2008-07-08

Rational Schur Rings over Abelian Groups

Brent L. Kerby
Brigham Young University - Provo

Rational Schur Rings over Abelian Groups

by

Brent Kerby

A thesis submitted to the faculty of

Brigham Young University

in partial fulfillment of the requirements for the degree of

Master of Science

Department of Mathematics

Brigham Young University

August 2008

BRIGHAM YOUNG UNIVERSITY

GRADUATE COMMITTEE APPROVAL

of a thesis submitted by

Brent Kerby

This thesis has been read by each member of the following graduate committee and by majority vote has been found to be satisfactory.

Date	Stephen Humphries, Chair
Date	Darrin Doud
Date	William E. Lang

BRIGHAM YOUNG UNIVERSITY

As chair of the candidate's graduate committee, I have read the thesis of Brent Kerby in its final form and have found that (1) its format, citations, and bibliographical style are consistent and acceptable and fulfill university and department style requirements; (2) its illustrative materials including figures, tables, and charts are in place; and (3) the final manuscript is satisfactory to the graduate committee and is ready for submission to the university library.

Date	Stephen Humphries Chair, Graduate Committee
Accepted for the Department	William E. Lang Graduate Coordinator
Accepted for the College	Thomas Sederberg, Associate Dean College of Physical and Mathematical Sciences

ABSTRACT

Rational Schur Rings over Abelian Groups

Brent Kerby

Department of Mathematics

Master of Science

In 1993, Muzychuk showed that the rational S-rings over a cyclic group Z_n are in one-to-one correspondence with sublattices of the divisor lattice of n, or equivalently, with sublattices of the lattice of subgroups of Z_n. This idea is easily extended to show that for any finite group G, sublattices of the lattice of characteristic subgroups of G give rise to rational S-rings over G in a natural way. Our main result is that any finite group may be represented as the automorphism group of such a rational S-ring over an abelian p-group. In order to show this, we first give a complete description of the automorphism classes and characteristic subgroups of finite abelian groups. We show that for a large class of abelian groups, including all those of odd order, the lattice of characteristic subgroups is distributive. We also prove a converse to the well-known result of Muzychuk that two S-rings over a cyclic group are isomorphic if and only if they coincide; namely, we show that over a group which is not cyclic, there always exist distinct isomorphic S-rings. Finally, we show that the automorphism group of any S-ring over a cyclic group is abelian.

ACKNOWLEDGMENTS

I would like to thank Darrin Doud for the use of his computer to carry out MAGMA computations, without which many results in this thesis would not have been discovered.

Contents

List of Tables

1 Basic definitions and elementary results

In this section, fix a commutative ring R with unity. Except where stated otherwise, all groups considered will be finite.

If G is a group, the group algebra of G with coefficients in R is denoted RG. If C is a subset of G, then we define $\overline{C} \in RG$ by $\overline{C} = \sum_{g \in C} g$, and call $\overline{C}$ a *simple quantity* of the group algebra RG. Given a subset $C \subseteq G$ and an integer m, we define $C^{(m)} = \{g^m : g \in C\}$. For any $x \in RG$, where $x = \sum_{g \in G} r_g g$, we define $x^{(m)} = \sum_{g \in G} r_g g^m$. Given a subset $X \subseteq RG$, we denote the R-submodule generated by X as RX, i.e.,

$$RX = \{\sum_{i=1}^{k} r_i x_i : k \in \mathbb{N}, r_i \in R, x_i \in X\}.$$

Definition 1.1. Let G be a finite group. An R-submodule S of the group algebra RG is called a *Schur ring* (or *S-ring*) over G if there are disjoint nonempty subsets $T_1, \ldots, T_n$ of G such that $S = R\{\overline{T}_1, \ldots, \overline{T}_n\}$ (i.e., $\overline{T}_1, \ldots, \overline{T}_n$ span S as an R-module), with the following properties,

(i) $\overline{T}_i \overline{T}_j \in S$ for all $i, j \in \{1, \ldots, n\}$.

(ii) For every i there is some j such that $T_i^{(-1)} = T_j$.

(iii) $T_1 = \{1\}$, and $G = T_1 \cup T_2 \cup \cdots \cup T_n$.

The sets $T_1, \ldots, T_n$ are called *basic sets* of S and are said to form a *Schur partition* of G. The corresponding $\overline{T}_1, \ldots, \overline{T}_n$ are called *basic quantities* of S. If S satisfies condition (i) and (ii) but perhaps not (iii) then S is called a *pseudo S-ring* (or *PS-ring*).

Note that condition (i) ensures that S is closed under multiplication, so that S is in fact a subalgebra of RG. It is easy to see that if S is a PS-ring, then the collection

of basic sets $T_1, \ldots, T_n$ (and corresponding basic quantities $\overline{T}_1, \ldots, \overline{T}_n$) is uniquely determined by S, so that there is no ambiguity in referring to them as *the* basic sets of S (and *the* basic quantities). Since $\overline{T}_1, \ldots, \overline{T}_n$ are clearly linearly independent, an S-ring is a free R-module; as such we may refer to the *rank* of an S-ring (or *dimension*, in case R is a field), which is simply the number of basic sets it possesses.

Example 1.2. Let $G = Z_6 = \langle t \rangle$ be the cyclic group of order 6 and let $S = R\{1, t^2, t^4, t + t^3 + t^5\}$. It is straightforward to check that S is an S-ring (of rank 4) over G. Its basic sets are $\{1\}$, $\{t^2\}$, $\{t^4\}$, and $\{t, t^3, t^5\}$. On the other hand, the R-module $M = R\{1, t + t^2, t^3 + t^4 + t^5\}$ is not an S-ring because it is not closed under multiplication, e.g., $t + t^2 \in M$ but $(t + t^2)^2 = t^2 + 2t^3 + t^4 \notin M$. Moreover, condition (ii) of an S-ring does not hold for M.

Example 1.3. Over any group G, the whole group algebra RG is an S-ring, with basic sets $\{g\}$, $g \in G$. The R-module $R\{1, \overline{G}\} = R\{1, \overline{G} - 1\}$ is also an S-ring, called the *trivial S-ring* over G, with basic sets $\{1\}$ and $G - \{1\}$.

We observe that the most tedious part of checking that a module $M = R\{\overline{T}_1, \overline{T}_2, \ldots, \overline{T}_n\}$ is an S-ring is verifying that M is closed under multiplication (condition (i)); in general one must check that $\overline{T}_i \overline{T}_j$ is in M for all basic quantities $\overline{T}_i, \overline{T}_j$. The following theorem simplifies this task slightly for small S-rings by showing that it is not necessary to check multiplication with the last basic quantity $\overline{T}_n$.

Theorem 1.4. *Let $T_1, \ldots, T_n$ be disjoint nonempty subsets of a group G satisfying conditions (ii) and (iii) of Definition 1.1, and let $S = R\{\overline{T}_1, \overline{T}_2, \ldots, \overline{T}_n\}$. If $\overline{T}_i \overline{T}_j \in S$ for all $i, j \in \{2, \ldots, n-1\}$, then S is an S-ring over G.*

Proof. We have $\overline{T}_1 \overline{T}_j = \overline{T}_j \overline{T}_1 = \overline{T}_j \in M$ for all j (since $\overline{T}_1 = 1$). And, since

$G = \cup_{j=1}^{n} T_i$, we have $\overline{T}_n = \overline{G} - \sum_{j=1}^{n-1} \overline{T}_j$. Thus for any $i \in \{1, \ldots, n-1\}$,

$$\begin{aligned}
\overline{T}_i \overline{T}_n &= \overline{T}_i (\overline{G} - \sum_{j=1}^{n-1} \overline{T}_j) \\
&= \overline{T}_i \overline{G} - \sum_{j=1}^{n-1} \overline{T}_i \overline{T}_j \\
&= |T_i| \overline{G} - \sum_{j=1}^{n-1} \overline{T}_i \overline{T}_j \in M,
\end{aligned}$$

since $\overline{G} = \sum_{j=1}^{n} \overline{T}_j \in M$ and by hypothesis each $\overline{T}_i \overline{T}_j \in M$ for $i, j \in \{1, \ldots, n-1\}$. Similarly $\overline{T}_n \overline{T}_i \in M$. Now it follows that $\overline{T}_n \overline{T}_n \in M$ by taking $i = n$ in the above argument. □

It is evident that, given a group G of order n, there are only finitely many S-rings over G, no more than the number of partitions of the non-identity elements of G. Enumerating the S-rings over a group in general appears to be a difficult problem. In the special case of cyclic groups Z_n, there is a classification which enables one to list all S-rings for small values of n; this classification is described below in §8. For large, highly-composite values of n, enumeration again becomes difficult because of the large number of S-rings (see Table 1). There is apparently no known classification for S-rings over noncyclic groups, even over, say, elementary abelian p-groups (see Question 8.6 and Example 8.5); for very small groups we are able to list all S-rings using a brute-force algorithm (see Table 2). This computation, and all other computer calculations referred to in this thesis, were carried out using MAGMA [3]; the code we used is given in §A.

In the case where R is a field, there is an alternative purely algebraic description of S-rings and PS-rings which avoids reference to the combinatorial notion of basic sets. This description, given below in Theorem 1.7 and Corollary 1.8, will be fundamental to the remainder of our discussion. In the rest of this section, F will denote an

Table 1: Number of S-rings over Z_n, $n < 192$, for coefficient ring R of characteristic 0

Z_2	1	Z_{40}	262	Z_{78}	284	Z_{116}	91	Z_{154}	360
Z_3	2	Z_{41}	8	Z_{79}	8	Z_{117}	291	Z_{155}	81
Z_4	3	Z_{42}	188	Z_{80}	1646	Z_{118}	13	Z_{156}	2157
Z_5	3	Z_{43}	8	Z_{81}	92	Z_{119}	69	Z_{157}	12
Z_6	7	Z_{44}	61	Z_{82}	25	Z_{120}	10130	Z_{158}	25
Z_7	4	Z_{45}	140	Z_{83}	4	Z_{121}	21	Z_{159}	41
Z_8	10	Z_{46}	13	Z_{84}	1397	Z_{122}	37	Z_{160}	11256
Z_9	7	Z_{47}	4	Z_{85}	60	Z_{123}	55	Z_{161}	53
Z_{10}	10	Z_{48}	1033	Z_{86}	25	Z_{124}	119	Z_{162}	1224
Z_{11}	4	Z_{49}	21	Z_{87}	41	Z_{125}	58	Z_{163}	10
Z_{12}	32	Z_{50}	79	Z_{88}	334	Z_{126}	2099	Z_{164}	121
Z_{13}	6	Z_{51}	35	Z_{89}	8	Z_{127}	12	Z_{165}	670
Z_{14}	13	Z_{52}	91	Z_{90}	1581	Z_{128}	2989	Z_{166}	13
Z_{15}	21	Z_{53}	6	Z_{91}	97	Z_{129}	53	Z_{167}	4
Z_{16}	37	Z_{54}	232	Z_{92}	61	Z_{130}	457	Z_{168}	12494
Z_{17}	5	Z_{55}	41	Z_{93}	53	Z_{131}	8	Z_{169}	43
Z_{18}	42	Z_{56}	334	Z_{94}	13	Z_{132}	1397	Z_{170}	411
Z_{19}	6	Z_{57}	40	Z_{95}	61	Z_{133}	99	Z_{171}	283
Z_{20}	47	Z_{58}	19	Z_{96}	6719	Z_{134}	25	Z_{172}	119
Z_{21}	27	Z_{59}	4	Z_{97}	12	Z_{135}	854	Z_{173}	6
Z_{22}	13	Z_{60}	1103	Z_{98}	128	Z_{136}	442	Z_{174}	284
Z_{23}	4	Z_{61}	12	Z_{99}	177	Z_{137}	8	Z_{175}	363
Z_{24}	172	Z_{62}	25	Z_{100}	563	Z_{138}	188	Z_{176}	2030
Z_{25}	13	Z_{63}	187	Z_{101}	9	Z_{139}	8	Z_{177}	27
Z_{26}	19	Z_{64}	657	Z_{102}	243	Z_{140}	2142	Z_{178}	25
Z_{27}	25	Z_{65}	67	Z_{103}	8	Z_{141}	27	Z_{179}	4
Z_{28}	61	Z_{66}	188	Z_{104}	514	Z_{142}	25	Z_{180}	17888
Z_{29}	6	Z_{67}	8	Z_{105}	670	Z_{143}	81	Z_{181}	18
Z_{30}	147	Z_{68}	77	Z_{106}	19	Z_{144}	21451	Z_{182}	658
Z_{31}	8	Z_{69}	27	Z_{107}	4	Z_{145}	67	Z_{183}	81
Z_{32}	151	Z_{70}	281	Z_{108}	2219	Z_{146}	37	Z_{184}	334
Z_{33}	27	Z_{71}	8	Z_{109}	12	Z_{147}	289	Z_{185}	100
Z_{34}	16	Z_{72}	2311	Z_{110}	281	Z_{148}	135	Z_{186}	366
Z_{35}	41	Z_{73}	12	Z_{111}	61	Z_{149}	6	Z_{187}	69
Z_{36}	284	Z_{74}	28	Z_{112}	2030	Z_{150}	2124	Z_{188}	61
Z_{37}	9	Z_{75}	185	Z_{113}	10	Z_{151}	12	Z_{189}	1225
Z_{38}	19	Z_{76}	90	Z_{114}	277	Z_{152}	496	Z_{190}	415
Z_{39}	41	Z_{77}	53	Z_{115}	41	Z_{153}	238	Z_{191}	8

Table 2: Number of S-rings over non-cyclic groups of order ≤ 20 for coefficient ring R of characteristic 0

$Z_2 \times Z_2$	5
S_3	10
$Z_2 \times Z_2 \times Z_2$	100
$Z_2 \times Z_4$	28
D_8	34
Q_8	26
$Z_3 \times Z_3$	40
D_{10}	25
$Z_2 \times Z_6$	76
D_{12}	120
A_4	52

$Z_3 \rtimes Z_4$	54
D_{14}	55
$Z_2 \times Z_2 \times Z_2 \times Z_2$	12537
$Z_2 \times Z_2 \times Z_4$	1121
$Z_2 \times Z_8$	163
$Z_4 \times Z_4$	537
D_{16}	247
$Z_8 \overset{3}{\rtimes} Z_2$	287
$Z_8 \overset{5}{\rtimes} Z_2$	205
$Z_4 \rtimes Z_4$	401
$K_4 \rtimes Z_4$	649

$Q_8 \rtimes Z_2$	607
Q_{16}	271
$Z_2 \times D_8$	1557
$Z_2 \times Q_8$	797
$Z_3 \times Z_6$	297
D_{18}	122
$S_3 \times Z_3$	233
$(Z_3 \times Z_3) \wr S_2$	1004
$Z_2 \times Z_{10}$	109
D_{20}	313
$Z_5 \overset{-1}{\rtimes} Z_4$	139
AGL(1,5)	154

arbitrary field.

Definition 1.5. Given $x, y \in FG$, where $x = \sum_{g \in G} a_g g, y = \sum_{g \in G} b_g g$, the *Hadamard product* is defined by

$$x \circ y = \sum_{g \in G} a_g b_g g.$$

We will use $x^{\circ n} = x \circ x \circ \cdots \circ x$ to denote the n-fold Hadamard product of x with itself.

Any element $x \in FG$ may be uniquely written in the form $x = a_1 \overline{C}_1 + \cdots + a_n \overline{C}_n$, where $C_1, \ldots, C_n$ are disjoint nonempty subsets of G and the coefficients $a_1, \ldots, a_n$ are distinct and non-zero. We will call this the *standard decomposition* of x. It is easy to verify that if $x \in S$, where S is an S-ring over G, then also $\overline{C}_1, \ldots, \overline{C}_n \in S$. The following lemma is a variation of this result which we will need in a moment.

Lemma 1.6. *Let V be a subspace of FG closed under $\circ$, and let $x = a_1 \overline{C}_1 + \cdots + a_n \overline{C}_n$ be the standard decomposition of an element $x \in V$. Then $\overline{C}_1, \ldots, \overline{C}_n \in V$.*

Proof. Since V is closed under the Hadamard product, the elements $x^{\circ i} = a_1^i \overline{C}_1 +$

$\cdots + a_n^i \overline{C}_n$ are in V for all integers $i \geq 1$. Consider the matrix

$$A = \begin{pmatrix} a_1 & a_1^2 & \dots & a_1^n \\ a_2 & a_2^2 & \dots & a_2^n \\ \dots & \dots & \dots & \dots \\ a_n & a_n^2 & \dots & a_n^n \end{pmatrix}.$$

We have

$$\det A = \left(\prod_{i=1}^{n} a_i \right) \det \begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ \dots & \dots & \dots & \dots & \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{pmatrix}.$$

Each a_i is nonzero, so $\prod_{i=1}^n a_i \neq 0$. The determinant of the Vandermonde matrix on the right is $\prod_{i>j}(a_i - a_j)$, which is also non-zero since $a_1, \dots, a_n$ are distinct. It follows that A is invertible, so that any standard basis vector $\mathbf{e}_i$ may be written as a linear combination of the columns $\mathbf{a}_1, \dots, \mathbf{a}_n$ of A, say $\mathbf{e}_i = b_1\mathbf{a}_1 + b_2\mathbf{a}_2 + \cdots + b_n\mathbf{a}_n$. Now define a vector space isomorphism $\phi : \mathbb{Q}^n \to \text{Span}\{\overline{C}_1, \dots, \overline{C}_n\}$ by $\phi(\mathbf{e}_i) = \overline{C}_i$. Then

$$\phi(\mathbf{a}_i) = \phi(a_1^i\mathbf{e}_1 + \cdots + a_n^i\mathbf{e}_n) = a_1^i\overline{C}_1 + \cdots + a_n^i\overline{C}_n = x^{\circ i},$$

so that ϕ maps $\mathbf{a}_i$ to $x^{\circ i}$. Then, applying ϕ to the equation $\mathbf{e}_i = b_1\mathbf{a}_1 + b_2\mathbf{a}_2 + \cdots + b_n\mathbf{a}_n$ yields $\overline{C}_i = b_1 x + b_2 x^{\circ 2} + \cdots + b_n x^{\circ n} \in V$, as desired. □

Versions of the following theorem and corollary may be found in [15, Proposition 3.1] and [16, Lemma 1.3] with simple proofs. We give a more elementary proof which does not depend on any results about semisimple algebras.

