Cayley gráfok izomorfizmus problémája

Mező József

Témavezető: Pálfy Péter Pál egyetemi tanár

Eötvös Loránd Tudományegyetem

Budapest, 2005

Tartalomjegyzék

1. fejezet

Bevezetés

A gráfelmélet egyik alapvető problémája két adott gráfról eldönteni, hogy izomorfak-e. Szakdolgozatomban ezt a problémát vizsgálom Cayley-gráfokra. Az első két fejezet ennek áttekintése, és bevezető jellegű a többi fejezethez, támaszkodva Cai Heng Li [13] összefoglaló cikkére és Pálfy Péter Pál egy akadémiai előadására.

A Cayley-gráfok csúcsai egy G véges csoport elemeinek felelnek meg, az adjacencia relációt pedig egy $S \subseteq G$ csatlakozó halmaz segítségével definiáljuk. A. Cayley 1878-ban absztrakt csoportok egy gráfreprezentációjaként vezette be az olyan típusú diagramot, amit ma *Cayley színezett diagram*-nak nevezünk. Ezt Coxeter és Moser [10] használták először generátorokkal és relációkkal megadott csoportok vizsgálatára. A Cayley színezett diagram egy irányított gráf színezett élekkel, és akkor lesz belőle Cayley-gráf, ha elhagyjuk a színeket. A Cayley színezett diagramok általánosítása a *Schreier mellékosztály diagram*ok, amit Schreier vezetett be 1927-ben. Ezeket mint gráfokat először Sabidussi [25] vizsgálta. A Cayley-gráfok és általánosításaik, a csúcstranzitív gráfok vizsgálata hosszú ideje aktív téma az algebrai gráfelméletben, lásd [7], [8] és [24].

A Cayley-gráfok izomorfiaosztályaival kapcsolatos kutatások 1967-ben kezdődtek Ádám Andrásnak [1] a Journal of Combinatorial Theory probléma-rovatában közzétett kérdésével. Azt sejtette, hogy két ciklikus gráf pontosan akkor izomorf, ha van közöttük olyan izomorfizmus is, ami egyúttal a hozzájuk tartozó ciklikus csoportnak egy automorfizmusa. Más szavakkal egy ciklikus csoport minden Cayley-gráfja *CI-gráf*. Sejtésére már 1970-ben ellenpéldát talált B. Elspas és J. Turner [11], azonban a teljes válasz csak 30 évvel a probléma megfogalmazása után született meg. M. Muzychuk [19] és [20] a Schur-gyűrűk elméletét felhasználva bebizonyította, hogy azokra az esetekre, amelyekre addig nem találtak ellenpéldát, a sejtés már igaz:

1.1 TÉTEL. *Ádám András sejtése pontosan akkor igaz, ha n négyzetmentes szám, vagy egy páratlan négyzetmentes szám négyszerese. Irányítatlan gráfokra igaz akkor is, ha $n = 8$, 9 vagy 18.*

Időközben a problémát több irányban általánosították. Kézenfekvő, hogy ciklikus csoport helyett tetszőleges véges csoport Cayley-gráfjaira általánosítsuk a problémát, gráfok helyett pedig tetszőleges relációstruktúrákat is tekinthetünk. Ezt a kétirányú általánosítást

1977-ben fogalmazta meg Babai László [4]. A G alaphalmazú $\Re$ relációstruktúra *Cayley-objektum*, ha az összes jobb-eltolás automorfizmusa $\Re$-nek. $\Re$ *CI-objektum*, ha minden vele izomorf Cayley-objektumba átvihető egy csoport automorfizmussal is. Egy G csoportot *globálisan CI-csoport*nak nevezünk, ha minden Cayley-objektuma CI-objektum. 1987-ben a véges egyszerű csoportok osztályozásának egy nevezetes következményét, a kétszeresen tranzitív permutációcsoportok teljes leírását felhasználva Pálfy Péter Pál [23] meghatározta az összes ilyen csoportot:

1.2 TÉTEL. *A véges globálisan CI-csoportok a következők: azok a ciklikus csoportok, amelyeknek n rendjére $(n, \varphi(n)) = 1$ teljesül, továbbá a 4-elemű csoportok. Ha egy csoport nem globálisan CI-csoport, akkor van olyan Cayley-objektuma, ami egyetlen négyváltozós relációból áll és nem CI-objektum.*

Egy G véges csoportot *DCI-csoport*nak nevezünk, ha minden irányított Cayley-gráfja CI-gráf és *CI-csoport*nak, ha minden irányítatlan Cayley-gráfja CI-gráf. Muzychuk tétele (1.1) megadja, hogy a ciklikus csoportok közül melyek az ilyen csoportok. Könnyű látni, hogy CI-csoport minden részcsoportja is CI-csoport. Ezt (is) használva még 1978-ban Babai László és Frankl Péter [5] meghatározták, hogy mely csoportok lehetnek Sylow-részcsoportok egy CI-csoportban:

1.3 TÉTEL. *CI-csoport Sylow részcsoportja vagy elemi Abel-féle p-csoport (azaz Z_p^k), vagy Z_4, Z_8, Q, Z_9 valamelyike.*

A kérdés tehát az, hogy mely elemi Abel-csoportok, azaz mely Z_p^k csoportok CI-csoportok. A Schur-gyűrűk módszerével 2001-ben Hirasaka és Muzychuk [12] belátták, hogy Z_p^4 DCI-csoport, majd 2003-ban Muzychuk [21] megmutatta, hogy Z_p^k nem DCI-csoport, ha k (p-től függően) elég nagy. Irányított esetben tehát a következő a kérdés:

1.4 PROBLÉMA. *Van-e minden k-hoz olyan p páratlan prím, hogy Z_p^k DCI-csoport?*

Még 1992-ben L. A. Nowitz [22] megmutatta, hogy Z_2^6 nem CI-csoport, 1998-ban pedig Conder és Li [9] számítógép segítségével látták be, hogy Z_2^5 CI-csoport. Ha $p \neq 2$, akkor csak annyit tudunk, hogy Z_p^4 CI-csoport, tehát a következő kérdésre sem született még válasz:

1.5 PROBLÉMA. *Van-e minden p páratlan prímhez olyan k, hogy Z_p^k nem CI-csoport?*

A negyedik fejezetben Joy Morris egy közelmúltban megjelent cikkéből [18] kiindulva az elemi Abel esetet tárgyalom teljes részletességgel. Ennek során különféle segédgráfok használatával elemi bizonyítást adok a Z_p^4 esetre. Ezúton is szeretném megköszönni témavezetőmnek, Pálfy Péter Pálnak az érdekes témát, a sok értékes megjegyzést és segítséget.

2. fejezet

Cayley-gráfok

2.1. Cayley-gráfok és néhány izomorfizmus probléma

Az alábbiakban G mindig egy véges csoport, $S \subseteq G$ egy részhalmaz.

2.1 DEFINÍCIÓ. *A (G, S) párhoz tartozó Cayley gráfnak nevezzük és $Cay(G, S)$-sel jelöljük azt a Γ irányított gráfot, amelynek csúcsai G elemei és x-ből pontosan akkor vezet él y-ba, ha $yx^{-1} \in S$. Ekkor Γ-t a G csoport egy Cayley-gráfjának, S-et pedig a Γ Cayley-gráf csatlakozó halmazának mondjuk.*

$Cay(G, S)$ tehát egy $|S|$-reguláris irányított Γ gráf, ahol

$$V(\Gamma) = G, \quad E(\Gamma) = \{(g, sg) : g \in G, s \in S\}$$

Ha minden (g, sg) élnek megfeleltetünk egy s színt, akkor *színezett Cayley-gráfot*, ha pedig S egy generátorrendszer és minden s színt különbözőnek választunk, akkor *Cayley színezett diagram*mot kapunk.
Megjegyzés. Néhány egyszerű észrevétel:

(i) Az S halmaz pontosan akkor tartalmazza G egységelemét, ha $Cay(G, S)$ minden csúcsnál tartalmaz hurokélt. Ezért a továbbiakban feltesszük, hogy $e \notin S$.

(ii) $\langle S \rangle = G$ pontosan akkor, ha $Cay(G, S)$ összefüggő.

(iii) Ha $S = S^{-1}$, azaz $\forall s \in S$-re $s^{-1} \in S$, akkor $Cay(G, S)$ irányítatlan gráfnak tekinthető.

Egy alapvető probléma a *Cayley-gráfok izomorfizmusproblémája*:

2.2 PROBLÉMA. *Legyen $Cay(G, S)$ és $Cay(H, T)$ két adott Cayley-gráf. Döntsük el, hogy $Cay(G, S) \cong Cay(H, T)$?*

Most legyen Γ egy tetszőleges (reguláris) irányított gráf.

2.3 DEFINÍCIÓ. *A Γ irányított gráfot Cayley-gráfnak nevezük, ha $\exists$ hozzá egy (G, S) pár, melyre $\Gamma \cong Cay(G, S)$. Ezt a (G, S) párt pedig a Γ gráf egy Cayley reprezentációjának nevezzük.*

Γ két Cayley reprezentációja $Cay(G, S)$ és $Cay(H, T)$ *ekvivalens*, ha $\exists \sigma \in Sym(V)$, amely izomorfizmust indukál a G csoportból a H csoportba és $S^\sigma = T$. Speciálisan Γ két Cayley reprezentációja, $Cay(G, S)$ és $Cay(G, T)$ pontosan akkor ekvivalens, ha $S^\sigma = T$ valamely $\sigma \in Aut(G)$-re. Adódik a következő kérdés:

2.4 PROBLÉMA. *(Gráfok Cayley reprezentációs problémája) Határozzuk meg Γ összes nem ekvivalens Cayley reprezentációját.*

2.5 PÉLDA. *Legyen $\Gamma = K_n$ az n pontú irányítatlan teljes gráf. Ekkor $\Gamma \cong Cay(G, S)$, ahol G egy tetszőleges n rendű csoport, S pedig G összes nem egységelemeinek halmaza. Ezért Γ nem ekvivalens Cayley reprezentációinak száma egyenlő a nemizomorf n rendű csoportok számával.*

A $\Gamma = (V, E)$ irányított gráf automorfizmuscsoportjának nevezzük és AutΓ-val jelöljük az adjacencia relációt tartó $\sigma \in Sym(V)$ permutációk halmazát. Legyen Γ=$Cay(G, S)$. Jelölje g_R a $g \in G$-vel való jobb-eltolást, G_R pedig G jobb-eltolásainak csoportját:

$$G_R = \{g_R : g \in G\}, \ \textit{ahol } x^{g_R} = xg \ \forall x \in V.$$

Hasonlóan definiálható G bal-eltolásainak csoportja:

$$G_L = \{g_L : g \in G\}, \ \textit{ahol } x^{g_L} = gx \ \forall x \in V.$$

Ha $yx^{-1} \in S$, akkor $yg(xg)^{-1} = yx^{-1} \in S$, így $G_R \leq Aut\ \Gamma$. Minden $x, y \in V$-hez egyértelműen létezik egy $g_R = x_R^{-1} y_R \in G_R$ elem, melyre $x^{g_R} = y$, ezért G_R reguláris részcsoportja $Aut\ \Gamma$-nek. Tehát igazak a következők:

- A Cayley-gráfok *csúcstanzitív gráfok*
- Ha $Cay(G, S)$ nem összefüggő, akkor minden komponens izomorf egy kisebb Cayley-gráffal: $Cay(\langle S \rangle, S)$-el.
- $Cay(G, S) \cong Cay(G, T) \iff Cay(\langle S \rangle, S) \cong Cay(\langle T \rangle, T)$

Ha Γ a G csoport egy Cayley-gráfja, akkor $Aut\ \Gamma$-nak van egy G-vel izomorf reguláris részcsoportja: G_R. Ennél több is igaz:

2.6 TÉTEL. (Sabidussi [25]) *Egy Γ irányított gráf pontosan akkor lesz a G csoport egy Cayley-gráfja, ha $Aut\ \Gamma$ tartalmaz egy G-vel izomorf és V-n reguláris részcsoportot.*

Bizonyítás. Ha $\Gamma = Cay(G, S)$, akkor az előzőek szerint $G_R \leq Aut\ \Gamma$. Megfordítva, legyen $G_R \leq Aut\ \Gamma$, ahol $G \cong G_R$ és g képe az izomorfizmusnál g_R. G_R reguláris, így $|V| = |G|$, tehát bijekció létesíthető G elemei és Γ pontjai között a következő módon.

