Journal of Combinatorial Theory, Series A 157 (2018) 162–204

Contents lists available at ScienceDirect

Journal of Combinatorial Theory, Series A

www.elsevier.com/locate/jcta

Elementary abelian groups of rank 5 are DCI-groups[☆]

Yan-Quan Feng[a], István Kovács[b]

[a] Department of Mathematics, Beijing Jiaotong University, Beijing 100044, PR China
[b] IAM and FAMNIT, University of Primorska, Glagoljaška 8, 6000 Koper, Slovenia

ARTICLE INFO

Article history:
Received 25 April 2017
Available online 7 March 2018

Keywords:
Cayley graph
Isomorphism
CI-group
2-Closed permutation group
Schur ring

ABSTRACT

In this paper, we show that the group $\mathbb{Z}_p^5$ is a DCI-group for any odd prime p, that is, two Cayley digraphs $\mathrm{Cay}(\mathbb{Z}_p^5, S)$ and $\mathrm{Cay}(\mathbb{Z}_p^5, T)$ are isomorphic if and only if $S = T^\varphi$ for some automorphism φ of the group $\mathbb{Z}_p^5$.

1. Introduction

Let H be a finite group and S be a subset of H. The *Cayley digraph* $\mathrm{Cay}(H, S)$ is the digraph that has vertex set H, and arc set $\{(x, sx) : x \in H, s \in S\}$. It follows from the definition that $\mathrm{Aut}(\mathrm{Cay}(H, S))$ contains H_R, the group of all *right translations* $H_R = \{h_R : h \in H\}$, where $x^{h_R} = xh$, $x \in H$. Also, $\mathrm{Cay}(H, S)$ is loopless if the identity

[☆] Y.-Q. Feng was supported in part by the National Natural Science Foundation of China (11571035, 11731002) and the 111 Project of China (B16002). I. Kovács was supported in part by the Slovenian Research Agency (research program P1-0285, and research projects N1-0032, N1-0038, J1-5433 and J1-6720) and is grateful to Beijing Jiaotong University for hospitality.

E-mail addresses: yqfeng@bjtu.edu.cn (Y.-Q. Feng), istvan.kovacs@upr.si (I. Kovács).

https://doi.org/10.1016/j.jcta.2018.02.003
0097-3165/© 2018 Elsevier Inc. All rights reserved.

element $1 \notin S$, and it is regarded as an undirected graph when S is an inverse-closed set, that is, $S = S^{-1} = \{x^{-1} : x \in S\}$.

Two Cayley digraphs $\mathrm{Cay}(H,S)$ and $\mathrm{Cay}(H,T)$ are called *Cayley isomorphic* if $T = S^{\varphi}$ for some automorphism $\varphi \in \mathrm{Aut}(H)$. It is trivial to show that Cayley isomorphic Cayley digraphs are isomorphic as digraphs. The converse, however, does not hold in general. There are examples of Cayley digraphs which are isomorphic but not Cayley isomorphic. A subset $S \subseteq H$ is called a *CI-subset* if for any $T \subseteq H$, the isomorphism $\mathrm{Cay}(H,T) \cong \mathrm{Cay}(H,S)$ implies that $T = S^{\varphi}$ for some $\varphi \in \mathrm{Aut}(H)$. The group H is a *DCI-group* if each of its subsets are CI-subsets, and a *CI-group* if each of its inverse-closed subsets are CI-subsets. Motivated by a problem posed by Ádám in [1], Babai and Frankl [4] asked the following question: Which are the CI-groups? Although the candidates of CI-groups have been reduced to a restricted list [9,18], which was obtained by accumulating the work of several mathematicians, it is considered to be difficult to confirm that a particular group is a CI-group. We refer the reader to the survey paper [17] for most results on CI- and DCI-groups.

One of the crucial steps towards the classification of all CI-groups is to answer which elementary abelian p-groups are CI-groups (see also [17, Question 8.3]). It is known that the group $\mathbb{Z}_p^n$ is a CI-group in each of the following cases: $n = 1$ [7,10,29]; $n = 2$ [2,12]; $n = 3$ [2,8]; $n = 4$ and $p = 2$ [5]; $n = 4$ and $p > 2$ [13] (a proof for $n = 4$ with no condition on p was given recently in [19]); $n = 5$ and $p = 2$ [5]; and $n = 5$ and $p = 3$ [27]. On the other hand, some examples of groups $\mathbb{Z}_p^n$ are also known which are not CI-groups, and in each case the rank $n \geq 6$. Nowitz [23] found a non-CI-subset of $\mathbb{Z}_2^6$, and more recently, Spiga [27] constructed a non-CI subset of $\mathbb{Z}_3^8$. Constructions of non-CI-subsets of $\mathbb{Z}_p^n$ where n is expressed as a function in p were the subject of the papers [20,25,26]. The best bound is due to Somlai [25], which says that $\mathbb{Z}_p^n$ is not a CI-group if $n \geq 2p+3$. The question whether $\mathbb{Z}_p^5$ is a CI-group for any odd prime p is mentioned in [17] as a crucial task for classifying CI-groups (see Section 8.4 and Problem 8.10). The goal of this paper is to complete this task by proving the following theorem:

Theorem 1.1. *The group $\mathbb{Z}_p^5$ is a DCI-group for any prime p.*

Our starting point is the following group theoretical criterion due to Babai [3]: A subset $S \subseteq H$ 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 $\mathrm{Aut}(\mathrm{Cay}(H,S))$. Recall that, the group H_R of right translations is always contained in $\mathrm{Aut}(\mathrm{Cay}(H,S))$. Motivated by this criterion, the following definition was introduced by Hirasaka and Muzychuk [13]: A permutation group $G \leq \mathrm{Sym}(\Omega)$ containing a fixed subgroup F is *F-transjugate* if for each $g \in \mathrm{Sym}(\Omega)$, the condition $g^{-1}Fg \leq G$ implies that $g^{-1}Fg$ and F and are conjugate in G. In this context, Babai's result can be rephrased as to say that a subset $S \subseteq H$ is a CI-subset if and only if the group $\mathrm{Aut}(\mathrm{Cay}(H,S))$ is H_R-transjugate. It is well-known that $\mathrm{Aut}(\mathrm{Cay}(H,S))$ is a 2-closed permutation group for any $S \subseteq H$ (for the definition of a 2-closed permutation group, see Section 2.1). Following [13], we say that H is a *$\mathrm{CI}^{(2)}$-group* if all 2-closed subgroups of $\mathrm{Sym}(H)$ containing H_R are H_R-transjugate. Clearly, if H is a $\mathrm{CI}^{(2)}$-group, then it is necessarily a DCI-group. Theorem 1.1 was proved by Conder and Li [5] for $p = 2$, hence it will be sufficient to consider only the case when p is odd. In fact, instead of Theorem 1.1 we prove the following slightly more general theorem:

Theorem 1.2. *The group $\mathbb{Z}_p^5$ is a $CI^{(2)}$-group for any odd prime p.*

We prove Theorem 1.2 following the so called S-ring approach (S-ring is the abbreviation of *Schur ring*, and for a definition, see Section 2.2). Roughly speaking, S-rings are certain subalgebras of the group algebra $\mathbb{Q}H$ which were introduced by Schur [24] in order to study permutation groups containing a regular subgroup isomorphic to H. The usage of S-rings in the investigation of CI-groups was proposed by Klin and Pöschel [14, 15]. For a concise survey on S-rings and their applications in combinatorics, we refer the reader to [21].

We finish the introduction with a brief outline of the paper: Section 2 contains preliminary material, especially, a thorough introduction to S-ring theory. We intend to keep our text as self-contained as possible. In Sections 3, we turn to S-rings over elementary abelian p-groups of arbitrary rank. In particular, an equivalent condition will be derived for the group $\mathbb{Z}_p^n$ to be a $\mathrm{CI}^{(2)}$-group in terms of its S-rings (Proposition 3.4). We remark that, this condition is obtained by combining together several results proved in [13,19, 26]. Based on this equivalence, Theorem 1.2 will be reformulated in a statement involving a particular class of S-rings over the group $\mathbb{Z}_p^5$ (Theorem 3.5). Then, in Section 4, we derive a property of S-rings over $\mathbb{Z}_p^4$ which will be needed when dealing with S-rings over $\mathbb{Z}_p^5$. The proof of Theorem 3.5 will be divided into two parts depending on whether the S-rings in question are decomposable or not (for a definition of a decomposable S-ring, see Section 2.2). The decomposable S-rings will be handled in Section 5, while the indecomposable ones in Section 6.

2. Preliminaries

All groups in this paper are finite. In this section we collect all concepts and facts needed in this paper.

2.1. Permutation groups

Let $G \le \mathrm{Sym}(\Omega)$ be a permutation group of a finite set Ω. For $\omega \in \Omega$, we denote by G_ω the *stabilizer* of ω in G, and by ω^G the *G-orbit* of ω. For a subset $\Delta \subseteq \Omega$ and permutation $\gamma \in \mathrm{Sym}(\Omega)$, we say that γ fixes Δ if $\Delta^\gamma = \Delta$, and that γ fixes Δ pointwise if $\omega^\gamma = \omega$ for all $\omega \in \Delta$. The *setwise stabilizer* and *pointwise stabilizer* of Δ in G will be denoted by $G_{\{\Delta\}}$ and G_Δ, resp., that is, $G_{\{\Delta\}} = \{g \in G : \Delta^g = \Delta\}$ and $G_\Delta = \{g \in G : \omega^g = \omega, \omega \in \Delta\}$. The set of all G-orbits is denoted by $\mathrm{Orb}(G, \Omega)$. Suppose that G is transitive on Ω. If $\delta = \{\Delta_1, \ldots, \Delta_n\}$ is a *block system* for G, then we write G_δ for the kernel of the action of G on δ, and G^δ for the permutation group of δ induced by G.

Two permutation groups $H, G \leq \mathrm{Sym}(\Omega)$ are said to be 2-*equivalent*, denoted by $H \approx_2 G$, if $\mathrm{Orb}(H, \Omega^2) = \mathrm{Orb}(G, \Omega^2)$, see [31]. The equivalence class of G contains a largest subgroup, which is called the 2-*closure* of G, denoted by $G^{(2)}$. The group G is called 2-*closed* if $G^{(2)} = G$.

Proposition 2.1. *For any $G \leq \mathrm{Sym}(\Omega)$, $Z(G) \leq Z(G^{(2)})$.*

Proof. Let $g_1 \in Z(G)$, $\gamma \in G^{(2)}$ and $\omega \in \Omega$. Since $\mathrm{Orb}(G, \Omega^2) = \mathrm{Orb}(G^{(2)}, \Omega^2)$, we have $(w, w^{g_1})^G = (w, w^{g_1})^{G^{(2)}}$, and so there exists $g \in G$, depending on w and w^{g_1}, such that $(w, w^{g_1})^g = (w, w^{g_1})^\gamma$. Then $\omega^{g_1\gamma} = \omega^{g_1 g} = \omega^{g g_1} = \omega^{\gamma g_1}$. As ω was chosen arbitrarily from Ω and γ from $G^{(2)}$, it follows that $g_1 \in Z(G^{(2)})$, hence $Z(G) \leq Z(G^{(2)})$, and the assertion follows. □

A transitive permutation group G and its 2-closure $G^{(2)}$ have the same block systems (see [31, Theorem 4.11]).

Proposition 2.2. ([13, Proposition 2.1]) *Let $G \leq \mathrm{Sym}(\Omega)$ be a transitive permutation group, and let δ be a block system for G. Then*

(i) $(G^{(2)})^\delta \leq (G^\delta)^{(2)}$.
(ii) If G is 2-closed and F^δ is 2-closed for some $F \leq G$, then FG_δ is also 2-closed.

The following statement is given as Exercise 5.8 in [31]. It also appears as 5.1. Proposition in the preprint [22], where the authors give a proof. Regarding the fact that [22] is a university preprint, we also present a proof.

Proposition 2.3. (cf. [31]) *If $G \leq \mathrm{Sym}(\Omega)$ is a p-group, then $G^{(2)}$ is also a p-group.*

Proof. If G is intransitive, then $G^{(2)}$ is a subdirect product of the 2-closures of the transitive components of G. Thus, it is sufficient to prove the theorem for transitive groups $G \leq \mathrm{Sym}(\Omega)$. Suppose to the contrary that G is a counterexample to the proposition whose order is the smallest possible. If G is abelian, then it is regular on Ω. By Proposition 2.1, $G^{(2)}$ centralizes G, and it follows that $G^{(2)} = G$. Thus, we may assume that G is non-abelian, and so $|G| \geq p^3$. The center $Z(G)$ is nontrivial. Let $P \leq Z(G)$ such that $|P| = p$, and let $g \in G^{(2)}$ be an element of order q for some prime $q \neq p$. Then $\mathrm{Orb}(P, \Omega)$ is a block system of G on Ω. Let us consider the natural action of G on $\mathrm{Orb}(P, \Omega)$. To simplify notation, we write $\delta = \mathrm{Orb}(P, \Omega)$. The permutation group $G^\delta \leq \mathrm{Sym}(\delta)$ induced by G is transitive on δ and has order less than $|G|$. By the minimality of G the group $(G^\delta)^{(2)}$ is a p-group. Thus $(G^{(2)})^\delta$ is also a p-group, see Proposition 2.2(i), which implies that g acts on δ as the identity permutation. Equivalently, g fixes any P-orbit $\Delta \in \delta$. By Proposition 2.1, $P \leq Z(G^{(2)})$, hence g centralizes P. This implies that g is semiregular on Δ. Since g has order q and $|\Delta| = p$, g fixes pointwise Δ, and as this is true for any $\Delta \in \delta$, g is the identity permutation of Ω, a contradiction. □

Proposition 2.4. ([13, Proposition 3.6(ii)]) *Let H be an abelian p-group whose order $|H| \geq p^3$, and let $G \leq \mathrm{Sym}(H)$ with $G \geq H_R$. If there exists a G_1-orbit T such that $|T| = p$ and $\langle T \rangle = H$, then $|G| = p \cdot |H|$.*

Finally, we recall a recent result of Morris [19]. Let $H \cong \mathbb{Z}_p^n$ for an arbitrary prime p. Assume that $G \leq \mathrm{Sym}(H)$ is a p-group such that

$$G = \left\langle H_R, \pi^{-1} H_R \pi \right\rangle \text{ for some } \pi \in \mathrm{Sym}(H).$$

Let P be a Sylow p-subgroup of $\mathrm{Sym}(H)$ with $G \leq P$. Then P is permutation isomorphic to the iterated wreath product $\mathbb{Z}_p \wr \cdots \wr \mathbb{Z}_p$ (n copies of $\mathbb{Z}_p$), and this shows that P admits block systems $\delta_0, \ldots, \delta_{n-1}$ such that δ_i has blocks of size p^{i+1}, and if $0 \leq i < j \leq n-1$, then each class of δ_i is contained in a class of δ_j. Since H_R is abelian, the kernel $(H_R)_{\delta_i}$ has order p^{i+1}. In particular, there exist τ_0, $\tau_1 \in H_R$ such that $(H_R)_{\delta_0} = \langle \tau_0 \rangle$ and $(H_R)_{\delta_1} = \langle \tau_0, \tau_1 \rangle$. Note that, we can write $\delta_0 = \mathrm{Orb}(\langle \tau_0 \rangle, H)$ and $\delta_1 = \mathrm{Orb}(\langle \tau_0, \tau_1 \rangle, H)$.

Proposition 2.5. ([19, Corollary 3.2]) *With the above notation, there exists $\psi \in G^{(2)}$ such that ψ commutes with τ_0, and $\psi^{-1}\pi^{-1} H_R \pi \psi$ contains τ_1.*

Let us consider once more the above groups $G = \langle H_R, \pi^{-1} H_R \pi \rangle$ and P, where P is a Sylow p-subgroup of $\mathrm{Sym}(H)$ with $G \leq P$. Then $Z(P) \leq \pi^{-1} H_R \pi$ because $\pi^{-1} H_R \pi$ is abelian and regular on H. Similarly, $Z(P) \leq H_R$. On the other hand, $P_{\delta_0} \lhd P$ and $\tau_0 \in P_{\delta_0}$, implying $P_{\delta_0} \cap Z(P) \neq 1$ because P is p-group. Then $P_{\delta_0} \cap Z(P) \leq H_R$ implies $P_{\delta_0} \cap Z(P) = \langle \tau_0 \rangle$, hence $\tau_0 \in P_{\delta_0} \cap Z(P) \leq \pi^{-1} H_R \pi$. Proposition 2.5 together with the condition that ψ centralizes τ_0 shows that $\tau_0, \tau_1 \in \psi^{-1}\pi^{-1} H_R \pi \psi$, and hence $|C_{H_R}(\psi^{-1}\pi^{-1} H_R \pi \psi)| \geq p^2$. This inequality will be used later.

2.2. S-rings

In this subsection, we give the definition of an S-ring, and review several basic properties. Let H be a finite group with identity element 1, and let $\mathbb{Q}H$ denote the group algebra of H over the rational number field. For a subset $T \subseteq H$, we define the $\mathbb{Q}H$-element $\underline{T}$ as the formal sum $\underline{T} = \sum_{h \in H} a_h h$ with $a_h = 1$ if $h \in T$, and $a_h = 0$ otherwise. We remark that the $\mathbb{Q}H$-element $\underline{T}$ is traditionally called *simple quantity*, see [30].

By a *Schur-ring* over H (*S-ring* for short) we mean a subalgebra $\mathcal{A} \subseteq \mathbb{Q}H$, which can be associated with a partition π of H satisfying the following conditions:

- The set $\{1\}$ belongs to π.
- For every $T \in \pi$, the set T^{-1} belongs to π.
- $\mathcal{A}$ is spanned by the $\mathbb{Q}H$-elements $\underline{T}$, $T \in \pi$.

The elements (classes) of π are also called the *basic sets* of $\mathcal{A}$, and from now on we will use the notation $\mathrm{Bsets}(\mathcal{A})$ for π. The cardinality $|\mathrm{Bsets}(\mathcal{A})|$ is called the *rank* of $\mathcal{A}$. The concept of S-ring is due to Wielandt [30], which was motivated by the following result of Schur [24]:

Theorem 2.6. (cf. [30, Theorem 24.1]) *Let H be a finite group, and let $G \leq \mathrm{Sym}(H)$ with $H_R \leq G$. Then the $\mathbb{Q}H$-elements $\underline{T}$, $T \in \mathrm{Orb}(G_1, H)$ span an S-ring over H.*

The S-ring in the above theorem is also called the *transitvity module* of G_1, denoted by $V(H, G_1)$. We note that, there exist S-rings which do not arise as transitivity modules. Given an arbitrary S-ring $\mathcal{A}$ over a group H, we say that $\mathcal{A}$ is *Schurian* if $\mathcal{A} = V(H, K_1)$ for some permutation group $K \leq \mathrm{Sym}(H)$ with $H_R \leq K$, and that $\mathcal{A}$ is *non-Schurian* otherwise.

Remark 2.7. It should be noted that the pair $(H, \{\mathrm{Cay}(H,T) : T \in \mathrm{Bsets}(\mathcal{A})\})$ forms a *Cayley (association) scheme* in the sense of [21]. Thus, S-ring theory can be regarded as a part of the theory of association schemes, and several concepts defined for S-rings can be understood in this context.

Let $\mathcal{A}$ be any S-ring over a group H. A subset $S \subseteq H$ (subgroup $K \leq H$, resp.) is called an $\mathcal{A}$-*subset* ($\mathcal{A}$-*subgroup*, resp.) if $\underline{S} \in \mathcal{A}$ ($\underline{K} \in \mathcal{A}$, resp.). The *radical* of a subset $S \subseteq H$ is the subgroup of H defined as

$$\mathrm{rad}(S) = \{h \in H : hS = Sh = S\}.$$

In other words, $\mathrm{rad}(S)$ is the largest subgroup $E \leq H$ for which S is equal to the union of some left E-cosets and also some right E-cosets. If S is an $\mathcal{A}$-subset, then both groups $\mathrm{rad}(S)$ and $\langle S \rangle$ are $\mathcal{A}$-subgroups (see [30, Propositions 23.5 and 23.6]). If $K, L \leq H$ are two $\mathcal{A}$-subgroups, then it can be easily checked that both $K \cap L$ and $\langle K \cup L \rangle$ are $\mathcal{A}$-subgroups. The *thin radical* of $\mathcal{A}$ is defined as

$$\mathbf{O}_\theta(\mathcal{A}) = \{g \in G : \{g\} \in \mathrm{Bsets}(\mathcal{A})\}.$$

The following simple, but useful property is a simple observation:

$$\text{If } e \in \mathbf{O}_\theta(\mathcal{A}) \text{ and } T \in \mathrm{Bsets}(\mathcal{A}), \text{ then both sets } eT \text{ and } Te \text{ are in } \mathrm{Bsets}(\mathcal{A}). \quad (1)$$

Here $eT = \{et : t \in T\}$ and $Te = \{te : t \in T\}$. It follows that the thin radical $\mathbf{O}_\theta(\mathcal{A})$ is an $\mathcal{A}$-subgroup.

Let $K \leq H$ be an $\mathcal{A}$-subgroup. Then, for any basic set $T \in \mathrm{Bsets}(\mathcal{A})$ there exist positive integers k and k' such that

$$|Kh \cap T| = k \text{ and } |hK \cap T| = k' \quad \text{for all } h \in T. \quad (2)$$

These can be verified by considering the products $\underline{K} \cdot \underline{T}$ and $\underline{T} \cdot \underline{K}$. Here and in what follows the symbol $\cdot$ denotes the multiplication of $\mathbb{Q}H$. Since both products belong to $\mathcal{A}$, these can be expressed as a linear combination of the simple quantities $\underline{T'}$, $T' \in \mathrm{Bsets}(\mathcal{A})$. The coefficient by $\underline{T}$ is equal to k in the case of $\underline{K} \cdot \underline{T}$, and it is equal to k' in the case of $\underline{T} \cdot \underline{K}$.

The subalgebra $\mathbb{Q}K \cap \mathcal{A}$ is an S-ring over an $\mathcal{A}$-subgroup K, denoted by $\mathcal{A}_K$, which is called the *S-subring of $\mathcal{A}$ induced by K.*

Assume, in addition, that $K \trianglelefteq H$ for an $\mathcal{A}$-subgroup K. For a subset $S \subseteq H$, we let $S/K = \{Kh,\ h \in S\}$. Let $T_1, T_2 \in \mathrm{Bsets}(\mathcal{A})$ such that $KT_1 \cap KT_2 \neq \emptyset$, or equivalently, $k_1t_1 = k_2t_2$ holds for some $k_i \in K$ and $t_i \in T_i$ $(i = 1, 2)$. This shows that, the coefficient $a_{T_1} > 0$ by the linear combination $\underline{K} \cdot \underline{T_2} = \sum_{T \in \mathrm{Bsets}(\mathcal{A})} a_T \underline{T}$. This implies that $T_1 \subseteq KT_2$, and hence $KT_1 \subseteq KT_2$. Similarly, $b_{T_2} > 0$ by $\underline{K} \cdot \underline{T_1} = \sum_{T \in \mathrm{Bsets}(\mathcal{A})} b_T \underline{T}$, hence $T_2 \subseteq KT_1$, and so $KT_2 \subseteq KT_1$ also holds. We conclude that $KT_1 = KT_2$, and thus the sets $KT, T \in \mathrm{Bsets}(\mathcal{A})$ form a partition of H, and consequently, the sets T/K, $T \in \mathrm{Bsets}(\mathcal{A})$ form a partition of H/K. The corresponding $\mathbb{Q}\, H/K$-elements $\underline{T/K}$ span an S-ring over H/K, which is called the *quotient of $\mathcal{A}$ by K,* denoted by $\mathcal{A}_{H/K}$.