Theorem 1.7. *Let A be a subalgebra of FG. Then A is an PS-ring if and only if A is closed under $\circ$ and $^{(-1)}$.*

Proof. First assume A is a PS-ring. Given any two basic quantities $\overline{T}_i$, $\overline{T}_j$ of A, the

disjointness of basic sets implies $\overline{T}_i \circ \overline{T}_j = 0$ unless $i = j$, in which case $\overline{T}_i \circ \overline{T}_j = \overline{T}_i \circ \overline{T}_i = \overline{T}_i$, so in either case we have $\overline{T}_i \circ \overline{T}_j \in A$. Since any element of A may be written as a linear combination of basic quantities, this implies A is closed under $\circ$. Given any basic quantity $\overline{T}_i$, we have $\overline{T}_i^{(-1)} = \overline{T_i^{(-1)}} = \overline{T}_j \in A$ for some j. From the linearity of $^{(-1)}$, it follows that A is closed under $^{(-1)}$.

Now assume A is closed under $*$, $\circ$, and $^{(-1)}$. Define a subset $C \subseteq G$ to be a *A-set* if $\overline{C} \in A$, and call a nonempty A-set C a *minimal A-set* if no proper nonempty subset $D \subset C$ is an A-set. Let $T_1, \ldots, T_n$ be the minimal A-sets of A. We claim that A is an S-ring with basic sets $T_1, \ldots, T_n$.

First we must show that $T_1, \ldots, T_n$ are disjoint. Suppose $T_i \cap T_j \neq \emptyset$ for some $i \neq j$. Then since A is closed under $\circ$ we have $\overline{T_i \cap T_j} = \overline{T}_i \circ \overline{T}_j \in A$, so that $T_i \cap T_j$ is an A-set. But since $T_i \cap T_j$ is a proper subset of T_i this contradicts the minimality of T_i.

Now we must show that $\{\overline{T}_1, \ldots, \overline{T}_n\}$ is a basis for A as a vector space (so that condition (i) of a PS-ring is satisfied). So, letting V be the vector space spanned by $\overline{T}_1, \ldots, \overline{T}_n$, given any $x \in A$, we want to show $x \in V$. First consider the case that x is a basic quantity, so that $x = \overline{C}$ for some $C \subseteq G$. If there is such an x which is not in V, choose x with $|C|$ minimal. But then C is an A-set, so there is a minimal A-set T_i contained in C. But then we have $x - \overline{T}_i = \overline{C \setminus T_i} \notin V$, contradicting the minimality of $|C|$. So $x \in V$ if x is a basic quantity. Now, given an arbitrary $x \in A$, let $x = a_1\overline{C}_1 + \cdots + a_n\overline{C}_n$ be the standard decomposition of x. By Lemma 1.6 we have $\overline{C}_1, \ldots, \overline{C}_n \in A$, hence $\overline{C}_1, \ldots, \overline{C}_n \in V$, from which it immediately follows that $x \in V$. Thus $\overline{T}_1, \ldots, \overline{T}_n$ span A.

To prove condition (ii) we must show that for every i there is some j such that $T_i^{(-1)} = T_j$. Since A is closed under $^{(-1)}$, we have that $\overline{T_i^{(-1)}} = \overline{T}_i^{(-1)} \in A$, so that $T_i^{(-1)}$ is an A-set. If $T_i^{(-1)}$ is not a minimal A-set, then there is a proper nonempty subset $D \subset T_i^{(-1)}$ which is an A-set. Again since A is closed under inverses, we have

$\overline{D^{(-1)}} = \overline{D}^{(-1)} \in A$, so $D^{(-1)}$ is an A-set. But since $D^{(-1)}$ is a proper nonempty subset of T_i, this contradicts the minimality of T_i. Hence $T_i^{(-1)}$ is a minimal A-set, so $T_i^{(-1)} = T_j$ for some j. This proves that A is an S-ring. □

Corollary 1.8. *Let A be a subalgebra of FG. Then A is an S-ring if and only if A is closed under the operations $\circ$ and $^{(-1)}$ and contains 1 and $\overline{G}$.*

Proof. Assume first that A is an S-ring with basic sets $T_1, \ldots, T_n$. Then A contains $\overline{T}_1 = 1$ and $\sum_{i=1}^n \overline{T}_i = \overline{\cup_{i=1}^n T_i} = \overline{G}$. A is closed under $\circ$ and $^{(-1)}$ by Theorem 1.7.

Conversely, assume A contains 1 and $\overline{G}$ and is closed under $\circ$ and $^{(-1)}$. By the theorem, A is a PS-ring; let $T_1, \ldots, T_n$ be its basic sets. Since $1 \in A$, $\{1\}$ is an A-set, and, considering that it has no nonempty proper subsets, $\{1\}$ is a minimal A-set, so $\{1\} = T_i$ for some i ; without loss of generality, $T_1 = \{1\}$. Since $\overline{G} \in A$, we have $\overline{G} = \sum_{i=1}^n a_i \overline{T}_i$ for some $a_1, \ldots, a_n \in \mathbb{Q}$; so every element $g \in G$ must be contained in some T_i, otherwise the coefficient of g in $\overline{G}$ and $\sum_{i=1}^n a_i \overline{T}_i$ would not agree. Thus $\cup_{i=1}^n T_i = G$. This proves that condition (iii) holds for A. □

The notion of a minimal A-set introduced in the proof of Theorem 1.7 will be useful to us again later on; for reference, we state here a fact which was proven above:

Theorem 1.9. *Let S be a PS-ring. Then the minimal S-sets are precisely the basic sets of S.*

The following example shows that the above theorem and corollary are false if F is replaced by a ring R which is not a field.

Example 1.10. Let R be a ring which is not a field, and let $r \in R$ be a nonzero element which is not invertible. Let $G = Z_3 = \langle t \rangle$. Then $A = R\{1, t + t^2, r \cdot t\}$ is a subalgebra of RG which is closed under $\circ$ and $^{(-1)}$ and contains 1 and $\overline{G}$ but A is not a PS-ring.

It is natural to ask whether the choice of coefficient ring R will make any essential difference at all; namely, given a group G, is it possible for a partition of G to be a Schur partition with respect to one coefficient ring but not to another. The following example shows that this is indeed possible:

Example 1.11. Let $G = Z_8 = \langle t \rangle$. Then $\{1\}, \{t^2 + t^6\}, \{t + t^3 + t^4 + t^5 + t^7\}$ is a Schur partition of G with respect to the coefficient ring $\mathbb{F}_2$ but not with respect to $\mathbb{Z}$ or $\mathbb{Q}$. For, considering $S = F_2\{1, t^2 + t^6, t + t^3 + t^4 + t^5 + t^7\}$, we have

$$(t^2 + t^6)^2 = 2 + 2t^4 = 0 \in S,$$

so S is an S-ring by Theorem 1.4. On the other hand, $S' = \mathbb{Q}\{1, t^2 + t^6, t + t^3 + t^4 + t^5 + t^7\}$ is not an S-ring since $2 + 2t^4 \notin S'$.

However, the only property of R which makes a difference in this regard is its characteristic, as the following shows:

Theorem 1.12. *Let $T_1, \ldots, T_r$ be a partition of a group G. Let R_1 and R_2 be commutative rings with unity of characteristic m and n respectively. If n divides m and $T_1, \ldots, T_r$ is a Schur partition with respect to the coefficient ring R_1 then $T_1, \ldots, T_r$ is also a Schur partition with respect to R_2. In particular, if R_1 and R_2 have the same characteristic, then $T_1, \ldots, T_r$ is a Schur partition with respect to R_1 if and only if it is a Schur partition with respect to R_2.*

Proof. Let $S_1 = R_1\{\overline{T}_1, \ldots, \overline{T}_r\}$ and $S_2 = R_2\{\overline{T}_1, \ldots, \overline{T}_r\}$. (In the first equation, the $\overline{T}_1, \ldots, \overline{T}_r$ are to be taken as elements of R_1G while in the second equation, they are taken as elements of R_2G. This slight ambiguity of notation should not lead to confusion.) To show that S_2 is an S-ring, we only need to show that $\overline{T}_i\overline{T}_j \in S_2$ for all $i, j \in \{1, \ldots, r\}$. Since S_1 is an S-ring, in R_1G we may write $\overline{T}_i\overline{T}_j = \sum_{k=1}^{r} \lambda_{ijk}\overline{T}_k$ for some $\lambda_{ijk} \in R_1$. In fact, it is clear that the coefficients λ_{ijk} lie in the subring

of R_1 generated by 1, namely $\lambda_{ijk} \in \mathbb{Z}/m\mathbb{Z}$. Since n divides m, there is a natural homomorphism $\pi : Z/m\mathbb{Z} \to Z/n\mathbb{Z}$, and π extends to an algebra homomorphism from $(Z/m\mathbb{Z})G$ to $(Z/n\mathbb{Z})G$. Under this map, we have $\pi(\overline{T}_i) = \overline{T}_i$ for all i, so that in R_2G,

$$\overline{T}_1\overline{T}_2 = \pi(\overline{T}_1\overline{T}_2) = \pi(\sum_{k=1}^{n} \lambda_{ijk}\overline{T}_k) = \sum_{k=1}^{r} \pi(\lambda_{ijk})\overline{T}_k,$$

which proves S_2 is an S-ring. □

The following shows that in one sense we do not lose any generality by restricting R to be a field, or even a prime field (i.e., $\mathbb{F}_p$ or $\mathbb{Q}$):

Theorem 1.13. *If $\{T_1, \ldots, T_n\}$ is a Schur partition of a group G with respect to a coefficient ring R, then there is a prime field F with respect to which $\{T_1, \ldots, T_n\}$ is also a Schur partition.*

Proof. Let m be the characteristic of R. Then take n to be any prime dividing m and apply Theorem 1.12 with $R_2 = \mathbb{F}_n$. □

However, given a group G and coefficient ring R, there is not necessarily a field F such that the set of Schur partitions of G is precisely the same with respect to R and F, as the following example shows:

Example 1.14. Let $G = Z_{12}$. By computer, we find that with respect to $\mathbb{Z}/4\mathbb{Z}$ there are 34 Schur partitions of G. With respect to $\mathbb{F}_2$ and $\mathbb{F}_3$ there are 62 and 37 respectively. With respect to any other prime field (i.e., $\mathbb{Q}$, $\mathbb{F}_5$, $\mathbb{F}_7$, etc.) there are 32 Schur partitions of G. A specific example of a partition which is a Schur partition over $\mathbb{Z}/4\mathbb{Z}$ but over no prime field except $\mathbb{F}_2$ is

$$\{1\}, \{t^2, t^4, t^8, t^{10}\}, \{t, t^3, t^5, t^6, t^7, t^9, t^{11}\},$$

while, on the other hand, there are many Schur partitions over $\mathbb{F}_2$ which are not Schur

partitions over $\mathbb{Z}/4\mathbb{Z}$, for instance,

$$\{1\}, \{t^3, t^9\}, \{t, t^2, t^4, t^5, t^6, t^7, t^8, t^{10}, t^{11}\}.$$

2 Central and rational S-rings

From now on, fix F to be any field.

Definition 2.1. A PS-ring S over a group G is *central* if $S \subseteq Z(FG)$, i.e., S is contained in the center of the group algebra.

Remark. It is not difficult to check that this is equivalent to requiring that every basic set T_i be a union of conjugacy classes of G. See, for instance, [17, 12.2.19] or [7, p. 861].

Of course, over an abelian group every S-ring is central. We will primarily be interested in a special class of central S-rings known as rational S-rings:

Definition 2.2. A PS-ring S over a group G is *rational* if for every $x \in S$ and $\phi \in \mathrm{Aut}(G)$, we have $\phi(x) = x$.

Remark. It is likewise not difficult to check that this is equivalent to requiring that every basic set T_i be a union of automorphism classes of G, where the *automorphism classes* of G are the orbits of $\mathrm{Aut}(G)$ acting on G in the natural way.

For us, the most important use of Theorem 1.7 and its corollary is that it leads to the construction of many interesting central and rational S-rings:

Theorem 2.3. *Let G be any finite group, and let $\mathcal{L}$ be any sublattice of the lattice of normal subgroups of G. Then the vector space $F(\mathcal{L}) = F\{\overline{H} : H \in \mathcal{L}\}$ is a central PS-ring over G with the following properties, for all $H, K \in \mathcal{L}$:*

(i) $\overline{H}^{(-1)} = \overline{H}$

(ii) $\overline{H} \circ \overline{K} = \overline{H \cap K}$

(iii) $\overline{H}\ \overline{K} = |H \cap K|\overline{HK}$

(iv) $F(\mathcal{L})$ *is an S-ring if and only if* $1, G \in \mathcal{L}$.

(v) $F(\mathcal{L})$ *is rational if and only if* $\mathcal{L}$ *consists entirely of characteristic subgroups.*

Proof. (i) is clear since H, as a subgroup, is closed under inverses. (ii) is immediate from the definition of the Hadamard product. (iii) is clear since, by elementary group theory, every element of HK can be written in $|H \cap K|$ ways as a product of an element in H with an element in K. Now, since the subgroups H and K are normal, HK is also a subgroup of G; since $\mathcal{L}$ is a lattice, we have $H \cap K, HK \in \mathcal{L}$. Thus, (i)–(iii) show that $F(\mathcal{L})$ is closed under $^{(-1)}$, multiplication, and the Hadamard product, so by Theorem 1.7, $F(\mathcal{L})$ is a PS-ring. Since each subgroup H is normal, we have $g\overline{H}g^{-1} = \overline{gHg^{-1}} = \overline{H}$ for all $g \in G$ and $H \in \mathcal{L}$, so that $\overline{H} \in Z(FG)$. It follows that $F(\mathcal{L})$ is a central PS-ring.

Now, if $1, G \in \mathcal{L}$ then $1, \overline{G} \in F(\mathcal{L})$, so by Corollary 1.8, $F(\mathcal{L})$ is an S-ring. Suppose, conversely, that $F(\mathcal{L})$ is an S-ring. Let $L = \bigcap_{H \in \mathcal{L}} H$, so that $L \in \mathcal{L}$. If $|L| > 1$, then since $L \subseteq H$ for every basis element $\overline{H}$ of $F(\mathcal{L})$, it follows that every element of $S(\mathcal{L})$ with a non-zero coefficient of $1 \in G$ also has other non-zero coefficients (namely, the other elements of L have non-zero coefficients), so that $1 \notin F(\mathcal{L})$, contrary (by Corollary 1.8) to the assumption that $F(\mathcal{L})$ is an S-ring. So we must have $L = 1$, hence $1 \in \mathcal{L}$, as desired. Now define $M = \prod_{H \in \mathcal{L}} H$. If $M \neq G$, then since $H \subseteq M$ for every basis element $\overline{H}$ of $F(\mathcal{L})$, it follows that the nonzero coefficients of every element $x \in F(\mathcal{L})$ are contained in M, so that $\overline{G} \notin F(\mathcal{L})$, again contradicting (by Corollary 1.8) that $F(\mathcal{L})$ is an S-ring. So $G \in \mathcal{L}$ as desired.

Finally, $F(\mathcal{L})$ is rational if and only if $\phi(\overline{H}) = \overline{H}$ for every $\phi \in \mathrm{Aut}(G)$ and each basis element $\overline{H}$ of $F(\mathcal{L})$; this holds if and only if $\phi(H) = H$ for each $H \in \mathcal{L}$, i.e. if and only if each $H \in \mathcal{L}$ is characteristic. □

If G is a cyclic group, then every subgroup of G is characteristic; consequently, the construction of Theorem 2.3 only produces rational S-rings. In this context, we may state the main theorem of [15]:

Theorem 2.4. (Muzychuk) *Every rational S-ring over a finite cyclic group may be constructed as in Theorem 2.3.*

We will soon see that there are rational S-rings over abelian groups which cannot be constructed as in Theorem 2.3 (see Example 5.8). However, there are other types of groups for which Theorem 2.3 produces the complete set of rational S-rings; Theorem 2.6 below gives one example. Before proving it, we need an elementary lemma (a version of which may be found in [20, Proposition 23.6]):

Lemma 2.5. *Let S be an S-ring over a group G, and let $D_1, \ldots, D_k$ be S-sets, i.e., assume $\overline{D}_i \in S$ for all i. Then $\overline{\langle D_1, \ldots, D_k \rangle} \in S$.*

Proof. Since $D = D_1 \cup \cdots \cup D_k$ is also an S-set and $\langle D_1, \ldots, D_k \rangle = \langle D \rangle$, it is sufficient to prove that $\overline{\langle D \rangle} \in S$. Now, for a sufficiently large choice of n, every element of $\langle D \rangle$ is a product of no more than n elements of D, hence every element of $\langle D \rangle$ has nonzero coefficient in $\overline{D}^n$. Let $\overline{D}^n = \sum_{i=1}^r a_i \overline{C}_i$ be the standard decomposition of $\overline{D}^n$, so that $C_1, \ldots, C_r$ form a partition of $\langle D \rangle$. By Lemma 1.6, each $\overline{C}_i \in S$, hence $\overline{\langle D \rangle} = \sum_{i=1}^r \overline{C}_i \in S$. □

Theorem 2.6. *Every rational S-ring over a finite dihedral group may be constructed as in Theorem 2.3.*

Proof. Suppose S is a rational S-ring over the dihedral group $G = \langle r, s \mid s^2 = r^n = (sr)^2 = 1 \}$. Let $T_1, \ldots, T_r$ be the basic sets of S, where $T_1 = \{1\}$. Note that all the reflections of G are automorphic (since the map determined by $s \mapsto rs$ and $r \mapsto r$ is an automorphism, although it is only inner if n is odd). Thus all the reflections of G lie in a single basic set, say T_2. So the remaining basic sets $T_3, \ldots, T_r$ all lie in $Z_n = \langle r \rangle$. If

we let Z_d be the subgroup generated by $T_3, \ldots, T_r$, then it follows by Lemma 2.5 that $\overline{Z}_d \in S$. Thus $S' = F\{1, \overline{T}_3, \ldots, \overline{T}_r\}$ is an S-ring over Z_d. By Theorem 2.4, $S' = F(\mathcal{L})$ for some sublattice $\mathcal{L}$ of the lattice of subgroups of Z_d. We claim $S = F(\mathcal{L} \cup \{G\})$. Clearly $\mathcal{L} \cup \{G\}$ is a sublattice of the lattice of characteristic subgroups of G. For $i \neq 2$, we have $\overline{T}_i \in S' = F(\mathcal{L}) \subseteq F(\mathcal{L} \cup \{G\})$, while $\overline{T}_2 = \overline{G} - \overline{Z}_d \in F(\mathcal{L} \cup \{G\})$, hence $S \subseteq F(\mathcal{L} \cup \{G\})$. Since $F(\mathcal{L}) = S' \subseteq S$ and $\overline{G} \in S$, we also have the reverse inclusion $F(\mathcal{L} \cup \{G\}) \subseteq S$. □

3 Isomorphisms and Automorphisms of S-rings

Definition 3.1. Let S_1 and S_2 be S-rings over groups G_1 and G_2 respectively. An algebra isomorphism $\phi : S_1 \to S_2$ is called an *S-ring isomorphism* if ϕ maps basic quantities to basic quantities, i.e., if for every basic set C of S_1 there is some basic set D of S_2 such that $\phi(\overline{C}) = \overline{D}$.

