1. Részcsoportok

A részcsoport fogalma

2.2.15. Definíció
Legyen G csoport. A $H \subseteq G$ részhalmaz *részcsoport*, ha maga is csoport G műveleteire nézve. Jele: $H \leq G$.

Az altér fogalmához hasonlít.

Példák

(1) $\mathbb{C}^+ \geq \mathbb{R}^+ \geq \mathbb{Q}^+ \geq \mathbb{Z}^+$.

(2) $\mathbb{C}^\times \geq \mathbb{R}^\times \geq \mathbb{Q}^\times$.

(3) $\mathbb{Q}^\times$ *nem* részcsoportja $\mathbb{C}^+$-nak, mert más a művelet!

(4) $\mathbb{Z}_5^+$ *nem* részcsoportja $\mathbb{Z}^+$-nak: $6 = 2 + 4 \neq 2 +_5 4 = 1$.

(5) A páros permutációk részcsoportot alkotnak S_n-ben.
Neve *alternáló csoport*, jele A_n.

(6) A mozgások (forgatások) részcsoport $\mathrm{O}(2)$-ben, jele $\mathrm{SO}(2)$.

A részcsoport jellemzése

Tétel (2.2.16. Feladat)
Legyen G csoport, melyben a művelet jele $*$. A $H \subseteq G$ nem üres részhalmaz pontosan akkor részcsoport, ha

(1) *H zárt a szorzásra*, azaz tetszőleges $h_1, h_2 \in H$ esetén $h_1 * h_2 \in H$.

(2) *H tartalmazza G neutrális elemét.*

(3) *H zárt a G-beli inverzképzésre*, azaz tetszőleges $h \in H$ esetén $h^{-1} \in H$.

Állítás (4.4.27. Feladat)

(1) Részcsoportok metszete is részcsoport.

(2) Két részcsoport uniója *csak akkor* részcsoport, ha valamelyikük tartalmazza a másikat. $\square$

Komplexusműveletek

4.4.2. Definíció
Ha X és Y tetszőleges részhalmazai egy G csoportnak,
akkor $XY = \{xy : x \in X, y \in Y\}$ az X és Y *komplexusszorzata*,
és $X^{-1} = \{x^{-1} : x \in X\}$ az X *komplexusinverze*.

Alterek összege (vektortérben) szintén komplexusösszeg.

Tétel (4.4.4. Gyakorlat, <u>HF</u>)
Egy G csoport egy H nem üres részhalmazára ekvivalens:

(1) H részcsoport.

(2) $HH = H^{-1} = H$.

(3) $HH^{-1} \subseteq H$.

Ha H részcsoport és $h \in H$, akkor $hH = Hh = H$. Minden részcsoport tartalmazza a neutrális elemet.

2. Mellékosztályok

Lagrange tétele

Lagrange tétele (4.4.11)
Véges csoport minden részcsoportjának elemszáma osztója a csoport elemszámának (bizonyítás később).

<u>Elnevezések:</u> A csoport *elemszáma* a csoport *rendje*, jele $|G|$.
Valódi részcsoport: nem az egész csoport.
Triviális részcsoport: az egész csoport, és az $\{1\}$ részcsoport.

Prímrendű csoportnak csak két részcsoportja van: a triviálisak.

Bizonyítás
Ha a G csoport elemszáma a p prím, akkor Lagrange tétele miatt minden H részcsoport rendje csak 1 vagy p lehet. Ha $|H| = p$, akkor $H = G$. Ha $|H| = 1$, akkor $H = \{1\}$. □

Mellékosztályok

A Lagrange-tétel bizonyításának vázlata
Ha $H \leq G$, akkor a G csoportot felbontjuk gH alakú halmazokra. Ezek mindegyikének elemszáma ugyanaz lesz, mint H elemszáma. Páronként diszjunktak lesznek, így $|G| = k|H|$, ahol k ezeknek a részhalmazoknak a száma.

4.4.6. Definíció
Ha $H \leq G$ és $g \in G$, akkor $gH = \{gh : h \in H\}$ bal oldali, $Hg = \{hg : h \in H\}$ jobb oldali H szerinti *mellékosztály*.

Példa
$G = \mathbb{C}^+$, $H = \mathbb{R}^+$. Ekkor a H szerinti mellékosztályok az x-tengellyel (a valós tengellyel) párhuzamos egyenesek.
Például $(2+3i)+H = (8+3i)+H$ az $y=3$ egyenletű egyenes.

