The Cayley isomorphism property for groups of order p^3q

Gábor Somlai
Department of Algebra and Number Theory
Eötvös Loránd University
1117 Budapest, Pázmány Péter sétány 1/C , Hungary
email: gsomlai@cs.elte.hu*

Abstract

For every prime $p > 3$ and for every prime $q > p^3$ we prove that $\mathbb{Z}_q \times \mathbb{Z}_p^3$ is a DCI-group.

1 Introduction

Let G be a finite group and S a subset of G. The Cayley graph $Cay(G, S)$ is defined by having the vertex set G and g is adjacent to h if and only if $gh^{-1} \in S$. The set S is called the connection set of the Cayley graph $Cay(G, S)$. A Cayley graph $Cay(G, S)$ is undirected if and only if $S = S^{-1}$, where $S^{-1} = \left\{ s^{-1} \in G \mid s \in S \right\}$. Every right multiplication via elements of G is an automorphism of $Cay(G, S)$, so the automorphism group of every Cayley graph on G contains a regular subgroup isomorphic to G. Moreover, this property characterises the Cayley graphs of G.

It is clear that automorphism μ of the group G induces an isomorphism between $Cay(G, S)$ and $Cay(G, S^\mu)$. Such an isomorphism is called a Cayley isomorphism. A Cayley graph $Cay(G, S)$ is said to be a CI-graph if, for each $T \subset G$, the Cayley graphs $Cay(G, S)$ and $Cay(G, T)$ are isomorphic if and only if there is an automorphism μ of G such that $S^\mu = T$. Furthermore, a group G is called a DCI-group if every Cayley graph of G is a CI-graph and it is called a CI-group if every undirected Cayley graph of G is a CI-graph.

The problem of investigating the isomorphism problem of Cayley graphs started with Ádám's conjecture [1], which states that every circulant graph if a CI-graph. Using our terminology, it was conjectured that every cyclic group is a DCI-group. This conjecture was first disproved by Elspas and Turner [8] for directed Cayley graphs of $\mathbb{Z}_8$ and for undirected graphs of Cayley graphs of $\mathbb{Z}_{16}$.

*Research supported by the Hungarian Scientific Fund (OTKA), grant no. K84233

By investigating the spectrum of circulant graph Elspas and Turner [8], and independently Djoković [6] proved that every cyclic group of order p is a CI-group if p is a prime. Also a lot of research was devoted to the investigation of circulant graphs. One of the most important results for our investigation is that $\mathbb{Z}_{pq}$ is a DCI-group for every pair of primes $p < q$. This result was first proved by Alspach and Parsons [2] and later by Pöschel and Klin [11] using Schur rings, and by Godsil [9]. Finally, Muzychuk [14, 15] proved that a cyclic group $\mathbb{Z}_n$ is a DCI-group if and only if $n = k$ or $n = 2k$, where k is square-free. Furthermore, $\mathbb{Z}_n$ is a CI-group if and only if n is as above or $n = 8, 9, 18$.

It is easy to see that every subgroup of a (D)CI-group is also a (D)CI-group so it is natural to investigate p-groups which are the Sylow p-subgroups of a finite group. Babai and Frankl [5] proved that if G is a p-group, which is a CI-group, then G can only be elementary abelian p-group, the quaternion group of order 8 or one of a few cyclic groups $\mathbb{Z}_4$, $\mathbb{Z}_8$, $\mathbb{Z}_9$ or $\mathbb{Z}_{27}$. Muzychuk's result about cyclic groups shows that $\mathbb{Z}_{27}$ is not a CI-group and $\mathbb{Z}_8$ is not a DCI-group. They also asked whether every elementary abelian p-group is a CI-group.

The cyclic group of order p, which is a CI-group, can also be considered as an elementary abelian p-group of rank 1. The best general result was given by Hirasaka and Muzychuk [10] who proved that $\mathbb{Z}_p^4$ is a CI-group for every prime p. For our investigation the following weaker results are also important. Dobson [7] proved that $\mathbb{Z}_p^3$ is a CI-group for every prime p and Alspach and Nowitz shoved [3] that $\mathbb{Z}_p^3$ is a CI-group with respect to Cayles color digraphs. However Muzychuk [16] showed that an elementary abelian p-group of $2p - 1 + \binom{2p-1}{p}$ rank is not a CI-group.

Severe restriction on the structure of CI-groups was given by Li and Praeger and then a more precise list of candidates for CI-groups was given by Li, Lu and Pálfy [13].

New family of CI-groups was found by Kovács and Muzychuk [12], that is, $\mathbb{Z}_{p^2} \times \mathbb{Z}_q$ is a CI-group for every prime p and q. It was also conjectured in [12], that the direct product of CI-groups of coprime order is a CI-group.

Theorem 1. *For every prime p and every prime $q > p^3$ the group $\mathbb{Z}_{p^3} \times \mathbb{Z}_q$ is a DCI-group.*

Our paper is organized as follows. In Section 2 we introduce the notation that will be used throughout this paper. In Section 3 we collect important ideas that we will use in the proof of Theorem 1. Finally, Section 4 contains the proof of Theorem 1.

2 Technical details

In this section we introduce some notation. Let G be a group. We use $H \leq G$ to denote that H is a subgroup of G and by $N_G(H)$ and $C_G(H)$ we denote the normalizer and the centralizer of H in G, respectively. The center of a group G will be denoted by $Z(G)$.

