

1. Kristályok szimmetriái

Háromszög-szimmetria



Rubin
aluminium-oxid: Al_2O_3



Zafir



Kalcit
kalcium-karbonát: $CaCO_3$



Hematit
vasoxid: Fe_2O_3



Ametiszt
szilícium-dioxid: SiO_2



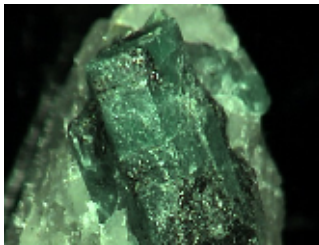
Kvarc

Hatszög-szimmetria

Berill (berillium–aluminium–szilikát): $Be_3Al_2(SiO_3)_6$
Egy szimmetriatengely körüli 60°-os elforgatás.



Vörös berill



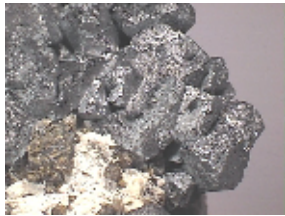
Smaragd



Akvamarin

Kocka-oktaéder-szimmetria

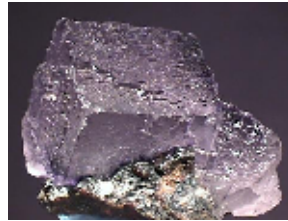
Összesen 48 szimmetria.



Galenit
ólom-szulfid: PbS



Gyémánt
szén: C



Fluorit
kalcium-fluorid: CaF_2

2. Szimmetriák a fizikában

A bolygómozgás szimmetriája

C.5.2. Példa: ekliptika

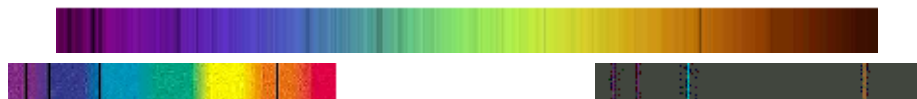
A bolygók keringése során a bolygó *energiája*, *perdületének nagysága* és *iránya* nem változik a mozgás során. A nap középpontja, a Föld középpontja és sebességvektora egy *síkot* határoz meg, melyre a kiindulóállapot *szimmetrikus*. Így az egész mozgás is tükörszimmetrikus, azaz a Föld mindvégig benne marad ebben a síkban.

C.5.4. Tétel

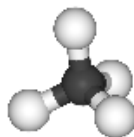
Emmy Noether eredménye szerint összefüggés van a *téridő szimmetriái* és a fizika *megmaradó mennyiségei* (lendület, energia, perdület) között.

Színképvonalak felhasadása

A Nap színképe, a hidrogén elnyelési és emissziós vonalai.



Metánmolekula: CH_4 , 24 szimmetria (szabályos tetraéder).



Zeeman-hatás: a mágneses tér a színképvonalakat két vagy három komponensre bontja szét. Oka: mágneses térben *megszűnnek egyes szimmetriák*.

Matematikai apparátus: a szimmetriák *csoportján* alapul.

Lorentz-transzformációk

A speciális relativitáselméletben a téridő szimmetriáit a *Lorentz-transzformációk* adják meg.



Lásd Kiss-jegyzet, 4.1. és C.6. szakasz. A C.7. szakaszban az Androméda-ködbe is elutazunk. A fenti kép az infravörös tartományban készült.

3. Matematikai alkalmazások

Kártyakeverés

„Emelés”: a csomag tetejéről az aljára teszünk egy lapot.

HF: Az emelés és a felső két lap cseréjének sokszori alkalmazásával minden sorrend megkapható (ha elég ügyesek vagyunk.)

Tétel

Ha mindkét mozdulatot $1/2$ valószínűséggel, függetlenül, nagyon sokszor, *véletlenszerűen* alkalmazzuk, akkor egy idő után a csomag *jól megkeveredik*, azaz a lapok minden sorrendjét közel egyforma valószínűséggel megkapjuk.

