NYILATKOZAT

Név: Szoboszlai Brigitta

ELTE Természettudományi Kar, szak: Matematika, BSc

NEPTUN azonosító: H7X206

Szakdolgozat címe:
Gráfok izomorfizmus problémája algebrai eszközökkel

A **szakdolgozat** szerzőjeként fegyelmi felelősségem tudatában kijelentem, hogy a dolgozatom önálló szellemi alkotásom, abban a hivatkozások és idézések standard szabályait következetesen alkalmaztam, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Budapest, 2020.12.28

Szoboszlai B.

a hallgató aláírása

EÖTVÖS LÓRÁND TUDOMÁNYEGYETEM
TERMÉSZETTUDOMÁNYI KAR

GRÁFOK IZOMORFIZMUS PROBLÉMÁJA ALGEBRAI ESZKÖZÖKKEL

Szakdolgozat

Szoboszlai Brigitta

Témavezető: **Dr. Somlai Gábor**

Algebra és Számelmélet Tanszék

Budapest, 2020

Köszönetnyílvánítás

Szeretném megköszönni témavezetőmnek, Dr. Somlai Gábornak, hogy elvállalta a konzulensi feladatokat. Köszönöm, hogy mindig rendelkezésemre állt, valamint türelmével és tanácsaival hozzájárult a szakdolgozat elkészüléséhez.

Valamint köszönöm családomnak, szerelmemnek és barátaimnak, hogy mindig mellettem álltak és támogattak az egyetemi éveim alatt.

Tartalomjegyzék

1. Bevezetés **4**

2. Alapfogalmak **5**

2.1. Algebrai alapfogalmak 5

2.2. Cayley-gráfok 9

3. Cayley izomorfizmusok **12**

3.1. CI-gráfok és CI-tulajdonság 12

3.2. Minimális generátorokkal 14

4. Diédercsoportok **21**

4.1. D_{30} automorfizmus csoportjának az orbitjai 21

4.2. D_{30} Cayley gráfjának a vizsgálata 26

5. Függelékek - Programok **30**

1. Bevezetés

A gráfelmélet egyik fontos kérdésköre az izomorfizmus probléma. Babai László, magyar matematikus a múltszázad második felében elindított egy kérdéskört az úgynevezett CI-csoportokkal kapcsolatban, melyben egy csoport Cayley gráfjainka az izomorfiáit vizsgálják. A téma egyszerűbbnek hangzik, mint amilyen valójában. A munkásságának bonyolultságát és elismerését is bizonyítja, hogy az ismert Csillagkapu: Atlantis nevű tv-sorozatban is megemlítik a nevét [1]:

- Ezredes, találtam valamit. Feltételezem, hogy mint mondta, a szerkezet, amit elvittek végigsugárzott valamit a szubtérben.
- Tudja követni?
- Ha Atlantiszról sugározna, igen tudnám, de láthatóan már nincs így.
- Szóval?
- Szóval. Babai László munkáját használom segítségként. Tudja, kombinatorika és ... ne vegye zokon, de olyan bonyolult, nem tudom eléggé lebutítani, hogy értelme legyen.
- Csak rajta!

Sok neves matematikus foglalkozott a témával és ért el kiemelkedő eredményeket. Hatalmas áttörést a témában Babai 2015-ben megjelent cikke hozott [3], melyben kvázipolinomális algoritmust talált a gráfizomorfizmus problémára. Ezt az évtized legnagyobb számítógéptudományi áttöréseként tartják számon. Harald Helfgott ellenőrizte az algoritmust és a bizonyítást, és több hónapnyi munka után egy súlyos hibát talált benne, melyet Babai egy hét alatt javított és mely által le is egyszerűsítette a bizonyítást.

A szakdolgozatomban a Cayley-gráfokkal és adott Cayley-gráfok izomorfizmusaival fogok foglalkozni. Majd a minimális generátorokkal és azok hatásaival foglalkozom az úgynevezett CI-tulajdonságra. Ezen kívül előállítok egy folyamatot több program segítségével, melyek végül megadják egy diédercsoport (pontosabban a D_{30} diédercsoport) automorfizmus csoportjának az orbitjait, illetve le is ellenőrzöm a Burnside-lemma leprogramozásával az eredményem.

2. Alapfogalmak

A téma feldolgozásához ismertetek néhány alapfogalmat. Ebben a részben olyan definíciók és tételek fognak szerepelni, melyek a későbbiekben elengedhetetlenek lesznek.

A fejezet első felében algebrai alapfogalmak kerülnek elő, főleg a csoportelmélet kapcsán. A második részben a Cayley gráfokkal és azok alaptulajdonságaival foglalkozom.

2.1. Algebrai alapfogalmak

Első lépésként ismertetem a csoport fogalmát, majd néhány elengedhetetlen csoportelméleti definíciót és állítást.

2.1. Definició. A csoport egy olyan $(G, \cdot)$ struktúra, ahol a $\cdot : G \times G \to G$ kétváltozós művelet asszociatív, van egységeleme és inverze. Azaz:

(1) $\forall a, b, c \in G : \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(2) $\exists e \in G \forall a \in G : \qquad e \cdot a = a \cdot e = a$

(3) $\forall a \in G \exists a' \in G : \qquad a' \cdot a = a \cdot a' = e$

Az a elem inverzét általában a^{-1}-gyel, az egységelemet 1-gyel szokás jelölni.

Egy egyszerű példa a csoportokra az egészszámok halmaza az összeadásra nézve, melyet $\mathbb{Z}^+$-nak szokás jelölni. A $\mathbb{Z}^+$ egy asszociaítv csoport, mert pédául $2+(3+4) = (2+3)+4$. Létezik egységeleme: a 0, hiszen $0 + a = a$ minden egészre, és zárt az inverzképzésre is, pl.: $2 + (-2) = -2 + 2 = 0$.

2.2. Definició. Abel csoportnak vagy kommutatív csoportnak nevezzük azokat a csoportokat, melyekeben a csoportművelet kommutatív is.

A későbbiekben több tételt és állítást említek, ahol kihasználom, hogy Abel-csoportokról van szó. Ilyenek lesznek például Cai Heng Li tételei is a minimális generátorhalmazokkal képzett Cayley gráfok izomorfizmusával kapcsolatban [5].

2.3. Definició. Egy G csoport S részhalmaza generátorrendszer, ha G minden eleme előáll S elemeinek és azok inverzeinek véges szorzataként.

2.4. Definició. Legyen G véges csoport, és $S \leq G$. Ekkor S minimális generátorrendszer, ha S bármely elemét elhagyva már nem lesz generátorrendszer.

Fontos megjegyzni, hogy van különbség minimális generátorrendszer és minimális elemszámú generátorrendszer között. Az utóbbi az összes minimális generátorrendszer közül a legkevesebb elemszámút jelenti.

2.5. Definició. Azt mondjuk, hogy a $(G, \cdot)$ csoport ciklikus, ha van olyan G-beli elem, melyre $G = \{a^n | n = 0, \pm 1, \pm 2, ...\}$. Ekkor a-t a G (egyik) generátorelemének nevezzük.

2.6. Definició. Legyen G és H adott csoportok. Azt mondjuk, hogy a $\varphi : G \to H$ leképezeés homomorfizmus, ha $a, b \in G$ esetén $\varphi(ab) = \varphi(a)\varphi(b)$. Ha a leképezés bijektív is, akkor izomorfizmusnak nevezzük.

2.7. Definició. Legyen G egy csoport, és $\varphi : G \to G$ egy bijektív leképezés. Ezt a leképezést automorfizmusnak nevezzük, ha bármely $a, b \in G$ esetén $\varphi(ab) = \varphi(a)\varphi(b)$.

Tehát az automorfizmusok olyan izomorfizmusok, melyek a csoportot önmagára képezik le. Így bármely tetszőleges csoportnak az identikus leképezés egy automorfizmusa. Ezt szokás triviális automorfizmusnak is nevezni.

Egy csoport automorfizmusai is csoportot alkotnak. Egy adott G csoport automorfizmusainak a csoportját $Aut(G)$-vel jelöljük, és az egységeleme az identikus leképezés.

2.8. Definició. Azt mondjuk, hogy egy G csoport hat az X halmazon, ha bármely $g \in G$ és $x \in X$-re teljesül, hogy $gx \in X$, és $gh * x = g * (h * x)$ és ha 1 az egységeleme a G-nek, akkor $1 * x = x$ bármely $x \in X$-re.

Ebből levonható, hogy egy csoport hat önmagán is jobbszorzással. Ebből következik, hogy a Cayley-gráfok szimmetrikusak és a gráfok automorfizmus csoportjai tranzitívak,mert él élbe megy. Ez azért van, mert ha $sg = h$, akkor $sgx = h$, ahol $s \in S$. Ezen felül az is látszik, hogy tartalmaznak egy reguláris részcsoportot is. Ez igazából ugyanaz a gondolat, amivel a következő tételt is be lehet látni.

2.9. Tétel (Cayley-tétel)**.** *Minden csoport izomorf egy szimmetrikus csoport egy részcsoportjához. Ha G egy n rendű csoport, akkor G izomorf egy S_n szimmetrikus részcsoporthoz.*

2.10. Megjegyzés. Egy egyszerű példán keresztül bebizonyítom a Cayley-tételt. Tekintsük a négyzet forgásszimmetriáit, mely a D_4 diédercsoport. Ehhez azonban előtte ismertetem a D_n diédercsoportot.

