1. Generált részcsoport

Generált altér és ciklikus részcsoport

Emlékeztető
Ha V vektortér, akkor a $v_1, \ldots, v_n \in V$ elemek által *generált altér* elemei a $\lambda_1 v_1 + \ldots + \lambda_n v_n$ alakú vektorok. Jele $\langle v_1, \ldots, v_n \rangle$.
Ez a *legszűkebb* altér, ami $v_1, \ldots, v_n$-et tartalmazza. Azaz minden W altérre, ha $v_1, \ldots, v_n \in W$ akkor $\langle v_1, \ldots, v_n \rangle \subseteq W$.

Emlékeztető
Ha G csoport, akkor a $g \in G$ elem által *generált részcsoport* elemei a g^n alakú elemek (ahol n egész). Jele $\langle g \rangle$.
Ez a *legszűkebb* részcsoport, ami a g-t tartalmazza. Azaz minden H részcsoportra, ha $g \in H$, akkor $\langle g \rangle \subseteq H$.

Mi legyen $\langle g_1, \ldots, g_n \rangle$?

Generálás $\mathbb{Z}^+$-ban

Tegyük föl, hogy $\mathbb{Z}^+$ egy H részcsoportja tartalmazza a 18 és 26 számokat. Milyen számokat kell még tartalmaznia?

Mivel H zárt a kivonásra, $\mathit{8} = 26 - 18 \in H$.
Mivel H zárt az összeadásra, $\mathit{16} = 8 + 8 \in H$.
Mivel H zárt a kivonásra, $\mathit{2} = 18 - 16 \in H$.
Mivel H zárt az összeadásra és a kivonásra, minden *páros szám* H-ban van (a pozitívak és a negatívak is). Ezek részcsoportot alkotnak, több számot nem kell bevenni.

Vagyis a 18 és 26 számokat tartalmazó *legszűkebb* részcsoport a páros számok részcsoportja. Kézenfekvő: $\langle 18, 26 \rangle =$ *páros számok*.

<u>HF:</u> Az m és n-et tartalmazó legszűkebb részcsoport az m és n legnagyobb közös osztójának többszöröseiből áll.

Generálás a nemkommutatív esetben

Tegyük föl, hogy S_4 egy H részcsoportja tartalmazza az (123) és (12)(34) permutációkat. Mit kell még tartalmaznia?

Mivel H zárt a szorzásra, *(134)* $= (123)(12)(34) \in H$.
Hasonlóan *(243)* $= (12)(34)(123) \in H$, továbbá
(132) $= (123)^2 \in H$, *(143)* $= (134)^2 \in H$, *(234)* $= (243)^2 \in H$.
Ez eddig összesen 8 elem az *id* permutációval együtt. *Addig kellene folytatni, amíg részcsoportot nem kapunk.*
<u>Gyorsítás:</u> (123) és (12)(34) páros permutáció, ezért minden szorzásnál, inverzképzésnél páros permutációt kapunk. Lagrange tétele miatt A_4-nek legalább 8 elemű részcsoportja csak maga A_4 lehet. Ezért csak A_4-nél állhatunk le.

Vagyis az (123) és (12)(34) permutációkat tartalmazó *legszűkebb* részcsoport az A_4 alternáló csoport. Kézenfekvő: $\langle (123), (12)(34) \rangle = A_4$.

Generált részcsoport

4.6.3. Definíció
Tetszőleges G csoport esetén az $X \subseteq G$ által *generált részcsoport* a *legszűkebb* X-et tartalmazó részcsoportja G-nek, jele $\langle X \rangle$.

Ez azt jelenti, hogy G minden olyan H részcsoportja, amely tartalmazza X elemeit, tartalmazza az $\langle X \rangle$ részcsoportot is. Az X részhalmazt G *generátorrendszerének* nevezzük (illetve azt mondjuk, hogy X *generálja* G-t), ha $\langle X \rangle = G$.

4.6.7. Állítás
A generált részcsoport egyértelműen létezik. Úgy kapható, mint az X-et tartalmazó részcsoportok metszete.

Megjegyzés: az üres halmaz által generált részcsoport az egységelemből áll.

A generált részcsoport létezése
Az X által generált részcsoport olyan $H \supseteq X$ részcsoportja G-nek, melyre tetszőleges $K \leq G$ esetén $X \subseteq K \iff H \subseteq K$.

4.6.7. Állítás
Ha X részhalmaza a G csoportnak, akkor az X által generált részcsoport egyértelmű, és létezik is, mint a G azon részcsoportjainak metszete, melyek X-et tartalmazzák.

