22. szakkör (Csoportelméleti alapfogalmak 1.)

A) A PERMUTÁCIÓK CIKLIKUS SZERKEZETE

1. feladat:
Egy húsztagú társaság ül az asztal körül. Néhányat közülük (esetleg az összeset) párba állítunk, és a párok tapsszóra helyet cserélnek (1. lépés). Majd ismét kiválasztunk néhány embert (esetleg az összeset) és párba állítjuk őket, s a párok tapsszóra ismét helyet cserélnek (2. lépés). El szeretnénk érni, hogy mindenki a tőle jobbra levő székre üljön át. Elérhető-e ez két lépésben?

MEGOLDÁS: Számozzuk meg a társaság tagjait az ülésrend sorrendjében 1-től 20-ig, az 1-es két szomszédja a 20-as és a 2-es, a 2-esé az 1-es és a 3-as, stb. Az első lépésben cseréljen helyet az 1-es és a 20-as, a 2-es és a 19-es, a 3-as és a 18-as, stb. (az i-es a $21-i$-essel cserél helyet). Ekkor a 20-as már a helyére került, s tőle indulva a sorrend most ez: 20, 19, 18, 17, …, 3, 2, 1 vagyis „megfordult a sorrend”. Ezután cseréljen helyet az 1-es a 19-essel, a 2-es a 18-assal, és általában az i-es a $20-i$-essel. Így éppen a megfelelő sorrendet kapjuk: 20, 1, 2, 3, …, 18, 19.

Megjegyezzük, hogy a második lépésben a 10-es számú ember nem cserél helyet: ő is már a helyén ül: ott, ahol eredetileg a 11-es ült.

2. feladat:
Hány tagú társaság esetén oldható meg két lépésben a feladat?

MEGOLDÁS: Jelöljük n-nel a társaság tagjainak számát. Könnyen látható, hogy a fenti megoldás minden páros n-re működik. Az első lépésben az i-edik ember az $n+1-i$-edikkel cserél helyet, így létrejön a következő sorrend:

$n, n-1, n-2, \ldots, 3, 2, 1.$

Az n-edik tehát már a helyén van. Az ő kivételével most az i-edik az $n-i$-edikkel cserél helyet. Így megkapjuk a kívánt

$n, 1, 2, 3, \ldots, n-2, n-1$

sorrendet. Most is igaz, hogy az $n/2$-edik ember a második lépésben már a helyén marad, s ez így is van rendjén, mert ő már a helyén ült.

Ha n páratlan, akkor van „középső” ember: az $(n+1)/2$-edik és az első lépésben ő a helyén marad, nem lévén párja, akivel felcseréljük. Most is megkapjuk az

$n, n-1, n-2, \ldots, 3, 2, 1$

sorrendet az első lépés után. Most is alkalmazhatjuk ugyanazt a második lépést, mint páros n-re, csak most az n-edik ember kivételével mindenki ténylegesen helyet fog cserélni valakivel. Ismét megkapjuk a kívánt
$n, 1, 2, 3, \ldots, n-2, n-1$
sorrendet.

Fel is állíttathatjuk a társaságot és megkérhetjük, hogy álljanak sorba úgy, hogy az első álljon legelöl, utána a második, stb. A feladat ezesetben az, hogy mindenki eggyel előbbre lépjen, kivéve a legelsőt, akinek leghátulra kell kerülnie. A megoldás szerint ez mindig elérhető két lépésben. Természetesen vetődik fel a kérdés, hogy milyen más sorrend érhető el két lépésben. Erről szól tehát a következő feladat. Fogalmazzunk így:

3. feladat:
Egy osztály tanulói állnak tornasorban, azaz nagyság szerinti sorrendben, *nem* köralakban, hanem egyenesvonalban. Egy lépés most is, mint az előző két feladatnál, diszjunkt párok cseréjéből áll. A cél most az, hogy átrendezzük őket névsor szerinti sorrendbe. A kérdés az, hogy elérhető-e minden esetben két lépésben?

MEGOLDÁS: Ismét megszámozzuk a tanulókat, de most egy kicsit bonyolultabban számozunk: legyen a sor elején álló tanuló az 1-es. Nézzük meg, kinek a helyére kell kerülnie ennek az 1-es számú tanulónak, ő lesz a 2-es tanuló. Ezután nézzük meg, kinek a helyére kell kerülnie a 2-es tanulónak, ő lesz a 3-as tanuló. Folytassuk így a számozást (egyesével), amíg el nem jutunk ahhoz a tanulóhoz, akinek az 1-es helyére kell kerülnie. Nyilván eljutunk hozzá, legkésőbb akkor, amikor mindenki sorra került. Így kapunk egy *ciklust*, ami azt jelenti, hogy ha a számozás sorrendjében leültetjük őket egy asztal mellé, akkor pontosan az előző feladatokkal állunk szemben: mindenkinek a tőle eggyel jobbra ülő helyére kell két lépésben átülnie. Azokat a tanulókat, akik benne vannak ebben a ciklusban, két lépésben a helyükre tudjuk juttatni.
De mi lesz a többi tanulóval? (Persze, ha már nincs több tanuló, mert mindenki benne van az első ciklusban, akkor kész vagyunk.)
Vegyünk ki egy olyan tanulót, aki nincs benne az első ciklusban. Kezdjük el újra a számozást és legyen ő az 1-es, akinek a helyére kell állnia, az lesz megint a 2-es, és így folytatjuk tovább a számozást: ismét kapunk egy *ciklust*, vagyis tanulóknak egy olyan bezáruló sorát, ahol mindenki az utána következő helyére kell, hogy kerüljön, kivéve az utolsót, akinek az első helyére kell kerülnie. Ez pedig ismét az előbbi ültetéses feladat. Tehát őket is két lépésben átjuttathatjuk a helyükre. Az is nyilvánvaló, hogy az első ciklusbeli cserék és a második ciklusbeli cserék nem zavarják egymást: egy párban csak azonos ciklusbeli tanulók cserélnek helyet.
Így folytatva az eljárást minden tanulót a helyére juttathatunk két lépésben: ha maradt még olyan tanuló, aki nincs benne az első két ciklusban, akkor ő lesz az új 1-es és megkeressük az ő ciklusát. S ezt addig folytatjuk, amíg van még tanuló, aki nem került bele a korábbi ciklusokba.

Most átfogalmazzuk a 3. feladat megoldásában használt gondolatot permutációkra. Újra megszámozzuk a tanulókat, de most az eredeti nagyság szerinti sorrendben. Ez azt jelenti, hogy kezdetben az 1,2,3,…,*n* sorrendben állnak. A névsor szerinti sorrend viszont tetszőleges lehet, vagyis az 1,2,3,…,*n* számok egy *tetszőleges permutációja* lehet. A megoldásban valójában azt használtuk fel, hogy egy ilyen permutáció mindig *diszjunkt ciklusokra* bontható: cikluson egy olyan $(a_1\, a_2 \ldots a_k)$ sorozatot értünk, ahol a_1 az a_2 helyére kerül, a_2 az a_3 helyére, és általában a ciklus minden tagja az utána következő helyére kerül, az utolsó, a_k pedig az a_1 helyére. Ha egy osztályban történő karácsonyi ajándékozásra gondolunk, akkor könnyen megértjük, miről van szó: az első átadja az ajándékát, aki ajándékot kap, az átadja a saját ajándékát, stb., amíg a ciklus be nem fejeződik, majd valaki új ciklust kezd. Ha például a 35124 sorrendet akarjuk előállítani az 12345 sorrendből, ez azt jelenti, hogy az 1-est a 3-as helyére kell vinnünk, a 3-ast pedig az 1-es helyére, ez egy kételemű ciklus lesz, ezt így jelöljük: (1 3). A 2-es a 4-es helyére kerül, a 4-es az 5-ösére, az 5-ös a 2-esére, ezt így jelöljük: (2 4 5). Ez a permutáció tehát így írható fel: (1 3)(2 4 5). Ha egy elem helyben marad, akkor azt nem feltétlenül írjuk ki, ha eleve tudjuk, milyen elemeket mozgat a permutáció.

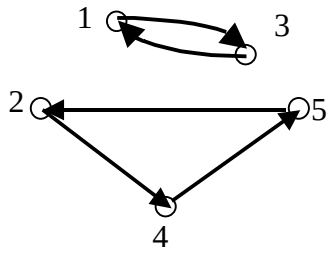
Még egy módon megvilágíthatjuk ezt a felírási módot. Ábrázoljuk nyíllal azt, hogy melyik szám melyiknek a helyére kerül. A 35124 permutációnál így a következőt kapjuk:

$1\to3$, $2\to4$, $3\to1$, $4\to5$, $5\to2$.

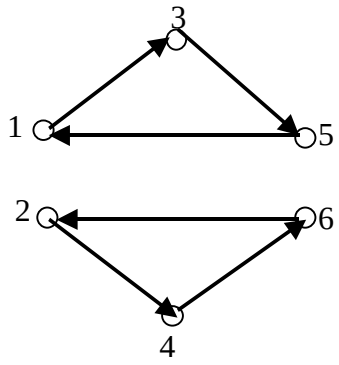
Másik példaként vegyük az 561234 permutációt. Itt a következőt kapjuk:

$1\to3$, $2\to4$, $3\to5$, $4\to6$, $5\to1$, $6\to2$.

Innen már leolvashatjuk a ciklusokat, de még egyszerűbben leolvashatók, ha egy irányított gráf éleivel ábrázoljuk azt, ami történik. A 35124 permutáció esetében a következő ötpontú gráfot kapjuk:



Az 561234 permutáció esetében a következő hatpontú gráfot kapjuk:



Innen leolvasható a permutáció ciklikus szerkezete: (135)(246).

DEFINÍCIÓ: Általában a következőképpen definiálhatjuk egy permutáció ciklikus alakját. Tekintsük az {1,2,…,*n*} halmaz egy σ permutációját, ez azt jelenti, hogy σ az 1 és *n* közötti számok halmazát egy-egyértelműen leképezi önmagára. A σ permutációnak megfeleltethetünk egy irányított gráfot, amelynek pontjai az 1, 2, …, *n* számok. Az *i* pontból a *j* pontba pontosan akkor mutat él, ha az *i* számot a σ permutáció a *j* számba viszi. Az így kapott irányított gráf minden pontjából pontosan egy él indul ki és minden pontjába pontosan egy él érkezik be, vagyis minden pont kifoka is, befoka is egy. (Ez pontosan azt fejezi ki, hogy σ egy-egy értelmű hozzárendelés.) Lehet benne hurokél is: az *i* pontból pontosan akkor indul hurokél önmagába, ha az *i* szám σ hatására a helyén marad. A fenti első ábrán pedig láthatjuk, hogy két pont között oda-vissza él is futhat: az *i* és *j* pont között akkor fut oda-vissza él, ha a σ permutáció felcseréli *i*-t és *j*-t.

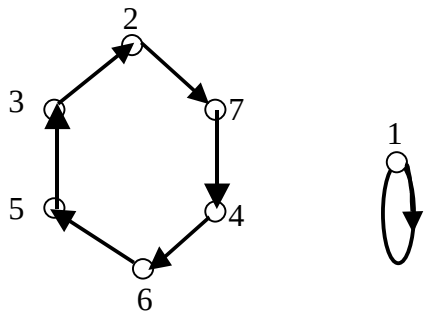
A kapott irányított gráf nyilván irányított ciklusokra bomlik, ahol
– cikluson irányított kört értünk, de megengedjük az 1 és 2 hosszú kört is (előbbi a hurokél, utóbbi az oda-vissza nyíl);
– a ciklusoknak nincs közös pontjuk, sem közös élük;
– ha felírjuk a ciklusokban a pontok sorrendjét (a kezdő elem bármelyik lehet, és nem írjuk ki kétszer), a különböző ciklusokat pedig zárójellel választjuk el egymástól, akkor megkapjuk a σ permutáció **ciklikus alakját**.
Egy permutáció **ciklusszerkezete** pedig azt adja meg, hogy a permutáció milyen hosszú ciklusokból áll.

