S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 14, стр. 443–450 (2017) УДК 512.541
DOI 10.17377/semi.2017.14.037 MSC 20G43

Special issue: Graphs and Groups, Spectra and Symmetries — G2S2 2016

SCHUR RINGS OVER THE ELEMENTARY ABELIAN GROUP OF ORDER 64

S. REICHARD

Abstract. We report on the classification of S-rings over the group E_{64} up to scheme isomorphism. A total of 2082 schemes were found.

Keywords: commutative group, algebra.

1. Introduction

S-rings were introduced by I. Schur [9] in 1933 and further investigated by Wielandt [11]. In the beginning they were used for purely group theoretic investigations.

More recently they have played a prominent role in the area of Algebraic Graph Theory and in the isomorphism problem for certain classes of graphs and other combinatorial objects. Information on the set of all S-rings over a given group H helps in the solution of the isomorphism problem for Cayley graphs over H.

S-rings over all groups of order 63 have previously been classified [12]. The subject of this text is the classification of S-rings over the elementary group $\mathbb{Z}_2^6$ of order 64. From certain points of view, this is the most difficult group of this order.

2. Preliminaries

We follow the exposition in [5].

Let H be a finite multiplicative group with neutral element e. We consider the set $\mathbb{C}[H]$ of formal sums $\sum_{h\in H} a_h h$, $a_h \in \mathbb{C}$.

Reichard, S., Schur rings over the elementary abelian group of order 64.

Received September, 30, 2016, published May, 20, 2017.

On the set $\mathbb{C}[H]$ we have the following operations:

$$\left(\sum_{g\in H} a_g g\right) + \left(\sum_{h\in H} b_h h\right) = \sum_{h\in H}(a_h + b_h)h;$$

$$\left(\sum_{g\in H} a_g g\right) \circ \left(\sum_{h\in H} b_h h\right) = \sum_{h\in H}(a_h b_h)h \qquad \text{(point-wise multiplication);}$$

$$\left(\sum_{g\in H} a_g g\right) \cdot \left(\sum_{h\in H} b_h h\right) = \sum_{g\in H}\sum_{h\in H}(a_g b_h)(gh) \qquad \text{(ordinary multiplication).}$$

For $X \subseteq H$ we denote by $\underline{X}$ the sum of the elements of X. For a family of subsets $\mathcal{X} = \{X_i\}_{i\in I}$ let $\underline{\mathcal{X}} = \{\underline{X_i}\}_{i\in I}$.

By X^{-1} we denote the set $\{x^{-1}|x \in X\}$. Similarly we define inverses on $\mathbb{C}[H]$.

Then we have

- $(\mathbb{C}[H], +, \cdot)$ is a ring with identity $\underline{\{e\}}$.
- $(\mathbb{C}[H], +, \circ)$ is a ring with identity $\underline{H}$.

A subring $\mathcal{A}$ of $\mathbb{C}[H]$ is an S-ring or Schur ring, if the following holds:

- There is a partition $\mathcal{T}$ of H with $\underline{\{e\}} \in \mathcal{T}$ and $\mathcal{T}^{-1} = \mathcal{T}$ such that $\underline{\mathcal{T}}$ is a $\mathbb{C}$-basis of $\mathcal{A}$.

One can show the following:

Lemma 1. *A subspace $\mathcal{A}$ of $\mathbb{C}[H]$ is an S-ring if and only if*

- *$\mathcal{A}$ is a subring with identity $\underline{\{e\}}$ with respect to ordinary multiplication;*
- *$\mathcal{A}$ is a subring with identity $\underline{H}$ with respect to point-wise multiplication;*
- *$\mathcal{A}^{-1} = \mathcal{A}$.*

The basis $\underline{\mathcal{T}}$ consists of the primitive idempotents with respect to "$\circ$". In particular, $\underline{\mathcal{T}}$ (and hence $\mathcal{T}$) is uniquely determined. It is called the standard basis of $\mathcal{A}$.

Two S-rings $\mathcal{A}$ and $\mathcal{A}'$ over a group H are isomorphic ("Cayley-isomorphic") if there is an automorphism ϕ of H which maps $\mathcal{A}$ to $\mathcal{A}'$.