Let us assume that the group H acts on the set Ω and let G be an arbitrary group. Then by $G \wr_\Omega H$ we denote the wreath product of G and H. Every element $g \in G \wr_\Omega H$ can be uniquely written as hk, where $k \in K = G^\Omega$ and $h \in H$. The group $K = G^\Omega$ is called the base group of $G \wr_\Omega H$ and the elements of K can be treated as functions from Ω to G. If $g \in G \wr_\Omega H$ and $g = hk$ we denote k by $(g)_b$. In order to simplify the notation Ω will be omitted if it is clear from the definition of H and we will write $G \wr H$.

The symmetric group on the set Ω will be denoted by $Sym(\Omega)$. Let G be a permutation group on the set Ω. For a G-invariant partition $\mathcal{B}$ of the set Ω we use $G^{\mathcal{B}}$ to denote the permutation group on $\mathcal{B}$ induced by the action of G and similarly, for every $g \in G$ we denote by $g^{\mathcal{B}}$ the action of g on the partition $\mathcal{B}$.

For a group G, let $\hat{G}$ denote the subgroup of the symmetric group $Sym(G)$ formed by the elements of G acting by right multiplication on G. For every Cayley graph $\Gamma = Cay(G, S)$ the subgroup $\hat{G}$ of $Sym(G)$ is contained in $Aut(\Gamma)$.

Definition 1. *Let $G \leq Sym(\Omega)$ be a permutation group. Let*

$$G^{(2)} = \left\{ \pi \in Sym(\Omega) \middle| \begin{array}{l} \forall a, b \in \Omega\ \exists g_{a,b} \in G \text{ with } \quad \pi(a) = g_{a,b}(a) \text{ and} \\ \qquad\qquad\qquad\qquad\qquad\qquad \pi(b) = g_{a,b}(b) \end{array} \right\}.$$

We say that $G^{(2)}$ is the 2-closure of the permutation group G.

Lemma 1. *Let Γ be a graph. If $G \leq Aut(\Gamma)$, then $G^{(2)} \leq Aut(\Gamma)$.*

3 Basic ideas

In this section we collect some results and some important ideas that we will use in the proof of Theorem 1.

We begin with a fundamental lemma that we will use all along this paper.

Lemma 2 (Babai [4])**.** *$Cay(G, S)$ is a CI-graph if and only if for every regular subgroup $\mathring{G}$ of $Aut(Cay(G, S))$ isomorphic to G there is a $\mu \in Aut(Cay(G, S))$ such that $\mathring{G}^\mu = \hat{G}$.*

We introduce the following definition.

Definition 2. *(a) We say that a Cayley graph $Cay(G, S)$ is a CI$^{(2)}$-graph if and only if for every regular subgroup $\mathring{G}$ of $Aut(Cay(G, S))$ isomorphic to G there is a $\sigma \in \langle \mathring{G}, \hat{G} \rangle^{(2)}$ such that $\mathring{G}^\sigma = \hat{G}$.*

(b) A group G is called a DCI$^{(2)}$-group if for every $S \subset G$ the Cayley graph $Cay(G, S)$ is a CI$^{(2)}$-graph.

Definition 3. *Let Γ be an arbitrary graph and $A, B \subset V(\Gamma)$ such that $A \cap B = \emptyset$. We write $A \sim B$ if one of the following four possibilities holds:*

(a) For every $a \in A$ and $b \in B$ there is an edge from a to b but there is no edge from b to a.

(b) For every $a \in A$ and $b \in B$ there is an edge from b to a but there is no edge from a to b.

(c) For every $a \in A$ and $b \in B$ the vertices a and b are connected with an undirected edge.

(d) There is no edge between A and B.

We also write $A \nsim B$ if none of the previous four possibilities holds.

Lemma 3. *Let A, B be two disjoint subsets of cardinality p of a graph. We write $A \cup B = \mathbb{Z}_p \cup \mathbb{Z}_p$. Let us assume that $\hat{\mathbb{Z}}_p$ acts naturally on $A \cup B$ and for a generator $\mathring{g}$ of the cyclic group $\mathring{Z}_p$ the action of $\mathring{a}$ is defined by $(a_1, a_2)\mathring{g} = (a_1 + b, a_2 + c)$ for some $b, c \in \mathbb{Z}_p$.*

(a) If $b = c$, then the action of $\hat{\mathbb{Z}}_p$ and $\mathring{Z}_p$ on $A \cup B$ are the same.

(b) If $A \nsim B$, then $b = c$.

(c) If $A \sim B$, then every $\pi \in Sym(A \cup B)$ which fixes A and B setwise is an automorphism of the graph defined on $A \cup B$ if $\pi \restriction A \in Aut(A)$ and $\pi \restriction B \in Aut(B)$.

Proof. These statements are obvious. ■

Lemma 4. *Let us assume that H is a regular abelian subgroup of $Sym(p^n)$ and let $P \geq H$ be a Sylow p-subgroup of $Sym(p^n)$. Then H contains $Z(P)$.*

Proof. It is well known that the center of P is a cyclic p-group. Let z be a generator of $Z(P)$. Then $\langle H, z\rangle$ is a transitive abelian group. Hence $\langle H, z\rangle$ is regular. Since H is also regular, we have that z has to be in H. ■

4 Main result

In this section we will prove that $\mathbb{Z}_p^3 \times \mathbb{Z}_q$ is a DCI-group if $q > p^3$ and $p > 3$.