Egy diédercsoport olyan transzformációcsoport, mely egy szabályos sokszöget önmagába leképző egybevágóságai alkotnak. Az egybevágóságok két csoportra oszthatók, a forgatásokra és a tükrözésesforgatásokra. A forgatások mindig a középpontkörüli $\frac{360°}{n}$-os forgatások, a tükrözések pedig a szimmetriatengelyekre vett tükrözések. Így a D_n diédercsoport generátorai a $\langle t, f \rangle$, ahol t az előzőekben leírt tükrözést, f pedig a forgatást jelöli. Ezek alapján D_n elemei a következők:

$$\begin{aligned} D_n = \{&id, f, f^2, f^3, \ldots, f^{n-1}, \\ &t, tf, tf^2, tf^3 \ldots, tf^{n-1}\} \end{aligned}$$

Ekkor a képzési szabályok pedig az alábbiak:

$$t^2 = id \tag{1}$$

$$f^n = id \tag{2}$$

$$tf = f^{-1}t \tag{3}$$

A 4. fejezetben a D_{30}-as diédercsoporttal fogok foglalkozni, és egy általam írt program segítségével megvizsgálom, hogy az automorfizmuscsoportjának milyen orbitjai vannak, illetve, hogy rendelkeznek-e a CI-tulajdonsággal izomorfia erejéig.

Térjünk vissza az eredeti példánkra, a D_4-re. Jelölje f a 90°-os forgatást. Ekkor

az f által generált csoport a D_4 diédercsoport egy részcsoportja, azaz

$$\langle f \rangle = \{id, f, f^2, f^3\} \leq D_4.$$

Ennek a rendje: $|\langle f \rangle| = 4$. Ekkor a Cayley-tétel szerint ez izomorf az S_4 egy részcsoportjával. Ez könnyen igazolható, hiszen az f forgatásnak megfelel az (1234) permutáció. Az ez által generált csoport a következő: $\{id, (1234), (13)(24), (1432)\} \leq S_4$, melyek rendre megfeleltethetők az $\{id, f, f^2, f^3\}$ csoport elemeinek.

A Cayley-tétel következménye, hogy minden tétel, ami permutációcsoportokra igaz, az csoportokra is igaz lesz, mivel minden csoport ábrázolható permutációcsoportként. Ezt később felhasználom a Burnside-lemma alkalmazásánál is.

2.11. Definició. Legyen G egy permutációcsoport az X halmazon. 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.

2.12. Definició. Legyen $G \leq S_X$ transzformációcsoport és $x \in X$. 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.

A szakdolgozat későbbi részében szó lesz a π-csoportokról és a Hall π-részcsoportokról, így ezekről is szót ejtek. A szakdolgozatban felsorolt tételek és bizonyítások között utalok majd a Sylow-tételekre, így azok is említésre kerülnek itt.

2.13. Definició. Legyen P a pozitív prímek halmaza. $\pi \subseteq P$ részhalmazra $\pi' = P \setminus \pi$. Ekkor n-et π-számnak nevezzük, ha n minden prímosztója π-ben van.

2.14. Definició. Egy véges G csoport π-csoport, ha $|G|$ egy π-szám.

2.15. Definició. $H \leqslant G$ egy π-Hall-részcsoport, ha $|H|$ egy π-szám és $|G : H|$ egy π'-szám. Jelölés: $H \in Hall\pi(G)$.

Másképpen, ha $|G| = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $\pi \cap \{p_1, \dots p_r\} = \{p_{i_1}, \dots, p_{i_k}\}$ és $H \in Hall_\pi(G)$, akkor $|H| = p_{i_1}^{\alpha_{i_1}} \dots p_{i_k}^{\alpha_{i_k}}$.

Ha $\pi = \{p\}$, akkor a $Hall_\pi(G) = Hall_p(G), Hall_{\pi'}(G) = Hall_{p'}(G)$ jelöléseket is használjuk. Ebben az esetben $Hall_p(G) = Syl_p(G)$.

2.16. Lemma (Cauchy-tétel)**.** *Minden olyan p prímre, amely osztja a G csoport rendjét, van p rendű elem G-ben.*

2.17. Tétel (Sylow 1. tétele)**.** *Legyen a G véges csoport rendje $n = mp^h$, ahol p prím, $h \geq 1$, p nem osztója m-nek. Ekkor minden $k \leq h$-ra van G-nek p^k rendű részcsoportja, amit normálosztóként tartalmaz egy p^{k+1}- rendű részcsoport.*

2.18. Tétel (Sylow 2. tétele)**.** *Adott p prímre, amely osztója a G csoport rendjének, G összes P-Sylowja konjugált. Sőt, az összes p^k rendű részcsoport konjugált egymással, ahol $1 \leq k \leq h$.*

Ennek következménye, hogy G összes P-Sylowja izomorf és a P-Sylowok száma osztója m-nek.

2.19. Tétel (Sylow 3. tétele)**.** *A p-Sylowok száma p-vel osztva 1-et ad maradékul.*

2.2. Cayley-gráfok

Most pedig következzenek a Cayley gráfok, melyek a szakdolgozatom alapját adják.

A Cayley gráfok Arthur Cayley (1821-1895) brit matematikus nevéhez fűződnek, aki jelentős eredményeket ért el gráfelméletben és csoportelméletben egyaránt [2]. A nevéhez fűződik a Cayley-formula, mely megadja, hogy hány darab különböző n csúcsú fa adható meg: n^{n-2}.

2.20. Definició. Azt mondjuk, hogy G és G' gráfok izomorfak, ha van a csúcsok között szomszédságtartó bijekció.

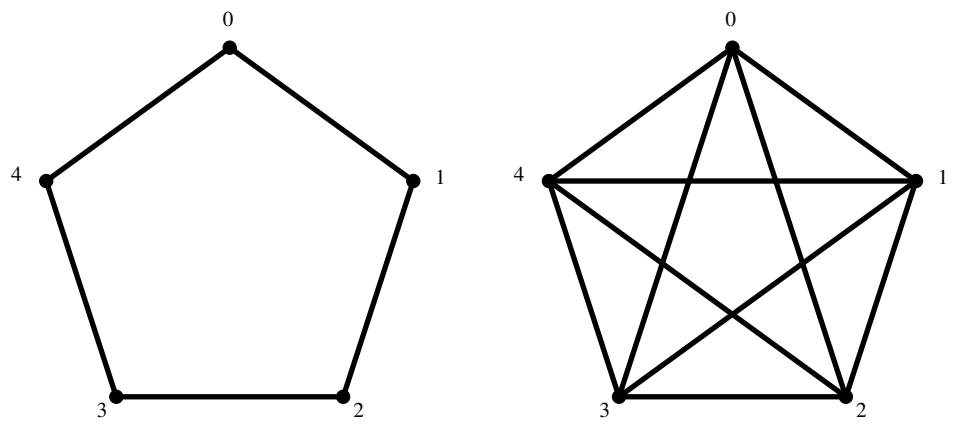
2.21. Definició. Egy gráf csúcsainak olyan p permutációját, melyben bármely két u és v csúcsok pontosan akkor szomszédosak egymással, ha $p(u)$ és $p(v)$ is szomszédosak, azt gráfautomorfizmusnak nevezzük.

Kézenfekvő elemi tulajdonságai a gráfautomorfizmusoknak, hogy gráfautomorfizmusok kompozíciója és inverze is gráfautomorfizmus. Valamint, egy $G(V, E)$ gráf automorfizmusai a V permutációcsoportjának egy részcsoportját alkotják.

2.22. Definició. Legyen G egy csoport, és S a G csoport egy generátorhalmaza. A G csoport S által generált $Cay(G, S)$ Cayley gráfján azt a $\Gamma = (V, E)$ gráfot értjük, amelyre $V = G$ és bármely két $g, h \in G$ csúcsra $(g, h) \in E$ pontosan akkor, ha létezik $s \in S$, melyre $h = gs$.

Ha feltesszük az S generátorhalmazról, hogy szimmetrikus, azaz $|S| < \infty$ és $S = S^{-1}$, akkor ebben az esetben a Cayley gráf irányítatlan. Valamint ha S nem tartalmazza a neutrális elemét, akkor a Cayley gráf egyszerű, vagyis hurokmentes.

Egy egyszerű példa a Cayley-gráfokra ugyanazon csoporton, de különböző generátorhalmazzal: Legyen a $G = (\mathbb{Z}_5, +)$, és az első esetben a generátorhalmaz $S = \{\pm 1\}$, a második esetben pedig $S = \{\pm 1, \pm 2\}$. Ekkor az előbbi esetben a C_5 kört kapjuk, míg az utóbbiban a K_5 teljes gráfot.



Általánosabban elmondható egy csoportról a következő állítás.

2.1. Állítás. *Ha a generátorhalmaz m elemű, akkor minden csúcs fokszáma is m lesz, vagyis általánosan elmondható, hogy ilyenkor m-reguláris gráfot kapunk. Ha a generátorhalmaz csak egy elemből áll, akkor irányított körök unióját kapjuk, ha S tartalmazza az inverzét is, akkor pedig irányítatlan körök unióját.*

2.2. Állítás. *Legyen G egy adott csoport és S egy részcsoportja G-nek. Ekkor $Cay(G, S)$ teljes gráfok uniója.*

Ha S részhalmaz nem generátorrendszer, akkor a $\Gamma(V, E)$ gráf minden összefüggési komponense megfelel az S által generált részcsoport egy mellékosztályának.

