On a Huge Family of Non-Schurian Schur Rings

Akihide Hanaki*
Faculty of Science, Shinshu University,
Matsumoto, Japan
hanaki@shinshu-u.ac.jp

Takuto Hirai
Department of Science,
Graduate School of Science and Technology,
Shinshu University,
Matsumoto, Japan
takuto.hirai2021@gmail.com

Ilia Ponomarenko
St. Petersburg Department of the Steklov Mathematical Institute,
St. Petersburg, Russia
inp@pdmi.ras.ru

Submitted: Sep 3, 2021; Accepted: Feb 10, 2022; Published: Apr 22, 2022

Abstract

In his famous monograph on permutation groups, H. Wielandt gives an example of a Schur ring over an elementary abelian group of order p^2 ($p > 3$ is a prime), which is non-schurian, that is, it is the transitivity module of no permutation group. Generalizing this example, we construct a huge family of non-schurian Schur rings over elementary abelian groups of even rank.

Mathematics Subject Classifications: 20C05

1 Introduction

A *Schur ring* over a finite group H is a subring of a group algebra of H, which has a distinguished linear basis corresponding to a certain partition of H. A typical example of a Schur ring is obtained when H is a regular subgroup of a group $G \leqslant \mathrm{Sym}(H)$ and the partition is formed by the orbits of the stabilizer of 1_H in G. These rings were introduced by I. Schur (1933) and named after him *schurian*. However there are non-schurian Schur rings. Apparently, the first such example was given by H. Wielandt [10, Theorem 26.4] for elementary abelian groups H of rank 2; some other examples can be found in [3, 9]. A

*Supported by JSPS KAKENHI Grant Number JP17K05165.

goal of the present paper is to generalize Wielandt's example by constructing non-schurian Schur rings over all elementary abelian groups of even rank except for the order 2^2, 3^2, and 2^4.

Let $\mathbb{F} = \mathbb{F}_q$ be a Galois field of order q. We denote by $\mathcal{L}$ the set of all lines, 1-dimensional subspaces, in the 2-dimensional $\mathbb{F}$-vector space $V = \mathbb{F}^2$. Then $\mathcal{L} = \{L_\alpha \mid \alpha \in \mathbb{F} \cup \{\infty\}\}$, where

$$\begin{aligned} L_\alpha &= \{(x, \alpha x) \mid x \in \mathbb{F}\} \quad (\alpha \in \mathbb{F}), \\ L_\infty &= \{(0, x) \mid x \in \mathbb{F}\}. \end{aligned}$$

Let $\Pi = \{P_1, \ldots, P_r\}$ be a partition of $\mathcal{L}$ into a disjoint union of $r \geqslant 1$ subsets P_i, $i = 1, \ldots, r$. This partition induces a partition $\widetilde{\Pi} = \{\{(0,0)\}, \widetilde{P}_1, \ldots, \widetilde{P}_r\}$ of the vector space V, where $\widetilde{P}_i = \bigcup_{L_\alpha \in P_i} L_\alpha^\sharp$ and $L_\alpha^\sharp = L_\alpha \setminus \{(0,0)\}$. It is easy to see that the partition $\widetilde{\Pi}$ defines a Schur ring $\mathcal{S}(\Pi)$ over the additive group V^+ which is an elementary abelian group of order q^2 (Theorem 1). We set

$$\mathcal{M}(\Pi) = \{\alpha \in \mathbb{F} \cup \{\infty\} \mid \{L_\alpha\} \in \Pi\}. \tag{1}$$

Our main theorem shows that, if $\{\infty, 0, 1\} \subset \mathcal{M}(\Pi)$ and $\mathcal{M}(\Pi) \setminus \{\infty\}$ is not a subfield of $\mathbb{F}$, then the Schur ring $\mathcal{S}(\Pi)$ is not schurian (Theorem 2). The above mentioned Wielandt's example is just the case when $q \geqslant 5$ is a prime number and $\Pi = \{\{L_\infty\}, \{L_0\}, \{L_1\}, \mathcal{L} \setminus \{L_\infty, L_0, L_1\}\}$.