Bizonyítás
Létezés: Legyen H az X-et tartalmazó részcsoportok metszete. Ez X-et tartalmazó részcsoport (mert részcsoportok metszete). Ha $X \subseteq K \leq G$, akkor K tényezője a H-t adó metszetnek, így $H \subseteq K$.
Egyértelműség: Ha H_1 és H_2 is ilyen, akkor $X \subseteq H_1$ és $X \subseteq H_2$. A feltételt $K = H_2$-re alkalmazva $X \subseteq H_2 \implies H_1 \subseteq H_2$. Szerepcserével $H_2 \subseteq H_1$. $\square$

A generált részcsoport elemei
Tudunk-e képletet adni a generált részcsoport elemeire?

4.6.1. Állítás (bizonyítás, mint vektorterekre)
Legyen A kommutatív csoport, melyben a művelet jele a $+$ és $g_1, \ldots, g_n \in A$. Tekintsük az $m_1 g_1 + \ldots + m_n g_n$ elemek („lineáris kombinációk”) L halmazát, ahol m_i egész számok. Ekkor $L = \langle g_1, \ldots, g_n \rangle$.

4.6.8. Tétel (NB)
Legyen G csoport és $X \subseteq G$. Ekkor $\langle X \rangle$ a G azon elemeiből áll, melyek fölírhatók az X elemeiből és azok inverzeiből képzett akárhány tényezős szorzatként (X minden eleme többször is felhasználható egy ilyen szorzatban).

(Ide kapcsolódik a szabad csoportokól szóló 4.10.2. Tétel.)

2. Homomorfizmus

Izomorfizmus és homomorfizmus

4.3.1. Definíció (ismétlés)
Legyen G csoport a $*$ műveletre, és H csoport a $\bullet$ műveletre. A $\psi : G \to H$ leképezés *csoporthomomorfizmus*, ha *művelettartó*: $\psi(a*b) = \psi(a)\bullet\psi(b)$ minden $a, b \in G$-re. Ha ψ kölcsönösen egyértelmű, akkor ψ *izomorfizmus*.

4.7.7. Homomorfizmusok, amik nem izomorfizmusok

(1) $G = \mathbb{Z}^+$, $H = \mathbb{Z}_n^+$, $\varphi(k) = k$ *maradéka mod* n.

(2) $G = \mathrm{GL}(n, T)$, $H = T^\times$, $\varphi(A) = \det(A)$.

(3) $G = S_n$, $H = \mathbb{Z}^\times$, $\varphi(f)$ az f *előjele* (azaz ± 1).

(4) $G = D_n$, $H = \mathbb{Z}_2^+$, $\varphi(x) = 0$ ha x forgatás, 1 ha t. tükrözés.

(5) $G = H = \mathbb{C}^\times$, $\varphi(z) = |z|$ (*abszolút érték*).

(6) $G = \mathbb{R}[x]^+$, $H = \mathbb{C}^+$, $\varphi(f) = f(i)$ (φ az i *behelyettesítése*).

Az izomorfizmus és a homomorfizmus haszna

Az izomorfizmus azért hasznos, mert az *egyformán viselkedő* struktúrák közül *csak egyet* kell megértenünk.

Egy olyan homomorfizmus, amely nem izomorfizmus, sokszor egy *bonyolult* struktúrát képez egy *egyszerűbbe*. Az egyszerűbb struktúrában már tudunk dolgozni, és ezzel információt nyerünk a bonyolultabbról is. Ezt tesszük az életben is, folyamatok modellezésekor. A „modellezés” a „lényeget megőrző” leképezés.

4.7.1 Kérdés
Előáll-e az (12) transzpozíció hármasciklusok szorzataként?

Az összes szorzatot nem tudjuk áttekinteni. Az *előjelképzés* (homomorfizmus!) segít, mert ± 1-gyel könnyű számolni.

Elemi tulajdonságok

2.2.44. Feladat
Legyen $\varphi : G \to H$ csoporthomomorfizmus. Ekkor φ az *egységelemet az egységelembe* viszi, és *inverz képe a kép inverze* lesz (azaz φ az inverzképzés műveletét is tartja).

Bizonyítás
$\varphi(1_G) = \varphi(1_G * 1_G) = \varphi(1_G) \bullet \varphi(1_G)$. Innen $\varphi(1_G)$-vel egyszerűsítve (vagyis az inverzével szorozva) $1_H = \varphi(1_G)$. Az inverzre vonatkozó állítás bizonyítása <u>HF</u>.