Association schemes [1] are relational systems defined on finite sets. Let Ω be a set, and $\mathcal{R} = \{R_0, \ldots, R_d\}$ a partition of Ω^2. Then $W = (\Omega, \mathcal{R})$ is an association scheme if the following axioms hold:

(1) $R_0 = Id_\Omega$, the diagonal relation.
(2) For each $R_i \in \mathcal{R}$, $R_i^{-1} = \{(y, x)|(x, y) \in R_i\} \in \mathcal{R}$.
(3) There are numbers p_{ij}^k such that for any $(x, y) \in R_k$,

$$|\{z \in \Omega|(x, z) \in R_i, (z, y) \in R_j\}| = p_{ij}^k.$$

Note that we do not require an association scheme to be *commutative* ($p_{ij}^k = p_{ji}^k$ for all i, j, k) or even *symmetrical* ($R_i^{-1} = R_i$ for all i). While these axioms were originally included, most authors now use this more general notion. Compare the investigation of non-commutative association schemes of rank six by Zieschang and Hanaki [4].

Given any transitive permutation group H on Ω, the set $\mathcal{R}$ of orbits of H on Ω^2 forms an association scheme. Any association scheme that arises in this way is called *schurian*.

For a binary relation R on Ω its adjacency matrix $A = A(R)$ is defined as follows: $A_{xy} = 1$ if $(x, y) \in R$, and $A_{xy} = 0$ otherwise. We consider this as a matrix over the complex numbers.

For the binary relations R_i, set $A_i = A(R_i)$. Then we get the following:

Lemma 2. *The relations R_i form an association scheme if and only if the A_i form the linear basis of a matrix algebra containing both identity matrix I and the all-one matrix J.*

The algebra $\langle A_i \rangle$ is the *adjacency algebra* (or Bose-Mesner algebra) of the association scheme.

Two association schemes $W = (\Omega, \{R_i\})$ and $W' = (\Omega', \{S_j\})$ are isomorphic, if there are bijections $\varphi : \Omega \to \Omega'$ and $\rho : \{R_i\} \to \{S_j\}$ such that whenever $(x, y) \in R_i$, then $(\varphi(x), \varphi(y)) \in \rho(R_i)$. An isomorphism (φ, ρ) of a scheme W to itself is called a *color automorphism* of W; it is a (proper) automorphism if ρ is the identity, i.e., each relation is mapped to itself.

An algebraic isomorphism between two schemes W and W' is an algebra isomorphism between the corresponding adjacency algebras. Such an isomorphism is uniquely determined by a bijection between the two standard bases.

The sets of proper, color, and algebraic automorphisms of a scheme W form groups which we will denote by $Aut(W)$, $CAut(W)$, and $AAut(W)$.

3. Previous results

S-rings over a given group H can be seen as mergings of the group ring $\mathbb{C}[H]$ or the corresponding coherent configurations $W = (\Omega, R)$. These mergings correspond to partitions of the point set of the configuration. A general algorithm for the enumeration of mergings of coherent configurations was described in [2]:

- Determine all subsets of Ω that can possibly form a part of such a partition ("good" subsets).
- Enumerate all partitions of Ω consisting only of good subsets.
- For each such partition check whether it yields a merging.

Different criteria have been suggested for subsets to be good. We call a subset *coherent* if it is in fact a basis set of some merging. In order to consider all relevant sets we require each coherent set to be good. On the other hand the test for goodness should be efficient and effective.

Usually small powers of a given set are computed, and it is checked that they do not split the set. In the language of S-rings this means that the powers of $\underline{T}$ be constant on T, i.e., for $g, h \in T$,

$$(\underline{T})^2(g) = (\underline{T})^2(h);$$
$$(\underline{T})^3(g) = (\underline{T})^3(h).$$

If the number of good sets is not large, all partitions can be enumerated and checked for coherence. However this fails for S-rings over most groups.

Several improvements have since been introduced. Since the coherence of a partition depends only on the structure constants of the configuration, this property is invariant under algebraic automorphisms. Hence we can use the group $AAut(W)$ for isomorph rejection [7]. An approach for the enumeration of non-isomorphic sets is described in [6].

Given any partition P of Ω we can efficiently compute the coarsest coherent refinement of P using the algorithm of Weisfeiler-Leman (WL-Stabilization, [10]). This reduces the number of sets that need to be considered, as well as the need to look at all possible partitions.

There have been several previous efforts to enumerate all S-rings over small groups: by Fiedler and Klin (up to order 31); by Pech and Reichard (up to order 47); and by Ziv-Av [12] (up to order 63). Ziv-Av stated: "For the groups of order 64 (especially for E_{64}) an innovative approach is necessary, as the current algorithms cannot finish the calculations in a reasonable time."