Assume that $H = E \times F$ is the internal direct product of its subgroups E and F, and that $\mathcal{A}$ is an S-ring over H such that both E and F are $\mathcal{A}$-subgroups. Since $E \cap F = \{1\}$, it follows that $\underline{XY} = \underline{X} \cdot \underline{Y}$ for any subsets $X \subseteq E$ and $Y \subseteq F$. A straightforward computation yields that the simple quantities $\underline{RS}$, $R \in \mathrm{Bsets}(\mathcal{A}_E)$, $S \in \mathrm{Bsets}(\mathcal{A}_F)$ span an S-ring over H. The latter S-ring is called the *tensor product* of $\mathcal{A}_E$ with $\mathcal{A}_F$, denoted by $\mathcal{A}_E \otimes \mathcal{A}_F$. Clearly, $\mathcal{A}_E \otimes \mathcal{A}_F = \mathcal{A}_F \otimes \mathcal{A}_E$, and $\mathcal{A}_E \otimes \mathcal{A}_F \subseteq \mathcal{A}$. The following lemma can be easily shown using Eq. (1).

Lemma 2.8. *Let $\mathcal{A}$ be an S-ring of the internal direct product $H = E \times F$ such that both E and F are $\mathcal{A}$-subgroups. If $\mathcal{A}_E = \mathbb{Q}E$ or $\mathcal{A}_F = \mathbb{Q}F$, then $\mathcal{A} = \mathcal{A}_E \otimes \mathcal{A}_F$.*

The following result is also known as Schur's first theorem on multipliers (see [21]).

Theorem 2.9. (cf. [30, Theorem 23.9(a)]) *Let $\mathcal{A}$ be an S-ring over an abelian group H, $T \in \mathrm{Bsets}(\mathcal{A})$ be any basic set, and suppose that k is an integer coprime to $|H|$. Then the set $T^{(k)} := \{h^k : h \in T\}$ is a basic set of $\mathcal{A}$.*

Finally, we recall the concept of *E/F-wreath product* after [21]. This was defined in [16] under the name *wedge product*, and independently in [11] under the name *generalized wreath product*. Let $\mathcal{A}$ be an S-ring over a group H. If there exist $\mathcal{A}$-subgroups E and F such that

$$F \leq E,\ F \lhd H, \text{ and } F \leq \mathrm{rad}(T) \text{ for all } T \in \mathrm{Bsets}(\mathcal{A}), T \subset H \setminus E,$$

then we say that $\mathcal{A}$ is an *E/F-wreath product* and write $\mathcal{A} = \mathcal{A}_E \wr_{E/F} \mathcal{A}_{H/F}$. Note that, the S-ring $\mathcal{A}$ can be reconstructed uniquely from the S-rings $\mathcal{A}_E$ and $\mathcal{A}_{H/F}$. In the particular case when $E = F$, we use term *wreath product*, and write $\mathcal{A}_E \wr \mathcal{A}_{H/E}$ for

$\mathcal{A}_E \wr_{E/E} \mathcal{A}_{H/E}$. In what follows we say that $\mathcal{A}$ is *decomposable* if it can be decomposed as $\mathcal{A} = \mathcal{A}_E \wr_{E/F} \mathcal{A}_{H/F}$ where $E \neq H$ and $F \neq \{1\}$, and that $\mathcal{A}$ is *indecomposable* otherwise.

2.3. Automorphisms of S-rings

Let $\mathcal{A} \subseteq \mathbb{Q}H$ be an S-ring over a group H. By an *automorphism* of $\mathcal{A}$ we mean a permutation of H that is an automorphism of all Cayley graphs $\mathrm{Cay}(H, T)$, $T \in \mathrm{Bsets}(\mathcal{A})$. This definition is due to Klin and Pöschel [14] (see also [21]). The group of all automorphisms of $\mathcal{A}$ will be denoted by $\mathrm{Aut}(\mathcal{A})$, that is,

$$\mathrm{Aut}(\mathcal{A}) = \bigcap_{T \in \mathrm{Bsets}(\mathcal{A})} \mathrm{Aut}(\mathrm{Cay}(H, T)).$$

In what follows, we write $\mathrm{Aut}(\mathcal{A})_1$ for the stabilizer $(\mathrm{Aut}(\mathcal{A}))_1$. Note that, as a permutation group of H, $\mathrm{Aut}(\mathcal{A})$ is 2-closed. Moreover, if $\mathcal{A} = V(H, G_1)$ for some $G \leq \mathrm{Sym}(H)$ with $G \geq H_R$, then $\mathrm{Aut}(V(H, G_1)) = G^{(2)}$. If $K \leq G$ is a subgroup with $H_R \leq K$, then $V(H, K_1) \supseteq V(H, G_1)$. Also, given two S-rings $\mathcal{A}$ and $\mathcal{B}$ of the same group H, the inequality $\mathcal{B} \subseteq \mathcal{A}$ implies that $\mathrm{Aut}(\mathcal{B}) \geq \mathrm{Aut}(\mathcal{A})$.

For two arbitrary S-rings $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Q}H$, their intersection $\mathcal{A} \cap \mathcal{B}$ is also an S-ring over H (cf. [13,21]). Therefore, given any subset $S \subset H$, it is possible to define the S-ring $\langle\langle S \rangle\rangle := \cap_{\mathcal{A}^*} \mathcal{A}^*$, where $\mathcal{A}^*$ runs over the set of all S-rings over H that contain $\underline{S}$. Then, the following identity holds:

$$\mathrm{Aut}(\mathrm{Cay}(H, S)) = \mathrm{Aut}(\langle\langle S \rangle\rangle). \tag{3}$$

Indeed, let $G = \mathrm{Aut}(\mathrm{Cay}(H, S))$ and $\mathcal{A} = V(H, G_1)$. The fact that $G \geq \mathrm{Aut}(\langle\langle S \rangle\rangle)$ follows if we observe that S can be expressed as $S = \cup_{i=1}^k T_i$ for some basic sets $T_i \in \mathrm{Bsets}(\langle\langle S \rangle\rangle)$, and thus $\mathrm{Aut}(\langle\langle S \rangle\rangle) \leq \bigcap_{i=1}^k \mathrm{Aut}(\mathrm{Cay}(H, T_i)) \leq G$. On the other, since G is 2-closed, $G = \mathrm{Aut}(\mathcal{A})$. Also, as any element of G_1 maps S to itself, it follows that $\underline{S} \in \mathcal{A}$. This implies in turn that $\langle\langle S \rangle\rangle \subseteq \mathcal{A}$, and so $\mathrm{Aut}(\langle\langle S \rangle\rangle) \geq \mathrm{Aut}(\mathcal{A}) = G$, and Eq. (3) follows.

Suppose that $K \leq H$ is an $\mathcal{A}$-subgroup and write $G = \mathrm{Aut}(\mathcal{A})$. Then any element of the stabilizer G_1 maps K to itself. This implies that the setwise stabilizer $G_{\{K\}}$ factorizes as $G_{\{K\}} = G_1 K_R$. In particular, $G_1 \leq G_{\{K\}}$, and hence the $G_{\{K\}}$-orbit of 1 is a block for G (see [6, Theorem 1.5A]). The latter orbit is K, and we conclude that the induced block system $\delta = \{K^g : g \in G\}$ is equal to the set H/K of all right cosets of K in H.

Finally, we point out a relation between $\mathrm{Aut}(\mathcal{A})$ and the thin radical $\mathbf{O}_\theta(\mathcal{A})$. For $h \in H$, the *left translation* $h_L \in \mathrm{Sym}(H)$ is the permutation acting as $x^{h_L} = h^{-1}x$, $x \in H$. If $\mathcal{A}$ is a Schurian S-ring over H, then its thin radical $\mathbf{O}_\theta(\mathcal{A})$ satisfies the following:

$$\mathbf{O}_\theta(\mathcal{A}) = \{h \in H : h_L \in C_{\mathrm{Sym}(H)}(\mathrm{Aut}(\mathcal{A}))\}. \tag{4}$$

Indeed, if $h \in \mathbf{O}_\theta(\mathcal{A})$ then every $g \in \mathrm{Aut}(\mathcal{A})$ acts as an automorphism of $\mathrm{Cay}(H, \{h\})$. It is straightforward to check that this implies that g and $(h^{-1})_L$ commute, and so

$h_L \in C_{\mathrm{Sym}(H)}(\mathrm{Aut}(\mathcal{A}))$. On the other hand, if $h_L \in C_{\mathrm{Sym}(H)}(\mathrm{Aut}(\mathcal{A}))$ and $g \in \mathrm{Aut}(\mathcal{A})_1$, then $(h^{-1})^g = 1^{h_L g} = 1^{g h_L} = h^{-1}$. Therefore, the orbit of h^{-1} under $\mathrm{Aut}(\mathcal{A})_1$ is equal to the set $\{h^{-1}\}$. Now, since $\mathcal{A}$ is Schurian, its basic sets are the $\mathrm{Aut}(\mathcal{A})_1$-orbits on H, in particular, $h^{-1} \in \mathbf{O}_\theta(\mathcal{A})$, and this implies that $h \in \mathbf{O}_\theta(\mathcal{A})$ as well.

2.4. Isomorphisms of S-rings

Let $\mathcal{A}$ be an S-ring over a group H and $\mathcal{B}$ be an S-ring over a group K. A bijection $f : H \to K$ is called an *(combinatorial) isomorphism* between $\mathcal{A}$ and $\mathcal{B}$ if

$$\big\{\, \mathrm{Cay}(H,T)^f : T \in \mathrm{Bsets}(\mathcal{A}) \big\} = \big\{\, \mathrm{Cay}(K,S) : S \in \mathrm{Bsets}(\mathcal{B}) \big\}.$$

Here $\mathrm{Cay}(H,T)^f$ is the image of the digraph $\mathrm{Cay}(H,T)$ under f, that is, it has vertex set K and arc set $\{(x^f, y^f) : x, y \in H \text{ and } yx^{-1} \in T\}$.

It follows from the definition that f induces a bijection $f^* : \mathrm{Bsets}(\mathcal{A}) \to \mathrm{Bsets}(\mathcal{B})$ defined by $T^{f^*} = S$ for $T \in \mathrm{Bsets}(\mathcal{A})$ exactly when $\mathrm{Cay}(H,T)^f = \mathrm{Cay}(K,S)$. We say that f is *normalized* if f maps the identity element 1_H to the identity element 1_K. In the special case when f is an isomorphism from H to K, we call f a *Cayley isomorphism.* Notice that, when f is a normalized isomorphism of $\mathcal{A}$, then $T^{f^*} = T^f$ holds for all $T \in \mathrm{Bsets}(\mathcal{A})$. It is well-known that the linear map defined by $\underline{T} \mapsto \underline{T^{f^*}}$ is an algebra isomorphism between the $\mathbb{Q}$-algebras $\mathcal{A}$ and $\mathcal{B}$ (cf. also [13,21]). Using this fact, it is not hard to show that $(ST)^f = S^f T^f$ holds for any normalized isomorphism f of $\mathcal{A}$ and any basic sets $S, T \in \mathrm{Bsets}(\mathcal{A})$. Some properties are listed below.

Proposition 2.10. ([13, Proposition 2.7]) *Let $f : \mathcal{A} \to \mathcal{B}$ be a normalized isomorphism from an S-ring $\mathcal{A}$ over a group H to an S-ring $\mathcal{B}$ over a group K, and let $E \le H$ be an $\mathcal{A}$-subgroup. Then,*

- *(i) the image E^f is a $\mathcal{B}$-subgroup of K. Moreover, the restriction $f_E : E \to E^f$ is an isomorphism between $\mathcal{A}_E$ and $\mathcal{A}_{E^f}$.*
- *(ii) For each $h \in H$, $(Eh)^f = E^f h^f$.*
- *(iii) If $E \trianglelefteq H$ and $E^f \trianglelefteq K$, then the mapping $f^{H/E} : H/E \to K/E^f$, defined by $(Eh)^{f^{H/E}} := E^f h^f$ is a normalized isomorphism between $\mathcal{A}_{H/E}$ and $\mathcal{B}_{K/E^f}$.*

In this paper, we will be interested exclusively in isomorphisms between S-rings over the same group H. We adopt the notation used in [13], and denote by $\mathrm{Iso}(\mathcal{A})$ the set of all isomorphisms from $\mathcal{A}$ to S-rings over H, that is,

$$\mathrm{Iso}(\mathcal{A}) = \{f \in \mathit{Sym}(H) : f \text{ is an isomorphism from } \mathcal{A} \text{ onto an S-ring over } H\};$$

and let $\mathrm{Iso}_1(\mathcal{A}) = \{f \in \mathrm{Iso}(\mathcal{A}) : 1^f = 1\}$.

Note that, $\mathrm{Iso}(\mathcal{A}) \subseteq \mathrm{Sym}(H)$, but it is not necessarily a subgroup. It follows from the definition that for any $\gamma \in \mathrm{Aut}(\mathcal{A})$ and $\psi \in \mathrm{Aut}(H)$, their product $\gamma\psi$ is an isomorphism from $\mathcal{A}$ to an S-ring over H. Therefore, $\mathrm{Aut}(\mathcal{A})\,\mathrm{Aut}(H) \subseteq \mathrm{Iso}(\mathcal{A})$. Now, we say that $\mathcal{A}$ is a *CI-S-ring* or simply that $\mathcal{A}$ is CI, if $\mathrm{Iso}(\mathcal{A}) = \mathrm{Aut}(\mathcal{A})\,\mathrm{Aut}(H)$. This definition was given by Hirasaka and Muzychuk in [13], where the following proposition was proved:

Proposition 2.11. ([13, Theorem 2.6]) *Let $G \le \mathrm{Sym}(H)$ be a 2-closed group with $H_R \le G$, and let $\mathcal{A} = V(H, G_1)$. Then the following conditions are equivalent:*

(i) *G is H_R-transjugate.*
(ii) $\mathrm{Iso}(\mathcal{A}) = \mathrm{Aut}(\mathcal{A})\,\mathrm{Aut}(H)$.
(iii) $\mathrm{Iso}_1(\mathcal{A}) = \mathrm{Aut}(\mathcal{A})_1\,\mathrm{Aut}(H)$.

Thus, the $\mathrm{CI}^{(2)}$-property for a group H is equivalent to the CI-property for all Schurian S-rings over H. In the last lemma of this subsection we collect further properties of S-ring isomorphisms.

Lemma 2.12. *Let $\mathcal{A}$ be an S-ring over a group H, and let $f \in \mathrm{Iso}_1(\mathcal{A})$.*

(i) *If H is abelian and $T^f = T$ for some $T \in \mathrm{Bsets}(\mathcal{A})$, then $(T^{(k)})^f = T^{(k)}$ for any integer k coprime to $|H|$.*
(ii) *Let $E \le H$ be an $\mathcal{A}$-subgroup such that $E \le \mathrm{rad}(T)$ for some $T \in \mathrm{Bsets}(A)$. If $(TE)^f = TE$ then $T^f = T$.*

Proof. (i): Since $T^f = T$, $f \in \mathrm{Aut}(\mathrm{Cay}(H,T))$. Let us consider the S-ring $\langle\langle T \rangle\rangle$. By Eq. (3), $f \in \mathrm{Aut}(\langle\langle T \rangle\rangle)$. On the other hand, by Theorem 2.9, $T^{(k)} \in \mathrm{Bsets}(\langle\langle T \rangle\rangle)$, and (i) follows.

(ii): This follows from $(TE)^f = TE$ and $ET = TE = T$ as $E \le \mathrm{rad}(T)$. □

2.5. p-S-rings

We say that an S-ring $\mathcal{A}$ over a group H is a *p-S-ring* if H is a p-group, and all basic sets $T \in \mathrm{Bsets}(\mathcal{A})$ have p-power size, see [13]. The following proposition follows from results about p-schemes proved in [32] (see [13, Theorem 3.3]). For sake of easier reading, we give a proof using only the definition of an S-ring.

Proposition 2.13. *Let $\mathcal{A}$ be a p-S-ring over a p-group H. Then*

(i) *the thin radical $\mathbf{O}_\theta(\mathcal{A})$ is nontrivial;*
(ii) *there exists a chain of $\mathcal{A}$-subgroups*

$$H_0 = \{1\} < H_1 < \cdots < H_r = H,$$

such that $|H_{i+1} : H_i| = p$ for all $i \in \{0, \ldots, r-1\}$.

Table 1
p-S-rings over $\mathbb{Z}_p^3$ for an odd prime p.

No.	p-S-ring	Schurity	Indecomposability
1.	$\mathbb{Q}\mathbb{Z}_p^3$	yes	yes
2.	$\mathbb{Q}\mathbb{Z}_p^2 \wr \mathbb{Q}\mathbb{Z}_p$	yes	no
3.	$\mathbb{Q}\mathbb{Z}_p \wr \mathbb{Q}\mathbb{Z}_p^2$	yes	no
4.	$(\mathbb{Q}\mathbb{Z}_p \wr \mathbb{Q}\mathbb{Z}_p) \otimes \mathbb{Q}\mathbb{Z}_p$	yes	no
5.	$\mathbb{Q}\mathbb{Z}_p \wr \mathbb{Q}\mathbb{Z}_p \wr \mathbb{Q}\mathbb{Z}_p$	yes	no
6.	$V(\mathbb{Z}_p^3, \langle x \rangle)$, $x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$	yes	yes

Proof. By definition, $\sum_{T \in \mathrm{Bsets}(\mathcal{A}), T \neq \{1\}} |T| = |H| - 1$. Since all cardinality $|T|$ as well as $|H|$ are p-powers, (i) follows.

We prove (ii) by induction on $|H|$. The statement is trivial for $|H| = p$. For the rest of the proof it is assumed that $|H| > p$. Choose a maximal nontrivial $\mathcal{A}$-subgroup $K < H$, that is, H is the only $\mathcal{A}$-subgroup which contains properly K. Let $|K| = p^m$. Let us consider the sets KTK, $T \in \mathrm{Bsets}(\mathcal{A})$. These sets form a partition of H because $T_1 \subseteq KT_2K$ or $T_1 \cap KT_2K = \emptyset$ for any basic sets $T_1, T_2 \in \mathrm{Bsets}(\mathcal{A})$ by Eq. (2), and therefore, $KT_1K = KT_2K$ or $KT_1K \cap KT_2K = \emptyset$. Note that, p^m divides $|KTK|$ for all T, and $KTK = K$ for all basic sets $T \subset K$. Thus, $|H| = \sum_{T \in \mathrm{Bsets}(\mathcal{A}), T \nsubseteq K} |KTK| + |K|$, and so there exists a basic set T_1 such that $T_1 \nsubseteq K$ and $|KT_1K| = p^m$. Then, $Kt \subseteq KT_1K$ and $tK \subseteq KT_1K$ for all $t \in T_1$. This together with $|Kt| = |tK| = |KT_1K| = p^m$ shows that any $t \in T_1$ normalizes K. Thus, $K \trianglelefteq \langle K, T_1 \rangle = H$, where the latter equality follows by the maximality of K. Now, (ii) follows by applying the induction hypothesis to the S-rings $\mathcal{A}_K$ and $\mathcal{A}_{H/K}$. □

Proposition 2.14. ([13, Proposition 3.4(i)]) *Let $\mathcal{A}$ be a p-S-ring over an abelian p-group H. If there exists a basic set $T \in \mathrm{Bsets}(A)$ with $|T| = |H|/p$, then $\mathcal{A}$ decomposes to the wreath product $\mathcal{A} = \mathcal{A}_K \wr \mathcal{A}_{H/K}$, where $K \leq H$ is an $\mathcal{A}$-subgroup with index $|H : K| = p$.*

The next result is the classification of all p-S-rings over $\mathbb{Z}_p^3$.

Theorem 2.15. ([13,28]) *Every p-S-ring over the group $\mathbb{Z}_p^3$ for an odd prime p is Cayley isomorphic to one of the S-rings given in Table 1.*

Remark 2.16. Hirasaka and Muzcyhuk [13] classified the Schurian S-rings, and it was proved later by Spiga and Wang [28] that all p-S-rings over $\mathbb{Z}_p^3$ are Schurian (see [28, Theorem 1]).

Let H be a group isomorphic to $\mathbb{Z}_p^3$ for an odd prime p. An S-ring $\mathcal{A}$ over H is called *exceptional* if it is Cayley isomorphic to the S-ring in the 6th row of Table 1, see [13]. Exceptional S-rings will play an important role in later sections.

Lemma 2.17. *Let $\mathcal{A}$ be an exceptional S-ring over a group H, $H \cong \mathbb{Z}_p^3$. Then $|\operatorname{Aut}(\mathcal{A})| = p^4$ and $\operatorname{Iso}_1(\mathcal{A}) = \operatorname{Aut}(H)$.*

Proof. Consider the S-ring in the 6th-row of Table 1. Denote by T its basic set containing the element $(1, 0, 0) \in \mathbb{Z}_p^3$. Since $p > 2$, it follows quickly that $|T| = p$ and $\langle T\rangle = \mathbb{Z}_p^3$. This implies that $\mathcal{A}$ has also a basic set T' such that $|T'| = p$ and $\langle T'\rangle = H$. The S-ring $\mathcal{A}$ is Schurian. Thus, T' is equal to an $\operatorname{Aut}(\mathcal{A})_1$-orbit, and by Proposition 2.4, $|\operatorname{Aut}(\mathcal{A})| = p^4$. Thus, $H_R \trianglelefteq \operatorname{Aut}(\mathcal{A})$, and so $\operatorname{Aut}(\mathcal{A})_1 \le \operatorname{Aut}(H)$. Since H is a $\mathrm{CI}^{(2)}$-group, $\mathcal{A}$ is a CI-S-ring, see Proposition 2.11, and we can write $\operatorname{Iso}_1(\mathcal{A}) = \operatorname{Aut}(\mathcal{A})_1 \operatorname{Aut}(H) = \operatorname{Aut}(H)$. □

We finish the subsection with further properties.