Sokkal általánosabban is igaz. Az $1/2$ helyett minden pozitív valószínűség jó, és a mozdulatok másmilyenek is lehetnek (csak ki lehessen keverni belőlük minden sorrendet). Bizonyítás: ugyanaz az apparátus, mint a metánmolekulánál.

Csoportok a geometriában

Sokféle geometriát hasznos vizsgálni. Példák:

- euklideszi geometria,
- Bolyai-geometria,
- gömbi geometria,
- projektív geometria.

Erlangeni program (Felix Klein, 1872). Általános vezérlő elv: milyen *szimmetriák* érvényesek. A „helyes” fogalmak ezek „nyelvén” definiálhatók.

Projektív geometriában az *egyenestartó* transzformációk. Ilyen például a *vetítés* (fényképezés, panorámaképek illesztése).

Számelméleti alkalmazások

Binom kongruenciák

Az $x^k \equiv a \pmod{p}$ kongruenciát akarjuk megoldani (p prím). Csoportok segítségével lineáris kongruenciává alakítható. Ezeket már meg tudjuk oldani euklideszi algoritmussal.

Dirichlet tétele

Ha $(a, b) = 1$ és $a \neq 0$, akkor van $ak + b$ alakú prím.

Bizonyítás (nagyon nehéz)

Két alapvető matematikai apparátust használ:

- Komplex függvények analízise, becslések;
- *csoportkarakterek* véges kommutatív csoportokra.

Szalay Mihály: Számelmélet (középiskolai tagozatos tankönyv).

További alkalmazások

- Logikai játékok (Rubik-kocka, 4×4 -es tologatós).
- Leszámlálási problémák (amikor például vannak „azonosnak” számító megoldások: *Burnside-lemma*).
- Egyenletek megoldhatósága (a legalább ötödfokú polinomok gyökeit általában nem lehet a négy alapművelettel és gyökvonásokkal meghatározni).
- Csomók (kibogozásának) elmélete.
- Felületek osztályozása (*homológiacsoportok*).
- Differenciálegyenletek megoldhatósága (*Lie-csoportok*).
- Képtömörítés wavelet-ek segítségével, Fast Fourier Transform.

A csoportelmélet rendkívül mély! A *véges egyszerű csoportok osztályozásának* bizonyítása több, mint *tízezer* oldal! Alkalmazásai: kombinatorikában, *algoritmuselméletben*.

4. A csoport fogalma

A csoport definíciója (lásd 19. Algebra és számelmélet dia)

2.2.13. Definíció (számozás: Kiss, Bevezetés az algebrába)

A G nem üres halmaz *csoport*, ha értelmezett rajta egy kétváltozós $*$ művelet úgy, hogy

- (1) a $*$ művelet *asszociatív*, azaz minden $g, h, k \in G$ esetén $(g*h)*k = g*(h*k)$;
- (2) létezik $e \in G$ kétoldali *neutrális elem*, melyre $e * g = g * e$ teljesül minden $g \in G$ -re; (**HF**: csak egy neutrális elem lehet)
- (3) minden $g \in G$ -nek van kétoldali g^{-1} *inverze*, melyre $g * g^{-1} = g^{-1} * g = e$. (**HF**: minden elemnek csak egy inverze lehet)

Kommutatív csoport, vagy *Abel-csoport*:

- (4) a $*$ *kommutatív*, azaz minden $g, h \in G$ esetén $g * h = h * g$.

A műveletek jelölése

Általában $*$ helyett egymás mellé írás, neve *szorzás*. A neutrális elem neve *egységelem*, jele 1. A g és h *fölcserélhető*, ha $gh = hg$.

HF: A gh inverze $(gh)^{-1} = h^{-1}g^{-1}$.

Kommutatív művelet jele gyakran $+$, neve *összeadás*. A neutrális elem neve *nullelem*, jele 0. Az inverz neve *ellentett*, jele $-g$.

A *kivonás* az ellentett hozzáadása: $g - h = g + (-h)$.

Asszociatív műveletnél egy *soktényezős* szorzatot akárhogy zárójelezünk, ugyanazt kapjuk (2.2.2. Feladat). Ha kommutatív is, akkor a tényezők sorrendje sem számít (2.2.5. Feladat).

