ON NILPOTENT SCHUR GROUPS

GRIGORY RYABOV

Abstract. A finite group G is called a *Schur* group if every S-ring over G is *schurian*, i.e. associated in a natural way with a subgroup of $\mathrm{Sym}(G)$ that contains all right translations. We prove that every nonabelian nilpotent Schur group belongs to one of a few explicitly given families of groups.

Keywords: Schur rings, Schur groups, nilpotent groups.

MSC: 05E30, 20B25.

1. Introduction

A *Schur ring* or *S-ring* over a finite group G can be defined as a subring of the group ring $\mathbb{Z}G$ that is a free $\mathbb{Z}$-module spanned by a partition of G closed under taking inverse and containing the identity element e of G as a class (see Section 2 for the exact definition). The theory of S-rings was initiated by Schur [14], and further it was developed by Wielandt [15]. Schur and Wielandt used S-rings for studying permutation groups. In particular, Schur proved a generalization of the Burnside theorem on a permutation group with a regular cyclic p-subgroup using S-rings [15, Theorem 25.3].

With every group $K \leq \mathrm{Sym}(G)$ containing all right translations of G, one can associate the S-ring determined by the partition of G into the orbits of the stabilizer of e in K. Every S-ring obtained in such way was called *schurian* in [10]. Wielandt wrote in [16] that "Schur had conjectured for a long time that every S-ring is determined by a suitable permutation group", in our terms that every S-ring is schurian. However, this conjecture was disproved in [15] by Wielandt. In [10], Pöschel introduced the following definition. The group G is called a *Schur* group if every S-ring over G is schurian. He also posed the next problem.

Problem. *Determine all Schur groups.*

To prove that a given group G is Schur, it is necessary to check that every S-ring over G is schurian. The main difficulty of the above problem is that the number of S-rings over G is exponential in the order of G in general, and sometimes it is not easy to obtain a description of all S-rings over G. On the other hand, to prove that G is not Schur, it is necessary to find a nonschurian S-ring over G. However, in many cases it is unclear how to find such S-ring.

The first result on the schurity problem was obtained by Pöschel [10]. He proved that cyclic p-groups of odd order are Schur. Using this result, Klin and Pöschel solved the isomorphism for Cayley graphs over these groups [6]. Schurity of cyclic 2-groups was proved in [5]. The complete classification of cyclic Schur groups was obtained in [3].

Strong necessary conditions of schurity for abelian groups were obtained in [4]. Schurity of some infinite families of noncyclic abelian groups was verified in [7, 12]. Abelian Schur

The work is supported by Russian Scientific Fund (project No. 22-71-00021).

groups of odd order were classified in [8]. Finally, the complete classification of abelian Schur groups was obtained in [13].

All Schur groups of order at most 63 were enumerated in [17]. It turns out that there exist nonabelian Schur groups. However, it is not known to the present moment whether there exists an infinite family of nonabelian Schur groups. The attempts to describe all S-rings over some nonabelian groups, e.g. dihedral groups or groups whose order has few prime divisors, lead to such hard unsolved problems as the problem of existence of a difference set in a cyclic group and the problem of computing cyclotomic numbers (see [7]).

Nevertheless, there are some general results on nonabelian Schur groups. In [9], it was proved that every nonabelian Schur group G is metabelian and the number of distinct prime divisors of $|G|$ is at most 7. Some partial results one nonabelian Schur groups were obtained in [7, 11]. In particular, in [11] it was proved that every Schur p-group of odd order must be abelian and in [7] it was proved that every nonabelian 2-group of order at least 32 must be dihedral.

In this paper, we prove that every nilpotent Schur group belongs to one of a few explicitly given families of groups. The cyclic and dihedral groups of order n are denoted by $\mathbb{Z}_n$ and D_n, respectively. The quaternion group and the central product of D_8 and $\mathbb{Z}_4$ are denoted by Q_8 and G_{16}, respectively. The main result of the paper is the following theorem.

Theorem 1.1. *A nonabelian nilpotent Schur group is isomorphic to one of the groups below:*

(1) Q_8, G_{16}, D_{2^k}, *where* $k \geq 3$,

(2) $Q_8 \times \mathbb{Z}_p$, *where* $p \geq 11$ *is a prime such that* $p \not\equiv 1 \mod 4$ *and* $p \not\equiv 1 \mod 6$.

Moreover, the groups Q_8, G_{16}, *and* D_{2^k}, *where* $3 \leq k \leq 5$, *are Schur.*

We do not know whether infinite families of groups from Theorem 1.1 consist of Schur groups. So we suggest the following question.

Question. *Are the groups* D_{2^k}, $k \geq 6$, *and* $Q_8 \times \mathbb{Z}_p$, $p \not\equiv 1 \mod 4$, $p \not\equiv 1 \mod 6$, *Schur?*

It should be mentioned that all S-rings of rank at most 5 over D_{2^k}, $k \geq 3$, were classified in [7].

We finish the introduction with a brief outline of the paper. Section 2 contains a necessary background on S-rings. In Sections 3 and 4, we construct new infinite families of nonschurian S-rings over the groups $D_8 \times \mathbb{Z}_p$ and $Q_8 \times \mathbb{Z}_p$, where p is prime; in case of $Q_8 \times \mathbb{Z}_p$, we also assume that $p \equiv 1 \mod 4$ or $p \equiv 1 \mod 6$, respectively. The latter condition on p is substantial for constructing a nonschurian S-ring over $Q_8 \times \mathbb{Z}_p$. Finally, we prove Theorem 1.1 in Section 5. One of the key ingredients of the proof is [9, Corollary 4.3], which provides some necessary conditions of schurity for nilpotent groups.

The author would like to thank Dr. M. Ziv-Av for the help with computer calculations and the anonymous referee for the valuable comments which help us to improve the text.

2. Preliminaries

In this section, we provide all necessary definitions and statements on S-rings. All of them can be found, e.g., in [7, 12].