2.23. Definició. Legyen $G = (V, E)$ egy adott gráf. Egy $f : V \to V$ bijektív függvény csucsokon bijektiv gráf automorfizmus, ha $(u, v) \in E \Leftrightarrow (f(u), f(v)) \in E$. Azaz a gráfautomorfizmus a gráf egy olyan p permutációja, ahol bármely két $u, v \in V$ csúcs pontosan akkor szomszédos, ha $p(u), p(v)$ is szomszédosak.

2.3. Állítás. *Gráfautomorfizmusok kompozíciója és inverze is gráfautomorfizmus.*

2.24. Definició. Egy $G = (V, E)$ gráfot csúcstranzitívnak vagy tranzitívnak nevezünk, ha minden $u, v \in V$ csúcsra létezik egy $f : V \to V$ gráfautomorfizmus, hogy $f(u) = v$.

2.4. Állítás. *Egy $G = (V, E)$ gráf automorfizmusai a V permutációcsoportjának egy részcsoportját alkotják.*

A Cayley gráf definíciójában hazsnált jobbszorzás miatt $Aut(Cay(G, S))$ tranzitív is.

3. Cayley izomorfizmusok

Gráfizomorfiát ellenőrizni, a mai napig egy lassú folyamat. Ma már sok algoritmus létezik, melyek kis számokra gyorsan megadják a választ, azonban nagyobbakra még mindig elég lassúak. Többek között ezért is hatalmas áttörés a bevezetőben említett eredménye Babainak [3]. Azonban nem csak ilyen irányú eredmények születtek az elmúlt évtizedekben. Sok más matematikus foglalkozott a témával az elmúlt 50 évben. Ebben a fejezetben az ő eredményeik egyrészét próbáltam összegyűjteni.

3.1. CI-gráfok és CI-tulajdonság

Egy $Cay(G, S)$ Cayley gráfot a G véges csoport CI-gráfjának nevezzük, ha bármely $Cay(G, T)$ Cayley gráf esetén ha $Cay(G, S) \cong Cay(G, T)$-hez, akkor $S^\sigma = T$, ahol $\sigma \in Aut(G)$. Azt, hogy egy csoport rendelkezik ilyen részhalmazokkal, CI-tulajdonságnak nevezzük. (A CI a Cayley Isomorphism rövidítése)

Ilyenkor felmerül a kérdés, hogy milyen csoportok rendelkeznek a CI-tulajdonsággal. Ebben a részben ezekről gyűjtök össze nagyrészt felsorolás szinten minél több információt. Jórészt Cai Heng Li és kollégái [6], [11] eredményeiről lesz szó, de Muzychuk [10], [**?**], [7], és Somlai Gábor [9] tételeit is összeszedtem.

C.H. Li a [6] cikkében a következőeket bizonyított be ciklikus csoportokról.

3.1. Állítás. *Legyen G egy ciklikus csoport, melynek rendje p^r, ahol p egy prím, és $r \geq 1$. Ekkor:*

(1) Ha $r \geq 4$ és $p = 2$, vagy $r \geq 3$ és $p = 3$, vagy $r \geq 2$ és $p \geq 5$, akkor G tartalmaz öninverz, nem-CI-részhalmazt, melynek a mérete $2(p + 1)$.

(2) Ha $r \geq 3$ és $p = 2$, vagy $r \geq 2$ és $p \geq 3$, akkor G tartalmaz nem-CI-részcsoportot, melynek a mérete $p + 1$.

Muzychuk is foglalkozott a ciklikus csoportokkal. Ő azt bizonyította be a [7]

cikkében, hogy bizonyos ciklikus csoportok rendelkeznek a CI-tulajdonsággal. A tétele így hangzott.

3.1. Tétel. *Egy n-rendű ciklikus csoport CI-csoport, akkor és csak akkor, ha vagy $n \in \{8, 9, 18\}$, vagy $n = k, 2k$ vagy $4k$, ahol k egy négyzetmentes páratlan egész.*

Ezt a 4. fejezetben fel is használom majd a probléma megoldásához. Muzychuk és társai tovább vitték ezt a gondolatmenetet, és belátták, hogy minden véges ciklikus csoport kielégíti a CI-tulajdonságot a kiegyensúlyozott konfigurációkra [**?**]. Somlai Gábor bebizonyította, hogy $8p$-rendű csoportok közül melyek CI-gráfok [9].

3.2. Állítás. *Minden $p > 3$ prímre a $Q \times \mathbb{Z}_p$ és $\mathbb{Z}_2^3 \times \mathbb{Z}_p$ DCI-csoportok, ahol Q a 8 elemű kvaternió csoportot jelöli. (DCI=Directed Cayley Isomorphism)*

Ugyanezen cikkében bebizonyította a 3.2 állítást $p > 8$-ra, illetve $p = 5$-re és $p = 7$-re is a DCI-tulajdonságot.

3.3. Állítás. *Minden Cayley gráfja a $Q \times \mathbb{Z}_5$-nek, $Q \times \mathbb{Z}_7$-nek, $mathds Z_2^3 \times \mathbb{Z}_5$-nek és $mathds Z_2^3 \times \mathbb{Z}_7$-nek CI-gráf.*

Muzychuk Hirasaka-val együtt dolgozva egy közös cikkükben a következőt látták be [10]:

3.2. Tétel. *Minden összefüggő, 2 fokszámú, egyszerű csoporthoz tartozó Cayley gráf CI-gráf.*

A fokszámokkal és CI-tulajdonsággal C.H. Li is foglalkozott [11]. Ő a p-csoportokat vizsgálta meg ebből a szemszögből.

3.4. Állítás. *Legyen p egy prím, és G egy p-csoport. Ekkor minden összefüggő Cayley-gráf, aminek kevesebb a fokszáma, mint p, és minden összefüggő irányítatlan Cayley-gráfnak legfeljebb $(2p-2)$ fokszámmal CI-gráfok. Sőt, a ciklikus $\mathbb{Z}_p$ csoport összes Cayley-gráfja is CI-gráf.*

Ennek az állításnak a bizonyításához a Sylow-tételeket is felhasználta, hogy tanulmányozhassa a prím rendű CI-gráfokot. Ezt az állítást tovább lehet álltalánosítani, melyet Wielandt meg is tett. Az állítása így hangzott [12]:

3.3. Tétel. *Legyen a G véges csoportnak egy nilpotens Hall π-részcsoportja, melyet jelöljünk H-val. Ekkor G minden π-részcsoportja benne van H egy konjugáltjában. Sőt, minden Hall π-részcsoport konjugált.*

3.4. Definició. A G csoport nilpotens, ha létezik véges centrállánca.

Li a nilpotens csoportokat is vizsgálta [6].

3.5. Állítás. *Legyen G egy véges csoport, és Σ egy Cayxle gráfja G-nek. Legyen $A = Aut(\Sigma)$ és i a G identitása. Tegyük fel, hogy G páratlan rendű vagy nilpotens. Ha $(|G|, |A_i|) = 1$, akkor Σ egy Cayley gráfja G-nek.*

A gondolatot tovább vitte és a következőt is bebizonyította [6].

3.6. Állítás. *Legyen G egy Abel csoport és $\Sigma = Cay(G, S)$, $A = Aut(\Sigma)$. Tegyük fel, hogy $(|G|, |A_i|) = p$, ahol p egy prím. Ekkor Σ vagy G CI-gráfja, vagy S tartalmaz nem-triviális G-részcsoport részhalmazt.*

3.2. Minimális generátorokkal

3.5. Definició. Egy G csoportot DCI- csoportnak nevezünk, ha minden részhalmaza G-nek egy CI-részhalmaz.

Legyen m egy pozitív egész. Egy G csoportot m-DCI- (vagy m-CI-) csoport, ha G minden részhalmaza (vagy inverzre zárt részhalmaza), aminek a nagysága legfeljebb m, CI-részhalmaz. Ez a két állítás hasznos az alacsony fokszámú Cayley gráfok izomorfia vizsgálatához.

A mai tudásunk alapján kevés CI- és DCI-csoportról tudunk. Mégis, a szakirodalomban sokan foglakoztak a témával és sok cikk található a CI- és a DCI-csoportokkal kapcsolatban [6], [11], [13]. Én a minimális generátorok szemszögéből igyekeztem összegyűjteni az eddig elért eredményeket. Azért foglalkoztatott ez a téma, mert a generátorok segítségével lehet a legtöbbet megtudni a csoportok struktúrájáról.

Ezzel a témával foglalkozott Ming Yao Xu [13], Yan-Quan Feng [17] és Cai Heng Li és még sokan mások a cikkeikben . Nagyrészt az előbb említett matematikusok publikációit dolgozom fel ebben a részben.

A most következő tételekhez fontosak az alábbi fogalmak és állítások. Legyen G egy csoport és jelölje $R(G)$ egy jobboldali reguláris permutációcsoportját G-nek, ahol $R(G) = \{\pi_g \in Sym(G) | g \in G\} \leq Sym(G)$.