Our technique is based on Lemma 2 so we fix a Cayley graph $\Gamma = Cay(\mathbb{Z}_p^3 \times \mathbb{Z}_q, S)$. Let $A = Aut(\Gamma)$ and $\mathring{G} = \mathring{\mathbb{Z}}_p^3 \times \mathring{\mathbb{Z}}_q$ be a regular subgroup of A isomorphic to $\mathbb{Z}_p^3 \times \mathbb{Z}_q$. In order to prove Theorem 1 we have to find an $\alpha \in A$ such that $\mathring{G}^\alpha = \hat{G} = \hat{\mathbb{Z}}_p^3 \times \hat{\mathbb{Z}}_q$, what we will achieve in three steps.

4.1 Step 1

We may assume $\hat{\mathbb{Z}}_q$ and $\mathring{\mathbb{Z}}_q$ lie in the same Sylow q-subgroup Q of $Sym(p^3q)$. Then both $\mathring{\mathbb{Z}}_p^3$ and $\hat{\mathbb{Z}}_p^3$ are subgroups of $N_{Sym(p^3q)}(Q) \cap A$ so we may assume that $\mathring{\mathbb{Z}}_p^3$ and $\hat{\mathbb{Z}}_p^3$ lie in the same Sylow p-subgroup of $N_{Sym(p^3q)}(Q) \cap A$ which is contained in a Sylow p-subgroup P of A.

The Sylow q-subgroup Q gives a partition $\mathcal{B} = \{B_1, B_2, \ldots, B_{p^3}\}$ of the vertices of Γ, where $|B_i| = q$ for every $i = 1, \ldots, p^3$. It is easy to see that $\mathcal{B}$ is invariant under the action of $\hat{\mathbb{Z}}_p^3$ and $\mathring{\mathbb{Z}}_p^3$ and hence $\langle \hat{G}, \mathring{G} \rangle \leq Sym(q) \wr Sym(p^3)$. Moreover, both $\mathring{G}$ and $\hat{G}$ are regular so $\mathring{\mathbb{Z}}_p^3$ and $\hat{\mathbb{Z}}_p^3$ induce regular action on $\mathcal{B}$ which we denote by H_1 and H_2, respectively. The assumption that $\mathring{\mathbb{Z}}_p^3$ and $\hat{\mathbb{Z}}_p^3$ lie in the same Sylow p-subgroup of A implies that H_1 and H_2 are in the same Sylow p-subgroup of $Sym(p^3)$, what we denote by P_1.

4.2 Step 2

Let us assume that $\hat{\mathbb{Z}}_q \neq \mathring{\mathbb{Z}}_q$ which is generated by p^3 disjoint q-cycles. We intend to find an element $\alpha \in A$ such that $\mathring{\mathbb{Z}}_q^\alpha = \hat{\mathbb{Z}}_q$.

We define a graph Γ_0 on $\mathcal{B}$ such that B_i is connected to B_j if and only if $B_i \nsim B_j$. This is an undirected graph with vertex set $\mathcal{B}$ and both $\mathring{\mathbb{Z}}_p^3$ and $\hat{\mathbb{Z}}_p^3$ are regular subgroups of $Aut(\Gamma_0)$. It follows that Γ_0 is a Cayley graph of $\mathbb{Z}_p^3$.

Definition 4. *(a) For a pair $(B_i, B_j) \in \mathcal{B}^2$ we write $B_i \equiv B_j$ if either there exists a path $C_1, C_2, \ldots, C_n$ in Γ_0 such that $C_1 = B_1$, $C_n = B_2$ or $i = j$.*

(b) For a pair $(B_i, B_j) \in \mathcal{B}^2$ we write $B_i \not\equiv B_j$ if $B_i \equiv B_j$ does not hold.

(c) If both H and K are subsets of the vertices of Γ_0 such that $H \cap K = \emptyset$ and for every $B_i \in H$, $B_j \in K$ we have $B_i \not\equiv B_j$, then we write $H \not\equiv K$.

Observation 1. *(a) The relation $\equiv$ defines an equivalence relation on $\mathcal{B}$. The connected components of Γ_0 will be called equivalence classes.*

(b) Since H_1 acts transitively on $\mathcal{B}$ we have that the size of the equivalence classes defined by the relation $\equiv$ divides p^3.

We can also define a colored graph Γ_1 on $\mathcal{B}$ by coloring the edges of the complete directed graph on p^3 points. B_i is connected to B_j with the same color as B_i' is connected to B_j' in Γ_1 if and only if there exists a graph isomorphism ϕ from $B_i \cup B_j$ to $B_i' \cup B_j'$ such that $\phi(B_i) = B_i'$ and $\phi(B_j) = B_j'$. The graph Γ_1 is a colored Cayley graph of the elementary abelian p-group $\mathbb{Z}_p^3$. Moreover, both H_1 and H_2 act regularly on Γ_1.

We prove the following two lemmas what we will use several times in this step.