It should be noted that the number of (pairwise nonisomorphic) constructed Schur rings is really huge. Indeed, the number of all (not necessarily nonisomorphic) rings is roughly equal to the number of all partitions of the set $\mathcal{L} \setminus \{L_\infty, L_0, L_1\}$, which is of order $c^{\sqrt{q}}$, where c is a positive constant. On the other hand, when q is a prime, the group $H = V^+$ is elementary abelian of order q^2. It is known (see [1] and [6, Theorem 3.9]) that any two Schur rings over such a group are isomorphic if and only if the partition of one of them is the image of the partition of the other with respect to a suitable element of the group $\mathrm{Aut}(H) = \mathrm{GL}(2, q)$. It follows that the isomorphism class of a Schur ring over H is of cardinality at most q^4. Thus if q is prime, then the number of pairwise nonisomorphic Schur rings in the constructed family is exponential in q.

We complete the introduction by remarking that there is a one-to-one (isomorphism and schurity preserving) correspondence between Schur rings and association schemes admitting a regular automorphism group, see [7, Subsection 2.2]. The classes of the association scheme corresponding to a Schur ring over a group H are the Cayley graphs on H, the connecting sets of which are the classes of the partition of the ring. In the sense of the correspondence, the Schur rings constructed in our paper correspond to fusions of amorphic association schemes appeared in [4, Sec. 3]; some other non-schurian fusions were studied in [5]. Thus Theorem 1 can also be deduced by using from [4, Theorem 3.3].

2 Proofs of the main results

2.1 Schur rings

Let H be a finite group, $\mathbb{Z}H$ the group ring of H over the ring of rational integers $\mathbb{Z}$, and Π a partition of H. Set

$$\mathcal{A} = \bigoplus_{X \in \Pi} \mathbb{Z}\underline{X} \subset \mathbb{Z}H,$$

where for any set $X \subset H$, we put $\underline{X} = \sum_{x \in X} x \in \mathbb{Z}H$. Following [10], we say that $\mathcal{A}$ is a *Schur ring* over H if the following conditions are satisfied:

(S1) $\{1_H\} \in \Pi$,

(S2) $\{x^{-1} \mid x \in X\} \in \Pi$ for all $X \in \Pi$, and

(S3) $\mathcal{A}$ is a subring of $\mathbb{Z}H$.

A typical example of a Schur ring is obtained as follows. Let $G \leqslant \mathrm{Sym}(H)$ be a (transitive) permutation group containing H as a regular subgroup, and let G_1 be the stabilizer of the point 1_H in G. Then the partition of H into the G_1-orbits defines a Schur ring over H [10, Theorem 24.1]. Any Schur ring obtained in this way is said to be *schurian*.

For more details on Schur rings the reader is referred to [7].

2.2 Construction

Keeping the notations from Introduction, let q be a power of prime and H an elementary abelian group of order q^2. To avoid misunderstanding, we use multiplicative notation for H and fix an isomorphism $\rho : V^+ \to H$. Let $\Pi = \{P_1, \ldots, P_r\}$ be a partition of $\mathcal{L}$, and let $\widetilde{P}_1, \ldots, \widetilde{P}_r$ be as in Introduction. Set

$$\underline{\widetilde{P}_i} = \sum_{L_\alpha \in P_i} \sum_{\boldsymbol{x} \in L_\alpha^\sharp} \rho(\boldsymbol{x}) \in \mathbb{Z}H, \quad i = 1, \ldots, r,$$

and

$$\mathcal{S}(\Pi) = \mathbb{Z}\rho(0,0) \oplus \left(\bigoplus_{i=1}^{r} \mathbb{Z}\underline{\widetilde{P}_i} \right) \subset \mathbb{Z}H.$$

Theorem 1. *Let Π be an arbitrary partition of $\mathcal{L}$. Then $\mathcal{S}(\Pi)$ is a Schur ring over the group H.*

Proof. The conditions (S1) and (S2) are clear by definition. It is easily seen that if

$$Q_i = \sum_{L_\alpha \in P_i} \sum_{\boldsymbol{x} \in L_\alpha} \rho(\boldsymbol{x}) \in \mathbb{Z}H, \quad i = 1, \ldots, r,$$

then

$$\mathcal{S}(\Pi) = \mathbb{Z}\rho(0,0) \oplus \left(\bigoplus_{i=1}^{r} \mathbb{Z}Q_i \right). \tag{2}$$