Így például az (1 2 3)(4 5 6) permutáció azt a permutációt jelenti, amely az 1-et a 2-be, a 2-t a 3-ba, a 3-at az 1-be, a 4-et az 5-be, az 5-öt a 6-ba, a 6-ot a 4-be viszi: a végeredmény a 123645 sorrend.

A ciklikus felírás először kissé szokatlan, mert nem közvetlenül olvasható le belőle az, hogy milyen is lesz a létrejövő új permutáció. Ez a ciklikus felírás azt mondja el, hogy milyen hozzárendelés (vagy művelet) hozza létre a permutációt. Mint látni fogjuk, ez sok információt ad, amit körülményesebben kapnánk meg, ha a létrejött permutációt írnánk fel. Érdemes megjegyezni, hogy az újkori tudomány egy általános és nagyon erős jellemzője, hogy a ***kész eredményről*** áthelyezi a hangsúlyt arra a ***mozgásra***, amely az eredményt ***létrehozza***: így végső soron a kész eredményről is sokkal több információhoz jut. (Érdemes még egy módszertani megjegyzést tenni: a 3. feladat megoldása szerint tetszőleges permutáció előállítható két olyan permutáció egymás utáni alkalmazásával, amelyek mindegyike diszjunkt párok cseréjéből áll. A megoldáshoz a feladatot olyan részfeladatokra bontottuk, amelyek mindegyike már könnyen megoldható volt: először egy konkrét ciklusra oldottuk meg a feladatot, majd megállapítottuk, hogy ez a megoldás bármely ciklusra működik, harmadik lépésben pedig megmutattuk, hogy bármely permutáció felírható diszjunkt ciklusok összetételeként, s elég volt ezekre megoldani a feladatot. Az elgondolást, hogy egy feladatot lehetőleg olyan részekre osszunk fel, amelyek mindegyike már külön-külön hamar megoldható, Descartes avatta módszerré.)

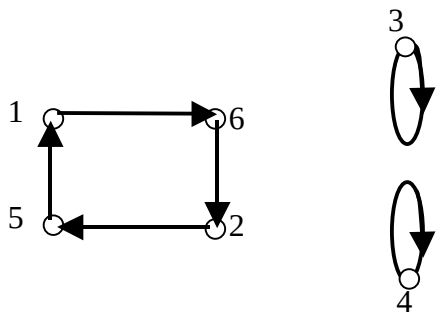
4. feladat:
Rajzoljuk fel a következő permutációk gráfját és írjuk fel ciklikus alakjukat:
a) 1357642, b) 563421, c) 135246, d) 246135, e) 3456712.

MEGOLDÁS:
a) Az 1357642 permutáció az 1-est helyén hagyja, az 1-esből tehát önmagába megy hurokél. A többi elemet egy ciklusban mozgatja:



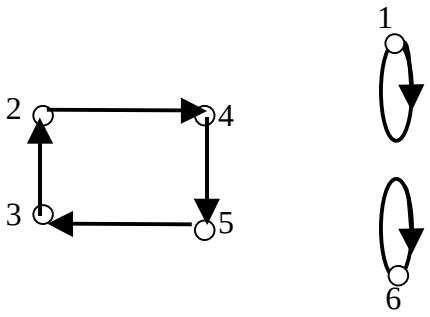
A ciklikus alakja: (2 7 4 6 5 3). Ez tehát egy egyes és egy hatos ciklusból áll.

b) Az 563421-ben a 3-as és a 4-es marad a helyén, ennek a permutációnak a gráfja:



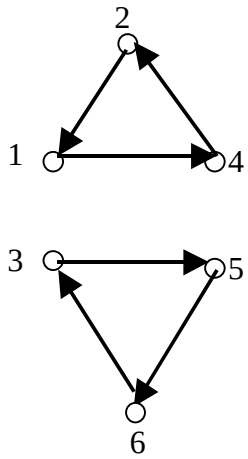
a ciklikus alakja: (1 6 2 5).

c) Az 135246 permutációban az 1 és 6 marad a helyén, a gráf:

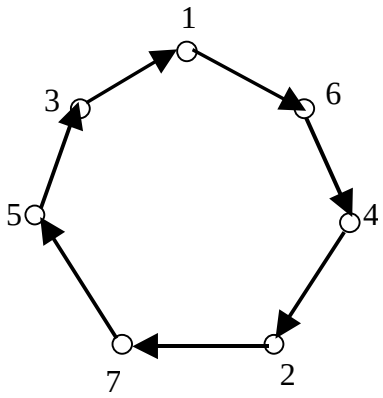


a ciklikus alak: (2 4 5 3).

d) A 246135 permutációban nincs fixpont, a gráf:



a ciklikus alak: (1 4 2)(3 5 6).
e) A 3456712 permutáció gráfja:



ciklikus alakja: (1 6 4 2 7 5 3). Ez tehát egy hételemű ciklus.

5. feladat:
Írjuk fel a következő ciklikus alakban felírt permutációk eredményét:
a) (1 3 5)(2 4 6) (hatelemű permutáció),
b) (1 3 5)(2 4 6) (hételemű permutáció),
c) (1 2)(3 4)(7 8) (nyolcelemű permutáció),
d) (1 2 3 4 5 6) (hatelemű permutáció).

MEGOLDÁS:
a-b) Az (1 3 5)(2 4 6) permutáció eredménye: 561234, ha hat elemet permutáltunk, ha a 7-es is szerepel, akkor helyén marad, tehát az 5612347 permutációt kapjuk.
c) Az (1 2)(3 4)(7 8) permutáció eredménye: 21435687.
d) Az (1 2 3 4 5 6) hatelemű permutáció eredménye: 612345.

23. szakkör (Csoportelméleti alapfogalmak 2.)

B) A PERMUTÁCIÓK INVERZE ÉS A CIKLIKUS SZERKEZET

A ciklikus felírásnak több előnye is van. Így például nagyon könnyű leolvasni, hogy egy adott permutáció végrehajtása után milyen permutációt kell végrehajtanunk *az elemeken*, ha vissza akarjuk kapni eredeti sorrendet.

DEFINÍCIÓ: Egy σ permutáció **inverzén** azt a σ^{-1} hozzárendelést értjük, amelyet σ után végrehajtva minden elem az eredeti helyére kerül vissza. σ^{-1} nyilván szintén egy-egy értelmű hozzárendelés, vagyis nyilván maga is permutáció.

Másképp fogalmazva ez azt jelenti, hogy ha σ az i elemhez a j elemet rendelte, akkor σ^{-1} a j elemhez rendeli az i elemet. Mint említettük, ha a σ permutáció végeredményét írjuk fel, abból körülményes leolvasni az inverzét. Tekintsük például a már szerepelt 35124 permutációt. „Kapásból” nehéz volna megmondani, mi az inverze. Ha azonban az irányított gráfos megfeleltetésre gondolunk, akkor világos, hogy az inverzét úgy kapjuk, hogy minden élen megfordítjuk az irányítást: ha eredetileg i-ből j-be mutatott egy él, az azt jelenti, hogy σ i-hez rendelte j-t. Ekkor σ^{-1} j-hez rendeli i-t, vagyis valóban meg kell fordítani az él irányítását. Ez azonban azt jelenti, hogy a ciklusokat is meg kell fordítani, vagyis

a* s *permutáció inverzének ciklikus alakját úgy kapjuk* s *ciklikus alakjából, hogy minden ciklusban megfordítjuk az elemek sorrendjét.

S valóban, az előbbi példánkon, a 35124 permutáción is láthatjuk, hogy ha ebből vissza akarjuk kapni az eredeti 12345 sorrendet, akkor az 1-es és 3-as helyen álló elemeket ismét fel kell cserélnünk, ez az (1 3) ciklus ismételt végrehajtását jelenti. Az 5-öst a 4-es helyére kell vinnünk, a 4-est a 2-es helyére, a 2-est pedig az 5-ös helyére. Ez az (5 4 2) ciklus végrehajtását jelenti. Az (1 3)(2 4 5) permutáció inverze tehát valóban az (1 3)(5 4 2) permutáció. Egy másik példán is megvizsgálhatjuk ugyanezt: az (1 2 3 4 5 6) permutáció eredménye a 612345 permutáció. Ennek inverze a fentiek szerint a (6 5 4 3 2 1) permutáció, s valóban: ha végrehajtjuk a $6\to5\to4\to3\to2\to1\to6$ cserét a 612345 permutáción, visszakapjuk az elemek eredeti 123456 sorrendjét.

A fenti állításból következik az is, hogy

Minden permutációnak és inverzének ugyanaz a ciklus-szerkezete, vagyis minden* k*-ra ugyanannyi* k *elemű ciklus van* s*-ban és az inverzében.

C) PERMUTÁCIÓK ÖSSZETÉTELE

Eddig azt kérdeztük, hogy egy adott permutáció végrehajtása után milyen permutációt kell végrehajtanunk, ha vissza akarjuk kapni az eredeti permutációt. Általában is felmerül a kérdés, hogy mi történik, ha két permutációt egymás után hajtunk végre. Ha a permutációkat a végeredményükkel jellemzünk, akkor már a kérdést is nehéz értelmezni. De ha a ciklikus felírást vesszük, akkor is kétértelmű a kérdés. Vegyük például először az (1 2 3 4) permutációt. Ez azt jelenti, hogy az 1-est a 2-es helyére visszük, a 2-est a 3-as helyére visszük, a 3-ast a 4-es helyére, azt pedig az 1-es helyére. Így végeredményül a 4123 permutációt kapjuk. Erre a kapott eredményre szeretnénk alkalmazni az (1 2)(3 4) permutációt. De hogy ez mit jelent, azt már kétféleképpen is értelmezhetjük. Az világos, hogy az 1-es számot a 2-es helyére kell vinnünk. De az már kérdés, hogy hogy értjük a helyét? Oda visszük, ahol ***eredetileg*** állt a kettes, vagyis „a” második helyre, vagy oda visszük, ahol éppen most, tehát az első permutáció végrehajtása ***után*** áll a kettes. A csoportelméletben általában az ***utóbbi*** értelmezést használják, ezért mi is ezt fogjuk használni. Ez azonban, mint látni fogjuk, egy helyen odafigyelést fog igényelni.

Az (1 2) (3 4) permutáció tehát értelmezésünk szerint felcseréli az 1-es és 2-est, valamint a 3-ast és 4-est, így a 4123 sorrendből a 3214 sorrendet állítja elő. Ez ciklikus alakban az (1 3)(2)(4) permutációt jelenti.

Ha ugyanezt az eredményt a ciklikus felírások egymásutánjából akarjuk leolvasni, akkor meg kell gondolnunk a következőt. A permutációt egy-egyértelmű ***függvényként*** értelmeztük. Amikor permutációkat akarunk egymás után alkalmazni, akkor tehát függvényeket akarunk egymás után alkalmazni. Gondoljuk meg, hogyan írjuk fel, ha például a logaritmus és a cos függvényt akarjuk egymás után alkalmazni. Ha azt írjuk, hogy log cos x, akkor ***először*** alkalmaztuk a cos függvényt és utána a log függvényt! Ha viszont a logaritmus függvényt akarjuk először alkalmazni és utána a cos függvényt, akkor a cos log x függvényhez jutunk. A két függvény egyáltalán nem azonos: a cos log x függvény csak pozitív x-ekre értelmes és csak –1 és 1 közötti értékeket vesz fel, a log cos x függvény pedig ott van értelmezve, ahol a cos függvény értéke pozitív, $-\pi/2 + 2k\pi < x < \pi/2 + 2k\pi$ esetén. Így például cos log 0 nem értelmes, míg log cos 0 = 0.

Ugyanígy a permutációk összetételénél sem mindegy, melyiket alkalmazzuk először és melyiket másodszor. Az (1 2 3 4) és az (1 2 (3 4) permutációkat egymás után alkalmazva akkor kapjuk a 3412 sorrendet eredményül, ha először az (1 2 3 4)-et alkalmazzuk, utána az (1 2)(3 4)-et.