3.7. Állítás. *Legyen $X = Cay(G, S)$ irányított Cayley gráf. Ekkor*
(1) *$Aut(X)$ tartalmazza $R(G)$-t, így X csúcstranzitív.*
(2) *X összefüggő akkor és csak akkor, ha $G = \langle S \rangle$.*
(3) *X irányítatlan akkor és csak akkor, ha $S^{-1} = S$.*

Ebből az állításból már következik a 3.8 állítás.

3.8. Állítás. *Az irányított $X = (V, E)$ gráf egy csoport irányított Cayley-gráfja akkor és csak akkor, ha $Aut(X)$ tartalmaz egy reguláris részcsoportot.*

Ming-Yao Xu a [13] cikkében az izomorfiákat vizsgálta. Az egyik fő kérdése a következő volt:

Legyen G egy véges csoport, és S egy minimális generátorhalmaza G-nek. Ekkor S és $S \cup S^{-1}$ CI-részhalmazok? Huang és Meng a következőket bizonyították be [14]-[16].

3.9. Állítás. *Legyen G egy véges ciklikus csoport és S a minimális generátora. Legyen $X = Cay(G, S)$ és $\overline{X} = Cay(G, S \cup S^{-1})$. Legyen σ egy automorfizmusa G-nek, ahol $\forall g \in G$-re $g^{\sigma} = g^{-1}$ és $\sum = \langle \sigma \rangle$. Ekkor $Aut(X) = R(G)$ és $Aut(\overline{X}) = R(G) \sum$.*

Ekkor Ming főkérdésére a válasz igen, S és $S \cup S^{-1}$ CI-részhalmazok. Abel-csoportokra C.H. Li adott egy példát [6], mely megcáfolja ezt, azonban, ha a csoport páratlan rendű, akkor mégis igaz. Az állítása a következő volt.

3.10. Állítás. *(1) Legyen $G = \langle a \rangle \times \langle x \rangle \times \langle e \rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_2$ és legyen $S = \{x, xe, ax^2\}$ és $T = \{x, xe, ax^2e\}$. Ekkor S egy minimális generátor részhalmaza G-nek és az irányított $Cay(G, S)$ Cayly-gráf izomorf a $Cay(G, T)$*

Cayley-gráffal. Azonban, nincs olyan automorfizmusa G-nek, mely S-et T-be vinné. Azaz, S nem CI-részhalmaz.

(2) *Egy páratlan rendű Abel-csoport minden minimális generátor részhalmaza CI-részhalmaz.*

Ebben az állításában azonban Li egy hibát vétet. A T generátorhalmaz nem minimális, melyet egyszerű ellenőrizni. Vegyük az ax^2e és az xe inverzének a szorzatát. Ekkor $(ax^2e)(xe)^{-1} \in G$ és

$$(ax^2e)(xe)^{-1} = (ax^2e)(e^{-1}x^{-1}) = ax$$

Mivel az x 4-rendű, azaz $x^4 = id$, az a pedig 3-rendű, így az alábbi összefüggéseket kapjuk:

$$\begin{aligned}(ax)^4 &= a\\ (ax)^3 &= x^{-1}\end{aligned}$$

Ebből már látszik, hogy T nem minimális, hiszen 2 generátorral előállítottuk a harmadikat. Végül pedig $(xe)x^{-1} = e$. Vagyis T valóban generátorhalmaz, de nem minimális.

Fontos tehát észrevenni, hogy az előzőek azt is mutatják, hogy a Cayley gráfok gráfstruktúrájából nem látszódik az, hogy a hozzá tartozó generátorrendsz minimális-e vagy sem.

Y.-Q. Feng vette észre ezt a hibát [17], és javította az állítást.

3.11. Állítás. *Legyen G egy véges Abel-csoport, és S és T két minimális generátorhalmaza G-nek. Legyen $X = Cay(G, S)$ és $Y = Cay(G, T)$ izomorfak. Akkor létezik egy $\alpha \in Aut(G)$, melyre $S^\alpha = T$.*

Bizonyítás. Ha $|S| = 1$, akkor G cikikus és az állítás igaz. Ezért tegyük fel, hogy $|S| > 1$.

Vegyünk egy σ izomorfizmust $Cay(G, S)$ és $Cay(G, T)$ között, ahol σ az egységelemeket egymásba viszi, azaz $1^\sigma = 1$. Ekkor $T = S^\sigma$. Ezután definiáljunk egy

” $\sim$ ” ekvivalencia relációt G-n úgy, hogy

$$g \sim h \Leftrightarrow g^2 = h^2, \forall g, h \in G \tag{4}$$

Ekkor ez a $\sim$ kikötés S-re (vagy T-re) is egy ekvivalenciareláció S-en (vagy T-n). Legyenek $S_1, \dots S_k$ az ekvivalenciaosztályai S-nek a $\sim$ ekvivalenciarelációnak S-en. Ekkor $S = \bigcup_{i=1}^{k} S_i$. Legyen $T_i = S_i^{\sigma}$.

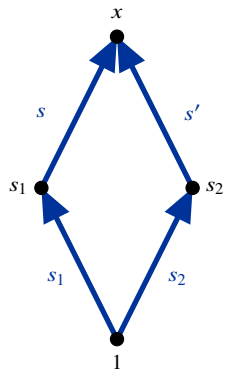
3.12. Állítás. *Ekkor megállapítható, hogy $T_1, \dots T_k$-k is ekvivalenciaosztályai a $\sim$ relációnak.*

Ahhoz, hogy ezt bizonyítsuk, nézzük meg a következő állítást.

3.6. Lemma. *Bármely $s_1, s_2 \in S, s_1 \neq s_2$ esetén, ha az s_1 és s_2 kifelé mutató szomszédjainak a halmaza $X_1(s_1)$ és $X_1(s_2)$ az X gráfban, akkor ezek metszéspontja*

$$X_1(s_1) \cap X_1(s_2) = \begin{cases} \{s_1, s_2\}, & \text{ha } s_1 \nsim s_2, \\ \{s_1, s_2, s_1^2\}, & \text{ha } s_1 \sim s_2. \end{cases} \tag{5}$$

Bizonyítás. Azt tudjuk, hogy $X_1(s_1) \cap X_1(s_2)$ tartalmazza $\{s_1, s_2\}$-t vagy $\{s_1, s_2, s_1^2\}$-et attól függően, hogy $s_1 \nsim s_2$ vagy $s_1 \sim s_2$. Tegyük fel, hogy létezik egy másik csúcs s_1 és s_2 szomszédságában, ami $x = s_1 s = s_2 s'$, ahol $s, s' \in S$. Ekkor legalább az egyik, tegyük fel, hogy s, nincs benne $\{s_1, s_2\}$-ben. Akkor $s_1 s = s_2 s'$, amiből következik, hogy $s = s_1^{-1} s_2 s'$ és G-t generálja az $S \backslash \{s\}$ halmaz. Ez viszont ellentmondás, ugyanis azt tettük fel S-ről, hogy minimális.



A szimmetria miatt bármely $t_1, t_2 \in T, t_1 \neq t_2$ esetén

$$Y_1(t_1) \cup Y_1(t_2) = \begin{cases} \{t_1, t_2\}, & \text{ha } t_1 \nsim t_2, \\ \{t_1, t_2, t_1^2\}, & \text{ha } t_1 \sim t_2. \end{cases} \tag{6}$$

Most már minden adott, hogy belássuk, hogy $T_1, \dots T_k$-k is ekvivalenciaosztályai a $\sim$ relációnak. Adottak $s_1, s_2 \in S$, és legyen $t_i = s_i^\sigma, i = 1, 2$. Ekkor a (2) és (3) alapján $s_1 \sim s_2 \Leftrightarrow |X_1(s_1) \cap X_1(s_2)| = 2 \Leftrightarrow |(X_1(s_1) \cap X_1(s_2))^\sigma| = |Y_1(t_1) \cap Y_1(t_2)| = 2 \Leftrightarrow t_1 \sim t_2$, ami az állításunk volt.

□

Tekintsük a σ szerinti szorzat képét az $s_1 s_2 \dots s_n$-nek, ahol $s_i \in S$ minden $i = 1, 2, \dots, n$-re. Bizonyítsuk be a következő lemmát.