A mellékosztályok diszjunktak

Lemma (4.4.14. Gyakorlat)
Legyen $H \leq G$ és $a, b \in G$. Ha $a \in bH$, akkor $aH = bH$.

Bizonyítás
Mivel $a \in bH$, ezért $a = bh$ alkalmas $h \in H$ elemre. Ekkor $aH = bhH = bH$, mert $hH = H$. □

A $hH = H$ bizonyításában felhasználtuk az inverz létezését!

4.4.13. Következmény
Ha cH-nak és dH-nak van közös eleme, akkor egyenlők.

Bizonyítás
Ha $a \in cH \cap dH$, akkor az előző miatt $cH = aH = dH$. □

Részcsoport indexe

A Lagrange-tétel bizonyítása
Ha $H \leq G$ és $g \in G$, akkor $h \mapsto gh$ kölcsönösen egyértelmű megfeleltetés H és gH között (az egyszerűsítési szabály miatt). Ezért minden mellékosztály elemszáma $|H|$. A mellékosztályok egyesítése az egész G, mert $g \in gH$. Az egyenlő mellékosztályok közül csak egyet vegyünk, ezek páronként diszjunktak. Ha számuk k, akkor $|G| = k|H|$. □

4.4.12. Definíció
Ha $H \leq G$, akkor a különböző H szerinti bal mellékosztályok számát a H részcsoport G-beli *indexének* hívjuk, jele $|G : H|$.

Tehát véges csoportban $|G| = |H||G : H|$.
A bal és jobb mellékosztályok száma megegyezik, mert $(gH) \leftrightarrow (gH)^{-1} = Hg^{-1}$ bijektív megfeleltetés (4.4.18. Feladat).

3. Ciklikus részcsoportok

Egy elem által generált részcsoport

Állítás (4.3.14. Gyakorlat)
Ha G csoport és $g \in G$, akkor a g elem egész kitevőjű hatványai részcsoportot alkotnak G-ben (HF). Ez a g *által generált részcsoport*, jele $\langle g \rangle$. A $\langle g \rangle$ részcsoport rendje ugyanaz, mint a g elem rendje.

4.4.21. Következmény
Minden elem rendje osztója a csoport rendjének, így $g^{|G|} = 1$.

A második állítás igaz, mert $o(g) \Big| |G|$ miatt $|G|$ jó kitevője g-nek.

4.4.21. Következmény
Ebből következik a számelméletben tanult Euler–Fermat-tétel.
$G = \mathbb{Z}_n^\times$, ekkor $|G| = \varphi(n)$, így ha $(g, n) = 1$, akkor $g^{\varphi(n)} \equiv 1$ (n).

Csoportok kevés részcsoporttal

4.4.23. Tétel
Egy G csoportnak akkor és csak akkor van pontosan két részcsoportja (a két triviális részcsoport), ha G *prímrendű.* Ilyenkor G ciklikus csoport (és így kommutatív).

Bizonyítás
Láttuk, hogy prímrendű csoportnak csak két részcsoportja van. Tegyük föl, hogy G-nek pontosan két részcsoportja van. Ekkor $|G| > 1$, és így G-nek létezik 1-től különböző eleme. Minden ilyen g-re a feltétel miatt $\langle g \rangle = G$, azaz G ciklikus. Nem lehet $G \cong \mathbb{Z}^+$, mert itt a páros számok részcsoport. Ha $o(g) = n (\neq 1)$ és p prímosztója n-nek, akkor a hatvány rendjének képlete miatt $h = g^{n/p}$ rendje p. Így $1 \neq h$ is generálja G-t, azaz G prímrendű és ciklikus. □

Ciklikus részcsoportja ciklikus

4.3.26. Lemma
Ciklikus csoport minden részcsoportja ciklikus.

Bizonyítás
Legyen $G = \langle g \rangle$ és $H \leq G$. Ha $H = \{1\}$, akkor ciklikus. Ha nem, akkor van olyan $k \neq 0$, hogy $g^k \in H$. Ekkor $g^{-k} = (g^k)^{-1} \in H$, azaz van ilyen pozitív k is. Legyen m a *legkisebb pozitív* egész, melyre $g^m \in H$. Megmutatjuk, hogy ekkor $\langle g^m \rangle = H$. Nyilván $\langle g^m \rangle \subseteq H$. Ha $g^k \in H$, akkor $k = mq + r$ ahol $0 \leq r < m$. Ekkor $g^r = g^{k-mq} = g^k(g^m)^{-q} \in H$, hiszen $g^k, g^m \in H$. Mivel m minimális pozitív volt, csak $r = 0$ lehetséges. Ezért $g^k = (g^m)^q$, vagyis g^k hatványa g^m-nek. Így $H \subseteq \langle g^m \rangle$. □

Így $\mathbb{Z}^+$ részcsoportjai az m-mel osztható számok minden m-re.