Example 3.2. Let $G_1 = Z_6 = \langle t \rangle$ and let G_2 be the symmetric group of degree 3. Let $S_1 = R\{1, t^2, t^4, t + t^3 + t^5\}$ and $S_2 = R\{1, (123), (132), (12) + (13) + (23)\}$. It is straightforward to verify that the R-module map $\phi : S_1 \to S_2$ determined by

$$\begin{aligned} 1 &\mapsto 1, \\ t^2 &\mapsto (123), \\ t^4 &\mapsto (132), \\ t + t^3 + t^5 &\mapsto (12) + (13) + (23), \end{aligned}$$

is an S-ring isomorphism. Thus it is possible for S-rings over nonisomorphic groups to be isomorphic.

Example 3.3. Let $G = Z_6 = \langle t \rangle$. The S-rings $\mathbb{C}\{1, t + t^2 + t^4 + t^5, t^3\}$ and $\mathbb{C}\{1, t + t^3 + t^5, t^2 + t^4\}$ are isomorphic as $\mathbb{C}$-algebras, since by Wedderburn's Theorem both

are isomorphic to $\mathbb{C}^3$, but they are not isomorphic as S-rings, since, e.g., the former has a basic quantity t^3 whose square is 1 while the latter does not.

The following theorem gives a purely algebraic characterization of S-ring isomorphisms.

Theorem 3.4. *Let S_1 and S_2 be S-rings over groups G_1 and G_2 respectively. Then an F-algebra isomorphism $\phi : S_1 \to S_2$ is an S-ring isomorphism if and only if ϕ respects the Hadamard product, i.e., if and only if $\phi(x \circ y) = \phi(x) \circ \phi(y)$ for all $x, y \in S_1$.*

Proof. First assume ϕ is an S-ring isomorphism. Let $T_1, \ldots, T_n$ be the basic sets of S_1 and let $U_1, \ldots, U_n$ be the basic sets of S_2. Relabeling the $U_1, \ldots, U_n$ if necessary, we may assume $\phi(\overline{T}_i) = \overline{U}_i$. For any $i, j \in \{1, \ldots, n\}$, if $i \neq j$ we have

$$\phi(\overline{T}_i \circ \overline{T}_j) = \phi(0) = 0 = \overline{U}_i \circ \overline{U}_j = \phi(\overline{T}_i) \circ \phi(\overline{T}_j),$$

while if $i = j$, we have

$$\phi(\overline{T}_i \circ \overline{T}_i) = \phi(\overline{T}_i) = \overline{U}_i = \overline{U}_i \circ \overline{U}_i = \phi(\overline{T}_i) \circ \phi(\overline{T}_i),$$

so in either case $\phi(\overline{T}_i \circ \overline{T}_j) = \phi(\overline{T}_i) \circ \phi(\overline{T}_j)$, proving that ϕ respects the Hadamard product.

Suppose conversely that ϕ respects the Hadamard product. If T is any basic set of S_1, then we have $\phi(\overline{T}) = \phi(\overline{T} \circ \overline{T}) = \phi(\overline{T}) \circ \phi(\overline{T})$. If we write $\phi(\overline{T}) = \sum_{g \in G_2} a_g g$, then the equation $\phi(\overline{T}) = \phi(\overline{T}) \circ \phi(\overline{T})$ gives $a_g = a_g^2$ for all $g \in G_2$. So each coefficient a_g is either 0 or 1, i.e. $\phi(\overline{T})$ is a nonzero simple quantity $\overline{U}$, for some $U \subseteq G_2$. We wish to show that $\phi(\overline{T})$ is a basic quantity. By Theorem 1.9 this is equivalent to showing that U is a minimal S_2-set. So suppose there is a nonempty proper subset $D \subset U$ with $\overline{D} \in S_2$. We may write $\phi(\overline{T}) = \overline{D} + \overline{U - D}$, hence $\overline{T} = \phi^{-1}(\overline{D}) + \phi^{-1}(\overline{U - D})$. Since ϕ^{-1}, together with ϕ, respects the Hadamard product and hence maps simple

quantities to simple quantities, we have expressed the basic quantity $\overline{T}$ as the sum of two nonzero simple quantities, which is impossible. Hence $\phi(\overline{T})$ is a basic quantity, so ϕ maps basic quantities to basic quantities, i.e. ϕ is an S-ring isomorphism. $\square$

An isomorphism from an S-ring onto itself is called an *automorphism*. The set of automorphisms of an S-ring S clearly forms a group, which we denote $\mathrm{Aut}(S)$.

Example 3.5. Let $G = Z_7 = \langle t \rangle$. Then $S = F\{1, t + t^6, t^2 + t^5, t^3 + t^4\}$ is an S-ring with $\mathrm{Aut}(S) \cong Z_3$. A generator for $\mathrm{Aut}(S)$ is determined by

$$\begin{aligned} 1 &\mapsto 1, \\ t + t^6 &\mapsto t^2 + t^5, \\ t^2 + t^5 &\mapsto t^3 + t^4, \\ t^3 + t^4 &\mapsto t + t^6. \end{aligned}$$

A natural question arises: Which groups can occur as the automorphism group of an S-ring? If we take S to be the full group ring FG, then it is easy to see that $\mathrm{Aut}(S) \cong \mathrm{Aut}(G)$. Thus, any group which may be represented as the automorphism group of a group may also be represented as the automorphism group of an S-ring (in a rather trivial way). However, Example 3.5 shows that Z_3 may also be represented as the automorphism group of a S-ring, whereas it is known that Z_3 cannot be represented as the automorphism group of any group (see Theorem 3.6 below). Our main result (Theorem 6.1) is that *any* finite group may be represented as the automorphism group of an S-ring, even of an S-ring of a rather restricted type, namely a rational S-ring over an abelian p-group; so, in particular, any finite group may be represented as the automorphism group of a commutative S-ring. Theorem 8.7 shows that a similar result cannot be obtained by considering only S-rings over cyclic groups.

Theorem 3.6. *Let n be an odd integer, $n \geq 3$. Then there is no group G (finite or infinite) with* $\mathrm{Aut}(G) \cong Z_n$.

Proof. Suppose G is a group with $\mathrm{Aut}(G) \cong Z_n$. Then $\mathrm{Inn}(G) \cong G/Z(G)$ is isomorphic to a subgroup of Z_n, hence is cyclic, which implies G is abelian. Now the map $\phi : G \to G$ given by $\phi(g) = g^{-1}$ is an automorphism of G. Since $\mathrm{Aut}(G)$ does not have an element of order 2, ϕ must be trivial. So G has exponent 2. It follows that G is the direct sum of a cardinal number α copies of Z_2 [17, 5.1.9]. If $\alpha \geq 2$, then there would be an automorphism of G of order 2 which interchanges the first two components of G. Thus $\alpha \leq 1$, i.e. $G = Z_2$ or $G = 1$, but in both these cases $\mathrm{Aut}(G)$ is trivial. □

For further information on the types of groups which occur as automorphism groups of groups, see [19].

The task of determining $\mathrm{Aut}(S)$ is often made easier by the following theorem, which shows that S-ring isomorphisms map basic sets to basic sets of the *same size*.

Theorem 3.7. *Let S_1 and S_2 be isomorphic S-rings over groups G_1 and G_2 respectively, and let $\phi : S_1 \to S_2$ be an isomorphism. Then $\phi(\overline{G}_1) = \overline{G}_2$, and if $C \subseteq G_1$ is any S_1-set, then $\phi(\overline{C}) = \overline{D}$ for some subset $D \subseteq G_2$, and we will write $\phi(C) = D$. Moreover, $|C| = |D|$. In particular, $|G_1| = |G_2|$.*

Proof. Let $T_1, \ldots, T_n$ and $U_1, \ldots, U_n$ be the basic sets of S_1 and S_2 respectively. Then, for some permutation $\sigma \in \mathrm{Sym}_n$, we have

$$\phi(\overline{G}_1) = \phi(\sum_{i=1}^{n} \overline{T}_i) = \sum_{i=1}^{n} \phi(\overline{T}_i) = \sum_{i=1}^{n} \overline{U}_{\sigma(i)} = \overline{G}_2.$$

Now, since any simple quantity $\overline{C}$ may be written as a sum of distinct basic quantities, and ϕ maps distinct basic quantities to distinct basic quantities, it follows that $\phi(\overline{C})$ is a sum of distinct basic quantities, i.e., $\phi(\overline{C})$ is a simple quantity $\overline{D}$.

Further, we have on the one hand,

$$\phi(\overline{C}\ \overline{G}_1) = \phi(\overline{C})\phi(\overline{G}_1) = \overline{D}\ \overline{G}_2 = |D|\overline{G}_2,$$

while on the other hand,

$$\phi(\overline{C}\ \overline{G}_1) = \phi(|C|\overline{G}_1) = |C|\phi(\overline{G}_1) = |C|\overline{G}_2,$$

hence $|C| = |D|$. □

If S is an S-ring over G, then every automorphism $\phi \in \mathrm{Aut}(G)$ induces an injective F-algebra homomorphism $\phi : S \to FG$ by defining $\phi(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g \phi(g)$. It is entirely straightforward to check that $\phi(S)$ is an S-ring with basic sets $\phi(T_1), \ldots, \phi(T_n)$ if $T_1, \ldots, T_n$ are the basic sets of S. Thus $\phi : S \to \phi(S)$ is in fact an S-ring isomorphism. We call such an isomorphism a *strong isomorphism* of S-rings. A strong isomorphism from an S-ring S onto itself is called a *strong automorphism*. We denote the set of all strong automorphisms of S by $\mathrm{Aut}^*(S)$. In Example 3.5 the generating automorphism of $\mathrm{Aut}(S)$ was in fact a strong automorphism, induced by the automorphism $\phi : t \mapsto t^2$ of G , so in this case $\mathrm{Aut}(S) = \mathrm{Aut}^*(S)$. The following example shows that the automorphism group and strong automorphism group of an S-ring do not generally coincide, even over cyclic groups.

Example 3.8. Let $G = Z_9 = \langle t \rangle$. Then $S = F\{1, t^3, t^6, t + t^4 + t^7, t^2 + t^5 + t^8\}$ is an S-ring with $\mathrm{Aut}(S) \cong Z_2 \times Z_2$ but $\mathrm{Aut}^*(S) \cong Z_2$.

Clearly, if S_1 and S_2 are isomorphic S-rings, then their automorphism groups are isomorphic. On the other hand, the following example shows that this is not the case for their strong automorphism groups.

Example 3.9. Let $G = Z_2 \times Z_4 = \langle a \rangle \times \langle b \rangle$, and let $S_1 = F\{1, a, b^2, ab^2, b+b^3, ab+ab^3\}$

and $S_2 = F\{1, a, b^2, ab^2, b+ab^3, ab+b^3\}$. Then $S_1 \cong S_2$ but $\mathrm{Aut}^*(S_1) \cong Z_2 \times Z_2$ while $\mathrm{Aut}^*(S_2) \cong Z_2$.

Example 3.10. Over the same group, let $S_1 = F\{1, b^2, a+b+ab+ab^2+b^3+ab^3\}$ and $S_2 = F\{1, a, b+ab+b^2+ab^2+b+ab^3\}$. Then $S_1 \cong S_2$ in spite of the fact that S_1 is a rational S-ring while S_2 is not.

The preceding examples show that in one sense, S-ring isomorphism is a fairly weak condition, as it fails to preserve many of the properties that we ordinarily think of as being associated with an S-ring.

A remarkable theorem of Muzychuk states:

Theorem 3.11 ([16])**.** *Two S-rings over a cyclic group Z_n are isomorphic if and only if they are identical.*

Below we will prove a converse to this result, but first we need the following lemma:

Lemma 3.12. *Let G be a finite group which is not cyclic. Then G has a subgroup which is not characteristic.*

Proof. By way of contradiction, suppose every subgroup of G is characteristic. Then in particular every subgroup of G is normal. If G is non-abelian, then G is a Hamiltonian group (i.e., a nonabelian group in which every subgroup is normal) and we may write $G = Q \times A$ where Q is an 8-element quaternion group $\langle i, j\rangle$ and A is abelian [17, 9.7.4]. But in this case $\langle i\rangle$ is a subgroup of G which is not characteristic, since there is an automorphism of Q mapping $\langle i\rangle$ to $\langle j\rangle$ and this automorphism extends to an automorphism of G. Therefore G must be abelian.

Since G is not cyclic, some Sylow p-subgroup of G is not cyclic and, by the Fundamental Theorem of finitely-generated abelian groups, we may write $G = \langle t\rangle \times \langle s\rangle \times A$ where $|t| = p^a$ and $|s| = p^b$ for some a and b where $1 \leq a \leq b$. Then $\langle s\rangle$ is not

characteristic, since an automorphism ϕ is determined by setting $\phi(s) = ts$, $\phi(t) = t$, and $\phi(a) = a$ for all $a \in A$. □

We remark that, by a similar method of proof, Lemma 3.12 may be extended to infinite non-abelian groups and to finitely generated abelian groups. However, there are non-cyclic infinitely generated abelian groups in which every subgroup is characteristic, an example being the direct sum $\sum_{p \text{ prime}} Z_p$.

Theorem 3.13. *Let G be a group which is not cyclic. Then there exist distinct strongly isomorphic S-rings S_1 and S_2 over G.*

Proof. By Lemma 3.12, let H be a subgroup of G which is not characteristic. Choose some $\phi \in \mathrm{Aut}(G)$ such that $\phi(H) \neq H$. Then $S_1 = F\{1, \overline{H}, \overline{G}\}$ and $S_2 = F\{1, \overline{\phi(H)}, \overline{G}\}$ are S-rings over G which are strongly isomorphic. We only need to verify that they are distinct. The basic quantities of S_1 are $\{1, \overline{H} - 1, \overline{G} - \overline{H}\}$ while the basic quantities of S_2 are $\{1, \overline{\phi(H)} - 1, \overline{G} - \overline{\phi(H)}\}$. If $S_1 = S_2$ then the basic quantities of the two S-rings must be the same (in some order), so either $\overline{H} - 1 = \overline{\phi(H)} - 1$ or $\overline{H} - 1 = \overline{G} - \overline{\phi(H)}$. The former is impossible since $H \neq \phi(H)$. The latter would imply $G = H \cup \phi(H)$, which is impossible, since no group is the union of two proper subgroups. □

4 Automorphism Classes of Abelian Groups

In this and the following section, we give a complete description of the automorphism classes and characteristic subgroups of finite abelian groups. This topic was considered already in 1934 by Baer for the more general case of periodic abelian groups, and some of the results below were obtained in one form or another in [1]. Our method, however, differs greatly from that of [1]. We recently discovered that this topic was considered even earlier in 1905 by G. A. Miller [13] (see also [14, pp. 109-112]) and that Miller's treatment is similar to that which we developed below. Miller, however,

did not always offer proofs of his claims, and this led him to an incorrect description of the characteristic subgroups of abelian 2-groups in [13, p. 23, "there are as many additional C's which correspond to the conjugates of such a t as there are combinations of k things taken $2, 3, \ldots, k$ at a time"]. A correct version (necessarily more complicated) of the formula described by Miller is given in Theorems 5.16 and 5.20 below.

It is well known that any finite abelian group G may be written as the direct product of its Sylow subgroups:

$$G = G_{p_1} \times G_{p_2} \times \cdots \times G_{p_n}.$$

Since the Sylow subgroups of an abelian group are characteristic, it follows that every automorphism $\phi \in \mathrm{Aut}(G)$ may be written

$$\phi = \phi_1 \times \phi_2 \times \cdots \times \phi_n, \text{ where } \phi_i \in \mathrm{Aut}(G_{p_i}).$$

From this it follows that the automorphism classes of G are precisely the sets

$$O_1 \times O_2 \times \cdots \times O_n, \text{ where } O_i \text{ is an automorphism class of } G_{p_i},$$

while the characteristic subgroups of G are

$$H_1 \times H_2 \times \cdots \times H_n, \text{ where } H_i \text{ is a characteristic subgroup of } G_{p_i}.$$

Using these facts, the problem of determining the automorphism classes and characteristic subgroups of G is completely reduced to the case in which G is a p-group. So for the remainder of this section and the next we will assume G is a p-group.

Up to isomorphism, we may write

$$G = Z_{p^{\lambda_1}} \times Z_{p^{\lambda_2}} \times \cdots \times Z_{p^{\lambda_n}},$$

where $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. We define $\lambda(G)$ to be the tuple $(\lambda_1, \ldots, \lambda_n)$. As we will be working extensively with such tuples of integers, it will be convenient to introduce some notation for dealing with them:

Definition 4.1. Given tuples $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$ with integer entries, define

$$\begin{aligned}
&\mathbf{a} \leq \mathbf{b} \text{ if } a_i \leq b_i \text{ for all } i \in \{1, \ldots, n\} \\
&\mathbf{a} \wedge \mathbf{b} = (\min\{a_1, b_1\}, \min\{a_2, b_2\}, \ldots, \min\{a_n, b_n\}) \\
&\mathbf{a} \vee \mathbf{b} = (\max\{a_1, b_1\}, \max\{a_2, b_2\}, \ldots, \max\{a_n, b_n\})
\end{aligned}$$

Define $\Lambda(G)$ to be the set of tuples

$$\Lambda(G) = \{\mathbf{a} : \mathbf{0} \leq \mathbf{a} \leq \lambda(G)\}.$$

It is evident that $\Lambda(G)$, under the partial order $\leq$, forms a finite lattice in which $\wedge$ and $\vee$ are the greatest lower bound and least upper bound operators respectively.