3.7. Lemma. $(s_1 s_2 \dots s_n)^\sigma = y_1 y_2 \dots y_n$, *ahol* $y_i \in T$ *minden* $i = 1, 2, \dots n$*-re* $y_i \sim s_i^\sigma$ *minden i-re.*

Bizonyítás. Amikor $n = 1$ eset áll fenn, akkor triviálisan igaz az állítás. Indukciót használva elég bebizonyítanunk azt, hogy bármely $x \in G$-re és $s_1, s_2 \in S$-re, ha $(s_i x)^\sigma = y_i x^\sigma$ $(i = 1, 2)$, ahol $y_i \sim s_i^\sigma$, akkor $(s_1 s_2 x)^\sigma = z_1 z_2 x^\sigma$, ahol $z_i \sim s_i^\sigma$ $(i = 1, 2)$-re. Ahhoz, hogy ezt bebizonyítsuk két részre bontjuk a problémát: az első esetben $s_i \nsim s_2$, a második esetben pedig $s_i \sim s_2$. Az első esetben a 3.12 állítás alapján kapjuk, hogy $y_1 \nsim y_2$. A 3.6 lemmához hasonlóan, ahogy $s_1 s_2 x$ az egyetlen közös kifelé mutató csúcsszomszédja $s_1 x$-nek és $s_2 x$-nek, ugyanígy a $y_1 y_2 x^\sigma$ az egyetlen kifelé mutató csúcsszomszédja $y_1 x^\sigma$-nak és $y_2 x^\sigma$-nak, így $(s_1 s_2 x)^\sigma = y_1 y_2 x^\sigma$, tehát igaz az állítás. A második esetben, szintén 3.12 állítás miatt $y_1 \sim y_2$. Ebben az esetben $s_1 x$-nek és $s_2 x$-nek (illetve $y_1 x^\sigma$-nak és $y_2 x^\sigma$-nak) két közös kifelé mutató csúcsszomszédja van, $s_1 s_2 x$ és $s_1^2 x$ (illetve $y_1 y_2 x^\sigma$ és $y_1^2 x^\sigma$, így $(s_1 s_2 x)^\sigma = y_1 y_2 x^\sigma$ vagy $y_1^2 x^\sigma$. Tehát a következtetés helyes volt.

□

Most már minden adott, hogy bebizonyítsuk a 3.11 állítást.

Legyen $S_i = \{s_i1, s_i2, \dots, s_{in_i}\}$ $i = 1, 2, \dots, k$. Legyen $s_{ij}^{\sigma} = t_{ij}$ $i = 1, \dots k$, $j = 1, \dots n_i$. Akkor $T_i = S_i^{\sigma} = \{t_{i1}, t_{i2}, \dots, t_{in_i}\}$ és $S = \bigcup_{i=1}^{k} S_i$, $T = \bigcup_{i=1}^{k} T_i$. Tekintsük az $\alpha : G \to G$ függvényt, mely

$$\prod_{i=1}^{k} \prod_{j=1}^{n_i} s_{ij}^{e_{ij}} \to \prod_{i=1}^{k} \prod_{j=1}^{n_i} t_{ij}^{e_{ij}},$$

ahol e_{ij} egy tetszőleges nem-negatív egész. Be kell bizonyítanunk, hogy α egy automorfizmusa G-nek, és így teljesül a 3.11 állítás. Emlékeztetőül, S és T generátor részhalmazai a G-nek, így elegendő azt bizonyítani, hogy α jól definiált. Ehhez szükségünk lesz a következő állításra.

3.13. Állítás. *Ha* $\prod_{i=1}^{k} \prod_{j=1}^{n_i} s_{ij}^{e_{ij}} = 1$, *akkor* $\prod_{i=1}^{k} \prod_{j=1}^{n_i} t_{ij}^{e_{ij}} = 1$.

Bizonyítás. Tegyük fel, hogy

$$\prod_{i=1}^{k} \prod_{j=1}^{n_i} s_{ij}^{e_{ij}} = 1 \tag{7}$$

Először vizsgáljuk meg, hogy ha S_i-nek legalább 2 eleme van valamely i-re, akkor az e_{ij} kitevő páros bármely $j = 1, \dots n_i$-re. (Ha bármely e_{ij} páratlan lenne bármely j-re, akkor $s_{ij}^{e_{ij}} = s_{ij} s_{ij'}^{e_{ij}-1}$ minden $j \neq j'$, hiszen $s_{ij}^2 = s_{ij'}^2$. Kicserélve $s_{ij}^{e_{ij}}$-t $s_{ij} s_{ij'}^{e_{ij}-1}$-re a 7-es képletben, s_{ij}-t kifejezhetjük egy $S \setminus \{s_{ij}\}$-beli szorzattal, ami ellentmond az S minimalitásának. Tehát csak páratlan kitevő lehet.) Mégegyszer, mivel $s_{ij}^2 = s_{ij'}^2$ minden i, j, j'-re, így kapju azt, hogy

$$\prod_{i=1}^{k} \prod_{j=1}^{n_i} s_{ij}^{e_{ij}} = \prod_{i=1}^{k} s_{i1}^{e_i} = 1, \tag{8}$$

ahol $e_i = \sum_{j=1}^{n_i} e_{ij}$. Hasonlóképpen kapjuk, hogy

$$\prod_{i=1}^{k} \prod_{j=1}^{n_i} t_{ij}^{e_{ij}} = \prod_{i=1}^{k} t_{i1}^{e_i} \tag{9}$$

Használjuk σ-t a 7-es képleten, akkor a 3.7 lemma alapján

$$(\prod_{i=1}^{k} \prod_{j=1}^{n_i} s_{ij}^{e_{ij}})^{\sigma} = \prod_{i=1}^{k} \prod_{j=1}^{n_i} t_{ij}^{f_{ij}} = 1, \tag{10}$$

ahol $\sum_{j=1}^{n_i} f_{ij} = e_i$ és f_{ij} páros, ha $|T_i| = |S_i| > 1$. Így azt kapjuk, hogy

$$\prod_{i=1}^{k} t_{ij}^{e_{ij}} = 1, \tag{11}$$

ahogy azt bizonyítani is szerettük volna.

□

Ennek a tételnek a következményeképp minden minimális generátor halmaz CI-részhalmaz. Tehát Ming fő kérdésére a válasz igen. Babai a p-csoportokra vizsgálta ezt a [18] cikkében.

3.14. Állítás. *Legyen G egy véges p-csoport és S pedig G egy generátor halmaza, ahol $|S| < p$. Ekkor S egy CI-részhalmaz.*

Ennek a következménye, hogy egy G p-csoport minden minimális generátor részhalmaza CI-részhalmaz, ha G-nek van legalább $(p-1)$ generátora. Megjegyzésként, a p-csoportoknak minden minimális részhalmazának ugyanannyi generátora van. Ez az úgynevezett Burnside-bázistétel miatt van [**?**].

Li [6] általánosította Babai László eredményét, mely szerint minden prímrendű ciklikus csoport CI-csoport.

3.15. Állítás. *Legyen G egy véges csoport és p a kegkisebb osztója $|G|$-nek. Legyen S a generátor részhalmaza G-nek, ahol $|S| < p$. Ekkor S egy CI-részhalmaz.*

4. Diédercsoportok

4.1. D_{30} automorfizmus csoportjának az orbitjai

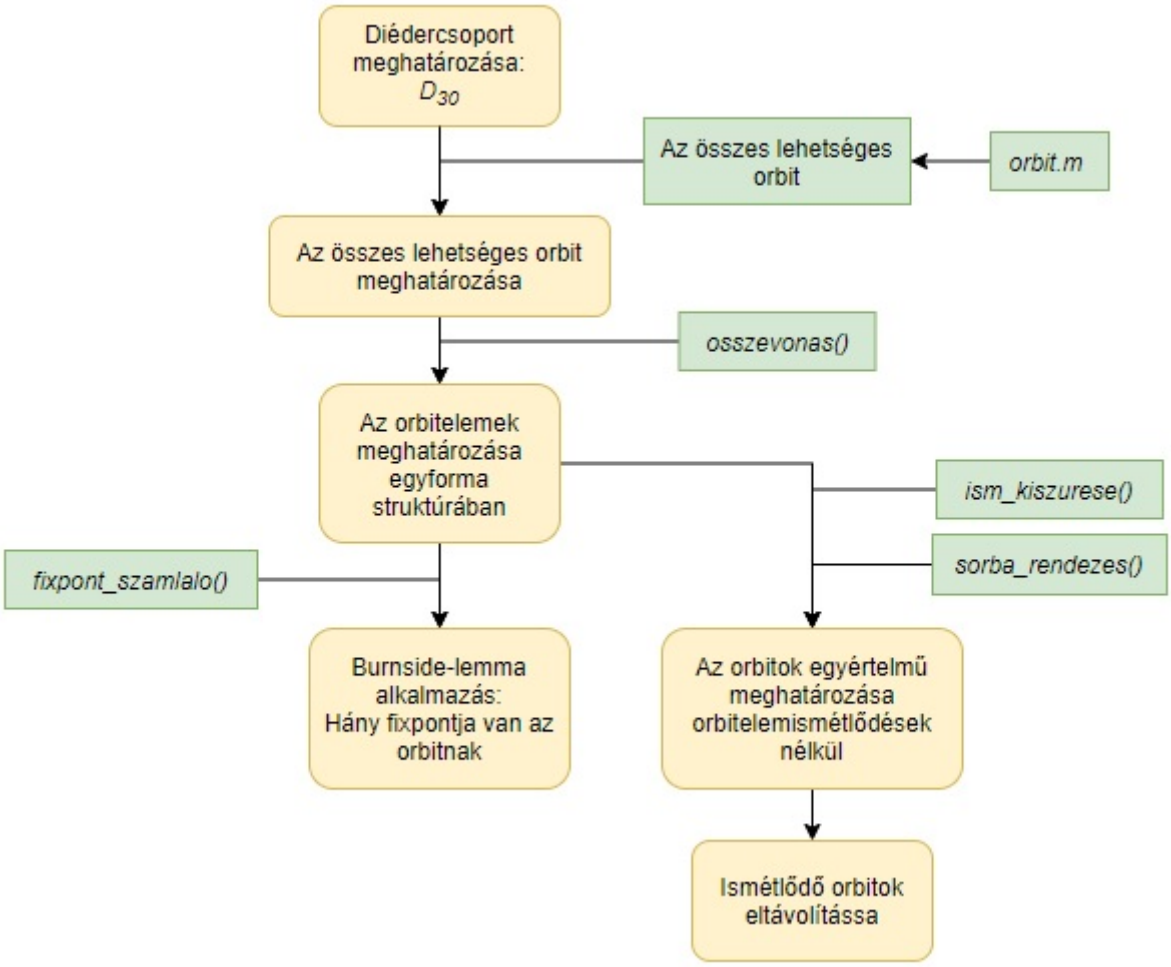
Az a kérdés foglalkoztatott, hogy egy D_n diédercsoport automorfizmus csoportjának az orbitjait meg tudom-e határozni abban az esetben, ha 3 elemű a generátorhalmaz. Irányítatlan gráfokkal szerettem volna foglalkozni, így a generátorrendszernek szimmetrikusnak kellett lennie. Ezzel meg lehet számolni a diéder csoport Cayley gráfjait, amlyek foka 3.