6. feladat:
Milyen sorrendet kapunk, ha először az (1 2)(3 4) permutációt alkalmazzuk és utána az (1 2 3 4) permutációt?

MEGOLDÁS: Az (1 2)(3 4) permutáció eredménye: 2143. Most erre kell alkalmazni az (1 2 3 4) ciklust. Az 1-est tehát át kell vinni a 2-es helyére, vagyis az első helyre. A 2-est át kell vinni a 3-as helyére, vagyis az utolsó helyre, a 3-ast vissza kell vinni a helyére, a 4-est pedig az 1-es helyére: 1432 a végső sorrend.

Mint látjuk, az eredmény valóban különbözik az előző 3412 végeredménytől. Annak ciklikus alakja (1 3)(2)(4), ennek viszont (1)(4)(2 3). A kétféle sorrendben kapott eredmény ciklikus szerkezete ugyanaz, hogy ez véletlen-e, arra még visszatérünk.

Egyelőre próbáljuk meg a végeredményt közvetlenül a ciklikus felírásból kiolvasni. Ha az (1 2 3 4) és az (1 2)(3 4) permutációkat, tehát függvényeket ilyen sorrendben hajtjuk végre, akkor az eredmény az (1 3)(2 4). Az előbb már megbeszéltük, hogy a függvények egymásutánját viszont *nem* balról jobbra, hanem jobbról balra írjuk fel: jobbra írjuk azt, amit először hajtunk végre, és tőle balra azt, ami utána jön. Írjuk fel tehát most is így a permutációk összetételét:

(1 2)(3 4)(1 2 3 4) = (1 3)(2)(4),

és

(1 2 3 4)(1 2)(3 4) = (1)(3)(2 4).

Nézzük először az elsőt, s nézzük még egyszer, mi történik ott az 1-essel. A (3 4) ciklus nem mozgatja, azt tehát kihagyhatjuk. Az (1 2) ciklus hatására az 1-es átkerül a 2-es helyére. De hol van a 2-es? Ahova ***korábban***, tehát az előző két ciklus vitte! A (3 4) ciklus a 2-est sem mozgatta, tehát a 2-es ott van, ahova az (1 2 3 4) hatására került: a 3-as helyén. Vagyis az 1-est a 3-asba kell átvinni. Hova megy a 3-as? Az (1 2) nem változtat a helyzetén, a (3 4) viszont oda viszi, ahol az (1 2 3 4) hatására a 4-es áll, vagyis az 1-es helyére. Ez azt jelenti (amit már tudunk), hogy az 1 és 3 helyet cserél. Hogyan lehet ezt könnyen leolvasni a ciklikus alakból? Térjünk vissza a ciklusok nyilakkal való ábrázolásához. Az (1 2) ciklust az $1\to2$ és $2\to1$ nyilak ábrázolják, a (3 4) ciklust a $3\to4$ és $4\to3$ nyilak, az (1 2 3 4) ciklust az $1\to2$, $2\to3$, $3\to4$, $4\to1$ nyilak. Vagyis írjuk fel így:

(1 2): $1\to2$, $2\to1$
(3 4): $3\to4$, $4\to3$,
(1 2 3 4): $1\to2$, $2\to3$, $3\to4$, $4\to1$.

Azt mondtuk: az 1-est a 2-es helyére kell vinni, ezt jelöli az $1\to2$ nyíl. De meg kell keresnünk a 2-es helyét, ezt jelöli a harmadik sorban levő $2\to3$ nyíl. Ha a két nyilat összerakjuk, kijön az „eredmény”: $1\to3$. Ugyanígy a 3-as helyét úgy keressük meg, hogy megnézzük a nyilakat. Az első sorban nem szerepel, ott tehát nem történik vele semmi. A második sor tanúsága szerint a 4-es helyére kerül, ezt jelenti a $3\to4$ nyíl, s hogy hol van most a 4-es, azt a harmadik sor $4\to1$ nyila árulja el. Vagyis megint összerakjuk a $3\to4$ és $4\to1$ nyilakat, és megkapjuk az eredményt: $3\to1$. Ha megnézzük, hova jut a 2-es, azt kapjuk, hogy az 1-es helyére, viszont az 1-est a harmadik ciklus éppen a 2-es helyére vitte. Vagyis a $2\to1$ és $1\to2$ nyilakat kell összerakni, s ennek eredménye valóban az, hogy a 2-es a helyén marad: $2\to2$. Hasonlóképpen kapjuk, hogy a 4-es is a helyén marad a $4\to3$ és a $3\to4$ nyilak „összerakásának” eredményeképpen.

Gondoljuk meg általában is, hogy hogyan olvashatjuk ki két tetszőleges ciklus összetételének az eredményét! Ha először az $(a_1\ a_2\ \dots\ a_k)$ ciklust, majd a $(b_1\ b_2\ \dots\ b_m)$ ciklust alkalmazzuk, akkor ez a

$(b_1\ b_2\ \dots\ b_m)(a_1\ a_2\ \dots\ a_k)$

szorzatot jelenti. Itt az b_i-t b_{i+1} helyére kell vinnünk, amit az $b_i \to b_{i+1}$ nyíllal jelölünk. Hogy éppen hol áll b_{i+1}, azt viszont a másodiknak felírt permutációból olvashatjuk ki: ha ott szerepel a b_{i+1}, éspedig $=a_j$, akkor az a_{j+1} helyére került, amit az $b_{i+1}=a_j \to a_{j+1}$ nyíl jelöl. A két nyilat összerakva: $b_i \to b_{i+1}=a_j \to a_{j+1}$ kapjuk b_i helyét: $b_i \to a_{j+1}$. Most látszik, hogy miért előnyös, hogy a két permutációt „fordított sorrendben", jobbról balra írtuk fel: az eredményt viszont könnyen leolvashatjuk balról jobbra haladva: *először* olvassuk le a $b_i \to b_{i+1}$ nyilat, ami azt jelenti: megnézzük, mi áll b_i mellett jobbra az első ciklusban, majd utána a $b_{i+1}=a_j \to a_{j+1}$ nyilat, ami azt jelenti, hogy megnézzük, mi áll b_{i+1} mellett jobbra a második ciklusban. Ha b_{i+1} nem szerepel a másodiknak írt ciklusban, akkor b_i egyszerűen b_{i+1} helyére kerül, hiszen a másodiknak írt ciklus nem mozgatta. S ez megint könnyen kiolvasható a ciklikus alakokat balról jobbra olvasva.

7. feladat: Határozzuk meg az
a) (1 3)(2 4 5) majd az (1 2 3 4 5) permutáció,
b) az (1 2 3) és a (2 3 4) permutáció,
c) az (1 2 3) és a (3 4 5) permutáció
egymás utáni alkalmazásának eredményét mindkét sorrend esetén!

MEGOLDÁS:
a) Ha az (1 3)(2 4 5) permutációt alkalmazzuk először, s utána az (1 2 3 4 5) permutációt, akkor az eredmény:

(1 3)(2 4 5)(1 2 3 4 5) = (1 4)(2 5 3).

(Ez a 24513 sorrendet jelenti.)

Ha a két permutációt fordított sorrendben hajtjuk végre, annak eredménye:

(1 2 3 4 5)(1 3)(2 4 5) = (1 4 2)(3 5).

(Ez a 24315 sorrendet jelenti.)

b) (1 2 3)(2 3 4) = (1 3)(2 4)
és
(2 3 4)(1 2 3) = (2 1)(3 4).

c) (1 2 3)(3 4 5) = (1 2 4 5 3), és
(3 4 5)(1 2 3) = (1 2 3 4 5).

Megjegyezzük, hogy a ciklikus szerkezet most is mindig azonos volt a két sorrend esetén.
További gyakorló példák:

8. feladat:
Állapítsuk meg, mi az eredménye az alábbi permutációk egymás utáni alkalmazásának:
a) (1 2)(1 3) és a') (1 3)(1 2);
b) (1 3)(2 3);
c) (1 3)(2 3)(4 5)(2 4);
d) (1 2)(2 3)(3 4)(4 5)(5 1);
e) (1 2 3)(3 4 5)(5 6 1);

f) (1 2)(1 3)(1 4);
g) (1 4)(1 3)(1 2).

MEGOLDÁS:
a) (1 2)(1 3) = (1 2 3) és (1 3)(1 2) = (1 3 2).
b) (1 3)(2 3) = (1 2 3).
c) (1 3)(2 3)(4 5)(2 4):
Az (1 3)(2 3) eredményét már tudjuk: (1 2 3). Könnyen kiszámolhatjuk a (4 5)(2 4) eredményét is, hiszen ez ugyanaz, mint a (4 5)(4 2), s ez viszont ugyanolyan alakú, mint az a)-ban szereplő (1 2)(1 3), tehát
(4 5)(2 4) = (4 5)(4 2) = (4 5 2).

Tehát a feladat az (1 2 3)(4 5 2) szorzat kiszámolása:
(1 2 3)(4 5 2) = (1 4 5 2 3).

d) (1 2)(2 3)(3 4)(4 5)(5 1):
Tudjuk, hogy (1 2)(2 3) = (1 3 2) és ugyanígy (3 4)(4 5) = (3 5 4). A 7.c feladathoz teljesen hasonlóan e két permutáció szorzata
(1 3 2)(3 5 4) = (2 1 3)(3 5 4) = (2 1 5 4 3).

Most már csak ezt kell megszorozni (5 1)-gyel:
(2 1 5 4 3)(5 1) = (1)(2 5 4 3), vagy másképp (1)(5 4 3 2).

e) Ismét a 7.c feladatot alkalmazva (1 2 3)(3 4 5) = (1 2 4 5 3), s ezt kell megszorozni (5 6 1)-gyel:
(1 2 4 5 3)(5 6 1) = (1 2 4 6)(3 5).

f) (1 2)(1 3)(1 4) = (1 2 3)(1 4) = (1 2 3 4).
g) (1 4)(1 3)(1 2) = (1 4 3)(1 2) = (1 4 3 2) = (4 3 2 1).

E feladat megoldása során már többször észrevehettük, hogy az, amit két ciklus szorzatának kiszámolásáról mondtunk, akárhány ciklus kiszámolásánál is használható:

Ha több ciklust szorzunk össze, és egy tetszőleges* a *elemről akarjuk kiszámolni, hogy végeredményben melyik elem helyére kerül, akkor a következőképpen járunk el:

megkeressük a balról számolva első ciklust, amelyben* a *szerepel, és vesszük e ciklusban a jobb oldali szomszédját. Ha ez* b*, akkor megkeressük az első olyan ciklust tőle balra, amelyben szerepel* b*, és vesszük* b *jobb oldali szomszédját, majd ezzel folytatjuk az eljárást. Az utolsónak kapott* c *elem helyére fog kerülni* a*, tehát a végeredmény ciklikus alakjában* a *jobb oldali szomszédja* c *lesz.

Ha a végeredmény ciklikus alakját akarjuk felírni, akkor nem kell mást tennünk, mint megkeresni ezután* c *jobb oldali szomszédját, majd ennek jobb oldali szomszédját, és így tovább.

Mindez világos a nyilakkal történő ábrázolásból és világos akkor is, ha végiggondoljuk, hogy mi történik *a*-val az egyes permutációkban.

DEFINÍCIÓ: Azt a permutációt, amely minden elemet a helyén hagy, **identitásnak** nevezzük.

A továbbiak kedvéért megemlítjük azt a nyilvánvaló tényt, hogy egy σ permutáció és az identitás szorzata mindig σ (akármelyik oldalról szorozzuk is az identitással).

Az eddigiek alapján megállapíthatjuk a következőket: ha *n* elem permutációit tekintjük, ezek az összetételre mint „szorzásra” nézve rendelkeznek a következő tulajdonságokkal:

- Az identitás és egy σ permutáció szorzata σ.
- Minden σ permutációnak van egy σ^{-1} inverze, amellyel „szorozva” az identitást adja. Megjegyezzük, hogy σ^{-1} inverze pedig σ.
- A nyilakkal való ábrázolás alapján könnyen ellenőrizhető, hogy az összetétel asszociatív, vagyis ha σ, σ', σ'' három permutáció, akkor $(\sigma\sigma')\sigma'' = \sigma(\sigma'\sigma'')$. (De ellenőrízhető úgy is, ahogyan a geometriai transzformációk asszociativitását ellenőrizzük.)