G egységelemének feleljen meg V egy tetszőleges v_0 pontja, majd minden $g \in G$-re g-nek a $v_0 g_R$ pont. Végül az S halmaz álljon azon G-beli elemekből, melyeknek az imént v_0 szomszédait feleltettük meg. Ezzel $\Gamma \cong Cay(G,S)$, hiszen a fenti bijekciónál g szomszédaihoz éppen azokat a pontokat rendeltük, amiket az sg alakú elemekhez. ■

Természetes kérdések a következők:

2.7 PROBLÉMA. *Legyen $\Gamma = (V,E)$ egy irányított gráf.*

1. *Határozzuk meg $Aut\ \Gamma$-t és döntsük el, van-e V-n reguláris részcsoportja.*
2. *Határozzuk meg a Γ Cayley-gráf $Aut\ \Gamma$ automorfizmuscsoportjának az összes V-n reguláris részcsoportját.*
3. *Határozzuk meg a Γ Cayley-gráf összes nem ekvivalens $Cay(G,S)$ G-hez tartozó Cayley reprezentációját.*

2.2. Példák

2.8 PÉLDA.

$$G = \langle a \rangle \cong Z_{n^2},\ H = \langle x, y | x^n = y^2 = 1, y^{-1}xy = x^{-1} \rangle \cong D_{2n}.$$

Ekkor

$$Cay(G, \{a, a^{-1}\}) \cong C_{2n} \cong Cay(H, \{y, xy\}),\ \text{és}\ Aut(C_{2n}) \cong D_{4n}.$$

2.9 DEFINÍCIÓ. *Jelölje $K_{m;d}$ az irányítatlan teljes d-partíció gráfot, ahol az osztályok m eleműek. Itt pontosan akkor van összekötve két pont, ha különböző osztályból valók.*

2.10 DEFINÍCIÓ. *Legyen G az $\Omega_1 = \{x_1, \ldots, x_m\}$, H pedig az $\Omega_2 = \{y_1, \ldots, y_n\}$ halmazon egy permutációcsoport. Ekkor G és H koszorú szorzatának nevezzük, és $G \wr H$-val jelöljük a következő permutációcsoportot $\Omega_1 \times \Omega_2$-n:*

$$G \wr H = \{(g_1, \ldots, g_n, h) : h \in H,\ g_i \in G,\ i = 1, \ldots, n\},\ \text{ahol}$$
$$(g_1, \ldots, g_n, h)(x_i, y_j) = (g_j(x_i), h(y_j)),\ (j = 1, \ldots, n).$$

Könnyen látható, hogy $AutK_{m;d} \cong S_m \wr S_d$.

2.11 DEFINÍCIÓ. *A $B \subseteq V$ halmazt G – blokknak hívjuk, ha minden $g \in G$-re $g(B) = B$ vagy $g(B) \cap B = \emptyset$. Ha emellett G tranzitív permutációcsoport, akkor a $\mathbf{B} = \{g(B) : g \in G\}$ partíciót G-invariáns partíciónak nevezzük. Ha $\mathbf{B}$ G_1- és G_2-invariáns, akkor nyilván $\langle G_1, G_2 \rangle$-invariáns, tehát erre a tulajdonságra nézve van egy M maximális részcsoport $Sym(V)$-ben. Ekkor $\mathbf{B}$-t nevezzük M-partíciónak.*

2.12 ÁLLÍTÁS. *A G csoportnak pontosan akkor van egy $K_{m;d}$-vel izomorf Cayley-gráfja, ha G rendje md és van egy m-ed rendű részcsoportja.*

Bizonyítás. Legyen $Cay(G,S) \cong K_{m;d}$, valamilyen $S \subset G$-re. Nyilvánvalóan $K_{m;d}$ d-partíciójának osztályai a csúcsok egy $\mathbf{B}$ $Aut\Gamma$-invariáns partícióját adják. Speciálisan $\mathbf{B}$ G_R-invariáns, és $B \in \mathbf{B}$-re a $(G_R)_B$ stabilizátor indexe G_R-ben d, G_R rendje pedig épp a csúcsok száma, azaz md. Megfordítva, legyen $G_0 \leq G_R$ egy m rendű részcsoport. Az S halmaz legyen G_0 komplementere. Ekkor $Cay(G,S) \cong K_{m;d}$. ■

Fogalmazzuk meg ezt a permutációcsoportok nyelvén.

2.13 ÁLLÍTÁS. *Legyen $X \cong S_m \wr S_d$ egy imprimitív permutációcsoport az md rendű Ω halmazon. Ekkor egy G csoport pontosan akkor ágyazható be X-be Ω-n reguláris részcsoportként, ha G-nek van egy m rendű részcsoportja.*

2.14 DEFINÍCIÓ. *A $\Gamma_1 = (V_1, E_1)$ és $\Gamma_2 = (V_2, E_2)$ irányított gráfok Descartes-szorzata az a $\Gamma_1 \times \Gamma_2$-vel jelölt azt Γ irányított gráf, melyre:*

$$V(\Gamma) = V_1 \times V_2,\ E(\Gamma) = \{((a_1,a_2),(b_1,b_2)) : (a_1,b_1) \in E_1 \textit{ és } a_2 = b_2$$

$$\textit{vagy } (a_2,b_2) \in E_2 \textit{ és } a_1 = b_1\}$$

2.15 PÉLDA.

$$\Gamma \cong C_n^d,\ \textit{ahol } n = 3 \textit{ vagy } n \geq 5.$$

Ekkor

$$Aut\Gamma \cong D_{2n} \wr S_d = D_{2n}^d S_d.$$

Ha n páratlan, akkor Γ izomorf Z_n^d egy Cayley gráfjával, ha pedig n páros, akkor egy $G_1 \times G_2 \times \cdots \times G_d$ csoport Cayley-gráfjával, ahol $G_i \cong Z_n$ vagy D_n.

2.16 DEFINÍCIÓ. *A $\Gamma_1 = (V_1, E_1)$ és $\Gamma_2 = (V_2, E_2)$ irányított gráfok lexikografikus szorzatának nevezzük és $\Gamma_1[\Gamma_2]$-vel jelöljük azt a Γ irányított gráfot, melyre:*

$$V(\Gamma) = V_1 \times V_2,\ E(\Gamma) = \{((a_1,a_2),(b_1,b_2)) : (a_1,b_1) \in E_1 \textit{ vagy } a_1 = b_1 \textit{ és } (a_2,b_2) \in E_2\}$$

2.17 PÉLDA.

$$G = \langle a \rangle \cong Z_{n^2},\ S = a\langle a^n \rangle,\ \textit{illetve } H = \langle b, c \rangle \cong Z_n \times Z_n,\ T = b\langle c \rangle.$$

$$Cay(G,S) \cong C_n[\overline{K_n}] \cong Cay(H,T),$$

ahol C_n egy irányított n hosszú kör, $\overline{K_n}$ pedig az n pontú él nélküli gráf. Hasonlóan

$$S' = a\langle a^n \rangle \cup a^{-1}\langle a^n \rangle,\ \textit{illetve } T' = b\langle c \rangle \cup b^{-1}\langle c \rangle$$

$$Cay(G,S') \cong C_n[\overline{K_n}] \cong Cay(H,T'),$$

ahol C_n most egy irányítatlan n hosszú kör.

2.3. CI-gráfok

2.18 DEFINÍCIÓ. *A $Cay(G,S)$ Cayley-gráfot CI-gráfnak nevezzük, ha minden vele izomorf $Cay(G,T)$ Cayley-gráfhoz van olyan $\sigma \in Aut(G)$, hogy $S^\sigma = T$.*

Érdemes a bevezetésben már említett általánosabb esetet nézni, vagyis gráfok helyett tetszőleges relációstruktúrákat vizsgálni.

2.19 DEFINÍCIÓ. *Legyen G egy véges csoport. Egy G alaphalmazú $\Re$ relációstruktúrát G Cayley-objektumának nevezünk, ha $G_R \leq Aut(\Re)$. Egy $\Re$ Cayley-objektumot CI-objektumnak hívunk, ha minden vele izomorf $\Im$ Cayley-objektumhoz létezik egy $\alpha \in Aut(G)$, hogy $\Im = \Re^\alpha$.*

A következő lemma alapvető fontosságú a különféle CI-csoportok vizsgálatában.

2.20 LEMMA. (Babai [4]) *Egy G véges csoport $\Re$ Cayley-objektuma pontosan akkor CI-objektum, ha*

$$\varphi G_R \varphi^{-1} \leq Aut(\Re)\ (\varphi \in Sym(G)) \ \Rightarrow\ \exists \psi \in Aut(\Re):\ \varphi G_R \varphi^{-1} = \psi G_R \psi^{-1}.$$

Bizonyítás. Legyen $\Re$ CI-objektum és $\varphi G_R \varphi^{-1} \leq Aut(\Re)$ valamilyen $\varphi \in Sym(G)$-re $Aut(\Re^\varphi) = \varphi^{-1} Aut(\Re)\varphi \geq G_R$, ezért $\Re^\varphi$ Cayley-objektum és létezik $\alpha \in Aut(G)$, hogy $\Re^\alpha = \Re^\varphi$. $\Re^{\varphi\alpha^{-1}} = \Re$, ezért $\psi := \varphi\alpha^{-1} \in Aut(\Re)$ és $\varphi G_R \varphi^{-1} = \psi\alpha G_R \alpha^{-1}\psi^{-1} = \psi G_R \psi^{-1}$.