A ciklikus csoportok részcsoportjai

4.3.24. és 4.3.27. Állítás
Ha G egy n rendű (véges) ciklikus csoport, akkor n minden pozitív d osztójához pontosan egy d rendű részcsoport létezik. Ez $g^{n/d}$ hatványaiból áll, ahol $\langle g \rangle = G$. G bármely két d rendű eleme egymás hatványa, számuk $\varphi(d)$.

Bizonyítás
Ha H egy d rendű részcsoport, akkor legyen $g^k \in H$. Lagrange tétele miatt $(g^k)^d = 1$, azaz $n \mid kd$, így $(n/d) \mid k$. Az n/d számnak $0, 1, \ldots, n-1$ között csak d többszöröse van, ezért H csakis a $g^{n/d}$ elem d darab hatványából állhat. Ha $h \in G$ rendje d, akkor $\langle h \rangle$ rendje d, ezért $\langle h \rangle = H$, azaz $h \in H$. Így H generátorelemei pontosan G-nek a d rendű elemei. $\square$

4. Pálya és stabilizátor

Permutációcsoportok

4.5.1 Definíció
Legyen X halmaz, ennek elemeit néha *pontoknak* hívjuk. Az S_X szimmetrikus csoport részcsoportjait *transzformációcsoportoknak*, illetve véges X esetén *permutációcsoportoknak* nevezzük.

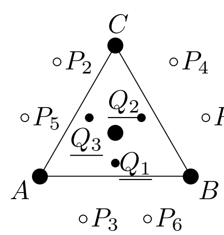
Ezek sokszor úgy keletkeznek, hogy egy alakzat összes szimmetriáit vesszük (példák szerepeltek az első előadáson).

Példák
A szabályos n-szögnek $2n$ szimmetriája van (4.1.23).
Egy rombusznak, ami nem négyzet, 4 szimmetriája van.
Egy téglalapnak, ami nem négyzet, úgyszintén (4.5.27).
Egy kockának 48 szimmetriája van.

Hogyan lehet ezeket megszámolni?

Példa pályára és stabilizátorra

X a sík, G az ABC szabályos háromszög szimmetriacsoportja. A $G = D_3$ diédercsoport elemei: 3 forgatás, 3 tükrözés. Alkalmazzuk egy rögzített pontra a G csoport összes elemét.



P_1 *pályája*: ahová G elemei el tudják vinni

P_1 *pályája* hatelemű

Q_1 *pályája* háromelemű,
mert AB felező merőlegesén van

A középpont *pályája* egyelemű

P_1-et 1 transzformáció hagyja fixen (csak az identitás).
Q_1-et 2 transzformáció hagyja fixen (egy tükrözés is).
A középpontot 6 transzformáció hagyja fixen (mindegyik).

(Pálya elemszáma) $\times$ (fixáló trafók száma) $=$ csoport rendje

A pálya és stabilizátor elemszámának összefüggése
Legyen $G \leq S_X$ transzformációcsoport és $x \in X$.

4.5.5. Definíció
A $g(x)$ alakú pontok halmazát, ahol g befutja G elemeit, az x *pályájának* (orbitjának) nevezzük, és $G(x)$-szel jelöljük. A pálya elemszámát a pálya *hosszának* hívjuk.

4.5.2. Definíció
Tekintsük azokat a $g \in G$ elemeket, melyek x-et *fixen hagyják*, azaz $g(x) = x$. Ezek nyilván részcsoportot alkotnak G-ben, melynek neve az x pont G-beli *stabilizátora*, jele G_x.

4.5.8. Tétel
Egy pont pályájának a hossza a stabilizátorának az indexe.
Képletben: $|G(x)| = |G : G_x|$, és így $|G(x)| \cdot |G_x| = |G|$.

A stabilizátor szerinti mellékosztály jelentése

4.5.3. Lemma
Legyen $G \leq S_X$, $g \in G$, $x \in X$ és $y = g(x)$. Ekkor azok az $f \in G$ elemek, melyekre $f(x) = y$, a gG_x mellékosztályt alkotják.