Since $\mathcal{S}(\Pi)$ is closed with respect to addition, it suffices to show that $\mathcal{S}(\Pi)$ written in form (2) is closed with respect to multiplication. Let α and β be distinct elements of $\mathbb{F} \cup \{\infty\}$. Then

$$\left(\sum_{\boldsymbol{x} \in L_\alpha} \rho(\boldsymbol{x}) \right) \left(\sum_{\boldsymbol{y} \in L_\beta} \rho(\boldsymbol{y}) \right) = \sum_{\boldsymbol{x} \in L_\alpha} \sum_{\boldsymbol{y} \in L_\beta} \rho(\boldsymbol{x} + \boldsymbol{y}) = \sum_{\boldsymbol{z} \in V} \boldsymbol{z} \in \mathcal{S}(\Pi),$$

because L_α and L_β are distinct 1-dimensional subspaces of the 2-dimensional vector space V. Also we have

$$\left(\sum_{\boldsymbol{x} \in L_\alpha} \rho(\boldsymbol{x}) \right)^2 = q \left(\sum_{\boldsymbol{x} \in L_\alpha} \rho(\boldsymbol{x}) \right).$$

Thus, if $i \neq j$, then

$$Q_i Q_j = |P_i|\,|P_j| \sum_{\boldsymbol{z} \in V} \boldsymbol{z} \in \mathcal{S}(\Pi),$$

and

$$Q_i{}^2 = qQ_i + |P_i|(|P_i| - 1) \sum_{\boldsymbol{z} \in V} \boldsymbol{z} \in \mathcal{S}(\Pi).$$

Thus, $\mathcal{S}(\Pi)$ is a Schur ring over H. □

2.3 The main theorem

We are ready to state the main result of the present paper.

Theorem 2. *Let $\mathbb{F}$ be a Galois field of order q, $\mathcal{L}$ the set of all lines in the vector space $V = \mathbb{F}^2$, Π a partition of $\mathcal{L}$, and $\mathcal{S}(\Pi)$ the Schur ring over the elementary abelian group $H \cong V^+$ of order q^2. Suppose that*

$$\{\infty, 0, 1\} \subset \mathcal{M}(\Pi) \quad \textit{and} \quad \mathcal{M}(\Pi) \setminus \{\infty\} \textit{ is not a subfield of } \mathbb{F}, \tag{3}$$

where $\mathcal{M}(\Pi)$ is defined by (1). *Then the Schur ring $\mathcal{S}(\Pi)$ is non-schurian.*

Remark 3. The first assumption in (3) can be replaced by the assumption $|\mathcal{M}(\Pi)| \geqslant 3$. This follows from the fact that the action of $\mathrm{GL}(2,q)$ on $\mathcal{L}$ is 3-transitive for $q > 3$ [2, p. 245]. Note that the second assumption in (3) is invariant with respect to the action of $\mathrm{GL}(2,q)$ on $\mathcal{L}$ under the assumption $\{\infty, 0, 1\} \subset \mathcal{M}(\Pi)$.

To prove Theorem 2, let $q = p^e$, where p is a prime and $e \geqslant 1$ is an integer. We need the following auxiliary lemma.

Lemma 4. *Let σ be an $\mathbb{F}_p$-linear transformation on V such that the sets L_0, L_1, and L_∞ are σ-invariant. Let $\alpha, \beta \in \mathbb{F}$ be such that the sets L_α and L_β are σ-invariant. Then so are $L_{\alpha+\beta}$ and $L_{\alpha\beta}$.*

Proof. We fix an element $\zeta \in \mathbb{F}$ such that $\mathbb{F} = \mathbb{F}_p[\zeta]$; for example, ζ is a primitive (p^e-1)th root of unity. Then the set $\{1, \zeta, \ldots, \zeta^{e-1}\}$ is an $\mathbb{F}_p$-basis of $\mathbb{F}$. Given $x \in \mathbb{F}$ or $x \in V$, we define the column vector

$$V(x) = [x, \zeta x, \ldots, \zeta^{e-1}x]^T.$$

Let $M(e,p)$ be the full matrix algebra of degree e over $\mathbb{F}_p$, and let $\Psi : \mathbb{F} \to M(e,p)$ be the regular representation of $\mathbb{F}$ as an $\mathbb{F}_p$-algebra with respect to the basis $\{1, \zeta, \ldots, \zeta^{e-1}\}$. Namely, $\Psi(\gamma)V(1) = V(\gamma)$ for all $\gamma \in \mathbb{F}$.