Ha a generátorrendszer 2 elemű, akkor $\langle t, tf^a \rangle$ alakú, ahol az a relatív prím a diédercsoport elemszámának a feléhez. Ilyen esetekben ezek mindig izomorfak lesznek, mert automorfizmussal egymásba vihetőek a generátorok. Ha van forgatás a generátorok között, akkor az inverze is kell, és egy generátorrendszerbe kell forgatás is, így csak $\langle t, tf^a \rangle$ alakúak lehetnek a 2 elemű generátorrendszerek.

Ha 3 elemű a generátorrendszer esetén $\langle tf^i, tf^j, tf^{-j} \rangle$ alakúakat veszem, ahol j relatív prím az n-hez. Ezek az előzőekben leírtak miatt izomorfak.

A második fejezetben bemutattam a diédercsoportokat általánosan. Most kifejezetten a D_{30}-cal foglalkozom. Ennek különösebb oka nincs, egyszerűen ezt már elég nagy csoportnak tekintettük, hogy még ne számolják ki és érdekes legyen foglalkozni vele. Mindazonáltal az általam írt programok minimális átírással bármely diédercsoportra alkalmazhatók.

Az első feladatom az volt, hogy határozzam meg az automorfizmuscsoportjának az orbitjait, ha a generátorrendszer minimális és 3-elemű. Ehhez 2 programfajtát használtam. Először a Matlab-ban írtam programot, mely meghatározza az összes lehetséges orbitot. Ezeket az átláthatóság érdekében kimentettem excelbe és a könnyebben olvashatóság érdekében formáztam egy kicsit. Ezután írtam egy program sorozatot, mely megszámolja a különböző orbitok számát. Ezt végül a Burnside-lemmával ellenőriztem, szintén a programom segítségével. Ezekhez VBA Macro programnyelvet használtam. A 4.1. ábra összefoglalja a folyamatmodellemet.



Folyamatábra a programok használatához

Az első programhoz elször kiszámoltam egy adott generátorral számított automorfizmusnak az orbitját. Ehhez írtam egy $orbit.m$ függvényt, melynek a bementi paraméterei a diédercsoport száma, és a generátorok. (5. kép)

A könnyebb számolás érdekében a programban a számok azt jelölik, hogy egy adott f forgatás a hanyadikon szerepel. Így például, ha arról van szó, hogy az α automorfizmus $t \to tf^x$, $f \to f^y$, akkor az azután kapott $\alpha(b_1, b_2, b_3) = \{tf^a, tf^b, tf^c\}$ generátorokat egy abc számhármással tudtam jelölni.

Ahhoz, hogy minimális legyen az automorfizmus, az α automorfizmusnak a

következő alakúnak kellett lennie:

$$t \to tf^x$$
$$f \to f^y,$$

ahol $(y, 30) = 1$. Ha a generátorrendszer minimális és 3-elemű, akkor az automorfizmuscsoportjának az elemszáma legfeljebb $n\phi(n)$, ahol n a diédercsoport elemszámát jelöli, $\phi(n)$ pedig az Euler függvényt. Az én esetmebn ez $30 * 8 = 240$. Vagyis legfeljebb 240 elemű lehet egy orbit. Arra törekedtem, hogy a programom bármilyen diédercsoportra alkalmazható lehessen a későbbiekben, így a programmal számoltattam ki a $\phi(n)$ értékét, és elmentettem egy vektorba az n -nel relatív prímeket. Ehhez a Matlabban található beépített $gcd()$ függvényt használtam, mely visszaadja a legnagyobb közös osztóját két számnak. Ez a vektor jelölte, hogy az automorfizmus csoportból melyik $f \to f^y$ leképezésről volt szó.

Ezután létrehoztam egy $i()$ vektort, mely pedig a $t \to tf^x$ leképezéseket tárolta, így ez 0-tól 29-ig vett fel értékeket. Egy-egy generátornak a képzési szabálya a következőképp történt: Legyen az $\alpha : t \to tf^i, f \to f^j$, ahol $(j, 30) = 1$, akkor ha a generátorelemünk a tf^k, akkor

$$\alpha(tf^k) = (tf^i)(f^j)^k = tf^{i+jk}.$$

Egy-egy orbitot egy 3 sorú mátrixban tároltam el úgy, hogy a 3 db generátor mind a 240 féle leképezését tartalmazzák. Így egy-egy orbitelem a mátrix oszlopai lesznek. Ezt az egészet elmentettem az $orbit.m$ függvénybe, mely visszaadja a 3 sorú mátrixot. (lsd.: 5 ábrán a függelékben)

Ezután szükségem van az összes $\{tf^a, tf^b, tf^c\}$ generátorra. Ez uyge, 30^3, de az ismétlődéseket ki szerettem volna zárni, így elég volt $28 * 29 * 30$ esetet megvizsgálnom. Egy tripla forciklussal ezeket a generátorkombinációkat is elő tudtam állítani úgy, hogy ezekkel meghívhatam az $orbit.m$ függvényt, aminek az eredményét végül hozzá csatoltam az eredménymátrixomhoz. Végül pedig kimentettem egy excel file-ba a megoldásomat. (lsd.: 5 ábrán)

Az excel file akkor még nem volt jó felépítésű, így egy apró alakításra volt

szükséges. A szóközöket átalakítottam tabulátorokká, így minden mezőbe egy-egy adat került.

Ezután az orbitok elemeit szerettem volna számhármasokká alakítani. Ehhez az excelben található Visual Basic-et használtam, és ott írtam egy kódot, mely egy új munkalapon összeírja a számhármásokat. Vagyis, minden hármas blokkban az első, második és harmadik sorokat összefűztem. Ahhoz, hogy másik diédercsoportra alkalmazzuk, összesen a forciklusok futási végét kell átírni: a külső forciklusét az "összes" munkalapon lévő adatok sorára, a belsőt pedig az $n\phi(n)$ értékre. (Fontos megjegyezni, hogy a munkalapokat a kódok futtatása előtt létre kell hozni megfelelő nevekkel, melyek a kód legelején az értékadásnál vannak meghatározva.)

Ekkor az orbitokon belül az elemek ismétlődhetnek olyan formában, hogy például a $\{tf^2, tf^3, tf^8\}$-nak megfelelő $(2-3-8)$ számhármas előfordul $(3-8-2)$-ként is. Ezek mind ekvivalensek, hiszen ezekre mint halmazokra kell gondolnunk, viszont a program erre nem képes. Ezért sorba kellett rendeznem a számhármasok elemeit, hogy később össze tudjam hasonlítani őket. A sorbarendezést egymásba ágyazott $if()$ függvényekkel oldottam meg. Ez a függvény a 5. ábrán látható.

Ezután meg szerettem volna számolni, hogy hány darab különböző orbitja van az automorfizmusnak. Ehhez kettő darab függvényt írtam. Az egyik kiszűtei az orbitokon belüli számhármasok ismétlődését egy segédvektor és egymásbaágyazott forciklusok segítségével, a másik pedig sorbarendezte az orbitokon belüli elemeket. Az utóbbihoz az excel beépített sorbarendezés funkcióját használtam. Ezután már csak az ismétlődéseket kellett eltávolítanom, melyeket az Adatok/Ismétlődés eltávolítása funkcióval meg is tettem. Ekkor visszakaptam a D_{30} automorfizmus csoport orbitjait. Ebből összesen 25 db találtam. (A programokat lsd.: 5, 5 ábrák)