Bizonyítás
Mivel $g(x) = y$, ezért tetszőleges $f \in G$ esetén
$f(x) = y \iff g^{-1}f(x) = x \iff g^{-1}f \in G_x \iff f \in gG_x$. $\square$

A pálya-stabilizátor tétel bizonyítása
$\forall y \in G(x)$-hez hozzárendeljük: $\alpha(y) = \{f \in G : f(x) = y\}$.
A Lemma szerint ez a halmaz egy G_x szerinti bal mellékosztály.
<u>α szürjektív:</u> Ha $g \in G$ és $y = g(x) \in G(x)$, akkor $gG_x = \alpha(y)$.
<u>α injektív:</u> Ha $y_1 \neq y_2$, akkor $\alpha(y_1) \neq \alpha(y_2)$, mert ha g közös elemük lenne, akkor $y_1 = g(x) = y_2$ teljesülne. $\square$

5. A pályák partíciót alkotnak

A pályák diszjunktak
Legyen X a sík.

Ha G az O pont körüli forgatások csoportja, akkor minden $P \in X$ pályája egy O körüli *körvonal* (kivéve O pályája $\{O\}$).

Ha G az x-tengellyel párhuzamos eltolások csoportja, akkor minden $P \in X$ pályája egy x-tengellyel párhuzamos *egyenes*.

Mindkét esetben a pályák páronként diszjunkt halmazokra osztják fel a síkot, azaz a sík egy *partícióját* alkotják.

4.5.6. Állítás
Legyen $G \leq S_X$ transzformációcsoport. Ekkor G összes pályái az X halmaz egy partícióját alkotják, vagyis a pályák páronként diszjunktak, és egyesítésük az egész X.
<u>Elnevezés:</u> G *tranzitív*, ha az egész X egyetlen pálya.

Ekvivalenciareláció

4.4.8. Definíció, E.1. Függelék
Az R relációt *ekvivalenciarelációnak* nevezzük, ha bármely $x, y, z \in X$ esetén teljesül az alábbi három tulajdonság.

(1) R *reflexív*, azaz $x\ R\ x$ minden x-re.

(2) R *szimmetrikus*, azaz ha $x\ R\ y$, akkor $y\ R\ x$.

(3) R *tranzitív*, azaz ha $x\ R\ y$ és $y\ R\ z$, akkor $x\ R\ z$.

4.4.9. Tétel, <u>HF</u>
Ha R ekvivalenciareláció az X halmazon és $a \in X$ esetén R_a azoknak az X-beli x elemeknek a halmaza, melyekre $a\ R\ x$, akkor az R_a halmazok az X egy partícióját adják. □

Az R_a halmazok között lehetnek egyenlők; az állítást úgy kell érteni, hogy bármely kettő vagy egyenlő, vagy diszjunkt.

Példák ekvivalenciarelációra

Az egész számok halmazán a *kongruenciák*.
Pl. $m\ R\ n$ akkor és csak akkor, ha $m \equiv n$ (3) (azaz $3 \mid m - n$).
Ekkor három osztály van: a modulo 3 *maradékosztályok*.
Például R_6 a hárommal osztható számok halmaza.

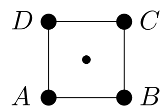
Az előző általánosításaként legyen H részcsoport G-ben.
$a\ R\ b$ akkor és csak akkor, ha $ab^{-1} \in H$.
Ekkor b osztálya $R_b = bH$ (bal oldali mellékosztály).
Lagrange tételét így is bizonyíthattuk volna!

Legyen $G \leq S_X$ transzformációcsoport.
$x\ R\ y$ akkor és csak akkor, ha $g(x) = y$ alkalmas $g \in G$-re.
Ekkor R_x az $x \in X$ pályája, így a pályák partíciót alkotnak. □

Mindhárom esetben ellenőrizni kell, hogy R ekvivalenciareláció!

6. Leszámlálási alkalmazások

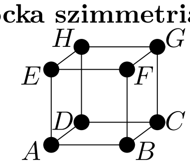
A négyzet szimmetriáinak a száma



$ABCD$ egy négyzet,
G a szimmetriacsoportja.

A G elemei a négyzet csúcsait permutálják. A G *tranzitív*: bármely csúcs bármely másikba átforgatható. Ezért az A csúcs pályája *négyelemű*: $\{A, B, C, D\}$.
Legyen $H = G_A \leq G$ az A csúcs stabilizátora. Ekkor $|G| = 4|H|$.
Mely csúcsokba viheti egy $h \in H$ elem a B csúcsot?
Mivel h távolságtartó, AB hossza egyenlő $h(A)h(B)$ hosszával. De $h(A) = A$, ezért $h(B)$ nem lehet C. Ha $h = id$ akkor $h(B) = B$. Ha h az AC-re tükrözés: $h(B) = D$. Ezért H-nál a B pályája $\{B, D\}$, azaz *kételemű*. A H_B stabilizátor egyelemű, mert A, B-t G-ben csak id fixálja. Így $|H| = 2|H_B| = 2$. Tehát $|G| = 4|H| = 4 \cdot 2 = 8$.