Let $\boldsymbol{x} = (1,0)$ and $\boldsymbol{y} = (0,1) \in V$. Then

$$\{\boldsymbol{x}, \zeta\boldsymbol{x}, \ldots, \zeta^{e-1}\boldsymbol{x}\},\ \{\boldsymbol{y}, \zeta\boldsymbol{y}, \ldots, \zeta^{e-1}\boldsymbol{y}\},\ \{(\boldsymbol{x}+\boldsymbol{y}), \zeta(\boldsymbol{x}+\boldsymbol{y}), \ldots, \zeta^{e-1}(\boldsymbol{x}+\boldsymbol{y})\}$$

are $\mathbb{F}_p$-bases of L_0, L_∞, and L_1, respectively. Since L_0, L_1, and L_∞ are σ-invariant, there exist matrices $A, B, C \in M(e,p)$ such that

$$\sigma(\boldsymbol{s}V(\boldsymbol{x})) = \boldsymbol{s}AV(\boldsymbol{x}),\ \sigma(\boldsymbol{s}V(\boldsymbol{y})) = \boldsymbol{s}BV(\boldsymbol{y}),\ \sigma(\boldsymbol{s}V(\boldsymbol{x}+\boldsymbol{y})) = \boldsymbol{s}CV(\boldsymbol{x}+\boldsymbol{y})$$

for all row vectors $\boldsymbol{s} \in (\mathbb{F}_p)^e$. Since the set $\{\boldsymbol{x}, \zeta\boldsymbol{x}, \ldots, \zeta^{e-1}\boldsymbol{x}, \boldsymbol{y}, \zeta\boldsymbol{y}, \ldots, \zeta^{e-1}\boldsymbol{y}\}$ is $\mathbb{F}_p$-linearly independent, we have $A = B = C$.

By hypothesis, L_α is σ-invariant. Therefore by the above argument for $\mathbb{F}_p$-bases $\{\boldsymbol{x}, \zeta\boldsymbol{x}, \ldots, \zeta^{e-1}\boldsymbol{x}\}$, $\{\alpha\boldsymbol{y}, \zeta\alpha\boldsymbol{y}, \ldots, \zeta^{e-1}\alpha\boldsymbol{y}\}$, $\{(\boldsymbol{x}+\alpha\boldsymbol{y}), \zeta(\boldsymbol{x}+\alpha\boldsymbol{y}), \ldots, \zeta^{e-1}(\boldsymbol{x}+\alpha\boldsymbol{y})\}$ of L_0, L_∞, and L_α, respectively, we have

$$\sigma(\boldsymbol{s}V(\alpha\boldsymbol{y})) = \boldsymbol{s}AV(\alpha\boldsymbol{y}) = \boldsymbol{s}A\Psi(\alpha)V(\boldsymbol{y}) \tag{4}$$

for all $\boldsymbol{s} \in (\mathbb{F}_p)^e$. On the other hand,

$$\sigma(\boldsymbol{s}V(\alpha\boldsymbol{y})) = \sigma(\boldsymbol{s}\Psi(\alpha)V(\boldsymbol{y})) = \boldsymbol{s}\Psi(\alpha)AV(\boldsymbol{y}).$$

Thus, $A\Psi(\alpha) = \Psi(\alpha)A$ and similarly $A\Psi(\beta) = \Psi(\beta)A$.