Let G be a finite group and $\mathbb{Z}G$ the integer group ring. The identity element and the set of all nonidentity elements of G are denoted by e and $G^{\#}$, respectively. The symmetric group of the set G is denoted by $\mathrm{Sym}(G)$. If $K \leq \mathrm{Sym}(G)$, then the set of all orbits of K on G is denoted by $\mathrm{Orb}(K, G)$. The subgroup of $\mathrm{Sym}(G)$ induced by the right multiplications of G is denoted by G_r. If $X \subseteq G$, then the element $\sum_{x \in X} x$ of the group ring $\mathbb{Z}G$ is denoted by $\underline{X}$. The set $\{x^{-1} : x \in X\}$ is denoted by X^{-1}.

A subring $\mathcal{A} \subseteq \mathbb{Z}G$ is called an *S-ring* (a *Schur* ring) over G if there exists a partition $\mathcal{S} = \mathcal{S}(\mathcal{A})$ of G such that:

(1) $\{e\} \in \mathcal{S}$;

(2) if $X \in \mathcal{S}$, then $X^{-1} \in \mathcal{S}$;

(3) $\mathcal{A} = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : \ X \in \mathcal{S}\}$.

The elements of $\mathcal{S}$ are called the *basic sets* of $\mathcal{A}$. A set $X \subseteq G$ is called an *$\mathcal{A}$-set* if $\underline{X} \in \mathcal{A}$. A subgroup $A \leq G$ is called an *$\mathcal{A}$-subgroup* if A is an $\mathcal{A}$-set.

Let $\{e\} \leq A \trianglelefteq B \leq G$. A section B/A is called an *$\mathcal{A}$-section* if B and A are $\mathcal{A}$-subgroups. If $S = B/A$ is an $\mathcal{A}$-section, then the module

$$\mathcal{A}_S = Span_{\mathbb{Z}}\left\{\underline{X}^{\pi} : \ X \in \mathcal{S}(\mathcal{A}), \ X \subseteq B\right\},$$

where $\pi : B \to B/A$ is the canonical epimorphism, is an S-ring over S.

Let $S = B/A$ be an $\mathcal{A}$-section of G. The S-ring $\mathcal{A}$ is called the *S-wreath product* of $\mathcal{A}_B$ and $\mathcal{A}_{G/A}$ if $A \trianglelefteq G$ and every basic set X of $\mathcal{A}$ outside B is a union of some A-cosets. The S-wreath product is called *nontrivial* or *proper* if $A \neq \{e\}$ and $B \neq G$.

Let A and B be $\mathcal{A}$-subgroups such that $G = A \times B$. The S-ring $\mathcal{A}$ is called the *tensor product* of $\mathcal{A}_A$ and $\mathcal{A}_B$ if

$$\mathcal{S}(\mathcal{A}) = \{X_1 \times X_2 : \ X_1 \in \mathcal{S}(\mathcal{A}_A), \ X_2 \in \mathcal{S}(\mathcal{A}_B)\}.$$

In this case we write $\mathcal{A} = \mathcal{A}_A \otimes \mathcal{A}_B$. The tensor product is called *nontrivial* if $\{e\} < A < G$ and $\{e\} < B < G$.

Let $X, Y \in \mathcal{S}$. If $Z \in \mathcal{S}$, then the number of distinct representations of $z \in Z$ in the form $z = xy$ with $x \in X$ and $y \in Y$ does not depend on the choice of $z \in Z$. Denote this number by c_{XY}^{Z}. One can see that $\underline{X}\ \underline{Y} = \sum_{Z \in \mathcal{S}(\mathcal{A})} c_{XY}^{Z} \underline{Z}$. Therefore the numbers c_{XY}^{Z} are the structure constants of $\mathcal{A}$ with respect to the basis $\{\underline{X} : \ X \in \mathcal{S}\}$. It can be verified that

$$|Z| c_{XY}^{Z^{-1}} = |X| c_{YZ}^{X^{-1}} = |Y| c_{ZX}^{Y^{-1}} \tag{1}$$

for all $X, Y, Z \in \mathcal{S}(\mathcal{A})$ (see, e.g., [12, Lemma 2.3]).

Let $\mathcal{A}'$ be an S-ring over a group G'. A bijection f from $\mathcal{S}(\mathcal{A})$ to $\mathcal{S}(\mathcal{A}')$ is called an *algebraic isomorphism* from $\mathcal{A}$ to $\mathcal{A}'$ if $c_{X^f Y^f}^{Z^f} = c_{XY}^{Z}$ for all $X, Y, Z \in \mathcal{S}(\mathcal{A})$. An algebraic isomorphism from $\mathcal{A}$ to itself is called an *algebraic automorphism* of $\mathcal{A}$. The following statement is known as the first Schur theorem on multipliers (see [15, Theorem 23.9, (a)]).

Lemma 2.1. *Let $\mathcal{A}$ be an S-ring over an abelian group G. Then the mapping $X \mapsto X^{(m)} = \{x^m : \ x \in X\}$, $X \in \mathcal{S}(\mathcal{A})$, is an algebraic automorphism of $\mathcal{A}$ for every $m \in \mathbb{Z}$ coprime to $|G|$.*

Put $\mathcal{R}(\mathcal{A}) = \{r(X) : \ X \in \mathcal{S}(\mathcal{A})\}$, where $r(X) = \{(g, xg) : \ x \in X, \ g \in G\}$. A bijection α from G to G' is called a *(combinatorial) isomorphism* from $\mathcal{A}$ to $\mathcal{A}'$ if $\mathcal{R}(\mathcal{A})^{\alpha} = \mathcal{R}(\mathcal{A}')$, where $\mathcal{R}(\mathcal{A})^{\alpha} = \{r(X)^{\alpha} : \ X \in \mathcal{S}(\mathcal{A})\}$ and $r(X)^{\alpha} = \{(g^{\alpha}, h^{\alpha}) : \ (g, h) \in r(X)\}$. If there exists an isomorphism from $\mathcal{A}$ to $\mathcal{A}'$, then $\mathcal{A}$ and $\mathcal{A}'$ are called *isomorphic*.

