpen, minden permutáció transzpozíciók szorzatára bontható (de ez általában nem egyértelmű).

29. Példa. $(1\ 2\ 3\ 4)(5\ 6) = (1\ 2)(1\ 3)(1\ 4)(5\ 6)$, de mivel $(1\ 2\ 3\ 4) = (2\ 3\ 4\ 1)$, ezért $(1\ 2\ 3\ 4)(5\ 6) = (2\ 3)(2\ 4)(2\ 1)(5\ 6)$, vagy $(1\ 2\ 3\ 4)(5\ 6) = (2\ 3)(5\ 6)(2\ 4)(2\ 1)$, mert idegen transzpozíciók felcserélhetők.

30. Tétel. *Minden permutáció vagy csak páros vagy csak páratlan sok transzpozíció szorzataként írható fel.*

31. Definíció. A $\pi \in S_n$ permutációt párosnak nevezzük, ha felbontható páros sok transzpozíció szorzatára. A nempáros permutációkat páratlannak nevezzük. Továbbá definiáljuk:

$$\operatorname{sgn}\pi = \begin{cases} +1, & \text{ha } \pi \text{ páros,} \\ -1, & \text{ha } \pi \text{ páratlan.} \end{cases}$$

32. Kérdések. Az alábbi állítások közül melyek igazak és melyek hamisak?

(1) Az identitás páros.
(2) Minden transzpozíció páratlan.
(3) Minden páros hosszú ciklus páros.
(4) Minden páratlan hosszú ciklus páros.
(5) Páros permutációk szorzata páros.
(6) Páratlan permutációk szorzata páros.
(7) Páros és páratlan permutáció szorzata páratlan.
(8) Páratlan permutációk inverze páratlan.

33. Példa. Megmutatjuk, hogy a 4×4-gyes tologatós játékban a baloldali kezdőállásból nem lehet előállítani a jobboldalit:

$$A = \begin{array}{|c|c|c|c|} \hline 1 & 2 & 3 & 4 \\ \hline 5 & 6 & 7 & 8 \\ \hline 9 & 10 & 11 & 12 \\ \hline 13 & 14 & 15 & \\ \hline \end{array} \qquad B = \begin{array}{|c|c|c|c|} \hline 2 & 1 & 3 & 4 \\ \hline 5 & 6 & 7 & 8 \\ \hline 9 & 10 & 11 & 12 \\ \hline 13 & 14 & 15 & \\ \hline \end{array}$$

A játék minden állásához hozzárendeljük az S_{16} csoport egyik elemét, mégpedig úgy, hogy az üres mező helyébe a 16-os számot képzeljük, és a kapott

$$T = \begin{array}{|c|c|c|c|} \hline a_1 & a_2 & a_3 & a_4 \\ \hline a_5 & a_6 & a_7 & a_8 \\ \hline a_9 & a_{10} & a_{11} & a_{12} \\ \hline a_{13} & a_{14} & a_{15} & a_{16} \\ \hline \end{array}$$

táblázatot felhasználva képezzük a

$$\pi_T = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & a_9 & a_{10} & a_{11} & a_{12} & a_{13} & a_{14} & a_{15} & a_{16} \end{pmatrix}$$

permutációt. Vegyük észre, hogy ha egy állapotban eltolunk egy négyzetet, akkor lényegében felcseréltük a 16-os számot valamely másik számmal. Tehát egy transzpozíciót hajtottunk végre, azaz az állapothoz rendelt permutáció paritása megváltozik. Mivel mind az A mind a B állapotban az üres mező a jobb alsó sarokban van, ezért biztos hogy páros sok lépest kell megtennünk A-ból B-be (ugyanannyiszor kell a 16-os számnak felfelé és lefelé, illetve balra és jobbra mozognia). Páros sok lépes során a hozzárendelt permutáció paritása nem változik. De az A kezdőállapotra $\pi_A = \mathrm{id}$ ami páros, míg a jobboldali állapotra $\pi_B = (1\ 2)$ ami páratlan. Tehát nem lehet az A állapotból a B állapotba jutni.

34. Definíció. Az S_n csoportot az n-edrendű szimmetrikus csoportnak nevezzük. A páros permutációk $A_n = \{\, \pi \in S_n : \pi \text{ páros} \,\}$ halmaza szintén csoportot alkot, amelynek neve az n-edrendű alternáló csoport.

35. Kérdések.

(1) Hány páratlan permutáció van S_3-ban?
(2) Hány páros permutáció van S_3-ban?
(3) Hány páratlan permutáció van S_1-ben?
(4) Hány páros permutáció van S_1-ben?

36. Tétel. *Tetszőleges $n \geq 2$ egészre $|A_n| = \frac{n!}{2}$.*