The set $\{\boldsymbol{x}+\alpha\boldsymbol{y}+\beta\boldsymbol{y}, \zeta(\boldsymbol{x}+\alpha\boldsymbol{y}+\beta\boldsymbol{y}), \ldots, \zeta^{e-1}(\boldsymbol{x}+\alpha\boldsymbol{y}+\beta\boldsymbol{y})\}$ is a basis of $L_{\alpha+\beta}$. Since also

$$\begin{aligned}
\sigma(\boldsymbol{s}V(\boldsymbol{x}+\alpha\boldsymbol{y}+\beta\boldsymbol{y})) &= \sigma(\boldsymbol{s}V(\boldsymbol{x})) + \sigma(\boldsymbol{s}V(\alpha\boldsymbol{y})) + \sigma(\boldsymbol{s}V(\beta\boldsymbol{y})) \\
&= \boldsymbol{s}AV(\boldsymbol{x}) + \boldsymbol{s}AV(\alpha\boldsymbol{y}) + \boldsymbol{s}AV(\beta\boldsymbol{y}) \\
&= \boldsymbol{s}AV(\boldsymbol{x}+\alpha\boldsymbol{y}+\beta\boldsymbol{y}) \in L_{\alpha+\beta}
\end{aligned}$$

by (4), the set $L_{\alpha+\beta}$ is σ-invariant.

The set $\{\boldsymbol{x}+\alpha\beta\boldsymbol{y}, \zeta(\boldsymbol{x}+\alpha\beta\boldsymbol{y}), \ldots, \zeta^{e-1}(\boldsymbol{x}+\alpha\beta\boldsymbol{y})\}$ is a basis of $L_{\alpha\beta}$. Since also

$$\begin{aligned}
\sigma(\boldsymbol{s}V(\boldsymbol{x}+\alpha\beta\boldsymbol{y})) &= \sigma(\boldsymbol{s}V(\boldsymbol{x})) + \sigma(\boldsymbol{s}V(\alpha\beta\boldsymbol{y})) \\
&= \sigma(\boldsymbol{s}V(\boldsymbol{x})) + \sigma(\boldsymbol{s}\Psi(\alpha)\Psi(\beta)V(\boldsymbol{y})) \\
&= \boldsymbol{s}AV(\boldsymbol{x}) + \boldsymbol{s}\Psi(\alpha)\Psi(\beta)AV(\boldsymbol{y}) \\
&= \boldsymbol{s}AV(\boldsymbol{x}) + \boldsymbol{s}A\Psi(\alpha)\Psi(\beta)V(\boldsymbol{y}) \\
&= \boldsymbol{s}AV(\boldsymbol{x}) + \boldsymbol{s}AV(\alpha\beta\boldsymbol{y}) = \boldsymbol{s}AV(\boldsymbol{x}+\alpha\beta\boldsymbol{y}) \in L_{\alpha\beta},
\end{aligned}$$

the set $L_{\alpha\beta}$ is σ-invariant. □

The next lemma can be extracted from the proof of [10, Lemma 26.3]. To make the paper self-contained, we give a full proof of it.

Lemma 5. *Let G be a transitive permutation group on a finite abelian group H containing H as a regular subgroup. Suppose that there are subgroups A, B and C of H such that $H = A \times B = A \times C = B \times C$ and A, B and C are invariant with respect to the action of the stabilizer G_1 of $1_H \in H$ in G. Then H is a normal subgroup of G.*

Proof. By assumption, A is invariant with respect to the action of G_1. This means $G_1AG_1 \subset G_1A$ and thus G_1A is a subgroup of G. Similarly, G_1B is also a subgroup of G. We set $M = \{g \in G \mid (G_1Ab)g = G_1Ab \text{ for all } b \in B\}$ and $N = \{g \in G \mid (G_1Ba)g = G_1Ba \text{ for all } a \in A\}$. Clearly, $A \leqslant M$ and $B \leqslant N$.

Let $m \in M$, $g \in G$, $b \in B$. There exist $x \in G_1A$ and $b' \in B$ such that $bg^{-1} = xb'$. Now $(G_1Ab)(g^{-1}mg) = G_1Axb'mg = G_1Ab'mg = G_1Ab'g = G_1Ax^{-1}b = G_1Ab$ and thus $g^{-1}mg \in M$. This means that $M \lhd G$ and similarly $N \lhd G$.

Suppose $g \in M \cap N$. Let $a \in A$ and $b \in B$. Then $(G_1ab)g \subset (G_1Ab)g = G_1Ab$ and $(G_1ab)g \subset (G_1Ba)g = G_1Ba$. Now $(G_1ab)g \subset G_1Ab \cap G_1Ba = G_1ab$. Since $H = AB$ is regular, $g = 1$ holds. We have $M \cap N = 1$, and thus $MN = M \times N$.

