An answer to Hirasaka and Muzychuk: every p-Schur ring over C_p^3 is Schurian

Dedicated to the memory of Jiping (Jim) Liu

Pablo Spiga [a] and Qiang Wang [b,1]

[a] *Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta, T1K 3M4, CANADA*

[b] *School of Mathematics and Statistics, Carleton University, Ottawa, Ontario, K1S 5B6, CANADA*

Abstract

In [HiMu] the authors, in their analysis on Schur rings, pointed out that it is not known whether there exists a non-Schurian p-Schur ring over an elementary abelian p-group of rank 3. In this paper we prove that every p-Schur ring over an elementary abelian p-group of rank 3 is in fact Schurian.

1 Introduction

Let H be a finite group with identity 1_H. We denote the group algebra of H over the field $\mathbb{Q}$ of rational numbers by $\mathbb{Q}H$. For $B \subseteq H$ we define $\underline{B}$ to be the sum $\sum_{b\in B} b$, elements of this form will be called simple quantities, see [Wi]. A subalgebra $\mathcal{A}$ of the group algebra $\mathbb{Q}H$ is called a Schur ring over H if the following conditions are satisfied:

(1) there exists a basis of $\mathcal{A}$ consisting of simple quantities $\underline{T}_0, \ldots, \underline{T}_r$;
(2) $T_0 = \{1_H\}$, $\cup_{i=0}^{r} T_i = H$ and $T_i \cap T_j = \emptyset$ if $i \neq j$;
(3) for each i there exists i' such that $T_{i'} = \{t^{-1} \mid t \in T_i\}$.

We denote by $\mathrm{Bsets}(\mathcal{A})$ the set $\{T_0, \ldots, T_r\}$, by $\mathrm{Sym}(H)$ the symmetric group on the set H, and by $\mathrm{GL}(V)$ the general linear group on the vector space V.

Email address: spiga@cs.uleth.ca, wang@math.carleton.ca.

[1] The research is supported by NSERC of Canada

A Schur ring $\mathcal{A}$ over a p-group H is said to be a p-Schur ring, p-S ring for short, if every set in $\mathrm{Bsets}(\mathcal{A})$ has size a power of p.

Consider a permutation group G in $\mathrm{Sym}(H)$ containing the right regular representation of H. Denote by $T_0 = \{1\}, T_1, \ldots, T_r$, the orbits of the stabilizer $G_1 = \{g \in G \mid 1^g = 1\}$. The transitivity module $V(H, G_1)$ of the group G is the vector space spanned by $\underline{T}_i$, for $i = 0, \ldots, r$. It was proved by Schur, see [Wi], that $V(H, G_1)$ is a Schur ring over H.

It is customary to say that a Schur ring $\mathcal{A}$ is Schurian if $\mathcal{A}$ is the transitivity module $V(H, G_1)$ of some group G containing the right regular representation of H.

It is well-known that not every Schur ring is the transitivity module of an appropriate group. Furthermore, it is easy to check that every p-S ring over an elementary abelian p-group of rank 1 or 2 is in fact Schurian.

Schur rings are a really powerful tool for solving some fairly hard isomorphism problems on Cayley graphs, see [HiMu] and [Mu]. In particular, in these applications of Schur rings it is important to have a good understanding of Schur rings over elementary abelian p-groups and hopefully to have a complete classification of these algebras. In this context, in [HiMu] the authors point out that it is not even known whether every p-S ring over an elementary abelian p-group of rank 3 is actually Schurian. In this paper we answer this question with the following theorem.

Theorem 1 *Every p-S ring over an elementary abelian p-group of rank 3 is Schurian.*

2 Proof of Theorem 1

Let $\mathcal{A}$ be a Schur ring over H, we say that the subgroup K of H is an $\mathcal{A}$-subgroup of H if $\underline{K} \in \mathcal{A}$. We assume that the reader is familiar with the basic results on Schur rings and we refer the rusty reader to [Wi]. We present the results that we are going to extensively use, see [Zi] and [Wi].

