Discrete Mathematics 309 (2009) 3393–3398

Contents lists available at ScienceDirect

Discrete Mathematics

journal homepage: www.elsevier.com/locate/disc

Note

CI-property of elementary abelian 3-groups

Pablo Spiga

Universitá degli Studi di Padova, Dipartimento di Matematica Pura ed Applicata, 35131 Via Trieste 63, Padova, Italy

ARTICLE INFO

Article history:
Received 31 May 2007
Received in revised form 5 August 2008
Accepted 6 August 2008
Available online 5 September 2008

Keywords:
Cayley graph
CI-group
Schur ring
2-closure

ABSTRACT

In this paper we are concerned with 3-groups. We prove that an elementary abelian 3-group of rank 5 is a $\mathrm{CI}^{(2)}$-group, and that an elementary abelian 3-group of rank greater than or equal to 8 is not a CI-group. In Section 4, we present a conjecture.

1. Introduction

We begin collecting in the next three paragraphs some definitions, and notations that are needed throughout the paper.

If X is a set, then 2^X denotes the power set of X. We use the acronym "rea" for "regular elementary abelian". We denote by $\xi(G)$, the centre of a group G and by $\gamma_i(G)$ the ith term of the lower central series of G, i.e. $\gamma_1(G) = G$ and $\gamma_i(G) = [\gamma_{i-1}(G), G]$ for every $i \geq 2$. We denote by $\mathrm{Sym}(\Omega)$ the symmetric group on the set Ω, and by $\mathrm{Sym}(n)$ the symmetric group on the set $\{1, \ldots, n\}$. Moreover, if Σ is a block system for the permutation group G on Ω, then G^Σ denotes the permutation group on Σ induced by G on the block system Σ. If V is a group and Ω is a set, then we denote by $\mathrm{Fun}(\Omega, V)$ the group, under point-wise multiplication, of all functions from Ω to V. Furthermore, if W is a permutation group on Ω, then W acts as an automorphism group on $\mathrm{Fun}(\Omega, V)$. Namely, if $f \in \mathrm{Fun}(\Omega, V)$ and $w \in W$, then f^w is the function in $\mathrm{Fun}(\Omega, V)$ mapping α into $f(\alpha^{w^{-1}})$. The group $U = \mathrm{Fun}(\Omega, V) \rtimes W$ is denoted by $V \,\mathrm{wr}_\Omega\, W$ and is called the *wreath product* of V and W. The subgroup $\mathrm{Fun}(\Omega, V)$ is called the *base group* of U. Finally, we recall that if V is a permutation group on Δ, then U has a natural action on $\Omega \times \Delta$. Namely, if $wf \in U$ and $(\alpha, \delta) \in \Omega \times \Delta$, then $(\alpha, \delta)^{wf} = (\alpha^w, \delta^{f(\alpha^w)})$. In this paper, the symbol $V \,\mathrm{wr}\, W$ denotes the wreath product of V by W, where W acts on itself by right multiplication.

Let G be a permutation group on Ω and σ be in $\mathrm{Sym}(\Omega)$. We say that σ is in the *2-closure* of G if for every $\alpha, \beta \in \Omega$, there exists $g \in G$ such that $(\alpha^\sigma, \beta^\sigma) = (\alpha^g, \beta^g)$, i.e. the permutation σ preserves the orbitals of G (the orbitals of G are the orbits of G in its action on $\Omega \times \Omega$). We denote by $G^{(2)}$ the set $\{\sigma \in \mathrm{Sym}(\Omega) \mid \sigma \text{ is in the 2-closure of } G\}$. It is easy to check that $G^{(2)}$ is the maximal (with respect to inclusion) subgroup of $\mathrm{Sym}(\Omega)$ preserving the orbitals of G, see [8]. We say that the group G is *2-closed* if $G = G^{(2)}$. We note that the automorphism group of a graph or digraph is a 2-closed group, see [8].

Let H be a group and S a subset of H. The Cayley digraph of H with connection set S, denoted $\mathrm{Cay}(H, S)$, is the digraph with vertex set H and edge set $\{(h_1, h_2) \mid h_2h_1^{-1} \in S\}$. Two Cayley digraphs $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$ are said to be *Cayley isomorphic* if there exists an element g in $\mathrm{Aut}\, H$ such that $S^g = T$. A subset S of a group H is said to be a CI-*subset* (or Cayley isomorphic subset) if for each $T \subseteq H$ the digraphs $\mathrm{Cay}(H, S)$ and $\mathrm{Cay}(H, T)$ are isomorphic if and only if they are Cayley isomorphic. Finally, a group H is said to be a CI-*group* if every subset of H is a CI-subset.

In this paper we are concerned with the classification of CI-groups, and so with the Cayley isomorphism problem for the class of digraphs. We refer the reader to the very detailed survey article [4] for most results on CI-groups. We remark that

E-mail address: spiga@math.unipd.it.

0012-365X/$ – see front matter
doi:10.1016/j.disc.2008.08.002

one of the core problems in the classification of CI-groups relies in understanding whether an elementary abelian p-group of rank n is a CI-group, see [4].