Given a tuple $\mathbf{a} \in \Lambda(G)$, we define $T(\mathbf{a})$ to be the set of elements $g \in G$ for which the ith component of g has order p^{a_i}:

$$T(\mathbf{a}) = \{(g_1, g_2, \ldots, g_n) \in G : |g_i| = p^{a_i} \text{ for all } i = 1, \ldots, n\}.$$

Note that the sets $T(\mathbf{a})$ partition the group G. If $g \in T(\mathbf{a})$, we say that $T(\mathbf{a})$ is the *type* of g.

Before proceeding further, we need a couple of elementary lemmas:

Lemma 4.2. *In a finite cyclic p-group H, if two elements h_1 and h_2 have the same order then h_1 and h_2 are automorphic, i.e., there is an automorphism $\phi \in \mathrm{Aut}(H)$ such that $\phi(h_1) = h_2$.*

Remark. This result immediately extends to all finite cyclic groups, but we will not need this.

Proof. Write $H = Z_{p^m} = \langle t \rangle$. Then we may write $h_1 = t^{ap^i}$ for some integers a and i where a is relatively prime to p and $i = m - |h_1|$. It is clear then that defining $\phi_1 : H \to H$ by $\phi_1(t) = t^a$ determines an automorphism of H with $\phi_1(t^{p^i}) = t^{ap^i} = t^{h_1}$. Similarly, there is an automorphism ϕ_2 with $\phi_2(t^{p^i}) = t^{h_2}$. Then $\phi_2 \circ \phi_1^{-1}$ is an automorphism mapping h_1 to h_2. □

Lemma 4.3. *If $g, h \in G$ have the same type $T(\mathbf{a})$, then g and h are automorphic.*

Proof. Write $g = (g_1, \ldots, g_n)$ and $h = (h_1, \ldots, h_n)$. Since g and h have the same type, we have $|g_i| = |h_i|$ for each $i \in \{1, \ldots, n\}$. So by Lemma 4.2, there are automorphisms $\phi_i \in \mathrm{Aut}(Z_{p^{\lambda_i}})$ with $\phi_i(g_i) = h_i$. Then $\phi = \phi_1 \times \phi_2 \times \cdots \times \phi_n$ is an automorphism of G with $\phi(g) = h$. □

Note that Lemma 4.3 is equivalent to saying that each automorphism class of G is a union of types. From this it follows that given two types $T(\mathbf{a})$ and $T(\mathbf{b})$, if some element of $T(\mathbf{a})$ is automorphic to some element of $T(\mathbf{b})$, then all elements of $T(\mathbf{a})$ are automorphic to all elements of $T(\mathbf{b})$, and we will say in this case that $T(\mathbf{a})$ and $T(\mathbf{b})$ are *automorphic*.

Definition 4.4. Given a type $T(\mathbf{a})$, the automorphism class of G containing $T(\mathbf{a})$ is denoted $O(\mathbf{a})$.

Definition 4.5. A type $T(\mathbf{a})$ is *canonical* if for all $i \in \{1, \ldots, n-1\}$,

(i) $a_i \leq a_{i+1}$ and

(ii) $a_{i+1} - a_i \leq \lambda_{i+1} - \lambda_i$.

This says that $a_1, \ldots, a_n$ is a (weakly) increasing sequence but that at each step it increases by "not too much", namely, by no more than the difference between the corresponding λ's. In this case we will also say that the tuple $\mathbf{a}$ itself is canonical. The set of canonical tuples will be denoted $\mathcal{C}(G)$.

For what follows, it will be helpful to introduce some additional notation. Let $t_1, t_2, \ldots, t_n$ be generators for the respective cyclic factors in $G = Z_{p^{\lambda_1}} \times Z_{p^{\lambda_2}} \times \cdots \times Z_{p^{\lambda_n}}$. Also, for $0 \leq a \leq \lambda_i$, define $t_{i,a} = t_i^{p^{\lambda_i - a}}$, so that $t_{i,a}$ is an element of order p^a in $\langle t_i \rangle$, with $t_{i,\lambda_i} = t_i$.

The definition of "canonical" is justified by the following theorem.

Theorem 4.6. *Every type is automorphic to a unique canonical type. Moreover, every canonical type is the maximum type in its automorphism class, i.e., if a type $T(\mathbf{a})$ is canonical then $\mathbf{a}$ is the maximum element of $\{\mathbf{b} : T(\mathbf{b}) \subseteq O(\mathbf{a})\}$.*

Before proving this, we will need the following lemma.

Lemma 4.7. *Let $T(\mathbf{a})$ be a noncanonical type, and let $i \in \{1, \ldots, n-1\}$ be such that either $a_i > a_{i+1}$ or $a_{i+1} - a_i > \lambda_{i+1} - \lambda_i$. (Such an i exists by the definition of noncanonical). In the former case, define $\mathbf{a}'$ by $a'_j = a_j$ for all $j \neq i+1$ and $a'_{i+1} = a_i$; in the latter case, define $\mathbf{a}'$ by $a'_j = a_j$ for all $j \neq i$ and $a'_i = a_{i+1} - (\lambda_{i+1} - \lambda_i)$. Then in either case, $T(\mathbf{a}')$ is automorphic to $T(\mathbf{a})$.*

Remark. In other words, if a type is noncanonical because there are two consecutive entries a_i and a_{i+1} with a decrease from a_i to a_{i+1}, then we may increase a_{i+1} to match a_i, and the resulting type will be automorphic to the original (and will be "closer" to being canonical, since it no longer has this decrease). Likewise, if a type is noncanonical because there are two consecutive entries a_i and a_{i+1} with a difference which is too large, then we may increase a_i just enough to make the difference not

too large (namely, to make the difference precisely $\lambda_{i+1} - \lambda_i$), and again the resulting type will be automorphic to the original.

Proof. One element of type $T(\mathbf{a})$ is $g = \prod_{j=1}^{n} t_{j,a_j}$, so it is enough to show that there is an automorphism ϕ with $\phi(g) \in T(\mathbf{a}')$.

First consider the case $a_{i+1} < a_i$. Define a homomorphism $\phi : G \to G$ by setting $\phi(t_i) = t_i t_{i+1,\lambda_i}$ and $\phi(t_j) = t_j$ for all $j \neq i$. This is well-defined since $|\phi(t_j)|$ divides $|t_j|$ for all j, because in fact equality holds: For $j \neq i$ this is trivial, while for $j = i$ we have

$$|\phi(t_i)| = |t_i t_{i+1,\lambda_i}| = \operatorname{lcm}(|t_i|, |t_{i+1,\lambda_i}|) = \operatorname{lcm}(p^{\lambda_i}, p^{\lambda_i}) = p^{\lambda_i} = |t_i|.$$

The image of ϕ contains each generator t_j where $j \neq i$, and since $\phi(t_i t_{i+1,\lambda_i}^{-1}) = t_i$, the image of ϕ also contains t_i. Thus ϕ is onto, which, since G is finite, implies ϕ is an automorphism. Now,

$$\phi(t_{i,a_i}) = \phi(t_i)^{p^{\lambda_i - a_i}} = (t_i t_{i+1,\lambda_i})^{p^{\lambda_i - a_i}} = t_{i,a_i} t_{i+1,a_i},$$

hence

$$\phi(g) = t_{i+1,a_i} \prod_{j=1}^{n} t_{j,a_j} = t_{i+1,a_{i+1}} t_{i+1,a_i} \prod_{j \neq i} t_{j,a_j}.$$

Since $|t_{i+1,a_{i+1}}| = p^{a_{i+1}}$ and $|t_{i+1,a_i}| = p^{a_i}$ and $a_{i+1} < a_i$, it follows that $|t_{i+1,a_{i+1}} t_{i+1,a_i}| = p^{a_i}$, so that $\phi(g)$ has type $\mathbf{a}'$, as desired.

Now consider the case $a_{i+1} - a_i > \lambda_{i+1} - \lambda_i$. In this case, define $\mathbf{a}'$ by $a'_j = a_j$ for all $j \neq i$ and $a'_i = a_{i+1} - (\lambda_{i+1} - \lambda_i)$, so that $\mathbf{a}' > \mathbf{a}$. Now define ϕ by $\phi(t_{i+1}) = t_i t_{i+1}$ and $\phi(t_j) = t_j$ for $j \neq i$. Again, this is well-defined since

$$|\phi(t_{i+1})| = |t_i t_{i+1}| = \operatorname{lcm}(|t_i|, |t_{i+1}|) = \operatorname{lcm}(p^{\lambda_i}, p^{\lambda_{i+1}}) = p^{\lambda_{i+1}} = |t_{i+1}|.$$

Since ϕ is clearly surjective, it is an automorphism of G. We have

$$\phi(t_{i+1,a_{i+1}}) = \phi(t_{i+1})^{p^{\lambda_{i+1}-a_{i+1}}} = (t_i t_{i+1})^{p^{\lambda_{i+1}-a_{i+1}}} = t_{i,a_{i+1}-(\lambda_{i+1}-\lambda_i)} t_{i+1,a_{i+1}},$$

hence

$$\phi(g) = t_{i,a_{i+1}-(\lambda_{i+1}-\lambda_i)} \prod_{j=1}^{n} t_{j,a_j} = t_{i,a_{i+1}-(\lambda_{i+1}-\lambda_i)} t_{i,a_i} \prod_{j\neq i} t_{j,a_j}.$$

Since $a_{i+1}-(\lambda_{i+1}-\lambda_i) > a_i$ it follows that $|t_{i,a_{i+1}-(\lambda_{i+1}-\lambda_i)} t_{i,a_i}| = p^{a_{i+1}-(\lambda_{i+1}-\lambda_i)} = p^{a'_{i+1}}$, so that $\phi(g)$ has type $\mathbf{a}'$, as desired. □

Proof of Theorem 4.6. Let $T(\mathbf{a})$ be a type which is non-canonical. Lemma 4.7 implies that $T(\mathbf{a})$ is automorphic to another type $T(\mathbf{a}')$ where $\mathbf{a}' > \mathbf{a}$. If $\mathbf{a}'$ is non-canonical, then we may again apply Lemma 4.7 to obtain another automorphic type $T(\mathbf{a}'')$ where $\mathbf{a}'' > \mathbf{a}'$. This process may be continued but must eventually terminate since there are no infinite increasing sequences in Λ. Hence $T(\mathbf{a})$ is automorphic to a canonical type $T(\mathbf{b})$. Since $\mathbf{b} \geq \mathbf{a}$, this also shows that $\mathbf{b}$ is the maximum type in its automorphism class, assuming the uniqueness of $\mathbf{b}$ which we now prove.

So let $\mathbf{a}$ and $\mathbf{a}'$ be distinct canonical types. We will show that $T(\mathbf{a})$ is not automorphic to $T(\mathbf{a}')$. Let $g = \prod_{j=1}^{n} t_{j,a_j}$ and $g' = \prod_{j=1}^{n} t_{j,a'_j}$, so g and g' are elements of type $\mathbf{a}$ and $\mathbf{a}'$ respectively. Let i be the least positive integer such that $a_i \neq a'_i$. Without loss of generality, assume $a_i < a'_i$. Consider the elements $h = g^{p^{a_i}}$ and $h' = (g')^{p^{a_i}}$. Let $\mathbf{b}$ and $\mathbf{b}'$ be the types of h and h' respectively. By condition (i) of $\mathbf{a}$ being canonical, we have $a_j \leq a_i$ for all $j < i$, hence $b_j = 0$ for all $j \leq i$, while $b'_j = 0$ for all $j < i$ but $b'_i \neq 0$. We have $b_j = a_j - a_i$ for all $j \geq i$. By condition (ii) of $\mathbf{a}$ being canonical, we have $\lambda_j - a_j \geq \lambda_i - a_i$ for all $j > i$, hence $\lambda_j - b_j \geq \lambda_i$ for all $j \geq i$. It follows that h has a p^{λ_i}th root while h' does not, so h and h' are not automorphic. Consequently, g and g' cannot be automorphic, hence $T(\mathbf{a})$ and $T(\mathbf{a}')$ are not automorphic. □

We now obtain an important corollary, which was already discovered by Miller

[13, p. 23] and (apparently independently) by Baer [1, Corollary 2]:

Corollary 4.8 (Miller-Baer)**.** *For any prime p, the number of automorphism classes of $Z_{p^{\lambda_1}} \times Z_{p^{\lambda_2}} \times \cdots \times Z_{p^{\lambda_n}}$ (where $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$) is*

$$\prod_{i=1}^{n} (\lambda_i - \lambda_{i-1} + 1),$$

where by convention we let $\lambda_0 = 0$.

Remark. This count includes the trivial automorphism class (containing only the identity element of the group), in spite of Miller's curious statement to the contrary in [13, p. 23].

Proof. Theorem 4.6 shows that the automorphism classes of G are in one-to-one correspondence with the canonical tuples of $\Lambda(G)$. The canonical tuples $\mathbf{a}$ are precisely those which satisfy $a_{i-1} \leq a_i \leq a_{i-1} + \lambda_i - \lambda_{i-1}$ for each $i \in \{1, \ldots, n\}$ (by convention, setting $a_0 = 0$). Thus there are $\lambda_i - \lambda_{i-1} + 1$ choices for each coordinate a_i, and the result follows. □

Example 4.9. Let $G = Z_2 \times Z_8 = Z_2 \times Z_{2^3} = \langle s \rangle \times \langle t \rangle$. Then there are $(1 - 0 + 1)(3 - 1 + 1) = 6$ automorphism classes of G, namely:

$$\begin{aligned}
O(0,0) &= T(0,0) = \{1\}, \\
O(0,1) &= T(0,1) = \{t^4\}, \\
O(0,2) &= T(0,2) = \{t^2, t^6\}, \\
O(1,1) &= T(1,1) \cup T(1,0) = \{s, st^4\}, \\
O(1,2) &= T(1,2) = \{st^2, st^6\}, \\
O(1,3) &= T(1,3) \cup T(0,3) = \{t, st, t^3, st^3, t^5, st^5, t^7, st^7\}.
\end{aligned}$$

5 Characteristic Subgroups of Abelian Groups

We let $\mathrm{Char}(G)$ denote the lattice of characteristic subgroups of G.

Definition 5.1. Given an n-tuple $\mathbf{a} \in \Lambda(G)$, we define the subgroup $R(\mathbf{a}) = \bigcup_{\mathbf{b} \leq \mathbf{a}} T(\mathbf{b})$ and call $R(\mathbf{a})$ the *regular subgroup below* $\mathbf{a}$.

Remark. We use the term "regular", following Baer ([1]). But this concept of regular should not be confused with the notion of a regular permutation group, nor of a regular p-group.

Theorem 5.2. *$R(\mathbf{a})$ is a characteristic subgroup if and only if $T(\mathbf{a})$ is a canonical type.*

Proof. Suppose first that $\mathbf{a}$ is noncanonical. Then by Lemma 4.7, there is another tuple $\mathbf{a}' > \mathbf{a}$ with $O(\mathbf{a}') = O(\mathbf{a})$. Then $R(\mathbf{a})$ contains $T(\mathbf{a})$ but not $T(\mathbf{a}')$; this means that $R(\mathbf{a})$ contains some but not all of the automorphism class $O(\mathbf{a})$, so $R(\mathbf{a})$ is not characteristic.

Now assume $\mathbf{a}$ is canonical. We need to show that $R(\mathbf{a})$ is a union of automorphism classes. Suppose by way of contradiction that there is a type $T(\mathbf{b})$ with $T(\mathbf{b}) \subseteq R(\mathbf{a})$ but not $O(\mathbf{b}) \subseteq R(\mathbf{a})$. Take $\mathbf{b}$ to be a maximal such tuple. If $\mathbf{b}$ is canonical, then for every type $T(\mathbf{c})$ contained in $O(\mathbf{b})$, we have $\mathbf{c} \leq \mathbf{b}$ since $\mathbf{b}$ is the maximum type of its automorphism class by Theorem 4.6. Hence $\mathbf{c} \leq \mathbf{a}$, so $T(\mathbf{c}) \subseteq R(\mathbf{a})$. This implies $O(\mathbf{b}) \subseteq R(\mathbf{a})$, contrary to assumption. So $\mathbf{b}$ must be noncanonical. So there is some $i \in \{1, \ldots, n-1\}$ such that either $b_{i+1} < b_i$ or $b_{i+1} - b_i > \lambda_{i+1} - \lambda_i$. In the first case, define $\mathbf{b}'$ by $b'_j = b_j$ for $j \neq i+1$ and $b'_{i+1} = b_i$. By Lemma 4.7, $T(\mathbf{b})$ and $T(\mathbf{b}')$ are automorphic types, i.e. $O(\mathbf{b}) = O(\mathbf{b}')$. Since $\mathbf{a}$ is canonical, we have $a_i \leq a_{i+1}$, hence $b'_{i+1} = b_i \leq a_i \leq a_{i+1}$, so that $\mathbf{b}' \leq \mathbf{a}$. Then $T(\mathbf{b}') \subseteq R(\mathbf{b})$ but not $O(\mathbf{b}') \subseteq R(\mathbf{a})$. Since $\mathbf{b}' > \mathbf{b}$, this contradicts the maximality of $\mathbf{b}$.

In the second case, i.e., if $b_{i+1} - b_i > \lambda_{i+1} - \lambda_i$, define $\mathbf{b}'$ by $b'_j = b_j$ for $j \neq i$ and $b'_i = b_{i+1} - (\lambda_{i+1} - \lambda_i)$. Again by Lemma 4.7, $T(\mathbf{b})$ and $T(\mathbf{b}')$ are automorphic types.

Since $\mathbf{a}$ is canonical, we have $a_{i+1} - (\lambda_{i+1} - \lambda_i) \leq a_i$. Hence $b'_i = b_{i+1} - (\lambda_{i+1} - \lambda_i) \leq a_{i+1} - (\lambda_{i+1} - \lambda_i) \leq a_i$, so $\mathbf{b}' \leq \mathbf{a}$. Then, as in the previous case, $T(\mathbf{b}') \subseteq R(\mathbf{b})$ but not $O(\mathbf{b}') \subseteq R(\mathbf{a})$, which this contradicts the maximality of $\mathbf{b}$, since $\mathbf{b}' > \mathbf{b}$, □

The following is easily verified by direct calculation:

Theorem 5.3. *For any* $\mathbf{a}, \mathbf{b} \in \Lambda(G)$,

(i) $R(\mathbf{a}) \cap R(\mathbf{b}) = R(\mathbf{a} \wedge \mathbf{b})$

(ii) $\langle R(\mathbf{a}), R(\mathbf{b}) \rangle = R(\mathbf{a} \vee \mathbf{b})$

(iii) $|R(\mathbf{a})| = p^{\sum_{i=1}^{n} a_i}$

From (i) and (ii) and the fact that the meet and join of characteristic subgroups is characteristic, it follows that the regular characteristic subgroups form a sublattice of $\mathrm{Char}(G)$. Using Theorem 5.2, this then implies that if $\mathbf{a}$ and $\mathbf{b}$ are canonical tuples then so are $\mathbf{a} \wedge \mathbf{b}$ and $\mathbf{a} \vee \mathbf{b}$. (This is also not difficult to verify directly.)