Proposition 1 *Let $\mathcal{A}$ be a p-S ring over H. Then*

(a) $\mathcal{O}_*(\mathcal{A}) = \{h \in H \mid \{h\} \in \mathrm{Bsets}(\mathcal{A})\}$ *is a nontrivial $\mathcal{A}$-subgroup of H.*
(b) $\mathcal{O}^*(\mathcal{A}) = \langle\{T^{-1}T \mid T \in \mathrm{Bsets}(\mathcal{A})\}\rangle$ *is a proper $\mathcal{A}$-subgroup of H.*

Proposition 2 *Let $\mathcal{A}$ be a Schur ring over an abelian group H (additive notation), if $T \in \mathrm{Bsets}(\mathcal{A})$ and i is coprime to $|H|$ then $(i)T = \{it \mid t \in T\}$ lies in $\mathrm{Bsets}(\mathcal{A})$.*

Proposition 3 *Let $\mathcal{A}$ be a Schur ring. If $T, \{m\} \in \mathrm{Bsets}(\mathcal{A})$ then $T + m = \{t + m \mid t \in T\}$ lies in $\mathrm{Bsets}(\mathcal{A})$.*

Proposition 4 *Let $\mathcal{A}$ be a Schur ring over H. If $T \in \mathrm{Bsets}(\mathcal{A})$ then $\mathrm{St}(T) = \{h \in H \mid Th = T$ and $hT = T\}$ is an $\mathcal{A}$-subgroup of H.*

From now on let H be an elementary abelian p-group of rank 3 and let $\mathcal{A}$ be a p-S ring over H. We use an additive notation for H.

The following is a well-known result, see for example [HiMu] page 351.

Lemma 1 *If $T \in \mathrm{Bsets}(\mathcal{A})$ and $|T| = p^2$ then $\mathcal{A}$ is Schurian.*

Proof. It is easy to see that if $\mathcal{B}$ is a p-S ring over an elementary abelian group M of rank 2 then either $\mathrm{Bsets}(\mathcal{B}) = \{\{m\} \mid m \in M\}$ or there exists a subgroup L of order p in M such that $\mathrm{Bsets}(\mathcal{B}) = \{L + m \mid m \in M \backslash L\} \cup \{\{l\} \mid l \in L\}$.

Let $T \in \mathrm{Bsets}(\mathcal{A})$ such that $|T| = p^2$. Denote $\mathcal{O}^*(\mathcal{A})$ by R. Proposition 1(b) yields $p^2 = |T| \leq |T - T| \leq |R| \leq p^2$. Therefore, since $T - T \subseteq R$, we have $T - T = R$. This proves that T is a coset $R + t$ of R. Now, Proposition 2 yields that $R + t, \ldots, R + (p-1)t$ are $p - 1$ elements of $\mathrm{Bsets}(\mathcal{A})$. These elements are distinct because otherwise $|T|$ would be divisible by a proper divisor of $p - 1$. Further $\cup_{i=1}^{p-1}(R + it) = H \backslash R$.

This says that for every U in $\mathrm{Bsets}(\mathcal{A})$ either $U \subseteq R$ or U is a coset of R. In particular, $\{U \in \mathrm{Bsets}(\mathcal{A}) \mid U \subseteq R\}$ determines a p-S ring over R. Therefore, by the comment made in the first paragraph of this proof we have that either $\mathrm{Bsets}(\mathcal{A}) = \{\{r\} \mid r \in R\} \cup \{R + it \mid i = 1, \ldots, p-1\}$ or there exists a subgroup L of R of order p and $y \in R \backslash L$ such that $\mathrm{Bsets}(\mathcal{A}) = \{\{l\} \mid l \in L\} \cup \{L + iy \mid i = 1, \ldots, p-1\} \cup \{R + it \mid i = 1, \ldots, p-1\}$. We leave to the reader to check that in the latter case $\mathcal{A}$ is the transitivity module of a Sylow p-subgroup of $\mathrm{Sym}(H)$. In the former case, consider the affine permutation group $G = H \rtimes C_{\mathrm{GL}(H)}(R)$, where $C_{\mathrm{GL}(H)}(R)$ denotes the set of linear isomorphisms of H fixing pointwise R. The stabilizer of 0_H in G is $C_{\mathrm{GL}(H)}(R)$. The set of orbits of $C_{\mathrm{GL}(H)}(R)$ is exactly $\mathrm{Bsets}(\mathcal{A})$, therefore $\mathcal{A} = V(H, C_{\mathrm{GL}(H)}(R))$. □

We note that if $\mathcal{O}_*(\mathcal{A}) = H$ then $\mathcal{A}$ is Schurian, indeed $\mathcal{A} = V(H, 1_{\mathrm{Sym}(H)})$. So, from now on we may assume that $|T| \leq p$ for any $T \in \mathrm{Bsets}(\mathcal{A})$ and $\mathcal{O}_*(\mathcal{A}) \neq H$. We let K denote $\mathcal{O}_*(\mathcal{A})$.