There are at least two explanations why the orders 32, 48 and 64 posed particular difficulties. For one, the number of different groups of these orders is particularly large. On the other hand these orders have many small prime factors. This leads to big search spaces, in particular in the case of products of elementary abelian groups E_{32}, $3 \times E_{16}$, E_{64}, where we have a great number of involutions.

For some groups the enumeration has first been performed using lots of computing power. However, better algorithms and implementations allowed to speed up the search. In the case of the alternating group A_5, the CPU time was reduced from one month via 20 hours [12] to 20 minutes.

4. An outline of the algorithm

The traditional approach to enumerating S-rings fails for the group E_{64}, since the orbits of good sets are too large to be fully expanded and kept in memory. We therefore introduced an intermediate step in which we enumerate compatible pairs of coherent sets up to isomorphism. Here two coherent sets are compatible if they appear together in a merging.

So we do the following:

(1) Enumerate good sets up to equivalence under $AAut(W)$, using only the condition on $(\underline{T})^2$.
(2) For each good set check if it is coherent using WL-Stabilization.
(3) For each coherent set T do the following:
   (a) Enumerate coherent sets U compatible with T, up to equivalence under the stabilizer of T in $AAut(W)$.
   (b) Find the orbits of compatible coherent sets under the stabilizer.
   (c) From these compatible sets, construct coherent partitions containing T.
(4) Perform an isomorphism test on the results.

Some remarks on the implementation:

- The group operation is implemented using bit-operations on integers.
- To check that a set T is good we have to verify that its square, i.e., the complex product $\underline{T} \cdot \underline{T}$ is constant on R. We build the set one element at a time. If $T \subseteq H$ and $i \in H \setminus T$, then
$$(\underline{T} + \underline{i})^2 = \underline{T}^2 + \underline{T} \cdot \underline{i} + \underline{i} \cdot \underline{T} + \underline{i}^2.$$
- Recall that the elements of the group ring are functions $H \to \mathbb{C}$. In fact, for elements of an S-ring the images are integers. We evaluate both sides of the previous equation at $k \in H$ and get
$$((\underline{T} + \underline{i})^2)(k) = (\underline{T}^2)(k) + \sum_{j \in T} p_{ji}^k + \sum_{j \in T} p_{ij}^k + p_{ii}^k.$$

- In the case of S-rings we have that $p_{ij}^k = \delta_{ij,k}$. So the equation above simplifies to
$$((\underline{T} + \underline{i})^2)(k) = (\underline{T}^2)(k) + \underline{T}(k^{-1}i) + \underline{T}(ik^{-1}) + \underline{k}(i^2).$$
- In practice, we go through the sets iT, Ti and $\{i^2\}$ and increment each corresponding component of the product.
- We see that each entry of the product changes by at most 2 in each step. This allows us to break off the search early if the differences of entries is too great with respect to the number of possible elements to be added to T. In general it is sufficient to consider only sets whose size is less than $|H|/2$.
- When constructing pairs of compatible sets starting from a set T, it is sufficient to consider sets U with $|U| \leq |T|$. In order for U to be compatible, it has to be a subset of a basic set of the smallest merging containing T.
- The enumeration was performed by programs written in C++ by the author. The final isomorphism check was performed in GAP [3].

5. Results

All computations were performed on a dual-core Intel i5 processor. The search for good sets ran on a single thread for one week. It found 100 non-isomorphic good sets of size at most 31. Of those, 61 are primitive; that is, they are not contained in a proper subgroup. This part was implemented in C++ under Linux.

The search for pairs of compatible sets was performed using a variation of the previous algorithm. Given one coherent set, we use Weisfeiler-Leman to find the coarsest coherent partition containing it. Any compatible set needs to be contained in a single class of that partition. The stabilizer of the given set was used for isomorph rejection. A total of 1242 pairs was found.

Finally the pairs were extended to coherent partitions, which led to some 300,000 mergings. The resulting mergings were tested for scheme isomorphisms. As noted before, two S-rings can be isomorphic as schemes, while not Cayley-isomorphic. In total, 2082 non-isomorphic schemes were found. Some information can be found in Table 1 on Page 448. The full data is available at [8].

Finally, the schemes were classified up to algebraic isomorphism. Here we find 1879 classes. Of those, 85 classes contain non-isomorphic schemes.

6. Evidence for correctness

As in any complex computer search there is the possibility of error in the algorithm, the implementation or - unlikely - the hardware. Ideally we would like to have independent confirmation of our result. However we performed two independent sanity checks which revealed no immediate inconsistencies.