A kocka szimmetriáinak a száma



$ABCDEFGH$ egy kocka,
G a szimmetriacsoportja.

4.5.9. Állítás
A átvihető B-be az AB felező merőleges síkjára tükrözéssel. Hasonlóan minden csúcs a szomszédjába, ezért G *tranzitív*.
Így az A csúcs pályája *nyolcelemű*: $\{A, B, C, D, E, F, G, H\}$.
Legyen $H = G_A \leq G$ az A csúcs stabilizátora. Ekkor $|G| = 8|H|$.
Minden $h \in H$ távolságtartó és $h(A) = A$, így $h(B) \in \{B, D, E\}$. Ezeket meg is kapjuk AG körüli forgatással ($\pm 120°$). Ezért H-nál a B pályája *háromelemű*, és így $|H| = 3|H_B|$.
Legyen $L = H_B$, ennél C pályája a *kételemű* $\{C, F\}$ (HF).
Végül L-ben C stabilizátora már egyelemű lesz (HF).
Így $|G| = 8|H| = 8 \cdot 3|L| = 8 \cdot 3 \cdot 2|L_C| = 8 \cdot 3 \cdot 2 \cdot 1 = 48$.

7. Lényegesen különböző megoldások

Burnside-(Cauchy-Frobenius-)lemma

4.5.30. Feladat
Ha $G \leq S_X$ permutációcsoport, akkor G pályáinak száma éppen a G elemei fixpontjainak átlagos száma.

Példa

Legyen $G = A_4$. Ez tranzitív, a pályák száma 1. Az egységelemnek 4 fixpontja van. A hármasciklusoknak 1 fixpontja van, 8 darab hármasciklus. Az $(ab)(cd)$ alakú permutációknak 0 fixpontja van, 3 darab. Az átlag: $\dfrac{4 + 8 \cdot 1 + 3 \cdot 0}{12} = 1$.

Olyan leszámlálási feladatoknál hasznos, ahol bizonyos megoldásokat „nem tekintünk különbözőnek." Ezek valamilyen *szimmetriával* vihetők egymásba.

Egy leszámlálási feladat

A 3×3-as sakktáblán hányféleképp választhatunk két mezőt? És ha a forgatással egymásba vihető megoldásokat azonosnak vesszük? És ha a tükrözéssel egymásba vihetőket is?

Mivel $3 \cdot 3$ mező van, az első kérdésre a válasz $\binom{9}{2} = 36$.

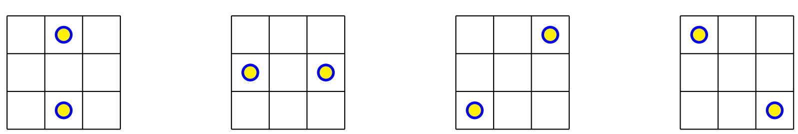
Legyen G a négy forgatásból álló (ciklikus) csoport, ez permutálja a 36 megoldást. Két megoldás akkor vihető forgatással egymásba, ha egy pályán vannak. Ezért a második kérdés a pályák száma!

A feladat harmadik kérdésénél a csoport a négyzet szimmetriacsoportja, azaz a D_4 diédercsoport.

A feladat megoldása

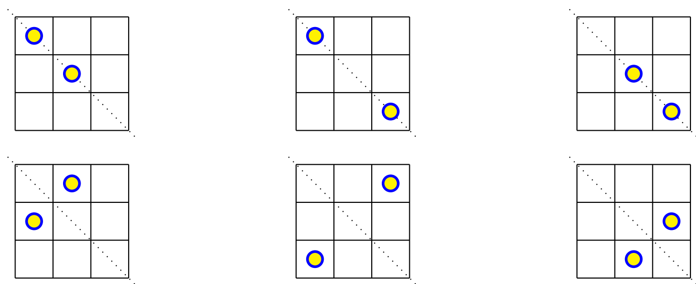
A 3×3-as sakktáblán hányféleképp választhatunk két mezőt, ha a forgatással egymásba vihető megoldásokat azonosnak vesszük?