Lemma 5. *Let us assume that $C_1', C_2', \ldots C_k'$ are the equivalence classes defined in $V(\Gamma_0)$ and let $C_i = \cup C_i' \subset V(\Gamma)$ for every $i = 1, \ldots, k$. Let α be a permutation on the vertex set $V(\Gamma)$ such that for every $1 \leq i \leq k$ the restriction $\alpha \restriction C_i = \eta_i \restriction C_i$ for some $\eta_i \in Aut(\Gamma)$ and $\alpha^{V(\Gamma_0)}$ is an automorphism of Γ_0. Then α is an automorphism of Γ.*

Proof. Let x and y be points in $V(\Gamma)$. We have to prove that x is connected to y if and only if $\alpha(x)$ is connected to $\alpha(y)$. This holds if x and y are in the same C_i for some $1 \leq i \leq k$ since $\alpha \restriction C_i$ is defined by an automorphism of Γ on C_i. If $x \in B_m$ and $y \in B_n$, where $B_m \sim B_n$ and x is connected to y, then every element of B_m is connected to every element of B_n. Since $\alpha^{V(\Gamma_0)} \in Aut(\Gamma_0)$ the same holds for $\alpha(B_m)$ and $\alpha(B_n)$ and hence $\alpha(x)$ is connected to $\alpha(y)$. Similar argument shows that if $x \in B_m$ and $y \in B_n$, where $B_m \sim B_n$ and x is not connected to y, then $\alpha(x)$ is not connected to $\alpha(y)$. ■

Lemma 6. *(a) Let A and B be two disjoint subsets of cardinality q of $V(\Gamma)$. We write $A = \{(a,x) \mid x \in \mathbb{Z}_q)\}$ and $B = \{(b,x) \mid x \in \mathbb{Z}_q\}$. Let us assume that $\hat{g}$ and $\mathring{g}$ are automorphisms of the graph Γ with $\hat{g}(a,x) = \mathring{g}(a,x) = (a, x+1)$, $\hat{g}(b,x) = (b, x+1)$ and $\mathring{g}(b,x) = (b, x+d)$ for some $d \in \mathbb{Z}_q$ for all $x \in \mathbb{Z}_q$. Furthermore, let us assume that $\hat{w}$ and $\mathring{w}$ are automorphisms of the graph Γ with $\hat{w}(A) = \mathring{w}(A) = B$ and $\hat{w}$ and $\mathring{w}$ commute with $\hat{g}$ and $\mathring{g}$, respectively. Then for $\alpha = \mathring{w}\hat{w}^{-1}$ we have $\mathring{g}^{\alpha} \restriction_B = \hat{g} \restriction_B$.*

(b) Let us assume that $C = \{(c,x) \mid x \in \mathbb{Z}_q\}$ is a subset of $V(\Gamma)$ with $A \cap B = A \cap C = \emptyset$. We also assume that $\hat{g}(c,x) = (c, x+1)$ and $\mathring{g}(c,x) = (c, x+d)$ for every $x \in \mathbb{Z}_q$. Let us assume that $\mathring{v} \in Aut(\Gamma)$ with $\mathring{v}(A) = C$ and we also assume that $\mathring{g}$ and $\mathring{v}$ commute. Then for $\beta = \mathring{v}\hat{w}^{-1}$ we have $\mathring{g}^{\beta} \restriction_B = \hat{g} \restriction_B$.

Proof. (a) Let us assume that $\hat{w}(a,0) = (b, b_0)$ and $\mathring{w}(a,0) = (b, b_0')$ for some $b_0, b_0' \in \mathbb{Z}_q$. Using that $\hat{w}$ and $\hat{g}$ commute we get that $\hat{w}(a,x) = (b, b_0 + x)$ for every $x \in \mathbb{Z}_q$ and similarly we have $\mathring{w}(a,x) = (b, b_0' + dx)$. Thus

$$\begin{aligned}\alpha\,(b,x) &= \alpha\,(b, b_0 + (x - b_0)) = \mathring{w}\,(a, x - b_0) = (b, b_0' + (x - b_0)d) \\ &= (b, (b_0' - db_0) + dx)\,.\end{aligned}$$

It is easy to derive that $\alpha^{-1}(b,x) = \left(b, \frac{x-(b_0'-db_0)}{d}\right)$. Using the previous two equations we get

$$\begin{aligned}&\alpha^{-1}\mathring{g}\alpha \restriction_B (b,x) = \alpha^{-1}\mathring{g}\,(b, (b_0' - db_0) + dx) = \alpha^{-1}\,(b, (b_0' - db_0) + dx + d) \\ &= \left(b, \frac{(b_0' - db_0) + dx + d - (b_0' - db_0)}{d}\right) = (b, x+1).\end{aligned}$$

(b) Let us assume that $\mathring{v}(a,0) = (c, c_0)$ for some $c_0 \in \mathbb{Z}_q$. Then $\mathring{v}(a,x) = (c, c_0 + dx)$ for all $x \in \mathbb{Z}_q$ Thus

$$\begin{aligned}\beta(b,x) &= \mathring{v}\hat{w}^{-1}\,(b, b_0 + (x - b_0)) \\ &= \mathring{v}\,(a, x - b_0) = (c, c_0 + (x - b_0)d)\end{aligned}$$

and hence $\beta^{-1}(c,x) = (b, \frac{x-c_0+b_0d}{d})$. Similarly to the previous case we have

$$\begin{aligned}\beta^{-1}\mathring{g}\beta\,(b,x) &= \beta^{-1}\mathring{g}\,(c, c_0 + (x - b_0)d) = \beta^{-1}\,(c, c_0 + (x - b_0)d + d) \\ &= \left(b, \frac{c_0 + (x - b_0)d + d - c_0 + b_0d}{d}\right) = (b, x+1)\,.\end{aligned}$$

■

The points of the graph Γ_0 and Γ_1 can be identified with the elements of $\mathbb{Z}_p^3$ and we may assume that the action of an element r of the Sylow p-subgroup P_1 is the following:

$$r(a,b,c) = (a+x, b+s_a, c+t_{a,b}),$$

where s_a only depends on a and $t_{a,b}$ depends on a and b.