5. Példák csoportokra

Additív és multiplikatív csoport

Minden R gyűrű (és vektortér) csoport az *összeadásra*.

Ez az R *additív csoportja*, jele R^+ .

Példák: $\mathbb{C}^+, \mathbb{R}^+, \mathbb{Q}^+, \mathbb{Z}^+, \mathbb{Z}_n^+, T^n, T^{n \times m}, \text{Hom}(V, W)$.

Ha R egységelemes gyűrű, akkor az invertálható elemek csoportot alkotnak a *szorzásra*. Ez az R *multiplikatív csoportja*, jele R^\times .

Példák: A nem nulla komplex/valós/racionális számok.

A \mathbb{Z}^\times csoport elemei 1 és -1 (a \mathbb{Z} gyűrű egységei).

$(T^{n \times n})^\times$ elemei a nem nulla determinánsú mátrixok. E csoport neve *általános lineáris csoport*, jele $\text{GL}(n, T)$.

HF: A \mathbb{Z}_n^\times csoport elemei $0, 1, \dots, n-1$ közül az n -hez *relatív prím* számok (2.2.3. Feladat). Speciálisan \mathbb{Z}_p^\times elemszáma $p-1$, ha p prím.

A kvaterniócsoport

4.5.21. Gyakorlat

Elemek: $\pm 1, \pm i, \pm j, \pm k$. Szabályok: $i^2 = j^2 = k^2 = -1$,
 $ij = k, jk = i, ki = j$, viszont $ji = -k, kj = -i, ik = -j$.
 Az asszociativitás ellenőrzése mátrixokkal a gyűrűknél.

Q	1	i	j	k	-1	$-i$	$-j$	$-k$
1	1	i	j	k	-1	$-i$	$-j$	$-k$
i	i	-1	k	$-j$	$-i$	1	$-k$	j
j	j	$-k$	-1	i	$-j$	k	1	$-i$
k	k	j	$-i$	-1	$-k$	$-j$	i	1
-1	-1	$-i$	$-j$	$-k$	1	i	j	k
$-i$	$-i$	1	$-k$	j	i	-1	k	$-j$
$-j$	$-j$	k	1	$-i$	j	$-k$	-1	i
$-k$	$-k$	$-j$	i	1	k	j	$-i$	-1

A szimmetrikus csoport

Legyen X halmaz. Az $X \rightarrow X$ kölcsönösen egyértelmű leképezéseket X *transzformációinak* nevezzük, halmazuk S_X .

Figyelem: A *lineáris transzformációk* között megengedtünk nem bijektíveket is! A mostani terminológia más.

Ha X véges, akkor inkább *permutációkról* beszélünk.

Ismétlés

Ha $f, g \in S_X$, akkor legyen $(f \circ g)(x) = f(g(x))$. $f \circ g$ az f és g *kompozíciója* vagy *szorzata*, jele néha fg . Ez asszociatív művelet, de általában nem kommutatív. Az identitás egységelem: $id(x) = x$ minden $x \in X$ -re. Minden $f \in S_X$ függvénynek van kétoldali inverze: $h = f^{-1}$ azt jelenti, hogy $f(x) = y \iff h(y) = x$. Ezért S_X csoport a kompozícióra. Neve: *szimmetrikus csoport*.

Ciklusfelbontás

4.2.17. Definíció (lásd 15. Algebra és számelmélet dia)

Legyen X halmaz és $x_1, x_2, x_3, \dots, x_{k-1}, x_k \in X$. Ekkor $(x_1, x_2, x_3, \dots, x_{k-1}, x_k)$ az a permutáció, amelynél $x_1 \mapsto x_2 \mapsto x_3 \mapsto \dots \mapsto x_{k-1} \mapsto x_k \mapsto x_1$, és X többi eleme a helyén (fixen) marad. Neve: *ciklus*, melynek *hossza* k .

Diszjunkt ciklusok: nincs közös elemük.

Tétel (4.2.21. és 4.2.22)

Ha X véges halmaz, akkor minden S_X -beli permutáció a sorrendtől eltekintve egyértelműen felírható páronként diszjunkt ciklusok szorzataként.

