Permutációcsoportok[1]

Definiáljuk először a permutáció fogalmát:

D.: A permutáció egy halmaz önmagára való kölcsönösen egyértelmű leképezése. A továbbiakban mi az {1, 2, .. . , n} halmaz permutációival foglalkozunk. A fenti definíció szemléletes jelentése, hogy egy permutáció az 1, 2, ... , n számok valamilyen sorrendje. Egy π_1 permutáció természetes jelölése a következő:

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \downarrow & \downarrow & \downarrow & & \downarrow \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}, \text{ ahol} \{a_1, a_2, \dots, a_n\} = \{1, 2, \dots, n\}.$$

Nyilvánvaló, hogy egy n elemű halmaz permutációinak száma $n!$

Mindez önmagában elég semmitmondó, ezért vezessünk be egy permutációk közötti műveletet. Kézenfekvőnek tűnik a

$$\pi_1 = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix} \text{ és a } \pi_2 = \begin{pmatrix} 1 & 2 & \dots & n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$$

permutációk $\pi_1 \cdot \pi_2$ szorzatát a következőképpen definiálni: az $1 \leqq i \leqq n$- re alkalmazzuk π_1-et, majd az így nyert a_i számra π_2-t. Könnyen látható, hogy $\pi_1 \cdot \pi_2$ is egy permutáció, tehát a permutációk halmaza *zárt* erre a műveletre nézve. A szorzás további tulajdonságai is könnyen ellenőrizhetők.

1. Asszociatív: $(\pi_1 \cdot \pi_2) \cdot \pi_3 = \pi_1 \cdot (\pi_2 \cdot \pi_3)$.

2. Az $\epsilon = \begin{pmatrix} 1\,2 \dots n \\ 1\,2 \dots n \end{pmatrix}$ permutációt egységelemnek véve minden π-re $\pi\epsilon = \epsilon\pi = \pi$.

3. Minden π_1-re létezik pontosan egy olyan π_2, hogy $\pi_1 \cdot \pi_2 = \pi_2 \cdot \pi_1 = \epsilon$. $\pi_2 = \pi_1^{-1}$, a π_1 permutáció *inverze.*

4. Nem kommutativ. Ezt egy példával igazoljuk:

$$\begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} \cdot \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix} \neq \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix} \cdot \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix},$$

hiszen

$$\begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} \cdot \begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix} = \begin{pmatrix} 1\,2\,3 \\ 3\,1\,2 \end{pmatrix},$$

míg

$$\begin{pmatrix} 1\,2\,3 \\ 1\,3\,2 \end{pmatrix} \cdot \begin{pmatrix} 1\,2\,3 \\ 2\,1\,3 \end{pmatrix} = \begin{pmatrix} 1\,2\,3 \\ 2\,3\,1 \end{pmatrix}.$$

Tetszőleges n-re pedig a következő példát készíthetjük ezek alapján $(n \geqq 3)$:

$$\pi_1 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \dots n \\ 2\,1\,3\,4\,5\,6 \dots n \end{pmatrix} \text{ és } \pi_2 = \begin{pmatrix} 1\,2\,3\,4\,5\,6 \dots n \\ 1\,3\,2\,4\,5\,6 \dots n \end{pmatrix}.$$

Az első három tulajdonság és a zártság alapján kimondhatjuk, hogy a permutációk az itt definiált szorzásra nézve *csoportot* alkotnak. Ezt S_n-nel jelöljük és *n-ed-fokú szimmetrikus csoport*nak nevezzük.

S_n-en belül a következő módon megkülönböztetünk *páros és páratlan* permutációkat: tekintsük a

$$\prod_{1 \leqq i < j \leqq n} (j - i)$$

szorzatot. Alkalmazzuk a π permutációt minden tényezőn belül minden tagra. Így a

$$\prod_{1 \leqq i < j \leqq n} (a_j - a_i)$$

[1] A fenti előadás az Ifjúsági Matematikai Kör Téli Ankétján hangzott el. (Lejegyezték: Kőszegi Botond és Matolcsi Máté, a Budapesti Fazekas Mihály Gimn. III. osztályos tanulói.)