Let $\hat{g}$ and $\mathring{g}$ denote the generator of $\hat{\mathbb{Z}}_q$ and $\mathring{\mathbb{Z}}_q$, respectively. We may assume that $\hat{g} \restriction B_1 = \mathring{g} \restriction B_1$.

(a) Let us assume first that Γ_0 is a connected graph.

Using Lemma 3 (b) we get that $\hat{g} \restriction B_i = \mathring{g} \restriction B_j$ if there exists a path in Γ_0 from B_i to B_j. This shows that $\hat{g} = \mathring{g}$ since Γ_0 is connected in this case.

(b) Let us assume that Γ_0 is the empty graph.

For every $B_m \in \mathcal{B}$ there exist $\hat{r}_m$ and $\mathring{r}_m$ such that $\hat{r}_m(B_1) = \mathring{r}_m(B_1) = B_m$.

Let α be defined as follows

$$\begin{aligned} \alpha \restriction B_1 &= id \\ \alpha \restriction B_m &= \mathring{r}_m \hat{r}_m^{-1} \ \text{ for } \ 2 \le m \le p^3. \end{aligned} \tag{1}$$

It is easy to see that $\alpha^{\mathcal{B}} = id$ so using Lemma 5 we get that α is an automorphism of Γ. Using Lemma 6 (a) we get that $\mathring{g}^{\alpha} = \hat{g}$.

(c) Let us assume that the size of the connected components of Γ_0 is p.

Let $C'_1, C'_2, \ldots, C'_{p^2}$ denote the equivalence classes defined by the relation $\equiv$ on Γ_0 and for $1 \le m \le p^2$ let $C_m = \cup C'_m$. For $C_2, \ldots, C_{p^2}$ we choose an element $\hat{u}_m$ of $\hat{\mathbb{Z}}_p^3$ such that $\hat{u}_m(C_1) = C_m$. We may assume that $B_1 \subset C_1$. Since H_2 is regular on Γ_0, for every $2 \le m \le p^2$ there exists $\mathring{u}_m$ such that $\mathring{u}_m(B_1) = \hat{u}_m(B_1)$. For $2 \le m \le p^2$ let $\tilde{u}_m = \mathring{u}_m \hat{u}_m^{-1}$. Now we define the following permutation:

$$\begin{aligned} \alpha_1 \restriction C_1 &= id \\ \alpha_1 \restriction C_m &= \tilde{u}_m \text{ for } 2 \le m \le p^2. \end{aligned}$$

Clearly, for $2 \le m \le p^2$ we have $\tilde{u}_m(B_j) = B_j$ for at least one $B_j \subset C_m$. Since H_1 and H_2 are in the same Sylow p-subgroup of $Sym(p^3)$ the order of $\tilde{u}_m^{\mathcal{B}}$ is a power of p. We also have that C_m is the union of p elements of $\mathcal{B}$ for $1 \le m \le p^2$ hence $\alpha_1^{\mathcal{B}} = id$. We also have that $\alpha_1 \restriction C_m$ is the restriction of an automorphism of the graph Γ for $m = 1, \ldots p$. Therefore by Lemma 5 α_1 is an automorphism of the graph Γ.

Finally, Lemma 6 (b) gives $\mathring{g}^{\alpha_1} = \hat{g}$.

(d) Let us assume that the size of the connected components of Γ_0 and hence the size of the equivalence classes is p^2. Let $D'_0, D'_1, \ldots, D'_{p-1}$ denote the equivalence classes and let $D_m = \cup D'_m$ for $0 \le m \le p-1$.

Using Lemma 4 we get that $H_1 \cap H_2 \neq \{1\}$. Let z be an element of order p of $H_1 \cap H_2$ and we denote by z_1 and z_2 the element of $\hat{\mathbb{Z}}_p^3$ and $\mathring{\mathbb{Z}}_p^3$ such that $z_1^{\mathcal{B}} = z_2^{\mathcal{B}} = z$, respectively. Then $(z_2^{-i} z_1^i)^{\mathcal{B}} = id$ for $i = 1, \dots, p-1$.

Let us assume first that $z_1(D_0) \neq D_0$. We may assume that $z_1^i(D_0) = D_i$ for $i = 0, 1, \dots, p-1$. We define α_2 in the following way:

$$\begin{aligned} \alpha_2 \restriction D_0 &= id \\ \alpha_2 \restriction D_i &= z_2^i z_1^{-i} \text{ for } 1 \leq i \leq p-1. \end{aligned}$$

Since $z_1^{\mathcal{B}} = z_2^{\mathcal{B}} = z$ we have $\alpha_2^{\mathcal{B}} = id$. Using Lemma 5 again we get that $\alpha_2 \in Aut(\Gamma)$ and Lemma 6 gives $\mathring{g}^{\alpha_2} = \hat{g}$.

Therefore we may assume that $z_1(D_0) = D_0$. In this case the orbits of z give a $\langle H_1, H_2 \rangle$-invariant partition $\mathcal{E} = \{E_{a,b} \mid a, b \in \mathbb{Z}_p\}$ of $\mathcal{B}$. Using that the elements of $\mathcal{B} = V(\Gamma_0)$ can be identified with elements of $\mathbb{Z}_p^3$ we may assume that $E_{a,b}$ has the following form for every pair $(a, b) \in \mathbb{Z}_p^2$:

$$E_{a,b} = \{(a, b, c) \in \mathbb{Z}_p^3 \mid c \in \mathbb{Z}_p\}.$$

We may also assume that $D'_a = \cup_{b \in \mathbb{Z}_p} E_{a,b}$ for all $a \in \mathbb{Z}_p$.