Ki kell számolnunk a fixpontok átlagos számát.
Az identitásnak nyilván 36 fixpontja van.
A $180°$-os forgatásnak a középpontra tükrös megoldások a fixpontjai. Ezek száma $(9 - 1)/2 = 4$.
Egyik $90°$-os forgatásnak sincs fixpontja a 36 között (ehhez 1, vagy legalább 4 mezőt kellene választani a feladatban). Így a pályák száma $(36+4+2 \cdot 0)/4 = 10$.



A forgatás és tükrözés esete

Ha tükrözést is megengedünk, akkor nyolc szimmetria van. Az identitás, illetve a forgatások fixpontjainak száma ugyanaz, mint az előző esetben. Mind a négy tengelyes tükrözés esetében hat fixpont van, ebből három olyan, ahol a kiválasztott mezők a tengelyen vannak. Az eredmény $(36+4+2\cdot 0+4\cdot 6)/8 = 8$.



Négy csúcsú gráfok

Négy számozott csúcson $2^{\binom{4}{2}} = 64$ gráf van. És izomorfia erejéig? Az S_4 teljes szimmetrikus csoport permutálja ezeket a gráfokat.

identitás	1 permutáció	64 gráf fixpont	$64 = 1 \cdot 64$
(123)	8 permutáció	4 gráf fixpont	$32 = 8 \cdot 4$
(1234)	6 permutáció	4 gráf fixpont	$24 = 6 \cdot 4$
(12)	6 permutáció	16 gráf fixpont	$96 = 6 \cdot 16$
(12)(34)	3 permutáció	16 gráf fixpont	$48 = 3 \cdot 16$
Összesen:	24 permutáció		$264 = 24 \cdot 11$

Tehát 11 darab nemizomorf négycsúcsú gráf van.

Az (123) permutáció ($1 \mapsto 2 \mapsto 3 \mapsto 1$ és $4 \mapsto 4$) fixpont-gráfjai:

A Burnside-lemma bizonyítása

Legyenek G pályái az X halmazon $O_1, \ldots, O_k$. (Ezek páronként nem metszik egymást és lefedik X-et.) Kétféleképpen megszámoljuk azokat a (g, A) párokat, ahol $g(A) = A$ (és $g \in G$, $A \in X$). A számuk legyen N.

Rögzített A mellett ez A stabilizátorának elemszáma. A pálya-stabilizátor tétel miatt a $|G|/|O_i|$ számokat kell összeadni, a $|G|/|O_i|$-t annyiszor, ahány eleme O_i-nek van. Ezért $N = k|G|$ (ahol k a pályák száma).

Rögzített g mellett g fixpontjainak számát kapjuk. Tehát N a fixpontok számának összege is egyúttal. A G elemszámával osztva az állítást kapjuk: a fixpontok számának átlaga a pályák száma. $\square$

Csoporthatás: Példa

4.5.29. Feladat
Egy kockának három szemköztes lappárja van. Ezeket a kocka G szimmetriacsoportja permutálja. Mik a pályák, és a stabilizátorok?

90 fokos forgatásokkal egymásba vihetők: tranzitív. Ezért a stabilizátorok G-nek $48/3 = 16$ elemű részcsoportjai.

Probléma:
G elemei egybevágósági transzformációk, a tér pontjait permutálják. G nem is részcsoportja a három lapból álló halmaz permutációiból álló csoportnak. Mit jelent a pálya és stabilizátor?

Megoldás: G elemei *„hatnak”* a szemköztes lappárok halmazán.
Ugyanígy: hatnak pl. a kocka éleinek halmazán is. Ha $g \in G$, akkor g az AB élt a $g(A)g(B)$ élbe *„viszi”*.

Csoporthatás: definíció

4.5.12. Definíció
A G csoport *hat* az X halmazon, ha minden $g \in G$ és $x \in X$ esetén értelmezve van $g * x \in X$ úgy, hogy
$g * (h * x) = (gh) * x$ (a szorzat kompozícióként hat), és
$1 * x = x$ (az egységelem identikusan hat).

Minden $G \leq S_X$ permutációcsoport hatás: $g * x = g(x)$.

4.5.14. Definíció
Ha G hat X-en, akkor $x \in X$ *pályája* $\{g(x) : g \in G\}$;
$g \in G$ *stabilizátora* $\{g \in G : g(x) = x\}$.

Mind a pálya-stabilizátor-tétel, mind a Burnside-lemma érvényes csoporthatásokra is, ugyanazzal a bizonyítással.