The following theorem shows that irregular characteristic subgroups can only exist in the case $p = 2$.

Theorem 5.4 (Miller-Baer)**.** *Let G be an abelian p-group where $p \neq 2$. Then every characteristic subgroup of G is regular.*

Remark. This theorem was shown by Baer in [1, Theorem 9]. It was known to Miller although it is, at the very least, questionable whether his footnote in [13, p. 21] constitutes a complete proof.

Proof. Let H be any characteristic subgroup of G. Define the n-tuple $\mathbf{m}$ by $m_i = \max\{a_i : \mathbf{a} \in \Lambda(G), T(\mathbf{a}) \subseteq H\}$. It is clear then that $H \leq R(\mathbf{m})$. We will show that on the other hand $R(\mathbf{m}) \leq H$, from which the result immediately follows.

For any i, by our definition of $\mathbf{m}$ there is a type $\mathbf{a}$ such that $T(\mathbf{a}) \subseteq H$ and $a_i = m_i$. Then $g = \prod_{j=1}^{n} t_{j,a_j}$ and $g' = t_{i,m_i} \prod_{j \neq i} t_{j,a_j}^{-1}$ are two elements of $T(\mathbf{a})$. Since

H is a subgroup, $gg' = t_{i,m_i}^2 \in H$. Since $p \neq 2$, we have $\langle t_{i,m_i}^2 \rangle = \langle t_{i,m_i} \rangle$, so $t_{i,m_i} \in H$. Since the elements t_{i,m_i} generate $R(\mathbf{m})$, it follows that $R(\mathbf{m}) \leq H$, as desired. □

Corollary 5.5. *Let G be an abelian p-group where $p \neq 2$. Then the lattice of characteristic subgroups of G is distributive.*

Proof. From Theorem 5.3 it is clear that the lattice of regular characteristic subgroups of G is isomorphic to the lattice $\mathcal{C}(G)$, which is a sublattice of $\Lambda(G)$. The latter lattice is distributive since it is a direct product of chains. Since in our case every characteristic subgroup is regular, the result follows. □

Corollary 5.6. *Let $G = Z_{p^{\lambda_1}} \times Z_{p^{\lambda_2}} \times \cdots \times Z_{p^{\lambda_n}}$ be an abelian p-group with $p \neq 2$. Let $q \neq 2$ be any other odd prime, and set $G' = Z_{q^{\lambda_1}} \times Z_{q^{\lambda_2}} \times \cdots \times Z_{q^{\lambda_n}}$. Then* $\mathrm{Char}(G) \cong \mathrm{Char}(G')$.

Proof. This is immediate since $\mathrm{Char}(G) \cong \mathcal{C}(G) \cong \mathcal{C}(G') \cong \mathrm{Char}(G')$. □

Corollary 5.7. *Let G be an abelian p-group where $p \neq 2$. Then the set $\{\overline{H} : H \in \mathrm{Char}(G)\}$ forms a basis for the discrete rational S-ring $\mathcal{W}(G)$.*

Proof. The S-ring $\mathcal{W}(G)$ is spanned by $\{\overline{O(\mathbf{a})} : \mathbf{a} \in \mathcal{C}(G)\}$. Given any characteristic subgroup $R(\mathbf{a})$, we can write $\overline{R(\mathbf{a})} = \sum_{\mathbf{b} \in \mathcal{C}(G)} \overline{O(\mathbf{b})}$, so that $\{\overline{H} : H \in \mathrm{Char}(G)\} \subseteq \mathcal{W}(G)$. On the other hand, we can write

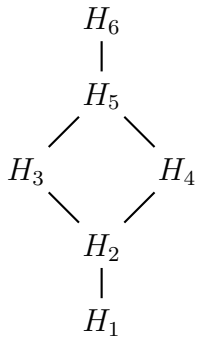
$$\overline{O(\mathbf{a})} = \overline{R(\mathbf{a})} - \sum_{\substack{\mathbf{b} \in \mathcal{C}(G) \\ \mathbf{b} < \mathbf{a}}} \overline{O(\mathbf{b})},$$

so that by induction each $\overline{O(\mathbf{a})}$ is in the span of $\{\overline{H} : H \in \mathrm{Char}(G)\}$. □

Example 5.8. Let $G = Z_p \times Z_{p^3}$ for an odd prime p. Let $H_1, \ldots, H_6$ be the characteristic subgroups of G, in the order shown in Table 3. Using Theorem 1.7, it is easy to check that $S = F\{1, \overline{H}_2, \overline{H}_3 + \overline{H}_4, \overline{H}_5, \overline{G}\}$ is a rational S-ring. We show that S

Table 3: Characteristic subgroups of $G = Z_p \times Z_{p^3}$ for odd prime p

H_1	R(0,0)
H_2	R(0,1)
H_3	R(0,2)
H_4	R(1,1)
H_5	R(1,2)
H_6	R(1,3)



cannot be constructed as in Theorem 2.3. Suppose $S = F(\mathcal{L})$ for some lattice $\mathcal{L}$. By Corollary 5.7, the elements $\{\overline{H} : H \in \mathcal{L}\}$ are linearly independent, hence form a basis for S. So $\dim S = |\mathcal{L}|$. Now $\dim S = 5$, yet, by applying Corollary 5.7 again, it is easy to see that $1, H_2, H_5$, and G are the only four subgroups of G which are S-sets, hence $|\mathcal{L}| \leq 4$, a contradiction.

Example 5.9. Let $G = Z_p \times Z_{p^3} \times Z_{p^5}$ for an odd prime p. Let $H_1, \ldots, H_{18}$ be the characteristic subgroups of G, in the order shown in Table 4. Note that the sublattice of $\mathrm{Char}(G)$ between $R(0,1,2)$ and $R(1,2,3)$ forms a cube; i.e., this sublattice is isomorphic to the boolean lattice $\mathcal{P}(X)$ of subsets of a set X of cardinality 3.

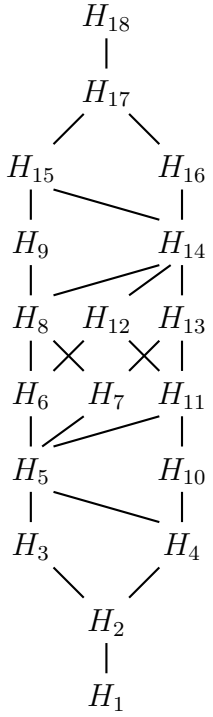
The following theorem gives a generalization of preceding two examples which will be important to us later on.

Theorem 5.10. *Let X be a (finite) set containing n elements. There is an embedding ψ of the boolean lattice $\mathcal{P}(X)$ into* $\mathrm{Char}(Z_p \times Z_{p^3} \times \cdots \times \mathbb{Z}_{p^{2n-1}})$. *Further, ψ has the property that for all subsets Y_1, Y_2 of X, $|Y_1| = |Y_2| \iff |\psi(Y_1)| = |\psi(Y_2)|$.*

Proof. We will map $\mathcal{P}(X)$ into the lattice of characteristic subgroups contained in $R(1,2,3,\ldots,n)$ and containing $R(0,1,2,\ldots,n-1)$. Write $X = \{x_1, \ldots, x_n\}$. Define

Table 4: Characteristic subgroups of $G = Z_p \times Z_{p^3} \times Z_{p^5}$ for odd prime p

H_1	R(0,0,0)
H_2	R(0,0,1)
H_3	R(0,0,2)
H_4	R(0,1,1)
H_5	R(0,1,2)
H_6	R(0,1,3)
H_7	R(0,2,2)
H_8	R(0,2,3)
H_9	R(0,2,4)
H_{10}	R(1,1,1)
H_{11}	R(1,1,2)
H_{12}	R(1,1,3)
H_{13}	R(1,2,2)
H_{14}	R(1,2,3)
H_{15}	R(1,2,4)
H_{16}	R(1,3,3)
H_{17}	R(1,3,4)
H_{18}	R(1,3,5)



$\psi(Y) = R(\mathbf{a}(Y))$ where the ith component of the n-tuple $\mathbf{a}(Y)$ is defined to be $i-1$ if $x_i \notin Y$ and i if $x_i \in Y$; note that ψ is well-defined since each such tuple $\mathbf{a}(Y)$ is canonical, as the difference between two consecutive coordinates of $\mathbf{a}(Y)$ is either 0, 1, or 2. We have

$$\begin{aligned}\psi(Y_1 \cap Y_2) &= R(\mathbf{a}(Y_1 \cap Y_2)) = R(\mathbf{a}(Y_1) \wedge \mathbf{a}(Y_2)) \\ &= R(\mathbf{a}(Y_1)) \cap R(\mathbf{a}(Y_2)) = \psi(Y_1) \cap \psi(Y_2)\end{aligned}$$

and

$$\begin{aligned}\psi(Y_1 \cup Y_2) &= R(\mathbf{a}(Y_1 \cup Y_2)) = R(\mathbf{a}(Y_1) \vee \mathbf{a}(Y_2)) \\ &= \langle R(\mathbf{a}(Y_1)), R(\mathbf{a}(Y_2))\rangle = \langle \psi(Y_1), \psi(Y_2)\rangle,\end{aligned}$$

so that ϕ is a lattice homomorphism. By construction ϕ is injective, so ϕ is an embedding. Theorem 5.3(iii) shows that $|\phi(Y)| = p^{\frac{n(n-1)}{2}+|Y|}$, which proves the last claim. □

The following theorem shows that adding a duplicate factor in the direct decomposition of G does not change its lattice of characteristic subgroups.

Theorem 5.11. *Let $G = Z_{p^{\lambda_1}} \times Z_{p^{\lambda_2}} \times \cdots \times Z_{p^{\lambda_n}}$ be an abelian p-group with $p \neq 2$. Then for any $i \in \{1, \ldots, n\}$, $\mathrm{Char}(G) \cong \mathrm{Char}(G \times Z_{p^{\lambda_i}})$.*

Proof. Let $G' = Z_{p^{\lambda_1}} \times Z_{p^{\lambda_2}} \times \cdots \times Z_{p^{\lambda_{i-1}}} \times Z_{p^{\lambda_i}} \times Z_{p^{\lambda_i}} \times Z_{p^{\lambda_{i+1}}} \times \cdots \times Z_{p^{\lambda_n}}$, so $G' \cong G \times Z_{p^{\lambda_i}}$. Every canonical tuple of G' has the form $(a_1, a_2, \ldots, a_{i-1}, a_i, a_i, a_{i+1}, \ldots, a_n)$, i.e., the ith and $(i+1)$th coordinates are forced to be equal. It follows that the correspondence

$$R(a_1, \ldots, a_n) \mapsto R(a_1, \ldots, a_{i-1}, a_i, a_i, a_{i+1}, \ldots, a_n)$$

is an isomorphism of $\mathrm{Char}(G)$ onto $\mathrm{Char}(G')$. $\square$

The case $p = 2$

In this section fix G to be an abelian 2-group.

Given any characteristic subgroup H of G, as in the proof of Theorem 5.4 we can define the n-tuple $\mathbf{m}$ by $m_i = \max\{a_i : \mathbf{a} \in \Lambda(G), T(\mathbf{a}) \subseteq H\}$. We say then that H is a characteristic subgroup *below* $\mathbf{m}$. For a canonical tuple $\mathbf{m}$, an example of a characteristic subgroup below $\mathbf{m}$ is $R(\mathbf{m})$; when $p \neq 2$, this is the unique such subgroup, as Theorem 5.4 shows. When $p = 2$, there may be several characteristic subgroups below a given canonical tuple $\mathbf{m}$. The set of such subgroups will be denoted $\mathrm{Char}_{\mathbf{m}}(G)$. Our goal in this section is to give a description of these subgroups.

Definition 5.12. A subgroup H of a direct product $K_1 \times K_2 \times \cdots \times K_l$ is *projection-surjective* if $\pi_i(H) = K_i$ for each $i \in \{1, \ldots, l\}$, where π_i is the natural projection map onto the ith component of the product. (In other words, H is a subdirect product of $K_1, K_2, \ldots, K_l$.)

Definition 5.13. A coordinate i of a canonical tuple $\mathbf{a} \in \mathcal{C}(G)$ is *degenerate* if

(i) $a_i = a_{i-1}$, or

(ii) $a_{i+1} - a_i = \lambda_{i+1} - \lambda_i$,

where by convention $a_0 = 0$. Otherwise, i is *nondegenerate*.

Recall that in a canonical tuple, each coordinate must increase by between 0 and $\lambda_{i+1} - \lambda_i$. So, a coordinate is degenerate if it has increased the least possible from the previous coordinate (namely, not at all) or if it is followed by a greatest possible increase.

Definition 5.14. For $i \in \{1, \ldots, n\}$, we define $\mathbf{e}_i \in \Lambda(G)$ to be the tuple with zeros in each coordinate except with a 1 in the ith component.

We observe that if $a_i = 0$, then condition (i) of a canonical tuple implies $a_{i-1} = 0$, so that the coordinate i of $\mathbf{a}$ is degenerate (of type (i)). The following Lemma, on the other hand, gives a characterization of when i is degenerate, provided $a_i \neq 0$:

Lemma 5.15. *Let $\mathbf{a} \in \mathcal{C}(G)$ be a canonical type, and let $i \in \{1, \ldots, n\}$ be given with $a_i \neq 0$. Define $\mathbf{a}' = \mathbf{a} - \mathbf{e}_i$ (where the subtraction is defined componentwise so $\mathbf{a}'$ is identical to $\mathbf{a}$ except the ith coordinate has been decreased by 1). Then i is a degenerate coordinate of $\mathbf{a}$ if and only if $\mathbf{a}'$ is noncanonical. Moreover, if i is degenerate then $O(\mathbf{a}') = O(\mathbf{a})$.*

Proof. The first claim follows directly from the definition of degenerate. The last claim follows from Lemma 4.7. □

Theorem 5.16. *Given $\mathbf{m} \in \mathcal{C}(G)$, the characteristic subgroups below $\mathbf{m}$ are in one-to-one correspondence with the projection-surjective subgroups of Z_2^r, where r is the number of non-degenerate coordinates of $\mathbf{m}$.*

Proof. Let H be any characteristic subgroup below $\mathbf{m}$. By the definition of $\mathbf{m}$, for each i there is some type $T(\mathbf{a}) \subseteq H$ with $a_i = m_i$. Then $g = \prod_{j=1}^{n} t_{j,a_j}$ and $g' = t_{i,m_i} \prod_{j \neq i} t_{j,a_j}^{-1}$ are two elements of $T(\mathbf{a})$. Since H is a subgroup, $gg' = t_{i,m_i}^2 = t_{i,\underline{m_i - 1}} \in H$, where $\underline{x}$ is the "clipping" function defined by

$$\underline{x} = \begin{cases} x, & \text{if } x \geq 0, \\ 0, & \text{if } x < 0. \end{cases}$$

If we define $\mathbf{m}'$ by $m_i' = \underline{m_i - 1}$, then it is clear that $R(\mathbf{m}') \subseteq H$, since the set $\{t_{i,\underline{m_i - 1}} : i = 1, \ldots, n\}$ generates $R(\mathbf{m}')$. Clearly $R(\mathbf{m}') \subseteq R(\mathbf{m})$ and $R(\mathbf{m})/R(\mathbf{m}') \cong Z_2^l$ where l is the number of nonzero entries of $\mathbf{m}$. To be more specific, let $\pi : R(\mathbf{m}) \to R(\mathbf{m})/R(\mathbf{m}')$ be the natural projection map, and set $K_i = \pi(\langle t_{i,m_i} \rangle)$; then $K_i \cong Z_2$ if $m_i \neq 0$, while K_i is trivial if $m_i = 0$. Let k_i be the generator for K_i (so $|k_i| = 2$

unless $m_i = 0$, in which case $k_i = 1$). The lattice isomorphism theorem implies that the subgroups of $R(\mathbf{m})$ containing $R(\mathbf{m}')$ (among which are all the subgroups H in $\mathrm{Char}_{\mathbf{m}}(G)$) are in one-to-one correspondence with subgroups of $\pi(R(\mathbf{m})) \cong Z_2^l$. Now, note that by definition, for any i, if $m_i = 0$ then i is a degenerate coordinate. If i is a nonzero degenerate coordinate of $\mathbf{m}$, define $\mathbf{a}'$ by $a'_j = a_j$ for all $j \neq i$ and $a'_i = a_i - 1$. Then observe that the degeneracy of i ensures $O(\mathbf{a}') = O(\mathbf{a})$ by Lemma 5.15. Thus $T(\mathbf{a}') \subseteq H$, and so $\hat{g} = \prod_{i=1}^n t_{1,a'_i} \in H$. If we write $\pi(g) = \prod_{j=1}^n k_j^{\epsilon_j}$, where each $\epsilon_j \in \{0, 1\}$, then $\pi(\hat{g}) = \prod_{j \neq i} k_j^{\epsilon_j}$. Since $a_i = m_i$, we have $\epsilon_i = 1$, and it follows that $\pi(g\hat{g}) = k_i^{\epsilon_i} \prod_{j \neq i} k_j^{2\epsilon_j} = k_i$, so that $K_i \leq \pi(H)$. Thus, if D is the set of nonzero degenerate coordinates of $\mathbf{m}$, we may write

$$\pi(H) = K \times \prod_{j \in D} K_j,$$

where K is a projection-surjective subgroup of $\prod_{j \in D'} K_j$, where D' is the set of non-degenerate coordinates of $\mathbf{m}$. This gives us an injective map $H \mapsto K$ from $\mathrm{Char}_{\mathbf{m}}(G)$ into the set of projection-surjective subgroups of $\prod_{j \in D'} K_j \cong Z_2^r$. It remains only to show that this correspondence is surjective.