Megfordítva, legyen $\Im$ is egy Cayley-objektum, $\varphi \in Sym(G)$ izomorfizmus: $\Im = \Re^\varphi$. $Aut(\Re) = \varphi Aut(\Im)\varphi^{-1} \geq \varphi G_R \varphi^{-1}$, és a feltételből $\exists \psi \in Aut(\Re):\ \varphi G_R \varphi^{-1} = \psi G_R \psi^{-1}$. Legyen $\gamma := \psi^{-1}\varphi$, $g := 1\gamma^{-1}$, $\delta := g_R\gamma$. Ekkor $\gamma^{-1} G_R \gamma = \delta^{-1} G_R \delta = G_R$ és $1\delta = 1$. Ez a δ indukál egy $\alpha \in Aut(G)$ automorfizmust G_R-n: $\delta^{-1} g_R \delta = (g^\alpha)_R = \alpha^{-1} g_R \alpha$. Tehát $\delta\alpha^{-1}$ centralizálja G_R-t $Sym(G)$-ben. Ismert, hogy ez a centralizátor G_L, így $\delta\alpha^{-1} = id_G$, $\alpha = \delta = g_R\gamma = g_R\psi^{-1}\varphi$ és $\varphi = \psi g_R^{-1}\alpha$. Végül $\Im = \Re^\varphi = \Re^{\psi g_R^{-1}\alpha} = \Re^\alpha$. ■

2.21 LEMMA. *Legyen p egy prim, G egy véges p-csoport és tegyük fel, hogy G_R p-Sylow részcsoportja $Aut(\Re)$-nek, G valamely $\Re$ Cayley-objektumára. Ekkor $\Re$ CI-objektum.*

Bizonyítás. $Aut(\Re) \geq \varphi^{-1} G_R \varphi \cong G_R$, ezért következik Sylow II. tételéből és a 2.20 lemmából. ■

2.4. CI-csoportok

2.22 DEFINÍCIÓ. *Egy G véges csoportot globálisan CI-csoportnak hívunk, ha minden Cayley-objektuma CI-objektum, DCI-csoportnak, ha minden irányított Cayley-gráfja CI-gráf, és CI-csoportnak, ha minden irányítatlan Cayley-gráfja CI-gráf.*

2.23 DEFINÍCIÓ. *Egy G véges csoport H részcsoportját pronormálisnak nevezzük, ha $\forall g \in G$-re: $g^{-1}Hg$ és H konjugáltak $\langle H, g^{-1}Hg\rangle$-ben.*

2.24 ÁLLÍTÁS. *Egy G véges csoport pontosan akkor lesz globálisan CI-csoport, ha G_R pronormális részcsoportja $Sym(G)$-nek.*

Bizonyítás. Egy relációstruktúra izomorfizmuscsoportja tetszőleges permutációcsoport lehet, ezért minden $\varphi \in Sym(G)$-re van olyan $\mathfrak{R}$, hogy $Aut(\mathfrak{R}) = \langle G_R, \varphi^{-1} G_R \varphi \rangle$. Viszafelé triviális. ■

2.25 TÉTEL. *Z_p globálisan CI-csoport.*

Bizonyítás. Minden $\delta \in Sym(Z_p)$-re $(Z_p)_R$ és $(Z_p)_R^\delta$ p-Sylow részcsoportok $\langle (Z_p)_R, (Z_p)_R^\delta \rangle$-ben, Sylow II. tétele szerint konjugáltak, azaz $(Z_p)_R$ pronormális, tehát az előző állításból következik a tétel. ■

2.26 ÁLLÍTÁS. *$(D)CI$-csoport minden részcsoportja is $(D)CI$-csoport.*

Bizonyítás. Legyen G egy $(D)CI$-csoport, $H \leq G$, $S, T \subseteq H$ és teljesüljön: $Cay(H, S) \cong Cay(H, T)$. Feltehető, hogy a gráf összefüggő, azaz $\langle S \rangle = \langle T \rangle = H$, mert különben vesszük a komplementert. Láttuk, hogy ekkor $Cay(G, S) \cong Cay(G, T)$, tehát létezik $\alpha \in AutG$, melyre $S^\alpha = T$. Végül $H^\alpha = \langle S^\alpha \rangle = \langle T \rangle = H$, tehát $\alpha|_H \in AutH$. ■

3. fejezet

(D)CI-csoportok

3.1. Ciklikus gráfok

3.1 DEFINÍCIÓ. *Legyenek $0 < k_1 < k_2 < \cdots < k_m < n$ egész számok és képezzük azt a $G_n(k_1, \ldots, k_m)$ irányított gráfot a $P_1, \ldots, P_n$ csúcsok halmazán, ahol P_i-ből P_j-be pontosan akkor vezet él, ha valamely t-re $k_t \equiv j - i \pmod n$. Az ilyen gráfot ciklikus gráfnak nevezzük.*

A ciklikus gráfban a csúcsok $P_i \mapsto P_{i+k}$ permutációi (ahol az indexeket modulo n kell tekinteni, valamint $k = 0, \ldots, n-1$) mind automorfizmusai a gráfnak. Két ilyen gráf, $G_n(k_1, \ldots, k_m)$ és $G_n(k'_1, \ldots, k'_m)$ izomorfiájához elegséges feltétel egy olyan r szám valamint az $1, \ldots, m$ halmaz egy α permutációjának létezése, amelyekre $0 < r < n$, r relatív prím n-hez és $k'_t \equiv rk_{\alpha(t)} \pmod n$ minden t-re ($1 \leq t \leq m$). Ádám András [1] azt sejtette, hogy ez a feltétel szükséges is, az az minden ciklikus csoport DCI-csoport.

Foglalkozzunk először az irányítatlan esetettel. Néhány kis szám kivételével valamennyi négyzetszámra adott ellenpéldát Babai László és Frankl Péter [5]:

3.2 LEMMA. *Z_{n^2} nem CI-csoport, ha $n = 5$ vagy $n \geq 7$.*

Bizonyítás. Mivel $n \geq 5$ és $n \neq 6$, ezért $\varphi(n) > 2$, ahol φ az Euler függvény. Igy létezik egy n-hez relatív prim s, hogy $2 \leq s \leq n-2$. Tekintsük Z_{n^2} következő részhalmazait:

$$A = \{n, -n\}; \quad B = \{kn+1, kn-1 : k = 0, \ldots, n-1\}$$

$$H = A \cup B; \quad K = sA \cup B = \{sn, -sn\} \cup B$$

Világos, hogy minden $S \subseteq Z_n,\ S = -S$ esetén $Cay(Z_{n^2}, nS \cup B) \cong C_n[Cay(Z_n, S)]$, ahol C_n egy n hosszú irányítatlan kör. A mi esetünkben

$$Cay(Z_n, \{1, -1\}) \cong Cay(Z_n, \{s, -s\}) \cong C_n$$

tehát

$$Cay(Z_{n^2}, H) \cong Cay(Z_{n^2}, K) \cong C_n[C_n]$$

Ezzel szemben nem létezik olyan d, hogy $dH = K$, $(d, n^2) = 1$. Ebből ugyanis $dA = sA$, $dB = B$ $(mod\ n^2)$, majd $d \equiv \pm s\ mod\ n$ következne, ami ellentmond annak, hogy B minden eleme kongruens ± 1 $(mod\ n)$. ∎

Később Pálfy Péter Pál [23] újabb eseteket zárt ki.

3.3 LEMMA. *Z_{8m} nem CI-csoport, ha $m > 1$.*

Bizonyítás. Legyenek $T_1 = \{\pm 2, \pm(2m+1), \pm(2m-1)\}$ és $T_2 = \{\pm 2, \pm 1, \pm(4m-1)\}$ a csatlakozó halmazok. Könnyen látható, hogy az

$$x \mapsto \begin{cases} x, & \text{ha } x \text{ páros} \\ x + 2m, & \text{ha } x \text{ páratlan} \end{cases}$$

permutáció egy gráfizomorfizmus $Cay(Z_{8m}, T_1)$ és $Cay(Z_{8m}, T_2)$ között, de nincs olyan k, melyre $(k, 8m) = 1$ és az $x \mapsto kx$ csoportautomorfizmus T_1-et T_2-be vinné. ∎

3.4 LEMMA. *Z_{9m} nem CI-csoport, ha $m > 2$.*

Bizonyítás. Tekintsük a $T_i = \{\pm 1, \pm(3m+1), \pm(6m+1), \pm 3(im+1)\}, i = 0, 1, 2$ csatlakozó halmazokkal megadott Cayley-gráfokat és a következő $\varphi(i)$ permutációkat:

$$x \mapsto \begin{cases} (im+1)x, & \text{ha } x \equiv 0(mod\ 3) \\ (im+1)x - im, & \text{ha } x \equiv 1(mod\ 3) \\ (im+1)x - 2im, & \text{ha } x \equiv 2(mod\ 3) \end{cases}$$

Ha $im+1$ nem osztható 3-mal, akkor $\varphi(i)$ izomorfizmus $Cay(Z_{9m}, T_0)$-ból $Cay(Z_{9m}, T_i)$-be. Ha $kT_0 = T_i$, akkor $k = \pm(3jm+1)$, $0 \le j \le 2$, és $\pm 3(im+1) = k(\pm 3) = \pm 3(3jm+1) = \pm 3$. Ha $3(im+1) = 3$, akkor $i = 0$. Ha pedig $3(im+1) = -3$, akkor $3im \equiv -6(mod\ 9m)$, $3m$ osztja a 6-ot, ami $m > 2$ miatt lehetetlen. Mivel $m+1$, vagy $2m+1$ nem osztható 3-mal, ezért $Cay(Z_{9m}, T_0)$ és $Cay(Z_{9m}, T_i)$ $(i = 1$ vagy $2)$ szolgáltatják a szükséges ellenpéldát. ∎

3.5 TÉTEL. *Ha Z_n CI-csoport, akkor*

$$n \in \{8, 9, 18\} \text{ vagy } n = k, 2k \text{ vagy } 4k,$$

ahol k páratlan négyzetmentes szám.

Bizonyítás. Legyen $G = Z_n$ CI-csoport. A 2.26 állítás szerint CI-csoport minden részcsoportja CI, ezért az előző három lemmából következik, hogy G p-Sylow részcsoportja csak Z_p, Z_4, Z_8 vagy Z_9 lehet.Ha az utóbbi két eset valamelyike fennáll, akkor az utolsó két lemmából $n = 8, 9$ vagy 18. Ha nem, akkor $n = k, 2k$ vagy $4k$, ahol k páratlan négyzetmentes szám. ∎

Irányított gráfokkal az $n = 8, 9, 18$ esetekben is adható ellenpélda. Már a vizsgálatok legelején B. Elspas és J. Turner [3] megmutatták, hogy 8 csúcsra az a két ciklikus gráf, amelyre P_8 szomszédai P_1, P_2 és P_5, illetve amelyikre P_1, P_5 és P_6 egymással izomorfak (egy izomorfizmus például a $P_{2i} \to P_{10-2i}$, $P_{2i-1} \to P_{9-2i}$ $(i = 1, 2, 3, 4)$ leképezés), de nincs olyan r, amellyel $r\{1, 2, 5\} \equiv \{1, 5, 6\} \pmod 8$. Az irányított esetben tehát a következő adódik.

3.6 TÉTEL. *Ha Z_n DCI-csoport, akkor*

$$n = k, 2k \textit{ vagy } 4k,$$

ahol k páratlan négyzetmentes szám.

3.2. Általános eset

Babai László és Frankl Péter [5] vették észre a CI csoportok alábbi fontos tulajdonságát.