4.3.15, 4.3.16. Gyakorlat
Legyen $\varphi : G \to H$ csoporthomomorfizmus és $g \in G$. Ekkor $\varphi(g)$ rendje *osztója* g rendjének. Oka: φ tartja az egész kitevőjű hatványozást: $\varphi(g^k) = \varphi(g)^k$.

Homomorfizmus képe

4.7.2. Definíció
Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Im}(\varphi) = \{\varphi(a) \mid a \in G\} \subseteq H$$

a φ *képe* (vagyis a φ függvény értékkészlete). Nyilván $\mathrm{Im}(\varphi)$ *részcsoport* H-ban (4.5.23. Gyakorlat), és φ akkor és csak akkor szürjektív, ha $\mathrm{Im}(\varphi) = H$.

Példák

(1) $G = H = \mathbb{C}^\times$, $\varphi(z) = |z|$ (abszolút érték).
Ekkor $\mathrm{Im}(\varphi)$ a *pozitív valós számok* részcsoportja.

(2) $G = \mathbb{R}^+$, $H = \mathbb{C}^+$, $\varphi(r) = ri$.
Ekkor $\mathrm{Im}(\varphi)$ a *tisztán képzetes számok* részcsoportja.

(3) G csoport, $G \leq H$, $\varphi(g) = g$. Ekkor $\mathrm{Im}(\varphi) = G$, és így *minden részcsoport egy alkalmas homomorfizmus képe.*

Homomorfizmus magja

4.7.4. Definíció
Ha $\varphi : G \to H$ egy csoporthomomorfizmus, akkor legyen

$$\mathrm{Ker}(\varphi) = \{a \in G \,:\, \varphi(a) = 1_H\} \subseteq G$$

a φ *magja* (itt 1_H a H csoport egységeleme). Nyilván $\mathrm{Ker}(\varphi)$ *részcsoport* G-ben, és φ akkor és csak akkor injektív, ha $\mathrm{Ker}(\varphi) = \{1_G\}$.

Példák

(1) $G = S_n$, $H = \mathbb{Z}^\times$, $\varphi(f)$ az f előjele (azaz ± 1).
$\mathrm{Ker}(\varphi)$ az A_n *alternáló csoport.*

(2) $G = \mathrm{GL}(n, T)$, $H = T^\times$, $\varphi(A) = \det(A)$.
$\mathrm{Ker}(\varphi)$ a *speciális lineáris csoport,* jele $\mathrm{SL}(n, T)$.

(3) $G = \mathbb{R}[x]^+$, $H = \mathbb{C}^+$, $\varphi(f) = f(i)$ (φ az i behelyettesítése).
$\mathrm{Ker}(\varphi)$ az $x^2 + 1$ *többszöröseiből áll* (HF).

3. Normálosztó és faktorcsoport

Nem minden részcsoport homorfizmusmag

4.7.11. Tétel
A G csoport N részcsoportja akkor és csak akkor *magja egy alkalmas, G-n értelmezett homomorfizmusnak*, ha a szerinte vett *bal és jobb oldali mellékosztályok megegyeznek*, vagy ami ezzel ekvivalens, minden $g \in G$ elemre $gN = Ng$.
Az ilyen részcsoport neve *normálosztó*, jele $N \triangleleft G$.

Legyen $\varphi : G \mapsto H$ és $\varphi(g) = h$. Ekkor $gN = Ng$, mert

$\varphi(g') = h \iff \varphi(g') = \varphi(g) \iff \varphi(g^{-1}g') = 1_H \iff$
$\iff g^{-1}g' \in \mathrm{Ker}(\varphi) = N \iff g' \in gN.$

$\varphi(g') = h \iff \varphi(g') = \varphi(g) \iff \varphi(g'g^{-1}) = 1_H \iff$
$\iff g'g^{-1} \in \mathrm{Ker}(\varphi) = N \iff g' \in Ng.$

Az S_3 csoportban $H = \{id, (12)\}$ nem normálosztó,
mert $(123)H = \{(123), (13))\} \neq H(123) = \{(123), (23)\}$.