A bijection $\alpha \in \mathrm{Sym}(G)$ is defined to be a *(combinatorial) automorphism* of $\mathcal{A}$ if $r(X)^\alpha = r(X)$ for every $X \in \mathcal{S}(\mathcal{A})$. The set of all automorphisms of $\mathcal{A}$ forms the group called the *automorphism group* of $\mathcal{A}$ and denoted by $\mathrm{Aut}(\mathcal{A})$. One can see that $\mathrm{Aut}(\mathcal{A}) \geq G_r$ and $\mathcal{A}$ is isomorphic to an S-ring over a group H if and only if $\mathrm{Aut}(\mathcal{A})$ has a regular subgroup isomorphic to H. If $\alpha \in \mathrm{Aut}(\mathcal{A})$, then

$$(Xy)^\alpha = Xy^\alpha \tag{2}$$

for every $X \in \mathcal{S}(\mathcal{A})$ and $y \in G$. If A is an $\mathcal{A}$-subgroup of G, then the set of all right A-cosets is an imprimitivity system of $\mathrm{Aut}(\mathcal{A})$, and if $\alpha \in \mathrm{Aut}(\mathcal{A})$, then $\alpha^{G/A}$ denotes the permutation induced by α on G/A. If $\mathcal{A} = \mathcal{A}_A \otimes \mathcal{A}_B$, then $\mathrm{Aut}(\mathcal{A}) = \mathrm{Aut}(\mathcal{A}_A) \times \mathrm{Aut}(\mathcal{A}_B)$.

Let K be a subgroup of $\mathrm{Sym}(G)$ containing G_r. Schur proved in [14] that the $\mathbb{Z}$-submodule

$$V(K, G) = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : \ X \in \mathrm{Orb}(K_e, \ G)\},$$

where K_e is a stabilizer of e in K, is an S-ring over G. An S-ring $\mathcal{A}$ over G is called *schurian* if $\mathcal{A} = V(K, G)$ for some $K \leq \mathrm{Sym}(G)$ with $K \geq G_r$. One can verify that $\mathcal{A}$ is schurian if and only if $\mathcal{A} = V(\mathrm{Aut}(\mathcal{A}), G)$, or equivalently, $\mathcal{S}(\mathcal{A}) = \mathrm{Orb}(\mathrm{Aut}(\mathcal{A})_e, G)$. Clearly, two isomorphic S-rings are schurian or not simultaneously.

Let $K \leq \mathrm{Aut}(G)$. Then $\mathrm{Orb}(K, G)$ forms a partition of G that defines an S-ring $\mathcal{A}$ over G. In this case $\mathcal{A}$ is called *cyclotomic* and denoted by $\mathrm{Cyc}(K, G)$. If $\mathcal{A} = \mathrm{Cyc}(K, G)$ for some $K \leq \mathrm{Aut}(G)$, then $\mathcal{A} = V(G_r K, G)$. So every cyclotomic S-ring is schurian.

The group G is called a *Schur* group if every S-ring over G is schurian. A section (in particular, a subgroup) of a Schur group is also Schur (see, e.g., [9, Theorem 2.4]).

3. Nonschurity of $D_8 \times \mathbb{Z}_p$

The main result of this section is the following proposition.

Proposition 3.1. *The group $D_8 \times \mathbb{Z}_p$ is not Schur for every prime p.*

Proof. The statement of the proposition for $p \in \{2, 3\}$ follows from [9, Lemma 3.1]. Further we assume that $p \geq 5$.

Let $H = \langle a, b : \ a^4 = b^2 = e, a^b = a^{-1} \rangle \cong D_8$, $A_1 = \langle a^2 \rangle$, $A_2 = \langle ab \rangle$, C a cyclic group of order p, c a generator of C, and $G = H \times C \cong D_8 \times \mathbb{Z}_p$. Let us construct a nonschurian S-ring over G. Put

$$Z_0 = \{e\}, \ Z_1 = \{a^2\}, \ Z_2 = \{ab\}, \ Z_3 = \{a^3b\}, \ Z_4 = \{a, a^3, b, a^2b\},$$
$$X_1 = c\{e, a^2\}, \ X_2 = c\{ab, a^3b\}, \ X_3 = c\{a, b\}, \ X_4 = c\{a^3, a^2b\},$$
$$Y_1 = c^{-1}\{e, a^2\}, \ Y_2 = c^{-1}\{ab, a^3b\}, \ Y_3 = c^{-1}\{a^3, b\}, \ Y_4 = c^{-1}\{a, a^2b\},$$
$$T_{1k} = c^k\{e, a^2\}, \ T_{2k} = c^k\{ab, a^3b\}, \ T_{3k} = c^k\{a, a^3, b, a^2b\}, \ k \in \{2, \dots, p-2\}.$$

One can see that the sets Z_i, X_i, Y_i, T_{jk} form the partition of G. Denote this partition by $\mathcal{S}$.

Lemma 3.2. *The $\mathbb{Z}$-module $\mathcal{A} = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : \ X \in \mathcal{S}\}$ is an S-ring over G.*

Proof. It is easy to check that $Z_i = Z_i^{-1}$ and $Y_i = X_i^{-1}$ for every $i \in \{1, 2, 3, 4\}$ and $T_{j\ p-k} = T_{jk}^{-1}$ for every $j \in \{1, 2, 3\}$ and $k \in \{2, \dots, p-2\}$. To complete the proof of the lemma, it suffices to check that $\underline{XY} \in \mathcal{A}$ for every $X, Y \in \mathcal{S}$. The definition of $\mathcal{S}$ yields that $X = c^i X_0$ and $Y = c^j Y_0$ for some $i, j \in \{0, \dots, p-1\}$ and $X_0, Y_0 \subseteq H$. So $\underline{XY} = c^{i+j}\underline{X_0 Y_0}$. The straightforward computation in $H \cong D_8$ implies that $\underline{X_0 Y_0} \in \mathrm{Span}_{\mathbb{Z}}\{\underline{\{e, a^2\}}, \underline{\{ab, a^3b\}}, \underline{\{a, a^3, b, a^2b\}}\}$

if $i+j \not\equiv 0 \mod p$ and $\underline{X_0Y_0} \in \mathrm{Span}_{\mathbb{Z}}\{\underline{Z_0}, \underline{Z_1}, \underline{Z_2}, \underline{Z_3}, \underline{Z_4}\}$ if $i+j \equiv 0 \mod p$. Thus, $\underline{XY} \in \mathcal{A}$. □

Lemma 3.3. *In the above notations, the stabilizer* $\mathrm{Aut}(\mathcal{A}_{G/A_1})_{A_1}$ *of* A_1 *in* $\mathrm{Aut}(\mathcal{A}_{G/A_1})$ *is generated by the involution* $\sigma \in \mathrm{Sym}(G/A_1)$ *which interchanges* A_1ac^k *and* A_1bc^k *and fixes* A_1c^k *and* A_1abc^k *for every* $k \in \{0, \dots, p-1\}$.