3.7 LEMMA. *Legyen G egy véges $(D)CI$-csoport,*

$$U_1 \leq \cdots \leq U_n = G\ ,\ V_1 \leq \cdots \leq V_n = G\ ,\ |U_i| = |V_i| \quad (i = 1, \ldots n).$$

Ekkor létezik $\alpha \in Aut(G)$, hogy

$$\alpha(U_i) = (V_i) \ \ (i = 1, \ldots n).$$

Bizonyítás. Legyenek $S_0 = T_0 = U_0 = T_0 = \{0\}$,

$$n_i := |U_i/U_{i-1}| = |V_i/V_{i-1}|,\ \ S_i := U_i \setminus S_{i-1},\ \ T_i := V_i \setminus T_{i-1} \ \ (i = 1, \ldots, n)$$

Ekkor $Cay(U_1, S_1) \cong Cay(V_1, T_1) \cong K_{n_1}$, $Cay(U_{i+1}, S_{i+1})$ izomorf $Cay(U_i, S_i)$ komplementerének n_{i+1} darab példányával és ugyanez elmondható U és S helyett V-vel és T-vel. Ezért $Cay(U_i, S_i) \cong Cay(V_i, T_i)$ $(i = 1, \ldots, n)$, $Cay(G, S_n) \cong Cay(G, T_n)$ G egy $(D)CI$-csoport, így létezik $\alpha \in Aut(G)$, hogy $S_n^\alpha = T_n$. Tegyük fel, hogy $S_{n-k}^\alpha = T_{n-k}$ valamilyen $0 \leq k \leq n-1$. Ekkor $U_{n-k}^\alpha = \langle S_{n-k}^\alpha \rangle = \langle T_{n-k}^\alpha \rangle = V_{n-k}$ és $S_{n-k-1}^\alpha = (U_{n-k} \setminus S_{n-k} \setminus \{0\})^\alpha =$ $= (V_{n-k} \setminus T_{n-k} \setminus \{0\}) = T_{n-k-1}$. Teljes indukcióval $\alpha(U_i) = (V_i)$ $(i = 1, \ldots n)$. ■

3.8 DEFINÍCIÓ. *Legyen M egy Abel csoport, melynek minden Sylow részcsoportja elemi Abel, $n \in \{2, 3, 4, 8, 9\}$ pedig olyan, hogy $(|M|, n) = 1$. Ekkor*

$$E(M, n) := M\langle z \rangle, \textit{ ahol } o(z) = n \textit{ és minden } x \in M\textit{-re}:$$

$$x^z := \begin{cases} x^{-1}, & \textit{ha } n = 2, 4 \textit{ vagy } 8 \\ x^l, & \textit{ha } n = 3 \textit{ vagy } 9, \textit{ és itt } l^3 \equiv 1 \pmod{exp(M)},\ (l(l-1), exp(M)) = 1 \end{cases}$$

Cai Heng Li és Pálfy Péter Pál készülő cikkéből kiderül, hogy jelenleg mely csoportok lehetnek CI-csoportok:

3.9 TÉTEL. *Legyen G egy véges CI-csoport.*

(a) Ha G nem tartalmaz 8- vagy 9-rendű elemet, akkor $G = H_1 \times H_2 \times H_3$, ahol a tényezők rendjei páronként relatív primek és

H_1 Abel és minden Sylow részcsoportja elemi Abel vagy Z_4;
H_2 a következő csoportok valamelyike: $E(M,2)$, $E(M,4)$, Q vagy 1;
H_3 pedig a következőké: $E(M,3)$, A_4 vagy 1.

(b) Ha G tartalmaz 8-rendű elemet, akkor $G \cong E(M,8)$ vagy Z_8.

(c) Ha G tartalmaz 9-rendű elemet, akkor G egy a következő csoportok közül: $Z_9 \rtimes Z_2$, $Z_9 \rtimes Z_4$, $Z_2^2 \rtimes Z_9$, vagy $Z_9 \times Z_2^n$, ahol $n \leq 5$.

Li, Praeger és Xu [14] pedig az irányított esetben adták meg a legjobb eredményt:

3.10 TÉTEL. *Legyen G egy véges DCI-csoport.*
Ekkor G minden Sylow részcsoportja elemi Abel, Z_4 vagy Q, valamint $G = U \times V$, ahol $(|U|,|V|) = 1$, U Abel és $V = 1$, Q, A_4, $E(M,2)$ vagy $E(M,2)$.

4. fejezet

Az elemi Abel csoportok esete

4.1. G-invariáns partíciók

Az alábbiakban mindig

$$G = Z_p^n \text{ és } \Gamma = Cay(Z_p^n, S)$$

4.1 LEMMA. *Legyen $G_R^\delta \leq Aut\Gamma$ $(\delta \in Sym(G))$. Ekkor léteznek $P \in Syl_P(Aut\Gamma)$ és $\gamma \in Aut\Gamma$, hogy*

$$\langle G_R, G_R^{\gamma\delta} \rangle \leq P$$

Bizonyítás. A Sylow tételek miatt nyilvánvaló. ■

Ismét a Sylow tételeket alkalmazva $P \leq P^* \in Syl_P(Sym(G))$, ahol $P^* \cong \underbrace{Z_p \wr Z_p \wr \cdots \wr Z_p}_{n}$ meghatároz P^*-invariáns partíciók egy $\mathbf{B} = \{\mathbf{B}_i | i = 1, \ldots, n+1\}$ rendszerét:

$$\mathbf{B}_i = \{(B_i)p : p \in P^*\},\ \{0\} = B_1 < \cdots < B_n < B_{n+1} = G, \text{ és } \mathbf{B}_i\ M_i\text{-partíció.}$$

$$B_{i+1} = \langle g_1, \ldots, g_i \rangle,\ \tau_i := (g_i)_R,\ T_i := \langle \tau_1 \rangle \wr \cdots \wr \langle \tau_i \rangle \wr Sym(\mathbf{B}_{i+1}) \leq M_{i+1},\ T_n = P^*.$$

$$G_R \leq P \leq P^* \Rightarrow \mathbf{B}_i = \{(B_i)p : p \in P\} = \{(B_i)\tau : \tau \in \langle \tau_i, \ldots \tau_n \rangle\}$$

4.2 DEFINÍCIÓ. *Minden $1 \leq i \leq n$-re jelölje ι_i a következő $M_i \rightarrow Sym(\mathbf{B}_i)$ homomorfizmust:*

$$(g + B_i)(\iota_i(m)) = (g + B_i)m \quad (g \in G, m \in M_i)$$

Ekkor $\iota_i(P^*) \in Syl_P(Sym(\mathbf{B}_i))$ a $\{\mathbf{B}_j | j = i, \ldots, n\}$ rendszert határozza meg, ezért

$$\iota_i((B_{i+1})_R) = Z(\iota_i(P^*)) \leq Z(\iota_i(P)).$$

4.3 LEMMA. *Legyen* $\langle G_R,\ G_R^\delta\rangle \le P \in Syl_p(Aut\Gamma)$ $(\delta \in Sym(G))$. *Ekkor minden* $1 \le i \le n$*-re létezik* $\upsilon_i \in G_R^\delta$*, hogy*

$$\iota_i(\tau_i) = \iota_i(\upsilon_i),\ \textit{speciálisan}\ \tau_1 = \upsilon_1.$$

Bizonyítás. Az előzőek szerint $\iota_i(\tau_i) \in Z(\iota_i(P))$, $\iota_i(G_R^\delta)$ tranzitív és Abel, következésképp $\langle\iota_i(\tau_i), \iota_i(G_R^\delta)\rangle$ is tranzitív és Abel. Tehát mindkettő reguláris, igy $\iota_i(\tau_i) \in \iota_i(G_R^\delta)$. Végül $\mathbf{B}_1 = G$ miatt $\iota_1 = id_P$. ■

4.4 KÖVETKEZMÉNY. Z_p *DCI-csoport*

Bizonyítás. Legyen $\Gamma = Cay(Z_p, S)$ és $(Z_p)_R^\delta \le Aut\Gamma$. Az előző két lemma szerint $\tau_1 = \upsilon_1$, $(Z_p)_R = (Z_p)_R^{\gamma\delta}$ $(\gamma \in Aut\Gamma)$, a Babai lemmából pedig Γ CI-gráf. ■

4.5 KÖVETKEZMÉNY. *Legyen* $\langle G_R,\ G_R^\delta\rangle \le P \in Syl_p(Aut\Gamma)$ $(\delta \in Sym(G))$. *Ekkor létezik* $\alpha \in Aut(G)$*, hogy* $\delta\alpha \in P^*$.

Bizonyítás. Teljes indukcióval belátjuk, hogy léteznek $\alpha_1, \dots, \alpha_n \in Aut(G)$, hogy minden $1 \le i \le n$-re $\delta\alpha_1 \dots \alpha_i \in T_i$. A lemma szerinti $\upsilon_1 \in G_R^\delta$-hez létezik $w_1 \in G$ és $\alpha_1 \in Aut(G)$, hogy $\delta(w_1)_R\delta^{-1} = \upsilon_1$ és $(w_1)\alpha_1 = g_1$. Legyen $\delta_1 := \delta\alpha_1$.

$$\delta_1(g_1)_R\delta_1^{-1} = \delta\alpha_1(g_1)_R\alpha_1^{-1}\delta^{-1} = \delta(w_1)_R\delta^{-1} = \upsilon_1 = \tau_1 = (g_1)_R$$

$$\big(\delta_1^{-1}(0)\ \ \delta_1^{-1}(g_1)\ \dots\ \delta_1^{-1}((p-1)g_1)\big)\dots = \big(0\ g_1\ \dots\ (p-1)g_1\big)\dots$$

Ebből $\delta_1 \in T_1$, tehát $i = 1$-re igaz.
Most tegyük fel, hogy minden $1 \le i \le k(< n))$-re már találtunk megfelelő α_i-t, és a $\delta_i := \delta\alpha_1 \dots \alpha_i$ jelöléssel $\delta_i \in T_i \le M_{i+1}$. Mivel $(B_{k+1})_R \le ker(\iota_{k+1}) \lhd M_{i+1}$, $\upsilon_{k+1} \notin ker(\iota_{k+1})$, ezért $w \in (B_{k+1})$ esetén $\iota_{k+1}(\delta_k w_R \delta_k^{-1}) \ne \iota_{k+1}(\upsilon_{k+1})$, tehát léteznek $w_{k+1} \in G \setminus B_{k+1}$ és $\alpha_{k+1} \in Aut(G)$:

$$\delta_k(w_{k+1})_R\delta_k^{-1} = \upsilon_{k+1},\ (w_{k+1})\alpha_{k+1} = g_{k+1},\ (g_i)\alpha_{k+1} = g_i\ \ (i = 1, \dots, k).$$

Innen $\delta_{k+1} := \delta_k\alpha_{k+1} \in M_{k+1}$ és

$$\iota_{k+1}(\delta_{k+1})\iota_{k+1}((g_{k+1})_R)\iota_{k+1}(\delta_{k+1}^{-1}) = \iota_{k+1}(\delta_{k+1}g_{k+1}\delta_{k+1}^{-1}) = \iota_{k+1}(\delta_k w_{k+1}\delta_k^{-1}) =$$

$$= \iota_{k+1}(\upsilon_{k+1}) = \iota_{k+1}(\tau_{k+1}) = \iota_{k+1}((g_{k+1})_R)$$

$$\Big(\iota_{k+1}(\delta_{k+1})^{-1}\Big(B_{k+1}\Big)\ \ \iota_{k+1}(\delta_{k+1})^{-1}\Big(g_{k+1} + B_{k+1}\Big)\ \dots$$

$$\ldots\ \iota_{k+1}(\delta_{k+1})^{-1}\Big((p-1)g_{k+1}+B_{k+1}\Big)\Big)\ldots$$

$$=\Bigg(B_{k+1}\ \ \Big(g_{k+1}+B_{k+1}\Big)\ \ldots\ \Big((p-1)g_{k+1}+B_{k+1}\Big)\Bigg)\ldots$$

azaz $\iota_{k+1}(\delta_{k+1}) \in \iota_{k+1}(T_{k+1}) = \iota_{k+1}\big(\langle\tau_{k+1}\rangle\big) \wr Sym(\mathbf{B}_{k+2})$. Viszont $\delta_{k+1} = \delta_k\alpha_{k+1} \in T_k$, ezért $\delta_{k+1} \in T_{k+1}$, és ezzel minden $1 \leq i \leq n$-re beláttuk, hogy $\delta_i \in T_i$. Az $\alpha := \alpha_1 \ldots \alpha_n$ jelöléssel pedig kapjuk:

$$\delta\alpha = \delta_n \in T_n = P^*.$$

■

4.6 ÁLLÍTÁS. *Legyen* $G_R^\delta \leq Aut\Gamma$ $(\delta \in Sym(G))$. *Ekkor*

(1) léteznek $\gamma \in Aut\Gamma$ *és* $\alpha \in Aut(G)$, *hogy a* $\delta' := \gamma\delta\alpha$ *jelöléssel*

$$\langle G_R,\ G_R^{\delta'}\rangle \leq P \leq P^*,\ \text{és}\ G_R^{\delta'} = G_R^{\gamma\delta}$$

ahol $P \in Syl_p(Aut\Gamma)$ *és* $\delta' \in P^* \in Syl_p(Sym(G))$, *valamint*