Faktorcsoport

4.7.12. Állítás
Legyen G csoport, és N részcsoportja G-nek, melyre $gN = Ng$ minden $g \in G$-re. Álljon a K halmaz az N szerinti mellékosztályokból, és vezessünk be rajta szorzást a

$$(g_1N) \cdot (g_2N) = g_1g_2N$$

képlettel. Ekkor K csoport, egységeleme az $N = 1 \cdot N$ mellékosztály, a gN inverze $g^{-1}N$. Az a $\psi : G \to K$ leképezés, ami g-hez gN-et rendeli, homomorfizmus, melynek képe K, magja N.

A fenti konstruckió részletes motivációja a jegyzetben!

4.7.15. Definíció
A K a G csoport N szerinti *faktorcsoportja*, jele G/N.
A ψ neve *természetes homomorfizmus*.

A jóldefiniáltság problémája

Értelmes-e a $(g_1N) \cdot (g_2N) = g_1g_2N$ definíció?

Mit jelent a „narancsszín"? Egy narancsnak a színe. Mindegy melyiké: ha másik narancsot veszünk, ugyanaz a szín.

Mit jelent az „autószín"? Semmit, *rosszul definiált* fogalom. Hiszen az egyik autó zöld, a másik ezüstszínű, a harmadik kék.

Mi legyen az M_1 és M_2 mellékosztályok szorzata?

Vegyünk egy $g_1 \in M_1$-et, akkor $M_1 = g_1N$.
Vegyünk egy $g_2 \in M_2$-t, akkor $M_2 = g_2N$.
Definiáljuk: $M_1 \cdot M_2 = g_1g_2N$.
Ha máshogy választunk: $M_1 = g_1'N$ és $M_2 = g_2'N$, akkor *AZT KELL ELLENŐRIZNI*, hogy $g_1g_2N = g_1'g_2'N$. Vagyis ha máshogy *reprezentáljuk*, ugyanaz lesz a szorzat.

A jóldefiniáltság bizonyítása

Kell: $M_1 = g_1N = g_1'N$ és $M_2 = g_2N = g_2'N \implies g_1g_2N = g_1'g_2'N$.

Tudjuk, hogy $gN = Ng$ minden $g \in G$-re. Ezért

$$g_1g_2N = g_1g_2'N = g_1Ng_2' = g_1'Ng_2' = g_1'g_2'N.$$

Tehát a szorzás a K halmazon tényleg jóldefiniált.

A G/N *egységeleme* $N = 1 \cdot N$.

Valóban, $(1N)(gN) = (1 \cdot g)N = gN$ és hasonlóan $(gN)N = gN$.

Házi feladat (megoldás a jegyzetben)
A szorzás K-ban *asszociatív*.
Minden elemnek van kétoldali *inverze*.
A $\psi(g) = gN$ természetes homomorfizmus tényleg *homomorfizmus*, melynek *magja* tényleg N.

A homomorfizmustétel

4.7.16 Homomorfizmustétel
Ha G és H csoportok, és $\varphi : G \to H$ homomorfizmus, akkor $\mathrm{Im}(\varphi) \cong G/\mathrm{Ker}(\varphi)$.

Bizonyítás
Legyen $N = \mathrm{Ker}(\varphi)$. Ekkor a $gN \leftrightarrow \varphi(g)$ megfeleltetés jóldefiniált, műveletartó és kölcsönösen egyértelmű. $\square$

Speciálisan $|\mathrm{Im}(\varphi)| = |G|/|\mathrm{Ker}(\varphi)|$.
Ez analóg a lineáris algebra *dimenziótételével:* $\dim \mathrm{Im}(A) = \dim V - \dim \mathrm{Ker}(A)$.
Hiszen ha a T alaptest véges, akkor $|V| = |T|^{\dim V}$,
és ezért $|\mathrm{Im}(A)| = |V|/|\mathrm{Ker}(A)|$.
Létezik az analóg *faktortér* (és a faktorgyűrű) fogalma is.
Alkalmazás: a komplex számok precíz bevezetése (később).

A faktor kiszámítása homomorfizmustétellel

4.7.17. Gyakorlat
Melyik ismert csoporttal izomorf $\mathbb{R}^+ / \mathbb{Z}^+$?

Megoldás
Legyen K a komplex egységkör (az 1 abszolút értékű számok). Ez csoport a szorzásra. Belátjuk, hogy $\mathbb{R}^+ / \mathbb{Z}^+ \cong K$.
Legyen $\varphi : \mathbb{R}^+ \to \mathbb{C}^\times$, melyre $\varphi(r) = \cos(2\pi r) + i\sin(2\pi r)$.
Ez homomorfizmus, hiszen komplex számok szorzásakor a szögek összeadódnak.
Nyilván $\mathrm{Im}(\varphi) = K$.
Viszont $\mathrm{Ker}(\varphi) = \mathbb{Z}$, mert $\cos(2\pi r) + i\sin(2\pi r) = 1$ akkor és csak akkor, ha r egész szám.
Ezért a homomorfizmustétel miatt $K = \mathrm{Im}(\varphi) \cong \mathbb{R}^+ / \mathrm{Ker}(\varphi) = \mathbb{R}^+ / \mathbb{Z}^+$. $\square$

Ennél a módszernél előre meg kell tippelni, mi a faktorcsoport.