	A	B	C	D	E	F	G	H	I	J	K
1	0-11-19	0-11-22	0-1-2	0-1-29	0-13-17	0-13-26	0-16-23	0-28-29	0-4-17	0-7-14	0-7-23
2	0-1-28	0-1-3	0-14-21	0-14-23	0-17-21	0-17-26	0-19-22	0-19-27	0-2-29	0-2-3	0-27-28
3	0-11-14	0-11-27	0-1-27	0-13-21	0-13-22	0-1-4	0-16-19	0-16-27	0-21-23	0-21-28	0-2-23
4	0-11-16	0-11-25	0-1-26	0-14-19	0-14-25	0-1-5	0-17-22	0-17-25	0-2-25	0-23-25	0-23-28
5	0-12-17	0-12-25	0-1-25	0-13-18	0-13-25	0-1-6	0-18-23	0-18-25	0-19-24	0-19-25	0-24-25
6	0-11-17	0-11-18	0-11-23	0-11-24	0-1-13	0-1-18	0-12-13	0-12-19	0-12-23	0-12-29	0-1-24
7	0-11-13	0-11-28	0-1-14	0-1-17	0-1-23	0-13-14	0-13-29	0-16-17	0-16-29	0-17-19	0-17-28
8	0-1-22	0-13-16	0-13-27	0-14-17	0-14-27	0-1-9	0-19-21	0-19-28	0-2-11	0-21-22	0-21-29
9	0-10-13	0-10-19	0-10-21	0-10-27	0-1-10	0-11-20	0-11-21	0-1-21	0-17-20	0-17-27	0-20-21
10	0-10-11	0-10-17	0-10-23	0-10-29	0-1-11	0-1-20	0-13-20	0-13-23	0-19-20	0-19-29	0-7-17
11	0-11-12	0-1-12	0-11-29	0-1-19	0-17-23	0-17-24	0-18-19	0-18-29	0-6-13	0-6-23	0-7-13
12	0-11-15	0-11-26	0-1-15	0-1-16	0-13-15	0-13-28	0-14-15	0-14-29	0-15-16	0-15-17	0-15-19
13	0-14-16	0-14-22	0-14-28	0-2-16	0-22-26	0-2-28	0-2-4	0-26-28	0-4-26	0-4-8	0-8-16
14	0-16-21	0-16-25	0-21-25	0-21-26	0-22-25	0-22-27	0-2-27	0-2-5	0-25-27	0-25-28	0-3-25
15	0-12-14	0-12-28	0-16-18	0-16-22	0-16-24	0-16-28	0-18-22	0-18-26	0-2-14	0-2-18	0-2-26
16	0-12-16	0-12-26	0-14-18	0-14-26	0-22-24	0-22-28	0-2-24	0-2-8	0-4-16	0-4-18	0-6-28
17	0-10-14	0-10-26	0-16-20	0-16-26	0-20-22	0-20-28	0-2-10	0-2-22	0-4-14	0-4-20	0-8-10
18	0-10-12	0-10-16	0-10-18	0-10-22	0-10-24	0-10-28	0-12-20	0-12-22	0-14-20	0-14-24	0-18-20
19	0-12-21	0-24-27	0-3-27	0-3-6	0-9-18	0-9-21	10-13-16	10-19-28	1-10-19	1-10-22	11-14-1
20	0-18-21	0-18-27	0-21-24	0-21-27	0-3-12	0-3-21	0-3-24	0-3-9	0-6-27	0-6-9	0-9-12
21	0-12-15	0-12-27	0-15-18	0-15-21	0-15-24	0-15-27	0-3-15	0-3-18	0-6-15	0-6-21	0-9-15
22	0-20-25	0-5-10	0-5-25	10-15-20	11-16-21	1-21-26	12-17-22	13-18-23	14-19-24	15-20-25	1-6-11
23	0-10-15	0-10-25	0-15-20	0-15-25	0-5-15	0-5-20	10-15-25	10-20-25	1-11-16	1-11-26	11-16-2
24	0-12-18	0-12-24	0-18-24	0-6-12	0-6-18	0-6-24	10-16-22	10-16-28	10-22-28	11-17-23	11-17-2
25	0-10-20	1-11-21	2-12-22	3-13-23	4-14-24	5-15-25	6-16-26	7-17-27	8-18-28	9-19-29	

A 25 db orbit (nem teljes kép)

A Burnside-lemmát használtam az eredményem ellenőrzéséhez. Viszont a lemma permutációcsoportokra vonatkozik, ám a 2.9 kihasználva alkalmazhatom csoportra is.

4.1. Tétel (Burnside-lemma)**.** *Ha $G \leq S_X$ permutációcsoport, akkor G pályáinak száma éppen a G elemei fixpontjainak átlagos száma.*

Amikor az adataim még nem voltak teljesek, vagyis csak a számhármasaim lettek kialakítva még (az "összevont" munkalapon), akkor megszámoltam, hogy hány fixpontja volt egy-egy orbitnak, és kiírtam az orbitok elé az első oszlopba. Szerencsére könnyű volt kitalálni, hogy egy-egy orbitnak mi a fixpontja, hiszen az *orbit.m* függvényben megalkotott mátrixnak első oszlopa mindig a generátort tartalmazta, hiszen az első elem azt a leképezés képét tartalmazta egy adott bázisra, mely $t \to t, f \to f$. Így csak össze kellett számolnom soronként, hogy hány

ugyanolyan elem van, mint a sor első eleme (lsd.: 5. ábra). Ezután ezeket összeadva és elosztva 240-gyel visszakaptam az orbitok számát, mely itt is 25 lett.

A4061 =SZUM(A1:A4060)/240

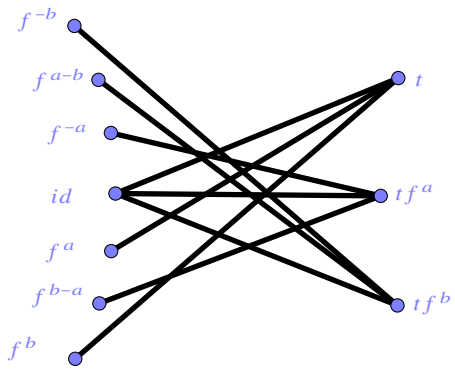
	A	B	C	D	E	F
4054	1	25-27-28	9-16-25	5-8-27	4-21-25	5-9-26
4055	2	25-27-29	9-23-25	5-19-27	17-21-25	5-9-13
4056	1	25-28-29	16-23-25	5-8-19	4-17-25	5-13-26
4057	2	26-27-28	2-9-16	8-16-27	4-8-21	9-22-26
4058	1	26-27-29	2-9-23	16-19-27	8-17-21	9-13-22
4059	1	26-28-29	2-16-23	8-16-19	4-8-17	13-22-26
4060	2	27-28-29	9-16-23	8-19-27	4-17-21	9-13-26
4061	25					

A Burnside-lemma által kapott

A programjaim minimális átírással használhatók bármely véges diédercsoport automorfizmusára orbitszámlálóként. Csak a forciklusok végét kell átírni a $n\phi(n)$-re és az "összes" munkalapon található sorok számára.

4.2. D_{30} Cayley gráfjának a vizsgálata

A következő feladatom az előző részben felírt D_{30} diédercsoport egy Cayley-gráfjának a vizsgálata volt. Ennek a generátora legyen a $\{t, tf^a, tf^b\}$. Ekkor, a D_{30} Cayley gráfja az alábbi kezdetleges gráf:



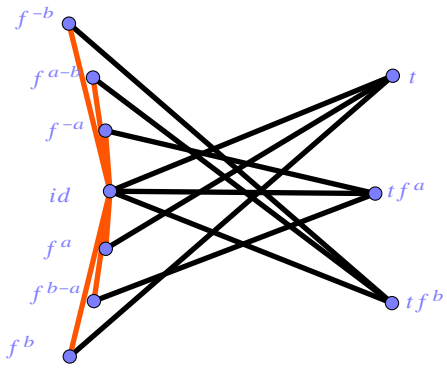
Ezt a gráfot az alábbi képzésekkel kaptam:

$$
\begin{aligned}
1 \to t \to tt f^a &= f^a \\
1 \to t \to tt f^b &= f^b \\
1 \to t f^a \to t f^a t &= f^{-a} \\
1 \to t f^a \to t f^a t f^b &= f^{b-a} \\
1 \to t f^b \to t f^b t &= f^{-b} \\
1 \to t f^b \to t f^b t f^a &= f^{a-b}
\end{aligned}
$$

Készítettem egy segédgráfot, ahol a fenti kettő hosszú utakat kicseréltem egyhosszú utakra. Ezek rendre az alábbiak lettek:

$$
\begin{aligned}
1 &\to f^a \\
1 &\to f^b \\
1 &\to f^{-a} \\
1 &\to f^{b-a} \\
1 &\to f^{-b} \\
1 &\to f^{a-b}
\end{aligned}
$$

Ezeket az éleket pirossal jelöltem a gráfomban.



Ekkor a C_{30} ciklikuscsoport egy Cayley-gráfját kaptuk, ahol a generátorok az $\{f^{\pm a}, f^{\pm b}, f^{\pm a-b}\}$. Muzychuk tétele alapján (3.1) a C_{30} is rendelkezik a CI-tulajdonsággal, hiszen a rendje 30, ami $30 = 2 * 15$, vagyis $2k$ alakú, ahol k egy négyzetmentes páratlan egész. (Itt latszik, hogy 30 helyett más egész számot is használhattam volna, amire Muzychuk tétele igaz.)