(2) minden $1 \leq i \leq n$*-re létezik* $\upsilon_i \in G_R^{\delta'}$, *hogy*

$$\tau_1 = \upsilon_1,\ \iota_i(\tau_i) = \iota_i(\upsilon_i),\ \text{és}\ (B_{i+1})_R^{\delta'} = \langle\upsilon_1, \ldots \upsilon_i\rangle$$

Bizonyítás. Az eddigieket felhasználva csak (2) második fele szorul bizonyításra. Mivel $N_i := ker\iota_{i+1} \cap P^* \lhd P^*$, $\delta' \in P^*$, és $(B_{i+1})_R = G_R \cap N_i$, ezért $(B_{i+1})_R^{\delta'} = G_R^{\delta'} \cap N_i$. Végül minden $j \leq i$-re $\iota_j(\upsilon_j) = \iota_j(\tau_j)$ és $\tau_j \in N_j \setminus N_{j-1}$ miatt $\upsilon_j\tau_j^{-1} \in N_{j-1} \leq N_j$ és $\upsilon_j \in N_j \setminus N_{j-1}$. Tehát $G_R^{\delta'} \cap N_i = \langle\upsilon_1, \ldots \upsilon_i\rangle$ és kész. ■

4.2. Koszorú reláció

A $\mathbf{B}_i$ partíció elemei között értelmezhető a következő, *koszorú reláció*:

$$B_i + a_1 \sim B_i + a_2 \iff \big\{(b'' + a_t) - (b' + a_l) \in S \Rightarrow (B_i + a_t) - (b' + a_l) \subseteq S\ \big\}$$

Ennek segítségével kapjuk az *i-dik Cayley segédgráfot*:

$$\Gamma_i = (\mathbf{B}_i, E),\ E := \{(B_i + x, B_i + y) | B_i + x \not\sim B_i + y\},\ \overline{\Gamma_i} = \Gamma \text{ komplementergráfja}$$

Nyílván $B_i + x \sim B_i + y$ pontosan azt jelenti, hogy

$$\{y - x + B_i \in S \text{ vagy } y - x + B_i \in G \setminus S\} \text{ és } \{x - y + B_i \in S \text{ vagy } x - y + B_i \in G \setminus S\}$$

Az elöbbiek tömör általánosítása a következő

4.7 DEFINÍCIÓ. *Legyenek* $H \subseteq G$, $\Xi_H : G \longrightarrow Z_2$ *és* $S : \mathcal{P}(G) \longrightarrow \mathcal{P}(G)$ *:*

$$\Xi_H(g) := \begin{cases} 1, & \text{ha } g + H \subseteq S \text{ vagy } g + H \subseteq G \setminus S \\ 0, & \text{különben} \end{cases}$$

$$S(H) := \{g \in G | \Xi_H(g) = 0 \text{ vagy } \Xi_H(g^{-1}) = 0\}, \ S_i := S(B_i) \ (i = 1, \dots, n)$$

$$\overline{S(H)} := G \setminus S(H) = \{g \in G | \Xi_H(g) = \Xi_H(g^{-1}) = 1\}.$$

$H_1 \subseteq H_2$ esetén $S(H_1) \subseteq S(H_2)$, tehát

$$\emptyset = S_1 \subseteq S_2 \subseteq \dots \subseteq S_n \quad \text{és} \quad G = \overline{S_1} \supseteq \overline{S_2} \supseteq \dots \supseteq \overline{S_n}$$

Ezzel $B_i + x \sim B_i + y$ pontosan azt jelenti, hogy $y - x \in S_i$, továbbá $\Gamma_i = (\mathbf{B}_i, S_i + B_i)$ és $\overline{\Gamma_i} = (\mathbf{B}_i, \overline{S_i} + B_i)$.

4.8 LEMMA. *Legyenek* $H_1, H_2 \subseteq H \subseteq G$, *ahol* $H + H_1 = H + H_2 = H$. *Ekkor*

$$g + H \subseteq \overline{S(H_1)} \cap \overline{S(H_2)} \Rightarrow g + H \subseteq \overline{S(H_1 + H_2)}.$$

Bizonyítás. Tegyük fel, hogy $g + h + h_1 + h_2 \in S$ $(g \in G, h \in H, h_1 \in H_1, h_2 \in H_2)$. Mivel $h + h_1 \in H$, $\Xi_{H_2}(g + h + h_1) = 1$, ezért $g + h + h_1 + h_2' \in S$ minden $h_2' \in H_2$-re. Tovább $h + h_2' \in H$, $\Xi_{H_1}(g + h + h_2') = 1$, tehát $g + h + h_1' + h_2' \in S$ minden $h_1' \in H_1$ és $h_2' \in H_2$-re. Másszóval $\Xi_{H_1+H_2}(g + h) = 1$. Hasonlóan $\Xi_{H_1+H_2}(-g - h) = 1$, vagyis $g + h \in \overline{S(H_1 + H_2)}$ minden $h \in H$-ra. ■

4.3. Cayley segédgráfok

4.9 DEFINÍCIÓ. *Legyen* $H \leq G$. *Ekkor* $Cay(G/H, S(H) + H)$*-t nevezzük a* $Cay(G, S)$ *Cayley gráf* H *szerinti Cayley segédgráfjának és jelöljük* $\Gamma(H)$*-val, a komplementerét pedig* $\overline{\Gamma(H)}$*-sal.*

Tegyük fel, hogy $\tau_i = \upsilon_i$, $(i = 1, \dots, k - 1 (< n))$, legyenek $\upsilon \in G_R^\delta$ és $a \in G$ képe a $G \to G/B_k$ természetes homomorfizmusnál $\overline{a}$. Ekkor minden $b \in B_k$-ra $[b_R, \upsilon] = [b_R, \tau] = 1$,

$$(a + b)\upsilon - (a + b)\tau = (a)\upsilon + b - ((a)\tau + b) = (a)\upsilon - (a)\tau \quad (\tau \in G_R).$$

4.10 DEFINÍCIÓ. $(\overline{a}, \upsilon, \tau) := (a)\upsilon - (a)\tau$

4.11 Megjegyzés. $(a + b)\upsilon\tau^{-1} = ((a + b)\tau + (a, \upsilon))\tau^{-1} = a + b + (\overline{a}, \upsilon, \tau)$

$$(a + b)\upsilon = (a)\tau + b + (\overline{a}, \upsilon, \tau)$$

$$(\overline{a}, \upsilon'\upsilon'', \tau'\tau'') = (a)\upsilon'\upsilon'' - (a)\tau'\tau'' = ((a)\tau' + (\overline{a}, \upsilon', \tau'))\upsilon'' - (a)\tau'\tau'' =$$

$$= (\overline{a}, \upsilon', \tau') + ((\overline{a})(\iota_k(\tau')), \upsilon'', \tau'').$$

4.12 LEMMA. *Legyen* $g := y - x$, *valamint* $(\overline{x}, \upsilon, \tau)$, $(\overline{y}, \upsilon, \tau) \in B_k$. *Ekkor*

$$g + B_k \subseteq \overline{S(\langle g^{**} \rangle)}, \text{ ahol } g^{**} := (\overline{y}, \upsilon, \tau) - (\overline{x}, \upsilon, \tau) \in B_k.$$

Bizonyítás. Ha $g^{**} = 0$, akkor $\overline{S(0)} = G$ miatt trivialitás. Legyen $b \in B_k$ tetszőleges, $g^{**} \neq 0$ és tegyük fel, hogy $g + b + rg^{**} \in S$ valamilyen $r \in \mathbf{F}_p$-vel. Ekkor minden $r' \in \mathbf{F}_p$-re

$$(y + b + rg^{**})(\upsilon\tau^{-1})^{r'} - (x)(\upsilon\tau^{-1})^{r'} = y + b + rg^{**} + r'(\overline{y}, \upsilon, \tau) - x - r'(\overline{x}, \upsilon, \tau) =$$

$$= g + b + (r + r')g^{**} \in S.$$

Ebből $\Xi_{\langle g^{**} \rangle}(g + b) = 1$ és ugyan így $\Xi_{\langle g^{**} \rangle}(-g - b) = 1$, azaz $(g + b) \in \overline{S(\langle g^{**} \rangle)}$. ∎

4.13 LEMMA. *Legyenek* $\{(\overline{x}, \phi_i, \varphi_i),\ (\overline{y_i}, \phi_i, \varphi_i),\ y_i - (x)\phi_j \mid i, j \in \{1, 2\},\ i \neq j\} \subseteq B_k$, $h_i =: y_i - x$ *és* $h_i^{**} := (\overline{y_i}, \phi_i, \varphi_i) - (\overline{x}, \phi_i, \varphi_i) \in B_k$. *Ekkor*

$$h_i + B_k \subseteq \overline{S(\langle h_j^{**} \rangle)}.$$

Bizonyítás. Először $(\overline{x}, \phi_1\phi_2, \varphi_1\varphi_2) = (\overline{x}, \phi_2\phi_1, \varphi_2\varphi_1)$, így

$$(\overline{x}, \phi_1, \varphi_1) + ((\overline{x})(\iota_k(\varphi_1)), \phi_2, \varphi_2) = (\overline{x}, \phi_2, \varphi_2) + ((\overline{x})(\iota_k(\varphi_2)), \phi_1, \varphi_1).$$

$$(\overline{x})(\iota_k(\varphi_i)) = (\overline{x})(\iota_k(\phi_i)) = \overline{y_j}. \quad (i, j \in \{1, 2\},\ i \neq j)$$

$$h_1^{**} := (\overline{y_1}, \phi_1, \varphi_1) - (\overline{x}, \phi_1, \varphi_1) = (\overline{y_2}, \phi_2, \varphi_2) - (\overline{x}, \phi_2, \varphi_2) = h_2^{**},$$

majd a 4.12 lemmát alkalmazva

$$h_i + B_k \subseteq \overline{S(\langle h_i^{**} \rangle)} = \overline{S(\langle h_j^{**} \rangle)}$$

∎

4.14 DEFINÍCIÓ. *Legyenek*

$$a^* := (\overline{a}, \upsilon_k, \tau_k), \text{ és } B_k(g) := \langle y^* - x^* \mid y - x = g \rangle \quad (a, g \in G).$$

vagy, ha félreértésre nem ad okot, $B(g) := B_k(g)$.