Lemma 2.18. *Let $\mathcal{A}$ be a p-S-ring over a group H, $K \le H$ be an $\mathcal{A}$-subgroup with index $|H : K| = p$, and let $T \in \operatorname{Bsets}(\mathcal{A})$. Then the following hold:*

(i) T is contained in a K-coset. In particular, $\operatorname{rad}(T) \le K$.
(ii) Let $L \le H$ be an $\mathcal{A}$-subgroup of order p such that $L \trianglelefteq H$ and $L \not\le \operatorname{rad}(T)$. Then for any $h \in T$, $hL \cap T = Lh \cap T = \{h\}$.
(iii) If H is an abelian group and $|\mathbf{O}_\theta(\mathcal{A}) \cap K||T| > |H|/p$, then $\mathbf{O}_\theta(\mathcal{A}) \cap \operatorname{rad}(T) \ne \{1\}$.

Proof. (i): Let us consider the quotient S-ring $\mathcal{A}_{H/K}$. By Eq. (2), $\mathcal{A}_{H/K}$ is a p-S-ring. Since $H/K \cong \mathbb{Z}_p$, its only p-S-ring is $\mathbb{Q}\, H/K$, and so $\mathcal{A}_{H/K} = \mathbb{Q}\, H/K$. In particular, $|T/K| = 1$, hence $T \subseteq Kh$ for a coset Kh and (i) follows.

(ii) By Eq. (2), there is a positive integer k such that $|hL \cap T| = |Lh \cap T| = k$ for all $h \in T$. As $|T|$ is a p-power, $k = 1$ or p. If $k = p$, then we find $LT = TL = T$, so $L \le \operatorname{rad}(T)$, which is excluded by one of the assumptions. Thus, $k = 1$ and (ii) follows.

(iii): Assume that $|\mathbf{O}_\theta(\mathcal{A}) \cap K||T| > |H|/p$. Let us consider the sets eT, $e \in \mathbf{O}_\theta(\mathcal{A}) \cap K$. By Eq. (1) and (i), these are all basic sets contained in a coset Kh. If these are pairwise distinct, then $|\mathbf{O}_\theta(\mathcal{A}) \cap K||T| = \sum_{e \in \mathbf{O}_\theta(\mathcal{A}) \cap K} |eT| \le |Kh| = |H|/p$, a contradiction. Thus, $eT = e'T$ for distinct $e, e' \in \mathbf{O}_\theta(\mathcal{A}) \cap K$. Using this and that H is abelian, we find $e^{-1}e'T = Te^{-1}e' = T$, and so $e^{-1}e' \in \mathbf{O}_\theta(\mathcal{A}) \cap \operatorname{rad}(T)$, by which (iii) follows. □

3. On CI-S-rings over $\mathbb{Z}_p^n$

In this section we give three propositions about CI properties of S-rings over the groups $\mathbb{Z}_p^n$. The first one is a necessary condition for an S-ring to be non-CI. It is essentially contained in the proof of [13, Proposition 3.9].

Proposition 3.1. *Suppose that $\mathcal{A} = V(H, P_1)$ is a non-CI-S-ring, where $H \cong \mathbb{Z}_p^n$ and $H_R \le P \le \operatorname{Sym}(H)$ is a p-group. Then the normalizer $N_{\operatorname{Aut}(\mathcal{A})}(H_R)$ contains a subgroup K for which the following hold:*

(i) $K \cong \mathbb{Z}_p^n$*, it is regular on* H*, and* $K \neq H_R$*.*
(ii) The stabilizer $(KH_R)_1$ *is elementary abelian, and*

$$|C_{H_R}((KH_R)_1)| \geq |K \cap H_R|.$$

Proof. Let $G = \mathrm{Aut}(\mathcal{A})$ and $N = N_{\mathrm{Aut}(\mathcal{A})}(H_R)$. Note that, since $G = P^{(2)}$ and P is a p-group, G is a p-group as well, see Proposition 2.3. We first show the existence of a subgroup $K \leq N$ that has all properties given in (i). If $G = N$, then the existence of the required subgroup K follows from the condition that $\mathcal{A}$ is a non-CI-S-ring. Now, suppose that $N < G$. Then, since G is a p-group, the normalizer $N_G(N) \neq N$, hence we may choose some $g \in N_G(N) \setminus N$. We let $K = (H_R)^g$. It is straightforward to see that K has all properties given in (i).

Now, we turn to part (ii). Consider the group $Q = KH_R$. Clearly, $Q = Q_1K = Q_1H_R$ and $Q_1 \cong Q/H_R \cong K/(K \cap H_R)$. Thus, Q_1 is an elementary abelian group. Also, as both K and H_R are abelian, $K \cap H_R \leq Z(Q)$, implying that $|C_{H_R}(Q_1)| \geq |K \cap H_R|$. This completes the proof of part (ii). □

The second proposition will be a sufficient condition for an S-ring over $\mathbb{Z}_p^n$ to be CI.

Definition 3.2. We say that an S-ring $\mathcal{A}$ over a group H is $\approx_2$*-minimal* if

$$\{X \leq \mathrm{Sym}(H) : X \geq H_R \text{ and } X \approx_2 \mathrm{Aut}(\mathcal{A})\} = \{\mathrm{Aut}(\mathcal{A})\}.$$

For example, the full group algebra $\mathbb{Q}H$ is a $\approx_2$-minimal S-ring. The obvious examples for non-$\approx_2$-minimal S-rings are the S-rings of rank 2 (the two basic sets are $\{1\}$ and $H \setminus \{1\}$). Clearly, $\mathrm{Aut}(\mathcal{A}) = \mathrm{Sym}(H)$, and thus $\mathrm{Aut}(\mathcal{A}) \approx_2 X$ whenever $H_R \leq X \leq \mathrm{Sym}(H)$ and X is 2-transitive on H.

Proposition 3.3. *Let* $\mathcal{A}$ *be a Schurian p-S-ring over a group* $H \cong \mathbb{Z}_p^n$*, and* $K \leq H$ *be an* $\mathcal{A}$*-subgroup of order* p *such that* $\mathcal{A}_{H/K}$ *is a* $\approx_2$*-minimal CI-S-ring. Then* $\mathcal{A}$ *is a CI-S-ring.*

Proof. Let $G = \mathrm{Aut}(\mathcal{A})$ and choose $L \leq G$ such that L is regular on H and $L \cong H$. Because of Proposition 2.11 it is enough to show that L and H_R are conjugate in G.

We write $\bar{G} = G^{H/K}$, $\bar{H}_R = (H_R)^{H/K}$ and $\bar{L} = L^{H/K}$. Note that $\bar{H}_R = (H/K)_R$. The group $\bar{L}$ is abelian acting transitively on H/K. It follows that it is regular, and $\bar{L} \cong \mathbb{Z}_p^{n-1}$. Since $\mathcal{A}_{H/K}$ is a CI-S-ring, $\bar{L} = (\bar{H}_R)^x$ for some $x \in \mathrm{Aut}(\mathcal{A}_{H/K})$. For sake of simplicity we denote by $\bar{1}$ the identity of H/K.

We claim that $\mathrm{Aut}(\mathcal{A}_{H/K}) = \bar{G}$. To settle this it is sufficient to show that $\mathrm{Aut}(\mathcal{A}_{H/K}) \approx_2 \bar{G}$, and use the assumption that $\mathcal{A}_{H/K}$ is $\approx_2$-minimal. We have to show that $\mathcal{A}_{H/K} = V(H/K, \bar{G}_{\bar{1}})$. Here we copy the proof of [13, Proposition 2.8(ii)]. Since K is an $\mathcal{A}$-subgroup, $K^g = K$ for any $g \in G_1$, and thus by Proposition 2.10(ii), the coset Kh is mapped by $g^{H/K}$ to $(Kh)^{g^{H/K}} = Kh^g$. A basic set of $\mathcal{A}_{H/K}$ is in the form

T/K where $T \in \mathrm{Bsets}(\mathcal{A})$. Since $\mathcal{A} = V(H, G_1)$, we find that $T = h^{G_1}$ for some $h \in H$. Observe that $G_{\{K\}} = K_R G_1$, and for any $g \in G$, $g^{H/K} \in \bar{G}_{\bar{1}}$ if and only if g fixes setwise the subgroup K. This implies that $g = k_R g'$ for some $k \in K$ and $g' \in G_1$. Now, we can express the $\bar{G}_{\bar{1}}$-orbit of Kh as

$$\begin{aligned}(Kh)^{\bar{G}_{\bar{1}}} &= \{(Kh)^{x^{H/K}} : x = k_R g,\, k \in K,\, g \in G_1\} = \{K(kh)^g : k \in K,\, g \in G_1\} \\ &= \{Kh^g : g \in G_1\} = h^{G_1}/K = T/K.\end{aligned}$$

We conclude that T/K is an orbit of $\bar{G}_{\bar{1}}$, and the claim follows.

Recall that $\bar{L} = (\bar{H}_R)^x$ for some $x \in \mathrm{Aut}(\mathcal{A}_{H/K}) = \bar{G}$. Choose $g \in G$ such that $g^{H/K} = x^{-1}$. Then $L^g \leq G_{H/K} H_R$, where $G_{H/K}$ denotes the kernel of G acting on H/K. Write $M = G_{H/K} H_R$. Since both G and $(H_R)^{H/K}$ are 2-closed groups, it follows by Proposition 2.2(ii) that M is also 2-closed. We are done if we show that M is H_R-transjugate, because then $(L^g)^{g'} = H_R$ for some $g' \in M$, showing that L and H_R are indeed conjugate in G.

Again, because of Proposition 2.11 we are done if we show that the S-ring $\mathcal{B} = V(H, M_1)$ is CI. Then $\mathcal{A} \subseteq \mathcal{B}$, and thus K is also a $\mathcal{B}$-subgroup. Note that $G_{H/K} \cap H_R = K_R$ and $M = M_1 H_R$. Then $|M_1| = |M|/|H_R| = |G_{H/K} H_R|/|H_R| = |G_{H/K}|/|K_R|$ and $|G_{H/K}| = |(G_{H/K})_1||K_R|$. It follows $|M_1| = |(G_{H/K})_1|$ and hence $M_1 = (G_{H/K})_1$. Since $(G_{H/K})_1 \lhd G_1$ and all orbits of $G_{H/K}$ are the cosets of K in H which have order p, we have $K \leq \mathbf{O}_\theta(\mathcal{B})$ and all basic sets of $\mathcal{B} = V(H, M_1)$ not contained in $\mathbf{O}_\theta(\mathcal{B})$ are K-cosets.

Let $f \in \mathrm{Iso}_1(\mathcal{B})$. In order to prove that $\mathcal{B}$ is a CI-S-ring, we have to find an automorphism $\varphi \in \mathrm{Aut}(H)$ such that

$$T^{f\varphi} = T \text{ for all } T \in \mathrm{Bsets}(\mathcal{B}). \tag{5}$$

Choose a minimal generating set $\{h_1, \ldots, h_n\}$ of H such that $\{h_1, \ldots, h_\ell\}$, $\ell \leq n$, is a generating set of $\mathbf{O}_\theta(\mathcal{B})$ with $h_1 \in K$. By Proposition 2.10, $K^f \leq H$ and $(Kh_i)^f = K^f h_i^f$. Since $1^f = 1$, $T^f \in \mathrm{Bsets}(\mathcal{B}^f)$ for every basic set $T \in \mathrm{Bsets}(\mathcal{A})$. Using this and that each Kh_i is a $\mathcal{B}$-subset, we find that each $K^f h_i^f$ is a $\mathcal{B}^f$-subset, and so $\langle K^f h_1^f, \ldots, K^f h_n^f\rangle \leq H$ is a $\mathcal{B}^f$-subgroup. By Proposition 2.10(i), $|\langle K^f h_1^f, \ldots, K^f h_n^f\rangle| = |\langle K^f h_1^f, \ldots, K^f h_n^f\rangle^{f-1}|$. Thus, $H = \langle K^f h_1^f, \ldots, K^f h_n^f\rangle$. Since $h_1 \in K$, it follows that $K^f h_1^f = K^f$, and $\{h_1^f, \cdots, h_n^f\}$ is also a minimal generating set of H. Define φ as the induced automorphism of H by $\varphi : h_i^f \mapsto h_i$ for $1 \leq i \leq n$. Then $h_i^{f\varphi} = h_i$. To finish the proof, it suffices to show that Eq. (5) holds.

Set $f_1 = f\varphi$. Clearly, $f_1 \in \mathrm{Iso}_1(\mathcal{B})$. Recall that for any $S, T \in \mathrm{Bsets}(\mathcal{B})$, $(ST)^{f_1} = S^{f_1} T^{f_1}$ (see the paragraph preceding Proposition 2.10). Then f_1 fixes each element in $\mathbf{O}_\theta(\mathcal{B})$ because f_1 fixes a generating set of $\mathbf{O}_\theta(\mathcal{B})$. In particular, $K^{f_1} = K$ as $K \leq \mathbf{O}_\theta(\mathcal{B})$, and Eq. (5) holds whenever $T \subset \mathbf{O}_\theta(\mathcal{B})$. Now, suppose that $T \not\subset \mathbf{O}_\theta(\mathcal{B})$. Let us consider the isomorphism $f_1^{H/K}$ of $\mathcal{B}_{H/K}$ induced by f_1 (for the definition of $f_1^{H/K}$, see Proposition 2.10(iii)). The quotient S-ring $\mathcal{B}_{H/K} = \mathbb{Q}\, H/K$. Since $\mathbb{Q}\, H/K$ is a CI-S-ring and $\mathrm{Aut}(\mathbb{Q}\,H/K) = (H/K)_R$, it follows that $\mathrm{Iso}_1(\mathcal{B}_{H/K}) = \mathrm{Aut}(\mathbb{Q}\,H/K)_1\,\mathrm{Aut}(H/K) = \mathrm{Aut}(H/K)$. Also, $f_1^{H/K} \in \mathrm{Iso}_1(\mathcal{B}_{H/K})$, because $K^{f_1} = K$, and so $f_1^{H/K} \in \mathrm{Aut}(H/K)$. On the other hand, as f_1 fixes all generators h_i, $f_1^{H/K}$ fixes a generating set of H/K, and so $f_1^{H/K}$ is the identity mapping. Since $T \not\subset \mathbf{O}_\theta(\mathcal{B})$, $T = Kh$ for some $h \in H \setminus K$, and we can write $T^{f_1} = (Kh)^{f_1} = (Kh)^{f_1^{H/K}} = Kh = T$. □

Proposition 3.3 will be especially useful in conjunction with the fact that all indecomposable Schurian p-S-rings over $\mathbb{Z}_p^4$ are $\approx_2$-minimal. We prove the latter fact in Section 4.

Recall that, the $\mathrm{CI}^{(2)}$-property for a group H is equivalent to the CI-property for all Schurian S-rings over H (see Proposition 2.11). The third proposition is the following refinement:

Proposition 3.4. *Let H be a group isomorphic to $\mathbb{Z}_p^n$ for a prime p. Then the following conditions are equivalent:*

(i) H is a $CI^{(2)}$-group.
(ii) All S-rings $V(H,A)$ are CI-S-rings where $A < \mathrm{Aut}(H)$ is a p-group with $|C_{H_R}(A)| \ge p^2$.

Proof. Notice that, the implication (i) ⇒ (ii) is a direct consequence of Proposition 2.11.

Now, we turn to the implication (ii) ⇒ (i). Let $G \le \mathrm{Sym}(H)$ be a 2-closed subgroup with $H_R \le G$, and let $K \le G$ be a regular subgroup such that $K \cong H$. We have to show that K and H_R are conjugate in G.

Now, choose a Sylow p-subgroup P of G such that $H_R \le P$. Since G is 2-closed, by Proposition 2.3, P is 2-closed, that is, $P^{(2)} = P$. By Sylow Theorem, $K^x \le P$ for some $x \in G$, hence we may assume that $K \le P$. According to Proposition 2.5 there exists some $y \in \langle H_R, K\rangle^{(2)} \le P^{(2)} = P$ such that $|C_{H_R}(K^y)| \ge p^2$. Let $Q = \langle H_R, K^y\rangle$. Then $Q^{(2)} \le P^{(2)} = P$, and $Q^{(2)}$ is also a p-group. It is sufficient to show that $Q^{(2)}$ is H_R-transjugate.

Let us consider the normalizer $N = N_{Q^{(2)}}(H_R)$. Since $|C_{H_R}(K^y)| \ge p^2$, it follows that $|C_{H_R}(Q)| \ge p^2$. By Proposition 2.1, $C_{H_R}(Q) = H_R \cap Z(Q) \le H_R \cap Z(Q^{(2)}) = C_{H_R}(Q^{(2)})$. Therefore, $|C_{H_R}(Q^{(2)})| \ge p^2$, and as $N^{(2)} \le Q^{(2)}$, it follows that $|C_{H_R}(N_1)| \ge p^2$. By the hypothesis in (ii), the S-ring $V(H,(N^{(2)})_1) = V(H,N_1)$ is a CI-S-ring. Equivalently, $N^{(2)}$ is H_R-transjugate.

We finish the proof by showing that $N^{(2)} = Q^{(2)}$. In doing this we use the same idea as in the proof of [27, Proposition 1]. Assume to the contrary that $N^{(2)} < Q^{(2)}$. Since $Q^{(2)}$ is a p-group, we can choose an element $z \in N_{Q^{(2)}}(N^{(2)}) \setminus N^{(2)}$. Then $(H_R)^z \le N^{(2)}$. Since $N^{(2)}$ is H_R-transjugate, $(H_R)^z = (H_R)^{z'}$ for some $z' \in N^{(2)}$, and so we find $z'z^{-1} \in N_{Q^{(2)}}(H_R) = N$, from which $z \in N^{(2)}$, a contradiction. Therefore, $Q^{(2)} = N^{(2)}$, showing that $Q^{(2)}$ is H_R-transjugate, as required. □

In fact, we are going to derive Theorem 1.2 by showing that the condition in case (ii) of Proposition 3.4 holds when $H \cong \mathbb{Z}_p^5$.

Theorem 3.5. *Let $H \cong \mathbb{Z}_p^5$ for an odd prime p. Then all S-rings $V(H, A)$ are CI-S-rings where $A < \mathrm{Aut}(H)$ is a p-group with $|C_{H_R}(A)| \geq p^2$.*

The proof of Theorem 3.5 will be given in Sections 5 and 6.

4. Indecomposable Schurian p-S-rings over $\mathbb{Z}_p^n$ are $\approx_2$-minimal for $n \leq 4$

We set some notation that will be used throughout the rest of the paper:

Notation. From now on p will stand for an odd prime, and H will denote a group isomorphic to $\mathbb{Z}_p^n$. The group H will be regarded as the additive group of an n-dimensional vector space over the field $GF(p)$. The elements of H will be denoted by lower case letters u, v, etc., while the subgroups of H by upper case letters U, V, etc. As usual, the identity element will be denoted by 0, and the inverse of an element $u \in H$ by $-u$. For an integer k and a subset $T \subseteq H$ we write $T^{(k)} = kT = \{ku : h \in T\}$, where $ku = u + \cdots + u$, with $|k|$ summands if $k > 0$, and $ku = -(u + \cdots + u)$ otherwise.

It turns out that all indecomposable p-S-rings over the group $\mathbb{Z}_p^n$ are $\approx_2$-minimal for any odd prime p and $n \leq 3$. This is not hard to see for the groups $\mathbb{Z}_p$ and $\mathbb{Z}_p^2$. The full group algebra $\mathbb{Q}\mathbb{Z}_p$ is the only p-S-ring over $\mathbb{Z}_p$; and up to Cayley isomorphisms, there are two p-S-rings over $\mathbb{Z}_p^2$: $\mathbb{Q}\mathbb{Z}_p^2$ and $\mathbb{Q}\mathbb{Z}_p \wr \mathbb{Q}\mathbb{Z}_p$, and the latter one is decomposable. Theorem 2.15 shows that, up to Cayley isomorphisms, there are two indecomposable p-S-rings over $\mathbb{Z}_p^3$: $\mathbb{Q}\mathbb{Z}_p^3$ and the exceptional p-S-ring given in the 6th row of Table 1. By Lemma 2.17, the automorphism group of an exceptional p-S-ring has order p^4, hence it is $\approx_2$-minimal. In this section, we extend this result to the Schurian indecomposable p-S-rings over $\mathbb{Z}_p^4$.

Theorem 4.1. *All indecomposable Schurian p-S-rings over the group $\mathbb{Z}_p^4$ are $\approx_2$-minimal for any odd prime p.*

Remark 4.2. We would like to remark that the above theorem cannot be generalized to Schurian indecomposable p-S-rings over $\mathbb{Z}_p^5$. A counterexample is the indecomposable S-ring $V(H, L)$ defined in Lemma 6.4, where $H \cong \mathbb{Z}_p^5$ and $L \leq \mathrm{Aut}(H)$ of order $|L| = p^2$. It is proved in Lemma 6.5 that $|\mathrm{Aut}(V(H, L))| = p^8$, hence $H_R L \approx_2 \mathrm{Aut}(V(H, L))$ but $H_R L < \mathrm{Aut}(V(H, L))$, and so $V(H, L)$ is not $\approx_2$-minimal.

The proof of the theorem will be given in the end of the section following three preparatory lemmas.

Recall that, if $\mathcal{A}$ is an S-ring over H and $W \leq H$ is an $\mathcal{A}$-subgroup, then the W-cosets in H form a block system for $\mathrm{Aut}(\mathcal{A})$.

Lemma 4.3. *Let $\mathcal{A}$ be an indecomposable S-ring over a group $H \cong \mathbb{Z}_p^n$, and let W be an $\mathcal{A}$-subgroup with $|W| = p$. Then the kernel*

$$\mathrm{Aut}(\mathcal{A})_\delta = W_R = \{w_R : w \in W\},$$

where δ denotes the block system H/W.

Proof. Let $K = \mathrm{Aut}(\mathcal{A})_\delta$. It is clear that $W_R \leq K$, and thus it is enough to prove that the stabilizer K_0 is trivial. By Lemma 2.18(ii), for every basic set $T \in \mathrm{Bsets}(\mathcal{A})$,

$$W \nleq \mathrm{rad}(T) \Rightarrow T \cap (W + u) = \{u\} \text{ for all } u \in T. \tag{6}$$

We define recursively a finite sequence $T_1, \dots, T_r$ of basic sets of $\mathcal{A}$ as follows. Let $T_1 = \{w\}$ where w is an arbitrary nonzero element in W. Now, suppose that the sets $T_1, \dots, T_i$ are already defined for $i \geq 1$. If $H = \langle T_1 \cup \cdots \cup T_i \rangle$, then finish the procedure and let $r = i$. Otherwise, choose T_{i+1} to be a basic set in $H \setminus \langle T_1 \cup \cdots \cup T_i \rangle$ such that $W \nleq \mathrm{rad}(T_{i+1})$. Notice that, such T_{i+1} does exist because $\mathcal{A}$ is indecomposable.