Since H_1 acts regularly on Γ_0, there exists $h_1 \in H_1$ such that $h_1(E_{0,0}) = E_{0,1}$. Since H_2 is also regular, there exists $h_2 \in H_2$ such that $h_2(E_{0,0}) = h_1(E_{0,0})$. Since the order of h_1 and h_2 are p and $h_1(D'_0) = h_2(D'_0) = D'_0$ we have that $h_1(D'_i) = h_2(D'_i) = D'_i$ for $i = 0, \dots, p-1$.

We may assume that z, h_1 and h_2 act in the following way on $\mathbb{Z}_p^3$.

$$\begin{aligned} z(a, b, c) &= (a, b, c+1) \\ h_1(a, b, c) &= (a, b+1, c) \\ h_2(a, b, c) &= (a, b+s_a, c+t_{a,b}). \end{aligned}$$

The assumption that $h_1(E_{0,0}) = h_2(E_{0,0}) = E_{0,1}$ gives that $s_0 = 1$.

We claim that $s_a = 1$ for $1 \leq a \leq p-1$. Since H_2 is regular on Γ_0 there exists $k_2 \in H_2$ such that $k_2(0,0,0) = (a,0,0)$. Since h_2 and k_2 commute we have that $k_2(0, i, 0) = (a, s_a i, w_i)$ for some $w_i \in \mathbb{Z}_p$. If $s_a \neq 1$, then such an element cannot be in the Sylow p-subgroup P_1.

Therefore $h_2(a, b, c) = (a, b+1, c+t_{a,b})$ for all $(a, b, c) \in \mathbb{Z}_p^3$, where $t_{a,b} \in \mathbb{Z}_p$ only depends on a and b.

Lemma 7. *Let $a \neq a'$ be elements of $\mathbb{Z}_p$ and we fix two more elements b and b' of $\mathbb{Z}_p$. Then either $E_{a,b} \sim E_{a',b'}$ or $t_{a,b+n} = t_{a',b'+n}$ for all $n \in \mathbb{Z}_p$.*

Proof. For all $m \in \mathbb{Z}_p$ the permutation $h_2^m h_1^{-m}$ fixes $E_{a,b}$ and $E_{a',b'}$. Moreover,

$$\begin{aligned} h_2^m h_1^{-m}(a, b, c) &= (a, b, c + \sum_{i=1}^{n} t_{a,b-i}) \text{ and} \\ h_2^m h_1^{-m}(a', b', c) &= (a', b', c + \sum_{i=1}^{n} t_{a',b'-i}) \end{aligned} \tag{2}$$

One can see using Lemma 3 (b) that if $\sum_{i=1}^{n} t_{a,b-i} \neq \sum_{i=1}^{n} t_{a',b'-i}$ for some $m \in \mathbb{Z}_p$, then $E_{a,b} \sim E_{a',b'}$. If $\sum_{i=1}^{n} t_{a,b-i} = \sum_{i=1}^{n} t_{a',b'-i}$ for all $m \in \mathbb{Z}_p$, then $t_{a,b+n} = t_{a',b'+n}$ for $n \in \mathbb{Z}_p$. ∎

For each $a \in \mathbb{Z}_p$ we define the following function from $\mathbb{Z}_p$ to $\mathbb{Z}_p$:

$$t'_a(b) := t'_{a,b}.$$

Lemma 8. *Let us assume that* $t_a(b+n) = t'_a(b'+n)$ *for all* $n \in \mathbb{Z}_p$ *and we denote by* k_2 *the unique element of* H_2 *which maps* $(a, b, 0)$ *to* $(a', b', 0)$*. Then* $k_2(a, b+d, e) = (a', b'+d, e)$ *for all* $d, e \in \mathbb{Z}_p$*.*

Proof. Since k_2 and z commute we have $k_2(a, b, m) = (a', b', m)$ for all $m \in \mathbb{Z}_p$. We also have that k_2 and h_2 commute which gives $k_2(a, b+d, e) = (a', b'+d, e)$ for all $d, e \in \mathbb{Z}_p$. ∎

Corollary 1. *If the conditions of Lemma 8 hold and* k_1 *is the unique element of* H_1 *such that* $k_1(a, b, 0) = (a', b', 0)$*, then* $k_1 \restriction_{E_{a,b}} = k_2 \restriction_{E_{a,b}}$*.*

We define an equivalence relation on the set $\{D'_0, D'_1, \ldots, D'_{p-1}\}$. We write $D'_a \doteq D'_{a'}$ if and only if there exist b and b' in $\mathbb{Z}_p$ such that $t_{a,b+n} = t_{a',b'+n}$ for all $n \in \mathbb{Z}_p$.

Now we can choose a point $(a, b_a, 0)$ in every D'_a such that if $D_a \doteq D_{a'}$, then $t_{a,b_a+n} = t_{a',b_{a'}+n}$ for all $n \in \mathbb{Z}_p$. For every $1 \leq a \leq p-1$ there exist $\hat{v}_a \in \hat{\mathbb{Z}}_p^3$ and $\mathring{v}_a \in \mathring{\mathbb{Z}}_p^3$ such that $\hat{v}_a^{\mathcal{B}}(0, b_0, 0) = \mathring{v}_a^{\mathcal{B}}(0, b_0, 0) = (a, b_a, 0)$ since both H_1 and H_2 are regular.