Lemma 2 *If $|K| = p^2$ then $\mathcal{A}$ is Schurian.*

Proof. Let T be an element of $\mathrm{Bsets}(\mathcal{A})$ of size p. We have $|\mathrm{St}(T)| \leq |T| = p$. If $\mathrm{St}(T) = 0_H$ then, by Proposition 3, $\{T + x \mid x \in K\}$ would be a set of p^2 disjoint elements in $\mathrm{Bsets}(\mathcal{A})$ covering the whole of H, a contradiction. This and Proposition 4 prove that $\mathrm{St}(T) = L$ is a subgroup of K of order p and

$T = L + t$ for some $t \in H \backslash K$.

Let $x_1, \ldots, x_p$ be a transversal of L in K. By Proposition 2 and Proposition 3, we have that $L + jt + x_i$ lies in $\mathrm{Bsets}(\mathcal{A})$, for $i = 1, \ldots, p$ and $j = 1, \ldots, p-1$. This yields that $\mathrm{Bsets}(\mathcal{A}) = \{L+jt+x_i \mid i = 1, \ldots, p, j = 1, \ldots, p-1\} \cup \{\{k\} \mid k \in K\}$.

Let l be a generator of L and $\varphi \in \mathrm{GL}(H)$ be the isomorphism of H mapping t into $t+l$ and fixing pointwise K. Let G be the affine permutation group $H \rtimes \langle\varphi\rangle$. The set of orbits of $G_{0_H} = \langle\varphi\rangle$ is exactly $\mathrm{Bsets}(\mathcal{A})$. Therefore $\mathcal{A} = V(H, \langle\varphi\rangle)$. $\square$

From now on we may assume that K has order p.

Lemma 3 *If* $|\mathrm{St}(T)| = p$ *for any* $T \in \mathrm{Bsets}(\mathcal{A})$ *of size* p *then* $\mathcal{A}$ *is Schurian.*

Proof. Let T be in $\mathrm{Bsets}(\mathcal{A})$ and $|T| = p$. Since $\mathrm{St}(T)$ is an $\mathcal{A}$-subgroup of H we have that $\mathrm{St}(T) = K$. This proves that every element in $\mathrm{Bsets}(\mathcal{A})$ of size p is a coset of K. Therefore $\mathrm{Bsets}(\mathcal{A}) = \{\{k\} \mid k \in K\} \cup \{K + x \mid x \in H \backslash K\}$.

Let x, y, k be a basis of H such that $k \in K$. Let $\varphi_1, \varphi_2 \in \mathrm{GL}(H)$ such that $\varphi_1 : x \mapsto x + k, y \mapsto y, k \mapsto k$ and $\varphi_2 : x \mapsto x, y \mapsto y + k, k \mapsto k$. The orbits of the group $\langle\varphi_1, \varphi_2\rangle$ are the elements of $\mathrm{Bsets}(\mathcal{A})$. Therefore $\mathcal{A} = V(H, \langle\varphi_1, \varphi_2\rangle)$. $\square$

To prove Theorem 1 it remains to consider the case where there exists $T \in \mathrm{Bsets}(\mathcal{A})$ of size p such that $\mathrm{St}(T) = 0_H$.

Lemma 4 *If* $\mathrm{St}(T) = 0_H$ *for some* $T \in \mathrm{Bsets}(\mathcal{A})$ *of size* p *then* $\mathcal{A}$ *is Schurian.*

Proof. Let T be in $\mathrm{Bsets}(\mathcal{A})$ such that $\mathrm{St}(T) = 0_H$ and $|T| = p$. By Proposition 2 and 3, we have that $(i)T + k$ is an element of $\mathrm{Bsets}(\mathcal{A})$ of size p, for $1 \leq i \leq p-1$ and $k \in K$.

We now prove 7 claims from which the lemma (and so Theorem 1) follows.