szorzatot kapjuk, amelynek abszolút értéke nyilván megegyezik az előbbi szorzat abszolút értékével. A π permutációt párosnak mondjuk, ha a szorzat előjele megmarad, és páratlannak, ha a szorzat előjele megváltozik. Vegyük észre, hogy a permutációknak pontosan a fele páros, és a fele páratlan ($n \geqq 2$) esetén. Tekintsük ugyanis a következő kölcsönösen egyértelmű megfeleltetést a páros és páratlan permutációk között: a π páratlan permutáció segítségével rendeljük a σ permutációhoz a $\sigma\pi$ permutációt. Nyilvánvaló, hogyσ és $\sigma\pi$ közül pontosan egy páros, és egy páratlan. Paritás szempontjából vizsgálva a szorzást, a következőket állapíthatjuk meg:

páros · páros=páros	páratlan · páros=páratlan
páros · páratlan =páratlan	páratlan · páratlan=páros

Azonnal következik, hogy a páros permutációk halmaza a szorzásra nézve zárt, így az n!/2 db páros permutáció S_n egy részcsoportját alkotja. Ennek neve *n-edfokú alternáló csoport,* jelölése A_n.

*

Térjünk vissza a permutációk jelöléséhez. Az eddigi $\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a_1 & a_2 & a_3 & \dots & a_n \end{pmatrix}$ jelölésnél célszerűbb az úgynevezett „ciklusos” jelölésmód: írjuk az első helyre az 1-et, majd az (i + 1)-dik helyre rendre azt a számot, amelyet a permutáció az i-dik helyen álló számhoz rendel, kivéve, ha visszajutottunk az 1-hez; ekkor zárjuk be a ciklust, és nyissunk újat a legkisebb eddig nem szereplő elemmel. Ezt addig végezzük, amíg az összes elem sorra nem kerül. Például:

$$\begin{pmatrix} 1\,2\,3\,4\,5\,6\,7 \\ 5\,4\,1\,2\,7\,6\,3 \end{pmatrix} = (1573)(24)(6)$$

(*Megjegyzés:* Mivel minden elemnek pontosan egy „őse” és egy „képe” van, egy ciklus csak az első eleméhez záródhat vissza.) Ilyen jelölésmóddal a szorzás gyorsabbá és átláthatóbbá válik.

D.: Az olyan permutációkat, amelyek ciklusos jelölésében egy kéttagú ciklus van, a többi ciklus pedig egytagú, *transzpozícióknak* nevezzük. Egy transzpozició tehát két elem cseréje a továbbiak helybenhagyásával.

Ha a kéttagú ciklus két szomszédos egészből áll, szomszédos transzpozícióról beszélünk.

1.T.: Minden permutáció előáll transzpozíciók szorzataként.

Bizonyítás. A permutációk ciklusos írásmódjából következik, hogy a tételt elég egyetlen ciklusra belátni. Valóban:

$$(a_1 a_2 a_3 \dots a_k) = (a_1 a_2)(a_1 a_3)(a_1 a_4) \dots (a_1 a_k).$$

2.T.: Minden permutáció előáll szomszédos transzpozíciók szorzataként.

Bizonyítás. Az előzőekből adódik, hogy elég a tételt transzpozíciókra belátni:

$$(a, a+i) = (a+i, a) =$$
$$= (a, a+1)(a+1, a+2) \dots (a+i-1, a+i)(a+i-1, a+i-2)(a+i-2, a+i-3) \dots (a+1, a).$$

3.T.: Minden permutáció előáll az (12) és az (12...n) permutációkból a szorzás műveletével. Ennek bizonyítása megtalálható a KöMaL 1990/7. 303. oldalán az F.2768. feladat megoldása során.

4.T.: Egy permutáció hatványaként nem állhat elő minden permutáció.

Bizonyítás. Mivel $\pi^k \cdot \pi^l = \pi^l \cdot \pi^k = \pi^{l+k}$, egy permutáció hatványai kommutatív csoportot alkotnak; márpedig $S_n(n \geqq\ 3-\text{ra})$ nem kommutatív.

A továbbiakban szükségünk lesz egy új fogalomra.

D.: π és σ ***konjugáltak*** egy H halmazban, ha létezik olyan ϱ, melyre $\varrho \in H$ és $\varrho^-1\pi\varrho = \sigma$.

5.T.: Ha H részcsoport, akkor a konjugáltság ekvivalencia-reláció:

1. reflexív: $\epsilon^{-1}\pi\epsilon = \pi$;
2. szimmetrikus: ha $\varrho^{-1}\pi\varrho = \sigma$, akkor $\varrho\sigma\varrho^{-1} = \pi$;
3. tranzitív: ha $\varrho_1^{-1}\pi_1\varrho_1 = \pi_2$ és $\varrho_2^{-1}\pi_2\varrho_2 = \pi_3$, akkor $(\varrho_1\varrho_2)^{-1}\pi_1(\varrho_1\varrho_2) = \pi_3$.