Proof. From the definition of $\mathcal{A}$ it follows that $\mathcal{A}_{G/A_1} = \mathcal{A}_{H/A_1} \otimes \mathbb{Z}C$. Therefore $\mathrm{Aut}(\mathcal{A}_{G/A_1}) = \mathrm{Aut}(\mathcal{A}_{H/A_1}) \times \mathrm{Aut}(\mathbb{Z}C)$. Clearly, $\mathrm{Aut}(\mathbb{Z}C) = C_r$. It is easy to see that $\mathrm{Aut}(\mathcal{A}_{H/A_1}) = (H/A_1)_r \rtimes \langle \sigma^{H/A_1} \rangle \cong \mathbb{Z}_2 \wr \mathbb{Z}_2$, where σ^{H/A_1} is the restriction of σ on H/A_1. Thus,

$$\mathrm{Aut}(\mathcal{A}_{G/A_1}) = ((H/A_1)_r \rtimes \langle \sigma^{H/A_1} \rangle) \times C_r.$$

The latter equality implies that $\mathrm{Aut}(\mathcal{A}_{G/A_1})_{A_1} = \langle \sigma \rangle$, as required. □

Lemma 3.4. *The* S*-ring* $\mathcal{A}$ *is nonschurian.*

Proof. Assume the contrary. Then $\mathcal{S} = \mathrm{Orb}(K, G)$, where $K = \mathrm{Aut}(\mathcal{A})_e$. Let $\alpha \in K_{ac}$. Observe that $\alpha^{G/A_1} \in \mathrm{Aut}(\mathcal{A}_{G/A_1})_{A_1}$. By Lemma 3.3, we have α^{G/A_1} is trivial or $\alpha^{G/A_1} = \sigma$. However, the latter case is impossible because $(A_1ac)^{\alpha^{G/A_1}} = A_1ac$. Thus, α^{G/A_1} is trivial.

Since $\alpha \in K_{ac}$, Eq. (2) implies that $(X_4ac)^\alpha = X_4ac$ and $T_{12}^\alpha = T_{12}$. So

$$\{c^2\}^\alpha = (X_4ac \cap T_{12})^\alpha = X_4ac \cap T_{12} = \{c^2\}.$$

By the above equality and Eq. (2), we have $(X_3c^2)^\alpha = X_3c^2$. In addition, $(A_1ac^3)^\alpha = A_1ac^3$ because α^{G/A_1} is trivial. So

$$\{ac^3\}^\alpha = (X_3c^2 \cap A_1ac^3)^\alpha = X_3c^2 \cap A_1ac^3 = \{ac^3\}.$$

Thus, $\alpha \in K_{ac^3}$ and hence $K_{ac} \le K_{ac^3}$.

On the one hand, $|K_{ac}| = |K|/|X_3| = |K|/2$ because X_3 is an orbit of K containing ac. On the other hand, $|K_{ac^3}| = |K|/|T_{33}| = |K|/4$ because T_{33} is an orbit of K containing ac^3. Therefore $|K_{ac}| = |K|/2 > |K|/4 = |K_{ac^3}|$, a contradiction to $K_{ac} \le K_{ac^3}$. □

Lemma 3.4 completes the proof of Proposition 3.1.

□

4. Nonschurity of $Q_8 \times \mathbb{Z}_p$

The main result of this section is the following statement.

Proposition 4.1. *The group* $Q_8 \times \mathbb{Z}_p$ *is not Schur for every prime* p *such that* $p \equiv 1 \mod 4$ *or* $p \equiv 1 \mod 6$.

Let p be a prime and l a divisor of $p-1$. Suppose that $C \cong \mathbb{Z}_p$. The group $\mathrm{Aut}(C)$ is a cyclic group of order $p-1$. Since $p-1$ is divisible by l, the group $\mathrm{Aut}(C)$ has a unique subgroup M of index l. Put $m = |M| = \frac{p-1}{l}$. It is easy to see that $|\mathrm{Orb}(M, C^\#)| = l$ and $\mathrm{Aut}(C)$ acts on the set $\mathrm{Orb}(M, C^\#)$ as the regular cyclic group of order l. Let $C_1, \dots, C_l$ be the nontrivial orbits of M on C such that the cycle $f = (C_1 \cdots C_l) \in \mathrm{Sym}(\mathrm{Orb}(M, C^\#))$ is the permutation induced by a generator of $\mathrm{Aut}(C)$ acting on $\mathrm{Orb}(M, C^\#)$. Clearly, $|C_i| = |C_j|$ for all i, j and $\mathrm{Orb}(M, C)$ is the set of the basic sets of the cyclotomic S-ring $\mathcal{C} = \mathrm{Cyc}(M, C)$. In case $l = 4$, we have $C_i = C_i^{-1}$ for every i if m is even and $C_3 = C_1^{-1}$, $C_4 = C_2^{-1}$ if m is odd. In case $l = 6$, we have $C_i = C_i^{-1}$ for every i if m is even and $C_4 = C_1^{-1}$, $C_5 = C_2^{-1}$, $C_6 = C_3^{-1}$ if m is odd.

Put $c_{ij}^k = c_{C_iC_j}^{C_k}$ and $c_{i^fj^f}^{k^f} = c_{C_i^fC_j^f}^{C_k^f}$. From Lemma 2.1 it follows that f is an algebraic automorphism of $\mathcal{C}$ and hence

$$c_{i+1,j+1}^{k+1} = c_{i^fj^f}^{k^f} = c_{ij}^k \tag{3}$$

for all $i, j, k \in \{1, \dots, l\}$, where additions in the indices are done modulo 6.