Példa: $\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 9 & 7 & 2 & 6 & 5 & 8 & 3 \end{bmatrix} = (14752)(39)$.

Az előjel kiszámítása

4.2.24. Következmény

Páros hosszú ciklus páratlan permutáció, páratlan hosszú ciklus páros permutáció. Egy permutáció pontosan akkor páratlan, ha ciklusfelbontásában a *páros* hosszú ciklusok száma *páratlan*.

Bizonyítás

HF: $(x_1 \dots x_k) = (x_1 x_2)(x_2 x_3) \dots (x_{k-2} x_{k-1})(x_{k-1} x_k)$.

Azaz egy k hosszú ciklus $k - 1$ darab transzpozíció szorzata. Használjuk föl, hogy $sg(fg) = sg(f)sg(g)$. \square

4.8.14. Gyakorlat, HF

Ha $f \in S_n$, akkor $f(x_1 \dots x_k) f^{-1} = (f(x_1) \dots f(x_k))$, így ha $g \in S_n$, akkor g és fgf^{-1} ugyanannyi, ugyanolyan hosszú ciklusból áll.

6. Szimmetriacsoportok

A háromszögek szimmetriái

Mik az ABC háromszög szimmetriái?

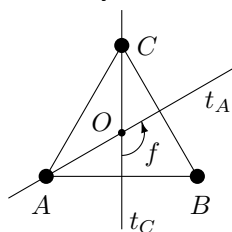
Ha egyenlő szárú, akkor *tükrözés* az alap felező merőlegesére. Ha szabályos, akkor a három tükrözés mellett három *forгатás*: a háromszög középpontja körül 120, 240, 0 fokkal. Ez utóbbi (az *identitás*) minden háromszögnek megvan.

Definíció

A háromszög szimmetriája a sík egy olyan *egybevágósági transzformációja*, ami a háromszöget önmagába képi. Ilyenek kompozíciója és inverze is ilyen. Ezért *a szimmetriák csoportot alkotnak*.

HF: A szabályos háromszögnek csak e hat szimmetriája van.

A szabályos háromszög szimmetriacsoportja



A t_A a BC felező merőlegesére tükrözés.

Az f az O körüli $+120$ fokos forгатás.

Az $f^2 = f \circ f$ a $+240$ fokos forгатás.

$$\begin{aligned} id &= \begin{bmatrix} A & B & C \\ A & B & C \end{bmatrix} & f &= \begin{bmatrix} A & B & C \\ B & C & A \end{bmatrix} & f^2 &= \begin{bmatrix} A & B & C \\ C & A & B \end{bmatrix} \\ t_A &= \begin{bmatrix} A & B & C \\ A & C & B \end{bmatrix} & t_B &= \begin{bmatrix} A & B & C \\ C & B & A \end{bmatrix} & t_C &= \begin{bmatrix} A & B & C \\ B & A & C \end{bmatrix} \end{aligned}$$

$ft_A = ?$ $A \mapsto A \mapsto B$; $B \mapsto C \mapsto A$; $C \mapsto B \mapsto C$. Azaz t_C .
 $t_C t_A = ?$ Forgatás a tengelyek szögének kétszeresével. Azaz f .

Cayley-táblázat

A csoport *szorzástáblája* (Cayley-táblázat): A g sorának és h oszlopának metszéspontjában gh .

D_3	id	f	f^2	t_A	t_B	t_C
id	id	f	f^2	t_A	t_B	t_C
f	f	f^2	id	t_C	t_A	t_B
f^2	f^2	id	f	t_B	t_C	t_A
t_A	t_A	t_B	t_C	id	f	f^2
t_B	t_B	t_C	t_A	f^2	id	f
t_C	t_C	t_A	t_B	f	f^2	id

D_3 elemei $\{id, f, f^2, t, tf, tf^2\}$, ahol $t = t_A$, $tf = t_B$, $tf^2 = t_C$.

Elég ennyit tudni: $f^3 = id$, $t^2 = id$, $tft = f^{-1} (= f^2)$.