E tétel alapján S_n elemei diszjunkt konjugáltosztályokba rendeződnek. (Ez egyébként minden csoportra igaz.)

Felmerül a kérdés, hogy két, ciklusszerkezetével megadott permutáció mikor konjugált S_n-ben.

Legyen

$$\pi_1 = (a_{11}a_{12} \dots a_{1k_1})(a_{21}a_{22} \dots a_{2k_2}) \dots (a_{l1}a_{l2} \dots a_{lk_l})$$

és

$$\pi_2 = (b_{11}b_{12}\dots b_{1m_1})(b_{21}b_{22}\dots b_{2m_2})\dots(b_{p1}b_{p2}\dots b_{pm_p}),$$

ahol $k_1 \geqq k_2 \geqq \dots k_l$ és $m_1 \geqq m_2 \geqq \dots \geqq m_p$. A π_1-nek és π_2-nek pontosan akkor egyezik meg a ciklusszerkezete, ha $l = p$ és $m_1 = k_1, m_2 = k_2, \dots, m_p = k_l$.

6.T.: Két permutáció pontosan akkor konjugált S_n -ben, ha azonos a ciklusszerkezetük.

Bizonyítás.

1.Ha π_1 és π_2 konjugáltak, azaz $\varrho^{-1}\pi_1\varrho = \pi_2$ valamilyen ϱ-ra, akkor ciklusszerkezetük megegyezik.

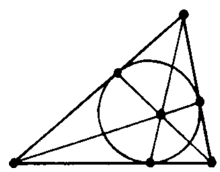
Írjuk fel ϱ^{-1}-et transzpozíciók szorzataként: $\varrho^{-1} = (i_1j_1)(i_2j_2)\dots(i_kj_k)$. Ekkor $\varrho = (i_kj_k)(i_{k-1}j_{k-1})\dots(i_1j_1)$ A szorzás asszociativitása miatt elég bizonyítani, hogy π_1 és $(i_gj_g)\pi_1(i_gj_g)$ ciklusszerkezete megegyezik. Ellenőrizhető, hogy ez a művelet nem csinál mást, mint az i_g és a j_g elemeket fölcseréli π_1-ben. Így a ciklusszerkezetet nem változtatja meg.

2. Ha π_1 és π_2 ciklusszerkezete ugyanaz, akkor konjugáltak. A bizonyítás első részében használt elemfelcserélésekkel a π_1 nyilvánvalóan átvihető π_2-be. A konjugáltság a csoportelméletben mélyebb fogalmakkal van kapcsolatban:

D.: Egy H csoport olyan G részcsoportját, amely minden elemének H-beli konjugáltjait is tartalmazza, a H *normális részcsoportjának* vagy *normálosztójának* nevezzük. Minden csoportnak van két triviális normálosztója: az egységelem és maga az egész csoport.

D.: Az olyan csoportokat, amelyeknek a két triviális normálosztón kívül nincs más normálosztójuk, *egyszerű csoportoknak* nevezzük.

Az egyszerű csoportok a prímszámokhoz hasonló szerepet játszanak a csoportok szerkezetében. Bizonyítható, hogy A_n ($n \geqq 5$ esetén) egyszerű csoport, és ezzel van kapcsolatban az, hogy ötöd- és ennél magasabb fokú egyenletekre nincs általános megoldóképlet. (A_5 a legkisebb egyszerű csoport.)



1. ábra

Érdekességként megadjuk a második legkisebb egyszerű csoportot: Vegyük a legkisebb, 7 pontból álló véges projektív síkot *(1.ábra)*. Ezen 7 pont egyenestartó permutációi egyszerű csoportot alkotnak. (A kör is egyenesnek számít.)

Érdemes gondolkodni a következő egyszerűbb és nehezebb feladatokon:

1. Minden transzpozíció páratlan permutáció.
2. A buborékrendezés felhasználásával bizonyítsuk az 1. tételt!
3. Bizonyítsuk be a 3. tételt!
4. Mutassuk meg, hogy a kocka mozgáscsoportja izomorf S_4-gyel!

*5. A dodekaéder mozgáscsoportja izomorf A_5-tel!

**6. A_n egyszerű csoport, ha $n \geqq 5$.

****7. A_n konjugáltosztályainak a száma nagyobb, mint S_n konjugáltosztályai számának a fele ($n \geqq 3-$ra).