Cayley tétele

4.12.3. Gyakorlat
Ha a G csoport hat az X halmazon, akkor legyen $\Psi : G \to S_X$ az a leképezés, amely a $g \in G$ elemhez a g hatását, mint permutációt rendeli,
azaz $\Psi(g)(x) = g * x$. Ekkor ψ csoporthomomorfizmus.

Biz.: $\Psi(gh)(x) = (gh) * x = g * (h * x) = [\Psi(g) \circ \Psi(h)](x)$. $\square$

4.6.24. Tétel (Cayley)
Minden csoport izomorf egy permutációcsoporttal.

Bizonyítás: A $g \in G$ elemnek megfelelő permutációt a Cayley-táblázat g-hez tartozó sora adja meg.
Formálisan: Legyen $X = G$ és $g * x = gx$ (vagyis G önmagán hat balszorzással). Legyen Ψ az ehhez tartozó homomorfizmus a fentiek szerint. $\mathrm{Ker}(\Psi) = \{1\}$, mert ha $g * h = h$ minden h-ra, akkor $g = 1$. A homomorfizmus-tétel miatt $G \cong \mathrm{Im}(\Psi) \leq S_G$. $\square$

4. Számolás a faktorcsoportban

Példa faktorcsoportra

4.8.38. Példa
Írjuk föl a $D_4/\{1, f^2\}$ faktorcsoport szorzástábláját.

$$N = \{1, f^2\}, \;\; F = fN = \{f, f^3\}, \;\; T = tN = \{t, tf^2\}, \;\; S = tfN = \{tf, tf^3\}.$$

	N	F	T	S
N	N	F	T	S
F	F	N	S	T
T	T	S	N	F
S	S	T	F	N

<u>Példaszorzat:</u> $ST = ?$
$S = tfN, \quad T = tN \implies ST = tftN = ?$
Mivel $ft = tf^{-1} = tf^3$, ezért $tft = ttf^3 = f^3 \in F$. Azaz $ST = F$.
<u>Elemrend:</u> F *rendje* 2, mert $F^2 = f^2N = N$, de $F \neq N$.
Viszont f *rendje* D_4*-ben* 4.

Elemrend a faktorcsoportban

4.7.20. Állítás
Legyen $N \lhd G$ és $g \in G$. Ekkor a $gN \in G/N$ elem rendje a legkisebb olyan pozitív n egész, melyre $g^n \in N$, és végtelen, ha nincs ilyen n. <u>HF:</u> $o(gN) \mid o(g)$.

Bizonyítás
$k \in \mathbb{Z}$ pontosan akkor jó kitevője a gN mellékosztálynak, ha $(gN)^k = N$ (a G/N csoport egységeleme). De $(gN)^k = g^kN$ (a szorzásnál minden tényezőből a g elemet választva reprezentánsként). Tehát k pontosan akkor jó kitevő, ha $g^kN = N$, azaz ha $g^k \in N$. Mivel a rend a legkisebb pozitív jó kitevő, az állítást beláttuk. $\square$

<u>Példa:</u> $\mathbb{Z}_{16}^\times/\{1, 15\}$ ciklikus, mert $3\{1, 15\}$ rendje 4.
$\mathbb{Z}_{16}^\times/\{1, 9\}$ nem ciklikus, minden elemrend 1 vagy 2.

5. Normálosztó keresése

A normálosztó jellemzései

4.7.9. Gyakorlat, 4.8.1. Állítás
Ha $N \le G$, akkor a következők ekvivalensek.

(1) Az N szerinti bal mellékosztályok G-nek ugyanazok a részhalmazai, mint az N szerinti jobb mellékosztályok.

(2) $gN = Ng$ minden $g \in G$-re.

(3) Minden $g \in G$ és $a \in N$ esetén $gag^{-1} \in N$.