Vagyis a permutációk az összetételre mint szorzásra nézve csoportot alkotnak. Az egység az identitás. Azt is láttuk, hogy ez a szorzás a legtöbb esetben nem kommutatív, vagyis ha σ és σ' két permutáció, akkor $\sigma\sigma'$ és $\sigma'\sigma$ legtöbbször nem ugyanazt az eredményt adja.

DEFINÍCIÓ: Az *n* elemen ható permutációk csoportját az *n*-edrendű szimmetrikus csoportnak nevezzük és $\mathbf{S}_n$-nel jelöljük.

24. szakkör (Csoportelméleti alapfogalmak 3.)

D) PERMUTÁCIÓK RENDJE

Fontos kérdés a csoportelméletben, hogy egy adott elem hanyadik hatványa lesz az egység.

DEFINÍCIÓ: A legkisebb olyan pozitív k számot, amelyre σ^k az egység, a σ **rendjének** nevezzük. Az egység rendje egy, minden más elemé nagyobb egynél.

Permutációk esetében tehát azt a legkisebb pozitív k számot nevezzük a σ permutáció rendjének, amelyre teljesül, hogy σ^k az identitás. Az identitás rendje egy.

Egy permutáció rendje ismét a ciklikus szerkezetéből olvasható ki.

9. feladat:

a) Ha σ egyetlen k elemű ciklusból áll, akkor σ^m pontosan akkor az identitás, ha $k|m$ (k osztója m-nek), és σ rendje k.
b) Ha σ ciklusainak hossza $k_1,k_2,\ldots,k_l$, akkor σ^m pontosan akkor az identitás, ha $[k_1,k_2,\ldots,k_l]|m$.
c) Ha σ ciklusainak hossza $k_1,k_2,\ldots,k_l$, akkor σ rendje $[k_1,k_2,\ldots,k_l]$.

MEGOLDÁS:
a) Ha $\sigma = (a_1\, a_2 \ldots a_k)$, akkor ez az $a_1 \to a_2 \to a_3 \to \ldots \to a_k \to a_1$ ciklikus cserét jelenti. Ha ezt még egyszer végrehajtjuk, akkor a_1 már a_3-ba kerül. Nyilván pontosan k-szori végrehajtás után kerül először vissza a_1-be, s aztán minden k ismétlés után. Ugyanez minden a_i-re elmondható, tehát pontosan akkor kerül vissza minden a_i a helyére, ha σ-t k többszöröse alkalommal ismételjük. És a) éppen ezt állítja.
b) A k_i hosszú ciklus elemei pontosan akkor kerülnek vissza a helyükre, ha σ-t k_i többszöröse alkalommal ismételjük. Minden elem tehát pontosan akkor kerül vissza a helyére, ha σ-t $[k_1,k_2,\ldots,k_l]$ többszöröse alkalommal ismételjük. És b) éppen ezt állítja.
c) egyszerű következménye b)-nek.

10. feladat:
Milyen ciklus szerkezete van azoknak a permutációknak, amelyeknek rendje pontosan kettő?

MEGOLDÁS: Az előző feladat b) pontja szerint minden ciklus hossza osztója kell, hogy legyen kettőnek. Vagyis csak egyes és kettes ciklusokból állhat. Másrészt kell lennie kettes ciklusnak, különben az identitásról van szó, aminek egy a rendje. Végül c)-ből az is következik, hogy ha egy permutáció csupa kételemű ciklusból áll, akkor a rendje kettő. Azt kaptuk, hogy

egy permutáció rendje pontosan akkor kettő, ha csupa egy és kettő hosszú ciklusból áll és van benne kettő hosszú ciklus.

Az 1. feladatban az volt a feladat, hogy egy húszelemű halmazt két lépésben át kellett rendezni (vagyis permutálni kellett) úgy, hogy mindkétszer csak diszjunkt párokat cserélünk. Ez azt jelenti, hogy két olyan permutációból kellett összetenni, amelyek kételemű (diszjunkt) ciklusok szorzata. Ennek alapján általánosítása, a 3. feladat így fogalmazható át:

Bármely permutáció felírható két másodrendű permutáció szorzataként.

Ebből rögtön az is kiderül, hogy két másodrendű elem (permutáció) szorzatának a rendje akármilyen nagy lehet, hiszen például egy n elemű ciklus rendje n. Megemlítjük azt is, hogy ha végtelen csoportokat is tekintünk, akkor két másodrendű elem szorzatának a rendje akár végtelen is lehet (ami azt jelenti, hogy van két olyan másodrendű elem, amelyek szorzatát akárhanyadik hatványra emelve nem kapjuk meg az identitást). Tekintsük például az egész számokat mint a számegyenes ponthalmazát és tekintsük az egészek összes egybevágósági transzformációját. Ezek az összetételre nézve csoportot alkotnak. Vegyük most a következő két transzformációt: t legyen a nullára való tükrözés, u pedig az ½-re való tükrözés. Mindkét tükrözés másodrendű (kétszeri tükrözés minden egészt a helyére visz vissza). Másrészt a tu összetétel eredménye az 1-gyel való eltolás és ezt akárhányszor ismételve sem kerülhet egyetlen szám sem a helyére. Megjegyezzük még, hogy ha tekintünk egy szabályos n-szöget és tekintjük az összes egybevágósági transzformációt, amely ezt az n-szöget önmagába viszi, akkor ezek a transzformációk is csoportot alkotnak az összetételre nézve. Ha tekintjük egyik oldalának felezőmerőlegesére való t tükrözést, majd az oldal egyik végpontján átmenő felezőmerőlegesre való u tükrözést, akkor ezek mindketten másodrendű elemek és szorzatuk a szabályos n-szög középpontja körüli $360°/n$ szögű forgatás. Ennek rendje pedig n (legalább n-szer kell forgatnunk $360°/n$-nel, hogy minden csúcs visszakerüljön a helyére). Ez egy további példa arra, hogy két másodrendű elem szorzata akármilyen nagy lehet.

11. feladat:
a) Milyen rendű elemek vannak a harmadrendű szimmetrikus csoportban, $\mathbf{S}_3$-ban?
b) Milyen rendű elemek vannak $\mathbf{S}_4$-ben és $\mathbf{S}_5$-ben?
c) Milyen rendű elemek vannak $\mathbf{S}_6$-ban?

MEGOLDÁS: A feladatra a ciklikus szerkezet segítségével adunk megoldást. Az identitás rendje mindig egy, ezzel nem foglalkozunk a továbbiakban.
a) $\mathbf{S}_3$-ban az identitáson kívül kétfajta permutáció van: az egyik egy háromelemű ciklusból áll, a másik egy kételemű és egy egyelemű ciklusból. Az előbbi rendje három, az utóbbié kettő. Tehát $\mathbf{S}_3$-ban az elemek rendje 1,2 vagy 3.

b) $\mathbf{S}_4$-ben az identitáson kívül négyfajta permutáció van: azok, amelyek
– egy kételemű és két egyelemű ciklusból állnak (2,1,1 a ciklusszerkezetük),
– egy háromelemű és egy egyelemű ciklusból állnak (3,1 a ciklusszerkezetük),
– egy négyelemű ciklusból állnak (4 a ciklusszerkezetük),
– két kételemű ciklusból állnak.
Az első és utolsó fajta permutáció rendje kettő, a második rendje három, a harmadiké négy. Tehát $\mathbf{S}_4$ elemeinek rendje 1,2,3 és 4.
$\mathbf{S}_5$-ben az identitáson kívül a következő féle permutációk vannak (csak a ciklusszerkezetet írjuk ki):
– 5, rendje: 5.
– 4,1, rendje: 4.
– 3,2, rendje: 6.
– 3,1,1, rendje: 3.
– 2,2,1, rendje: 2.
– 2,1,1,1, rendje: 2.
Tehát $\mathbf{S}_5$-ben az elemek rendje 1,2,3,4,5 vagy 6.
c) $\mathbf{S}_6$-ban az identitáson kívül a következő féle permutációk vannak (ismét csak a ciklusszerkezetet írjuk ki:)
– 7, rendje: 7.
– 6,1, rendje: 6.
– 5,2, rendje: 10.
– 5,1,1, rendje: 5.
– 4,3, rendje: 12.
– 4,2,1, rendje: 4.
– 4,1,1,1, rendje: 4.
– 3,3,1, rendje: 3.
– 3,2,2, rendje: 6.
– 3,2,1,1, rendje: 6.
– 3,1,1,1,1, rendje: 3.
Tehát $\mathbf{S}_7$-ben az elemek rendje lehet 1,2,3,4,5,6,7,10,12.

Visszatérve még arra a kérdésre, hogy mi lehet a rendje két másodrendű elem szorzatának: láttuk már, hogy akármekkora szám lehet a rendje. Ha azonban a két elem felcserélhető, akkor szorzatuk rendje is kettő.

12. feladat:
Bizonyítsuk be ezt az állítást!

MEGOLDÁS: Legyen a két elem a és b. Tudjuk, hogy $a^2=b^2=e$, az egység. Másrészt a kommutativitást is használva: $(ab)^2=abab=aabb=a^2b^2=ee=e$. Tehát ab rendje valóban kettő.

E) GENERÁTORRENDSZEREK

DEFINÍCIÓ: Láttuk, hogy másodrendű elemek szorzataként bármely permutáció megkapható. Ha bizonyos permutációknak megvan az a

tulajdonsága, hogy szorzatukként n elem bármely permutációja előáll, akkor azt mondjuk, hogy ezek az elemek **generálják** az n-edrendű szimmetrikus csoportot, $\mathbf{S}_n$-et. A szorzásnál egy elemet többször is használhatunk!

Korábbi állításunkat most úgy fogalmazhatjuk, hogy a másodrendű elemei generálják $\mathbf{S}_n$-et. De ebből az is következik, hogy már a kételemű ciklusok is generálják, hiszen minden másodrendű elem ilyenek szorzata.

DEFINÍCIÓ: Az olyan permutációt, amely egyetlen kételemű ciklusból áll (az összes többi elem a helyén marad), **transzpozíciónak** nevezzük.
MEGJEGYZÉS: Az elnevezés abból származik, hogy egy kételemű ciklus két elem helyét cseréli fel (két elemet helyez át, transzponál), minden más elemet a helyén hagy. A transzpozíciók alapvető szerepet játszanak a szimmetrikus csoportok elméletében.

Eddig azt láttuk be, hogy a transzpozíciók generálják az $\mathbf{S}_n$ szimmetrikus csoportot. Már ez is nagy egyszerűsítés, hiszen $\mathbf{S}_n$-nek $n!$ eleme van (ennyi permutáció van n elemen), míg transzpozícióból csak jóval kevesebb, $n(n-1)/2$. S ezek szerint elég ezeket jól ismerni, hogy információkat szerezzünk $\mathbf{S}_n$-ről. Ám még ez a szám is csökkenthető:

13. feladat:
Bizonyítsuk be, hogy az $\{1,2,\ldots,n\}$ halmaz permutációit már n–1 transzpozíció is generálja.

I. MEGOLDÁS: Megmutatjuk, hogy már az (1 2), (1 3), … (1 n) transzpozíciók is generálják az összes permutációt. Ehhez elég azt belátnunk, hogy ezek a transzpozíciók megfelelően összeszorozva minden más transzpozíciót kiadnak, hiszen akkor ilyenek szorzataként már minden permutációt megkapunk. Vagyis elég az (i j) transzpozíciót felírni (1 k) alakúak szorzatával. Rövid próbálkozás után megkapjuk, hogy
(i j) = (1 i)(1 j)(1 i).