4.15 LEMMA. $B(rg + th) \leq B(g) + B(h)$, $B(rg) = B(g)$ $(r, t = 1, \ldots, p - 1)$

Bizonyítás. $y^* - x^* \in B(g+h),\ y - x = g + h,$

$$y^* - x^* = ((g+h+x)^* - (h+x)^*) + ((h+x)^* - x^*) \in B(g) + B(h),$$

$$B(rg) \leq rB(g) = B(g),\ B(g) = B(r'rg) \leq r'B(rg) = B(rg) \quad (r = 1, \ldots, p-1),$$

$$B(rg + th) \leq B(rg) + B(th) = B(g) + B(h)$$

■

4.16 LEMMA. $rg + B_k \subseteq \overline{S(B(g))}, \quad (r = 1, \ldots, p-1)$

Bizonyítás. Legyen $g = y - x$. Ekkor $x^*, y^* \in B_k$, és a 4.12 lemmából $g + B_k \subseteq \overline{S(\langle y^* - x^* \rangle}$. Tehát

$$g + B_k \subseteq \bigcap_{y-x=g} \overline{S(\langle y^* - x^* \rangle)}$$

majd a 4.8 lemmából

$$g + B_k \subseteq \overline{S(\sum_{y-x=g} \langle y^* - x^* \rangle)} = \overline{S((B(g))}.$$

Ezt g helyett rg-vel is mondhatjuk, $B(rg) = B(g)$ és készen vagyunk. ■

4.4. A segédgráfok módszere

A segédgráfok módszere abból áll, hogy ha a bizonyítás során olyan esetbe ütközünk, amelyet nem tudunk megoldani, mert túl bonyolult vagy túl sok alesetre bomlana szét, akkor alkalmasan választott segédgráfok segítségével vagy megmutatjuk, hogy ez igazából olyan eset amelyet már elintéztünk, vagy az aleseteket ügyesen partícionálva, az egyes osztályokat visszavezetjük már megoldott esetekre.

4.17 DEFINÍCIÓ. *Legyen $(\cdot,\cdot) : G \times G \to \mathbf{F}_p$ szimmetrikus bilineáris függvény, melyre $(g_k, g_k) = 1$ és $(g_k, g_j) = 0$, ha $j < k$. Ekkor $\pi_k \in Sym(G)$ legyen a következő:*

$$(x)\pi_k := (x)\tau_k^{-(x,g_k)} \upsilon_k^{(x,g_k)} \quad (x \in G)$$

4.18 LEMMA.

(1) $\upsilon_k^{\pi_k} = \tau_k, \quad \pi_k \in C_{Sym(G)}((B_k)_R)$

(2) $y - x \in g_k^\perp \cap S \Rightarrow (y)\pi_k - (x)\pi_k \in S$

(3) $(y)\pi_k - (x)\pi_k = y - x + \sum_{i=1}^{(y,g)}(y-ig)^* - \sum_{i=1}^{(x,g)}(x-ig)^* \in y - x + B_k \quad (x,y \in G)$

(4) $y - x \in S \cap \overline{S_k} \Rightarrow (y)\pi_k - (x)\pi_k \in S$

Bizonyítás.

(1) Mivel $(x, g_k) + 1 = (x + g_k, g_k)$, így minden $x \in G$-re

$$(x)\pi_k \upsilon_k \pi_k^{-1} = (x)\tau_k^{-(x,g_k)} \upsilon_k^{(x,g_k)} \upsilon_k \pi_k^{-1} = (x)\tau_k \tau_k^{-((x,g_k)+1)} \upsilon_k^{(x,g_k)+1} \pi_k^{-1} =$$

$$= (x + g_k)\tau_k^{-(x+g_k,g_k)} \upsilon_k^{(x+g_k,g_k)} \pi_k^{-1} = (x + g_k)\pi_k \pi_k^{-1} = (x)\tau_k,$$

minden $b \in B_k$-ra $[b_R, \upsilon] = [b_R, \tau] = 1$ és $(x + b, g_k) = (x, g_k)$, ezért minden $x, y \in G$-re $(x)b_R\pi_k = (x+b)\tau_k^{-(x+b,g_k)}\upsilon_k^{(x+b,g_k)} = (x)b_R\tau_k^{-(x,g_k)}\upsilon_k^{(x,g_k)} = (x)\tau_k^{-(x,g_k)}\upsilon_k^{(x,g_k)}b_R = (x)\pi_k b_R$

(2) $y - x \in S,\ (x, g_k) = (y, g_k) =: i$, így $(y)\pi - (x)\pi = (y)\tau_k^i\upsilon_k^i - (x)\tau_k^i\upsilon_k^i \in S$

(3)

$$(y)\pi_k - (x)\pi_k = (y)\tau_k^{-(y,g)}\upsilon_k^{(y,g)} - (x)\tau_k^{-(x,g)}\upsilon_k^{(x,g)} =$$

$$= (y - (y,g)g_k)((\upsilon_k\tau_k^{-1})\tau)^{(y,g)} - (x - (x,g)g_k)((\upsilon_k\tau_k^{-1})\tau)^{(x,g)} =$$

$$= y - x + \sum_{i=1}^{(y,g)}(y-ig)^* - \sum_{i=1}^{(x,g)}(x-ig)^* \in y - x + B_k.$$

(4) $\overline{S_k}$ definíciójából és az előző pontból

$$(y)\pi_k - (x)\pi_k \in y - x + B_k \subseteq S$$

■

4.19 LEMMA. *Tegyük fel, hogy $g_k \notin \langle S_k \rangle < G$. Ekkor alkalmas $(\cdot,\cdot)$-el $\pi_k \in Aut(\Gamma)$.*

Bizonyítás. Válasszuk $(\cdot,\cdot)$-t úgy, hogy $g_k \in S_k^\perp$ is teljesüljön. Ha $y - x \notin g_k^\perp$, akkor $y - x \notin S_k$ vagyis $y - x \in \overline{S_k}$. Tehát az előző lemma szerint $y - x \in S$ $(x, y \in G)$ esetén $(y)\pi_k - (x)\pi_k \in S$. ■

4.20 KÖVETKEZMÉNY. *Z_p^2 DCI-csoport*

Bizonyítás. Legyen $G = Z_p^2$, $\Gamma = Cay(G,S)$ és $G_R^\delta \leq Aut\Gamma$. A 4.1 és 4.3 lemmák szerint $\upsilon_1 = \tau_1 \in G_R$. Ha $B(g_2) = \{0\}$, akkor minden $x \in G$-re $x^* =: b \in B_2$, $(x)\upsilon_2\tau_2^{-1} = (x)b_R$, és $\upsilon_2 = \tau_2 b_R \in G_R$. Ha $B(g_2) \neq \{0\}$, akkor $B(g_2) = B_2$, a 4.16 lemmából $rg_2 + B_2 \subseteq \overline{S_2}$ $(r = 1, \ldots, p-1)$, ebből $g_2 \notin \langle S_2 \rangle$, és az előző két lemmából $\pi_2 \in C_{Aut(\Gamma)}(\tau_1)$, $\upsilon_2^{\pi_2} = \tau_2$. Végül a Babai lemmát alkalmazva Γ CI-gráf. ∎

4.21 LEMMA. *Legyenek $G = Z_p^2$, $\Gamma = Cay(G,S)$, $\langle G_R, G_R^\delta \rangle \leq P \in Syl_p(Aut\Gamma)$. Ekkor*

$$G_R = G_R^\delta \;\; \text{vagy} \;\; rg_2 \in \overline{S_2} \;\; (r = 1, \ldots, p-1)$$

Bizonyítás. Az iménti következmény bizonyításából nyilvánvaló. ∎

4.22 DEFINÍCIÓ. *Legyen $B_{k+1} \leq H \leq G$.*

$$B_k(H) := \sum_{h \in H} B_k(h)$$

4.23 LEMMA. $rg_k + B_k \subseteq \overline{S(B_k(H))}$.

Bizonyítás. Legyen $y - x = h \in H \setminus B_{k+1}$. A regularitás miatt léteznek $\tau \in G_R$ és $\upsilon \in G_R^\delta$, hogy $(\overline{x})\iota_k(\upsilon) = (\overline{x})\iota_k(\tau) = \overline{y}$. A 4.13 lemma feltételei az $y_1 = y$, $y_2 = x + g_k$, $\phi_1 = \upsilon_k$, $\phi_2 = \upsilon$ szereposztás mellett definíció szerint teljesülnek, tehát

$$g_k + B_k \subseteq \overline{S(\langle y^* - x^* \rangle)}.$$

Ha $y - x \in B_{k+1}$, akkor ugyanez a 4.16 lemmából következik, tehát a 4.8 lemmát kétszer alkalmazva

$$g_k + B_k \subseteq \overline{S(\sum_{y-x=h} \langle y^* - x^* \rangle)} = \overline{S(B_k(h))} \text{ és } g_k + B_k \subseteq \overline{S(\sum_{h \in H} B_k(h))} = \overline{S(B_k(H))}.$$

Vegyünk υ helyett υ^r-t $(r \neq 0)$ és az előzővel analóg módon, a $B_k(H)$-nak megfelelő alteret $B_k(H,r)$-el jelölve:

$$rg_k + B_k \subseteq \overline{S(B_k(H,r))},$$

$$B_k(H,r) = \sum_{h \in H} \sum_{y-x=h} \left\langle \sum_{t=0}^{r-1} (y + tg_k)^* - \sum_{t=0}^{r-1} (x + tg_k)^* \right\rangle \leq$$

$$\leq \sum_{h \in H} \sum_{y-x=h} \sum_{t=0}^{r-1} \left\langle (y + tg_k)^* - (x + tg_k)^* \right\rangle \leq \sum_{h \in H} B_k(h) = B_k(H),$$

alkalmas $t \in \mathbf{F}_p$-vel $rt = 1$ és $B_k(H) = B_k(H, rt) \leq B_k(H,r) \leq B_k(H)$, tehát $B_k(H,r) = B_k(H)$. ∎

4.24 LEMMA. *Legyen* $B_{k+1} \underline{\leq H \leq} G$ *és tegyük fel, hogy minden* $h \in H \setminus B_{k+1}$*-ra* $B_k(H) = B_k(h)$ *vagy* $h + B_k \subseteq \overline{S(B_k(H))}$ *Ekkor minden* $x \in G$*-re*

$$\pi'_k|_{x+H} \in C_{Aut\Gamma_x}(((B_k)_R)|_{x+H}) \text{ és } \upsilon_k^{\pi'_k} = \tau'_k,$$

ahol $\tau'_k|_{x+H} := \tau_k|_{x+H} x^*_R$, $\upsilon'_k|_{x+H} := ((x^*)_R)^{-1}\upsilon_k|_{x+H}$, $V(\Gamma_x) := x+H$ *és* $\Gamma_x \cong Cay(H, S \cap H)$

Bizonyítás. Legyen $y - x = h \in S \cap H$ és válasszuk υ_k helyett $\upsilon'_k := (x^*_R)^{-1}\upsilon$-t. Erre $\iota_k(\upsilon'_k) = \iota_k(\upsilon_k)$, $(x+b)\upsilon'_k - (x+b)\tau = (x+b-x^*)\upsilon_k - (x+b)\tau = 0$, tehát $a^* \in B_k(H)$ minden $a \in x+H$-ra és a 4.18 lemma (3) pontja szerint $(y)\pi'_k - (x)\pi'_k \in y - x + B_k(H)$. $B_k(h) = B_k(H)$ esetén a 4.16, $h \in B_{k+1}$ esetén a 4.23 lemmából, egyébként pedig a feltételekből következik, hogy $y - x \in \overline{S(B(H))}$. Ezért $y - x + 0 \in S$ miatt $y - x + B(H) \subseteq S$ és $\pi'_k \in C_{Aut\Gamma_x}(((B_k)_R)|_{x+H})$. Végül $a \in x+H$-ra

$$(a)\pi'_k\upsilon_k(\pi'_k)^{-1} = (a)(x^*_R)^{-(a,g_k)}\pi_k\upsilon_k\pi_k^{-1}(x^*_R)^{(a,g_k)+1} = (a)\tau_k x^*_R.$$