Példa: $t_B t_C = (tf)(tf^2) = (tft)f^2 = f^{-1}f^2 = f$.

A diéderscsoport

A szabályos n -szög szimmetriacsoportja a D_n diéderscsoport.

Tétel (4.1.23. Állítás)

Legyen f a középpont körüli $2\pi/n$ szögű forgatás, t pedig a sokszög tetszőleges tengelyes szimmetriája.

Ekkor $D_n = \{f^0 = id = 1, f, f^2, \dots, f^{n-1}, t, tf, tf^2, \dots, tf^{n-1}\}$ (az első n transzformáció *forgatás*, a többi *tengelyes tükrözés*). A szabályos n -szögnek $2n$ szimmetriája van.

Érvényesek az $f^n = 1$, $t^2 = 1$, $tf^i t = f^{-i}$ összefüggések. Ezekből minden szorzat kiszámítható:

$$\begin{aligned} f^i f^j &= f^{i+j}, & (tf^i) f^j &= tf^{i+j}, \\ f^i (tf^j) &= tf^{j-i}, & (tf^i) (tf^j) &= f^{j-i}, \end{aligned}$$

ahol az f kitevőjében a $+$ és a $-$ jelek a mod n műveleteket jelentik. A tf^i elemek mindegyikének önmaga az inverze. \square

A kör és a gömb szimmetriacsoportja

A kör szimmetriacsoportjának jele $O(2)$.

Állítás (lásd 4.1. szakasz)

Az $O(2)$ elemei a középpont körüli α szögű f_α *forgatások*, továbbá az átmérőkre való *tengelyes tükrözések*. Nyilván $f_\alpha f_\beta = f_{\alpha+\beta}$ (az összeadás mod 360° értendő). Ha $t \in O(2)$ tükrözés, akkor $tf_\alpha t = f_{-\alpha} = f_\alpha^{-1}$. A tf_α és $f_\alpha t$ is tükrözés, két tükrözés szorzata pedig forgatás. \square

A gömb szimmetriacsoportjának jele $O(3)$.

Tétel (4.1.29. Feladat)

Az $O(3)$ irányítástartó elemei a középponton átmenő egyenesek körüli forgatások. A gömb többi szimmetriája egy ilyen forgatásnak és az xy síkra való tükrözésnek a szorzata.

A sík „szimmetriái”

$E(2)$, illetve $E(3)$ jelöli a sík, illetve a tér egybevágósági (távolságtartó) transzformációinak csoportját a kompozícióra.

4.1.13. Állítás

A sík egybevágósági transzformációi a következők.

- (1) Az *identitás*: minden pont *fixpont* ($id(P) = P$).
- (2) A nem identikus *eltolások*: nincs fixpontjuk.
- (3) A nem identikus *forgatások*: csak a forgáscentrum fixpont.
- (4) *Tengelyes tükrözések*: a fixpontok halmaza a tengely.
- (5) *Csúsztatva tükrözések* (egy tengelyre tükrözünk, utána a tengellyel párhuzamosan eltolunk): nincs fixpontjuk.

Az eltolások és a forgatások *mozgások* (irányítástartók), a tükrözések és a csúsztatva tükrözések nem. Minden egybevágóság előáll legfeljebb három tükrözés szorzataként.

7. Izomorf csoportok

A kételemű csoportok szerkezete

Legyen $G = \{1, b\}$ kételemű csoport, 1 az egységelem.

Ekkor $1 * 1 = 1$ és $1 * b = b = b * 1$. Mennyi lesz $b * b$? Csak 1 vagy b lehet.

Ha $b * b = b = b * 1$, akkor az egyszerűsítési szabály miatt $b = 1$ lenne, ami ellentmondás. Tehát $b * b = 1$. Vagyis az összes szorzatot ismerjük!

G	1	b	\mathbb{Z}^\times	1	-1	S_2	id	(12)	\mathbb{Z}_2^+	0	1
1	1	b	1	1	-1	id	id	(12)	0	0	1
b	b	1	-1	-1	1	(12)	(12)	id	1	1	0

E csoportok *teljesen EGYFORMA SZERKEZETŰEK!*

Képlettel: $\psi : 1 \mapsto id, -1 \mapsto (12)$ *bijektív és művelettartó*: $\psi(xy) = \psi(x)\psi(y)$.