II. MEGOLDÁS: Megmutatjuk, hogy az (1 2),(2 3),(3 4),…,(n–1 n) transzpozíciók is generálnak minden permutációt. Most az előző megoldás alapján már elég az (1 i) transzpozíciót felírni ezeknek a transzpozícióknak a szorzataként:
(1 i) = (1 2) (2 3) (3 4)…(i–2 i–1) (i–1 i) (i–2 i–1) … (3 4) (2 3) (1 2).

MEGJEGYZÉS: 1. Mindkét bizonyításban felhasználtuk azt a nyilvánvaló állítást, hogy ha permutációk egy H halmazából szorzással előállítható permutációk egy G generátorrendszere, akkor H is generátorrendszer.
2. Természetesen vetődik fel a kérdés, hogy a) nem elég-e kevesebb transzpozíció is $\mathbf{S}_n$ generálásához; b) minimálisan hány elem generálja $\mathbf{S}_n$-et. A következő feladatok mindkét kérdésre választ adnak.

14. feladat:
a) Írjuk fel az (1 3 5 2 4) és a (2 4 6 3 5) ciklusokat (1 i) alakú transzpozíciók szorzataként.
b) Írjuk fel általában is az (a_1 a_2… a_k) ciklust (1 i) alakú transzpozíciók szorzatként, ha tudjuk, hogy szerepel az a_j-k között az 1-es.
c) Írjuk fel az (a_1 a_2 … a_k) ciklust (1 i) alakú transzpozíciók szorzatként, ha az a_j-k között nem szerepel az 1-es.
d) Mutassuk meg, hogy az (1 3 5 2 4) permutáció felírható négy transzpozíció szorzataként, de kevesebb szorzataként nem írható fel. Mit állíthatunk általában egy ötelemű ciklusról?
e) Mutassuk meg, hogy általában egy k elemű ciklus előáll k–1 transzpozíció szorzataként, de kevesebb transzpozíció szorzataként nem áll elő.

25. szakkör (Csoportelméleti alapfogalmak 4.)

14. feladat:

a) Írjuk fel az (1 3 5 2 4) és a (2 4 6 3 5) ciklusokat (1 i) alakú transzpozíciók szorzataként.
b) Írjuk fel általában is az ($a_1\, a_2 \ldots\, a_k$) ciklust (1 i) alakú transzpozíciók szorzatként, ha tudjuk, hogy szerepel az a_j-k között az 1-es.
c) Írjuk fel az ($a_1\, a_2 \ldots\, a_k$) ciklust (1 i) alakú transzpozíciók szorzatként, ha az a_j-k között nem szerepel az 1-es.
d) Mutassuk meg, hogy az (1 3 5 2 4) permutáció felírható négy transzpozíció szorzataként, de kevesebb szorzataként nem írható fel. Mit állíthatunk általában egy ötelemű ciklusról?
e) Mutassuk meg, hogy általában egy k elemű ciklus előáll k–1 transzpozíció szorzataként, de kevesebb transzpozíció szorzataként nem áll elő.

MEGOLDÁS: a) Az (1 3 5 2 4) permutáció eredménye az 45123 permutáció. Ezt kell transzpozíciókkal előállítanunk. Kezdjük azzal, hogy az 4-est átvisszük az 1-esbe. Ezt az (1 4) transzpozícióval érhetjük el. E csere eredménye a 42315 sorrend lesz. Ez a transzpozíció az 1-est a 4-es helyére viszi. De a 4-es helyére a 2-est kell vinni, tehát most az 1-est ki kell cserélni a 2-essel, amit az (1 2) transzpozícióval tehetünk meg. Ennek hatására a 41325 sorrend jön létre. A 4-es és a 2-es már a helyén van, de most az 1-es a 2-es helyén van, ahova végül az 5-ösnek kell kerülnie. Ezt az (1 5) cserével érhetjük el. Ennek hatására a 45321 sorrend jön létre. Most már helyén van a 4-es, az 5-ös és a 2-es. Az 1-es most az 5-ös helyén van. Ide a 3-asnak kell kerülnie, tehát most az (1 3) cserét kell végrehajtanunk. Ennek eredményeképpen létrejön a kívánt 45123 sorrend. Tehát

(1 3 5 2 4) = (1 3)(1 5)(1 2)(1 4).

Ugyanezt az eredményt a „nyílas” jelöléssel sokkal egyszerűbben megkaphatjuk:
(1 3): 1→3, 3→1,
(1 5): 1→5, 5→1,
(1 2): 1→2, 2→1,
(1 4): 1→4, 4→1.

Ha ezeket a szokott módon „összerakjuk”, akkor az 1→3, 3→1→5, 5→1→2, 2→1→4 és 4→1 nyilakat kapjuk, vagyis valóban az 1→3→5→2→4→1 ciklus a végeredmény.

A (2 4 6 3 5) ciklus felírásához többféleképpen is eljuthatunk. Az egyik: az előző gondolatmenetet alkalmazva felírhatjuk, hogy

(2 4 6 3 5) = (2 4)(2 6)(2 3)(2 5),

majd minden (2 i) cserét felírhatunk (1 2)(1 i)(1 2) alakban:

(2 4 6 3 5) = (1 2)(1 4)(1 2)(1 2)(1 6)(1 2)(1 2)(1 3)(1 2)(1 2)(1 5)(1 2),

ezután felhasználjuk, hogy (1 2)-t kétszer egymás után alkalmazva éppen az identitást kapjuk, tehát

(2 4 6 3 5) = (1 2)(1 4)(1 6)(1 3)(1 5)(1 2).

b) Nyilván feltehetjük, hogy a_1=1. Az a) rész gondolatmenetével azt kapjuk, hogy

$(1\ a_2 \dots\ a_k) = (1\ a_2)(1\ a_3)\dots(1\ a_k)$.

c) Az a) rész gondolatmenetével most azt kapjuk, hogy

$(a_1\ a_2 \dots\ a_k) = (1\ a_1)(1\ a_2)(1\ a_3)\dots(1\ a_k)(1\ a_1)$.

d) Azt már láttuk a)-ban, hogy (1 3 5 2 4) felírható négy transzpozíció szorzataként. Azt kell csak belátnunk, hogy kevesebb szorzataként nem írható fel. Kettő szorzataként nem írható fel, mert a két transzpozíció összesen legfeljebb négy elemet mozgat, tehát legalább egy biztosan a helyén marad, márpedig az (1 3 5 2 4) permutációban nincs fixpont. Tegyük fel, hogy sikerül előállítanunk három transzpozíció szorzataként:

$(1\ 3\ 5\ 2\ 4) = (a_1\ b_1)\ (a_2\ b_2)\ (a_3\ b_3)$.

A jobb oldalon nyilván kell szerepelnie mind az öt számnak, hiszen a bal oldal mind az öt számot mozgatja. Elvileg elképzelhető, hogy szerepel egy hatodik szám is, ami a bal oldalon nem szerepel. De ekkor a jobb oldalon három diszjunkt transzpozíció áll, s ezek szorzata a 9. feladat szerint másodrendű, míg a bal oldal ötödrendű, ami ellentmondás. Azt kapjuk, hogy a jobb oldalon szereplő hat szám között pontosan kettő azonos. Nyilván feltehető, hogy valamelyik két a_i azonos, hiszen mindegy, hogy egy transzpozícióban melyik elemet írjuk előre. Tegyük fel először, hogy $a_1 = a_2$. Ekkor $(a_1\ b_1)(a_2\ b_2) = (a_1\ b_1)(a_1\ b_2) = (a_1\ b_1\ b_2)$, s ez harmadrendű. Azt kapjuk, hogy

$(1\ 3\ 5\ 2\ 4) = (a_1\ b_1\ b_2)\ (a_3\ b_3)$,

s itt a jobb oldalon álló két ciklus diszjunkt, tehát szorzatuk – megint csak a 9. feladat szerint – hat. Ez ismét ellentmondás. Pontosan így járhatunk el akkor is, ha $a_2 = a_3$, ekkor a második és harmadik transzpozíció szorzata harmadrendű, s ezt szorozzuk a tőle diszjunkt másodrendű ciklussal, tehát megint csak hatodrendű lesz a jobb oldal.
Marad az az eset, ha $a_1 = a_3$. De ekkor az $(a_2\ b_2)$ és az $(a_3\ b_3)$ ciklus diszjunkt, tehát sorrendjük felcserélhető, vagyis
$(a_1\ b_1)\ (a_2\ b_2)\ (a_3\ b_3) = (a_1\ b_1)\ (a_3\ b_3)\ (a_2\ b_2)$,

s így már alkalmazható az előző gondolatmenet.
Megjegyezzük, hogy természetesen ugyanez a bizonyítás megy minden ötelemű ciklusra. Vagyis beláttuk azt is, hogy ötelemű ciklus előáll négy transzpozíció szorzataként, de kevesebb szorzataként nem áll elő.

e) Láttuk b)-ben, hogy egy k elemű ciklus előáll k–1 transzpozíció szorzataként. Ha általában akarjuk bebizonyítani, hogy egy k elemű ciklus nem áll elő k–2 (vagy kevesebb) transzpozíció szorzataként, akkor másképp kell eljárnunk, mint d)-ben tettük. Tegyük fel, hogy a $(c_1\ c_2 \dots\ c_k)$ ciklust sikerült előállítanunk m darab transzpozíció szorzataként:

$(c_1\, c_2 \ldots c_k) = (a_1\, b_1)(a_2\, b_2) \ldots (a_m\, b_m)$.

Szorozzuk meg mindkét oldalt balról $(a_1\, b_2)$-vel, aztán $(a_2\, b_2)$-vel, majd sorban az összes transzpozícióval, utoljára $(a_m\, b_m)$-mel. Ekkor a jobb oldal így alakul:

$(a_m\, b_m)(a_{m-1}\, b_{m-1})\ldots(a_2\, b_2)(a_1\, b_1)(a_1\, b_1)(a_2\, b_2) \ldots (a_m\, b_m)$.

Ha egy transzpozíciót kétszer alkalmazunk egymás után, akkor végeredményben semmi nem történik, tehát szorzatuk kiesik. Így ebből a szorzatból kihúzhatjuk az $(a_1\, b_1)(a_1\, b_1)$ szorzatot. De akkor a két $(a_2\, b_2)$ kerül egymás mellé, ezek szorzata is az identitás, tehát kihúzható. Ezt folytatva azt kapjuk, hogy a fenti szorzat az identitás, azaz csupa egyelemű ciklusból áll.
Most vizsgáljuk meg, mi történik a bal oldalon. Ott a következő szorzatot kapjuk:

$(a_m\, b_m)(a_{m-1}\, b_{m-1})\ldots(a_2\, b_2)(a_1\, b_1)(c_1\, c_2 \ldots c_k)$.

Vagyis egy k elemű szorzatot szorzunk meg m darab transzpozícióval. Be fogjuk látni a következő állítást:

1. LEMMA:
Ha egy ciklust megszorzunk két benne szereplő elem transzpozíciójával, akkor a ciklus két ciklusra esik szét.
Ha pedig két diszjunkt ciklust megszorzunk egy olyan transzpozícióval, amely két különböző ciklusban levő elemet cserél fel, akkor a két ciklusból egy ciklus lesz. (Megjegyezzük, hogy ez utóbbi állítás akkor is igaz, ha az egyik ciklus egyelemű.)

Ebből az állításból már következik, hogy a $(c_1\, c_2 \ldots c_k)$ ciklust az $(a_1\, b_1)$ cserével szorozva legfeljebb két ciklust kapunk, ezt az $(a_2\, b_2)$ cserével szorozva vagy ismét egy ciklust, vagy három ciklust kapunk (attól függően, hogy a_2 és b_2 ugyanabban a ciklusban volt-e vagy másikban. Ugyanígy haladva tovább azt kapjuk, hogy minden cserével szorozva legfeljebb eggyel nő a ciklusok száma. Kezdetben egy darab ciklus volt, tehát a végeredmény legfeljebb m+1 ciklus lehet. Márpedig a végeredményről tudjuk, hogy csupa egyelemű ciklusból, tehát (legalább) k ciklusból áll. Ezért $m+1 \geq k$. Ami pontosan azt jelenti, hogy legalább k–1 csere kellett a k elemű ciklus előállításához.