Let $S = T_1 \cup \cdots \cup T_r$ and consider the Cayley graph $\mathrm{Cay}(H, S)$. Note that, $\mathrm{Aut}(\mathcal{A}) \leq \mathrm{Aut}(\mathrm{Cay}(H, S))$. It is clear from the construction that $\langle S \rangle = H$, hence $\mathrm{Cay}(H, S)$ is connected. We claim that S has the property that, whenever a W-coset intersects S, it does intersect it at exactly one element. Suppose to the contrary that there exist $u_1, u_2 \in S$ such that $u_1 \neq u_2$ and $u_1 - u_2 \in W$. Then $u_1 \in T_i$ and $u_2 \in T_j$ for some $i, j \in \{1, \dots, r\}$. It follows from the construction of S and Eq. (6) that $i \neq j$, and we may assume w. l. o. g. that $i < j$. Thus, $u_2 \in \langle T_i, W \rangle \leq \langle T_1, \dots, T_i \rangle$, and so $u_2 \in \langle T_1 \cup \cdots \cup T_{j-1} \rangle \cap T_j$, a contradiction. Now, using that $\mathrm{Aut}(\mathcal{A}) \leq \mathrm{Aut}(\mathrm{Cay}(H, S))$ and the above property of S, we find that every element in K_0 fixes all neighbors of 0 in $\mathrm{Cay}(H, S)$. This and the connectedness of $\mathrm{Cay}(H, S)$ yield that $|K_0| = 1$. □

For $x \in \mathrm{Aut}(H)$, we define $C_H(x) = \{u \in H : u^x = u\}$. Note that for $u \in H$, $u \in C_H(x)$ is equivalent to the condition that u_R and x commute with each other.

Lemma 4.4. *Let $\mathcal{A}$ be an indecomposable S-ring over a group $H \cong \mathbb{Z}_p^4$ and let $x \in N_{\mathrm{Aut}(\mathcal{A})}(H_R)$ such that $x \neq \mathrm{id}_H$ and $0^x = 0$. Then $|C_H(x)| \leq p^2$.*

Proof. Since $x \neq \mathrm{id}_H$, it follows that $|C_H(x)| \leq p^3$. Assume to the contrary that $|C_H(x)| = p^3$. Let $U = C_H(x)$, and for a fixed $v_1 \in H \setminus U$, let $W = \langle v_1^x - v_1 \rangle$. Then $|W| = p$, and it follows that the orbit $v^{\langle x \rangle} = W + v$ for all $v \in H \setminus U$. Observe that, W is not an $\mathcal{A}$-subgroup. For otherwise, x belongs to the kernel of $\mathrm{Aut}(\mathcal{A})$ acting on H/W, which is impossible by Lemma 4.3.

Let U' be an $\mathcal{A}$-subgroup of order p^3. If $U = U'$, then define $V = \bigcap_{T \in \mathrm{Bsets}(\mathcal{A}),\, T \subseteq H \setminus U} \mathrm{rad}(T)$. Clearly, V is an $\mathcal{A}$-subgroup such that $W \leq V \leq U$, and $\mathcal{A}$ is an U/V-wreath product, a contradiction. Hence, $U' \neq U$, and in particular, U is not an $\mathcal{A}$-subgroup.

Let $T_1 \in \mathrm{Bsets}(\mathcal{A})$ such that $T_1 \subset U'$ and $T_1 \not\subset U$. Then $|T_1| \geq p$, and since W is not an $\mathcal{A}$-subgroup, it follows that $|T_1| = p^2$. Indeed, if $|T_1| = p$, then T_1 is necessarily a W-coset, implying that $W = \mathrm{rad}(T_1)$, and so W is an $\mathcal{A}$-subgroup, which is not the case. By Proposition 2.14, T_1 is equal to a U''-coset for some $\mathcal{A}$-subgroup U'' such that $|U''| = p^2$ and $W < U''$. We find $U'' = W + W'$ for an $\mathcal{A}$-subgroup W' of order p. Since $W' \leq \mathbf{O}_\theta(\mathcal{A})$, $W' < U$, and it follows that $U'' = U' \cap U$.

Now, choose $T \in \mathrm{Bsets}(\mathcal{A})$ such that $T \not\subset U \cup U'$ and $T \cap U \neq \emptyset$. Notice that such T exists because U is not an $\mathcal{A}$-subgroup. Since $T \not\subset U$, it follows that T contains at least one W-coset not contained in U. This together with $T \cap U \neq \emptyset$ gives that $|T| > p$. Fix an element $v \in T \cap U$. Then $T \subseteq U' + v$, see Lemma 2.18(i). Since $\mathcal{A}$ is indecomposable, it follows from Proposition 2.14 that $|T| = p^2$. Let $v' \in T \setminus U$. If $W' \leq \mathrm{rad}(T)$, then we find $U'' + v' = W' + (W + v') \subseteq W' + T = T$. Thus, $T = U'' + v'$, contradicting that $T \cap U \neq \emptyset$. Thus, $W' \not\leq \mathrm{rad}(T)$, and by Eq. (2), every W'-coset intersects T in at most 1 element. Consequently, any U''-coset intersects T in at most p elements. The U''-cosets contained in $U' + v$ can be listed as $U'' + ku + v$, where $k \in \{0, 1, \ldots, p-1\}$ and u is any fixed element in $U' \setminus U$. Let $T_i = T \cap (U'' + iu + v)$, $i \in \{0, 1, \ldots, p-1\}$. It follows that the sets T_i form a partition of T, T_i is a W-coset for all $i > 0$, and $|T_0| = p$.

Let us consider the product $\underline{T} \cdot \underline{(-T)}$ in $\mathbb{Q}H$. Writing $\underline{T} \cdot \underline{(-T)} = \sum_{u \in H} a_u u$, it follows quickly from the above description of the sets T_i that $\sum_{u \in U'' \setminus \{0\}} a_u = p^3 - p^2$. On the other hand, $\underline{T} \cdot \underline{(-T)} \in \mathcal{A}$, and it can be expressed as the linear combination $\underline{T} \cdot \underline{(-T)} = \sum_{T' \in \mathrm{Bsets}(\mathcal{A})} b_{T'} \underline{T'}$. Let $w \in W$, $w \neq 0$. Since W is not an $\mathcal{A}$-subgroup, it follows that the coset $W' + w$ is a basic set of $\mathcal{A}$. Let us denote the latter basic set by $T(w)$. It also follows from the description of the sets T_i that $a_w \geq p^2 - p$. Thus, $b_{T(w)} \geq p^2 - p$ as well, and as w was chosen arbitrarily from $W \setminus \{0\}$, we arrive at a contradiction as follows:

$$p^3 - p^2 = \sum_{u \in U'' \setminus \{0\}} a_u \geq \sum_{w \in W \setminus \{0\}} b_{T(w)} |T(w)| \geq (p-1)(p^3 - p^2). \quad \square$$

Let $\mathcal{A}$ be a p-S-ring over H. In what follows, we call an ordered n-tuple $(v_1, \ldots, v_n)$ of generators of H an $\mathcal{A}$-*basis* if all subgroups in the chain below are $\mathcal{A}$-subgroups

$$\{0\} < \langle v_n \rangle < \langle v_{n-1}, v_n \rangle < \cdots < \langle v_1, \ldots, v_n \rangle = H.$$

Notice that, if $x \in \mathrm{Aut}(A)$ normalizes H_R and $0^x = 0$, then $x \in \mathrm{Aut}(H)$, and it can be written in an $\mathcal{A}$-basis as an upper triangular matrix having 1's in the diagonal.

Lemma 4.5. *Let $\mathcal{A}$ be an indecomposable p-S-ring over a group $H \cong \mathbb{Z}_p^4$. Then*

(i) $|N_{\mathrm{Aut}(\mathcal{A})}(H_R)| \leq p^6$;
(ii) H_R *is normal in* $\mathrm{Aut}(\mathcal{A})$.

Proof. Let $G = \mathrm{Aut}(\mathcal{A})$ and $N = N_{\mathrm{Aut}(\mathcal{A})}(H_R)$.

(i): Assume to the contrary that $|N| > p^6$, that is, for the stabilizer N_0 we have $|N_0| > p^2$. Let us fix an $\mathcal{A}$-basis (v_1, v_2, v_3, v_4). This means that $\langle v_4 \rangle$ is an $\mathcal{A}$-subgroup, and we can consider the action of N_0 on $H/\langle v_4 \rangle$. By Lemma 4.3, the latter action is faithful, and hence N_0 is isomorphic to a subgroup of the group of all upper triangular 3×3 matrices with each diagonal element equal to 1. Therefore, $|N_0| = p^3$, and we can choose $x \in Z(N_0)$ that can be written in the basis (v_1, v_2, v_3, v_4) as

$$x = \begin{pmatrix} 1 & 0 & 1 & a \\ 0 & 1 & 0 & b \\ 0 & 0 & 1 & c \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Then, the orbit $v_1^{N_0}$ has size at most p^2. This follows from Proposition 2.14 and the fact that $\mathcal{A}$ is indecomposable. Therefore, there exists $y \in N_0$ such that $y \neq \mathrm{id}_H$ and y fixes v_1. Using also that $[x, y] = 1$, we find that $(v_1^x)^y = (v_1^y)^x = v_1^x$, hence $v_1^x = v_1 + v_3 + av_4 \in C_H(y)$. It follows that each of v_1, v_3 and v_4 is in $C_H(y)$. This, however, contradicts Lemma 4.4.

(ii): We have to show that $G = N$. Assume to the contrary that $G > N$. Then $N_G(N) > N$. Choose $g \in N_G(N) \setminus N$ and let $P = (H_R)^g H_R$. Since $P_0 \leq N_0$, $|P_0| \leq p^2$. If $|P_0| = p$, then $|P| = |H_R| \cdot |P_0| = p^5$, hence $|(H_R)^g \cap H_R| = p^3$. Then every $x \in P_0$ satisfies $|C_{H_R}(x)| \geq |(H_R)^g \cap H_R| = p^3$, a contradiction to Lemma 4.4. Therefore, $|P_0| = p^2$, $P_0 = N_0$ and each $z \in N_0$ satisfies $|C_{H_R}(z)| \geq |(H_R)^g \cap H_R| = p^2$. By Lemma 4.4, $C_{H_R}(z) = (H_R)^g \cap H_R$ whenever $z \neq \mathrm{id}_H$. Therefore, letting $U = \{u \in H : u_R \in H_R^g \cap H_R\}$, we can write

$$C_H(z) = U \text{ for all } z \in N_0,\ z \neq \mathrm{id}_H. \tag{7}$$

Let us consider the S-ring $\mathcal{B} = V(H, N_0)$. Clearly, $U \leq \mathbf{O}_\theta(\mathcal{B})$. Fix a $\mathcal{B}$-subgroup V such that V has order p^3 and $U < V$. Let $v \in H \setminus V$ and $T \in \mathrm{Bsets}(\mathcal{B})$ be a basic set such that $v \in T$. By Lemma 2.18(i), $v^z - v \in V$. Suppose that $v^z - v \in U$ for all $z \in N_0$. This implies that $T \subseteq U + v$, and thus either $T = U + v$, or $|T| \leq p$. In the latter case, however, it follows from $|N_0| = p^2$ that N_0 contains a non-identity element z fixing some $v \in T$, and hence $C_H(z) \geq \langle U, v \rangle > U$, which contradicts Eq. (7). Observe that, if $T = U + v$, then it is also a basic set of $\mathcal{A}$. For otherwise, $\mathcal{A}$ would have a basic set of size p^3, contradicting that $\mathcal{A}$ is indecomposable (see Proposition 2.14). Now, since $\mathcal{A}$ is not a V/U-wreath product, there exists $v_1 \in H \setminus V$ and $x \in N_0$ for which $v_1^x - v_1 \notin U$.

Now, define the elements $v_2 = v_1^x - v_1$, $v_3 = v_2^x - v_2$, and let $v_4 \in U$ be an element such that $U = \langle v_3, v_4 \rangle$. It follows that (v_1, v_2, v_3, v_4) is a $\mathcal{B}$-basis, in which

$$x = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let $y \in N_0$ such that $N_0 = \langle x, y \rangle$. By Eq. (7), $C_H(y) = U = \langle v_3, v_4 \rangle$, and thus y can be written in the basis (v_1, v_2, v_3, v_4) in the form

$$y = \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & d & e \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Using also that $[x, y] = 1$, we find $d = a$ and $e = 0$. Thus, $v_2^y = v_2 + dv_3$. On the other hand, $v_2^{(x^d)} = v_2 + dv_3$ also holds, and we find $v_2 \in C_H(x^d y^{-1})$, where $x^d y^{-1} \neq \mathrm{id}_H$. This contradicts Eq. (7). □

All Schurian p-S-rings over $\mathbb{Z}_p^4$ are CI [13, Theorem 3.1]. Combining this with Lemma 4.5 yields the following corollary (see also the proof of Lemma 2.17):

Corollary 4.6. *Let $\mathcal{A}$ be an indecomposable Schurian p-S-ring over a group H, $H \cong \mathbb{Z}_p^4$ for an odd prime p. Then $\mathrm{Iso}_0(\mathcal{A}) = \mathrm{Aut}(H)$.*

Everything is prepared to prove the main result of this section.

Proof of Theorem 4.1. Assume to the contrary that $\mathcal{A}$ is a Schurian indecomposable p-S-ring over H, which is not $\approx_2$-minimal. Let $G = \mathrm{Aut}(\mathcal{A})$. By Lemma 4.5, $H_R \trianglelefteq G$ and $|G| \leq p^6$. As $\mathcal{A}$ is not $\approx_2$-minimal, $|G| = p^6$, and there exists $x \in G_0$ such that x has order p, and $\mathcal{A} = V(H, \langle x \rangle)$. In other words, $G \approx_2 K$ where $K = \langle H_R, x \rangle$. Note that $G = K^{(2)}$. Let $u \in C_H(x)$. Then $u_R \in Z(K)$, and by Proposition 2.1, $u_R \in Z(K^{(2)}) = Z(G)$, implying that $u \in C_H(y)$ for any $y \in G_0$. We obtain that $C_H(x) \leq C_H(y)$ for all $y \in G_0$. Also, as $\mathcal{A} = V(H, \langle x \rangle)$, every basic set of $\mathcal{A}$ has size at most p. Suppose for the moment that $|C_H(x)| = p^2$. Let T be a basic set of size p and fix an element $v \in T$. Clearly, $T \not\subset C_H(x)$. Also, since T is a G_0-orbit and $|G_0| = p^2$, we find that $G_0 \cap G_v$ is nontrivial. Hence if $y \in G_0 \cap G_v$ and $y \neq \mathrm{id}_H$, then $C_H(y) = \langle C_H(x), v \rangle$, contradicting Lemma 4.4. It remains to consider the case when $|C_H(x)| = p$. Equivalently, $\mathrm{rank}(x - I) = 3$, and this implies that, in a suitable basis, denoted by (v_1, v_2, v_3, v_4), x has the following Jordan normal form:

$$x = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since x has order p, it follows that $p > 3$. Let T be the orbit of v_1 under $\langle x \rangle$ (hence under G_0). It is not hard to check that $|T| = p$ and $\langle T \rangle = H$. Then, by Proposition 2.4, $|G_0| = p$, a contradiction. This completes the proof of the theorem. □

We finish the section with a corollary of Proposition 3.3 and Theorem 4.1, which will be used several times in the next two sections.

Corollary 4.7. *Let $\mathcal{A}$ be a Schurian p-S-ring over the group $H \cong \mathbb{Z}_p^5$, and let W be an $\mathcal{A}$-subgroup of order p. If $\mathcal{A}$ is a non-CI-S-ring, then the S-ring $\mathcal{A}_{H/W}$ is decomposable.*

5. Proof of Theorem 3.5 I: the decomposable S-rings

We record all assumptions of Theorem 3.5 in the following hypothesis:

Hypothesis 5.1. $\mathcal{A} = V(H, A)$ is an S-ring over a group $H \cong \mathbb{Z}_p^5$ for some odd prime p, and for some subgroup $A \leq \mathrm{Aut}(H)$ with $|C_H(A)| \geq p^2$.

Our eventual goal is to show that, assuming Hypothesis 5.1, the S-ring $\mathcal{A}$ is CI. In this section, we deal with the particular case when $\mathcal{A}$ is decomposable.

Theorem 5.2. *Assuming Hypothesis 5.1, suppose that $\mathcal{A}$ is decomposable. Then $\mathcal{A}$ is a CI-S-ring.*

The theorem will be proved in the end of the section following four preparatory lemmas. In the next three lemmas we study the S-ring $\mathcal{A}$ described in Theorem 5.2 which satisfies additional conditions.

Lemma 5.3. *Assuming Hypothesis 5.1, suppose that there exist $\mathcal{A}$-subgroups U_1, U_2, W_1 and W_2 with $|U_1| = |U_2| = p^4$, $|W_1| = |W_2| = p$, $U_1 \neq U_2$, $W_1 \neq W_2$ and $W_1 + W_2 < U_1 \cap U_2$, and also that the following hold:*

(1) $\mathcal{A}$ is both a U_1/W_2- and a U_2/W_1-wreath product.
(2) Both $\mathcal{A}_{U_1/W_1}$ and $\mathcal{A}_{U_2/W_2}$ are indecomposable.
(3) $|A_v| \neq 1$ for some $v \in H \setminus U_1 \cup U_2$.

Then one of the following possibilities holds:

(i) $|N_{\mathrm{Aut}(\mathcal{A})}(H_R)| = p^8$, and there exists an $\mathcal{A}$-subgroup U_3 such that $|U_3| = p^4$, $U_3 \neq U_i$ for $i \in \{1, 2\}$, and every basic set of $\mathcal{A}$ not contained in $U_1 \cup U_2 \cup U_3$ is equal to a $(U_1 \cap U_2)$-coset.
(ii) $|N_{\mathrm{Aut}(\mathcal{A})}(H_R)| = p^9$, and every basic set of $\mathcal{A}$ not contained in $U_1 \cup U_2$ is equal to a $(U_1 \cap U_2)$-coset.

Proof. We let $N = N_{\mathrm{Aut}(\mathcal{A})}(H_R)$, $W = W_1 + W_2$ and $U = U_1 \cap U_2$. Note that $\mathcal{A} = V(H, N_0)$, where N_0 denotes the stabilizer of 0 in N. Also notice that, $w^\gamma = w$ for all $w \in W$ and $\gamma \in N_0$. Fix a non-identity element $x \in A_v$, and some $u_1 \in U_1 \setminus U$ which is not fixed by x. Then there exists an integer k such that $ku_1 + v \in U_2$. Since $v \notin U_1$, it follows that $ku_1 + v \notin U$. We define the elements $v_1 = ku_1$, $v_2 = ku_1 + v$ and $v_3 = v_1^x - v_1$. We find that $v_2^x = v_2 + v_3$. For $i \in \{1, 2\}$, let $T_i = v_i^A$, the A-orbit containing

v_i (in other words, T_i is the basic set of $\mathcal{A}$ that contains v_i). Note that, since $\mathcal{A}_{U_i/W_i}$ is indecomposable, it follows that $\mathrm{rad}(T_i) = W_i$ for both $i = 1, 2$. Since $v_3 = v_i^x - v_i$, it follows that $v_3 \in T_i - T_i$, hence $v_3 \in U_i$. We conclude that $v_3 \in U_1 \cap U_2$. Suppose that $v_3 \in W$. Fix $i \in \{1, 2\}$. Then both v_i and v_i^x are in $T_i \cap \langle v_3\rangle + v_i$. Notice that $v_1^x \neq v_1$ because $v_1 = ku_1$ and u_1 was chosen so that it is not fixed by x. Thus $v_3 \neq 0$, and so $v_2^x \neq v_2$ also holds. We get $|T_i \cap \langle v_3\rangle + v_1| > 1$, and this together with Eq. (2) shows that $|T_i \cap \langle v_3\rangle + v'| = p$ for all $v' \in T_i$, implying that $\langle v_3\rangle \leq \mathrm{rad}(T_i)$. It follows that $\langle v_3\rangle \leq \mathrm{rad}(T_1) \cap \mathrm{rad}(T_2) = W_1 \cap W_2$, contradicting that $v_3 \neq 0$. We obtain that $v_3 \in (U_1 \cap U_2) \setminus W$.

Next, assume for the moment that $v_3^x - v_3 \in W_1$. Let us consider the automorphism x^{U_1/W_1}. First, as $v_1^x - v_1 = v_3 \notin W_1$, we see that x^{U_1/W_1} is not the identity mapping. On the other hand, x^{U_1/W_1} fixes W/W_1 pointwise and fixes also the element $W_1 + v_3$ (here $W_1 + v_3$ is regarded as an element of the group U_1/W_1). By all these we find $|C_{U_1/W_1}(x^{U_1/W_1})| = p^2$, which implies that $\mathcal{A}_{U_1/W_1}$ is a nontrivial generalized wreath product, a contradiction to the assumption given in (2). We conclude that $v_3^x - v_3 \notin W_1$.

Notice that, there is a symmetry between the conditions satisfied by the pairs (U_1, W_1) and (U_2, W_2). Therefore, any statement, which involves the subgroups U_1, U_2, W_1 and W_2, and which can be derived from these conditions, gives always rise to yet another statement that is obtained by replacing U_1 with U_2 and W_1 with W_2. In what follows, we will refer to the new statement as *the dual counterpart*. For instance, the statement $v_3^x - v_3 \notin W_1$ has dual counterpart: $v_3^x - v_3 \notin W_2$. Now, as $v_3^x - v_3 \notin W_1 \cup W_2$, we can choose non-zero elements $v_4 \in W_1$ and $v_5 \in W_2$ such that $v_3^x = v_3 + v_4 + v_5$.

Now, it follows from the above construction that $(v_1, v_2, v_3, v_4, v_5)$ is an $\mathcal{A}$-basis. In this basis, the automorphism x is represented by the matrix as shown in Eq. (8).

$$x = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad y_1 = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \quad y_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad (8)$$

Furthermore, it is straightforward to check that each of y_1 and y_2, defined in Eq. (8), acts on H as an automorphism of $\mathcal{A}$, and therefore, it belongs to N_0. Let $M = \langle x, y_1, y_2\rangle$. Clearly, $M \leq N_0$, and for $i \in \{1, 2\}$, the basic set T_i is equal to the orbit v_i^M.

Now, let $z \in N_0 \cap N_{v_1}$. For $i \in \{1, 2\}$, let us consider the automorphism $z^{U_i/W_i} \in \mathrm{Aut}(\mathcal{A}_{U_i/W_i})_0$. The latter group is generated by the element x^{U_i/W_i}, and we find $z^{U_i/W_i} \in \left\langle x^{U_i/W_i}\right\rangle$. Moreover, as $v_1^z = v_1$, it follows that z^{U_1/W_1} is the identity mapping. All these yield that z can be written in the following form:

$$z = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & a & a(a-1)/2 & b \\ 0 & 0 & 1 & a & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad a, b \in GF(p). \tag{9}$$

This shows that $|N_0 \cap N_{v_1}| \le p^2$, and therefore, $|N| = p^8$ or p^9.

Fix an element $v' = kv_1 + v_2$ for some $k \in \{1, \dots, p-1\}$, and let T be the basic set of $\mathcal{A}$ that contains v'. Since $\mathcal{A} = V(H, N_0)$ we can write $T = (v')^{N_0}$. It follows from Eqs. (8) and (9) that $W + v' \subseteq T \subseteq U + v'$. This together with Lemma 2.14 yields that $T = W + v'$ or $T = U + v'$. By Eq. (8), $(v')^x = kv_1 + kv_3 + v_2 + v_3 = v' + (k+1)v_3$.