Például $\psi((-1)(-1)) = id = \psi(-1)\psi(-1)$.

Példák izomorfizmusra

4.3.1. Definíció

Legyen G csoport a $*$ műveletre, és H csoport a \bullet műveletre. A $\psi : G \rightarrow H$ leképezés *csoporthomomorfizmus*, ha *művelettartó*: $\psi(a*b) = \psi(a)\bullet\psi(b)$ minden $a, b \in G$ -re. Ha ψ kölcsönösen egyértelmű is a G és H halmazok között, akkor ψ *izomorfizmus*. A G és a H *izomorf csoportok*, ha van közöttük izomorfizmus, jele $G \cong H$.

4.3.3. Példa

- (1) G a valós számok az összeadásra, H a pozitív valós számok a szorzásra, $\psi(g) = 10^g$.
- (2) G a sík P pontja körüli forgatások a kompozícióra, H a sík Q pontja körüli forgatások a kompozícióra, $\psi(g) = fgf^{-1}$, ahol f eltolás \overrightarrow{PQ} -val.

Példák négyelemű csoportra

\mathbb{Z}_5^\times	1	2	3	4	\mathbb{Z}_8^\times	1	3	5	7	\mathbb{Z}_4^+	0	1	2	3
1	1	2	3	4	1	1	3	5	7	0	0	1	2	3
2	2	4	1	3	3	3	1	7	5	1	1	2	3	0
3	3	1	4	2	5	5	7	1	3	2	2	3	0	1
4	4	3	2	1	7	7	5	3	1	3	3	0	1	2

Mely csoportok izomorfak ezek közül?

$\psi : \mathbb{Z}_4^+ \rightarrow \mathbb{Z}_5^\times$, $\psi(g) = 2^g$ (azaz $0 \mapsto 1$, $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 3$).

Ez művelettartó: $2^{x+y} = 2^x 2^y$, így $\mathbb{Z}_4^+ \cong \mathbb{Z}_5^\times$.

(Pontosabban azt kell ellenőrizni, hogy $2^{x+4y} = 2^x *_5 2^y$).

\mathbb{Z}_5^\times és \mathbb{Z}_8^\times *nem izomorfak*, mert utóbbinál $g * g = 1$ minden g -re, a másikban pedig nem (a két táblázat főátlójában látszik).

HF: izomorfizmusnál egységelem képe egységelem.

8. Elemrend

Hatványozás csoportban (ismétlés)

2.2.19. Definíció

Legyen $*$ asszociatív művelet és n pozitív egész. Ekkor a^n jelentse az n tényező $a * a * \dots * a$ szorzatot. Ez az a elem n -edik *hatványa*. Ha a művelet jele $+$, akkor a^n helyett na -t írunk. Ez az a elem n -szerese (*többszörös*).

Ha a $*$ szorzásra van 1 egységelem, akkor legyen $a^0 = 1$. Ha a $+$ összeadásra van nullelem, akkor legyen $0a = 0$.

Ha a -nak van egy b inverze, akkor legyen $a^{-n} = b^n$. Ha a -nak van egy b ellentettje, akkor legyen $(-n)a = nb$.

Értelmeztük az *egész kitevőjű* hatvány (többszörös) fogalmát.

A hatványozás tulajdonságai

2.2.20. Állítás

Legyenek a és b elemek egy G csoportban, ahol a művelet jele egymás mellé írás, és m, n egész számok. Ekkor a következők teljesülnek.

- (1) a^{-n} az a^n inverze.
- (2) $a^m a^n = a^{m+n}$.
- (3) $(a^m)^n = a^{mn}$.
- (4) Ha a és b *felcserélhetők* ($ab = ba$), akkor $(ab)^n = a^n b^n$.

Bizonyítás

Positív kitevőkre egyszerű leszámolás. A többi esetben esetszétválasztás (HF).