Hátra van még a dőlt betűs Lemma bizonyítása.

15. feladat:
Bizonyítsuk be az 1. lemmát!

BIZONYÍTÁS: Az egyszerűség kedvéért az (1 2 3 … k) ciklusra bizonyítjuk az első állítást. Nyilvánvaló, hogy ezzel nem vétünk az általánosság ellen, hiszen a ciklus elemeit átszámozhatjuk. Szorozzuk meg ezt az (i j) cserével, ahol $1 \le i < j \le k$:

$(i\ j)(1\ 2\ \dots\ i\ i{+}1\ \dots\ j\ j{+}1\ \dots\ k) = (1\ 2\ \dots\ i\ j{+}1\ \dots\ k)(i{+}1\ \dots\ j{-}1\ j)$,

tehát az eredeti ciklus valóban két ciklusra bomlott.
Ugyanígy ellenőrizhető az állítás, ha a másik oldalról szorzunk (i j)-vel.
Másrészt tegyük fel, hogy ($a_1\ a_2\ \dots\ a_m$) és ($b_1\ b_2\ \dots\ b_n$) két diszjunkt ciklus és szorozzuk meg a szorzatukat az ($a_1\ b_1$) cserével. (Megint nem megy az általánosság rovására az, hogy a két ciklus első elemét cseréljük, hiszen egy ciklust bármely eleménél elkezdhetünk írni.):

$(a_1\ b_1)(a_1\ a_2\ \dots\ a_m)(b_1\ b_2\ \dots\ b_n) = (a_1\ b_2\ \dots\ b_n\ b_1\ a_2\ a_3\ \dots\ a_m)$,

tehát a két ciklusból valóban egy ciklus lesz. Ugyanígy számolható ki, hogy hasonlóan egy ciklust kapunk, ha ($a_1\ b_1$)-gyel jobbról szorzunk.

A 14. feladat e) részéből már következik, hogy n–2 transzpozíció nem elég $\mathbf{S}_n$ generálásához, hiszen már az n elemű ciklusokat sem generálja ennyi transzpozíció. Vagyis beláttuk, hogy

$\mathbf{S}_n$ *generálható n–1 transzpozícióval, de kevesebbel nem.*

Az is megmutatható, hogy n–1 transzpozíció pontosan akkor elég $\mathbf{S}_n$ generálásához, ha összefüggő (tehát fa) az a gráf, amelynek pontjai az 1,2,…,n számok és két pont akkor van összekötve, ha transzpozíciójuk szerepel az n–1 transzpozíció között. Ennek bizonyítása megtalálható a Gráfelmélet könyvben, lásd a IV/63. feladatot és megoldását.

16. feladat:
Van-e $\mathbf{S}_n$-nek kételemű generátorrendszere?

MEGOLDÁS: Azt már tudjuk, hogy a cserék (transzpozíciók) generálják $\mathbf{S}_n$-et. Azt kell csak eldöntenünk, hogy van-e két olyan eleme $\mathbf{S}_n$-nek, amely minden cserét generál. Sőt, a 14.c feladat szerint az is elég, ha minden (1 i) alakú cserét generál. Nyilván célszerű az egyik elemnek például az (1 2) cserét választani. Ha a másik elemnek például a (2 3 … n) ciklust választjuk, akkor lényegében arról van szó, hogy van egy „tárcsánk”: ez a (2 3 …, n), ezt tudjuk „forgatni”. Az (1 2) pedig az 1-est ki tudja cserélni a 2-essel.
Tehát a következőt tehetjük: először elforgatjuk a tárcsát úgy, hogy a 2-es az i helyére kerüljön. Ezután kicseréljük az 1-est és a 2-est, most már az 1-es az i helyén lesz, ha a tárcsát visszaforgatjuk.
A (2 3 … n) ciklust annyiadik hatványra kell emelnünk, ahány hellyel arrébb akarjuk vinni az elemeket. A 2-t akarjuk az i helyére vinni, tehát i–2-edik hatványra kell emelnünk. Ezután következik az (1 2) csere, majd a visszaforgatás. A „vissza”-forgatás azt jelenti, hogy annyival forgatjuk „előre”, hogy összesen n–1-gyel forgassuk arrébb az elemeket: ekkor fog minden elem a helyére visszakerülni (természetesen az 1-est kivéve). Ez azt jelenti, hogy most a (2 3 … n) ciklust n–1–(i–2) = n–i+1-edik hatványra kell emelnünk:

$$(1\ i) = (2\ 3\ \dots\ n)^{n-i+1}(1\ 2)(2\ 3\ \dots\ n)^{i-2}.$$

Valóban ellenőrizhetjük, hogy ez történik. Balról jobbra olvasva a 2, 3, …, n elemekhez először n–i+1-et kell hozzáadni (túlcsordulás esetén pedig n–1-et még levonni). Az i-ediket kivéve, amely a 2-esbe kerül, a többit az (1 2) nem mozgatja, majd még i–2-t kell hozzáadnunk mindegyikhez. Így összesen n–1-et, azaz mod n–1 nullát adtunk hozzá minden elemhez, tehát minden elem a helyén maradt. Az i elemhez n–i+1-et adva éppen a 2-est kapjuk, ezt a nyilakkal történő ábrázolásban az $i\to2$ nyíl jelöli. Az (1 2) cserét a $2\to1$ (és az $1\to2$) nyíl jelöli, majd az 1-esből nem mutat tovább nyíl a harmadik ciklusban, mert ott nem szerepel. Tehát az i valóban az 1-esbe kerül. Hátra van még 1-es sorsa. Ezt az első ciklus nem mozgatja, az (1 2) cserét az $1\to2$ nyíl jelöli, az utolsó ciklusban pedig a 2-eshez i–2-t kell adni, tehát ott a $2\to i$ nyíl szerepel. Ezeket összerakva az $1\to i$ nyilat kapjuk, vagyis Az 1 és i elemeket valóban felcseréli a fenti felírás, a többit pedig a helyén hagyja.

Ezzel beláttuk, hogy

az (1 2) és a (2 3 … n) permutációk generálják az $\mathbf{S}_n$ szimmetrikus csoportot.

MEGJEGYZÉS: Ugyanígy generálja az $\mathbf{S}_n$ csoportot bármely n–1 hosszú ciklus és egy olyan csere, amely e ciklus egy elemét a kimaradó elemmel cseréli fel. Érdemes utána gondolni, hogy (1 2) és (1 2 … n) is generálja-e.

17. feladat:
Generálja-e valamely n–2 elemű ciklus és egy csere az $\mathbf{S}_n$ csoportot?

MEGOLDÁS: Két eset van: ha az n–2 elemű ciklusnak és a cserének van közös eleme, akkor egy elem kimarad, azt tehát egyikük sem mozgatja, így egyetlen olyan permutáció sem állítható elő belőlük, amely ezt az elemet mozgatja.
Ha viszont nincs közös elemük, akkor a cserében szereplő két elemet csak egymás között tudjuk cserélni, a ciklusban levőket is, tehát egyetlen olyan permutáció sem állítható elő, amely a ciklus egy elemét és a csere egy elemét felcseréli.
Egy n–2 elemű ciklus és egy csere tehát nem generálhatja $\mathbf{S}_n$-et.
MEGJEGYZÉS: Természetesen ugyanez igaz minden legfeljebb n–2 elemű ciklusra.

Térjünk még vissza a 15. feladatra, vagyis az 1. lemma bizonyítására. Ha pontosabban megnézzük, amit bizonyítottunk, a következő állítást is megkapjuk:

Ha egy τ permutációt jobbról is, balról is megszorzunk az (a b) transzpozícióval, akkor a kapott (a b)τ(a b) permutációban a és b helyet cserél, a többi elem változatlanul marad.

18.feladat:
Bizonyítsuk be ezt az állítást!

MEGOLDÁS: Két eset van. Ha a és b ρ-ban különböző ciklusban van, akkor legyen e két ciklus $(a\ a_1\ a_2 \dots\ a_k)$ és $(b\ b_1\ b_2\ \dots\ b_m)$. A felsorolt $k+m+2$ elem mind különböző. Ekkor

$$(a\ b)(a\ a_1\ a_2 \dots\ a_k)(b\ b_1\ b_2\ \dots\ b_m) = (a\ b_1\ b_2\ \dots\ b_m\ b\ a_1\ a_2 \dots\ a_k).$$

Ha most ez utóbbi ciklust jobbról megszorozzuk az $(a\ b)$ transzpozícióval, akkor az eredmény

$$(a\ b_1\ b_2\ \dots\ b_m\ b\ a_1\ a_2 \dots\ a_k)(a\ b) = (a\ b_1\ b_2\ \dots\ b_m)(b\ a_1\ a_2 \dots\ a_k).$$

tehát valóban annyi történik, hogy a és b helyet cserél.

A második eset az, amikor a és b-ban azonos ciklusban szerepel. Írjuk fel ezt a ciklust $(a\ b_1\ b_2\ \dots\ b_m\ b\ a_1\ a_2 \dots\ a_k)$ alakban és alkalmazzuk az utóbbi egyenletet: e szerint az $(a\ b)$ transzpozícióval jobbról való szorzás e ciklust a két a és b közötti ívekre vágja ketté. Most alkalmazhatjuk az előbbi egyenletet, ha felcseréljük a_i-k és b_j-k szerepét, és azt kapjuk, hogy $(a\ b)$-vel balról szorozva a kapott

$$(a\ b)(a\ b_1\ b_2\ \dots\ b_m)(b\ a_1\ a_2 \dots\ a_k) = (a\ a_1\ a_2\ \dots\ a_m\ b\ b_1\ b_2 \dots\ b_k) = (b\ b_1\ b_2 \dots\ b_k\ a\ a_1\ a_2\ \dots\ a_m)$$

ciklusban valóban annyi történt az eredeti $(a\ b_1\ b_2\ \dots\ b_m\ b\ a_1\ a_2 \dots\ a_k)$ ciklushoz képest, hogy a és b helyet cserélt.

A 14.b és 14.c feladatban láttuk, hogy tetszőleges permutáció felírható olyan transzpozíciók szorzataként, amelyek mindegyike ugyanazt az elemet cseréli ki egy-egy másik elemmel. (Ott

az állandó elem az 1-es volt.) Írjuk fel ennek alapján a σ permutációt σ = $(a\ b_1)(a\ b_2)\ldots(a\ b_m)$ alakban. A fenti állítás szerint ha egy tetszőleges ρ permutációt megszorzunk először balról és jobbról $(a\ b_m)$-mel, akkor a kapott ρ_1 permutációban annyi történik, hogy a és b_m helyet cserél. Ha most ρ_1-et megszorozzuk balról is, jobbról is az $(a\ b_{m-1})$ transzpozícióval, akkor a kapott $(a\ b_{m-1})\rho_1(a\ b_{m-1}) = \rho_2$ permutációban a és b_{m-1} cserél helyet. Mire eljutunk az

$(a\ b_1)(a\ b_2)\ldots(a\ b_m)\ \rho\ (a\ b_m)\ldots(a\ b_2)(a\ b_1)$

permutációhoz, a sorra helyet cserél minden b_i-vel. Ez önmagában is fontos észrevétel. De vegyük még észre azt is, hogy eközben ρ ciklusszerkezete nem változik! Másrészt nézzük, mivel szoroztuk meg ρ-t. Balról a σ permutációval. Jobbról viszont éppen σ inverzével! A következő állítást kapjuk:

Tetszőleges s ***és*** r ***permutációkra igaz, hogy*** r ***ciklusszerkezete megegyezik*** $s\ r\ s^{-1}$ ***ciklusszerkezetével.***

DEFINÍCIÓ: Tetszőleges σ permutációra a $\sigma\rho\sigma^{-1}$ permutációt a ρ permutáció **konjugáltjának** nevezzük.
Megjegyezzük, hogy ha $\rho' = \sigma\rho\sigma^{-1}$ konjugáltja ρ-nak, akkor fordítva, $\rho = \sigma^{-1}\rho'\sigma$ is konjugáltja ρ'-nek. Másrészt megjegyezzük azt is, hogy a konjugálás minden csoportban ugyanígy definiálható.