We set $A^G = \langle A^g \mid g \in G\rangle \lhd G$. Since $M \lhd G$, $A^G \leqslant M$ and similarly $B^G \leqslant N$. Thus A^G and B^G commute elementwise. The same is true for A^G and C^G, and B^G and C^G. Especially, C^G commutes with $H = AB$ elementwise. Since an abelian transitive group is regular [10, Proposition 4.4], we have $C^G \leqslant C_G(H) = H$, and similarly $A^G \leqslant H$, $B^G \leqslant H$. Now $H = AB \leqslant A^GB^G \leqslant H$ and thus $H = A^GB^G \lhd G$. □

Proof of Theorem 2. Suppose that the Schur ring $\mathcal{S}(\Pi)$ is schurian. Then there is a (transitive) permutation group $G \leqslant \mathrm{Sym}(H)$ containing $H = \rho(V^+)$ as a regular subgroup. Moreover,

$$H = \rho(L_0) \times \rho(L_1) = \rho(L_0) \times \rho(L_\infty) = \rho(L_1) \times \rho(L_\infty)$$

and

$$\underline{\rho(L_0)},\ \underline{\rho(L_1)},\ \underline{\rho(L_\infty)} \in \mathcal{S}(\Pi).$$

By Lemma 5, we conclude that H is normal in G. According to [8, Theorem 4.2], we may assume that the stabilizer G_1 is a subgroup of $\mathrm{Aut}(H) \cong \mathrm{GL}(2e, p)$.

Now let $\alpha, \beta \in \mathcal{M}(\Pi) \setminus \{\infty\}$. Then given $\sigma \in G_1$, the sets L_α and L_β are obviously σ-invariant. By Lemma 4, this implies that so are the sets $L_{\alpha+\beta}$ and $L_{\alpha\beta}$. It follows that

$$\underline{\rho(L_{\alpha+\beta})},\ \underline{\rho(L_{\alpha\beta})} \in \mathcal{S}(\Pi) \quad \text{and} \quad \alpha+\beta,\ \alpha\beta \in \mathcal{M}(\Pi).$$

Thus, $\mathcal{M}(\Pi) \setminus \{\infty\}$ must be a subfield of $\mathbb{F}$, which completes the proof. □

Acknowledgements

The authors thank to the anonymous referee for useful comments and suggestions improving the presentation of the paper.

References

[1] B. Alspach and L. Nowitz, *Elementary Proofs that* $\mathbb{Z}_p^2$ *and* $\mathbb{Z}_p^3$ *are CI-groups*, European J. Combin., **20** (1999), no. 7, 607–617.

[2] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer-Verlag, New York, 1996.

[3] S. Evdokimov and I. Ponomarenko, *On a family of Schur rings over a finite cyclic group*, Algebra i Analiz **13** (2001), no. 3, 139–154; translation in St. Petersburg Math. J. **13** (2002), no. 3, 441–451.

[4] Ja. Ju. Gol'fand, A. V. Ivanov and M. K. Klin, *Amorphic cellular rings*, in: Investigations in Algebraic Theory of Combinatorial Objects, Springer, Dordrecht, Math. App., Sov. Ser. **84** (1994), pp. 167–186.

[5] M. Klin, N. Kriger, and A. Woldar, *On the existence of self-complementary and non-self-complementary strongly regular graphs with Paley parameters*, J. Geom. **107** (2016), no. 2, 329–356.

[6] M. Muzychuk, M. Klin, and R. Pöschel, *The isomorphism problem for circulant graphs via Schur ring theory*, in: DIMACS, Ser. Discrete Math. Theor. Comput. Sci., **56** (2001), pp. 241–264.

[7] M. Muzychuk and I. Ponomarenko, *Schur rings*, European J. Combin. **30** (2009), no. 6, 1526–1539.

[8] D. S. Passman, *Permutation groups*, Dover Publications, Inc., Mineola, NY, 2012, Revised reprint of the 1968 original.

[9] I. Ponomarenko and A. Vasil'ev, *On non-abelian Schur groups*, J. Algebra Appl. **13** (2014), no. 8, 1450055, 22.

[10] H. Wielandt, *Finite permutation groups*, Academic Press, New York-London, 1964, Translated from the German by R. Bercov.