Assume at first that $k \ne p - 1$. Then $(v')^x \notin v' + W$, and hence $T = U + v'$. The latter condition together with Theorem 2.9 yields that every basic set of $\mathcal{A}$ contained in $\langle U, v' \rangle \setminus U$ is equal to a U-coset.

If $|N| = p^8$, then $M = N_0$, $v_3^{N_0} = v_3 + \langle v_4 + v_5 \rangle$, and this with the previous paragraph implies that (i) holds with $U_3 = \langle U, -v_1 + v_2 \rangle$. Finally, suppose that $|N| = p^9$. Then for z with $a = 1$ and $b = 0$ in Eq. (9), we find $(-v_1 + v_2)^z = -v_1 + v_2 + v_3$, thus $(-v_1 + v_2)^{N_0} = U + (-v_1 + v_2)$, and (ii) follows. □

Lemma 5.4. *With the notation of Lemma 5.3, the S-ring $\mathcal{A}$ is CI.*

Proof. We keep all notations from the previous proof, and let, in addition, $W_3 = \langle v_4 + v_5 \rangle$. Let $f \in \mathrm{Iso}_0(\mathcal{A})$ such that f fixes all elements v_i with $i \ne 2$, and also $-v_2$. Recall that, $(v_1, \dots, v_5)$ is the $\mathcal{A}$-basis defined in the proof of Lemma 5.3. We settle the lemma by showing that $T^f = T$ for all basic sets $T \in \mathrm{Bsets}(\mathcal{A})$. This will be done in five steps.

Claim (a). *$T^f = T$ for all $T \in \mathrm{Bsets}(\mathcal{A})$, $T \subset U_1 \cup U_2$.*

This is trivial for the basic sets $\{v_4\}$ and $\{v_5\}$, and hence Claim (a) follows for all basic sets $T \subset W = \langle v_4, v_5 \rangle$. Let $N = N_{\mathrm{Aut}(\mathcal{A})}(H_R)$. It follows from the proof of Lemma 5.3 that any basic set $T \subset U \setminus W$ is in the form $T = k(W_3 + v_3 + w)$ for some $w \in W$ and some $k \in \{1, \dots, p-1\}$ if $|N| = p^8$; whereas in the form $T = k(W + v_3)$ for some $k \in \{1, \dots, p-1\}$ if $|N| = p^9$.

Assume that $|N| = p^8$. As both $W_3 + v_3$ and $\{w\}$ are basic sets, we can write $(W_3 + v_3 + w)^f = (W_3 + v_3)^f + w^f = W_3^f + v_3^f + w^f = W_3 + v_3 + w$, where the second equality follows by Lemma 2.10(ii). Now, this together with Lemma 2.12(i) yields $T^f = T$ in the case when $|N| = p^8$. Similarly, $(W + v_3)^f = W + v_3$, and this with Lemma 2.12(i) yields $T^f = T$ if $|N| = p^9$.

Next, let us consider the isomorphism f^{U_1/W_1}. Since $\mathcal{A}_{U_1/W_1}$ is indecomposable, $f^{U_1/W_1} \in \mathrm{Aut}(U_1/W_1)$, see Lemma 2.17. This together with the fact that f fixes pointwise a generating set of U_1 shows that f^{U_1/W_1} is the identity mapping. Using this and that $\mathcal{A}_{U_1}$ is a U_1/W_1-wreath product, we deduce that $T^f = T$ for all basic sets $T \subset U_1 \setminus U$. Observe that, the latter statement has dual counterpart: $T^f = T$ for all basic sets $T \subset U_2 \setminus U$. This completes the proof of Claim (a).

Claim (b). *There exist an integer k and a function $F_2 : U_2 \to \{0, 1, \dots, p-1\}$ such that*

$$(v_1 + u)^f = v_1 + u^{x^k} + F_2(u)v_5 \text{ for all } u \in U_2. \tag{10}$$

The S-ring $\mathcal{A}_{H/U} = \mathbb{Q}\, H/U$. From this and the fact that f fixes a basis of H, we deduce that $f^{H/U}$ is the identity mapping, and therefore, f maps every U-coset to itself. In particular, it fixes the coset $U_2 + v_1$. Let $\tilde{f}$ denote the permutation of $U_2 + v_1$ induced by the action of f on $U_2 + v_1$. Choose an arbitrary basic set $T \in \mathrm{Bsets}(\mathcal{A}_{U_2})$, and let Σ be the subdigraph of $\mathrm{Cay}(H, T)$ induced by the set $U_2 + v_1$. By Claim (a), $T^f = T$, and this in turn implies that $f \in \mathrm{Aut}(\mathrm{Cay}(H, T))$, and $\tilde{f} \in \mathrm{Aut}(\Sigma)$. It is straightforward to check that $(v_1)_R$ is an isomorphism between $\mathrm{Cay}(U_2, T)$ and Σ. This implies that

$$(v_1)_R \tilde{f} (-v_1)_R \in \mathrm{Aut}(\mathrm{Cay}(U_2, T)). \tag{11}$$

We set g for $(v_1)_R \tilde{f}(-v_1)_R$. As $T \in \mathrm{Bsets}(\mathcal{A}_{U_2})$ was chosen arbitrarily, by definition, $g \in \mathrm{Aut}(\mathcal{A}_{U_2})$. Furthermore, $0^g = 0^{(v_1)_R \tilde{f}(-v_1)_R} = 0$. We have already shown that $\mathrm{Aut}(\mathcal{A}_{U_2/W_2})_0 = \langle x^{U_2/W_2} \rangle$, and thus we can write $g^{U_2/W_2} = (x^k)^{U_2/W_2}$ for some integer k. This allows us to define the function $F_2 : U_2 \to \{0, 1, \dots, p-1\}$, by letting $F_2(u)v_5 = u^g - u^{x^k}$ for each $u \in U_2$. Then, $u^{x^k} + F_2(u)v_5 = u^g = u^{(v_1)_R \tilde{f}(-v_1)_R} = (u + v_1)^f - v_1$, and Claim (b) follows.

Recall that $N = N_{\mathrm{Aut}(\mathcal{A})}(H_R)$.

Claim (c). *Suppose that $|N| = p^8$. Then for any $u, u' \in U_2$ with $u - u' \in U$, $F_2(u) = F_2(u')$.*

Suppose that $u, u' \in U_2$ such that $u - u' \in U$. Recall that $g \in \mathrm{Aut}(\mathcal{A}_{U_2})$ and g fixes every U-coset. Let us consider the automorphism g^{U_2/W_3}. It can be easily seen from the proof of Lemma 5.3(i) that $\mathcal{A}_{U/W_3} = \mathbb{Q}\, U/W_3$. By repeating the argument used to derive Eq. (11), we obtain that g^{U_2/W_3} acts on the coset $(U + u)/W_3 = (U/W_3) + (W_3 + u)$ as a translation by some element from U/W_3. This implies that, $u^g - u + u' - (u')^{\,g} \in W_3$. It follows from Eq. (8) that $u^{x^k} - u + u' - (u')^{\,x^k} \in W_3$ also holds, and by the definition of F_2 we can write

$$(F_2(u) - F_2(u'))v_5 = u^g - u^{x^k} - (u')^g + (u')^{x^k} \in W_3.$$

On the other hand, $\langle v_5 \rangle \cap W_3 = \{0\}$, and this yields Claim (c).

We turn next to the action of f on the coset $U_1 - v_2$. Notice that, the arguments given in (b) and (c) can be repeated after one replaces U_2 with U_1, W_2 with W_1, v_1 with $-v_2$, and w_5 with w_4. This gives rise to the following analogous statements:

Claim (d). *Suppose that $|N| = p^8$. Then there exist an integer l and a function $F_1 : U_1 \to \{0, 1, \dots, p-1\}$ such that*

$$(-v_2 + u)^f = -v_2 + u^{x^l} + F_1(u)v_4 \textit{ for all } u \in U_1. \tag{12}$$

Moreover, if $u, u' \in U_1$ *with* $u - u' \in U$*, then* $F_1(u) = F_1(u')$*.*

We are ready to handle the remaining basic sets of $\mathcal{A}$.

Claim (e). $T^f = T$ *for all* $T \in \mathrm{Bsets}(\mathcal{A})$*.*

In view of Claim (a), we can assume that $T \not\subset U_1 \cup U_2$. If $|N| = p^9$, then T is equal to a U-coset, see Lemma 5.3(ii). Using this and that f maps every U-coset to itself, Claim (e) follows at once if $|N| = p^9$.

In the rest of the proof it will be assumed that $|N| = p^8$. Let us consider the coefficient of v_3 in the linear combination of $(v_1 - v_2)^f$ with respect to the basis $(v_1, \dots, v_5)$. By Eq. (10), $(v_1 - v_2)^f = v_1 - (v_2)^{x^k} + F_2(-v_2)v_5$. Thus the required coefficient is equal to the coefficient of v_3 in $-(v_2)^{x^k}$, which can be computed directly using Eq. (8) to be equal to $-k$. On the other hand, by Eq. (12), $(v_1 - v_2)^f = -v_2 + (v_1)^{x^l} + F_1(v_1)v_4$. Thus the required coefficient is equal to the coefficient of v_3 in $(v_1)^{x^l}$, which can be computed directly using Eq. (8) to be equal to l. We conclude that $l = -k$.

Next, let us consider the element $w = (v_1 - v_2 + v_3)^f - (v_1 - v_2)^f$. Using Eq. (10) and Claim (c), we find

$$\begin{aligned} w &= v_1 + (-v_2)^{x^k} + v_3^{x^k} + F_2(-v_2 + v_3)v_5 - \big(v_1 + (-v_2)^{x^k} + F_2(-v_2)v_5\big) \\ &= v_3^{x^k} = v_3 + kv_4 + kv_5. \end{aligned}$$

On the other hand, using Eq. (12), the fact that $l = -k$ and Claim (d), we find

$$\begin{aligned} w &= -v_2 + (v_1)^{x^{-k}} + v_3^{x^{-k}} + F_1(v_1 + v_3)v_4 - \big(- v_2 + (v_1)^{x^{-k}} + F_1(v_1)v_4\big) \\ &= v_3^{x^{-k}} = v_3 - kv_4 - kv_5. \end{aligned}$$

We conclude that $k = 0$.

Let $U_3 = \langle U, v_1 - v_2 \rangle$. We have shown in the proof of Lemma 5.3(i) that all basic sets of $\mathcal{A}$ not contained in $U_1 \cup U_2 \cup U_3$ are U-cosets, and all basic sets contained in $U_3 \setminus U$ are W-cosets. Combining this with the fact that f maps every U-coset to itself, we get that Claim (e) holds whenever $T \not\subset U_1 \cup U_2 \cup U_3$. It remains to check whether the basic sets contained in $U_3 \setminus U$ are fixed by f. By Theorem 2.9, these basic sets are in the form $T^{(k)} = kT = \{ku : u \in T\}$, where $k \in \{1, \dots, p-1\}$ and $T \subset U_3 \cap (U_2 + v_1)$. Then, by Lemma 2.12(i), we are done if we show that $T^f = T$. Since $T \subset U_2 + v_1$, there exists some $u \in U_2$ such that $T = W + v_1 + u$. Now, applying Eq. (10) and using that $k = 0$, we finally get

$$T^f = W + (v_1 + u)^f = W + v_1 + u + F_2(u)v_5 = W + v_1 + u = T.$$

This completes the proof of Claim (e), and thus the proof of the lemma as well. □

Lemma 5.5. *Assuming Hypothesis 5.1, suppose that $\mathcal{A}$ is an U/W-wreath product, where $|U| = p^4$, $|W| = p$ and $\mathcal{A}_U$ is indecomposable. Then the S-ring $\mathcal{A}$ is CI.*

Proof. If $|A| = p$, then each basic set has size at most p, and therefore, each basic set $T \subset H \setminus U$ is equal to a W-coset. This implies that $\mathcal{A}_{H/W} = \mathbb{Q}H/W$. In particular, $\mathcal{A}_{H/W}$ is indecomposable, and we can apply Corollary 4.7 to get that $\mathcal{A}$ is a CI-S-ring. For the rest of the proof we assume that $|A| \geq p^2$.

Let A^U denote the group of automorphisms of U induced by restricting A to U. We show next that $|A^U| \leq p$. Assume to the contrary that $|A^U| > p$. Since $\mathcal{A}_U$ is indecomposable, it follows by Lemma 4.4 that $|\mathbf{O}_\theta(\mathcal{A})| = p^2$. Fix $u_1, u_2 \in \mathbf{O}_\theta(\mathcal{A})$ such that $\mathbf{O}_\theta(\mathcal{A}) = \langle u_1, u_2 \rangle$. Now, let $V < U$ be an $\mathcal{A}$-subgroup such that $|V| = p^3$ and $\mathbf{O}_\theta(\mathcal{A}) < V$, and fix an element $u_3 \in V \setminus \mathbf{O}_\theta(\mathcal{A})$. If A^U is not semiregular on the orbit u_3^A, then it follows that $|C_U(z)| = p^3$ for any non-identity $z \in (A^U)_{u_3}$. This contradicts Lemma 4.4, and thus $u_3^A = \mathbf{O}_\theta(\mathcal{A}) + u_3$ and $|A^U| = p^2$. There exist unique elements $x, y \in A$ that satisfy $u_3^x = u_1 + u_3$ and $u_3^y = u_2 + u_3$. Now, let u be an arbitrary element from $U \setminus V$. Then both $u^x - u$ and $u^y - u$ are in V. Therefore, there are integer numbers $k, l, m, k', l', m' \in \{0, 1, \ldots, p-1\}$ for which

$$u^x = u + ku_1 + lu_2 + mu_3 \text{ and } u^y = u + k'u_1 + l'u_2 + m'u_3.$$

Since $|A^U| = p^2$, the group A^U is abelian, and $u^{xy} = u^{yx}$. The coefficients of u_1 and u_2, resp., have to be the same in both sides, and this results in the equalities: $k + k' = k + k' + m'$ and $l + l' + m = l + l'$, resp., which gives that $m = m' = 0$. This implies that the orbit $u^{\langle x,y \rangle} = \mathbf{O}_\theta(\mathcal{A}) + u$, and therefore, $\operatorname{rad}(T) = \mathbf{O}_\theta(\mathcal{A})$ for the basic set of $\mathcal{A}$ that contains u. As u was chosen arbitrarily from $U \setminus V$, we obtain finally that $\mathcal{A}_U$ is a $V/\mathbf{O}_\theta(\mathcal{A})$-wreath product. This contradicts the assumption that $\mathcal{A}_U$ is indecomposable, and by this we have proved that $|A^U| \leq p$.

Let us fix $T_1 \in \operatorname{Bsets}(\mathcal{A})$ such that $T_1 \subset H \setminus U$ and $|\operatorname{rad}(T_1)|$ is the smallest among all $|\operatorname{rad}(T)|$ where T runs over the basic sets $T \in \operatorname{Bsets}(\mathcal{A})$, $T \subset H \setminus U$. Now, let $(v_1 \ldots, v_5)$ be an $\mathcal{A}$-basis such that $v_i \in U$ for all $i < 5$ and $v_5 \in T_1$. Let $f \in \operatorname{Iso}_0(\mathcal{A})$ such that f fixes v_i for all $i \in \{1, \ldots, 5\}$. We settle the lemma by showing that $T^f = T$ for all basic sets $T \in \operatorname{Bsets}(\mathcal{A})$.

Since f fixes all v_i and $U = \langle v_1, \ldots, v_4 \rangle$, the $\mathcal{A}$-subgroup U is mapped to itself by f. Then f^U is a normalized isomorphism of $\mathcal{A}_U$. Since $\mathcal{A}_U$ is indecomposable, by Corollary 4.6, $f^U \in \operatorname{Aut}(U)$, which implies that f^U is the identity mapping. In particular, $T^f = T$ for all basic sets $T \subset U$.

Now, we turn to the basic sets contained in $H \setminus U$. Let

$$V = \bigcap_{T \in \operatorname{Bsets}(\mathcal{A}),\, T \subset H \setminus U} \operatorname{rad}(T).$$

Let us consider the S-ring $\mathcal{A}_{H/V}$. Since $V \leq U$ and f fixes U pointwise, we get $V^f = V$, and thus $f^{H/V} \in \operatorname{Iso}_0(\mathcal{A}_{H/V})$ (see Proposition 2.10(iii)). We finish the proof by showing that $f^{H/V} = \mathrm{id}_{H/V}$. Indeed, then any basic set $T \subset H \setminus U$ satisfies $(T+V)^f = T+V$, and since $V \le \mathrm{rad}(T)$, it follows by Lemma 2.12(ii) that $T^f = T$.

Case 1. $|A| = p^2$.

Let $V_1 = \mathrm{rad}(T_1)$. Clearly, $V \le V_1$. We show at first that we may choose v_5 such that

$$T_1 = V_1 + v_5 \text{ and } V = V_1. \tag{13}$$

Since $|A^U| \le p$, there exists $x \in A$ such that $C_H(x) = U$. Then the $\langle x\rangle$-orbits not contained in U coincide with the cosets of a subgroup $W' < H$ of order p. Let T be a basic set of $\mathcal{A}$ outside U. It follows that $T + W + W' = T$. On the other hand, as $|A| = p^2$, $|T| \le p^2$. Thus if $W \ne W'$, then T is equal to a coset of $W + W'$, and this implies that Eq. (13) holds. Let $W' = W$. Let $A = \langle x, y\rangle$. Let us consider the S-ring $\mathcal{A}_{H/W}$. It follows that $\mathcal{A}_{H/W} = V(H/W, \langle y^{H/W}\rangle)$, where $y^{H/W}$ is the automorphism of H/W induced by the action of y on H/W. In view of Corollary 4.7 we may assume that $\mathcal{A}_{H/W}$ is decomposable. This implies that any $\langle y^{H/W}\rangle$-orbit is contained in a coset of a fixed subgroup of H/W of order p. It is not hard to show that this implies that $|C_{H/W}(y^{H/W})| = p^3$. Let U' be the unique subgroup of H that contains W and for which $U'/W = C_{H/W}(y^{H/W})$.

Suppose at first that $U' = U$. Then, any $\langle y\rangle$-orbit in U is contained in a W-coset, and hence $|C_U(y)| \ge p^3$. On the other hand, $\mathcal{A}_U$ indecomposable, and it follows from Lemma 4.4 that y acts as the identity on U. Hence, $C_H(y) = U$, and so $C_H(A) = U$. This shows that any basic set $T \subset H \setminus U$ is equal to a V-coset, in particular, Eq. (13) follows.

Next, suppose that $U' \ne U$, and choose an element $v \in U' \setminus U$. Then the basic set $T(v)$ containing v is equal to the coset $W + v$. Thus, $|\mathrm{rad}(T(v))| = p$, which is clearly minimal among all orders $|\mathrm{rad}(T)|$, $T \subset H \setminus U$. Then choosing v_5 to be v, we get $T_1 = T(v) = W + v_5$ and also $W = V_1 = V$, that is, Eq. (13) holds also in this case.

Let $U'' = \langle V, v_5\rangle$. The group H/V decomposes to the internal direct sum $H/V = \bar{U} + \bar{U}''$, where both factors $\bar{U} = U/V$ and $\bar{U}'' = U''/V$ are $\mathcal{A}_{H/V}$-subgroups. To simplify notation, we write $\bar{v}$ for the coset $V + v$, where v is any element in H, and $\bar{S}$ for the set $S/V \subseteq H/V$, where $S \subseteq H$. Notice that, $f^{H/V}$ fixes pointwise both $\bar{U}$ and $\bar{U}''$. Let $\bar{v} \in H/V$ be an arbitrary element. Then, $\bar{U} + \bar{v} = \bar{U} + \bar{u''}$ for some $\bar{u''} \in \bar{U}''$, and we can write

$$\bar{U} + \bar{v}^{f^{H/V}} = (\bar{U} + \bar{v})^{f^{H/V}} = (\bar{U} + \bar{u''})^{f^{H/V}} = \bar{U} + \bar{u''} = \bar{U} + \bar{v}.$$

Similarly, $\bar{U}'' + \bar{v} = \bar{U}'' + \bar{u}$ for some $\bar{u} \in \bar{U}$, and hence

$$\bar{U}'' + \bar{v}^{f^{H/V}} = (\bar{U}'' + \bar{v})^{f^{H/V}} = (\bar{U}'' + \bar{u})^{f^{H/V}} = \bar{U}'' + \bar{u} = \bar{U}'' + \bar{v}.$$

Therefore, $\bar{v}^{f^{H/V}} - \bar{v} \in \bar{U} \cap \bar{U}'' = \{\bar{0}\}$, and $f^{H/V} = \mathrm{id}_{H/V}$, as claimed.

Case 2. $|A| \geq p^3$.

Let K denote the kernel of A acting on the set U. Since $|A^U| \leq p$, $|K| \geq p^2$. Since $K \leq \mathrm{Aut}(H)$ and each element of K fixes U pointwise, there exists a subgroup $V' \leq U$ such that $|V'| = |K| \geq p^2$, and the K-orbits not contained in U are equal to the V'-cosets not contained in U. Note that, $V \geq V'$, and thus $|V_1| \geq |V| \geq p^2$, where $V_1 = \mathrm{rad}(T_1)$.

Suppose at first that $T_1 \neq V_1 + v_5$. By Proposition 2.4, $|T_1| = p^3$, which implies that $|V_1| = p^2$, and hence $V = V_1$. Also, the S-ring $\mathcal{A}_{H/V}$ is an exceptional S-ring over the group H/V, and it follows that $f^{H/V} \in \mathrm{Aut}(H/V)$. Since f fixes all generators v_i, it follows that $f^{H/V} = \mathrm{id}_{H/V}$.

Now, suppose that $T_1 = V_1 + v_5$. It is sufficient to show that $V = V_1$. Then the conditions in Eq. (13) hold, and $f^{H/V} = \mathrm{id}_{H/V}$ follows as in Case 1. Since $V \leq V_1$, $|V| \geq p^2$ and $|V_1| \leq p^3$, the equality $V = V_1$ follows if $|V_1| = p^2$. We are left with the case when $|V_1| = p^3$. Then, for each basis set $T \subset H \setminus U$, $|\mathrm{rad}(T)| = p^3$, implying that T is a coset of a subgroup that contains V. Assume to the contrary that $V \neq V_1$. Then $|H/V| = p^3$, and $\mathcal{A}_{H/V}$ has two basic sets which are cosets of distinct subgroups of order p. Since $|H/V| = p^3$, the S-ring $\mathcal{A}_{H/V}$ is Cayley isomorphic to one of the S-rings given in Table 1. A quick look at the table shows that none of these S-rings has two basic sets which are cosets of distinct subgroups of order p. Therefore, $V = V_1$, and this completes the proof of the lemma. □

Before we prove Theorem 5.2, one more technical lemma is needed.