Claim 4.1 *If* $(i_1)T + k_1 = (i_2)T + k_2$ *then* $i_1 = i_2$ *and* $k_1 = k_2$.

Assume $k_1 \neq k_2$. Since $\mathrm{St}((i_1)T) = 0_H$, we have $i_1 \neq i_2$. Set $i = i_2^{-1} i_1$, $k = k_1 - k_2$ and l the order of i in $\mathbb{F}_p^*$. We have $(i)T + i_2^{-1}k = T$. Consider the permutation $\varphi \in \mathrm{Sym}(T)$ defined by $t^\varphi = it + i_2^{-1}k$. If t lies in T then the $\langle\varphi\rangle$-orbit containing t, i.e. $\{t^{\varphi^i} \mid i \in \mathbb{Z}\}$, has exactly l elements, namely $t, it + i_2^{-1}k, i^2 t + i_2^{-1}(i+1)k, \ldots, i^{l-1}t + i_2^{-1}(i^{l-2} + \cdots + i + 1)k$. This proves that every $\langle\varphi\rangle$-orbit has size divisible by l, therefore l divides $|T| = p$, a contradiction. Thus $i_1 = i_2$ and $k_1 = k_2$. $\blacksquare$

Claim 4.2 $\mathrm{Bsets}(\mathcal{A}) = \{\{k\} \mid k \in K\} \cup \{K + ix \mid i = 1, \ldots, p-1\} \cup \{(i)T + k \mid i = 1, \ldots, p-1, k \in K\}$, *for some* $x \in H$.

Claim 4.1 says that the elements in $\{(i)T + k \mid i = 1, \ldots, p-1, k \in K\}$ cover $p^3 - p^2$ elements of H. Therefore, in Bsets($\mathcal{A}$) there is room only for other $p-1$ sets of size p, having necessarily stabilizer K. So, there exists $x \in H$ such that $K + x \in \mathrm{Bsets}(\mathcal{A})$. Thus, by Proposition 2, $K + ix \in \mathrm{Bsets}(\mathcal{A})$ for any $1 \leq i \leq p-1$. The claim is proved. ■

Note that $\cup_{i=0}^{p-1}(K + ix) = L$ is an $\mathcal{A}$-subgroup of H of order p^2.

Claim 4.3 *There exist t_1, t_2 in T and l in $L \backslash K$ such that $t_1 = t_2 + l$.*

The set $T+L$ cannot be the whole of H as $0 \notin T+L$. Therefore, $t_1+l_1 = t_2+l_2$ for some $t_1, t_2 \in T$, $l_1, l_2 \in L$ with $l_1 \neq l_2$. Hence $t_1 = t_2 + (l_2 - l_1)$. The element $l_2 - l_1$ cannot be in K otherwise we would have that $\mathrm{St}(T) = K$, a contradiction. So, $l_2 - l_1 \in L \backslash K$. ■

Claim 4.4 *For any $t \in T$ there exists a unique $f_t \in K$ such that $t+l+f_t \in T$.*

Since $\underline{T}$ and $\underline{K+l}$ lie in $\mathcal{A}$ and since $\mathcal{A}$, as vector space, is spanned by $\{\underline{U} \mid U \in \mathrm{Bsets}(\mathcal{A})\}$, we have $\underline{T} \cdot \underline{K+l} = \sum_U c_U \underline{U}$, where $\cdot$ denotes the product in the p-S ring $\mathcal{A}$.

By Claim 4.3, we have $c_T \geq 1$. Now, if $x_1 + (k_1 + l) = x_2 + (k_2 + l)$ for some $x_1, x_2 \in T$ and $k_1, k_2 \in K$ then $k_1 - k_2$ stabilizes T. Hence $k_1 = k_2$ and $x_1 = x_2$. This proves that $c_T = 1$. In particular, for any $t \in T$ there exists a unique $f_t \in K$ such that $t + f_t + l$ lies in T. ■

Fix a basis (e_1, e_2, e_3) of H such that $e_1 \in T$, $e_2 = l + f_{e_1}$ and $K = \langle e_3 \rangle$.