The following characterisation of CI-subsets was proved by Babai, and will be used extensively in this paper.

Lemma 1 *([1, Lemma 3.1]). The subset S of the group H is a* CI-*subset if and only if any two regular subgroups of* $\mathrm{Aut}(\mathrm{Cay}(H, S))$ *isomorphic to H are conjugate in* $\mathrm{Aut}(\mathrm{Cay}(H, S))$.

In [3] the authors proved that if H is a rea p-subgroup of rank n ($n \leq 4, p > 2$) of a 2-closed permutation group G, then any regular subgroup K of G isomorphic to H is conjugate to H in G. In particular, by Lemma 1, as the automorphism group of a digraph is a 2-closed group, we have that an elementary abelian p-group of rank less than or equal to 4 is a CI-group. Motivated by this result the authors of [3] gave the following definition, see [3, pp. 341].

Definition 1. The group H is said to be a $\mathrm{CI}^{(2)}$-group if for any 2-closed permutation group G on H containing the right regular permutation representation of H, we have that any two regular subgroups of G isomorphic to H are conjugate in G.

Clearly, if H is a $\mathrm{CI}^{(2)}$-group, then H is a CI-group. It is known that if an elementary abelian p-group of rank n is a $\mathrm{CI}^{(2)}$-group, then $n < 4p - 2$, see [6], and, if $n \leq 4$, then an elementary abelian p-group of rank n is a $\mathrm{CI}^{(2)}$-group, see [3]. It is interesting to point out that even if the class of $\mathrm{CI}^{(2)}$-groups is contained in the class of CI-groups, there is no known CI-group that is *not* a $\mathrm{CI}^{(2)}$-group.

In Sections 2 and 3 we improve, for elementary abelian 3-groups, the results in [3,6]. Namely, in Section 2 we prove the following theorem.

Theorem 1. *An elementary abelian 3-group of rank 5 is a* $\mathrm{CI}^{(2)}$*-group.*

We recall that, for classifying CI-groups, it is considered crucial to determine whether $\mathbb{Z}_p^5$ is a CI-group, see Section 8.4 and Problem 8.10 in [4]. In particular, Theorem 1 provides the first example of an odd elementary abelian p-group of rank 5 that is a $\mathrm{CI}^{(2)}$-group. This result might suggest that elementary abelian p-groups of rank 5 are $\mathrm{CI}^{(2)}$-groups.

In Section 3 we prove the following theorem.

Theorem 2. *An elementary abelian 3-group of rank greater than or equal to 8 is not a* CI*-group.*

Theorem 2 is the result of a refinement of the arguments which have already appeared in [6]. The technique used to prove Theorem 2 might be applied to get similar results for other odd primes, but only for $p = 3$ we managed to improve the upper bound on the rank of a Cayley isomorphic elementary abelian p-group given in [6] (we note that in [6] it was proved that an elementary abelian 3-group of rank greater than or equal to 10 is not a CI-group). We recall that the Sylow 3-subgroups of a CI-group are elementary abelian, see [4, Theorem 8.8]. Therefore a CI-group of 3-power order is an elementary abelian 3-group. Hence, by Theorems 1 and 2, to classify the CI-groups (and $\mathrm{CI}^{(2)}$-groups) of 3-power order it remains to study the elementary abelian 3-groups of rank 6 and 7.

Finally, in Section 4 we present a conjecture.

2. An elementary abelian 3-group of rank 5 is a $\mathrm{CI}^{(2)}$-group

Let G be a 2-closed group containing the right regular representation of a group H, we say that (G, H) has property $(*)$ if any two regular subgroups of G isomorphic to H are conjugate in G. In particular, a group H is a $\mathrm{CI}^{(2)}$-group if and only if (G, H) has property $(*)$ for every 2-closed group G containing the right regular representation of H. When H is a p-group, we have the following proposition.

Proposition 1. *Let H be a p-group. The group H is a* $\mathrm{CI}^{(2)}$*-group if and only if (G, H) has $(*)$ for any group of the form $G = N^{(2)}$, where N is a permutation p-group on H which normalises and contains the right regular representation of H.*

Proof. If H is a $\mathrm{CI}^{(2)}$-group, then any pair (G, H) has $(*)$ and so the forward implication holds. Vice versa, let G be a 2-closed group containing the right regular representation of H. We have to prove that (G, H) has $(*)$, i.e. two regular subgroups K_1, K_2 of G isomorphic to H, are conjugate in G.

Let P be a Sylow p-subgroup of G. Note that P is 2-closed (Sylow subgroups of a 2-closed group are 2-closed), see [8]. Now by Sylow's theorem there exist $x, y \in G$ such that $K_1^x, K_2^y \leq P$. In particular, it remains to prove that two regular subgroups of P isomorphic to H are conjugate in P, i.e. (P, H) has $(*)$. So, without loss of generality, we may assume $G = P$.