So let K be an arbitrary projection-surjective subgroup of $\prod_{j \in D'} K_j$. Set $K' = K \times \prod_{j \in D} K_j$ and let $H = \pi^{-1}(K')$. The projection-surjectivity of K ensures that H is a subgroup below $\mathbf{m}$. We only need to show that H is characteristic. To do this, it is enough to show that if $T(\mathbf{a})$ is a noncanonical type contained in H then there is another type $T(\mathbf{a}')$ contained in H with $\mathbf{a}' > \mathbf{a}$. Since H contains the characteristic subgroup $R(\mathbf{m}')$, it is sufficient to consider the case where $T(\mathbf{a})$ is not contained in $R(\mathbf{m}')$, namely $\mathbf{a} > \mathbf{m}'$. Since $T(\mathbf{a})$ is noncanonical, there is some i such that either $a_{i-1} > a_i$ or $a_{i+1} - a_i > \lambda_{i+1} - \lambda_i$. In the former case, we have $a_i < a_{i-1} \leq m_{i-1} \leq m_i$ since by condition (i) of $\mathbf{m}$ being canonical, while in the latter case, we have $a_i < a_{i+1} - (\lambda_{i+1} - \lambda_i) \leq a_{i+1} - (m_{i+1} - m_i) \leq a_{i+1} - (a_{i+1} - m_i) = m_i$.

So in either case we have $a_i < m_i$, which implies $a_i = m_i - 1$, since $\mathbf{a} \geq \mathbf{m}'$. Now if every such coordinate i was nondegenerate in $\mathbf{m}$, then by repeated application of Lemma 5.15, $\mathbf{a}$ would be canonical, contrary to assumption. So there must be some such i which is a degenerate coordinate of $\mathbf{m}$. Define $\mathbf{a}'$ by $a'_j = a_j$ for $j \neq i$ and $a'_i = m_i$. Let g be an element of type $T(\mathbf{a})$ and write $k = \pi(g) = \prod_{j=1}^{n} k_j^{\epsilon_j}$ with $\epsilon_j \in \{0, 1\}$ (namely, we will have $\epsilon_j = 1$ if and only if $a_j = m_j$). Then $k' = k_i \prod_{j \neq i} k_j^{\epsilon_j}$ is also in $\pi(H)$ (since $k_i \in \prod_{j \in D} K_j \subseteq K'$), and the set $\pi^{-1}(k')$ includes elements of type $\mathbf{a}'$, so $T(\mathbf{a}') \subseteq H$, as desired. □

A statement equivalent to the following is stated (without proof) in [13, p. 23]:

Corollary 5.17. *Irregular characteristic subgroups below a canonical tuple* $\mathbf{a} \in \mathcal{C}(G)$ *exist if and only if* $\mathbf{a}$ *has at least two nondegenerate coordinates.*

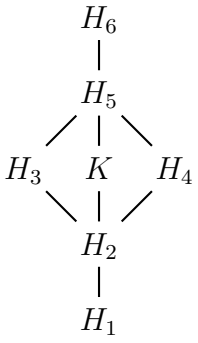
Proof. Since Z_2^k has proper projection-surjective subgroups if and only if $k \geq 2$, this follows from Theorem 5.16. □

Example 5.18. Let $G = Z_2 \times Z_8$. Let $H_1, \ldots, H_6$ be the regular characteristic subgroups of G, as shown in Table 5. We note that (1,2) is the only canonical tuple with two nondegenerate coordinates; consequently, there is an irregular characteristic subgroup K below (1,2) and this is the only irregular characteristic subgroup of G. Note that the lattice of characteristic subgroups of G is not distributive, in contrast to Theorem 5.5; see Theorem 5.25 below.

Definition 5.19. Given a canonical tuple $\mathbf{a}$ with $k \geq 2$ nondegenerate coordinates, we define $I(\mathbf{a})$ to be the characteristic subgroup corresponding (under the correspondence of Theorem 5.16) to the unique projection-surjective subgroup of Z_2^k of order 2. (This is simply the diagonal subgroup of Z_2^k). Explicitly, $I(\mathbf{a}) = R(\mathbf{b}) \cup T(\mathbf{a})$, where $\mathbf{b}$ is given by $b_j = a_j$ if j is a degenerate coordinate, while $b_j = a_j - 1$ otherwise.

Table 5: Characteristic subgroups of $Z_2 \times Z_8$

H_1	R(0,0)
H_2	R(0,1)
H_3	R(0,2)
H_4	R(1,1)
K	$\mathrm{R}(0,1) \cup \mathrm{T}(1,2)$
H_5	R(1,2)
H_6	R(1,3)



Note that $I(\mathbf{a})$ is then an irregular characteristic subgroup below $\mathbf{a}$. If every canonical tuple of $\mathcal{C}(G)$ has at most 2 nondegenerate coordinates, then every irregular characteristic subgroup of G may be written $I(\mathbf{a})$ for some $\mathbf{a}$. For instance, in Table 5, the irregular characteristic subgroup K may be written $I(1,2)$.

Theorem 5.16 leads to a method of enumerating the characteristic subgroups of abelian 2-groups, and hence the characteristic subgroups of arbitrary finite abelian groups. More specifically, Theorem 5.16 reduces this problem to the problems of

1. Enumerating the projection-surjective subgroups of Z_2^k, and

2. Enumerating the tuples $\mathbf{a} \in \mathcal{C}(G)$ with k non-degenerate coordinates.

A solution to the the first of these two problems is provided by the following theorem:

Theorem 5.20. *The number of projection-surjective subgroups of Z_2^k is*

$$n_k = \sum_{i=0}^{k} (-1)^{i+k} \binom{k}{i} \sum_{j=0}^{i} \binom{i}{j}_2,$$

where $\binom{i}{j}_2$ *are the Gaussian binomial coefficients given by*

$$\binom{i}{j}_2 = \frac{\prod_{l=0}^{j-1} \left(2^{i-l} - 1\right)}{\prod_{l=1}^{j} \left(2^l - 1\right)}.$$

Remark. The sequence n_k begins $1, 1, 2, 6, 26, 158, 1330, 15414, 245578, 5382862, \ldots$ for $k = 0, 1, 2, \ldots$ and may be found as A135922 of Sloane's on-line encyclopedia of integer sequences [18].

Proof. Let $X = \{1, \ldots, k\}$. For any subgroup H of Z_2^k, set $\rho(H)$ denote the set of integers $i \in X$ such that $\pi_i(H) = Z_2$. So H is projection-surjective if and only if $\rho(H) = X$. For any subset $Y \subseteq X$, let $n(Y)$ be the number of subgroups H of Z_2^k such that $\rho(H) = Y$. We would like to compute $n_k = n(X)$. Now define $m(Y)$ to be the number of subgroups H of Z_2^k with $\rho(H) \subseteq Y$. So

$$m(Y) = \sum_{Z \subseteq Y} n(Z).$$

Now $m(Y)$ is simply the total number of subgroups of $Z_2^{|Y|}$; this is the same as the number of subspaces of a $|Y|$-dimensional vector space over $\mathbb{F}_2$. Since the number of j-dimensional subspaces of such a vector space is known to be

$$\frac{\prod_{l=0}^{j-1} \left(2^{|Y|} - 2^l\right)}{\prod_{l=0}^{j-1} \left(2^j - 2^l\right)} = \frac{\prod_{l=0}^{j-1} \left(2^{|Y|-l} - 1\right)}{\prod_{l=0}^{j-1} \left(2^{j-l} - 1\right)} = \frac{\prod_{l=0}^{j-1} \left(2^{|Y|-l} - 1\right)}{\prod_{l=1}^{j} \left(2^l - 1\right)} = \binom{|Y|}{j}_2$$

(see, e.g., [7, p. 412]), it follows that

$$m(Y) = \sum_{j=0}^{|Y|} \binom{|Y|}{j}_2.$$

We note, in particular, that $m(Y)$ only depends on the size of Y. By the inclusion-exclusion principle (see, e.g., [4, p. 185]) we have

$$\begin{aligned} n(X) &= \sum_{Y \subseteq X} (-1)^{|Y|+|X|} m(Y) \\ &= \sum_{i=0}^{k} \sum_{\substack{Y \subseteq X \\ |Y|=i}} (-1)^{i+k} m(Y) \\ &= \sum_{i=0}^{k} \binom{k}{i} (-1)^{i+k} m(\{1, \ldots, i-1\}) \\ &= \sum_{i=0}^{k} (-1)^{i+k} \binom{k}{i} \sum_{j=0}^{i} \binom{i}{j}_2, \end{aligned}$$

as desired. □

As to the second problem, that of enumerating the tuples $\mathbf{a} \in \Lambda(G)$ with a given number of non-degenerate coordinates, we are not aware of a simple formula for counting the number of such tuples. However, it is nevertheless possible to enumerate them recursively without having to list each tuple; using such an approach we can easily enumerate the characteristic subgroups of an arbitrary finite abelian group. In Table 6, for example, we have listed the total number of characteristic subgroups of $Z_2 \times Z_{2^2} \times Z_{2^3} \times \cdots \times Z_{2^n}$ for $n \leq 40$.

A further application of the notion of degenerate coordinates is an explicit description, in a certain situation, of how an automorphism class splits up as a union of types:

Theorem 5.21. *Let G be an abelian p-group (for any prime p) with no repeated*

Table 6: Number of characteristic subgroups of $Z_2 \times Z_{2^2} \times Z_{2^3} \times \cdots \times Z_{2^n}$

1	2
2	4
3	9
4	21
5	52
6	134
7	363
8	1027
9	3054
10	9516
11	31229
12	107745
13	392792
14	1511010
15	6167551
16	26670383
17	122982386
18	603221064
19	3172965937
20	17817816493
21	107984192188
22	700497542494
23	4939837336979
24	37315530126171
25	309078760337078
26	2736173394567076
27	26852600855758373
28	279765993533235769
29	3279737127172518880
30	40284238921560357658
31	568574087799302502375
32	8225663800386744379975
33	1408869289534420400256 58
34	2392158426272284053385152
35	501378418125852753825799 29
36	993099669210856047011613573
37	257012288686092485421522149 80
38	589013066872810742690824633750
39	190053482155162040777486832862 67
40	498993627095578092364760281155059

factors (i.e., $0 < \lambda_1 < \lambda_2 < \cdots < \lambda_n$*), and let* $\mathbf{a} \in \mathcal{C}(G)$ *be a canonical tuple. Then*

$$O(\mathbf{a}) = \bigcup \{T(\mathbf{b}) : \mathbf{b} \leq \mathbf{a} \text{ and, for each nondegenerate coordinate } i \text{ of } \mathbf{a},\ b_i = a_i\}$$

Proof. Let

$$A = \bigcup \{T(\mathbf{b}) : \mathbf{b} \leq \mathbf{a} \text{ and, for each nondegenerate coordinate } i \text{ of } \mathbf{a},\ b_i = a_i\}.$$

We first show $O(\mathbf{a}) \subseteq A$. Given any $T(\mathbf{b}) \subseteq O(\mathbf{a})$, we have $\mathbf{b} \leq \mathbf{a}$ since $T(\mathbf{a})$ is the maximum type in $O(\mathbf{a})$ by Theorem 4.6. Now let i be a nondegenerate coordinate of $\mathbf{a}$ and suppose $b_i < a_i$. Then $\mathbf{a}' = \mathbf{a} - \mathbf{e}_i$ is canonical by Theorem 5.2, hence $R(\mathbf{a}')$ is a characteristic subgroup with $\mathbf{b} \leq \mathbf{a}'$, so $O(\mathbf{a}) = O(\mathbf{b}) \subseteq R(\mathbf{a}')$, which is a contradiction since $\mathbf{a} \not\leq \mathbf{a}'$. Consequently $b_i = a_i$, which proves $O(\mathbf{a}) \subseteq A$.

Now we must show $A \subseteq O(\mathbf{a})$. Suppose there is some $T(\mathbf{b}) \subseteq A$ with $T(\mathbf{b}) \nsubseteq O(\mathbf{a})$, i.e. $O(\mathbf{b}) \neq O(\mathbf{a})$. Take a maximal such $\mathbf{b}$. We must then have $\mathbf{b} < \mathbf{a}$. Let i be the first coordinate for which $b_i < a_i$. Then, by the definition of A, i must be a degenerate coordinate of $\mathbf{a}$. If i is degenerate because $a_i = a_{i-1}$, then we have $b_i < a_i = a_{i-1} = b_{i-1}$, so by Lemma 4.7, if we define $\mathbf{b}'$ by $b'_k = b_k$ for all $k \neq i$ and $b'_i = b_{i-1}$, then $O(\mathbf{b}') = O(\mathbf{b}) \neq O(\mathbf{a})$, while $\mathbf{b}' > \mathbf{b}$, contradicting the maximality of $\mathbf{b}$. On the other hand, if i is degenerate because $a_i + \lambda_{i+1} - \lambda_i = a_{i+1}$, then let j be the first coordinate greater than i such that $b_j = a_j$; such a j must exist since otherwise all the coordinates $i, \ldots, n$ of $\mathbf{a}$ would be degenerate and we would have $a_n = a_{n-1} = \cdots = a_{i+1} = a_i$, contradicting $a_i + \lambda_{i+1} - \lambda_i = a_{i+1}$ since $\lambda_{i+1} \neq \lambda_i$. Thus all of the coordinates $i, \ldots, j-1$ of $\mathbf{a}$ are degenerate. We find that each coordinate $k \in \{i, \ldots, j-1\}$ is degenerate of the second type, i.e. we find that $a_k + \lambda_{k+1} - \lambda_k = a_{k+1}$: For $k = i$ this holds by assumption, while for $k > i$, if k were degenerate of the first type, i.e. $a_k = a_{k-1}$, we would have a

contradiction since by induction, $a_{k-1} + \lambda_k - \lambda_{k-1} = a_k$ and $\lambda_k \neq \lambda_{k-1}$. So we have $b_{j-1} + \lambda_j - \lambda_{j-1} < a_{j-1} + \lambda_j - \lambda_{j-1} = a_j = b_j$, so by Lemma 4.7, if we again obtain a $\mathbf{b}' > \mathbf{b}$ with $O(\mathbf{b}') = O(\mathbf{b}) \neq O(\mathbf{a})$, contradicting the maximality of $\mathbf{b}$. □

Example 5.22. Let $G = Z_p \times Z_{p^3} \times Z_{p^5}$. The first and third coordinates of the tuple $(1, 3, 3)$ are degenerate. So we have

$$\begin{aligned} O(1,3,3) = T(0,3,0) \cup T(0,3,1) \cup T(0,3,2) \cup T(0,3,3) \\ \cup T(1,3,0) \cup T(1,3,1) \cup T(1,3,2) \cup T(1,3,3). \end{aligned}$$

Theorem 5.23. *The lattice of characteristic subgroups of a finite abelian group G is a chain if and only if $G \cong Z_{p^k}^{\mu_1} \times Z_{p^{k+1}}^{\mu_2}$ for some natural numbers $k, \mu_1, \mu_2 \geq 0$ and some prime p.*

Proof. First assume the lattice of characteristic subgroups of G is a chain. If $|G|$ were not a prime power, it would have distinct prime divisors p and q, and the Sylow p-subgroup and Sylow q-subgroup of G would be incomparable. So G must be an abelian p-group, and without loss of generality we may write $G = Z_{p^{\lambda_1}} \times \cdots \times Z_{p^{\lambda_n}}$, where $1 \leq \lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$. Note that the claim that G has the form $Z_{p^k}^{\mu_1} \times Z_{p^{k+1}}^{\mu_2}$ is equivalent to the claim that $\lambda_n - \lambda_1 \leq 1$. So suppose $\lambda_n - \lambda_1 \geq 2$. Define tuples $\mathbf{a}$ and $\mathbf{a}'$ by

$$\begin{aligned} a_i &= 1 \\ a_i' &= \lambda_i - \lambda_1. \end{aligned}$$

for all $i = 1, \ldots, n$. Then it is easy to see that $\mathbf{a}$ and $\mathbf{a}'$ are canonical tuples. Since $a_1 = 1 > 0 = a_1'$ we have $\mathbf{a} \not\leq \mathbf{a}'$, while since $a_n = 1 < 2 \leq \lambda_n - \lambda_1 = a_n'$, we have $\mathbf{a} \not\geq \mathbf{a}'$. The characteristic subgroups $R(\mathbf{a})$ and $R(\mathbf{a}')$ are then incomparable, contradicting the hypothesis. Hence $\lambda_n - \lambda_1 \leq 1$, as desired.

Conversely, suppose $\lambda_n - \lambda_1 \leq 1$. Then every canonical tuple $\mathbf{a} \in \mathcal{C}(G)$ then has the form

$$a_i = \begin{cases} 0, & \text{if } i < j \\ 1, & \text{if } i \geq j \end{cases}$$

for some natural number $j \geq 0$. In the case $p = 2$, since such a tuple has at most one nondegenerate coordinate, it follows from Theorem 5.16 that every characteristic subgroup of G is regular. (Since Z_2^k has only one projection-surjective subgroup if $k \in \{0, 1\}$, there is a unique characteristic subgroup below each canonical tuple $\mathbf{a}$, namely $R(\mathbf{a})$.) Since any two such tuples $\mathbf{a}$ and $\mathbf{a}'$ are clearly comparable, it follows that $R(\mathbf{a})$ and $R(\mathbf{a}')$ are comparable, so $\mathrm{Char}(G)$ is a chain. □

One may ask the general question: When do two finite abelian p-groups have isomorphic lattices of characteristic subgroups? Corollary 5.6 and Theorems 5.11 and 5.23 provide examples where this occurs. Another example is given by the following theorem, which may be verified by examining Tables 7 and 8:

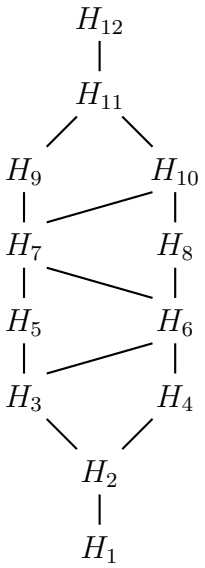
Theorem 5.24. *For any prime p,* $\mathrm{Char}(Z_{p^2} \times Z_{p^5}) \cong \mathrm{Char}(Z_p \times Z_{p^2} \times Z_{p^4})$.

As yet, we have not been able to give a complete answer to the question of when two abelian p-groups have isomorphic lattices of characteristic subgroups. But we are optimistic that with some work this question could be fully resolved. In particular, we know that no additional isomorphisms occur between the lattices of characteristic subgroups of two abelian p-groups of odd order, only those which can be derived from Corollary 5.6 and Theorems 5.11, 5.23, and 5.24. (Thus the isomorphism of Theorem 5.24 is truly exceptional.) The proof of this fact is, however, somewhat complicated and will not be given here.