■

4.25 KÖVETKEZMÉNY. Z_p^3 *DCI-csoport*

Bizonyítás. Legyen $G = Z_p^3$, $\Gamma = Cay(G,S)$ és $G_R^\delta \leq Aut\Gamma$. A 4.1 és 4.3 lemmák szerint $\upsilon_1 = \tau_1 \in G_R$. Ha $B_2(g) = \{0\}$ minden $g \in G$-re akkor minden $x \in G$-re $x^* =: b \in B_2$, $(x)\upsilon_2\tau_2^{-1} = (x)b_R$, és $\upsilon_2 = \tau_2 b_R \in G_R$. Ha valamilyen $g \in G$-re $B_2(g) \neq \{0\}$, akkor $B_2(g) = B_2$, a 4.23 lemmából $rg_2 + B_2 \subseteq \overline{S_2}$ $(r = 1, \ldots, p-1)$ Ebből $\langle S_2 \rangle \neq G$ esetén $g_2 \notin \langle S_2 \rangle$, a 4.18 és 4.19 lemmákból $\pi_2 \in C_{Aut(\Gamma)}(\tau_1)$, $\upsilon_2^{\pi_2} = \tau_2$. Ha $B_2(g) = B_2$, akkor a 4.16 lemmából $g + B_2 \subseteq \overline{S_2}$, azaz $g \notin S_2$. Tehát $g \in S_2$ esetén $B_2(g) = 0$, a 4.15 lemma szerint $B(rg + tg') \leq B(g) + B(g')$, amiből $\langle S_2 \rangle = G$ mellett $B_2(g) = \{0\}$ minden $g \in G$-re. Ha $B_3(g_3) = \{0\}$, akkor $B_3(g) = \{0\}$ minden $g \in G_R$ és mint előbb $\upsilon_3 \in G_R$. Ha $B_3(g_3) \neq \{0\}$, akkor a 4.24 lemma szerint $\pi'_k \in C_{Aut(\Gamma)}(\langle \tau_1, \tau_2 \rangle)$, $(\upsilon')_3^{\pi'_k} = \tau'_3$. Végül a Babai lemmából Γ CI-gráf. ■

Foglajuk össze, hogy mit bizonyítottunk az imént.

4.26 LEMMA. *Legyenek* $G = Z_p^3$, $\Gamma = Cay(G,S)$, $\langle G_R, G_R^\delta \rangle \leq P \in Syl_p(Aut\Gamma)$. *Ekkor*

(1) $\pi_2 \in C_{Aut(\Gamma)}(\tau_1)$ *és* $\langle S_2 \rangle = G$ *esetén* $\upsilon_2 \in G_R$

(2) $\tau_i = \upsilon_i$ $(i = 1, 2)$ *esetén* $\pi'_3 \in C_{Aut(\Gamma)}(\langle \tau_2, \tau_3 \rangle)$

Bizonyítás. Az elöbbi bizonyításból nyilvánvaló. ■

4.27 DEFINÍCIÓ. *Legyen* $B_{k+1} \underline{\leq H \leq} G$. *Ekkor* h *renitens* H*-ban, ha* $h \in H$ *és* $B_k(h) \neq B_k(H)$ *vagy* $h + B_k \not\subseteq \overline{S(B_k(H))}$, *valamint az* $R_k(H) := \langle h \in H | h \text{ renitens} \rangle$ *jelöléssel* H *renitens részcsoport, ha* $g_k \in R_k(H)$

4.28 Megjegyzés. *A 4.23 lemma szerint* g_k *nem renitens elem és* $B_k(B_k)=0$ *figyelembevételével, ha van renitens elem, akkor minden* $b \in B_k$ *is az.*

4.29 LEMMA. *Legyen* $B_{k+1} \leq H \leq G$ *és tegyük fel, hogy* H *nem renitens. Ekkor alkalmas* $(\cdot,\cdot)$*-el minden* $x \in G$*-re*

$$\pi'_k|_{x+H} \in C_{Aut\Gamma_x}(((B_k)_R)|_{x+H}) \text{ és } \upsilon_k^{\pi'_k} = \tau'_k,$$

$$\tau'_k|_{x+H} := \tau_k|_{x+H} x^*_R,\ \upsilon'_k|_{x+H} := ((x^*)_R)^{-1}\upsilon_k|_{x+H},\ V(\Gamma_x) := x+H,\ \Gamma_x \cong Cay(H, S \cap H)$$

Bizonyítás. Legyenek $y-x=h \in H \cap S$ és válasszuk υ_k helyett $\upsilon'_k := (x^*_R)^{-1}\upsilon$-t. Erre ugyan úgy, mint a 4.24 bizonyításában $\iota_k(\upsilon'_k) = \iota_k(\upsilon_k)$ és $a^* \in B_k(H)$ minden $a \in x+H$-ra. Mivel $g_k \notin R_k(H) < G$, ezért $(\cdot,\cdot)$ választható úgy, hogy $g_k \in R_k(H)^\perp$. Ekkor a 4.18 lemma (2) pontjából ha $y-x \in R_k(H)$, akkor $(y)\pi'_k - (x)\pi'_k \in S$, a (3) pontjából pedig $(y)\pi'_k - (x)\pi'_k \in y-x+B_k(H)$. Mivel $y-x \notin R_k(H)$ esetén $y-x \in \overline{S(B_k(H))}$, ezért $y-x+0 \in S$ miatt $y-x+B_k(H) \subseteq S$ és $\pi'_k \in C_{Aut\Gamma_x}(((B_k)_R)|_{x+H})$. A többi ugyan úgy adódik, mint a 4.24 bizonyításánál. ∎

4.30 DEFINÍCIÓ. *Legyenek* $H \leq K \leq G$ *és* $T : \mathcal{P}(G) \times \mathcal{P}(G) \longrightarrow \mathcal{P}(G)$*:*

$$T(H,K) := (g \in G | g+K \subseteq \overline{S(H)}).$$

Minden $g \in G$*-re definiáljuk a következő Cayley gráfokat*

$$\Gamma(g,l) := Cay(\mathbf{B}_k, T(B(g), B_k) \cap B_l + B_k),\ \Gamma(g) := \Gamma(g, n+1)\ (k \leq l \leq n+1)$$

4.31 LEMMA. $\iota_k(G^\delta_R) \in Aut\Gamma(g)$

Bizonyítás. Tegyük fel, hogy $y-x+B_k \subseteq \overline{S(B(g))}$ és legyen $(y)\upsilon-(x)\upsilon+b+b' \in S$, ahol $\upsilon \in G^\delta_R, b \in B_k, b' \in B(g))$. Mivel G^δ_R centralizálja $(B_k)_R$-t és része $Aut\Gamma$-nak, ezért $(y)\upsilon+b+b' = (y+b+b')\upsilon$ és $y-x+b+b' \in S$, majd minden $b'' \in B(g)$-re $y-x+b+b'' \in S$ és $(y+b+b'')\upsilon-(x)\upsilon = (y)\upsilon-(x)\upsilon+b+b'' \in S$. Másképp mondva $\Xi_{B(g)}((y)\upsilon-(x)\upsilon+b) = 1$ és ugyan így $\Xi_{B(g)}(-((y)\upsilon-(x)\upsilon+b)) = 1$. Tehát minden $b \in B_k$-ra $(y)\upsilon-(x)\upsilon+b \in \overline{S(B(g))}$. ∎

4.32 LEMMA. *Tegyük fel, hogy* $h_i \notin \langle h_j \rangle \cup \langle g_k \rangle$ $(i,j \in \{k,k+1\})$ *és* $\langle g_k, g_{k+1} \rangle = \langle h_k, h_{k+1} \rangle$*. Ekkor*

$$\iota_k((B_{k+2})_R) \neq \iota_k(\langle \upsilon_{k+1}, \upsilon_k, (B_k)_R \rangle) \Rightarrow rh_j + B_k \subseteq \overline{S(B(h_i))}\ (i \neq j)$$

Bizonyítás. Tekintsük a $\Gamma(h_i, k+2)$ gráfnak mondjuk azt a $\Gamma'_i = Cay(H, T_i)$ részgráfját, ahol $H := B_{k+2}/B_k$ és $T_i = T(B(h_i), B_k) \cap B_l + B_k$. Erre nyilván $H_R = \iota_k((B_{k+2})_R)|_{\overline{B_{k+2}}}$ és a 4.6 állításból a $\delta' := \iota_k(\delta)|_{\overline{B_{k+2}}}$ jelöléssel $H_R^{\delta'} = \iota_k(\langle v_{k+1}, v_k, (B_k)_R\rangle)|_{\overline{B_{k+2}}}$. A 4.31 lemmát felhasználva $H_R^{\delta'} \in Aut\Gamma'$, tehát

$$\langle H_R, H_R^{\delta'}\rangle \leq \iota_k(P^* \cap ker\iota_{k+2})|_{\overline{B_{k+2}}} \cap Aut\Gamma' \leq R \in Syl_p(Aut\Gamma')$$

majd a 4.21 lemmából $r\overline{g_{k+1}} \in \overline{T_i(\overline{B_{k+1}})}$ $(r = 1, \ldots, p-1)$. Eszerint, ha $\overline{r_1 g_{k+1} + t_1 g_k} \in T_i$, akkor $\overline{r_1 g_{k+1} + t g_k} \in T_i$ minden $t \in \mathbf{F}_p$-re. Legyenek $h_i = r_i g_{k+1} + t_i g_k$, $rh_j = r_j g_{k+1} + t_j g_k$ $(r \neq 0)$. A feltételek miatt $r_i \neq 0 \neq r_j$, tehát létezik $r' \in \mathbf{F}_p \setminus \{0\}$, hogy $r' r_i = r_j$. A 4.16 lemmából $r' h_i + B_k \subseteq \overline{S(B(h_i))}$, azaz $\overline{r_j g_{k+1} + r' t_i g_k} \in T_i$, és $\overline{rh_j} = \overline{r_j g_{k+1} + t_j g_k} \in T_i$. Másszóval $rh_j + B_k \subseteq \overline{S(B(h_i))}$. ∎