We may assume that K_1 is the right regular representation of H. Consider $N = N_G(K_1)$ and $\overline{G} = N^{(2)}$. We have $\overline{G} \subseteq G$ and, by hypothesis, $(\overline{G}, H)$ has $(*)$. We claim that $G = \overline{G}$. Deny it. Since G and $\overline{G}$ are p-groups, there exists $g \in N_G(\overline{G}) \backslash \overline{G}$. Now, K_1, K_1^g are two regular subgroups of $\overline{G}$ isomorphic to H, thus, there exists $x \in \overline{G}$, such that $K_1^{gx} = K_1$. Hence, $gx \in N_G(K_1) = N \subseteq \overline{G}$. Thus, $g \in \overline{G}$, a contradiction. This proves that $G = \overline{G}$. Since $(\overline{G}, H)$ has $(*)$, we have that (G, H) has $(*)$. The proposition is now proved. $\square$

The following proposition is rather technical but useful.

Proposition 2. *Let H be an elementary abelian p-group. Let G be a minimal (with respect to the inclusion) 2-closed p-group containing the right regular representation of H, such that (G, H) does not have $(*)$. Let Σ be a block system of G on H. If G^{Σ} contains a unique conjugacy class of rea subgroups, then G^{Σ} is regular.*

Proof. Assume G^{Σ} contains a unique conjugacy class of rea subgroups. We have to prove that G^{Σ} is regular. Denote by L the kernel of the permutation representation of G on Σ, i.e. $L = \{g \in G \mid \Delta^g = \Delta \text{ for every } \Delta \in \Sigma\}$. Since (G, H) does not have $(*)$, the group G contains two non-conjugate rea subgroups H_1, H_2. Now, $H_1^{\Sigma}, H_2^{\Sigma}$ are rea subgroups of G^{Σ}. By hypothesis on G^{Σ}, we have $(H_1^{\Sigma})^g = H_2^{\Sigma}$ for some $g \in G$. In other words, $(H_1L)^g = H_2L$. Set $\overline{G} = H_2L \subseteq G$. By Proposition 2.1(*ii*) in [3], the group $\overline{G}$ is 2-closed. The group $\overline{G}$ contains two non-conjugate rea subgroups, namely H_1^g and H_2. Thus $(\overline{G}, H)$ does not have $(*)$. By minimality of G, we have $G = \overline{G}$. Finally, $G^{\Sigma} = \overline{G}^{\Sigma} = (H_2L)^{\Sigma} = H_2^{\Sigma}$ is regular on Σ. The proof is complete. □

Before proving Theorem 1 we recall some definitions. Let G be a finite group, L be an abelian normal subgroup of G and W be a complement of L in G, i.e. $G = WL$ and $W \cap L = 1$. A function $\delta : W \to L$ is called a derivation from W to L if $(w_1w_2)^{\delta} = (w_1^{\delta})^{w_2} w_2^{\delta}$ for every $w_1, w_2 \in W$. The set of all derivations from W to L is written $\mathrm{Der}(W, L)$. There is a natural rule of addition of derivations, namely $w^{\delta_1+\delta_2} = w^{\delta_1}w^{\delta_2}$. With this binary operation $\mathrm{Der}(W, L)$ becomes an abelian group. If $l \in L$, we define a function $\delta_l : W \to L$ by the rule $w^{\delta_l} = [w, l] = w^{-1}w^l$. The function δ_l is a derivation. Such derivations are called inner. The set of all inner derivations is denoted by $\mathrm{Inn}(W, L)$, and is a subgroup of $\mathrm{Der}(W, L)$. We note that if Z is a central subgroup of G contained in L, then the group homomorphisms from W to Z are derivations from W to L. In particular $\mathrm{Hom}(W, Z)$ is a subgroup of $\mathrm{Der}(W, L)$. Therefore, using additive notation, we have $\mathrm{Inn}(W, L) + \mathrm{Hom}(W, Z)$ is a subgroup of $\mathrm{Der}(W, L)$.

Proof of Theorem 1. The proof of this theorem is entirely computational, see [2]. We explain what allowed us in succeeding in an exhaustive search on permutation groups on 3^5 symbols.

Step 1: Consider a rea 3-group H in $\mathrm{Sym}(243)$. Compute the normalizer A of H in $\mathrm{Sym}(243)$. Determine a set $\mathcal{S}'$ of representatives of the A-conjugacy classes of 3-subgroups of A containing H. We put an order $\prec$ in $\mathcal{S}'$, namely, $N_1 \prec N_2$ if $N_1 \leq N_2$ and $N_1^{(2)} = N_2^{(2)}$. Let $\mathcal{S}_1$ be the set of $\prec$-maximal elements in $\mathcal{S}'$. The set $\mathcal{S}_1$ turns out to have 219 elements.

Step 2: Compute the 2-closure of any group in the set $\mathcal{S}_1$ and store it in a set $\mathcal{S}_2$. There is a built-in function in `GAP` to perform this task. This operation is fairly fast for permutation groups of degree 243. We claim that to prove Theorem 1, it is enough to prove that (G, H) has $(*)$ for every G in $\mathcal{S}_2$. Indeed, by Proposition 1, it is enough to prove that (G, H) has $(*)$ for every 2-closed group G of the form $N^{(2)}$, where N is a permutation 3-group which normalizes and contains H. Now, by definition of A, the group N is a subgroup of A. Therefore, by definition of $\mathcal{S}'$ and $\mathcal{S}_1$, we get $N^g \prec M$ for some g in A and some M in $\mathcal{S}_1$. Clearly, $(N^{(2)}, H)$ has $(*)$ if and only if $((N^{(2)})^g, H) = (M^{(2)}, H)$ has $(*)$. Now, $M^{(2)}$ lies in $\mathcal{S}_2$ and so the claim is proved.