Lemma 4.2. *In the above notations, let $l = 4$.*

(1) *If m is even, then $p = r^2 + 4s^2$, where $s = c_{12}^1 - c_{14}^1$ and r is an integer.*

(2) *If m is odd, then $m = c_{32}^1 + c_{34}^1 + 2c_{41}^1$.*

Proof. Observe that $c_{ij}^1 = (k-1, j-1)_4$ (see, e.g. [1, Eq. (9)]) for all $i, j \in \{1, 2, 3, 4\}$, where $k \in \{1, 2, 3, 4\}$ is such that $C_k = C_i^{-1}$ and $(k-1, j-1)_4$ is a *cyclotomic number* of order 4 (see [2] for the definition). Therefore Statement (1) of the lemma follows from [2, p. 400, Eqs. (50)-(51)], whereas Statement (2) follows from [2, p. 401, Eq. (54)]. □

Lemma 4.3. *In the above notations, let $l = 6$.*

(1) *If m is even, then $4p = r^2 + 27s^2$, where $s = c_{12}^1 + 2c_{24}^1 + c_{15}^1 - c_{13}^1 - 2c_{25}^1 - c_{16}^1$ and r is an integer. Moreover, $3s = t = 2u$ or $3s = -t - 2u$, where $t = c_{12}^1 + 2c_{24}^1 - 3c_{15}^1 + 3c_{13}^1 - c_{16}^1 - 2c_{25}^1$ and $u = c_{12}^1 - c_{16}^1 - c_{24}^1 + c_{25}^1$.*

(2) *If m is odd, then $m = c_{43}^1 + c_{45}^1 + c_{51}^1 + c_{52}^1 + 2c_{56}^1$. Moreover, $3s = -t = 2u$ or $3s = t - 2u$, where $s = c_{42}^1 + 2c_{51}^1 + c_{45}^1 - c_{43}^1 - 2c_{52}^1 - c_{46}^1$, $t = c_{45}^1 + 2c_{51}^1 - 3c_{42}^1 + 3c_{46}^1 - c_{43}^1 - 2c_{52}^1$, and $u = c_{51}^1 - c_{52}^1 + c_{43}^1 - c_{45}^1$.*

Proof. As in the previous lemma, we use the connection between cyclotomic numbers and some intersection numbers that provided by the formula $c_{ij}^1 = (k-1, j-1)_4$ (see, e.g. [1, Eq. (9)]) for all $i, j \in \{1, 2, 3, 4, 5, 6\}$, where $k \in \{1, 2, 3, 4, 5, 6\}$ is such that $C_k = C_i^{-1}$. Now Statement (1) of the lemma follows from [2, p. 409, Eqs. (89)-(90)] and the relations between the parameters denoted in [2, p. 409] by M, B and F, whereas Statement (2) follows from [2, p. 410, Eqs. (95)-(96)] and the remark after these equalities. □

Let $H = \langle a, b : \ a^4 = e, a^2 = b^2, a^b = a^{-1} \rangle \cong Q_8$ and $G = H \times C \cong Q_8 \times \mathbb{Z}_p$. If $l = 4$, then put

$$X_0 = \{e\}, \ X_1 = \{a^2\}, \ X_2 = \{ab, a^3b\}, \ X_3 = \{a, a^3, b, a^2b\},$$
$$X_4 = C^{\#}, \ X_5 = a^2C^{\#}$$
$$X_6 = \{a, a^3\}(C_2 \cup C_4) \cup \{b, a^2b\}(C_1 \cup C_3),$$
$$X_7 = aC_1 \cup a^3C_3 \cup bC_2 \cup a^2bC_4,$$
$$X_8 = X_7a^2 = aC_3 \cup a^3C_1 \cup bC_4 \cup a^2bC_2,$$
$$X_9 = \{ab, a^3b\}C^{\#}.$$

If $l = 6$, then put

$$Y_0 = \{e\}, \ Y_1 = \{a^2\}, \ Y_2 = \{a, a^3, b, a^2b, ab, a^3b\},$$
$$Y_3 = C^{\#}, \ Y_4 = a^2C^{\#}$$
$$Y_5 = \{a, a^3\}(C_1 \cup C_4) \cup \{b, a^2b\}(C_2 \cup C_5) \cup \{ab, a^3b\}(C_3 \cup C_6),$$

$$Y_6 = \{a, a^3\}(C_2 \cup C_5) \cup \{b, a^2b\}(C_3 \cup C_6) \cup \{ab, a^3b\}(C_1 \cup C_4),$$
$$Y_7 = aC_3 \cup a^2bC_4 \cup abC_5 \cup a^3C_6 \cup bC_1 \cup a^3bC_2,$$
$$Y_8 = Y_7a^2 = aC_6 \cup a^2bC_1 \cup abC_2 \cup a^3C_3 \cup bC_4 \cup a^3bC_5.$$

The sets X_i, $i \in I = \{0, \dots, 9\}$, and Y_j, $j \in J = \{0, \dots, 8\}$, form the partitions of G. Denote these partition by $\mathcal{S}$ and $\mathcal{T}$, respectively. Put $\mathcal{A} = \mathrm{Span}_{\mathbb{Z}}\{\underline{X} : X \in \mathcal{S}\}$ and $\mathcal{B} = \mathrm{Span}_{\mathbb{Z}}\{\underline{Y} : Y \in \mathcal{T}\}$.

Lemma 4.4. *The $\mathbb{Z}$-modules $\mathcal{A}$ and $\mathcal{B}$ are S-rings over G.*

Proof. One can see that $X_i = X_i^{-1}$ for $i \in I \setminus \{7, 8\}$ and $Y_j = Y_j^{-1}$ for $j \in J \setminus \{7, 8\}$. If m is even, then $X_8 = X_7^{-1}$ and $Y_8 = Y_7^{-1}$; for otherwise $X_7 = X_7^{-1}$, $X_8 = X_8^{-1}$, $Y_7 = Y_7^{-1}$, and $Y_8 = Y_8^{-1}$.