Now we can define the following permutation:

$$\begin{aligned} \alpha_3 \restriction_{D_0} &= id \\ \alpha_3 \restriction_{D_a} &= \mathring{v}_a \hat{v}_a^{-1} \quad \text{for } 1 \leq a \leq p-1. \end{aligned}$$

Lemma 9. α_3 *is an automorphism of* Γ*.*

Proof. We prove that $\alpha_3^{\mathcal{B}}$ is an automorphism of the graph Γ_1. If $B_i \cup B_j$ is contained in D'_a for some $a \in \mathbb{Z}_p$, then α_3 is defined by the restriction of an automorphism of Γ. Therefore we only have to investigate those pairs B_i, B_j of points which are not in the same set D'_a for any $a \in \mathbb{Z}_p$.

Let us assume that $B_i \in E_{a,b}$ and $B_j \in E_{a',b'}$. By the definition of α_3, for every $c \in \mathbb{Z}_p$ at least one $E_{c,d}$ is fixed by $\alpha_3^{\mathcal{B}}$. Therefore $\alpha_3^{\mathcal{B}}$ fixes every set $E_{c,d}$ since the order of $\alpha_3^{\mathcal{B}} \restriction_{D'_c}$ is a power of p for every $c \in \mathbb{Z}_p$.

Let us assume first that $D_a \nsim D'_a$. Lemma 7 gives that B_i is connected to B_j if and only if $\alpha'_3(B_i)$ is connected to $\alpha'_3(B_j)$ since $E_{a,b} \sim E_{a',b'}$.

Let us now assume that $D'_a \sim D'_{a'}$. We denote by the pair $(\mathring{v}_a \hat{v}_a^{-1}, \mathring{v}_a \hat{v}_a^{-1})$ the restriction of the action of α_3 to $D'_a \cup D'_{a'}$. Since $\mathring{v}_a$ and $\hat{v}_a^{-1}$ are automorphisms of Γ the pair $((\mathring{v}_a \hat{v}_a^{-1})^{\mathcal{B}}, (\mathring{v}_{a'} \hat{v}_{a'}^{-1})^{\mathcal{B}})$ is an automorphism of the induced subgraph on $D'_a \cup D'_{a'}$ if and only $(id^{\mathcal{B}}, (\mathring{v}_a^{-1}\mathring{v}_{a'}\hat{v}_{a'}^{-1}\hat{v}_a)^{\mathcal{B}})$ is. Since both $\mathring{Z}_p^3$ and $\hat{Z}_p^3$ are abelian we have

$$\left(id^{\mathcal{B}}, (\mathring{v}_a^{-1}\mathring{v}_{a'}\hat{v}_{a'}^{-1}\hat{v}_a)^{\mathcal{B}}\right) = \left(id^{\mathcal{B}}, (\mathring{v}_{a'}\mathring{v}_a^{-1})^{\mathcal{B}}(\hat{v}_a\hat{v}_{a'}^{-1})^{\mathcal{B}}\right).$$

Clearly, $(\hat{v}_a\hat{v}_{a'}^{-1})^{\mathcal{B}}(a', b_{a'}, 0) = (a, b_a, 0)$ and $(\mathring{v}_{a'}\mathring{v}_a^{-1})^{\mathcal{B}}(a, b_a, 0) = (a', b_{a'}, 0)$. Using Corollary 1 we get that

$$\left(id^{\mathcal{B}}, (\mathring{v}_{a'}\mathring{v}_a^{-1})^{\mathcal{B}}(\hat{v}_a\hat{v}_{a'}^{-1})^{\mathcal{B}}\right) = \left(id^{\mathcal{B}}, id^{\mathcal{B}}\right)$$

which is clearly an automorphism on $D'_a \cup D'_{a'}$. This proves that $\alpha_3^{\mathcal{B}} \in Aut(\Gamma_1)$.

If $B_i \sim B_j$, then $\alpha_3(B_i) \sim \alpha_3(B_j)$ since $\alpha_3^{\mathcal{B}} \in Aut(\Gamma_1)$ thus $p_i \in B_i$ is connected to $p_j \in B_j$ if and only if $\alpha_3(p_i)$ is connected to $\alpha_3(p_j)$.

If $B_i \nsim B_j$, then there exists $a \in \mathbb{Z}_p$ such that B_i and $B_j \subset D_a$. Since α_3 is defined on D_a by an automorphism of Γ we have that $p_i \in B_i$ is connected to $p_j \in B_j$ if and only if $\alpha_3(p_i)$ is connected to $\alpha_3(p_j)$, finishing the proof of Lemma 9. ∎

Finally, one can see using Lemma 6 (b) that $\mathring{g}^{\alpha_3} = \hat{g}$.

4.3 Step 3

Let us assume that for the generators of the cyclic groups $\hat{g} \in \hat{\mathbb{Z}}_q$ and $\mathring{g} \in \mathring{\mathbb{Z}}_q$ we have $\mathring{g} = \hat{g}$.

Since $\mathring{g} = \hat{g}$ we have that $\hat{\mathbb{Z}}_p^3$ and $\mathring{\mathbb{Z}}_p^3$ are contained in $C_A(\hat{g})$. Using Sylow's theorem again we may assume that $\hat{\mathbb{Z}}_p^3$ and $\mathring{\mathbb{Z}}_p^3$ are in the same Sylow p-subgroup of $C_A(\hat{g})$. Using all these assumptions we prove the following Lemma.