Step 3: We have to prove that G contains a unique conjugacy class of rea subgroups for every G in $\mathcal{S}_2$. There is a very efficient built-in command in `magma` for computing a set of representatives of rea subgroups of a permutation group G up to conjugation (`RegularSubgroups(`G`:IsElementaryAbelian)`). We noticed that this command can deal with groups up to 3^{16} elements. Therefore, if G lies in $\mathcal{S}_2$ and $|G| \leq 3^{16}$, then we can check with `magma` that (G, H) has $(*)$. We store the remaining groups in a set $\mathcal{S}_3$.

Step 4: In this paragraph, we partition the set $\mathcal{S}_3$ in two subsets: $\mathcal{S}_3'$ and $\mathcal{S}_4$. Let G be an element in $\mathcal{S}_2$. The group G is a 3-group, therefore G is a nilpotent group of class c_G, for some c_G. Since $\gamma_i(G)$ is a normal subgroup of G, the orbits of $\gamma_i(G)$ form a block system, Σ_i say, for the group G. We store the group G in the set $\mathcal{S}_3'$ if, for some i in $\{1, \ldots, c_G\}$, the group G^{Σ_i} is not a regular permutation group and G^{Σ_i} satisfies one of the following conditions:

(a) $|G^{\Sigma_i}| \leq 3^{16}$ and G^{Σ_i} has a unique conjugacy class of rea subgroups;
(b) G^{Σ_i} is a 2-closed permutation group on Σ_i.

We store the remaining groups in the set $\mathcal{S}_4$. We point out that it is computationally easy to compute all the ingredients needed to partition $\mathcal{S}_3$ in the required subsets. In fact, if $|G^{\Sigma_i}| \leq 3^{16}$, then we can use the built-in `magma` command described in Step 3 to check whether (a) holds. Furthermore, we can check with the built-in command described in Step 2 whether (b) holds. Also, we remark that in (a) and (b) the group G^{Σ_i} has a unique conjugacy class of rea subgroups. Indeed, if (a) holds, then by definition G^{Σ_i} has a unique conjugacy class of rea subgroups. If (b) holds, then H^{Σ_i} is an elementary abelian 3-subgroup of rank at most 4 of the 2-closed group G^{Σ_i}. By [3], the group H^{Σ_i} is a $\mathrm{CI}^{(2)}$-group, and so G^{Σ_i} contains a unique conjugacy class of rea subgroups.

We claim that (G, H) has $(*)$ for every group G in $\mathcal{S}_3$ if and only if (G, H) has $(*)$ for every group G in $\mathcal{S}_4$. In particular, in our case-by-case analysis, we can disregard the groups in $\mathcal{S}_3'$, and study only the groups in $\mathcal{S}_4$. Since $\mathcal{S}_4 \subseteq \mathcal{S}_3$, the forward implication is clear. Vice versa, assume that G is a minimal element in $\mathcal{S}_3'$ such that (G, H) does not have $(*)$ and let i be in $\{1, \ldots, c_G\}$ such that G^{Σ_i} is not regular. By Proposition 2, there exists a proper subgroup G' of G such that (G', H) does not have $(*)$. By minimality, the group G' lies in $\mathcal{S}_4$. Thus the claim is proved. We note that the set $\mathcal{S}_4$ has size 11.

Step 5: We recall that if G is a subgroup of $U = V \,\mathrm{wr}\, W$ containing $W\xi(U)$, for some elementary abelian 3-groups V, W, then (G, H) has $(*)$ if and only if

$$\mathrm{Der}(W, L) = \mathrm{Inn}(W, L) + \mathrm{Hom}(W, \xi(U)), \tag{†}$$

where $L = B \cap G$ and B is the base group of U (see Lemma 2 in [6]).

In particular, it is computationally easy to check whether a permutation group is a subgroup of $V \,\mathrm{wr}\, W$, for some elementary abelian 3-groups V, W. Furthermore, for these groups we checked through the `GAP`-command `OneCocycles`

(G, L) that (†) holds. Therefore, we can disregard this class of groups from our analysis, and put the remaining groups in a set $\mathcal{S}_5$. Now, we have $|\mathcal{S}_5| = 5$.