Lemma 5.6. *Assuming Hypothesis 5.1, suppose that $\mathcal{A}$ is a U/W-wreath product, where $|U| = p^4$ and $|W| = p$. Furthermore, let V be an $\mathcal{A}$-subgroup such that $W < V < U$, $|V| = p^3$ and $|\mathbf{O}_\theta(\mathcal{A}) \cap V| \geq p^2$, and let $f \in \mathrm{Iso}_0(\mathcal{A})$. Then there exists $\varphi \in \mathrm{Aut}(H)$ such that $f\varphi$ maps each of U and W to itself, and the following conditions hold:*

(i) $T^{f\varphi}/W = T/W$ *for all* $T \in \mathrm{Bsets}(\mathcal{A})$.
(ii) $T^{f\varphi} = T$ *for all* $T \in \mathrm{Bsets}(\mathcal{A})$ *with* $T \subset V \cup (H \setminus U)$.
(iii) If either $V \subseteq \mathbf{O}_\theta(\mathcal{A})$, or each basic set of $\mathcal{A}$ contained in $V \setminus \mathbf{O}_\theta(\mathcal{A})$ is equal to a W-coset, then $f\varphi$ fixes pointwise V.

Proof. Let us fix five elements of H as follows:

$$v_5 \in W \setminus \{0\},\ v_4 \in (V \cap \mathbf{O}_\theta(\mathcal{A})) \setminus W,\ v_3 \in V \setminus \langle v_4, v_5\rangle,\ v_2 \in U \setminus V \text{ and } v_1 \in H \setminus U.$$

Clearly, $(v_1, \ldots, v_5)$ is an $\mathcal{A}$-basis. Let $\varphi_1 \in \mathrm{Aut}(H)$ be the automorphism defined by $\varphi : v_i^f \mapsto v_i$, $i \in \{1, \ldots, 5\}$, and let $f_1 = f\varphi$. It follows that $f_1 \in \mathrm{Iso}_0(\mathcal{A})$, and f_1 fixes all v_i. In particular, $W^{f_1} = W$, and thus $f_1^{H/W} \in \mathrm{Iso}_0(\mathcal{A}_{H/W})$.

The S-ring $\mathcal{A}_{H/W}$ is a CI-S-ring. Therefore, there exists some $\phi \in \mathrm{Aut}(H/W)$ such that $T^{f_1}/W = (T/W)^\phi$ for all $T \in \mathrm{Bsets}(\mathcal{A})$. Let $\phi_1 \in \mathrm{Aut}(H)$ such that ϕ_1 fixes W pointwise, and $\phi_1^{H/W} = \phi$. Then we have $W+v_4^{\phi_1} = (W+v_4)^{\phi_1^{H/W}} = (W+v_4)^{\phi} = W+v_4^{f_1} = W+v_4$. Thus, $v_4^{\phi_1} = v_4 + w$ for some $w \in W$. Now, let $\phi_2 \in \mathrm{Aut}(H)$ be defined by

$$\phi_2 : v_i \mapsto \begin{cases} v_i & \text{if } i = 1,2,3,5, \\ v_i - w & \text{if } i = 4, \end{cases}$$

and let $\varphi_2 = \phi_1\phi_2$. It follows that φ_2 satisfies the following:

(a) $u^{\varphi_2} = u$ for all $u \in \langle v_4, v_5\rangle$,
(b) $\varphi_2^{H/W} = \phi$.

Let $T_1 \in \mathrm{Bsets}(\mathcal{A})$ such that $v_3 \in T_1$. Then $T_1 = X + v_3$ for some subgroup $X \leq \langle v_4, v_5\rangle$, and we find $T_1^{f_1} = X^{f_1} + v_3^{f_1} = X + v_3 = T_1$. Thus, $T_1^{\varphi_2}/W = (T_1/W)^{\varphi_2^{H/W}} = (T_1/W)^{\phi} = T_1^{f_1}/W = T_1/W$. This gives $T_1^{\varphi_2} + W = T_1 + W$, and thus $T_1^{\varphi_2^{-1}}$ is contained in the coset $T_1 + W = X + W + v_3$. On the other hand, $X^{\varphi_2} = X$ follows by (a), implying that $T_1^{\varphi_2^{-1}} = X + v_3^{\varphi_2^{-1}}$. This with the previous observation yields that $T_1^{\varphi_2^{-1}} = T_1 + w_1$ for some $w_1 \in W$. Now, we define $\varphi_3 \in \mathrm{Aut}(H)$ by letting

$$\varphi_3 : v_i \mapsto \begin{cases} v_i & \text{if } i = 1,2,4,5, \\ v_3 + w_1 & \text{if } i = 3 \text{ and } X \neq W, \\ v_3^{\varphi_2^{-1}} & \text{if } i = 3 \text{ and } X = W. \end{cases}$$

Let $\varphi = \varphi_1\varphi_2^{-1}\varphi_3^{-1}$. Then $f\varphi = f_1\varphi_2^{-1}\varphi_3^{-1}$. It is easily seen that f_1 maps each of U and W to itself. The condition that φ_2 maps W to itself follows from (a) and the fact that $W = \langle v_5\rangle$. Then, $W \leq U^{\varphi_2}$, and for $U^{\varphi_2} = U$ it is enough to show that $U^{\varphi_2}/W = U/W$. This follows along the line: $U^{\varphi_2}/W = (U/W)^{\varphi_2^{H/W}} = (U/W)^{\phi} = U^{f_1}/W = U/W$. The definition of φ_3 shows that it also maps U and W to itself, and therefore, we obtain that $f\varphi$ maps each of U and W to itself. We finish the proof by showing that all conditions (i)–(iii) hold for $f\varphi$.

(i): Recall that $f_1 = f\varphi_1$. It follows from (b) that $T^{f_1\varphi_2^{-1}}/W = T/W$ for all $T \in \mathrm{Bsets}(\mathcal{A})$. We claim that $(W + v_i)^{\varphi_3} = W + v_i$ for all $i \in \{1, \dots, 5\}$. This is obvious if $i \neq 3$, or $i = 3$ and $X \neq W$. Let $i = 3$ and $X = W$. Then $T_1 = W + v_3$, and since $T_1^{f_1} = T_1$, it follows that $T_1^{\varphi_2}/W = T_1^{f_1}/W = T_1/W$, implying that $W + v_3^{\varphi_2^{-1}} = W + v_3$. Therefore, $(W + v_3)^{\varphi_3} = W^{\varphi_3} + v_3^{\varphi_3} = W + v_3^{\varphi_2^{-1}} = W + v_3$. Since $H = \langle v_1, \dots, v_5\rangle$, it follows that $(W+x)^{\varphi_3} = W+x$ for all $x \in H$. Consequently, $T^{f\varphi}/W = T^{f_1\varphi_2^{-1}\varphi_3^{-1}}/W = T^{\varphi_3^{-1}}/W = T/W$ for all $T \in \mathrm{Bsets}(\mathcal{A})$, and (i) follows.

(ii): Let T be an arbitrary basic set of $\mathcal{A}$. Note that, if $W \leq \mathrm{rad}(T)$, then using that $f\varphi$ maps W to itself, we can write $W + T^{f\varphi} = (W + T)^{f\varphi} = T^{f\varphi}$. Combining this with (i) yields $T^{f\varphi} = T^{f\varphi} + W = T + W = T$. In particular, (ii) holds whenever $T \subset H \setminus U$

or $T = T_1$ and $W = X$. Also, by (a) and the definition of φ_3, $f\varphi$ fixes pointwise $\langle v_4, v_5\rangle$, and this gives that (ii) also holds when $T \subset \langle v_4, v_4\rangle$. It remains to consider the case when $T \subset V \setminus \langle v_4, v_5\rangle$. Observe that, T can be written in the form $T = kT_1 + v$ for some $k \in \{1, \dots, p-1\}$ and some $v \in \langle v_4, v_5\rangle$. In view of Eq. (1) and Theorem 2.9, in order to prove $T^{f\varphi} = T$ it is sufficient to show that $T_1^{f\varphi} = T_1$. We have already shown above that this holds if $X = W$. If $X \neq W$, then the statement follows along the following line:

$$T_1^{f\varphi} = T_1^{f_1\varphi_2^{-1}\varphi_3^{-1}} = T_1^{\varphi_2^{-1}\varphi_3^{-1}} = (T_1 + w_1)^{\varphi_3^{-1}} = (X + v_3 + w_1)^{\varphi_3^{-1}} = X + v_3 = T_1.$$

(iii): Since $V = \langle v_3, v_4, v_5\rangle$, we are done if we show that $v_i^{f\varphi} = v_i$ for all $i \in \{3, 4, 5\}$. Using that $f\varphi = f_1\varphi_2^{-1}\varphi_3^{-1}$ and all v_i are fixed by f_1, it reduces to show that $v_i^{\varphi_2^{-1}\varphi_3^{-1}} = v_i$ for all $i \in \{3, 4, 5\}$. This follows immediately from (a) and the definition of φ_3 if $i = 4$ or $i = 5$. The condition $V \subset \mathbf{O}_\theta(\mathcal{A})$ is equivalent to $T_1 = \{v_3\}$, and therefore, $T_1 = \{v_3\}$ or $T_1 = W + v_3$. Now, recall that $T_1^{\varphi_2^{-1}} = T_1 + w_1$. This shows that, if $T_1 = \{v_3\}$, then $v_3^{\varphi_2^{-1}} = v_3 + w_1$, and so $v_3^{\varphi_2^{-1}\varphi_3^{-1}} = (v_3 + w_1)^{\varphi_3^{-1}} = v_3$. Finally, if $T_1 = W + v_3$, then $v_3^{\varphi_3} = v_3^{\varphi_2^{-1}}$, that is, $v_3^{\varphi_2^{-1}\varphi_3^{-1}} = v_3$. □

Everything is prepared to settle the main result of the section.

Proof of Theorem 5.2. Since $\mathcal{A}$ is decomposable, it is a U/W-wreath product where $W < U$, $|W| = p$ and $|U| = p^4$. Furthermore, we may assume because of Lemma 5.5 that $\mathcal{A}_U$ is a V/X-wreath product where $X < V < U$, $|X| = p$ and $|V| = p^3$.

Let $f \in \mathrm{Iso}_0(\mathcal{A})$. We have to show that there exists some $\varphi \in \mathrm{Aut}(H)$ such that $T^{f\varphi} = T$ for all basic sets $T \in \mathrm{Bsets}(\mathcal{A})$. By Lemma 5.6(i)–(ii), there exists some $\varphi_1 \in \mathrm{Aut}(H)$ such that $f_1 = f\varphi_1$ satisfies

$$T^{f_1}/W = T/W \text{ for all } T \in \mathrm{Bsets}(\mathcal{A}), \tag{14}$$

and

$$T^{f_1} = T \text{ for all } T \in \mathrm{Bsets}(\mathcal{A}) \text{ with } T \subset V \cup H \setminus U. \tag{15}$$

Now, if $W \le \mathrm{rad}(T)$ for every basic set $T \subset V \setminus U$, then Eq. (14) and Lemma 2.12(ii) imply that $T^{f_1} = T$ also holds, and hence we are done by letting $\varphi = \varphi_1$. For the rest of the proof it will be assumed that there exists some basic set $T_1 \subset U \setminus V$ such that $W \not\le \mathrm{rad}(T_1)$. Note that, this implies that $|T_1| = p$ or $|T_1| = p^2$. We consider below the two cases separately. For the rest of the proof u_1 will be a fixed element in T_1.

Case 1. $|T_1| = p$.

In this case $T_1 = X + u_1$. Since $W \not\le \mathrm{rad}(T_1)$, it follows that $X \neq W$. Since $X < V$, by Eq. (15), $X^{f_1} = X$, and thus $T_1^{f_1} = X^{f_1} + u_1^{f_1} = X + u_1^{f_1}$. Using this and Eq. (14), we conclude that $T_1^{f_1}+W = T_1+W$, implying that $T_1^{f_1}$ is contained in the coset $X+W+u_1$. Thus, $T_1^{f_1} = T_1+w_1$ for some $w_1 \in W$. Choose an automorphism $\varphi_2 \in \mathrm{Aut}(H)$ satisfying the following:

$$\varphi_2 : u_1 \mapsto u_1 - w_1,\ |C_H(\varphi_2)| = p^4 \text{ and } C_H(\varphi_2) \cap U = V.$$

Let $f_2 = f_1\varphi_2$. It is not hard to show that f_2 satisfies both Eqs. (14) and (15). We show below that $T^{f_2} = T$ also holds for each $T \in \mathrm{Bsets}(\mathcal{A})$ with $T \subseteq U\setminus V$, and therefore, we will be done by letting $\varphi = \varphi_1\varphi_2$.

First, $T_1^{f_2} = (T_1 + w_1)^{\varphi_2} = (X + u_1 + w_1)^{\varphi_2} = T_1$. Let us consider the S-ring $\mathcal{A}_{U/X}$ and its isomorphism $f_2^{U/X}$. Note that, the latter isomorphism belongs to $\mathrm{Iso}_0(\mathcal{A}_{U/X})$ because f_2 maps each of U and X to itself. The group U/X can be written as the internal direct sum $V/X + \langle X, u_1\rangle/X$ where both subgroups V/X and $\langle X, u\rangle/X$ are $\mathcal{A}_{U/X}$-subgroups. By Lemma 2.8, $\mathcal{A}_{U/X} = \mathcal{A}_{V/X} \otimes \mathcal{A}_{\langle X,u_1\rangle/X}$. Also, $f_2^{U/X}$ fixes every basic set $T' \in \mathrm{Bsets}(\mathcal{A}_{U/X})$ if $T' \subset V/X$ or $T' \subset \langle X, u_1\rangle/X$. This together with $\mathcal{A}_{U/X} = \mathcal{A}_{V/X} \otimes \mathcal{A}_{\langle X,u_1\rangle/X}$ yields that $f_2^{U/X}$ fixes all basic sets of $\mathcal{A}_{U/X}$. Then, using also that $\mathcal{A}_U$ is a V/X-wreath product, we conclude f_2 fixes all basic sets of $\mathcal{A}$ contained in $U \setminus V$, as required.

Case 2. $|T_1| = p^2$.

Assume for the moment that T_1 is equal to a coset $X' + u_1$ for some subgroup $X' < V$, $|X'| = p^2$, and $|W \cap X'| = 1$. It follows from Eq. (14) that $T_1^{f_1} = T_1 + w_1$ for some $w_1 \in W$. Repeating the argument used in Case 1, we find $\varphi_2 \in \mathrm{Aut}(H)$ such that $f_2 = f_1\varphi_2$ satisfies both Eqs. (14) and (15), and also $T_1^{f_2} = T_1$. Now, if $T \in \mathrm{Bsets}(\mathcal{A})$ is an arbitrary basic set such that $T \subset U \setminus V$, then it can be written in the form $T = k(T_1+w_2)$ for some $k \in \{1, \dots, p-1\}$ and some $w_2 \in W$. In view of Lemma 2.12(i), $T^{f_2} = T$ follows because $(T_1 + w_2)^{f_2} = T_1^{f_2} + w_2^{f_2} = T_1 + w_2$. All these show that we are done by choosing $\varphi = \varphi_1\varphi_2$.

For the rest of the proof it will be assumed that T_1 is not a coset. Equivalently, $\mathcal{A}_{U/X}$ is an exceptional S-ring. This implies that any basic set in $U \setminus V$ generates U, and therefore, V is the only $\mathcal{A}$-subgroup of order p^3 contained in U. This fact will be used later. Also, as $\mathcal{A}_{U/X}$ is exceptional, we have $\mathrm{rad}(T_1) = X$. Using also that $W \not\leq \mathrm{rad}(T_1)$, we obtain that $W \neq X$.

By Corollary 4.7, the S-ring $\mathcal{A}_{H/W}$ must be decomposable. Equivalently, there exist $\mathcal{A}$-subgroups Y and U' such that $W < Y < U'$, $|Y| = p^2$ and $|U'| = p^4$, and $\mathcal{A}_{H/W}$ is a $(U'/W)/(Y/W)$-wreath product.

Case 2.1. $U' = U$.

Assume that $Y = W + X$. In this case $\mathcal{A}$ is a U/X-wreath product, and we can finish this case by replacing first W with X, and then apply the argument used right after Eq. (15).

Now, suppose that $Y \neq W+X$. Since $W < Y$, this gives $X \cap Y = \{0\}$ and $|X+Y| = p^3$. Then $Y < U' = U$. We obtain that $X + Y$ is an $\mathcal{A}$-subgroup of order p^3 contained in U. As it was noted above, this forces that $X + Y = V$, in particular, $Y < V$. It follows that, either $V \subseteq \mathbf{O}_\theta(\mathcal{A})$, or any basic set contained in $V \setminus (W + X)$ is equal to a W-coset. By Lemma 5.6(iii), f_1 fixes pointwise V. Let us consider $f_1^{U/X}$, the isomorphism of $\mathcal{A}_{U/X}$ induced by f_1 acting on U/X. Then, $f_1^{U/X} \in \mathrm{Iso}_0(\mathcal{A}_{U/X})$, and since $\mathcal{A}_{U/X}$ is exceptional, $f_1^{U/X} \in \mathrm{Aut}(U/X)$, see Lemma 2.17. Also, as f_1 fixes pointwise V, $f_1^{U/X}$ centralizes V/X. This implies that $f_1^{U/X}$ acts on $U/X \setminus V/X$ as a translation by some element $X + v$ where $v \in V$. In particular, $T_1^{f_1}/X = (T_1 + v)/X$, and thus $T_1^{f_1} + X = T_1 + v + X$. Since $X \leq \mathrm{rad}(T_1)$, it follows that $X = X^{f_1} \leq \mathrm{rad}(T_1^{f_1})$, and we can write $T_1^{f_1} = T_1^{f_1} + X = T_1 + v + X = T_1 + v$. Using also that $|X \cap Y| = 1$, we can further write $T_1 + v = T_1 + v'$ for some $v' \in Y$. Then choose an automorphism $\varphi_2 \in \mathrm{Aut}(H)$ such that

$$u_1^{\varphi_2} = u_1 - v', \ |C_H(\varphi_2)| = p^4 \text{ and } C_H(\varphi_2) \cap U = V.$$

Recall that u_1 is the fixed element in T_1. Let $f_2 = f_1\varphi_2$. Using that $v' \in Y$ and $Y \leq \mathrm{rad}(T)$ for all $T \in \mathrm{Bsets}(\mathcal{A})$ with $T \subset H \setminus U$, it is not hard to show that f_2 satisfies Eq. (15). Also, $T_1^{f_2} = (T_1 + v')^{\varphi_2} = T_1$. Finally, let $T \in \mathrm{Bsets}(\mathcal{A})$ be an arbitrary basic set such that $T \subset U \setminus V$. Then, T can be written in the form $T = T_1 + w_2$, $w_2 \in W$, and thus we can write $T^{f_2} = T_1^{f_2} + w_2^{f_2} = T_1 + w_2 = T$. All these show that we are done by choosing $\varphi = \varphi_1\varphi_2$.

Case 2.2. $U' \neq U$.

Recall that, V is the only $\mathcal{A}$-subgroup of order p^3 contained in U. This implies that $U \cap U' = V$. Let $T \in \mathrm{Bsets}(\mathcal{A})$ such that $T \not\subset U \cup U'$. Since $\mathcal{A}$ is a U/W-wreath product and $\mathcal{A}_{H/W}$ is a $(U'/W)/(Y/W)$-wreath product, it follows that $Y \leq \mathrm{rad}(T) \leq U \cap U' = V$.

Suppose that $Y \neq W + X$. Then we obtain that $X + Y = V$ and it follows that, either $V \subseteq \mathbf{O}_\theta(\mathcal{A})$, or any basic set contained in $V \setminus (W + X)$ is equal to a W-coset. We can repeat the above argument used in Case 2.1 and find that $T_1^{f_1} = T_1 + v'$ holds for some $v' \in Y$. Then choose an automorphism $\varphi_2 \in \mathrm{Aut}(H)$ such that

$$u_1^{\varphi_2} = u_1 - v', \ |C_H(\varphi_2)| = p^4 \text{ and } C_H(\varphi_2) = U'.$$

It follows along the same line of reasoning as in Case 2.1 that the desired φ will be $\varphi_1\varphi_2$.

We are left with the case when $Y = W + X$. This shows that $\mathcal{A}$ is a U'/X-wreath product. The S-ring $\mathcal{A}_{U'}$ is a U'/W-wreath product, and we may assume that $\mathcal{A}_{U'/W}$ is indecomposable. Observe that, letting $U_1 = U$, $U_2 = U'$, $W_1 = X$ and $W_2 = W$, conditions (1) and (2) of Lemma 5.3 hold. Therefore, in view of Lemma 5.4, we may assume that condition (3) does not hold, that is, A acts regularly on any of its orbits not contained in $U \cup U'$. Now, fix an $\mathcal{A}$-basis $(v_1, \ldots, v_5)$ as follows:

$$v_1 \in U \setminus V, \ v_2 \in U' \setminus V, \ v_3 \in V \setminus (W + X), \ v_4 \in X \text{ and } v_5 \in W.$$

Then, let ψ be the automorphism of H defined by $\psi : v_i^f \mapsto v_i$ for all $i \in \{1, \dots, 5\}$, and let $f_3 = f\psi$. We finish the proof by showing that $T^{f_3} = T$ for all basic sets $T \in \mathrm{Bsets}(\mathcal{A})$. One can settle the equality $T^{f_3} = T$ for $T \subset U \cup U'$ by copying the argument used in the proof of Claim (a) in the proof of Lemma 5.4.

Now, suppose that $T \in \mathrm{Bsets}(\mathcal{A})$ with $T \subset H \setminus (U \cup U')$. By Lemma 2.18, T is contained in both a U-coset and a U'-coset, hence it is contained in a V-coset, recall that $V = U \cap U'$. We claim that T is, in fact, equal to a V-coset. Assume to the contrary that T is properly contained in a V-coset. In particular, we have $|T| \le p^2$. Let $G = H_R A$, $N = N_{\mathrm{Aut}(\mathcal{A})}(H_R)$, and N_0 be the stabilizer of 0 in N. Then, $\mathrm{Aut}(\mathcal{A}) = G^{(2)}$ and $C_{H_R}(A) \le Z(G)$. By Proposition 2.1, $C_{H_R}(A) \le Z(\mathrm{Aut}(\mathcal{A}))$, and hence $C_{H_R}(A) \le C_{H_R}(N_0)$. The S-ring $\mathcal{A}$ can be expressed as $\mathcal{A} = V(H, N_0)$ such that $p^2 \le |C_H(N_0)|$. Now, we can replace A with N_0, and assume, in addition, that N_0 is regular on T. Therefore, $|N_0| = |T| \le p^2$. On the other hand, N_0 contains two elements x and x' such that $C_H(x) = U$ and x acts on the elements $v \in H \setminus U$ as the right translation $v^x = v + w$ for a fixed nonzero $w \in W$, and $C_H(x') = U'$ and x' acts on the elements $v \in H \setminus U'$ as the right translation $v^x = v + w'$ for a fixed nonzero $w' \in X$. It is easily seen that $V(H, \langle x, x' \rangle) \ne \mathcal{A} = V(H, N_0)$, implying that $\langle x, x' \rangle < N_0$. This, however, contradicts the previously obtained bound $|N_0| \le p^2$, and by this we have proved that T is indeed equal to a V-coset.