Theorem 5.25. *The lattice of characteristic subgroups of an abelian 2-group G is distributive if and only if all of its characteristic subgroups are regular.*

Table 7: Characteristic subgroups of $\mathrm{Char}(Z_{p^2} \times Z_{p^5})$ and $\mathrm{Char}(Z_p \times Z_{p^2} \times Z_{p^4})$, $p \neq 2$

H_1	R(0,0)
H_2	R(0,1)
H_3	R(0,2)
H_4	R(0,3)
H_5	R(1,1)
H_6	R(1,2)
H_7	R(1,3)
H_8	R(1,4)
H_9	R(2,2)
H_{10}	R(2,3)
H_{11}	R(2,4)
H_{12}	R(2,5)



H'_1	R(0,0,0)
H'_2	R(0,0,1)
H'_3	R(0,0,2)
H'_4	R(0,1,1)
H'_5	R(0,1,2)
H'_6	R(0,1,3)
H'_7	R(1,1,1)
H'_8	R(1,1,2)
H'_9	R(1,1,3)
H'_{10}	R(1,2,2)
H'_{11}	R(1,2,3)
H'_{12}	R(1,2,4)

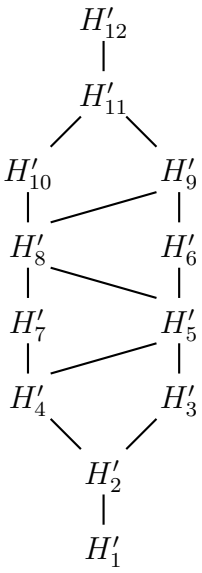
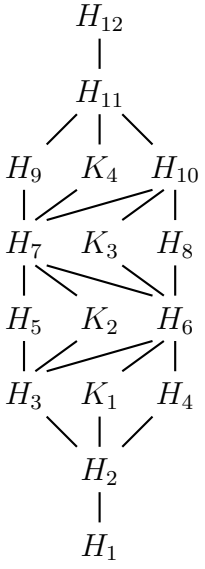
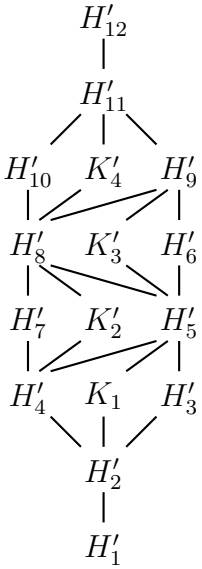


Table 8: Characteristic subgroups of $\mathrm{Char}(Z_{p^2} \times Z_{p^5})$ and $\mathrm{Char}(Z_p \times Z_{p^2} \times Z_{p^4})$, $p = 2$

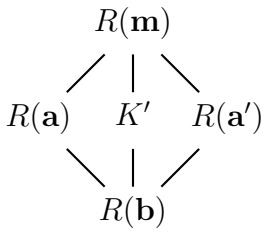
H_1	R(0,0)
H_2	R(0,1)
H_3	R(0,2)
H_4	R(0,3)
H_5	R(1,1)
H_6	R(1,2)
H_7	R(1,3)
H_8	R(1,4)
H_9	R(2,2)
H_{10}	R(2,3)
H_{11}	R(2,4)
H_{12}	R(2,5)
K_1	I(1,2)
K_2	I(1,3)
K_3	I(2,3)
K_4	I(2,4)



H'_1	R(0,0,0)
H'_2	R(0,0,1)
H'_3	R(0,0,2)
H'_4	R(0,1,1)
H'_5	R(0,1,2)
H'_6	R(0,1,3)
H'_7	R(1,1,1)
H'_8	R(1,1,2)
H'_9	R(1,1,3)
H'_{10}	R(1,2,2)
H'_{11}	R(1,2,3)
H'_{12}	R(1,2,4)
K'_1	I(0,1,2)
K'_2	I(1,1,2)
K'_3	I(1,1,3)
K'_4	I(1,2,3)



Proof. The "if" part is trivial, since the lattice of regular characteristic subgroups is clearly distributive. So suppose there is an irregular characteristic subgroup K below a tuple $\mathbf{m}$. By Corollary 5.17, there must be at least two distinct nondegenerate coordinates i and j of $\mathbf{m}$. Define $\mathbf{a} = \mathbf{m} - \mathbf{e}_i$, $\mathbf{a}' = \mathbf{m} - \mathbf{e}_j$, and $\mathbf{b} = \mathbf{m} - \mathbf{e}_i - \mathbf{e}_j$, where the subtraction is defined component-wise. Then $\mathbf{m}$, $\mathbf{a}$, $\mathbf{a}'$, and $\mathbf{b}$ are all canonical. Then define $K' = R(\mathbf{b}) \cup T(\mathbf{m})$, so K' is another irregular characteristic subgroup below $\mathbf{m}$. Since $R(\mathbf{a})$, K', and $R(\mathbf{a}')$ are distinct index 2 subgroups of $R(\mathbf{m})$ and each contains $R(\mathbf{b})$ as an index 2 subgroup, it follows that $R(\mathbf{b}), R(\mathbf{a}), K', R(\mathbf{a}')$, and $R(\mathbf{m})$ form a diamond:



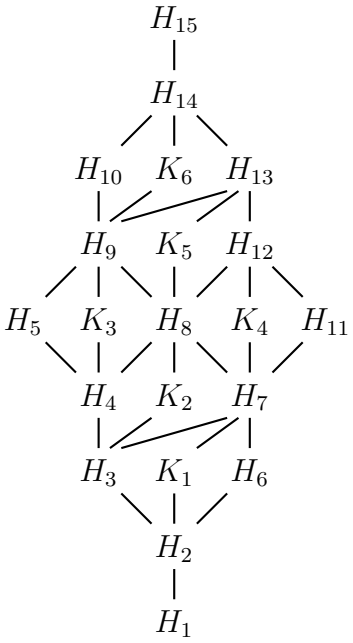
Thus, Char(G) is not distributive. □

The following example shows that it is possible for an abelian 2-group not to have any irregular characteristic subgroups, even if its lattice of characteristic subgroups is not a chain:

Example 5.26. Let $G = Z_2 \times Z_2 \times Z_8$. Then every canonical tuple $\mathbf{a} \in \mathcal{C}(G)$ can be written (a_1, a_1, a_3), i.e., the first two coordinates are forced to be identical. Consequently both the first and second coordinates are degenerate. So $\mathbf{a}$ has at most one nondegenerate coordinate, which by Corollary 5.17 implies that there are no irregular characteristic subgroups in G. The lattice of characteristic subgroups of G is then isomorphic to that of $Z_p \times Z_{p^3}$ for an odd prime p, shown in Table 3. This example shows that Theorem 5.11 does not hold for $p = 2$.

Table 9: Characteristic subgroups of $G = Z_4 \times Z_{64}$

H_1	$R(0,0)$
H_2	$R(0,1)$
H_3	$R(0,2)$
H_4	$R(0,3)$
H_5	$R(0,4)$
H_6	$R(1,1)$
H_7	$R(1,2)$
H_8	$R(1,3)$
H_9	$R(1,4)$
H_{10}	$R(1,5)$
H_{11}	$R(2,2)$
H_{12}	$R(2,3)$
H_{13}	$R(2,4)$
H_{14}	$R(2,5)$
H_{15}	$R(2,6)$
K_1	$R(0,1) \cup T(1,2)$
K_2	$R(0,2) \cup T(1,3)$
K_3	$R(0,3) \cup T(1,4)$
K_4	$R(1,2) \cup T(2,3)$
K_5	$R(1,3) \cup T(2,4)$
K_6	$R(1,4) \cup T(2,5)$



Example 5.27. Let $G = Z_4 \times Z_{64}$. Let $H_1, \ldots, H_{15}$ be the regular characteristic subgroups of G as shown in Table 9, and let $O_1 \ldots, O_{15}$ be the corresponding automorphism classes. The S-ring $S = F\{1, \overline{\mathcal{O}_2} + \overline{\mathcal{O}_3}, \overline{\mathcal{O}_4} + \overline{\mathcal{O}_5} + \overline{\mathcal{O}_6} + \overline{\mathcal{O}_7} + \overline{\mathcal{O}_{11}} + \overline{\mathcal{O}_{13}}, \overline{\mathcal{O}_8} + \overline{\mathcal{O}_9} + \overline{\mathcal{O}_{12}}, \overline{\mathcal{O}_{10}} + \overline{\mathcal{O}_{14}} + \overline{\mathcal{O}_{15}}\}$, of dimension five, contains only four subgroups quantities (i.e., simple quantities $\overline{H}$ where H is a subgroup of G), namely, 1, $\overline{H_3}$, $\overline{H_{13}}$, and $\overline{G}$. Consequently S cannot be constructed as in Theorem 2.3.

Note that in the preceding example, $|G| = 2^8$. An exhaustive computer search reveals that over any abelian 2-group of order $\leq 2^7$ every rational S-ring *can* be constructed as in Theorem 2.3. The smallest order for which an abelian 2-group can have three regular characteristic subgroups of the same order is 2^8 (and there are two such groups of this order: $Z_4 \times Z_{64}$ and $Z_2 \times Z_4 \times Z_{32}$). It seems probable that this fact has something to do with example just given. One problem would be to explain

and generalize the constructions given in Examples 5.8 and 5.27 with the goal of, if possible, classifying all rational S-rings over abelian p-groups.

In connection with this, another example which should be considered is the following:

Example 5.28. Let $G = Z_p \times Z_{p^3} \times Z_{p^5}$ where p is any prime. Let $H_1, \ldots, H_{18}$ be the regular characteristic subgroups of G, as in Table 4. By direct computation, one can show using Corollary 1.8 that

$$S = F\{1, \overline{H}_5, \overline{H}_6 + \overline{H}_7 + \overline{H}_{12} + \overline{H}_{13}, \overline{H}_8 + \overline{H}_{11} + \overline{H}_{12} + \overline{H}_{13}, \overline{H}_{14}, \overline{G}\}$$

is an S-ring over G if and only if $p = 3$. It is of course also possible to present S in terms of its basic elements:

$$S = F\{1, \overline{O}_2+\overline{O}_3+\overline{O}_4+\overline{O}_5, \overline{O}_6+\overline{O}_7+\overline{O}_{14}, \overline{O}_{12}+\overline{O}_{13}, \overline{O}_8+\overline{O}_{10}+\overline{O}_{11}, \overline{O}_9+\overline{O}_{15}+\overline{O}_{16}+\overline{O}_{17}+\overline{O}_{18}\}$$

This example shows that choice of prime p can make a difference in determining whether a partition of automorphism classes of G is a Schur partition or not, and that it is not merely a question of whether $p = 2$. It seems that this G is the unique smallest group for which such behavior occurs; namely, we have checked that given an abelian p-group G_1 and an abelian q-group G_2, where $|G_1| \leq p^9$ and $|G_2| \leq q^9$ and $\lambda(G_1) = \lambda(G_2)$, if neither $\lambda(G_1)$ nor $\lambda(G_2)$ are (1,3,5) and neither p nor q are 2, then the rational S-rings of G_1 and G_2 are in one-to-one correspondence, at least if $p, q \leq 11$. In contrast, over this group G, there are 7281 rational S-rings if $p = 3$ but only 7089 if $p > 3$. There are $7281 - 7089 = 192$ examples of partitions which correspond to S-rings if and only if $p = 3$, and they can all be derived from the example S given above by applying some combination of the following two modifications, (1) by adding some subset of $\{\overline{H}_2, \overline{H}_3, \overline{H}_4, \overline{H}_3+\overline{H}_4, \overline{H}_{15}, \overline{H}_{16}, \overline{H}_{15}+\overline{H}_{16}, \overline{H}_{17}\}$ to the basis given for

S (there are 64 possible ways of doing this: 8 subsets of $\{\overline{H}_2, \overline{H}_3, \overline{H}_4, \overline{H}_3 + \overline{H}_4\}$ are possible, and, independently, 8 subsets of $\{H_{15}, \overline{H}_{16}, \overline{H}_{15} + \overline{H}_{16}, \overline{H}_{17}\}$ are possible), or (2) by permuting the basis elements according to the permutation,

$$(\overline{H}_8, \overline{H}_{12}, \overline{H}_{13})(\overline{H}_{11}, \overline{H}_7, \overline{H}_6)$$

consisting of two disjoint 3-cycles (This corresponds to a symmetry of the sublattice $\mathrm{Char}(G) - \{H_9, H_{10}\}$). When $p = 2$, there are 22797 rational S-rings over G; 7089 of the corresponding Schur partitions are in common with those obtained when $p = 3$, precisely the ones which are Schur partitions for $p = 5$.

G is also the smallest abelian p-group with a cube in its lattice of characteristic subgroups. It would seem that this has something to do with the occurrence of these seemingly "exceptional" rational S-rings whose general construction we do not fully understand.

6 Main Theorem

We now turn to our main result:

Theorem 6.1. (Main Theorem) *Let p be an odd prime. Every finite group can be represented as the automorphism group of a rational S-ring over an abelian p-group.*

The proof relies on three key ideas:

(1) Every group can be represented as the automorphism group of a distributive lattice,

(2) Every distributive lattice can be embedded in a boolean lattice, and

(3) The lattice of characteristic subgroups of the group $Z_p \times Z_{p^3} \times \cdots \times Z_{p^{2n-1}}$ contains a boolean sublattice of order 2^n.

The proof of the Main Theorem, in outline, goes as follows: Given a group G, using (1) we are able to find a distributive lattice with automorphism group isomorphic to G. By (2), this lattice may be embedded in a boolean lattice, which by (3) may in turn be embedded as a sublattice of the lattice of characteristic subgroups of an appropriate abelian p-group P. Finally, using Theorem 2.3, we construct the rational S-ring over P associated with this lattice and show that the automorphism group of this S-ring is isomorphic to G.

(1) was shown by Birkhoff in [2]; alternative proofs are given in [9, 10] (see also [8]). (2) is a standard result in lattice theory (also first proven by Birkhoff; see also Theorem 5.12 in [6], 20.1 in [11], or 11.3 in [5]). We have already shown (3) in Theorem 5.10 above.

Since the proof of the Main Theorem will require some knowledge of the construction used in (2), we include a proof of (2) below (Theorem 6.6). For completeness, we also include a proof of (1) in Theorem 7.5.

In the following theorem we gather together some standard facts about lattices which we will need; the proof is entirely straightforward and will be omitted.

Theorem 6.2. *Let x, y, and z be elements of a lattice $\mathcal{L}$. Then*

(i) $x \wedge x = x$ *and* $x \vee x = x$ *(Idempotence)*

(ii) $x \wedge y = y \wedge x$ *and* $x \vee y = y \vee x$ *(Commutativity)*

(iii) $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ *and* $x \vee (y \vee z) = (x \vee y) \vee z$ *(Associativity)*

(iv) $x \leq y \iff x \wedge y = x \iff x \vee y = y$

The following elementary fact will also be useful:

Lemma 6.3. *Let x,y,z, and w be elements of a lattice $\mathcal{L}$ where $x \leq y$ and $z \leq w$. Then*

(i) $x \wedge z \leq y \wedge w$

(ii) $x \vee z \leq y \vee w$

Proof. By Theorem 6.2(ii,iii,iv) we have

$$(x \wedge z) \wedge (y \wedge w) = (x \wedge y) \wedge (z \wedge w) = x \wedge z$$

which, by another application of Theorem 6.2(iv), proves (i). (ii) is proved dually. □

Definition 6.4. An element j of a lattice $\mathcal{L}$ is said to be *join-reducible* if there exist $x < j$ and $y < j$ with $j = x \vee y$. Otherwise j is said to be *join-irreducible*.

Note that if j is join-irreducible and $j = x \vee y$ for some $x, y \in \mathcal{L}$, then either $j = x$ or $j = y$, since certainly $x \leq x \vee y = j$ and $y \leq x \vee y = j$ and strict inequality cannot occur in both places.

Lemma 6.5. *Let x, y, and j be elements of a distributive lattice $\mathcal{L}$ and let j be join-irreducible. Then*

$$j \leq x \wedge y \iff j \leq x \text{ and } j \leq y$$
$$j \leq x \vee y \iff j \leq x \text{ or } j \leq y$$

Proof. Since $x \wedge y \leq x$ and $x \wedge y \leq y$, it is clear that if $j \leq x \wedge y$ then $j \leq x$ and $j \leq y$. Conversely, if $j \leq x$ and $j \leq y$ then by Lemma 6.3, $j \wedge j \leq x \wedge y$, i.e., $j \leq x \wedge y$.

Since $x \leq x \vee y$ and $y \leq x \vee y$, it is clear that if $j \leq x$ or $j \leq y$ then $j \leq x \vee y$. (Note, to this point we have used neither the join-irreducibility of j nor the distributivity of $\mathcal{L}$.) Suppose conversely that $j \leq x \vee y$. Then

$$j = j \wedge (x \vee y) = (j \wedge x) \vee (j \wedge y).$$

The join-irreducibility of j then implies either $j = j \wedge x$ or $j = j \wedge y$, i.e. either $j \leq x$ or $j \leq y$, as desired. $\square$

Theorem 6.6. *Let $\mathcal{L}$ be a finite distributive lattice and let $J \subseteq \mathcal{L}$ be the set of join-irreducible elements. Then the map $\phi(x) = \{j \in J : j \leq x\}$ is a embedding of $\mathcal{L}$ into $\mathcal{P}(J)$. Moreover, $|\phi(\alpha(x))| = |\phi(x)|$ for all $\alpha \in \mathrm{Aut}(\mathcal{L})$ and $x \in \mathcal{L}$.*

Proof. Let $x, y \in \mathcal{L}$ be given. By Lemma 6.5 we have

$$\begin{aligned}
\phi(x \wedge y) &= \{j : j \in J, j \leq x \wedge y\} \\
&= \{j \in J : j \leq x \text{ and } j \leq y\} \\
&= \{j \in J : j \leq x\} \cap \{j \in J : j \leq y\} \\
&= \phi(x) \cap \phi(y)
\end{aligned}$$

and similarly $\phi(x \vee y) = \phi(x) \cup \phi(y)$, which proves that ϕ is a lattice homomorphism. It only remains to show that ϕ is injective.