Csoportelem rendje (lásd 25. Algebra és számelmélet dia)

4.3.9. Definíció, 4.3.10. Gyakorlat

Egy g csoportelem *rendje* a különböző hatványainak száma. Jele: $o(g)$. Az n *jó kitevője* g -nek, ha $g^n = 1$.

- (1) A g -nek vagy bármely két egész kitevőjű hatványa különböző (ilyenkor a rendje végtelen), vagy pedig a hatványok a rend szerint periodikusan ismétlődnek.
- (2) A rend a legkisebb pozitív jó kitevő (véges rendű elemre).
- (3) Tetszőleges k és ℓ egészekre, $o(g) \neq \infty$ esetén $g^k = g^\ell \iff o(g) \mid k - \ell$, speciálisan $g^k = 1 \iff o(g) \mid k$. A jó kitevők tehát pontosan a rend többszörösei.
- (4) A hatvány rendjének képlete: $o(g^k) = \frac{o(g)}{(o(g), k)}$.
- (5) A $g = 1$ az egyetlen olyan elem, melynek a rendje 1. □

Példák elemrendre

- (1) $G = \mathbb{Z}_5^\times$. Ekkor $o(2) = 4$, mert $2^1 = 2 \neq 1$, $2^2 = 4 \neq 1$, $2^3 = 4 \cdot 2 = 3 \neq 1$, de $2^4 = 3 \cdot 2 = 1$.

- (2) $G = \mathbb{Z}_8^\times$. Az 1-től különböző elemek rendje 2, mert négyzetük 1.
- (3) $G = \mathbb{Z}_6^+$. Ekkor $o(4) = 3$, mert $2 \cdot 4 = 8 \neq 0$, de $3 \cdot 4 = 0$.
Általában \mathbb{Z}_n^+ -ban $o(k) = n/(n, k)$ (alkalmazzuk a hatvány rendjének képletét a $g = 1$ elemre).
- (4) Tükrözés rendje 2, eltolás rendje ∞ (kivéve az identitást).
 $k360^\circ$ -os forgatás rendje akkor véges, ha k racionális. Ha $k = p/q$ egyszerűsíthetetlen tört, akkor a rend q .
- (5) Permutáció rendje a diszjunkt ciklushosszak legkisebb közös többszöröse (lásd 25. Algebra és számelmélet dia).

HF (4.3.16): Ha $\psi : G \rightarrow H$ izomorfizmus, akkor *megőrzi az elemrendet*, azaz minden $g \in G$ -re g és $\psi(g)$ rendje ugyanaz. Ezért \mathbb{Z}_5^\times nem izomorf \mathbb{Z}_8^\times -cal, mert \mathbb{Z}_5^\times -ben csak egy másodrendű elem van, \mathbb{Z}_8^\times -ben pedig három.

Ciklikus csoportok

4.3.17. Definíció

A G csoport *ciklikus*, ha egy eleme hatványaiból áll.
Az ilyen elem neve G egy *generátora*.

\mathbb{Z}_5^\times *ciklikus*, generátorai 2 és 3, vagyis a negyedrendű elemek.
 \mathbb{Z}_8^\times *nem ciklikus*, mert minden eleme legfeljebb másodrendű.
 \mathbb{Z}^+ *ciklikus*, az 1 és a -1 generálja (egész többszörösök!).
 \mathbb{Z}_n^+ *ciklikus*, például az 1 generálja.

4.3.20. Tétel

G ciklikus $\iff G \cong \mathbb{Z}^+$ vagy $G \cong \mathbb{Z}_n^+$.

Valóban: ha G ciklikus és g generálja, akkor legyen $n = o(g)$.

Ha $n < \infty$, akkor $\psi : \mathbb{Z}_n^+ \rightarrow G$, $\psi(k) = g^k$ izomorfizmus.

Ha $n = \infty$, akkor $\psi : \mathbb{Z}^+ \rightarrow G$, $\psi(k) = g^k$ izomorfizmus. □

Elemrend és generátorok ciklikus csoportban

4.3.24. Állítás

Egy n elemű ciklikus csoportban $\varphi(n)$ generátorelem van. Minden csoportelem rendje osztója n -nek. Minden $d \mid n$ -re $\varphi(d)$ darab d rendű elem van.