Step 6: Let G be in $\mathcal{S}_5$, Σ be the block system determined by the orbits of $\xi(G)$, $\pi : G \to \mathrm{Sym}(\Sigma)$ be the permutation representation of G on Σ and L be the kernel of π. We claim that if $|G^{\Sigma}| \leq 3^{16}$ and $|L||\Sigma| \leq 3^{16}$, then it is computationally feasible to check whether (G, H) has $(*)$. Indeed, since $|G^{\Sigma}| \leq 3^{16}$, using the `magma`-command `RegularSubgroups(`G^{Σ}`:IsElementaryAbelian)`, we can compute $H_1, \ldots, H_t$ the rea subgroups of G^{Σ} up to G-conjugation. Now, every rea subgroup of G is conjugate to a rea subgroup of $\overline{H_i} = \pi^{-1}(H_i)$, for some i (where $\pi^{-1}(H_i)$ denotes the preimage of H_i via the homomorphism π). So, to prove that (G, H) has $(*)$ it remains to prove that there exists an $\bar{i}$ such that for $i \neq \bar{i}$, the group $\overline{H_i}$ has no rea subgroups and $\overline{H_{\bar{i}}}$ has a unique conjugacy class of rea subgroups. Since $|\overline{H_i}| = |\Sigma||L| \leq 3^{16}$, we can check that with the `magma`-command `RegularSubgroups(`$\overline{H_i}$`:IsElementaryAbelian)`.

In $\mathcal{S}_5$ there are four groups with the required properties and, with the procedure described in the previous paragraph, it was proved that (G, H) has $(*)$. Now, we have only one group G left to check.

Step 7: Let Σ be the block system determined by the orbits of $\xi(G)$, $\pi : G \to \mathrm{Sym}(\Sigma)$ be the permutation representation of G on Σ and $\bar{L}$ be the kernel of π. It can be checked that $|\Sigma||\bar{L}| \leq 3^{16}$ and that G^{Σ} is a subgroup of $U = V \,\mathrm{wr}\, W$ containing $W\xi(U)$, for some elementary abelian 3-groups V, W. Let B be the base group of U and $L = B \cap G^{\Sigma}$. Using the `GAP`-command `OneCocycles` (G^{Σ}, L), we can see that G^{Σ} has three rea subgroups H_1, H_2, H_3 up to G-conjugation (we get H_1, H_2, H_3 through the `OneCocycles`-option `cocycleToComplement`). Now, every rea subgroup of G is conjugate to a rea subgroup of $\pi^{-1}(H_i)$, for $i = 1, 2, 3$. Since $|\pi^{-1}(H_i)| = |\Sigma||\bar{L}| \leq 3^{16}$, we can check with the `magma`-command `RegularSubgroups` that, up to relabelling the indices, $\pi^{-1}(H_1)$, $\pi^{-1}(H_2)$ have no rea subgroups, while $\pi^{-1}(H_3)$ has a unique conjugacy class of rea subgroups. This proves that (G, H) has $(*)$. Since there are no more groups to check, the proof is complete. □

3. An elementary abelian 3-group of rank 8 is not a CI-group

This section uses [6]. Before proving Theorem 2, we recall the definition of Schur ring and simple quantity. Let G be a finite group. We denote the group algebra of G over the field $\mathbb{Q}$ by $\mathbb{Q}G$. For $B \subseteq G$ we define $\underline{B}$ to be the sum $\sum_{b \in B} b$, elements of this form will be called simple quantities, see [7]. A subalgebra $\mathcal{A}$ of the group algebra $\mathbb{Q}G$, is called a Schur ring over G if the following conditions are satisfied:

(i) there exists a basis of $\mathcal{A}$ consisting of simple quantities $\underline{T_0}, \ldots, \underline{T_r}$;
(ii) $T_0 = \{1\}$, $\bigcup_{i=0}^{r} T_i = H$ and $T_i \cap T_j = \emptyset$ if $i \neq j$;
(iii) for each i there exists i' such that $T_{i'} = \{t^{-1} \mid t \in T_i\}$.

A subset S of G is said to be an $\mathcal{A}$-subset if $S = \cup_{i_j} T_{i_j}$ for some i_j.

To keep this section self-contained, we also recall the main construction and the main results in [6]. Let V and W be $\mathbb{F}_p$-vector spaces. From Section 1, we have that the group $U = V \,\mathrm{wr}\, W$ acts naturally on $W \times V$. Using additive notation, the action is given by $(w, v)^{xf} = (w + x, v + f(w + x))$. Denote by B the base group of U. If v lies in V, then the constant map f_v (the function mapping every element of W into v) lies in $\xi(U)$. We recall that $\xi(U) = \{f_v \mid v \in V\}$. In particular, $W\xi(U) \cong W \times V$. Also, as $W\xi(U)$ acts semiregulary on $W \times V$, we have that $W\xi(U)$ is a rea subgroup of U.

Let G be a subgroup of U containing the rea subgroup $W\xi(U)$ of U. We have $G = WL$, where $L = B \cap G$. The group G determines a map $H : W \to 2^V$ given by $w \mapsto H(w) = \{f(w) \mid f \in L, f(0) = 0\}$. Define

$$\mathrm{Hom}_H(W, V) = \{f : W \to V \mid f(w_1 + w_2) - f(w_1) - f(w_2) \in H(w_1) \cap H(w_2) \text{ for every } w_1, w_2 \in W, f(0) = 0\}.$$

Proposition 3 ([6, Lemma 4]). *$(G^{(2)}, W \times V)$ does not have $(*)$, if and only if, there exists $f \in \mathrm{Hom}_H(W, V)$ such that there exists no linear map Λ such that $(f + \Lambda)(w) \in H(w)$ for every $w \in W$.*

If $v \in V$, $w \in W$, then we denote by $(w, H(w) + v)$ the subset $\{(w, x + v) \mid x \in H(w)\}$ of $W \times V$. We recall that it was proved in [5] that the linear span of the simple quantities $\{\underline{(w, H(w) + v)}\}_{w \in W, v \in V}$ is a Schur ring $\mathcal{A}_H$ in the group algebra $\mathbb{Q}[W \times V]$ (the reader might use [5,7] for notation and terminology).