Finally, let us consider the S-ring $\mathcal{A}_{H/V}$, and the induced isomorphism $f_3^{H/V} \in \mathrm{Iso}_0(\mathcal{A}_{H/V})$. It is easily seen that $\mathcal{A}_{H/V} = \mathbb{Q}(H/V)$, and therefore, $f_3^{H/V} \in \mathrm{Aut}(H/V)$. Using this and that f_3 fixes all v_i, $i \in \{1, \dots, 5\}$, we find $f_3^{H/V} = \mathrm{id}_{H/V}$. Thus, $(T + V)^{f_3} = T + V$, and combining this with $V \le \mathrm{rad}(T)$, Lemma 2.12(ii) gives that $T^{f_3} = T$. This completes the proof of Case 2.2. □

6. Proof of Theorem 3.5 II: the indecomposable S-rings

In this section, we turn to the indecomposable S-rings in Theorem 3.5 and prove the following theorem:

Theorem 6.1. *Assuming Hypothesis 5.1, suppose that $\mathcal{A}$ is indecomposable. Then $\mathcal{A}$ is a CI-S-ring.*

Our main result Theorem 3.5 follows then as the consequence of Theorems 5.2 and 6.1.

Theorem 6.1 will be proved in the end of the section after six preparatory lemmas. In the first two lemmas we derive some properties of indecomposable p-S-rings with thin radical of order at least p^2.

Lemma 6.2. *Let $\mathcal{B}$ be an indecomposable p-S-ring over a group $H \cong \mathbb{Z}_p^5$ such that $|\mathbf{O}_\theta(\mathcal{B})| \ge p^2$, and let $x \in N_{\mathrm{Aut}(\mathcal{B})}(H_R)$ such that $x \ne \mathrm{id}_H$ and $0^x = 0$. Then $|C_H(x)| \le p^3$.*

Proof. Since $x \neq \mathrm{id}_H$, it follows that $C_H(x) \leq p^4$. Assume to the contrary that $|C_H(x)| = p^4$. Let $U = C_H(x)$, and for a fixed $v_1 \in H \setminus U$, let $W = \langle v_1^x - v_1 \rangle$. Then $|W| = p$, and it follows that the orbit $v^{\langle x \rangle} = W + v$ for all $v \in H \setminus U$. It can be shown in the same way as in the proof of Lemma 4.4 that neither U nor W are $\mathcal{B}$-subgroups.

Let $V_1 \leq \mathbf{O}_\theta(\mathcal{B})$ such that $|V_1| = p^2$ and let $V_2 = V_1 + W$. Then $V_1 < U$, $|V_1 \cap W| = 1$, and therefore $|V_2| = p^3$. Let U' be a $\mathcal{B}$-subgroup of order p^4 such that $V_1 < U'$. Then $U \neq U'$, and thus there exists $u \notin U \cup U'$. Let $T \in \mathrm{Bsets}(\mathcal{B})$ such that $u \in T$. Then $W + u \subseteq T$, implying that $W \leq U'$. We conclude that $U \cap U' = V_1 + W = V_2$.

Let $x^{U'}$ denote the restriction of x to the $\mathcal{B}$-subgroup U'. Clearly, $C_{U'}(x^{U'}) = V_2$, and thus by Lemma 4.4, $\mathcal{B}_{U'}$ is a V'/W'-wreath product for some $\mathcal{B}$-subgroups $0 < W' < V' < U'$, where $|W'| = p$ and $|V'| = p^3$. Let $T \in \mathrm{Bsets}(\mathcal{B})$ such that $T \subseteq U' \setminus V'$ and $T \not\subseteq U$. Then using that T contains a W-coset and $W' \leq \mathrm{rad}(T)$, it follows that T contains a $(W + W')$-coset (recall that $W' \neq W$ as W is not an $\mathcal{A}$-subgroup). This together with Proposition 2.18(ii) yields that $W \leq \mathrm{rad}(T) \leq V'$, and thus $W < V'$. On the other hand it is clear that $V_1 < V'$, and this with the previous observation yields $V' = W + V_1 = V_2$. In particular, V_2 is a $\mathcal{B}$-subgroup. Since U is not a $\mathcal{B}$-subgroup, the S-ring $\mathcal{B}_{H/V_2} \cong \mathbb{Q}\mathbb{Z}_p \wr \mathbb{Q}\mathbb{Z}_p$, and this implies that U' is the only $\mathcal{B}$-subgroup which has order p^4 and contains V_2. This property will be used later. Note also that,

$$W' + W \leq \mathrm{rad}(T) \text{ for all } T \in \mathrm{Bsets}(\mathcal{B}) \text{ such that } T \subset U' \setminus V_2. \tag{16}$$

Next, let us consider the S-ring $\mathcal{B}_{H/V_1}$. Let $T \in \mathrm{Bsets}(\mathcal{B})$ such that $T \cap U \neq \emptyset$ and $T \not\subseteq U$. The latter condition implies that T contains some W-coset, and thus $|T/V_1| \geq p^2$. It follows by Proposition 2.14, that T/V_1 is equal to a U'/V_1 coset. It is easy to see that $\mathcal{A}_{U'/V_1} \cong \mathbb{Q}\mathbb{Z}_p \wr \mathbb{Q}\mathbb{Z}_p$; and we conclude that $\mathcal{B}_{H/V_1} \cong \mathbb{Q}Z_p \wr \mathbb{Q}\mathbb{Z}_p \wr \mathbb{Q}\mathbb{Z}_p$.

Now, fix a coset $U' + v_1$ distinct from U', and let $T_1 \in \mathrm{Bsets}(\mathcal{B})$ such that $T_1 \subseteq U' + v_1$. Let $T \in \mathrm{Bsets}(\mathcal{B})$ be another basic set contained in $U' + v_1$. Since $\mathcal{B}_{H/V_1} \cong \mathbb{Q}Z_p \wr \mathbb{Q}\mathbb{Z}_p \wr \mathbb{Q}\mathbb{Z}_p$, it follows that both $T_1 \cap V_1 + v_1$ and $T \cap V_1 + v_1$ are nonempty. Choose $u_1 \in T_1 \cap V_1 + v_1$ and $u_2 \in T \cap V_1 + v_1$. Then, $u_2 - u_1 \in V_1 \leq \mathbf{O}_\theta(\mathcal{B})$, hence by Eq. (1), $T_1 + u_2 - u_1 = T$. Thus, $\mathrm{rad}(T) = \mathrm{rad}(T_1)$, and combining this with Theorem 2.9, we conclude that $\mathrm{rad}(T') = \mathrm{rad}(T_1)$ for any basic set $T' \not\subseteq U'$. Since $\mathcal{B}$ is indecomposable, it follows that $\mathrm{rad}(T_1)$ is trivial. This together with Lemma 2.18(ii) yields that

$$|T_1 \cap V_1 + v| = 1 \text{ for all } v \in U' + v_1. \tag{17}$$

Indeed, if $u_1, u_2 \in T_1 \cap V_1 + v$, then for $W = \langle u_1 - u_2 \rangle$, $|T_1 \cap W + u_2| \geq 2$, and so $W \leq \mathrm{rad}(T_1)$, a contradiction. Thus, $|T_1 \cap V_1 + v| \leq 1$, and since $|T_1 \cap V_1 + v| \geq 1$ also holds, see the above paragraph, Eq. (17) follows.

By Eq. (16), we can choose a subgroup $W_1 < V_1$ which satisfies the following property: for all $T \in \mathrm{Bsets}(\mathcal{B})$, $T \subset U' \setminus V_2$, either $|T| = p^3$ or $W_1 \not< \mathrm{rad}(T)$. Notice that, this property implies that $\mathcal{B}_{U'/W_1} \cong \mathbb{Q}Z_p \wr \mathbb{Q}\mathbb{Z}_p \wr \mathbb{Q}\mathbb{Z}_p$.

Let us consider x^{H/W_1}, the automorphism of H/W_1 induced by x acting on H/W_1. By Lemma 4.3, x cannot be in the kernel of $\mathrm{Aut}(\mathcal{B})$ acting on H/W_1, and so

$x^{H/W_1} \neq \mathrm{id}_{H/W_1}$. Then, $C_{H/W_1}(x^{H/W_1}) = U/W_1$, and thus by Lemma 4.4, $\mathcal{B}_{H/W_1}$ is an $(X/W_1)/(Y/W_1)$-wreath product for some $\mathcal{B}$-subgroups X and Y, where $|X| = p^4$, $|Y| = p^2$ and $W_1 < Y < X$. Notice that, $X \cap U'$ is a $\mathcal{B}$-subgroup of order p^3. On the other hand, since $\mathcal{B}_{U'/W_1} \cong \mathbb{Q}Z_p \wr \mathbb{Q}\mathbb{Z}_p \wr \mathbb{Q}\mathbb{Z}_p$, V_2 is the only $\mathcal{B}$-subgroup in U' that has order p^3 and contains W_1. Using this and that $W_1 < X \cap U'$, it follows that $V_2 = X \cap U'$. We have shown above that U' is the only $\mathcal{B}$-subgroup containing V_2, hence $X = U'$. Thus, $W_1 < Y < U'$, and using again that $\mathcal{B}_{U'/W_1} \cong \mathbb{Q}Z_p \wr \mathbb{Q}\mathbb{Z}_p \wr \mathbb{Q}\mathbb{Z}_p$, we can see that V_1 is the only $\mathcal{B}$-subgroup in U' that has order p^2 and contains W_1, and so $Y = V_1$. To sum up, $\mathcal{B}_{H/W_1}$ is an $(U'/W_1)/(V_1/W_1)$-wreath product. Recall that, T_1 is a basic set contained in the coset $U' + v_1$. Then, T_1 satisfies $V_1/W_1 < \mathrm{rad}(T_1/W_1)$. In particular, for any $u \in T_1$, $|T_1 \cap (V_1 + u)| \geq |T_1/W_1 \cap (V_1 + u)/W_1| = p$, which, however, contradicts Eq. (17). This completes the proof of the lemma. □

Lemma 6.3. *Let $\mathcal{B}$ be an indecomposable non-CI p-S-ring over a group $H \cong \mathbb{Z}_p^5$ such that $|\mathbf{O}_\theta(\mathcal{B})| \geq p^2$. Then $|N_{\mathrm{Aut}(\mathcal{B})}(H_R)| \geq p^7$.*

Proof. Let $N = N_{\mathrm{Aut}(\mathcal{B})}(H_R)$. Assume to the contrary that $|N| < p^6$. Let $K \leq N$ be the subgroup given in Proposition 3.1. The stabilizer $(KH_R)_0 \leq N_0$, hence we can write

$$\frac{|K||H_R|}{|K \cap H_R|} = |KH_R| = |(KH_R)_0| \cdot |H| \leq p \cdot |H|.$$

Since $K \neq H_R$, we can choose a non-identity element $x \in (KH_R)_0$. Then the above inequality yields $|C_H(x)| \geq |K \cap H_R| \geq |K|/p = p^4$. This, however, contradicts Lemma 6.2. □

The key step in proving Theorem 6.1 will be to show that, if $\mathcal{A}$ is non-CI, then $\mathrm{Aut}(\mathcal{A}) \cap \mathrm{Aut}(H)$ contains a subgroup L such that $|L| = p^2$ and $|C_H(L)| = p^3$. The next three lemmas are devoted to the arising S-ring $V(L, H)$.

Lemma 6.4. *Assuming Hypothesis 5.1, suppose that $\mathcal{A}$ is indecomposable, and let $L \leq \mathrm{Aut}(\mathcal{A}) \cap \mathrm{Aut}(H)$ such that $|L| = p^2$ and $|C_H(L)| = p^3$. Then the following conditions hold:*

(i) The S-ring $V(H, L)$ is indecomposable.
(ii) Let T be a basic set of $V(H, L)$ such that $|T| > 1$. Then T is equal to an X-coset for some subgroup $X < C_H(L)$ of order $|X| = p^2$.
(iii) Let T and T' be two basic sets of $V(H, L)$ of size p^2 for which $\langle T, C_H(L)\rangle \neq \langle T', C_H(L)\rangle$. Then $\mathrm{rad}(T) \neq \mathrm{rad}(T')$.

Proof. Let $N = N_{\mathrm{Aut}(\mathcal{A})}(H_R)$ and N_0 be the stabilizer of 0 in N. Note that, $L \leq N_0$ and $\mathcal{A} = V(H, N_0)$. Furthermore, we let $\mathcal{B} = V(H, L)$ and $U = C_H(L)$.

(i): Assume to the contrary that $\mathcal{B}$ is a X/Y-wreath product, where $X > Y$, $|X| = p^4$ and $|Y| = p$. Let $x \in \mathrm{Aut}(H)$ be defined by $v^x = v$ for all $v \in X$, and $v^x = v + v_1$ for all $v \in H \setminus X$, where $v_1 \in Y$ is a fixed non-zero element. Then $C_H(x) = X$ and $x \in \mathrm{Aut}(\mathcal{B})$. Also, as $L \le N_0$, $\mathcal{B} = V(H, L) \supseteq V(H, N_0) = \mathcal{A}$, and thus $\mathrm{Aut}(\mathcal{B}) \le \mathrm{Aut}(\mathcal{A})$. In particular, $x \in \mathrm{Aut}(\mathcal{A})$, which contradicts Lemma 6.2.

(ii): As $|L| = p^2$, $|T| \le p^2$, and if $|T| < p^2$, then L_v is nontrivial, where $v \in T$, and L_v is the stabilizer of v in L. Then for $x \in L_v$, $v \in C_H(x)$, and thus $|C_H(x)| \ge |\langle U, v\rangle| = p^4$, which contradicts Lemma 6.2, recall that $\mathcal{B}$ is indecomposable. We deduce that $|T| = p^2$. Note that, since there is no basic set of size p, it follows that every $\mathcal{B}$-subgroup of order p^2 must be contained in U. This fact will be used later.

Let $V < H$ be a $\mathcal{B}$-subgroup such that $U < V$ and $|V| = p^4$. If $T \subset V$, then it easy to see that T is equal to a coset of a subgroup of U of order p^2, and (ii) follows.

Now, suppose that $T \not\subset U$. By Lemma 2.18(iii), $U \cap \mathrm{rad}(T) \ne \{0\}$, and thus we can choose $W < U$ such that $|W| = p$ and $W \le \mathrm{rad}(T)$. Let us consider the S-ring $\mathcal{B}_{H/W}$. Then T/W is a basic set of $\mathcal{B}_{H/W}$ of size $|T/W| = p$. Denote by $L^{H/W}$ the subgroup of $\mathrm{Aut}(\mathcal{B}_{H/W})$ induced by L acting on H/W. By Lemma 4.3, $|L^{H/W}| = p^2$. It follows from this and Proposition 2.4 that T/W cannot generate H/W. This together with the fact that $W \le \mathrm{rad}(T)$ shows that $\langle T\rangle \ne H$, and thus $|\langle T\rangle| = p^3$ or $|\langle T\rangle| = p^4$. If $|\langle T\rangle| = p^3$, then it is easily seen that T is equal to a coset of a subgroup of U, and so (ii) follows.

Assume that $\langle T\rangle = p^4$, and let $V' = \langle T\rangle$. We show below that this case cannot occur. If $U < V'$, then it is easy to see that T is equal to a coset of a subgroup of U, contradicting that $\langle T\rangle = p^4$. Thus, $|U \cap V'| = p^2$, and H can be expressed as the internal direct sum $H = V' + X$ for some subgroup $X < U$, $|X| = p$. Note that, as $X \le \mathbf{O}_\theta(\mathcal{B})$, it follows from Lemma 2.8 that $\mathcal{B} = \mathcal{B}_{V'} \otimes \mathcal{B}_X$.

Let $Y = V \cap V'$. Then Y is a $\mathcal{B}$-subgroup of order p^3 such that $U \cap V' < Y$. Since $\langle T\rangle = V'$, $T \not\subset Y$. The radical $\mathrm{rad}(T) \ne U \cap V'$, for otherwise, T cannot generate V'. It follows that the basic sets of $\mathcal{B}$ contained in $V' \setminus Y$ are in the form $k(T + u)$ for some $k \in \{1, \dots, p-1\}$ and some $u \in U \cap V'$. Since $W \le \mathrm{rad}(T)$, we obtain that $\mathcal{B}_{V'}$ is a Y/W-wreath product. This implies that $\mathcal{B} = \mathcal{B}_{V'} \otimes \mathcal{B}_X$ is a $(Y + X)/W$-wreath product, which contradicts (i).

(iii): Assume to the contrary that $\mathrm{rad}(T) = \mathrm{rad}(T')$ and $\langle U, T\rangle \ne \langle U, T'\rangle$. Let $X = \mathrm{rad}(T)$, and let us consider the S-ring $\mathcal{B}_{H/X}$. By (ii), both T and T' are X-cosets. Since $\langle U, T\rangle \ne \langle U, T'\rangle$, we find that the elements T/X and T'/X generate a subgroup of H/X of order p^2, and this subgroup intersects U/X trivially. We conclude that $\mathcal{B}_{H/X} \cong \mathbb{Q}\,\mathbb{Z}_p^3$. Consequently, every basic set of $\mathcal{B}$ is contained in some X-coset. This together with (ii) shows that $\mathcal{B}$ is an U/X-wreath product, which contradicts (i). □

Lemma 6.5. *With the notation of Lemma 6.4,* $|\mathrm{Aut}(V(H, L))| = p^8$.

Proof. As in the previous lemma, we let $\mathcal{B} = V(H, L)$ and $U = C_H(L)$. We start with fixing a suitable $\mathcal{B}$-basis. Fix an element $v_1 \in H \setminus U$, and another $v_2 \in H \setminus \langle U, v_1\rangle$. For

$i = 1, 2$, let $T_i \in \mathrm{Bsets}(\mathcal{B})$ such that $v_i \in T_i$. By Lemma 6.4(ii)–(iii), $T_i - v_i$ is a subgroup of U of order p^2. It will be convenient to denote these subgroups by U_∞ and U_0, namely, we let $T_1 = U_\infty + v_1$ and $T_2 = U_0 + v_2$. Then $|U_\infty \cap U_0| = p$. Let $v_4 \in U_\infty \cap U_0$, $v_4 \neq 0$. Then, there exist $x, y \in L$ satisfying $v_2^x - v_2 = v_1^y - v_1 = v_4$. Let $v_3 = v_1^x - v_1$ and $v_5 = v_2^y - v_2$. We prove next that $\langle v_1, v_2, v_3, v_4, v_5\rangle = H$ and $\langle x, y\rangle = L$. For the first part it is enough to show that $\langle v_3, v_4, v_5\rangle = U$. Now, $v_1^x \in T_1 = U_\infty + v_1$, hence $v_3 \in U_\infty$. Suppose for the moment that $v_3 = kv_4$ for some integer k. Then $(kv_2)^x - kv_2 = kv_4 = v_3 = v_1^x - v_1$, implying that $kv_2 - v_1$ is fixed by x, and hence $kv_2 - v_1 \in C_H(x) = U$, which is impossible. We conclude that $U_\infty = \langle v_3, v_4\rangle$. We obtain by a similar argument that $U_0 = \langle v_4, v_5\rangle$, and therefore, $\langle v_3, v_4, v_5\rangle = U_\infty + U_0 = U$. For the second part, if $y = x^m$ for some integer m, then we can write $v_2 + v_5 = v_2^y = v_2^{x^m} = v_2 + mv_4$, contradicting that $\langle v_4, v_5\rangle = U_0$ has order p^2. Thus, $\langle x, y\rangle = L$, as required. It is clear that $(v_1, \dots, v_5)$ is a $\mathcal{B}$-basis.

Let $V = \langle v_1, v_2\rangle$. Then H can be written as the internal direct sum $H = V + U$. For $w \in H$, let w_V and w_U denote the projection of w into V and U, resp. Furthermore, let $I = GF(p) \cup \{\infty\}$; and for $i \in I$, define the elements $\hat{v}_i \in V$, and subgroups $U_i \leq U$ as follows

$$\hat{v}_i = \begin{cases} v_1 & \text{if } i = \infty \\ iv_1 + v_2 & \text{otherwise,} \end{cases} \qquad U_i = \begin{cases} \langle v_3, v_4\rangle & \text{if } i = \infty \\ \langle iv_3 + v_4, iv_4 + v_5\rangle & \text{otherwise.} \end{cases}$$

Let $G = \mathrm{Aut}(\mathcal{B})$ and G_w be the stabilizer of an element w in G. Observe that, the lemma is equivalent to show that $|G_0| = p^3$. We are going to derive this in six steps.

Claim (a). *The basic sets of $\mathcal{B}$ not contained in U are in the form*

$$U_i + j\hat{v}_i + u,\ i \in I,\ j \in GF(p) \setminus \{0\},\ u \in U. \tag{18}$$

By definition, the basic sets in question are equal to the L-orbits w^L, $w \in H \setminus U$, where $L = \langle x, y\rangle$. Now, $w = j\hat{v}_i + u$ for some $j \in GF(p) \setminus \{0\}$, $i \in I$ and $u \in U$. A direct computation yields that the L-orbit $\hat{v}_i^L = U_i + \hat{v}_i$. This together with the fact that $u \in C_H(L)$ yields Claim (a).

Let $\mathrm{Fun}_0(V, U)$ denote the set of all functions $F : V \to U$ such that $F(0) = 0$. For $F \in \mathrm{Fun}_0(V, U)$, we define the permutation $g_F \in \mathrm{Sym}(H)$ as follows:

$$w^{g_F} = w + F(w_V),\ w \in H, \tag{19}$$

where w_V denotes the projection of w to V (recall that, we have $H = V + U$).

Claim (b). *For every $g \in G_0$, $g = g_F$ for some $F \in \mathrm{Fun}_0(V, U)$.*

Since U is a $\mathcal{B}$-subgroup, the set H/U form a block system for G. Let us consider $g^{H/U}$, the permutation of H/U induced by g acting on H/U. Then, $g^{H/U} \in \mathrm{Aut}(\mathcal{B}/U)$. It is easy to see that $\mathcal{B}/U = \mathbb{Q}\, H/U$, and thus we get that $g^{H/U} = \mathrm{id}_{H/U}$. Equivalently,

g fixes setwise every U-coset. On the other hand, by Eq. (4), g centralizes u_R for all $u \in U$. These two facts imply Claim (b).