Let $\sigma_1, \sigma_2, \sigma_3 \in \mathrm{Aut}(H)$ such that $\sigma_1 : (a, b) \mapsto (b, a^3)$, $\sigma_2 : (a, b) \mapsto (a^3, b)$, and $\sigma_3 : (a, b) \mapsto (a^2b, a^3b)$. Put

$$U = \langle \sigma_1, \sigma_2 \rangle,\ V = \langle \sigma_1^2, \sigma_2, \sigma_3 \rangle,\ \text{and } U_0 = V_0 = \langle \sigma_1^2, \sigma_2 \rangle.$$

One can verify straightforwardly that $U \cong D_8$, $V \cong A_4$, and $U_0 = V_0 \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Moreover, $U_0 = V_0$ is normal in the both U and V. Put also $W = \mathrm{Aut}(C)$. Denote by W_0 the unique subgroup of W such that $W_0 > M$ and $|W_0 : M| = 2$ (such group W_0 exists because l is even). The canonical epimorphisms from U to U/U_0, from V to V/V_0, and from W to W/W_0 are denoted by π_1, π_2, and π_3, respectively.

If $l = 4$, then there exists the unique isomorphism ψ from $U/U_0 \cong \mathbb{Z}_2$ to $W/W_0 \cong \mathbb{Z}_2$. Put

$$K_1 = \{(\sigma, \tau) \in U \times W : \ (\sigma^{\pi_1})^{\psi} = \tau^{\pi_3}\} \leq \mathrm{Aut}(G).$$

If $l = 6$, then there exists the unique isomorphism θ from $V/V_0 \cong \mathbb{Z}_3$ to $W/W_0 \cong \mathbb{Z}_3$ such that $(V_0\sigma_3)^{\theta} = W_0^{f'}$, where $f' \in W$ acting on $\mathrm{Orb}(M, C^{\#})$ induces f. Put

$$K_2 = \{(\sigma, \tau) \in V \times W : \ (\sigma^{\pi_2})^{\theta} = \tau^{\pi_3}\} \leq \mathrm{Aut}(G).$$

The groups K_1 and K_2 are subdirect products of U and W and V and W, respectively. The straightforward check shows that the basic sets of the cyclotomic S-ring $\mathrm{Cyc}(K_1, G)$ are X_i, $i \in I \setminus \{7, 8\}$, and $X_7 \cup X_8$, whereas the basic sets of the cyclotomic S-ring $\mathrm{Cyc}(K_2, G)$ are Y_j, $j \in J \setminus \{7, 8\}$, and $Y_7 \cup Y_8$. This implies that $\underline{X_iX_j} \in \mathcal{A}$ for every $i, j \in I \setminus \{7, 8\}$ and $\underline{Y_iY_j} \in \mathcal{B}$ for every $i, j \in J \setminus \{7, 8\}$. Thus, to prove that $\mathcal{A}$ and $\mathcal{B}$ are S-rings, it remains to verify that $\underline{X_iX_j} \in \mathcal{A}$ and $\underline{Y_iY_j} \in \mathcal{B}$, where at least one of i, j belongs to the set $\{7, 8\}$. The latter can be done by the straightforward computation using Eq. (3). □

Lemma 4.5. *The S-ring $\mathcal{A}$ is not schurian.*

Proof. Assume the contrary. Then $\mathcal{S} = \mathrm{Orb}(K, G)$, where $K = \mathrm{Aut}(\mathcal{A})_e$. Let $c_2 \in C_2$ and $c_4 \in C_4$. The elements ac_2 and ac_4 belong to X_6. Since X_6 is an orbit of K, there exists $\alpha \in K$ such that $(ac_2)^{\alpha} = ac_4$. Due to Eq. (2), we have

$$(C_1c_2)^{\alpha} = (X_8ac_2 \cap X_4)^{\alpha} = X_8ac_4 \cap X_4 = C_1c_4. \tag{4}$$

The set Ca is a block of K because C is an $\mathcal{A}$-subgroup. Observe that $(ac_2)^{\alpha} = ac_4 \in (Ca)^{\alpha} \cap Ca$. So $(Ca)^{\alpha} = Ca$. Therefore

$$\{a\}^{\alpha} = (Ca \cap X_3)^{\alpha} = Ca \cap X_3 = \{a\}.$$

The above equality and Eq. (2) yield that

$$C_1^\alpha = (X_8a \cap X_4)^\alpha = X_8a \cap X_4 = C_1 \tag{5}$$

and

$$C_3^\alpha = (X_7a \cap X_4)^\alpha = X_7a \cap X_4 = C_3. \tag{6}$$

Suppose that m is even. Then $c_{11}^2 = |C_1c_2 \cap C_1|$ and $c_{11}^4 = |C_1c_4 \cap C_1|$. Eqs. (4) and (5) imply that

$$c_{11}^2 = |C_1c_2 \cap C_1| = |(C_1c_2 \cap C_1)^\alpha| = |C_1c_4 \cap C_1| = c_{11}^4.$$

By the latter equality and Eq. (1), we have $c_{12}^1 = c_{14}^1$. Therefore $p = r^2$ for some integer r by Lemma 4.2(1), a contradiction to primality of p.

Now suppose that m is odd. Then $c_{33}^2 = |C_1c_2 \cap C_3|$ and $c_{33}^4 = |C_1c_4 \cap C_3|$. From Eqs. (4) and (6) it follows that

$$c_{33}^2 = |C_1c_2 \cap C_3| = |(C_1c_2 \cap C_3)^\alpha| = |C_1c_4 \cap C_3| = c_{33}^4.$$

Due to the latter equality and Eq. (1), we have $c_{34}^1 = c_{32}^1$. Therefore $m = 2c_{32}^1 + 2c_{41}^1$ by Lemma 4.2(2), a contradiction to the oddity of m. □

Lemma 4.6. *The S-ring $\mathcal{B}$ is not schurian.*

Proof. Assume the contrary. Then $\mathcal{T} = \mathrm{Orb}(L, G)$, where $L = \mathrm{Aut}(\mathcal{B})_e$. Let $c_1 \in C_1$. The elements ac_1 and a^3c_1 belong to Y_5 and the elements abc_1 and a^3bc_1 belong to Y_6. Since Y_5 and Y_6 are orbits of L, there exist $\beta, \gamma \in L$ such that $(ac_1)^\beta = a^3c_1$ and $(abc_1)^\gamma = a^3bc_1$. Eq. (2) implies that

$$(C_3c_1)^\beta = (Y_8ac_1 \cap Y_3)^\beta = Y_8a^3c_1 \cap Y_3 = C_6c_1 \tag{7}$$

and

$$(C_2c_1)^\gamma = (Y_7abc_1 \cap Y_3)^\gamma = Y_7a^3bc_1 \cap Y_3 = C_5c_1. \tag{8}$$