Now, let f be an element in $\mathrm{Hom}_H(W, V)$ and E be a subset of W such that there exists no linear function Λ such that $(f + \Lambda)(w) \in H(w)$ for every $w \in E$.

Proposition 4 ([6, Proposition 1]). *If S is an $\mathcal{A}_H$-subset such that*

$$\underline{(w, H(w))} \in \langle\langle \underline{S} \rangle\rangle \quad \text{for every } w \in E,$$

then S is not a CI*-subset of $W \times V$. In particular, $W \times V$ is not a* CI*-group ($\langle\langle \underline{S} \rangle\rangle$ denotes the Schur ring generated by $\underline{S}$).*

We recall that Propositions 3 and 4 were first proved, in a slightly different context, in [5].

If we identify V with the additive group of a finite field with $|V|$ elements, and we fix a basis $e_1, \ldots, e_k$ of W, then it is really convenient to represent the elements of $B = \mathrm{Fun}(W, V)$ as polynomials $f(x_1, \ldots, x_k) \in V[x_1, \ldots, x_k]$. For example, the polynomial $ax_1 + bx_1x_2^2$ represents the function in B mapping $\lambda_1 e_1 + \cdots + \lambda_k e_k$ into $a\lambda_1 + b\lambda_1\lambda_2^2$. In particular, it is well-known that under this representation, every function in B can be uniquely written as a polynomial $\sum_{i_1, \ldots, i_k} a_{i_1 \cdots i_k} x_1^{i_1} \cdots x_k^{i_k}$, with $i_j \leq p - 1$ for every i_j. It is easy to see that the elements of $\xi(U)$ correspond to the constant polynomials.

We note that under this correspondence it is easy to compute the commutator in U between an element f of B and a basis element e_i of W. We have

$$\begin{aligned}[e_i,f](x_1,\ldots,x_k) &= (f-f^{e_i})(x_1,\ldots,x_k)\\ &= f(x_1,\ldots,x_k)-f(x_1,\ldots,x_{i-1},x_i-1,x_{i+1},\ldots,x_k).\end{aligned}$$

For instance, $[e_2, ax_1+bx_1x_2^2] = ax_1+bx_1x_2^2-(ax_1+bx_1(x_2-1)^2) = 2bx_1x_2-bx_1$.

In the rest of this section, we prove Theorem 2 using Propositions 3 and 4.

Take W an elementary abelian 3-group of rank 3 with basis e_1, e_2, e_3. Consider V a field with 3^5 elements and with $\mathbb{F}_3$-basis $a_{12^2}, a_{13^2}, a_{2^23}, a_{2^23}$ and a_{123} (the labels used would be shortly clear). Take

$$f = a_{12^2}x_1x_2^2 + a_{13^2}x_1x_3^2 + a_{2^23}x_2^2x_3 + a_{23^2}x_2x_3^2 + a_{123}x_1x_2x_3.$$

Set $G = W(\xi(U)+[W,f])$. In particular, G is a subgroup of U containing the rea subgroup $W\xi(U)$ of U, furthermore, $L = B\cap G = \xi(U)+[W,f]$. We leave it to the reader to check that $[e_i,f]\equiv g_i \bmod \xi(U)$ and $[e_i,[e_j,f]]\equiv g_{ij} \bmod \xi(U)$, where the g_i's and the g_{ij}'s are defined in the following way:

$$\begin{aligned}
&g_1 = a_{12^2}x_2^2 + a_{13^2}x_3^2 + a_{123}x_2x_3,\\
&g_2 = 2a_{12^2}x_1x_2 + 2a_{2^23}x_2x_3 + a_{23^2}x_3^2 + a_{123}x_1x_3 + 2a_{12^2}x_1 + 2a_{2^23}x_3,\\
&g_3 = 2a_{13^2}x_1x_3 + a_{2^23}x_2^2 + 2a_{23^2}x_2x_3 + a_{123}x_1x_2 + 2a_{13^2}x_1 + 2a_{23^2}x_2,\\
&g_{11} = 0, \qquad g_{22} = 2a_{12^2}x_1 + 2a_{2^23}x_3, \qquad g_{33} = 2a_{13^2}x_1 + 2a_{23^2}x_2,\\
&g_{12} = 2a_{12^2}x_2 + a_{123}x_3, \qquad g_{13} = 2a_{13^2}x_3 + a_{123}x_2,\\
&g_{23} = 2a_{2^23}x_2 + 2a_{23^2}x_3 + a_{123}x_1.
\end{aligned}\tag{1}$$