Az előbb kapott állítás így is fogalmazható:

Tetszőleges permutáció ciklusszerkezete megegyezik a konjugáltjai ciklusszerkezetével.

Érdemes elgondolkozni azon is, hogy ha két permutáció ciklusszerkezete azonos, következik-e ebből, hogy egymás konjugáltjai.

19. feladat:
Korábban megállapítottuk, hogy bár σρ és ρσ általában nem ugyanazt az eredményt adják, de a két eredmény ciklikus szerkezete példáinkban mindig megegyezett. Vajon így van-e ez mindig?

MEGOLDÁS: A most megfogalmazott állítás szerint a feladat állítása rögtön következik abból, hogy

$\sigma(\rho\sigma)\sigma^{-1} = \sigma\rho$,

tehát ρσ és σρ egymás konjugáltjai.

26. szakkör (Csoportelméleti alapfogalmak 5.)

F) PÁROS ÉS PÁRATLAN PERMUTÁCIÓK

A 14.e feladat szerint négy elem minden permutációja felírható legfeljebb három transzpozíció szorzataként. Hogy ez mit jelent, azt a szabályos tetraéderen szemléltethetjük. A szabályos tetraédernek négy csúcsa van, ezek egy permutációja a négy csúcsot valamilyen sorrendben átrendezi. Első pillanatra nem világos, hogy bárhogyan számozzuk is át a szabályos tetraéder csúcsait, mindig van a térnek olyan egybevágósága, amelynek a tetraéder csúcsain ez az átszámozás az eredménye. De tudjuk, hogy minden ilyen permutáció előállítható transzpozíciók szorzataként. Egy transzpozíció két csúcs cseréjét jelenti, a másik két csúcs a helyén marad. Ezt a két csúcs felezőmerőlegesére való tükrözéssel érhetjük el. Így azt kapjuk, hogy a tetraéder csúcsainak bármely átszámozása elérhető legfeljebb három élfelező merőlegesre való tükrözéssel.

Először is csoportosítsuk ezeket a permutációkat illetve transzformációkat a szerint, hogy hány csere illetve tükrözés eredményeképpen jönnek létre.

20. feladat:
Állapítsuk meg, hány olyan transzformáció van, amely a szabályos tetraédert önmagába viszi és 0, 1, 2, illetve három transzpozíció eredménye.

MEGOLDÁS:
0 transzpozíció/tükrözés: az identitás, ebből csak egy van.

1 transzpozíció/tükrözés: ebből annyi van, ahány él (ahány csúcspár): vagyis hat.

2 transzpozíció/tükrözés: ez kétféle lehet. Az egyik esetben a két élnek, amelyre tükrözünk, van közös pontja, a második esetben nincs. A második esetet könnyű megszámolni: itt két szemközti él felezőmerőlegesére tükrözünk. Minthogy a két ciklusnak nincs közös eleme, ezért mindegy, milyen sorrendben hajtjuk végre őket. Tehát csak azt kell megszámolnunk, hány szemközti élpár van a tetraéderben: nyilvánvalóan három. A három szemközti élpárra való tükrözés nyilván három különböző transzformációt eredményez.
Marad az az eset, amikor a két élnek, amelyek felezőmerőlegesére tükrözünk, van közös csúcsa. Ez a csúcs négyféle lehet, a két másik csúcsot pedig 3·2 féleképpen választhatjuk ki. Ez összesen 24 eset lenne. Csakhogy ezek között már vannak azonosak. Ha a közös csúcs P, a másik két csúcs Q és R (ilyen sorrendben), akkor a $(P\ Q)(P\ R) = (P\ Q\ R)$ permutációról van szó, s ez megegyezik például a $(Q\ R\ P) = (Q\ R)(Q\ P)$ permutációval. Itt tehát másféle módon kell számolnunk: minden ilyen transzformációt egy három elemű ciklus határoz meg, tehát a háromelemű ciklusokat kell megszámolnunk. A kimaradó csúcs négyféle lehet és a maradó három elemet kétféle képpen lehet ciklusba rendezni. Ez tehát nyolc transzformáció. (Egy-egy csúcs körüli két forgatásról van szó: +120°-os és –120°-os forgatásról.) Összesen tehát 11 olyan transzformáció van, amely két élre való tükrözés eredménye.

3 transzpozíció/tükrözés: Három élt kiválasztani már nagyon sok féleképpen lehet, s ha például egy lap három élét választjuk ki, s azok felezőmerőleges síkjaira tükrözünk, akkor a negyedik csúcs és a háromszög egyik csúcsai is a helyén marad, ez geometriailag is belátható, de kiszámolható algebrailag is. Ha a háromszög PQR háromszög PQ,QR,RP oldalainak felezőmerőlegeseire tükrözünk, akkor Q (és a negyedik csúcs) marad a helyén: $(P\ Q)(Q\ R)(P\ Q) = (P\ R)(Q)$. Az ilyen transzformációkat tehát már megszámoltuk az egy síkra való tükrözések között. Másrészt $(P\ Q)(Q\ R)(R\ S) = (P\ S\ R\ Q) = (P\ S)(P\ R)(P\ Q)$, tehát két teljesen különböző hármas is adhatja ugyanazt az eredményt. Most tehát másképp kell számolnunk. Nézzük meg, hogy négy elem permutációinak milyen lehet a ciklikus szerkezete, melyek azok, amelyek nem állnak elő háromnál kevesebb transzpozíció szorzataként. Az ilyen permutációk nem állhatnak egy vagy két kételemű ciklusból (transzpozícióból). De nem állhatnak egy háromelemű (és egy egyelemű) ciklusból sem, mert a 14.e feladat szerint ezek előállnak két transzpozíció szorzataként. Maradnak a négyelemű ciklusok. Tehát csak a négyelemű ciklusok nem állnak elő kevesebb transzpozíció szorzataként, csak a nekik megfelelő transzformációk nem állnak elő háromnál kevesebb élfelezőmerőleges síkra való tükrözéssel. A tetraéder négy csúcsából négyelemű ciklust hatféleképpen képezhetünk, tehát ilyen transzformációból hat van.

Csoportosítsuk a kapott transzformációkat a szerint, hogy megtartják-e a tetraéder irányítását, vagy megváltoztatják. Tudjuk, hogy egy síkra való tükrözés (azaz egy transzpozíció) megváltoztatja az irányítást. Ebből következik, hogy a 0 és a 2 síkra való tükrözés irányítástartó, az 1 és 3 síkra való tükrözés irányításváltó. Az előbbiből 1+11=12 van, az utóbbiból 6+6=12. Vagyis:

A térnek a szabályos tetraédert önmagába vivő egybevágósági transzformációi közül ugyanannyi* (12) *irányítástartó, mint irányításváltó.

Nemsokára látni fogjuk, hogy ez az állítás egy általánosabb csoportelméleti tény speciális eseteként is felfogható.

Magától értetődően használtuk az „irányítás” fogalmát a szemlélet alapján. A szemlélet alapján világos az is, hogy ha egy transzformáció irányítástartó, akkor nem lehet irányításváltó is. Vagyis hogy van értelme az irányításról beszélni. Felmerül a azonban a kérdés, hogy biztosak lehetünk-e ebben. Persze ha elgondoljuk, hogy a jobb kezünket bajosan tudnánk „átvinni” a bal kezünkbe, akkor a válasz egyértelműnek tűnik. Csakhogy megint a szemléletre hivatkozva hisszük el, hogy az „irányításváltó” azt jelenti, hogy a bal és a jobb kezünket felcseréli, az „irányítástartó” pedig nem cseréli fel. A kérdésre tehát más választ kell keresnünk, s ezt tulajdonképpen a 20. feladat fenti megoldása már magában foglalja. A tetraéder csúcsait ugyanis pontosan 24 féleképpen lehet permutálni. Márpedig a 18. feladat megoldásában pontosan ennyi permutációt találtunk, nem többet. Tehát nincs közöttük ismétlődés. Márpedig az összes 0,1,2 és 3 tükrözéssel előállítható transzformációt megszámoltuk. Ez viszont azt jelenti, hogy nem lehetséges, hogy egy transzformációt például egy és két tükrözéssel is előállíthatunk, vagyis nem lehetséges, hogy egy transzformáció irányításváltó is legyen és irányítástartó is.

De vajon valóban ennyire megnyugtató-e, amit kaptunk. Nem biztos. Ugyanis az eddigiek még megengedik például, hogy egy transzformáció előálljon három és négy tükrözéssel is! S ez esetben mégis lenne olyan transzformáció, amely egyszerre irányításváltó is és irányítástartó is. Megjegyezzük, hogy végig lehetne nézni, hogy a tetraéder minden négy tükrözéssel előállítható egybevágósági transzformációja (vagyis a tetraéder csúcsainak minden négy cserével előállítható permutációja) előáll (nulla vagy) két tükrözéssel is, s ez esetben már kész is vagyunk legalább annak bizonyításával, hogy a négy tükrözéssel előállítható (tehát irányítástartó) transzformációk nem lehetnek irányításváltók. Ez azonban sok számolással járna. Az öt- és több tükrözéssel előállítható transzformációkkal már nem kell foglalkoznunk, hiszen egy ismert geometriai tétel szerint a tér minden egybevágósága előáll legfeljebb négy síkra való tükrözéssel, s ezekről már egyértelműen eldöntöttük, hogy irányítástartók-e vagy irányításváltók.

Most egy más utat választunk:

21. feladat:
Bizonyítsuk be, hogy nincs olyan permutáció, amely előállítható lenne páros sok transzpozíció szorzataként is és páratlan sok transzpozíció szorzatként is.

MEGOLDÁS: Ha jobban szemügyre vesszük a 14.e feladat bizonyítását, ott a következőket láttuk be. Először, ha a $(c_1\, c_2 \ldots c_k)$ permutáció előáll m darab csere szorzatként, vagyis

$$(c_1\, c_2 \ldots c_k) = (a_1\, b_1)(a_2\, b_2) \ldots (a_m\, b_m),$$

akkor a

$$(a_m\, b_m)(a_{m-1}\, b_{m-1})\ldots(a_2\, b_2)(a_1\, b_1)(c_1\, c_2 \ldots c_k)$$

permutáció az identitás. Másrészt a LEMMA szerint (lásd 15. feladat) ha egy

permutációt megszorzunk egy transzpozícióval, ennek eredményeképp vagy egy ciklussá fűzünk össze két ciklust (beleértve azt az esetet is, amikor az egyik ciklus egyelemű volt), vagy épp fordítva, két ciklusra bontunk egy ciklust. Vagyis egy transzpozícióval való szorzás a ciklusok számát pontosan eggyel változtatja meg. Ebből minket csak annyi érdekel, hogy egy transzpozícióval való szorzás a ciklusok számának paritását megváltoztatja. A fenti szorzatban tehát a ciklusszám paritása m-szer fog megváltozni, s a végeredmény az identitás, ami nem függ m-től, csak attól, hogy hány eleme van a permutáció alaphalmazának. Ha tehát az alaphalmaznak n eleme van (a permutáció n elemet mozgat), akkor a $k+m$ és n paritása meg kell, hogy egyezzen, vagyis $k+m-n$ mindenképpen páros. Ebből viszont következik, hogy m paritása meg van határozva: egyenlő $k-n$ paritásával. Ezt akartuk belátni.