Bizonyítás

Ha g egy generátor, akkor $o(g) = n$, így $o(g^k) = n/(n, k) \mid n$ a hatvány rendjének képlete miatt. De g^d akkor generátor, ha rendje n , azaz ha $(n, k) = 1$. Az ilyenek száma $\varphi(n)$. A harmadik állítás következik egy későbbi tételből.

4.3.22. Tétel (nehéz, vö. primitív gyök számelméletből)

Véges test multiplikatív csoportja ciklikus. Így $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}^+$.

Négyelemű csoportok

A *Klein-csoport*: minden elem négyzete az egységelem; Bármely két egységtől különböző elem szorzata a harmadik.

Klein:	<table border="1" style="border-collapse: collapse; text-align: center;"><tr><td></td><td>1</td><td>a</td><td>b</td><td>c</td></tr><tr><td>1</td><td>1</td><td>a</td><td>b</td><td>c</td></tr><tr><td>a</td><td>a</td><td>1</td><td>c</td><td>b</td></tr><tr><td>b</td><td>b</td><td>c</td><td>1</td><td>a</td></tr><tr><td>c</td><td>c</td><td>b</td><td>a</td><td>1</td></tr></table>		1	a	b	c	1	1	a	b	c	a	a	1	c	b	b	b	c	1	a	c	c	b	a	1
	1	a	b	c																						
1	1	a	b	c																						
a	a	1	c	b																						
b	b	c	1	a																						
c	c	b	a	1																						

ciklikus:	<table border="1" style="border-collapse: collapse; text-align: center;"><tr><td></td><td>1</td><td>g</td><td>g^2</td><td>g^3</td></tr><tr><td>1</td><td>1</td><td>g</td><td>g^2</td><td>g^3</td></tr><tr><td>g</td><td>g</td><td>g^2</td><td>g^3</td><td>1</td></tr><tr><td>g^2</td><td>g^2</td><td>g^3</td><td>1</td><td>g</td></tr><tr><td>g^3</td><td>g^3</td><td>1</td><td>g</td><td>g^2</td></tr></table>		1	g	g^2	g^3	1	1	g	g^2	g^3	g	g	g^2	g^3	1	g^2	g^2	g^3	1	g	g^3	g^3	1	g	g^2
	1	g	g^2	g^3																						
1	1	g	g^2	g^3																						
g	g	g^2	g^3	1																						
g^2	g^2	g^3	1	g																						
g^3	g^3	1	g	g^2																						

Példák Klein-csoportra:

A téglalap/rombusz szimmetriacsoportja, \mathbb{Z}_8^\times , \mathbb{Z}_{12}^\times , $\mathbb{Z}_2^+ \times \mathbb{Z}_2^+$,
 $\{1, f^2, t, tf^2\} \subseteq D_4$, $\{id, (12)(34), (13)(24), (14)(23)\} \subseteq A_4$.

Példák négyelemű ciklikus csoportra:

\mathbb{Z}_4^+ , \mathbb{Z}_5^\times , $\{1, f, f^2, f^3\} \subseteq D_4$, $\{id, (1234), (13)(24), (1432)\} \subseteq S_4$.

9. Összefoglaló

A 10. előadáshoz tartozó vizsgaanyag

Fogalmak

Csoport, gyűrű additív és multiplikatív csoportja, \mathbb{Z}_n^+ és \mathbb{Z}_n^\times ,
a $GL(n, T)$ általános lineáris csoport, az S_n szimmetrikus csoport,
a D_n diédercsoport, a Q kvaterniócsoport. Egybevágósági transzformációk csoportjai. Cayley-táblázat. Klein-csoport Elemrend. Izomorfizmus. Ciklikus csoport.

Tételek

A hatványozás és az elemrend tulajdonságai, hatvány és permutáció rendje.
Kettő és négyelemű csoportok. Számolási szabályok a diédercsoportban.
A ciklikus csoportok osztályozása, az elemek rendjei.