Since C is a $\mathcal{B}$-subgroup, the sets Ca,Ca^3, Cab, and Ca^3b are blocks of L. Together with $(ac_1)^\beta = a^3c_1$ and $(abc_1)^\gamma = a^3bc_1$, this yields that $(Ca)^\beta = Ca^3$ and $(Cab)^\gamma = Ca^3b$. Therefore by Eq. (2), we have

$$\{a\}^\beta = (Ca \cap Y_2)^\beta = Ca^3 \cap Y_2 = \{a^3\}$$

and

$$\{ab\}^\gamma = (Cab \cap Y_2)^\gamma = Ca^3b \cap Y_2 = \{a^3b\}$$

Due to the above equalities and Eq. (2), we obtain

$$C_3^\beta = (Y_8a \cap Y_3)^\beta = Y_8a^3 \cap Y_3 = C_6, \tag{9}$$

$$C_6^\beta = (Y_7a \cap Y_3)^\beta = Y_7a^3 \cap Y_3 = C_3, \tag{10}$$

and

$$C_2^\gamma = (Y_7ab \cap Y_3)^\gamma = Y_7a^3b \cap Y_3 = C_5, \tag{11}$$

$$C_5^\gamma = (Y_8ab \cap Y_3)^\gamma = Y_8a^3b \cap Y_3 = C_2. \tag{12}$$

Suppose that m is even. Then $c_{33}^1 = |C_3c_1 \cap C_3|$ and $c_{66}^1 = |C_6c_1 \cap C_6|$. Eqs. (7) and (9) imply that $c_{33}^1 = c_{66}^1$. By the latter equality and Eq. (3), we have $c_{11}^2 = c_{11}^5$. Therefore

$$c_{12}^1 = c_{15}^1 \tag{13}$$

by Eq. (1). Since m is even, $c^1_{22} = |C_2c_1 \cap C_2|$ and $c^1_{55} = |C_5c_1 \cap C_5|$. Eqs. (8) and (11) imply that $c^1_{22} = c^1_{55}$. By the latter equality and Eq. (3), we have $c^3_{11} = c^6_{11}$. Therefore

$$c^1_{13} = c^1_{16} \tag{14}$$

by Eq. (1).

The definitions of t and u from Lemma 4.3(1) and Eqs. (13) and (14) yield that $t = -2u$. Together with each of the equalities $3s = t = 2u$ and $3s = -t - 2u$ (see the second part of Lemma 4.3(1)), the latter implies that $s = 0$. Therefore $4p = r^2$ for some integer r by the first part of Lemma 4.3(1), a contradiction to primality of p.

Now suppose that m is odd. Then $c^1_{33} = |C_6c_1 \cap C_3|$ and $c^1_{66} = |C_3c_1 \cap C_6|$. Due to Eqs. (7) and (10), we obtain $c^1_{33} = c^1_{66}$. By the latter equality and Eq. (3), we have $c^2_{44} = c^5_{44}$. Therefore

$$c^1_{42} = c^1_{45} \tag{15}$$

by Eq. (1). Since m is odd, $c^1_{22} = |C_5c_1 \cap C_2|$ and $c^1_{55} = |C_2c_1 \cap C_5|$. Eqs. (8) and (12) imply that $c^1_{22} = c^1_{55}$. By the latter equality and Eq. (3), we have $c^3_{44} = c^6_{44}$. Therefore

$$c^1_{43} = c^1_{46} \tag{16}$$

by Eq. (1).

Due to the definitions of t and u from Lemma 4.3(2) and Eqs. (15) and (16), we obtain $t = 2u$. Together with each of the equalities $3s = -t = 2u$ or $3s = t - 2u$ (see the second part of Lemma 4.3(2)), the latter implies that $s = 0$. Therefore

$$s = c^1_{42} + 2c^1_{51} + c^1_{45} - c^1_{43} - 2c^1_{52} - c^1_{46} = 2c^1_{45} + 2c^1_{51} - 2c^1_{43} - 2c^1_{52} = 0,$$

where the second equality holds by Eqs. (15) and (16). So $c^1_{45}+c^1_{52} = c^1_{43}+c^1_{52}$. Now from the first part of Lemma 4.3(2) it follows that $m = c^1_{43}+c^1_{45}+c^1_{51}+c^1_{52}+2c^1_{56} = 2(c^1_{43}+c^1_{52})+2c^1_{56}$, a contradiction to the oddity of m. □

Proposition 4.1 follows from Lemma 4.5 if $p \equiv 1 \mod 4$ and from Lemma 4.6 if $p \equiv 1 \mod 6$.

5. Proof of Theorem 1.1

We start with a lemma on the structure of nilpotent Schur groups.

Lemma 5.1. *Let G be a nonabelian nilpotent Schur group. Then $G = P \times H$, where P is isomorphic to one of the groups G_{16}, Q_8, D_{2^k}, $k \geq 3$, and H is a cyclic group of odd order.*

Proof. Since G is nilpotent, it is a direct product of its Sylow subgroups. At least one of the Sylow subgroups of G, say Sylow p-subgroup P, is nonabelian, because G is nonabelian. The group P is Schur as a subgroup of the Schur group G. From [9, Theorem 4.2], [7, Theorem 1.2], and [11, Theorem 1] it follows that $p = 2$ and P is isomorphic to one of the groups G_{16}, Q_8, D_{2^k}, $k \geq 3$. Let H be the Hall $2'$-subgroup of G. Then $G = P \times H$. Due to [9, Corollary 4.3], the group H is cyclic. □

We continue with one more lemma on the groups $Q_8 \times \mathbb{Z}_{pq}$.

Lemma 5.2. *The group $Q_8 \times \mathbb{Z}_{pq}$ is not Schur for every odd primes p and q.*

Proof. Let $A \cong \mathbb{Z}_4$, $B \cong \mathbb{Z}_2$, and $C \cong \mathbb{Z}_{pq}$. Let a, b, and c be generators of A, B, and C, respectively. Put $a_1 = a^2$, $A_1 = \langle a_1 \rangle$, $c_1 = c^q$, $C_1 = \langle c_1 \rangle \cong \mathbb{Z}_p$, and $G = A \times B \times C \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_{pq}$. To prove Proposition 5.2, we will show that the nonschurian S-ring $\mathcal{A}$ over G constructed in [4, Theorem 4.1] is isomorphic to an S-ring over $Q_8 \times \mathbb{Z}_{pq}$.