Claim 4.5 *$T = \{e_1 + ie_2 + f(i)e_3 \mid 0 \leq i \leq p-1\}$ for some function $f : \mathbb{F}_p \to \mathbb{F}_p$ such that $f(0) = 0$ and $f(1) = 0$.*

We prove that if $e_1 + ie_2 + f(i)e_3$ lies in T, for some $f(i) \in \mathbb{F}_p$, then there exists $f(i+1) \in \mathbb{F}_p$ such that $e_1 + (i+1)e_2 + f(i+1)e_3 \in T$. If $i = 0$ then, since $e_1 \in T$, we may take $f(0) = 0$. If $e_1 + ie_2 + f(i)e_3 \in T$ then, by Claim 4.4, there exists $ce_3 \in K$ such that $e_1 + ie_2 + f(i)e_3 + e_2 + ce_3 \in T$. In particular, define $f(i+1)$ as $f(i) + c$.

The set $\{e_1 + ie_2 + f(i)e_3 \mid i \in \mathbb{F}_p\}$ has size p and is contained in T, therefore it is T. Finally, by Claim 4.4, $e_1 + l + f_{e_1} = e_1 + e_2 \in T$, so $f(1) = 0$. ■

Claim 4.6 *For any $k \in \mathbb{F}_p \backslash \{0\}$ we have $\{f(i) - f(i-k) \mid i \in \mathbb{F}_p\} = \mathbb{F}_p$. In particular, we may assume $f(2) = 1$.*

Using the description of T given in Claim 4.5, it is easy to check that

$$\underline{T} \cdot \underline{(-1)T} = p\underline{0_H} + \sum_{k=1}^{p-1} \underline{K + ke_2}.$$

In particular, $\{(e_1+ie_2+f(i)e_3)-(e_1+(i-k)e_2+f(i-k)e_3) \mid i \in \mathbb{F}_p\} = K+ke_2$, for any $k \neq 0$. So, $\{f(i) - f(i-k) \mid i \in \mathbb{F}_p\} = \mathbb{F}_p$ for any $k \neq 0$.

Note that $f(2)$ cannot be 0, otherwise, since $f(0) = f(1) = 0$, we would have $\{f(i) - f(i-1) \mid i \in \mathbb{F}_p\} \subset \mathbb{F}_p$. Hence, without loss of generality, we may assume that $f(2) = 1$, indeed change the basis (e_1, e_2, e_3) in $(e_1, e_2, f(2)^{-1}e_3)$. ∎

Claim 4.7 $f(x) = (x^2 - x)/2$.

Obviously, p must be odd if Claim 4.6 holds. A function g such that $g(x+d)-g(x)$ is bijective for each $d \in \mathbb{F}_p^*$ is called a planar function. Gluck, Hiramine, Rónyai and Szönyi independently proved that any planar function over a finite field $\mathbb{F}_p$ with odd prime p is a quadratic polynomial (see [Gl], or Proposition 2 in [Hi], or Theorem 1 in [RoSz]).

Hence $f(x) = ax^2 + bx + c$, for some $a, b, c \in \mathbb{F}_p$. Using $f(0) = 0$, $f(1) = 0$ and $f(2) = 1$, we have $f(x) = (x^2 - x)/2$. ∎

Let $\varphi \in \mathrm{GL}(H)$ such that $\varphi : e_1 \mapsto e_1 + e_2, e_2 \mapsto e_2 + e_3, e_3 \mapsto e_3$. Using Claims 4.2, 4.5, 4.7, the reader can verify that the orbits of the group $\langle\varphi\rangle$ are the elements of Bsets($\mathcal{A}$). Therefore $\mathcal{A} = V(H, \langle\varphi\rangle)$. The proof of Lemma 4 and Theorem 1 is now complete. □

References

[Gl] D. Gluck, A note on permutation polynomials and finite geometry, *Discrete Mathematics* **80** (1990), 97–100.

[Hi] Y. Hiramine, A Conjecture on Affine Planes of Prime Order, *Journal of Combinatorial Theory*, Series A **52** (1989), 44–50.

[HiMu] M. Hirasaka, M. Muzychuk, An Elementary Abelian Group of rank 4 Is a CI-Group, *Journal of Combinatorial Theory*, Series A **94**, (2001), no. 2, 339–362.

[Mu] M. Muzychuk, An elementary abelian group of large rank is not a CI-Group, *Discrete Mathematics* **264** (2003), no. 1–3, 167–185.

[RoSz] L. Rónyai and T. Szönyi, Planar Functions over Finite Fields, *Combinatorica* **9** (1989), no. 3, 315–320.

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

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