Bizonyításvázlat
$\underline{(1) \iff (2)}$ Ha $gN = Ng'$, akkor $g \in gN = Ng'$.
De $g \in Ng$, és így $g \in Ng \cap Ng'$, azaz $gN = Ng' = Ng$.
$\underline{(2) \iff (3)}$ A (3)-beli feltétel azzal ekvivalens, hogy $gNg^{-1} \subseteq N$, azaz $gN \subseteq Ng$ minden $g \in G$-re. Ezt g helyett g^{-1}-re alkalmazva $g^{-1}N \subseteq Ng^{-1}$ adódik, ahonnan g-vel jobbról és balról szorozva $Ng \subseteq gN$.

Kis indexű részcsoportok

A G csoport *triviális normálosztói*: $\{1\}$ és G.

4.7.19. Állítás
Kettő indexű részcsoport mindig normálosztó.

Bizonyítás
Ha $|G : N| = 2$, akkor két bal oldali mellékosztály van N szerint. Az egyik N, a másik tehát N komplementuma, azaz $G - N$. Ugyanez azonban a jobb oldali mellékosztályokra is igaz. Tehát a bal és a jobb mellékosztályok halmaza is $\{N, G - N\}$. $\square$

A diédercsoportban a forgatások 2 indexű normálosztót alkotnak.
Az S_3-ban $\{id, (12)\}$ három indexű, és nem normálosztó.
Páratlan rendű csoportban viszont minden három indexű részcsoport normálosztó (4.12.42. Feladat).

A konjugálás

4.1.19. Definíció
Legyen G csoport és $g \in G$ rögzített elem. A gxg^{-1} szorzatot *az x elem g-vel vett konjugáltjának* nevezzük ($x \in G$). Az a $\varphi_g : G \to G$ leképezés, amely minden x elemhez gxg^{-1}-et rendel, a g elemmel való *konjugálás*.

4.1.18 Gyakorlat
Ha f α szögű forgatás P körül, akkor gfg^{-1} forgatás $g(P)$ körül, mégpedig α szöggel, ha g mozgás, és $-\alpha$ szöggel egyébként. $\square$

A konjugált elemek „egyformák". Azaz f és gfg^{-1} „ugyanaz", ha g-vel „átfestjük" a síkot.
Másképp: mindegy, hogy először alkalmazzuk f-et, és utána festünk g-vel, vagy először festünk g-vel, és utána alkalmazzuk f konjugáltját:
$gf(x) = (gfg^{-1})g(x)$. A bázistranszformáció és az izomorfizmus is átfestés.

Konjugálás és normálosztók

4.3.4. Gyakorlat (HF)
Ha $g \in G$, akkor a g-vel konjugálás (a $\varphi(x) = gxg^{-1}$ leképezés) a G csoportnak önmagára való izomorfizmusa, azaz *automorfizmusa.*

4.8.5. Gyakorlat (HF)
A konjugáltság ekvivalenciareláció. A kapott osztályokat a csoport *konjugáltosztályainak* nevezzük.

Láttuk: egy részcsoport akkor és csak akkor normálosztó, ha *zárt a konjugálásra*, azaz ha konjugáltosztályok egyesítése.

4.8.14. Gyakorlat
Az S_n szimmetrikus csoportban két elem pontosan akkor konjugált, ha a ciklusfelbontásuk „egyforma", azaz ugyanannyi, ugyanolyan hosszú ciklus szerepel bennük. $\square$

A szimmetrikus csoport két elemmel generálható

4.6.11/(3). és 4.2.28. Gyakorlat
Az S_n szimmetrikus csoportot generálja (12) és $(12\dots n)$.

Bizonyítás
Legyen H az (12) és $(12\dots n)$ által generált részcsoport. Láttuk (4.8.14. Gyakorlat), hogy ha $f \in S_n$, akkor
$$f(x_1 \dots x_k)f^{-1} = \big(f(x_1)\dots f(x_k)\big).$$
Ezért $(12\dots n)$-nel (12)-t konjugálva (23) adódik, azaz $(23) \in H$. Ezt ismételten konjugálva kapjuk, hogy $(34), \dots, (n-1, n) \in H$. Így a kérdés az (4.2.27. Gyakorlat), hogy szomszédos elemek cseréjével megkapható-e minden permutáció. Ha $g(n) = k$, akkor $h = (n, n-1)(n-1, n-2)\dots(k+1, k)g$ az n-et n-be viszi. Így n szerinti indukcióval érvelve $h \in H$, ahonnan $g \in H$. $\square$