Let us recall that $\mathcal{A}$ is the $(A \times C)/A_1$-wreath product in our notations (see [4, pp. 8-10]). Therefore $\sigma \in \mathrm{Aut}(G)$ such that $\sigma : (a, b, c) \mapsto (a, a_1 b, c)$ is an automorphism of $\mathcal{A}$. Since $G_r \leq \mathrm{Aut}(\mathcal{A})$, we conclude that $\sigma a_r, \sigma b_r \in \mathrm{Aut}(\mathcal{A})$. The straightforward computation implies that $|\sigma a_r| = |\sigma b_r| = 4$, $(\sigma a_r)^2 = (\sigma b_r)^2$, and $(\sigma a_r)^{\sigma b_r} = (\sigma a_r)^{-1}$. So $H = \langle \sigma a_r, \sigma b_r \rangle \cong Q_8$. Moreover, one can easily verify that H is transitive and hence regular on $A \times B$. Thus, $H \times C_r$ is a regular subgroup of $\mathrm{Aut}(\mathcal{A})$ isomorphic to $Q_8 \times \mathbb{Z}_{pq}$. The latter yields that $\mathcal{A}$ is isomorphic to an S-ring over $Q_8 \times \mathbb{Z}_{pq}$. Since $\mathcal{A}$ is nonschurian by [4, Theorem 4.1], the group $Q_8 \times \mathbb{Z}_{pq}$ is not Schur. □

Proof of Theorem 1.1. Schurity of the groups Q_8, G_{16}, and D_{2^k}, where $3 \leq k \leq 5$, follows from [9, Theorem 4.2]. Let G be a nonabelian nilpotent Schur group. Then $G = P \times H$, where P is isomorphic to one of the groups G_{16}, Q_8, D_{2^k}, $k \geq 3$, and H is a cyclic group of odd order be Lemma 5.1. We may assume that H is nontrivial because for otherwise the statement of the theorem holds. If P is isomorphic to D_{2^k}, $k \geq 3$, or G_{16}, then H has a subgroup isomorphic to D_8 and hence G has a subgroup isomorphic to $D_8 \times \mathbb{Z}_p$ for some odd prime p. The latter group is not Schur by Proposition 3.1. Therefore G is not Schur, a contradiction to the assumption.

The above paragraph yields that P is isomorphic to Q_8. If $|H|$ has at least two prime divisors (possibly, equal), then H has a subgroup isomorphic to $\mathbb{Z}_{pq}$ for some odd primes p and q and hence G has a subgroup isomorphic to $Q_8 \times \mathbb{Z}_{pq}$. The latter group is not Schur by Lemma 5.2. Therefore G is not Schur, a contradiction to the assumption. Thus, H is a cyclic group of odd prime order and we are done by [9, Lemma 3.1] if $p \leq 3$ and by Proposition 4.1 otherwise. □

References

1. *R. Bildanov, V. Panshin, G. Ryabov*, On WL-rank and WL-dimension of some Deza circulant graphs, Graphs Combin., **37**, No. 6 (2021), 2397–2421.
2. *L. E. Dickson*, Cyclotomy, higher congruences, and Waring's problem, Amer. J. Math., **57** (1935), 391–424.
3. *S. Evdokimov, I. Kovács, I. Ponomarenko*, Characterization of cyclic Schur groups, St. Petersburg Math. J., **25**, No. 5 (2014), 755–773.
4. *S. Evdokimov, I. Kovács, and I. Ponomarenko*, On schurity of finite abelian groups, Commun. Algebra, **44**, No. 1 (2016), 101–117.
5. *J. Golfand, N. Najmark, R. Pöschel*, The structure of S-rings over $\mathbb{Z}_{2^m}$, Preprint P-01/85 Akad. der Wiss. der DDR, ZIMM, Berlin (1985).
6. *M. Klin, Pöschel*, The König problem, the isomorphism problem for cyclic graphs and the method of Schur rings, in: "Algebraic Methods in Graph Theory, Szeged, 1978", Colloq. Math. Soc. János Bolyai, **25**, North-Holland, Amsterdam (1981), 405–434.
7. *M. Muzychuk, I. Ponomarenko*, On Schur 2-groups, J. Math. Sci. (N.-Y.), **219**, No. 4 (2016), 565–594.
8. *I. Ponomarenko, G. Ryabov*, Abelian Schur groups of odd order, Sib. Elect. Math. Reports, **15** (2018), 397–411.
9. *I. Ponomarenko, A. Vasil'ev*, On nonabelian Schur groups, J. Algebra Appl., **13**, No. 8, Article ID 1450055 (2014).
10. *R. Pöschel*, Untersuchungen von s-ringen insbesondere im gruppenring von p-gruppen, Math. Nachr. **60** (1974), 1–27.

11. *G. Ryabov*, On Schur 3-groups, Sib. Electron. Math. Rep., **12** (2015), 223–331.
12. *G. Ryabov*, On Schur p-groups of odd order, J. Algebra Appl., **16**, No. 3, Article ID 1750045 (2017).
13. *G. Ryabov*, Classification of abelian Schur groups, in preparation.
14. *I. Schur*, Zur theorie der einfach transitiven Permutationgruppen, S.-B. Preus Akad. Wiss. Phys.-Math. Kl., **18**, No. 20 (1933), 598–623.
15. *H. Wielandt*, Finite permutation groups, Academic Press, New York - London (1964).
16. *H. Wielandt*, Permutation groups through invariant relations and invariant functions, Lect. Notes Dept. Math. Ohio St. Univ., Columbus (1969).
17. *M. Ziv-Av*, Enumeration of Schur rings over small groups, Lecture Notes in Computer Science, **8660** (2014), 491–500.

Sobolev Institute of Mathematics, Novosibirsk, Russia

Novosibirsk State Technical University, Novosibirsk, Russia
Email address: gric2ryabov@gmail.com