Lemma 10. *(a)* $\mathring{\mathbb{Z}}_p^3 \times \mathring{\mathbb{Z}}_q \leq \hat{\mathbb{Z}}_q \wr Sym(p^3)$.

(b) If $\mathring{\mathbb{Z}}_p^3 \times \mathring{\mathbb{Z}}_q \leq \hat{\mathbb{Z}}_q \wr Sym(p^3)$, *then for every* $\mathring{u} \in \mathring{\mathbb{Z}}_p^3$ *we have* $(\mathring{u})_b = id$.

Proof. (a) $\mathring{\mathbb{Z}}_p^3 \times \mathring{\mathbb{Z}}_q \leq \hat{\mathbb{Z}}_q \wr Sym(p^3)$ since the elements of $\mathring{\mathbb{Z}}_p^3$ and $\hat{g}$ commute.

(b) Let $A' = A \cap \hat{\mathbb{Z}}_q \wr Sym(p^3)$. We have already assumed that $\mathring{\mathbb{Z}}_p^3$ and $\hat{\mathbb{Z}}_p^3$ lie in the same Sylow p-subgroup of A', which is generated by p^3 disjoint q-cycles. Let $\mathring{u}$ be an arbitrary element of $\mathring{\mathbb{Z}}_p^3$. For every $(b, s) \in \mathbb{Z}_p^3 \times \mathbb{Z}_q$ we have $\mathring{u}(b, s) = (c, s + t)$ for some $c \in \mathbb{Z}_p^3$ and $t \in \mathbb{Z}_q$, where t only depends on $\mathring{u}$ and b since $\mathring{u} \in \hat{\mathbb{Z}}_q \wr Sym(p^3)$. The permutation group $\hat{G}$ is transitive, hence there exist $\hat{u}_1, \hat{u}_2 \in \hat{\mathbb{Z}}_p$ such that $\hat{u}_1(0, s) = (b, s)$ and $\hat{u}_2(c, s + t) = (0, s + t)$. The order of $\hat{u}_2\mathring{u}\hat{u}_1$ is a power of p since $\hat{u}_2, \mathring{u}$ and $\hat{u}_1$ lie in a Sylow p-subgroup. Therefore $t = 0$ and hence $(\mathring{u})_b = id$.

∎

Lemma 10 says that for every $\mathring{u} \in \mathring{\mathbb{Z}}_p^3$ we have $(u)_b = id$. We use again the graph Γ_1 defined on $\mathcal{B}$. It is clear that H_1 and H_2 are regular subgroups in $Aut(\Gamma_1)$ and they are isomorphic to $\mathbb{Z}_p^3$. Since $\mathbb{Z}_p^3$ is a DCI$^{(2)}$-group [3] we have that there exists $\mu \in \langle H_1, H_2 \rangle^{(2)}$ such that $H_2^{\mu} = H_1$.

Let $\eta = \mu id_{\mathcal{B}}$ be an element of the wreath product $\mathbb{Z}_q \wr Sym(p^3)$. Clearly, $\eta \in \langle \hat{G}, \mathring{\mathbb{G}} \rangle^{(2)}$ and hence η is an automorphism of Γ_0, which conjugates $\mathring{\mathbb{Z}}_p^3$ to $\hat{\mathbb{Z}}_p^3$. Moreover, the base group part of η is the identity so $\eta \in C_A(\hat{g})$. This proves that $\mathring{G}^{\eta} = \hat{G}$, finishing the proof of Theorem 1.

References

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

[2] B. Alspach, T. D. Parsons, Isomorphism of Circulant graphs and digraphs, Discrete Mathematics **25** (1979) 97-108.

[3] B. Alspach, L. A. Nowitz, Elementary Proofs that Z_p^2 and Z_p^3 are CI-groups, Europ. J. Combinatorics **20** (1999), 607-617.

[4] L. Babai, P. Frankl, Isomorphism problem for a class of point-symmetric structures, Acta Math. Acad. Syi. Hungar. **29**, 329-336.

[5] L. Babai, P. Frankl, Isomorphisms of Cayley graphs I, in: Colloqzeria Mathematica Societatis János Bolyai, Vol. 18. Combinatorics, Keszthely, 1976, North-Holland, Amsterdam (1978) 35-52.

[6] D. Ž. Djoković, Acta Math. Acad. Sci. Hungar. **21** (1970), 267-270.

[7] E. Dobson, Isomorphism problem for Cayley graphs of $\mathbb{Z}_p^3$, Discrete Math. **147** (1995), 87-94.

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

[9] C. D. Godsil, On Cayley graph isomorphisms, Ars Combin. **15** (1983), 231-246.

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

[11] M. H. Klin and R. Poschel, 'The Konig problem, the isomorphism problem for cyclic graphs and the method of Schur rings', Algebraic methods in graph theory, Szeged, 1978, Colloquia Mathematica Societatis János Bolyai **25** (North-Holland, Amsterdam, 1981) 405-434.

[12] I. Kovács, M. Muzychuk, The group $\mathbb{Z}_{p^2} \times \mathbb{Z}_q$ is a CI-group, Comm. Alg. **37** (2009), 3500-3515.

[13] C. H. Li, Z. P. Lu, P. P. Pálfy, Further restrictions on the structure of finite CI-groups, J. Algebr. Comb, **26** (2007), 161-181.

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

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

[16] M. Muzychuk, An elementary Abelian group of large rank is not a CI-group, Discrete Math. **264(1-3)** (2003), 167-185.