Ekkor felmerül a kérdés, hogy meghatározhatóak-e az a, b számok? A válasz az, hogy 30-hoz relatív prím konstnasszorzó erejéig igen, hiszen ilyen esetekben igaz a CI-tulajdonság. Vagyis, a C_{30} két Cayley-gráfja, akkor lesz izomorf, ha a generátoraik megkaphatóak egymásból egy 30-hoz relatív prím konstans szorzás segítségével. Azaz, a $\{t, tf^{a}, tf^{b}\}$ generátorhalmazt elvihetjük $\{t, tf^{ax}, tf^{bx}\}$-ba, ahol x relatív prím 30-hoz. Ezzel tehat azt kaptuk, hogy konstans szorzo erejeig megkaptuk a $\pm a, \pm b, \pm(a-b)$ halmazt, amiből algebrai úton nem tudjuk visszakeresni az a, b számpárt, mert csak az látszik, hogy a különbségük és ellentettjeik a 6 szám között van. Ez ugyanígy igaz $a-b$-re és a-ra is.

Nézzünk tehát ezt a példát. Legyen a generátor a háromelemű $S = \{t, t^{a}, tf^{b}\}$ halmaz, a csoport a C_{30}, és $G = Cay(C_{30}, S)$. Jelölje $T = \{t, tf^{a-b}, tf^{a}\}$ egy másik generátorhalmazt. Ekkor az $f \to f^{-1}, tf^{a}$ jobbról való szorzást alkalmazva kapható meg a $\{t, tf^{a-b}, tf^{a}\}$-t. Vagyis a $Cay(C_{30}, T) \simeq Cay(C_{30}, S)$, hiszen az automorfizmusuk egymásba viszi T-t és S-et. Ezzel bebizonyosodott, hogy ez a háromelemű halmaz rendelkezik a CI-tulajdonsággal D_{30}-ban is, hiszen automorfizmus erejéig

előállítható G-ből $Cay(D_{30}, S)$.

5. Függelékek - Programok

```
function matrix=orbit(d,a,b,c)

p(1)=1;
for j=2:d
    if gcd(j,d)==1
    p(end+1)=j;
    end
end
p;
i=[0:1:d-1];
for x=1:d
    for y=1:length(p)
        sor_a(end+1)=mod(i(x)+a*p(y),d);
        sor_b(end+1)=mod(i(x)+b*p(y),d);
        sor_c(end+1)=mod(i(x)+c*p(y),d);
    end
end
matrix=[sor_a; sor_b; sor_c];
```

Orbit.m függvény

```
clear
m=zeros(1,240);
for i=0:27
    for j=i+1:28
        for k=j+1:29
            m=[m;orbit(30,i,j,k)];
        end
    end
end
save D_30.xls m
```

Az összes lehetséges orbit előállítása

```
Sub osszevonas()
o = "osszes"
vt = "osszevont"

For i = 0 To 4060
    For j = 2 To 241
        a = Sheets(o).Cells(i * 3 + 2, j)
        b = Sheets(o).Cells(i * 3 + 3, j)
        c = Sheets(o).Cells(i * 3 + 4, j)
        If a > b Then
            If a > c Then
                If b > c Then
                    Sheets(vt).Cells(i + 1, j) = c & "-" & b & "-" & a
                Else
                    Sheets(vt).Cells(i + 1, j) = b & "-" & c & "-" & a
                End If
            Else
                Sheets(vt).Cells(i + 1, j) = b & "-" & a & "-" & c
            End If
        Else
            If b > c Then
                If a < c Then
                    Sheets(vt).Cells(i + 1, j) = a & "-" & c & "-" & b
                Else
                    Sheets(vt).Cells(i + 1, j) = c & "-" & a & "-" & b
                End If
            Else
                Sheets(vt).Cells(i + 1, j) = a & "-" & b & "-" & c
            End If
        End If
    Next j
Next i
End Sub
```

A számhármas kialakításokhoz alkalmazott függvény

```
Sub ism_kiszurese()
Dim arr() As String
vt = "osszevont"
v = "vegleges"
ism = 0
ReDim Preserve arr(0)
arr(0) = 0
For i = 1 To 4060
    For j = 2 To 241
        For x = 1 To GetLength(arr)
            If Sheets(vt).Cells(i, j) = arr(x - 1) Then
                ism = 1
                Exit For
            End If
        Next x
        If ism = 0 Then
            p = GetLength(arr)
            ReDim Preserve arr(p)
            arr(p) = Sheets(vt).Cells(i, j)
            Sheets(v).Cells(i, p) = Sheets(vt).Cells(i, j)
        End If
        ism = 0
    Next j
    Erase arr
    ReDim Preserve arr(0)
    arr(0) = 0
Next i
End Sub

Public Function GetLength(a As Variant) As Integer
   If IsEmpty(a) Then
      GetLength = 0
   Else
      GetLength = UBound(a) - LBound(a) + 1
   End If
End Function
```

Az orbiton belüli ismétlődő elemek eltávolítása

```
Sub sorba_rendezes()
v = "vegleges"
r = "rendezett"
s = "segéd"
For i = 1 To 4060
    Sheets(v).Select
    Sheets(v).Cells(i, 1).EntireRow.Select
    Selection.Copy
    Sheets(s).Select
    Sheets(s).Cells(1, 1).Select
    Selection.PasteSpecial Paste:=xlPasteAll, Operation:=xlNone, SkipBlanks:= _
        False, Transpose:=True
    Application.CutCopyMode = False
    ActiveWorkbook.Worksheets(s).Sort.SortFields.Clear
    ActiveWorkbook.Worksheets(s).Sort.SortFields.Add Key:=Range("A1"), _
        SortOn:=xlSortOnValues, Order:=xlAscending, DataOption:=xlSortNormal
    With ActiveWorkbook.Worksheets(s).Sort
        .SetRange Range("A1:A240")
        .Header = xlNo
        .MatchCase = False
        .Orientation = xlTopToBottom
        .SortMethod = xlPinYin
        .Apply
    End With
    Sheets(s).Select
    Sheets(s).Range("A1:A240").Select
    Selection.Copy
    Sheets(r).Select
    Sheets(r).Cells(i, 1).Select
    Selection.PasteSpecial Paste:=xlPasteAll, Operation:=xlNone, SkipBlanks:= _
        False, Transpose:=True
Next i
End Sub
```

Az ismétlődő számhármasok nélküli orbitok elemeinek sorbarendezése

```
Sub fixpont_szamlalo()
vt = "osszevont"
szam = 1
For i = 1 To 4060
    For j = 3 To 241
        If Sheets(vt).Cells(i, j) = Sheets(vt).Cells(i, 2) Then
            szam = szam + 1
        End If
    Next j
    Sheets(vt).Cells(i, 1) = szam
    szam = 1
Next i
End Sub
```

A Burnside-lemma alkalmazásánál használt fixpontszámláló algoritmus

Hivatkozások

[1] https://hu.wikipedia.org/wiki/Babai_László

[2] Arthur Cayley: I.-X. Memoirs on Quantics (1854–78)

[3] László Babai: Graph Isomorphism in quasipolynomial time, STOC '16: Proceedings of the forty-eighth annual ACM symposium on Theory of Computing (2016)

[4] https://ematlap.hu/tudomany-tortenet-2017-03/426-babai-es-a-graf-izomorfizmus-problema#Ba

[5] Cai Heng Li: Isomorphisms of Connected Cayley Digraphs, Graphs and Combinatorics 14 (1998) 37.-44.

[6] Cai Heng Li: On isomorphisms of connected Cayley graphs, Discrete Mathematics 178 (1998) 109.-122.

[7] Mikhail Muzychuk: On Ádám's conjecture for circulant graphs, Discrete Mathematics 167-168, (1997), 497.-510.

[8] Hiroki Koike, István Kovács, Dragan Marušič, Mikhail Muzychuk: Cyclic groups are CI-groups for balanced configurations, Designs, Codes and Cryptography 87, (2019) 1227.–1235.

[9] Gábor Somlai: The Cayley isomorphism property for groups of order 8p, Cornell University arXiv:1301.6797v1 (2013)

[10] M.Hirasaka, Mikhail Muzychuk: Association schemes generated by a non-symmetric relation of valency 2, Discrete Mathematics 244 (2002) 109.-135.

[11] Cai Heng Li: On isomorphisms of finite Cayley graphs, European Journal of Combinatorics 19 (1998) 911.-919.

[12] Derek J.S. Robinson A Course in the Theory of Groups, Springer-Verlag New York, Inc. (1996)

[13] Ming-Yao Xu: Automorphism groups and isomorphism of Cayley digraphs, Discrete Mathematics 182 (1998) 309.-319.

[14] Q. Huang, J. Meng: Isomorphisms of circulant digraphs, Applied Mathematics-A Journal of Chinese Universities volume 9 (1994) 405.–409.

[15] Q. Huang, J. Meng: Automorphism groups of Cayley digraphs, Combinatorics, Graph Theory, Agorithsm and Applications, Y. Alavi, D.R. Lick, Jiuqiang Liu (Eds.), World Scientific, Singapore (1994) 77.-81

[16] Q. Huang, J. Meng: On the isomorphisms and automorphism groups of circulants, Graphs Combin. 12 (1996) 179.-187.

[17] Yan-Quan Feng: A note on isomorphisms of Cayley digraphs of Abelian groups, Australasian Journal of Combinatorics 15 (1997),87.-90.

[18] L. Babai: Isomorphism problem for a class of point-symmetric structures, Acta Math. Sci. Hungar. 29 (1977) 329.-336.

[19] `https://groupprops.subwiki.org/wiki/Burnside%27s_basis_theorem`

[20] Kiss Emil: Bevezetés az algebrába, Typotex Kiadó (2014)