As we worked in two stages, enumerating coherent sets first, followed by the construction of partitions, it is conceivable that sets which might have been missed in the first stage appear as part of the partitions in the second stage. No such new sets appeared, indicating that the first stage may be correct.

The second check depends on duality of S-rings over abelian groups. If H is such a group, then its characters are one-dimensional and form a group $\hat{H}$ isomorphic to H. Each character may be extended in a unique way to a ring homomorphism $\mathbb{C}[H] \to \mathbb{C}$.

Rank	Total	NS	P	NSP
2	1	-	1	-
3	20	10	15	10
4	57	30	23	18
5	74	27	5	3
6	106	29	1	-
7	112	25	-	-
8	142	20	1	-
9	151	27	1	-
10	151	16	-	-
11	130	17	-	-
12	160	14	-	-
13	113	10	-	-
14	133	9	-	-
15	117	10	-	-
16	130	10	-	-
17	70	2	-	-
18	105	4	-	-
19	47	3	-	-

Rank	Total	NS	P	NSP
20	70	2	-	-
21	32	3	-	-
22	53	3	-	-
23	9	1	-	-
24	36	1	-	-
25	6	-	-	-
26	14	-	-	-
27	4	1	-	-
28	18	-	-	-
30	3	-	-	-
32	5	-	-	-
33	2	-	-	-
34	2	-	-	-
36	4	-	-	-
40	3	-	-	-
48	1	-	-	-
64	1	-	-	-

TABLE 1. Numbers of all, non-schurian and primitive schemes of given rank

Let now be $\mathcal{A}$ an S-ring over H. Call two characters equivalent if they coincide on $\mathcal{A}$. Then the equivalence classes of characters form an S-ring $\hat{\mathcal{A}}$ over $\hat{H}$, the dual S-ring to $\mathcal{A}$. Due to the group isomorphism we get a ring isomorphic to the dual over the original group H.

Hence the full set of non-isomorphic S-rings over H should contain with each ring also its dual. We checked that our set of solutions has this property.

The two consistency checks described above give us some confidence in the correctness of our results.

7. Conclusion

All S-rings over the elementary abelian group of order 64 were determined up to scheme isomorphism, a group that had previously been considered as difficult. 2082 mergings were found, among them several primitive and non-schurian. A number of them can be explained on a theoretical level as certain products of smaller rings, however the majority is still unexplained.

It would be desirable to find all S-rings over these groups up to Cayley isomorphism, however this has not yet been fulfilled.

We were able to use the large automorphism group present in this problem to fulfill the task of enumeration of S-rings over the elementary abelian group. For most groups this symmetry group is considerably smaller, making it difficult even to consider other groups of order 64, let alone higher orders. Here one should probably make use of the inherent parallelism in the search for coherent subsets. Some ideas exist, however they will be saved for another article.

Rank	Subdegrees	Schurian	Group rank	Aut $/E_{64}$	$\lvert\,\mathrm{Aut}\,\rvert/64$
3	$1, 27, 36,$	$-$	5		1152
3	$1, 28, 35,$	$-$	8		96
3	$1, 28, 35,$	$+$		S_8	40320
3	$1, 28, 35,$	$-$	6	$C_2 \times A_5$	120
3	$1, 14, 49,$	$+$			50803200
3	$1, 18, 45,$	$+$		$(C_3.A_6) : C_2$	2160
3	$1, 28, 35,$	$-$	6		384
3	$1, 21, 42,$	$-$	4	$\mathrm{PSL}(3,2) : C_2$	336
3	$1, 27, 36,$	$-$	9	$C_2 \times A_4$	24
3	$1, 27, 36,$	$-$	6	$C_2 \times A_5$	120
3	$1, 27, 36,$	$+$		$O(5,3) : C_2$	51840
3	$1, 27, 36,$	$-$	7		160
3	$1, 28, 35,$	$-$	4	$(C_{14} \times C_2) : C_3$	84
3	$1, 28, 35,$	$-$	9	$C_2 \times A_4$	24
3	$1, 21, 42,$	$+$		$S_3 \times \mathrm{PSL}(3,2)$	1008
4	$1, 14, 21, 28,$	$-$	14	C_6	6
4	$1, 14, 21, 28,$	$-$	16	S_3	6
4	$1, 14, 21, 28,$	$-$	24	C_3	3
4	$1, 14, 21, 28,$	$-$	6	C_{14}	14
4	$1, 14, 21, 28,$	$-$	6	$C_7 : C_3$	21
4	$1, 14, 21, 28,$	$-$	12	A_4	12
4	$1, 14, 21, 28,$	$-$	12	A_4	12
4	$1, 18^2, 27,$	$-$	15	D_8	8
4	$1, 18^2, 27,$	$+$			216
4	$1, 21^3,$	$-$	24	C_3	3
4	$1, 9, 27^2,$	$+$			1296
4	$1, 21^3,$	$-$	10	C_7	7
4	$1, 18^2, 27,$	$-$	16	S_3	6
4	$1, 18^2, 27,$	$-$	14	C_6	6
4	$1, 14^2, 35,$	$-$	6	C_{14}	14
4	$1, 14, 21, 28,$	$-$	11	S_4	24
4	$1, 14, 21, 28,$	$-$	12	D_{16}	16
4	$1, 14, 21, 28,$	$+$		$\mathrm{PSL}(3,2) : C_2$	336
4	$1, 21^3,$	$-$	22	C_4	4
4	$1, 7, 21, 35,$	$+$		S_7	5040
4	$1, 21^3,$	$-$	24	C_3	3
4	$1, 21^3,$	$-$	22	C_4	4
4	$1, 21^3,$	$+$		$C_3 \times (C_7 : C_3)$	63
5	$1, 7, 14, 21^2,$	$+$		$(C_7 : C_3) : C_2$	42
5	$1, 14^3, 21,$	$-$	6	C_{14}	14
5	$1, 9^2, 18, 27,$	$+$			108
5	$1, 14^3, 21,$	$-$	10	C_7	7
5	$1, 14^3, 21,$	$-$	10	C_7	7
6	$1, 9^4, 27,$	$+$			54
8	$1, 9^7,$	$+$		D_{18}	18
9	$1, 7^7, 14,$	$+$		D_{14}	14