MEGJEGYZÉS: A most bizonyított tétel tehát azt mondja ki, hogy van értelme páros és páratlan permutációkról beszélni:

DEFINÍCIÓ: Egy permutációt **párosnak** nevezünk, ha páros sok transzpozíció szorzataként állítható elő, és **páratlannak** nevezünk, ha páratlan sok transzpozíció szorzataként állítható elő.
A 14.e feladat szerint minden permutáció előáll transzpozíciók szorzataként, tehát a fenti definíció minden permutációra érvényes, és a 21. feladat szerint nincs olyan permutáció, amely páros is volna és páratlan is, tehát minden permutációról egyértelműen eldönthető, hogy páros vagy páratlan.
Ez egyben azt is jelenti, hogy a tetraédernek sincsen egyszerre páros és páratlan permutációja, tehát valóban van értelme az irányításnak: a tetraéder páros permutációi az irányítástartó permutációk, a páratlan permutációk az irányításváltók.
Magasabb dimenzióban viszont éppen a most bizonyított tételt használhatjuk az irányítás definiálásához!
Megjegyezzük, hogy a páros és páratlan permutációk határozzák meg a determináns kifejtési tagjainak előjelét is.
Végül megjegyezzük, hogy a páros és páratlan permutációk sok szempontból úgy viselkednek, mint a pozitív és a negatív számok. Két páros permutáció szorzata is páros, két páratlan permutációé is. Viszont egy páros és egy páratlan permutáció szorzata páratlan.

22. feladat:
Bizonyítsuk be ez utóbbi állítást!

BIZONYÍTÁS: Ha egy σ permutáció előáll m transzpozíció szorzataként, egy σ' permutáció pedig m' transzpozíció szorzataként, akkor a szorzatuk, $\sigma\sigma'$ előáll $m+m'$ transzpozíció szorzataként. Ez pedig pontosan akkor páros, ha m és m' paritása megegyezik. Vagyis a szorzat pontosan akkor lesz páros permutáció, ha a két permutáció azonos paritású volt.

Korábban beláttuk, hogy a szabályos tetraéder csúcsainak ugyanannyi (12) páros és páratlan permutációja van. A szabályos tetraéder csúcsain ható permutációk csoportja definíció szerint $\mathbf{S}_4$. $\mathbf{S}_4$-ben tehát ugyanannyi páros és páratlan permutáció van. De ez általánosan is igaz.

23. feladat:
a) Bizonyítsuk be, hogy $\mathbf{S}_3$-ban ugyanannyi páros és páratlan permutáció van.
b) Bizonyítsuk be, hogy $\mathbf{S}_n$-ben ugyanannyi páros és páratlan permutáció van.

MEGOLDÁS: a) $\mathbf{S}_3$ felfogható úgy is, mint ami a szabályos háromszög csúcsainak permutációiból áll. Egy csere (transzpozíció) most egy oldal két végpontját cseréli ki, vagyis egy oldal felezőmerőlegesére való tükrözést jelent. A három forgatás nyilván két-két felezőmerőlegesre való tükrözést jelent, míg a három oldalfelezőmerőlegesre való tükrözés egy oldalfelező merőlegesre való tükrözést jelent. A forgatások páros permutációt eredményeznek, mert előállíthatók két transzpozíció szorzataként. A tengelyes tükrözések páratlant, mert előállnak egy transzpozícióból. Mindkettőből három van.

b) Általában, n elem esetén az n dimenziós szimplexszel kellene okoskodnunk, de ez nem olyan szemléletes (és az irányítást sem definiálhatjuk szemléletesen), így helyette a következőt tesszük. Veszünk egy tetszőleges transzpozíciót, mondjuk azt, amely az 1 és 2 elemet cseréli fel (nyilván feltehetjük, hogy az alaphalmaz n eleme az $1,2,\ldots,n$ számok). Szorozzuk végig ezzel az (1 2) cserével $\mathbf{S}_n$ összes permutációját. Az (1 2) csere páratlan, tehát a vele való szorzás minden permutáció paritását megváltoztatja. Ha kezdetben p darab páros és q darab páratlan permutáció volt, akkor a szorzás után p darab páratlan és q darab páros permutációt kapunk. De az (1 2) permutációval való szorzás eredményeképpen minden permutációt megkapunk (és mindegyiket pontosan egyszer), így például minden párosat is megkapunk. Tehát a páratlanok száma, q, megegyezik a párosak számával, p-vel. Ezt akartuk bizonyítani.

MEGJEGYZÉS: 1. Mit használtunk, amikor azt mondtuk, hogy az (1 2) permutációval való szorzás eredményeképpen minden permutációt megkapunk (éspedig pontosan egyszer)?

2. A fenti bizonyításban összesen két dolgot használtunk. Egyrészt azt, hogy permutációk egy csoportjáról (vagyis permutációcsoportról) van szó. Másrészt azt, hogy ebben a csoportban van egy páratlan permutáció. A fenti bizonyítás azt adja, hogy általában igaz a következő tétel:

Ha egy permutációcsoportban van páratlan permutáció, akkor a páros és páratlan permutációk száma megegyezik.

Befejezésül egy feladatot ismertetünk, amely az 1999-es olimpián szerepelt a kitűzésre javasolt feladatok között. (A feladatot több részre bontottuk.)

24. feladat:
Egy lányosztály n tanulója közül mindegyik kezében van egy labda. Azt játsszák, hogy mindenki mindenkivel egyszer labdát cserél. A cserék sorrendje tetszőleges, és amikor két lány sorra kerül, kicserélik az éppen kezükben levő labdát. Az a kérdés, hogy milyen n-ekre van a cseréknek olyan sorrendje, amely mellett mindenki a saját labdáját kapja vissza végül. Állapítsuk meg, hogy van-e a cseréknek ilyen sorrendje
a) n=3-ra; b) n=6-ra; c) n=7-re; d) n=10-re?
Adjuk meg a cserék megfelelő sorrendjét
e) n=4-re; f) n=8-ra; g) általában néggyel osztható n-ekre; h) n=5-re, i) általában $n=4k+1$ alakú számokra.
j) Állapítsuk meg, hogy milyen n-ekre van még megfelelő sorrend.

MEGOLDÁS: Általában megállapíthatjuk, hogy n elem összes transzpozícióját kell olyan sorrendben összeszorozni, hogy az eredmény az identitás legyen.
a) n=3-ra minden sorrend $(a\ b)(b\ c)(c\ a)$ alakú, s ennek eredményeképp a helyén marad, de b és c helyet cserél. Tehát n=3-ra nincs jó sorrend.
b) n=6-ra a végrehajtandó cserék száma 15, s ez páratlan, tehát a szorzatuk nem lehet az identitás, mert az páros permutáció.
c) és d) Ugyanígy kapjuk, hogy n=7-re és n=10-re is páratlan sok cserét kell végrehajtani, tehát nem jöhet ki az identitás eredményül.
j) Általában is igaz, hogy megfelelő sorrend csak akkor lehet, ha $n(n-1)/2$ páros, vagyis ha $n=4k$ vagy $n=4k+1$ alakú. Tehát $n=4k+2$ és $4k+3$ alakú számokra nincs megfelelő sorrend. A következők azt mutatják, hogy $n=4k$ és $n=4k+1$ alakú számokrav viszont van.
e) n=4-re megfelelő az (1 2)(2 3)(1 4)(2 4)(1 3)(3 4) sorrend.
f) n = 8-ra a következőt csináljuk. Láttuk e)-ben, hogy négy lány ki tudja cserélni a labdákat úgy, hogy végül mind a négyen a saját labdájukat kapják vissza. A nyolc lányt két négyes csoportra osztva végrehajtjuk ezt a cseresorrendet mindkét csoportban, ilyen például az

(1 2)(2 3)(1 4)(2 4)(1 3)(3 4)(5 6)(6 7)(5 8)(6 8)(5 7)(7 8)

sorrend. Ezután már csak a két négyes csoport közötti tizenhat cserét kell úgy megszervezni, hogy végül mindenki a saját labdájához jusson hozzá.
Ehhez vegyük észre, hogy ha e)-ben kihagyjuk az elejéről az (1 2) cserét, a végéről a (3 4) cserét, akkor a maradó (2 3)(1 4)(2 4)(1 3) eredménye az (1 2)(3 4). Ha tehát a 3-ast és 4-est például az 5-ös és 6-ossal helyettesítjük, akkor a (2 5)(1 6)(2 6)(1 5) cserék eredménye (1 2)(5 6). Ugyanígy a (2 7)(1 8)(2 8)(1 7) cserék eredménye is (1 2)(7 8). Tehát

(2 5)(1 6)(2 6)(1 5)(2 7)(1 8)(2 8)(1 7) = (5 6)(7 8).

Ha most ugyanezeket a cseréket az 1 és 2 helyett a 3 és 4 számokkal hajtjuk végre, akkor ugyanezt a végeredményt kapjuk:

(4 5)(3 6)(4 6)(3 5)(4 7)(3 8)(4 8)(3 7) = (5 6)(7 8).

Ha tehát a két csere sort végrehajtjuk, mindenki a saját labdájához jut vissza a végén. Másrészt minden cserét végrehajtottunk a két csoport között.

Ezzel n=8-ra megoldottuk a feladatot.

g) Ugyanúgy járhatunk el, mint f)-ben: a lányokat négyes csoportokra bontjuk, minden csoportban végrehajtjuk azt a hat cserét, amely során mindenkihez a saját labdája kerül vissza, majd minden két négyes csoport között is végrehajtjuk azt a tizenhat cserét, amelynek következtében mindenkihez a saját labdája kerül vissza.

h) Most az n=4-re adott megoldásba, tehát az (1 2)(2 3)(1 4)(2 4)(1 3)(3 4) cseresorozatba beillesztünk két blokkot, ami nem zavarja meg a sorrendet:

(1 5)(1 2)(2 5) (2 3)(1 4)(2 4)(1 3) (3 5)(3 4)(4 5)

is az identitást adja.

i) A h) ponthoz hasonlóan most is az n=4k alakú számokra adott megoldásból indulunk ki. Ott k darab négyes csoportra osztottuk a lányokat és először mindegyik csoportban végrehajtottuk azt a hat cserét, amelynek eredményeképpen mindenki a saját labdáját kapja vissza. Most az 4k+1-edik lányt minden ilyen négyes csoportba beiktatjuk a h)-ban látott módon, így ez a lány már mindenkivel cserélt egyszer és mindenki, így ő is a saját labdáját tartja kézben. Ez után a négyes csoportok közötti cseréket hajtjuk végre, így végül minden csere megvolt és mindenki a saját labdáját fogja a kezében.

MEGJEGYZÉS: Feltehető az a kérdés is, hogy milyen n-ekre van olyan sorrendje a cseréknek, amelynek végeredményeképpen mindenki valaki más labdáját kapja meg. Könnyen belátható, hogy n=3-ra nincs megfelelő sorrend. Páros n-ekre megfelelő a következő sorrend:

(1 2)(1 3)…(1 n) (2 3)(2 4)…(2 n) … (i i+1)(i i+2)…(i n) … (n–1 n).

Vagyis először az első lány cserél sorban a többivel labdát, aztán a második sorban azokkal, akikkel még nem cserélt, az i-edik blokkban az i-edik lány cserél sorban mindenkivel labdát, akivel még nem cserélt. Ennek a sorrendnek az eredménye a következőképpen számolható ki egyszerűen. A 14.b és c feladatban láttuk, hogy

(i i+1)(i i+2)…(i n) = (i i+1 i+2… n),

tehát

(1 2)(1 3)…(1 n) (2 3)(2 4)…(2 n) … (i i+1)(i i+2)…(i n) … (n–1 n) =
(1 2 … n) (2 3 … n) … (i i+1 i+2… n) … (n–1 n) =
(1 n) (2 n–1) … (i n–i+1) … (½n ½n+1).

Ha n páros, akkor i és n–i+1 nem lehet egyenlő, tehát ennek a sorrendnek az eredményében nincs fixpont, és ezt akartuk.
Ha n=2k+1 páratlan, akkor lesz egy fixpont. Ekkor az első n számra ugyanazt hajtjuk végre, de eléírjuk a következőt:
(1 2k+1)(2 2k+1)…(k 2k+1)(2k 2k+1)(2k–1 2k+1)…(k+1 2k+1).

Az így kapott sorrendnek nem lesz fixpontja.