4.33 TÉTEL. *Z_p^4 DCI-csoport*

Bizonyítás. Legyen $G = Z_p^4$, $\Gamma = Cay(G, S)$ és $G_R^\delta \leq Aut\Gamma$. A 4.1 és 4.3 lemmák szerint $v_1 = \tau_1 \in G_R$. Mivel $B_2(g) \leq B_2(G) \leq B_2$ és így $\overline{S_2} \subseteq \overline{S(B_2(G))}$ ezért itt $g \in G$ csak úgy lehet renitens, ha $g \in S_2$, és a 4.16 lemmát alkalmazva $g \in S_2$ mellett $B_2(g) = 0$. A 4.15 lemma szerint $B(rg + th) \leq B(g) + B(h)$, ezért az $\langle S_2\rangle = G$ esetben $B_2(G) = \{0\}$, az az nincs is renitens elem. Ha $S_2 \cap B_2(G) \neq \{0\}$, akkor $B_2(G) = B_2$ és a 4.23 lemmából $g_2 \in \overline{S_2}$, tehát $g_2 \notin S_2 + B_2$. Ebből az $|\langle S_2\rangle| \leq p^2$ esetben $g_2 \notin \langle S_2\rangle$, az az G nem renitens. Kaptuk, hogy csak az $|\langle S_2\rangle| = p^3$ esetben lehet G renitens. Most az összes nem renitens esetben alkalmazva a 4.29 lemmát $\pi_2 \in C_{Aut(\Gamma)}(\tau_1)$, $v_2^{\pi_2} = \tau_2$. Nézzük tovább ezeket az eseteket. Legyenek $h_i := ig_3 + g_4$ $(i \in \mathbf{F}_p)$. Ha $\{0\} \leq B_3(G) < B_3$, akkor legfeljebb egy i-re lehet $B_3(h_i) < B_3(G)$, mert különben a 4.15 lemmát használva minden $g \in G$-re $B_3(g) \leq B_3(h_i) + B_3(h_j) = \{0\}$, amiből $B_3(G) = \{0\}$ következne. Ekkor viszont $g_3 \notin R_3(G)$, azaz G nem renitens. Ha $B_3(G) = B_3$ és G renitens, akkor valamilyen j-re és $r' \in \mathbf{F} \setminus \{0\}$-re $r' h_j + B_3 \not\subseteq \overline{S(B_3(G))} = \overline{S_3}$, tehát $r' h_j \notin \overline{S_3}$ és valamilyen $i \neq j$-re $r' h_j + B_3 \not\subseteq \overline{S(B_3(h_i))}$. Most a 4.32 lemmát alkalmazva azt kapjuk, hogy $\iota_3(G_R) = \iota_3(G_R^\delta)$. Tehát léteznek $v_t' \in G_R^\delta$ $(t \in \{3, 4\})$, hogy a $g_3' := r' h_j$ jelöléssel $\iota_3(v_3') = \iota_3((g_3')_R)$ és $\iota_4(v_4') = \iota_4((g_4')_R)$ valamilyen $g_4' \notin \langle g_1, g_2, g_3'\rangle$-vel. Erre elmondva az előbbieket, $B_3(G) = B_3$ nem fordulhat elő, mert különben a 4.23 lemmából $g_3' = r' h_j \in \overline{S_3}$-t kapnánk ellentmondásban az előbbiekkel. Tehát G itt már nem renitens és alkalmas v_3'-vel mindig alkalmazhatjuk a 4.29 lemmát. Kaptuk, hogy $\tau_i = v_i$ $(i = 1, 2, 3)$ és $\iota_4(\tau_4) = v_4(\tau_4)$. Ekkor további renitens elem csak B_3-ban lehet, G itt sem renitens és újra alkalmazva a 4.29 lemmát, $G_R = G_R^{\pi\delta}$, $\pi \in Aut(\Gamma)$. Maradt a renitens $|\langle S_2\rangle| = p^3$ eset. Legyen a $H := \langle S_2\rangle$ szerinti mellékosztályok egy reprezentáns rendszere $X := \{x_1, \ldots, x_p\}$ és tekintsük azokat a Γ_{x_i} részgráfokat, ahol $V(\Gamma_{x_i}) := x_i + H$ és $\Gamma_{x_i} \cong Cay(H, S \cap H)$. Ugyanúgy mint a bizonyítás elején $R_2(H) = H$ esetén itt sincs renitens elem, az az H nem renitens, ahogy az $|R_2(H)| \leq p^2$ esetben sem az. Megint a 4.29 lemmát alkalmazva minden $i \in \mathbf{F}_p$-re $\pi_2'|_{x_i+H} \in C_{Aut\Gamma_{x_i}}(((B_2)_R)|_{x_i+H})$ és $v_2^{\pi_2'}|_{x_i+H} = \tau_k|_{x_i+H}(x_i^*)_R$. Tekintsünk egy Γ_{x_i}-t és legyen $g_3 \in H$. Erre $H \cong Z_p^3$ és $v_i'|_{x_i+H} \in H_R|_{x_i+H}$ $(i = 1, 2)$ miatt a 4.26 lemma (2) pontjából $\pi_3'|_{x_i+H} \in C_{Aut(\Gamma_{x_i})}((B_3)_R|_{x_i})$. Ez azt jelenti, hogy $y - x \in H \cap S$-ből $(y)\pi_3' - (x)\pi_3' \in H \cap S$ következik. Majd nézzük a $\vec{\Gamma}_2 = Cay(G/B_2, \vec{S}_2)$ segédgráfot, ahol

$(G/B_2)_R = \iota_2(G_R)$ és $\vec{S}_2 := \{\overline{g} \in G/B_2 | g + B_2 \subseteq S\}$. Itt $\overline{y} - \overline{x} \in \vec{S}_2 \setminus \overline{H}$ pontosan azt jelenti, hogy $y - x \in S \setminus H$. Mivel $\iota_2(G_R^\delta) \leq \iota_2(P) \leq R \in Syl_p(Aut\vec{\Gamma})$, ezért a 4.26 lemma (1) pontjából $\iota_2(\pi_3') \in C_{Aut\vec{\Gamma}}(\iota_2((B_3)_R))$. Ez pedig azt jelenti, hogy $\overline{y}-\overline{x} \in \vec{S}_2 \setminus \overline{H}$-ból $(\overline{y})\iota_2(\pi_3') - (\overline{x})\iota_2(\pi_3') \in \vec{S}_2 \setminus \overline{H}$ következik. Ez utóbbi esetén viszont minden $x' \in x+B_2$, $y' \in y+B_2$ párra $(y')(\pi_3') - (x')(\pi_3') \in S$. Ebből $(y)(\pi_3') - (x)(\pi_3') \in S$ minden $y - x \in S \setminus H$-ra és $\pi_3' \in Aut\Gamma$. Tehát ott tartunk, hogy $\tau_1 = \upsilon_1$, $\iota_2(\tau_j) = \iota_2(\upsilon_j)$ $(j = 2, 3)$ és $\upsilon_j|_{x_i+h} = \tau_j|_{x_i+h}$. Mivel $g_4 \notin H < G$, ezért a $(\cdot, \cdot)$-t választhatjuk úgy, hogy $g_4 \in H^\perp$ is teljesüljön. Ha $y - x \in S \cap H$, akkor a 4.18 lemma (2) pontjából, ha pedig $y - x \in S \setminus H$ akkor a $\vec{\Gamma}_2$ gráfot nézve a 4.26 lemma (2) pontjából következik, hogy $(y)\pi_4' - (x)\pi_4' \in S$, vagyis $\pi_4' \in Aut\Gamma$. Erre viszont már $\upsilon_4^{\pi_4'} = \tau_4$ és $\tau_4 \upsilon_j^{\pi_4'} = \upsilon_j^{\pi_4'} \tau_4$ figyelembevételével $\upsilon_j \in G_R$ $(j = 1, 2, 3, 4)$. Ha $g_3 \notin H$, akkor $(\cdot, \cdot)$-t rögtön választhatjuk úgy, hogy $g_3 \in H^\perp$ is teljesüljön, és itt elöbb a $\vec{\Gamma}_2$ gráfot nézve jutunk el oda, hogy $\tau_1 = \upsilon_1$, $\iota_2(\tau_j) = \iota_2(\upsilon_j)$ $(j = 2, 3)$. De itt már most $\tau_3\upsilon_2 = \upsilon_2\tau_3$, tehát $\upsilon_2|_{ig_4+B_3} \in G_R|_{ig_4+B_3}$ és $g_4 \in H$ miatt $\upsilon_j \in G_R$ $(j = 1, 2, 3)$. Korábban már láttuk, hogy itt is alkalmazható a 4.29 lemma, és így már minden esetben $G_R = G_R^{\pi\delta}$ valamilyen $\pi \in Aut(\Gamma)$-ra. Végül a Babai lemmát alkalmazva kapjuk,hogy Γ CI-gráf. ∎

Irodalomjegyzék

[1] A.Ádám, Research problem 2-10, J. Combin. Theory **2** (1967), 393.

[2] N. Alon, Tools from higher algebra,Handbook of Combinatorics (in: R. L. Graham et al. Eds.), Elsevier Science, Amsterdam, 1995, pp. 1751–1783.

[3] B. Alspach and T. D. Parsonc, Isomorphisms of circulant graphs and digraphs, Discrete Math. **25** (1979), 97–108.

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

[5] L. Babai and P. Frankl, Isomorphism of Cayley graphs, I, Colloq. Math. Soc. J. Bolyai **18** (1978), 35–52.

[6] L. Babai and P. Frankl, Isomorphism of Cayley graphs, II, Acta Math. Acad. Sci. Hungar. **34** (1979), 177–183.

[7] L. Babai, Automorphism groups, isomorphism, reconstruction, Handbook of Combinatorics (in: R. L. Graham et al. Eds.), Elsevier Science, Amsterdam, 1995, pp. 1449–1540.

[8] N. Biggs, Algebraic Graph Theory, Cambridge University Press, New York, 1992.

[9] M. Conder and C. H. Li, On isomorphisms of finite Cayley graphs, European J. Combin. **19** (1998), 911-919.

[10] H.S.M. Coxeter, W.O.J. Moser, Generators and Relations for Discrete Groups, Springer, Berlin-Göttingen, 1957.

[11] B. Elspas and J. Turner, Graphs with circulant adjacency matrices, J. Combin. Theory **9** (1970), 297–307.

[12] M. Hirasaka and M. Muzychuk, The elementary abelian group of rank 4 is a CI-group, J. Combin. Theory Ser. A **94** (2001), 339–362.

[13] C.H. Li, On isomorphisms of finite Cayley graphs — a survey, Discrete Math. **256** (2002), 301–334.

[14] C.H. Li, C.E. Praeger, M.Y. Xu, Isomorphism of finite Cayley digraphs of bounded valency, J. Combin. Theory Ser. B **73** (1998), 164–183.

[15] A. Lubotzky, R. Phillips, P. Sarnak, Ramanujan graphs, Combinatorica **8** (1988), 261–277.

[16] A. Lubotzky, Discrete Groups, Expanding Graphs and Invariant Measures, Progress in Mathematics, Vol. **125**, Birkhäuser - Basel - Boston, Berlin, 1994.

[17] G. A. Margulis, Explicit constructions of graphs without short cycles and low density codes, Combinatorica **2** (1982), 71–78.

[18] Morris,Joy, Result towards showing Z_p^n is a CI-group, Congr. Numer. **156** (2002), 143–153.

[19] M. Muzychuk, Ádám's conjecture is true in the square-free case, J. Combin. Theory Ser. A **72** (1995), 118–134.

[20] M. Muzychuk, On Ádám's conjecture for circulant graphs, Discrete Math. **167/168** (1997), 497–510; corrigendum **176** (1997), 285–298.

[21] Muzychuk, M. An elementary abelian group of large rank is not a CI-group, Discrete Math. **264** (2003), 167–185.

[22] L. A. Nowitz, A non-Cayley-invariant Cayley graph of the elementary Abelian group of order 64, Discrete Math. **110** (1992), 223–228.

[23] P. P. Pálfy, Isomorphism problem for relational structures with a cyclic automorphism, European J. Combin. **8** (1987), 35–43.

[24] C.E. Praeger, Finite transitive permutation groups and finite vertex-transitive graphs, in: Graph Symmetry: Algebraic Methods and Applications, NATO ASI Series C, Vol. **97**, 1997, pp. 277–318.

[25] G.O. Sabidussi, Vertex-transitive graphs, Monatsh. Math. **68** (1964), 426–438.