Claim (c). *For every $F \in \mathrm{Fun}_0(V, U)$, $g_F \in G_0$ if and only if the following conditions hold:*

$$F(v + \hat{v}_i) - F(v) \in U_i \text{ for all } v \in V \text{ and } i \in I. \tag{20}$$

Let $F \in \mathrm{Fun}_0(V, U)$. By definition, $g_F \in G_0$ if and only if $g_F \in \mathrm{Aut}(\mathrm{Cay}(H, T))$ for any basic set $T \in \mathrm{Bsets}(\mathcal{B})$. It is clear that g_F centralizes u_R for all $u \in U$. Hence, $g_F \in \mathrm{Aut}(\mathrm{Cay}(H, T))$ whenever $T \subset U$. Now, suppose that $T \not\subset U$. By Claim (a), $T = U_i + j\hat{v}_i + u$ for some $j \in GF(p) \setminus \{0\}$, $i \in I$ and $u \in U$. Therefore, $g_F \in \mathrm{Aut}(\mathrm{Cay}(H, T))$ if and only if

$$(U_i + j\hat{v}_i + u + w)^{g_F} = U_i + j\hat{v}_i + u + w^{g_F} \text{ for all } w \in H.$$

By Eq. (19), this reduces to

$$U_i + j\hat{v}_i + w + u + F(j\hat{v}_i + w_V) = U_i + j\hat{v}_i + w + u + F(w_V).$$

Equivalently, $F(v + j\hat{v}_i) - F(v) \in U_i$ for all $v \in V$. Since,

$$F(v + j\hat{v}_i) - F(v) = \sum_{k=1}^{j} \big(F(v + k\hat{v}_i) - F(v + (k-1)\hat{v}_i) \big),$$

it follows that $F(v + j\hat{v}_i) - F(v) \in U_i$ for all $v \in V$ if and only if $F(v + \hat{v}_i) - F(v) \in U_i$ for all $v \in V$, and Eq. (20) follows.

Claim (d). *If $i, j, k \in I$ are pairwise distinct, and $u_1, u_2, u_3 \in U$ are arbitrary elements, then $|U_i + u_1 \cap U_j + u_2 \cap U_k + u_3| = 1$.*

It is not hard to show that Claim (d) follows from $U_i \cap U_j \cap U_k = \{0\}$. Let $\alpha v_3 + \beta v_4 + \gamma v_5 \in U_i \cap U_j \cap U_k$. Suppose at first that none of i, j and k is equal to ∞. Then, using the definition of the subgroups U_i, U_j and U_k, we find α_1, α_2 and α_3 in $GF(p)$ such that

$$\begin{aligned} \alpha = \alpha_1 i \; &= \; \alpha_2 j \; = \; \alpha_3 k \\ \beta = \alpha_1 + \gamma i \; &= \; \alpha_2 + \gamma j \; = \; \alpha_3 + \gamma k. \end{aligned}$$

Using also that i, j and k are pairwise distinct, we deduce that $\beta = \gamma(i + j) = \gamma(i + k) = \gamma(j + k)$, and hence $\alpha = \beta = \gamma = 0$, and so $U_i \cap U_j \cap U_k = \{0\}$.

Now, suppose that $k = \infty$. Since $U_\infty = \langle v_3, v_4 \rangle$, $\gamma = 0$, and $\alpha v_3 + \beta v_4 = \alpha_1(i v_3 + v_4) = \alpha_2(j v_3 + v_4)$. Since $i \neq j$, it follows that $\alpha_1 = \alpha_2 = \alpha = \beta = 0$, and $U_i \cap U_j \cap U_k = \{0\}$, as required.

Claim (e). $|G_0 \cap G_{v_1}| \le p$.

Let $g \in G_0 \cap G_{v_1}$. By Claim (b), $g = g_F$ for some $F \in \mathrm{Fun}_0(V, U)$. Notice that, $F(0) = F(v_1) = 0$. Let us consider the image $F(2v_1)$. Then, we can express $2v_1$ as $2v_1 = v_1 + \hat{v}_\infty$, hence by Eq. (20), $F(2v_1) - F(v_1) \in U_\infty$. Also, $v_1 + v_2 = 2v_1 + \hat{v}_{-1}$ and $v_2 = 2v_1 + \hat{v}_{-2}$, and using again Eq. (20), we find $F(v_1 + v_2) - F(2v_1) \in U_{-1}$ and $F(v_2) - F(2v_1) \in U_{-2}$. All these yield

$$F(2v_1) \in U_\infty + F(v_1) \;\cap\; U_{-1} + F(v_1 + v_2) \;\cap\; U_{-2} + F(v_2). \tag{21}$$

On the other hand, $F(v_2) \in U_0 \cap U_{-1} = \langle -v_4 + v_5 \rangle$ and $F(v_1 + v_2) \in U_0 \cap U_1 = \langle v_4 + v_5 \rangle$. Using also that $F(v_1 + v_2) - F(v_2) \in U_\infty = \langle v_3, v_4 \rangle$, we find $F(v_2) = \alpha(-v_4 + v_5)$ and $F(v_1 + v_2) = \alpha(v_4 + v_5)$ for some $\alpha \in GF(p)$. Substitute these in Eq. (21). After a direct computation we find $F(2v_1) = 2\alpha v_3$. This shows that the orbit of $2v_1$ under the group $G_0 \cap G_{v_1}$ has size at most p. Therefore, $|G_0 \cap G_{v_1}| \le |G_0 \cap G_{v_1} \cap G_{2v_1}| \cdot p$, and to derive Claim (e) it is enough to show that $|G_0 \cap G_{v_1} \cap G_{2v_1}| = 1$.

Now, choose $g \in G_0 \cap G_{v_1} \cap G_{2v_1}$. Then, $F(0) = F(v_1) = F(2v_1) = 0$, thus applying Eq. (20) to $F(iv_1 + v_2)$, $i \in GF(p)$, and using Claim (d), we find $F(iv_1 + v_2) \in U_i \cap U_{i-1} \cup U_{i-2} = \{0\}$. Therefore, $F(iv_1 + v_2) = 0$ for all $i \in GF(p)$. In particular, $F(v_2) = F(v_1 + v_2) = F(2v_1 + v_2) = 0$, and we can repeat the same argument to have $F(iv_1 + 2v_2) = 0$ for all $i \in GF(p)$. Since $V = \langle v_1, v_2 \rangle$, the process can be continued to cover all $v \in V$, and this leads to that $F(v) = 0$ for all $v \in V$, that is, $g = \mathrm{id}_H$, as required.

Claim (f). $|G_0| = p^3$.

The G_0-orbit of v_1 is the basic set $U_\infty + v_1$. This together with Claim (e) shows that $|G_0| \le p^2 \cdot |G_0 \cap G_{v_1}| \le p^3$. To settle Claim (f) it is enough to find a non-identity automorphism $g \in G_0 \cap G_{v_1}$. We claim that g_F is such an automorphism where F is defined as follows:

$$F(iv_1 + jv_2) = i(i-1)v_3 + (2i-1)jv_4 + j^2 v_5, \quad i, j \in GF(p).$$

Then, $F(0) = 0$, and by Claim (c), we have $g_F \in G_0$ if F satisfies the conditions in Eq. (20). This can be verified directly. After letting $v = iv_1 + jv_2$ and using the above definition of F, we compute for $k \in GF(p)$,

$$\begin{aligned} F(v + \hat{v}_\infty) - F(v) &= 2iv_3 + 2jv_4, \\ F(v + \hat{v}_k) - F(v) &= (2i - 1 + k)(kv_3 + v_4) + (2j + 1)(kv_4 + v_5). \end{aligned}$$

These show that the conditions in Eq. (20) hold, and $g_F \in G_0$. Also, $F(v_1) = 0$ and $F(2v_1) = 2v_3$, and hence g_F is a non-identity element in $G_0 \cap G_{v_1}$. This completes the proof of the lemma. □

Lemma 6.6. *With the notation of Lemma 6.4, $V(H,L)$ is a CI-S-ring.*

Proof. We keep all notations from the previous proof, that is,

$$L = \langle x, y\rangle,\ G = \mathrm{Aut}(V(H,L)),\ U = \mathbf{O}_\theta(V(H,L)) = \langle v_3, v_4, v_5\rangle,\ V = \langle v_1, v_2\rangle.$$

In addition, let $N = N_G(H_R)$. In view of Lemma 2.11, it is enough to show that all regular subgroups of G isomorphic to H are conjugate in G. First, the number of subgroups of G that are conjugate to H_R is equal to the index $|G : N|$. By Lemma 6.5, $|G| = p^8$, and since $H_R L \le N$, it follows that $|N| \ge p^7$. If $G = N$, then for every non-identity element $z \in G_0 \cap G_{v_1}$, $C_H(z) = \langle v_1, v_3, v_4, v_5\rangle$, contradicting Lemma 6.2. Thus, $|N| = p^7$, and there are exactly p subgroups of G that are conjugate to H_R.

Therefore, to finish the proof it is sufficient to show that there are exactly p regular subgroups of G isomorphic to H. Note that, we have $L = N_0$. Let $K \le G$ be any regular subgroup isomorphic to H_R such that $K \ne H_R$. Let $M = \langle K, H_R\rangle$. Since $K \ne H_R$, $|M| \ge p^6$. This implies that $|M \cap L| > 1$. Indeed, if $|M| = p^6$, then $H_R \trianglelefteq M$, and hence $M_0 \ne 1$ and $M_0 \le N_0 = L$. If $|M| > p^6$, then $|M \cap L| > 1$ follows because $|L| = p^2$ and $|LM| \le |G| = p^8$. Using also that $K \cap H_R \le Z(M)$ and Lemma 6.2, we deduce that $|K \cap H_R| \le p^3$. On the other hand, since K is regular and abelian, it follows that $Z(G) \le K$, and hence $K \cap H_R = U_R$. Note that, we have proved that every regular subgroup isomorphic to H intersects H_R at U_R, unless it is equal to H_R. This fact will be used in the next paragraph.

We claim that $K \le N$. Suppose to the contrary that there exists some $g \in K \setminus N$. Then $g = z_1 v_R$ for some $z_1 \in G_0 \setminus L$ and $v \in H$. Since $U_R \le K$, the element v cannot be in U. On the other hand, $|N \cap K| \ge p^4$, and thus K also contains an element in the form $z_2 w_R$, $z_2 \in L$ and $w \in H \setminus U$ (again, $w \notin U$ because of $U_R \le K$). Then, $z_1 z_2 (v_R)^{z_2} w_R = z_1 v_R z_2 w_R = z_2 w_R z_1 v_R = z_2 z_1 (w_R)^{z_1} v_R$. By Lemma 6.5, G_0 is abelian, and we get $(w_R)^{z_1} = (v_R)^{z_2} w_R (v_R)^{-1} = (v^{z_2} + w - v)_R$. Thus, $(w_R)^{z_1} \in H_R$, and since $w \notin U$, $(w_R)^{z_1} \notin U_R$, and $|H_R^{z_1} \cap H_R| \ge p^4$. Now, it follows by the previous paragraph that $H_R^{z_1} = H_R$, and hence $z_1 \in L$, a contradiction.

Now, there exist $z_1, z_2 \in L$ such that

$$K = \big\langle z_1(v_1)_R,\ z_2(v_2)_R, U_R\big\rangle.$$

Recall that, the L-orbit of v_1 is in the form $v_1^L = U_\infty + v_1$, and the L-orbit of v_2 is in the form $v_2^L = U_0 + v_2$. Let $u = v_1^{z_2} - v_1$. Clearly, $u \in U_\infty$. Then, since $z_1(v_1)_R$ and $z_2(v_2)_R$ commute, $0^{z_1(v_1)_R z_2(v_2)_R} = v_1^{z_2} + v_2$ and $0^{z_2(v_2)_R z_1(v_1)_R} = v_2^{z_1} + v_1$, it follows that $u = v_2^{z_1} - v_2$. This shows that $u \in U_0$ also holds, and hence $u \in U_\infty \cap U_0 = \langle v_4\rangle$. Now, as L is regular on both orbits v_1^L and v_2^L, the automorphisms z_1 and z_2 are uniquely determined by u, and thus K is determined as well. This yields that there are exactly p regular subgroups of G isomorphic to H. This completes the proof of the lemma. □

Lemma 6.7. *Assuming Hypothesis 5.1, suppose that $\mathcal{A}$ is indecomposable, and let U and W be $\mathcal{A}$-subgroups such that $W < \mathbf{O}_\theta(\mathcal{A}) < U$, $|W| = p$ and $|U| = p^4$. Then $\mathcal{A}$ has a basic set T such that*

$$T \subset H \setminus U,\ 1 < |T| \le p^2 \text{ and } W \nleq \mathrm{rad}(T). \tag{22}$$

Proof. Since $\mathcal{A}$ is indecomposable, there exists a basic set $T_1 \subset H \setminus U$ such that $W \nleq \mathrm{rad}(T_1)$. It is clear that $|T_1| > 1$. We have to show that $|T_1| \le p^2$. To the contrary assume that $|T_1| \ge p^3$. If $|T_1| = p^4$, then $\mathcal{A}$ is decomposable, see Proposition 2.14, thus $|T_1| = p^3$. This together with $|\mathbf{O}_\theta(\mathcal{A}) \cap U| = |\mathbf{O}_\theta(\mathcal{A})| \ge p^2$ gives $|\mathbf{O}_\theta(\mathcal{A}) \cap U| \cdot |T_1| > p^4 = |H|/p$, and we can apply Lemma 2.18(iii) to obtain that $\mathbf{O}_\theta(\mathcal{A}) \cap \mathrm{rad}(T_1) \ne \{0\}$. Let $W' \le \mathbf{O}_\theta(\mathcal{A}) \cap \mathrm{rad}(T_1)$ such that $|W'| = p$. Since $W \nleq \mathrm{rad}(T_1)$, we get, using Eq. (1), pairwise distinct basic sets in the form $T_1 + w$, $w \in W$. As the union of the latter basic sets is equal to the coset $U + v_1$, it follows that $W' \le \mathrm{rad}(T)$ for all $T \in \mathrm{Bsets}(\mathcal{A})$ with $T \subset U + v_1$. This together with Theorem 2.9 yields that $W' \le \mathrm{rad}(T)$ for all $T \in \mathrm{Bsets}(\mathcal{A})$ with $T \not\subset U$, that is, $\mathcal{A}$ is a U/W'-wreath product, a contradiction. □

Everything is prepared to settle the main result of the section.

Proof of Theorem 6.1. Let $U = \mathbf{O}_\theta(\mathcal{A})$, $N = N_{\mathrm{Aut}(\mathcal{A})}(H_R)$ and N_0 be the stabilizer of 0 in N. Assume to the contrary that $\mathcal{A}$ is a non-CI-S-ring. We prove first the following:

$$\text{There exists } L \le N_0 \text{ such that } |L| = p^2 \text{ and } |C_H(L)| = p^3. \tag{23}$$

If $|U| \ge p^3$, then we are done by choosing L to be any subgroup of N_0 of order p^2 (see also Lemma 6.3). Thus we assume for the moment that $|U| = p^2$. Let $K \le N$ be the subgroup given in Proposition 3.1, and let $M = (KH_R)_0$. If $|M| \le p^2$, then

$$C_H(M) \ge |K \cap H_R| = \frac{|K| \cdot |H_R|}{|KH_R|} = \frac{|K| \cdot |H_R|}{|M||H|} \ge p^3.$$

By Lemma 6.2, M must have order p^2, and therefore, we are done by choosing L to be M.

Let $|M| \ge p^3$. It follows from Lemma 6.7 that there exists a basic set T such that $|T| \le p^2$ and $\mathrm{rad}(T) \ne U$. Let $v \in T$, and M_v be the stabilizer of v in M. Then $C_H(M_v) \ge \langle U, v\rangle$. If $|T| = p$ or the orbit $v^M \ne T$, then it follows that $|M_v| \ge p^2$. Using this and that $|\langle U, v\rangle| = p^3$, we can choose L to be any subgroup of M_v of order p^2. Now, suppose that $|T| = p^2$, and the orbit $v^M = T$. Choose a non-identity element $x_0 \in M_v$, and let $u \in T$ be an arbitrary element. Then $u = v^x$ for some $x \in M$, and since M is abelian, we can write $u^{x_0} = v^{xx_0} = v^{x_0x} = v^x = u$. As a corollary we find $C_H(x_0) \ge \langle U, T\rangle$. Clearly, $|\langle U, T\rangle| \ge p^3$; in fact, $\langle U, T\rangle| = p^3$ must hold by Lemma 6.2. It follows that T is equal to a U-coset, that is, $\mathrm{rad}(T) = U$. This is a contradiction, and Eq. (23) follows.

By Lemma 6.6, the S-ring $V(H,L)$ is a CI-S-ring. Therefore, $\mathcal{A} \neq V(H,L)$, hence $A > L$, in particular, $|A| \geq p^3$. For sake of simplicity we let $V = \mathbf{O}_\theta(V(H,L))$. Clearly, $U \leq V$ and $|V| = p^3$. Fix $W_1 < U$, $|W_1| = p$. By Lemma 6.7, there exists a basic set $T_1 \in \mathrm{Bsets}(\mathcal{A})$ such that $1 < |T_1| \leq p^2$ and $W_1 \not< \mathrm{rad}(T_1)$. Since every basic set of $V(H,L)$ outside V is a coset of a subgroup of V of order p^2, we find that either T_1 is contained in $H \setminus V$, $|T_1| = p^2$ and $\mathrm{rad}(T_1) < V$, or $T_1 \leq V$. In the former case $V = \mathrm{rad}(T_1) + W_1$, whereas in the latter case $V = \langle T_1, W_1 \rangle$ because $W_1 \not< \mathrm{rad}(T_1)$. We conclude that V is an $\mathcal{A}$-subgroup. This shows that we may choose the above T_1 such that $T_1 \subset H \setminus V$. Fix some $v_1 \in T_1$. Since $|N_0| \geq p^3$, there exists a non-identity element $x \in N_0$ such that $v_1^x = v_1$, and thus $C_H(x) \geq \langle U, v_1 \rangle$, and so $|C_H(x)| \geq p \cdot |U|$. This together with Lemma 6.2 shows that $|U| = p^2$, in particular, $U < V$. Now, using also that $W_1 < U$ and $W_1 \not< \mathrm{rad}(T_1)$, we infer in turn that $|U \cap \mathrm{rad}(T_1)| = p$, $\mathcal{A}_{\mathrm{rad}(T_1)} = \mathbb{Q}C_p \wr \mathbb{Q}C_p$, and finally that, $\mathcal{A}_V = (\mathbb{Q}C_p \wr \mathbb{Q}C_p) \otimes \mathbb{Q}C_p$. Let $W_2 = U \cap \mathrm{rad}(T_1)$. It is easy to see that every $\mathcal{A}$-subgroup of order p^2 contained in V contains W_2. (In fact, such an $\mathcal{A}$-subgroup intersects $\mathrm{rad}(T_1)$ at exactly W_2.) Now, apply Lemma 6.7 with $W = W_2$. We obtain that, there exists a basic set T_2 of $\mathcal{A}$ such that $T_2 \not\subset V$, $|T_2| = p^2$ and $W_2 \not< \mathrm{rad}(T_2)$. As before, $\mathrm{rad}(T_2)$ is an $\mathcal{A}$-subgroup of order p^2 contained in V, contradicting our earlier observation that such an $\mathcal{A}$-subgroup must contain W_2. This completes the proof of the theorem. □

References

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

[2] B. Alspach, L. Nowitz, Elementary proofs that Z_p^2 and Z_p^3 are CI-groups, European J. Combin. 19 (1999) 607–617.

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

[4] L. Babai, P. Frankl, Isomorphisms of Cayley Graphs I, Colloq. Math. Soc. János Bolyai, vol. 18, North-Holland, Amsterdam, 1978, pp. 35–52.

[5] M. Conder, C.H. Li, On isomorphism of Cayley graphs, European J. Combin. 19 (1998) 911–919.

[6] J.D. Dixon, B. Mortimer, Permutation Groups, Springer-Verlag, 1996.

[7] D.Ź. Djoković, Isomorphism problem for a special class of graphs, Acta Math. Acad. Sci. Hung. 21 (1970) 267–270.

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

[9] E. Dobson, J. Morris, P. Spiga, Further restrictions on the structure of finite DCI-groups: an addendum, J. Algebraic Combin. 42 (2015) 959–969.

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

[11] S. Evdokimov, I. Ponomarenko, On a family of Schur rings over a finite cyclic group, Algebra i Analiz 13 (2001) 139–154, English translation in: St. Petersburg Math. J. 13 (2002) 441–451.

[12] C.D. Godsil, On Cayley graph isomorphisms, Ars Combin. 15 (1983) 231–246.

[13] M. Hirasaka, M. Muyzychuk, An elementary abelian group of rank 4 is a CI-group, J. Combin. Theory Ser. A 94 (2001) 339–362.

[14] M.H. Klin, R. Pöschel, The isomorphism problem for circulant graphs and digraphs with p^n vertices, preprint, Akad. der Wiss. der DDR, ZIMM, Berlin, 1980.

[15] M.H. Klin, R. Pöschel, The König Problem, the Isomorphism Problem for Cyclic Graphs and the Method of Schur Rings, Colloq. Math. Soc. János Bolyai, vol. 25, North-Holland, Amsterdam, 1981, pp. 405–434.

[16] K.H. Leung, S.H. Man, On Schur rings over cyclic groups II, J. Algebra 183 (1996) 273–285.

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

[18] C.H. Li, Z.P. Lu, P.P. Pálfy, Further restriction on the structure of finite CI-groups, J. Algebraic Combin. 26 (2007) 161–181.

[19] J. Morris, Elementary proof that $\mathbb{Z}_p^4$ is a DCI-group, Discrete Math. 338 (2015) 1385–1393.

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

[21] M. Muzychuk, I. Ponomarenko, Schur rings, European J. Combin. 30 (2009) 1526–1539.

[22] M. Muzychuk, R. Pöschel, Isomorphism criterion for circulant graphs, Technische Universität Dresden, 1999, Preprint MATH-AL-9-1999.

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

[24] I. Schur, Zur Theorie der einfach transitiven Permutationgruppen, S.-B. Preuss. Akad. Wiss. Phys.-Math. Kl. (1933) 598–623.

[25] G. Somlai, Elementary abelian p-groups of rank $2p + 3$ are not CI-groups, J. Algebraic Combin. 34 (2011) 323–335.

[26] P. Spiga, Elementary abelian p-groups of rank greater than or equal to $4p - 2$ are not CI-groups, J. Algebraic Combin. 26 (2007) 343–355.

[27] P. Spiga, CI-property of elementary abelian 3-groups, Discrete Math. 309 (2009) 3393–3398.

[28] P. Spiga, Q. Wang, An answer to Hirasaka and Muzychuk: every p-Schur-ring over C_p^3 is Schurian, Discrete Math. 308 (2008) 1760–1763.

[29] J. Turner, Point-symmetric graphs with a prime number of points, J. Combin. Theory 3 (1967) 136–145.

[30] H. Wielandt, Finite Permutation Groups, Academic Press, Berlin, 1964.

[31] H. Wielandt, Permutation Groups Through Invariant Relations and Invariant Functions, Lecture Notes, Department of Mathematics, Ohio State University, Colombus, 1969.

[32] P.H. Zieschang, An Algebraic Approach to Association Schemes, Lecture Notes in Math., vol. 1628, Springer-Verlag, New York/Berlin, 1996.