TABLE 2. Information on primitive schemes

References

[1] E. Bannai and T. Ito, *Algebraic Combinatorics I: Association schemes*, The Benjamin/Cummings Publishing Co., Inc., Menlo Park CA, 1984. Zbl 0555.05019

[2] I.A. Faradžev, M.H. Klin, and M.E. Muzichuk, *Cellular rings and groups of automorphisms of graphs*, In I.A. Faradzhev (ed.) et al. Investigations in algebraic theory of combinatorial objects, Math. Appl. (Soviet Ser.), **84**, Kluwer Acad. Publ., Dordrecht, 1994, 1–152. Zbl 0795.05073

[3] The GAP Group, *GAP — Groups, Algorithms, and Programming, Version 4.7.8*, 2015. `http://www.gap-system.org`

[4] A. Hanaki and P.-H. Zieschang, *On imprimitive noncommutative association schemes of order* 6, Commun. Algebra, **42**:3 (2014), 1151–1199. Zbl 1297.05262

[5] M. Muzychuk and I. Ponomarenko, *Schur rings*, Eur. J. Comb., **30**:6 (2009), 1526–1539. Zbl 1195.20003

[6] P. Christian and S. Reichard, *Enumerating set orbits*, In M. Klin (ed.) et al., Algorithmic Algebraic Combinatorics and Gröbner Bases, Springer, Dordrecht, 2009, 137–150. Zbl 1183.20001

[7] R.C. Read, *Every one a winner, or how to avoid isomorphism search when cataloguing combinatorial configurations*, Ann. Discrete Math., **2** (1978), 107–120. Zbl 0392.05001

[8] S. Reichard, *Schur rings over E_{64}*, 2016. `http://www.math.tu-dresden.de/~reichard/schur/e64/`

[9] I. Schur, *Zur Theorie der einfach transitiven Permutationsgruppen*, Sitzungsber. Preuss. Akad. Wiss., Phys.-Math. Kl., **1933**:18–20 (1933), 598–623, 1933. Zbl 0007.14903

[10] B. Weisfeiler (ed.), *On Construction and Identification of Graphs*. Lecture Notes in Mathematics, **558**, Springer-Verlag, Berlin–Heidelberg–New York, 1976. Zbl 0366.05019

[11] H. Wielandt, *Finite permutation groups*. Academic Press, New York–London, 1964. Zbl 0138.02501

[12] M. Ziv-Av, *Enumeration of Schur rings over small groups*, in V.P. Gerdt (ed.) et al., Computer Algebra in Scientific Computing: 16th Int. Workshop, CASC 2014, Warsaw, Poland, September 8-12, 2014. Proceedings, Lecture Notes in Computer Science, **8660** (2014), 491–500. Zbl 1353.05005

Sven Reichard
Institut für Algebra,
TU Dresden, Germany
E-mail address: `sven.reichard@tu-dresden.de`