We have

$$\begin{aligned}
&g_1 = 2x_2g_{12} + 2x_3g_{13},\\
&g_2 = 2x_1g_{12} + 2x_3g_{23} + (2x_2+1)g_{22},\\
&g_3 = 2x_1g_{13} + 2x_2g_{23} + (2x_3+1)g_{33}.
\end{aligned}$$

This says that, if $w\in W$, then

$$\begin{aligned}H(w) &= \{f(w)\mid f(0)=0, f\in L\} = \langle g_i(w), g_{ij}(w)\mid 1\le i\le j\le 3\rangle\\ &= \langle g_{ij}(w)\mid 1\le i\le j\le 3\rangle.\end{aligned}\tag{2}$$

Note that if $w = \lambda_1e_1+\lambda_2e_2+\lambda_3e_3$, then

$$f(w) = 2\lambda_2^2g_{22}(w) + 2\lambda_3^2g_{33}(w) + a_{123}\lambda_1\lambda_2\lambda_3.\tag{3}$$

So, $f(w)\equiv a_{123}\lambda_1\lambda_2\lambda_3 \bmod H(w)$.

Proof of Theorem 2. Since the class of CI-groups is closed under taking subgroups, it is enough to prove that an elementary abelian 3-group of rank 8 is not a CI-group.

Since the base group B is abelian, we have $[G,f] = [WL,f] = [W,f][L,f] = [W,f]\subseteq G$. Hence, f normalizes G. Now, this yields that $f\in \mathrm{Hom}_H(W,V)$. Set $E = \{e_1, e_2, e_3, e_1+e_2, e_1+e_3, e_2+e_3, e_1+e_2+e_3, e_1+e_2+2e_3, e_1+2e_2+e_3, 2e_1+e_2+e_3\}$. We claim that there exists no linear function Λ such that $(f+\Lambda)(w)\in H(w)$ for every $w\in E$. By Proposition 3, this yields that $W\times V$ is not a $\mathrm{CI}^{(2)}$-group.

Set $\bar{f} = a_{123}x_1x_2x_3$. By Eqs. (2) and (3), it is enough to prove that there exists no linear function Λ such that $(\bar{f}+\Lambda)(w)\in H(w)$ for every $w\in E$. Deny it, and let Λ be a linear function such that $(\bar{f}+\Lambda)(w)\in H(w)$ for every $w\in E$. The rest of the proof requires several linear algebra computations, we just give a sketch of the proof giving the fundamental ingredients.

Using Eqs. (1) and (2), we have $H(e_1) = \langle a_{12^2}, a_{13^2}, a_{123}\rangle$. Since $\bar{f}$ is zero in e_1, we have that $(\bar{f}+\Lambda)(e_1)$ lies in $H(e_1)$ if and only if $\Lambda(e_1)$ lies in $H(e_1)$. In other words, $\Lambda(e_1) = y_1a_{12^2}+y_2a_{13^2}+y_3a_{123}$, for some $y_1,y_2,y_3\in\mathbb{F}_3$. Repeating the same argument for the element e_2 and e_3 we have that

$$\begin{aligned}\Lambda = {}&(y_1a_{12^2}+y_2a_{13^2}+y_3a_{123})x_1 + (y_4a_{12^2}+y_5a_{2^23}+y_6a_{23^2}+y_7a_{123})x_2\\ &+(y_8a_{13^2}+y_9a_{2^23}+y_{10}a_{23^2}+y_{11}a_{123})x_3,\end{aligned}$$

for some $y_1,\ldots,y_{11}\in\mathbb{F}_3$.

Using again Eqs. (1) and (2), we get $H(e_1+e_2) = \langle a_{12^2}, a_{13^2}+a_{23^2}, a_{2^23}, a_{123}\rangle$. So, we have

$$(\bar{f}+\Lambda)(e_1+e_2) = (y_1+y_4)a_{12^2} + y_2a_{13^2} + y_5a_{2^23} + y_6a_{23^2} + (y_3+y_7)a_{123}.$$

In particular, $(\bar{f}+\Lambda)(e_1+e_2)\in H(e_1+e_2)$, if and only if, $y_2 = y_6$.

The latter paragraph shows that imposing that $(\bar{f}+\Lambda)(w)\in H(w)$, yields a linear equation in $y_1,\ldots,y_{11}$. The function f and the set E have been chosen so carefully that the resulting set of linear equations (one for each w in E) in $y_1,\ldots,y_{11}$ does not have any solution. This is a straightforward but fruitful job in linear algebra that we leave to the reader. In particular, this yields a contradiction and our claim is proved.

Now, we use Proposition 4 to prove that $W \times V$ is not a CI-group. Since $W \times V$ has rank 8, the proof would be complete. We use the same notation as in [5] for computations inside the group algebra $\mathbb{Q}[W \times V]$. Take

$$S = \{(0, a_{12^2}), (0, a_{2^23}), (0, a_{23^2}), (0, a_{123})\} \cup \bigcup_{w \in E} (w, H(w)).$$

Clearly, S is an $\mathcal{A}_H$-subset. We claim that

$$\underline{(w, H(w))} \in \langle\langle \underline{S} \rangle\rangle \quad \text{for every } w \in E. \tag{‡}$$

Let us compute the element $C = (\underline{S} + \underline{S}) \circ \underline{S}$ of $\langle\langle \underline{S} \rangle\rangle$. We leave it to the reader to check that

$$\begin{aligned} C = {} & 4\underline{(e_1, H(e_1))} \uplus 6\underline{(e_2, H(e_2))} \uplus 8\underline{(e_3, H(e_3))} \uplus 76\underline{(e_1 + e_2, H(e_1 + e_2))} \\ & \uplus 78\underline{(e_1 + e_3, H(e_1 + e_3))} \uplus 76\underline{(e_2 + e_3, H(e_2 + e_3))} \\ & \uplus 126\underline{(e_1 + e_2 + e_3, H(e_1 + e_2 + e_3))} \uplus 108\underline{(e_1 + e_2 + 2e_3, H(e_1 + e_2 + 2e_3))} \\ & \uplus 108\underline{(e_1 + 2e_2 + e_3, H(e_1 + 2e_2 + e_3))} \uplus 72\underline{(2e_1 + e_2 + e_3, H(2e_1 + e_2 + e_3))}. \end{aligned}$$

By Proposition 22.1 in [7] (known as Schur–Wielandt principle), we have $\underline{(e_1, H(e_1))}$, $\underline{(e_2, H(e_2))}$, $\underline{(e_3, H(e_3))}$ are in $\langle\langle \underline{S} \rangle\rangle$. This is clearly enough to get (‡). The proof is now complete. □

4. A conjecture

The problem of understanding CI-groups is related to the *isomorphism problem* of Cayley digraphs, i.e. understanding whether two given Cayley digraphs are isomorphic. Namely, if H is a CI-group, then $\mathrm{Cay}(H, T) \cong \mathrm{Cay}(H, S)$, if and only if, $T = S^\varphi$ for some $\varphi \in \mathrm{Aut}(H)$. In particular, we note that it is computationally easier checking whether two subsets T, S of H are conjugate in $\mathrm{Aut}(H)$, than checking whether $\mathrm{Cay}(H, T)$ is isomorphic to $\mathrm{Cay}(H, S)$. Therefore, for Cayley digraphs defined over a CI-group, the isomorphism problem has a clear answer. The drawback in dealing with CI-groups is that their group structure is not very rich, for example the rank of an elementary abelian p-group contained in a CI-group is bounded. In the hope of enlarging the class of Cayley digraphs where the isomorphism problem might be computationally "easy", we set the following problem.

Let H be an elementary abelian p-group of rank n. We define two equivalence relations $\sim_1$, $\sim_2$ on the power set of H. If S, T are subsets of H, then we say that $S \sim_1 T$ if $\mathrm{Cay}(H, S) \cong \mathrm{Cay}(H, T)$. Similarly, if S, T are subsets of H, then we say that $S \sim_2 T$ if $S^\varphi = T$, for some $\varphi \in \mathrm{Aut}\,H$. Let o_i be the number of $\sim_i$-equivalence classes, $i = 1, 2$. Note that if $S \sim_2 T$, then $S \sim_1 T$, i.e. $\sim_2$ is a refinement of $\sim_1$. In particular, $o_1 \leq o_2$. Define $f(p, n) = o_2 - o_1$. Note that $f(p, n) = 0$, if and only if, an elementary abelian p-group of rank n is a CI-group. It is interesting to study the behaviour of the function f. For example, if f turns out to be bounded by a function of the prime p, then it might be feasible to characterise explicitly the equivalence relation $\sim_1$ and so to understand when two Cayley digraphs defined over an elementary abelian p-group are isomorphic. Unfortunately, we make the following conjecture.

Conjecture. $\lim_{n\to\infty} f(p, n) = \infty$.

Acknowledgements

The author would like to thank Dr. Joy Morris for her continuous support concerning this paper. The author is also deeply indebted to the Department of Mathematics and Computer Science of the University of Lethbridge for the use of their computers. Also, the author thanks Prof. Mikhail Muzychuk for drawing his attention to the computational aspects of the CI-problem.

References

[1] L. Babai, Isomorphism problem for a class of point-symmetric structures, Acta Mathematica Academiae Scientia Hungarica 29 (1977) 329–336.
[2] The GAP Group, GAP — Groups, Algorithms, and Programming, Version 4.4, 2005. http://www.gap-system.org.
[3] M. Hirasaka, M. Muzychuk, An elementary abelian group of rank 4 is a CI-group, Journal of Combinatorial Theory Series A 94 (2001) 339–362.
[4] C.H. Li, On Isomorphisms of finite Cayley graphs — A survey, Discrete Mathematics 256 (2002) 301–334.
[5] M. Muzychuk, An elementary abelian group of large rank is not a CI-group, Discrete Mathematics 264 (2003) 167–185.
[6] P. Spiga, Elementary Abelian p-groups of rank greather than or equal to $4p-2$ are not CI-groups, Journal of Algebraic Combinatorics 27 (2007) 343–355.
[7] H. Wielandt, Finite Permutation Groups, Academic Press, Berlin, 1964.
[8] H. Wielandt, Permutation groups through invariant relations and invariant functions, Lecture Notes Ohio State University, 1969.