So assume $x \neq y$ and we will show that $\phi(x) \neq \phi(y)$. Since $x \neq y$, either $x \not\leq y$ or $y \not\leq x$; without loss of generality, assume $x \not\leq y$. Let $S = \{z \in \mathcal{L} : z \leq x \text{ and } z \not\leq y\}$. Note that S is nonempty since $x \in S$. So S has a minimal element j. We will show that j is join-irreducible. For suppose $j = a \vee b$ but $a < j$ and $b < j$. By the minimality of j, $a, b \notin S$. However, $a < j \leq x$ and $b < j \leq x$, so we must have $a \leq y$ and $b \leq y$. But then $j = a \vee b \leq y \vee y = y$ by Lemma 6.3(ii), contradicting $j \in S$. Thus j is join-irreducible. By construction $j \in \phi(x)$ but $j \notin \phi(y)$. So, as desired, $\phi(x) \neq \phi(y)$.

To prove the last statement, note that lattice automorphisms map join-irreducible

elements to join-irreducible elements, i.e., $\alpha(J) = J$, so that

$$\begin{aligned}\phi(\alpha(x)) &= \{j \in J : j \leq \alpha(x)\} \\ &= \{\alpha(j) \in J : \alpha(j) \leq \alpha(x)\} \\ &= \{\alpha(j) \in J : j \leq x\} \\ &= \alpha(\phi(x)),\end{aligned}$$

hence $|\phi(\alpha(x))| = |\phi(x)|$. □

A version of the following lemma appears in [15, Lemma 3.3].

Lemma 6.7. *Let G be a group and let $x \in FG$ be a nonzero element of the group algebra. Then $x = \overline{H}$ for some subgroup $H \in G$ if and only if $x \circ x = x$ and $x^2 = cx$ for some $c \in F$. In this case, $c = |H|$.*

Proof. The necessity is obvious, so assume conversely that $x \circ x = x$ and $x^2 = cx$. Write $x = \sum_{g \in G} c_g g$. By comparing the coefficients of g in $x \circ x = x$ we have ${c_g}^2 = c_g$ for all $g \in G$, so that each c_g is either 0 or 1. Thus $x = \overline{H}$ for some subset $H \subseteq G$. The condition $x^2 = cx$ ensures that H is closed under multiplication. Since $x \neq 0$ implies $H \neq \emptyset$, it follows that H is a subgroup of G. □

Corollary 6.8. *Let S_1 and S_2 be S-rings over groups G_1 and G_2 respectively, let H be a subgroup of G_1, and let $\phi : S_1 \to S_2$ be an S-ring isomorphism. Then*

(i) $\phi(\overline{H}) = \overline{K}$ for some subgroup $K \leq G_2$. Moreover $|H| = |K|$.

(ii) If $G_1 = G_2 = Z_n$, then $\phi(\overline{H}) = \overline{H}$.

Proof. We have $\overline{H} \circ \overline{H} = \overline{H}$ and $\overline{H}^2 = c\overline{H}$ where $c = |H|$. Thus

$$\phi(\overline{H}) \circ \phi(\overline{H}) = \phi(\overline{H} \circ \overline{H}) = \phi(\overline{H})$$

and

$$\phi(\overline{H})\phi(\overline{H}) = \phi(\overline{H}^2) = \phi(c\overline{H}) = c\phi(\overline{H}),$$

so by Lemma 6.7, we may write $\phi(\overline{H}) = \overline{K}$ where K is a subgroup of G_2 of order $c = |H|$. Claim (ii) follows since in Z_n, H is the unique subgroup of order $|H|$. $\square$

Now we are able to prove the Main Theorem. Given a finite group G, by Birkhoff's theorem (Theorem 7.5 below) there is a finite distributive lattice $\mathcal{D}$ with $\mathrm{Aut}(D) \cong G$. By Theorem 6.6, there is an embedding ϕ of $\mathcal{D}$ into the boolean lattice $\mathcal{P}(J)$, where J is the set of join-irreducible elements of $\mathcal{D}$. In turn, by Theorem 5.10, there is an embedding ψ of $\mathcal{P}(J)$ into the lattice of characteristic subgroups $\mathrm{Char}(P)$ of an appropriate abelian p-group P. Let $\mathcal{L} = \psi(\phi(D)) \cup \{1\} \cup \{P\}$. We claim that $\mathrm{Aut}(F(\mathcal{L})) \cong G$.

It suffices to show $\mathrm{Aut}(\mathcal{D}) \cong \mathrm{Aut}(F(\mathcal{L}))$. Let α be any automorphism of the lattice $\mathcal{D}$. Then α corresponds to an automorphism β of the lattice $\mathcal{L}$ where $\beta = \psi \circ \phi \circ \alpha \circ \phi^{-1} \circ \psi^{-1}$ on $\psi(\phi(\mathcal{D}))$ and $\beta(1) = 1$ and $\beta(P) = P$. The proof will be complete once we show that β induces a (strong) automorphism of $F(\mathcal{L})$ and that every automorphism of $F(\mathcal{L})$ arises in this way.

Certainly β induces an F-linear map β' from $F(\mathcal{L})$ into the group algebra FP, by defining $\beta'(\overline{H}) = \overline{\beta(H)}$ and extending linearly (i.e., $\beta'(\sum_{H\in\mathcal{L}} c_H\overline{H}) = \sum_{H\in\mathcal{L}} c_H\overline{\beta(H)}$). Since β' then permutes the basis elements $\overline{H}$ of $F(\mathcal{L})$ it follows that β' is a vector space isomorphism of $F(\mathcal{L})$ onto itself. For any $H, K \in \mathcal{L}$, we have

$$\begin{aligned}\beta'(\overline{H} \circ \overline{K}) &= \beta'(\overline{H \cap K}) = \overline{\beta(H \cap K)} \\ &= \overline{\beta(H) \cap \beta(K)} = \overline{\beta(H)} \circ \overline{\beta(K)} = \beta'(\overline{H}) \circ \beta'(\overline{K})\end{aligned}$$

so β' preserves the Hadamard product.

Now we show that for all $H \in \mathcal{L}$, $|\beta(H)| = |H|$. For $H = 1$ or $H = P$ this is

trivially true since in these cases $\beta(H) = H$ by definition. For any other H, we have $\beta(H) = (\psi \circ \phi \circ \alpha \circ \phi^{-1} \circ \psi^{-1})(H)$. Let $x = (\phi^{-1} \circ \psi^{-1})(H)$, so $x \in \mathcal{D}$. Showing $|\beta(H)| = |H|$ then amounts to showing $|\psi(\phi(\alpha(x)))| = |\psi(\phi(x))|$. By Theorem 5.10 this equation is equivalent to $|\phi(\alpha(x))| = |\phi(x)|$, which in turn holds by Theorem 6.6. So we have proven $|\beta(H)| = |H|$ for all $H \in \mathcal{L}$. In particular, for any $H, K \in \mathcal{L}$, we have $|H \cap K| = |\beta(H \cap K)| = |\beta(H) \cap \beta(K)|$. Thus,

$$\begin{aligned}\beta'(\overline{H}\ \overline{K}) &= \beta'(|H \cap K|\overline{\langle H, K\rangle}) = |H \cap K|\overline{\beta(\langle H, K\rangle)} = |H \cap K|\overline{\langle \beta(H), \beta(K)\rangle} \\ &= |\beta(H) \cap \beta(K)|\overline{\langle \beta(H), \beta(K)\rangle} = \overline{\beta(H)}\ \overline{\beta(K)} = \beta'(\overline{H})\beta'(\overline{K})\end{aligned}$$

so that β' is an S-ring automorphism of $F(\mathcal{L})$, as desired.

Conversely, suppose β' is any S-ring automorphism of $S(\mathcal{L})$. For any $H \in \mathcal{L}$, we have $\beta'(\overline{H}) = \overline{K}$ for some subgroup $K \leq G$ by Corollary 6.8(i). Since $F(\mathcal{L})$ is a rational S-ring, K is necessarily characteristic. By the linear independence of characteristic subgroups (Corollary 5.7), we must have $K \in \mathcal{L}$. Thus β' permutes the basis elements $\{\overline{H} : H \in \mathcal{L}\}$ of $F(\mathcal{L})$. We can then define a bijection $\beta : \mathcal{L} \to \mathcal{L}$ by setting $\beta(H) = K$ where K is the subgroup of G such that $\beta'(\overline{H}) = \overline{K}$, so that $\overline{\beta(H)} = \beta'(\overline{H})$ for all $H \in \mathcal{L}$. Theorem 2.3 then implies

$$\begin{aligned}\overline{\beta(H \cap K)} &= \beta'(\overline{H \cap K}) = \beta'(\overline{H} \circ \overline{K}) \\ &= \beta'(\overline{H}) \circ \beta'(\overline{K}) = \overline{\beta(H)} \circ \overline{\beta(K)} = \overline{\beta(H) \cap \beta(K)}\end{aligned}$$

so that $\beta(H \cap K) = \beta(H) \cap \beta(K)$. Since Corollary 6.8(i) implies $|H \cap K| = |\beta(H \cap K)| = |\beta(H) \cap \beta(K)|$, Theorem 2.3 similarly implies

$$\begin{aligned}\overline{\beta(\langle H, K\rangle)} &= \beta'(\overline{\langle H, K\rangle}) = \beta'\left(\frac{1}{|H \cap K|}\overline{H}\ \overline{K}\right) = \frac{1}{|H \cap K|}\beta'(\overline{H})\beta'(\overline{K}) \\ &= \frac{1}{|H \cap K|}\overline{\beta(H)}\ \overline{\beta(K)} = \frac{1}{|\beta(H) \cap \beta(K)|}\overline{\beta(H)}\ \overline{\beta(K)} = \overline{\langle \beta(H), \beta(K)\rangle}\end{aligned}$$

so that $\beta(\langle H, K\rangle) = \langle \beta(H), \beta(K)\rangle$. This proves that β is a lattice automorphism of $\mathcal{L}$. It is then clear that β corresponds to a lattice automorphism α of $\mathcal{D}$ where $\alpha = \phi^{-1} \circ \psi^{-1} \circ \beta \circ \psi \circ \phi$, and that β' is the S-ring automorphism induced by α in the manner described above. This completes the proof.

7 Proof of Birkhoff's Theorem

In this section, we prove that every group G may be represented as the automorphism group of a distributive lattice. We essentially follow Birkhoff's original construction (as in [2]), albeit in somewhat different terms. We follow Birkhoff's proof because it is more elementary than the other proofs and because, to our knowledge, Birkhoff's construction has never before appeared in English. Although we are concerned only with the finite case, the interested reader will find the proofs not difficult to generalize to the infinite case, using the well-ordering principle.

Given a group G, the idea is to first find a poset with automorphism group isomorphic to G. We then show that every poset gives rise to a related distributive lattice with automorphism group isomorphic to that of the poset.

Theorem 7.1. *Let G be a group of order n. Then there is a partially ordered set X of order $n^2 + n$ such that* $\mathrm{Aut}(X) \cong G$.

Proof. Write $G = \{g_1, \ldots, g_n\}$, where $g_1 = 1$. Define X to be the disjoint union $X = G \cup (G \times G)$. Define the partial order on X by the following covering relation:

$$g > (hg, h), \text{ for all } g, h \in G \tag{1}$$

$$(g, g_i) > (g, g_{i+1}), \text{ for all } g \in G, i \in \{1, \ldots, n-1\} \tag{2}$$

It is easy to see that this determines a well-defined partial order in which the elements

(g, g_1) and (h, g_2) are comparable if and only if $g = h$. It is easy to see that the maps

$$\phi_a : g \mapsto ga, (g, g_i) \mapsto (ga, g_i)$$

are bijections on X which preserve (1) and (2), hence are automorphisms of X. The map $a \mapsto \phi_a$ is an injective homomorphism of G into $\mathrm{Aut}(X)$. If we can show that this map is surjective, the proof will be complete. This amounts to showing that every automorphism of X has the form ϕ_a for some a. So let ϕ be an arbitrary automorphism of X. For every $g \in G$, we have a chain in X of the maximum length possible (namely, n):

$$g > (g, g_1) > (g, g_2) > \cdots > (g, g_n) \tag{3}$$

hence

$$\phi(g) > \phi(g, g_1) > \phi(g, g_2) > \cdots > \phi(g, g_n)$$

is another maximum-length chain of X. Since every maximum-length chain has the form (3), it follows that $\phi(g, g_i) = (\phi(g), g_i)$ for all $g \in G$ and $i \in \{1, \ldots, n\}$. Now, set $a = \phi(1)$. If we can show $\phi(g) = ga$ for all $g \in G$, it will follow that $\phi = \phi_a$, completing the proof. To do this, we note that, among the elements of the chain $\{(1, g_i) : i \in \{1, \ldots, n\}\}$, the greatest element which is below g is $(1, g^{-1})$ (by (1), taking $h = g^{-1}$). It follows that, among the elements of the chain $\{\phi(1, g_i) : i \in \{1, \ldots, n\}\} = \{(a, g_i) : i \in \{1, \ldots, n\}\}$, the greatest element which is below $\phi(g)$ is $\phi(1, g^{-1}) = (a, g^{-1})$. But by (1) the greatest element below $\phi(g)$ in the chain $\{(a, g_i) : i \in \{1, \ldots, n\}\}$ is $(a, a\phi(g)^{-1})$. Thus we have $g^{-1} = a\phi(g)^{-1}$, hence $\phi(g) = ga$, as desired. □

Definition 7.2. A subset D of a poset X is called a *down-set* if for every $d \in D$ and $x \in X$, $x \leq d$ implies $x \in D$. The set of down-sets of a poset X is denoted $\mathcal{O}(X)$.

Clearly, the set of down-sets $\mathcal{O}(X)$ of a poset forms a lattice, with meet and join given by set intersection and union respectively. $\mathcal{O}(X)$ is distributive since it is a sublattice of $\mathcal{P}(X)$.

Definition 7.3. Given an element y of a poset X, the set $\{x \in X : x \leq y\}$ is called the *principal down-set* below y and is denoted $y^{\downarrow}$.

Theorem 7.4. *Let X be any finite poset. Then* $\mathrm{Aut}(\mathcal{O}(X)) \cong \mathrm{Aut}(X)$.

Proof. Every automorphism $\phi \in \mathrm{Aut}(X)$ induces a map ϕ' on $\mathcal{O}(X)$ by defining $\phi'(D) = \{\phi(d) : d \in D\}$. Given $\phi(d) \in \phi'(D)$ and $x \in X$ with $x \leq \phi(d)$, we have $\phi^{-1}(x) \leq d$ (since ϕ, hence ϕ^{-1}, is order-preserving), so $\phi^{-1}(x) \in D$, hence $x \in \phi(D)$, which shows $\phi(D)$ is a down-set, i.e. $\phi(D) \in \mathcal{O}(X)$. Now it is clear that $\phi' : \mathcal{O}(x) \to \mathcal{O}(X)$ is bijective with inverse given by $(\phi^{-1})'$. Since ϕ' is clearly order-preserving, it follows that $\phi' \in \mathrm{Aut}(\mathcal{O}(X))$. The correspondence $\phi \mapsto \phi'$ is then an homomorphism of $\mathrm{Aut}(X)$ into $\mathrm{Aut}(\mathcal{O}(X))$. Since $\phi'(x^{\downarrow}) = \phi(x)^{\downarrow}$, it follows that this correspondence is injective (for if $\phi_1' = \phi_2'$ then for all $x \in X$ we have $\phi_1'(x^{\downarrow}) = \phi_2'(x^{\downarrow})$, thus $\phi_1(x)^{\downarrow} = \phi_2(x)^{\downarrow}$, from which it follows that $\phi_1(x) = \phi_2(x)$ for all $x \in X$, so $\phi_1 = \phi_2$). The proof will be complete once we show this correspondence is surjective.

So let $\hat{\phi} \in \mathrm{Aut}(\mathcal{O}(X))$ be given. We will show there is a $\phi \in \mathrm{Aut}(X)$ such that $\hat{\phi} = \phi'$. Now $\hat{\phi}$ permutes the principal down-sets of X among themselves (for a down-set is principal if and only if it has a maximum element, and if down-set D has a maximum element then its image $\phi(D)$ does as well, since D and $\phi(D)$ are isomorphic posets). Hence we have that for any $x \in X$, there is a unique $y \in X$ with $\hat{\phi}(x^{\downarrow}) = y^{\downarrow}$, namely $y = \max(\phi(x^{\downarrow}))$. So we may define a bijection $\phi : X \to X$ by $\phi(x) = y$, where y is given by $\hat{\phi}(x^{\downarrow}) = y^{\downarrow}$. Now if $x \leq y$, then $x^{\downarrow} \subseteq y^{\downarrow}$, so $\hat{\phi}(x^{\downarrow}) \subseteq \hat{\phi}(y^{\downarrow})$, hence $\phi(x) \leq \phi(y)$. Thus ϕ is order-preserving, so $\phi \in \mathrm{Aut}(X)$. Since $\phi'(x^{\downarrow}) = \{\phi(z) : z \leq x\} = \{\phi(z) : \phi(z) \leq \phi(x)\} = \{x : x \leq y\} = y^{\downarrow}$, we have that

$\phi'(x^{\downarrow}) = \hat{\phi}(x^{\downarrow})$ for all $x \in X$, so ϕ' and $\hat{\phi}$ agree on principal down-sets. Now, since down-set $D \in \mathcal{O}(X)$ may be written $D = \cup_{x \in D} x^{\downarrow}$, we have $\hat{\phi}(D) = \hat{\phi}(\cup_{x \in D} x^{\downarrow}) = \cup_{x \in D} \hat{\phi}(x^{\downarrow}) = \cup_{x \in D} \phi'(x^{\downarrow}) = \phi'(\cup_{x \in D} x^{\downarrow}) = \phi'(D)$, so $\hat{\phi} = \phi'$, as desired. □

Remark. This correspondence between posets and distributive lattices given by $X \mapsto \mathcal{O}(X)$ is in fact invertible. Given a finite distributive lattice $\mathcal{L}$, the poset X of join-irreducible elements of $\mathcal{L}$ satisfies $\mathcal{O}(X) \cong \mathcal{L}$ (This is a strengthening of Theorem 6.6). This correspondence may be used to show that finite posets and finite distributive lattices (with an appropriate definition of morphisms) are in fact dual categories. Similar results can be obtained for infinite posets and lattices, although the correspondence is somewhat more complicated. For details, see [6, Theorem 5.19].

Theorem 7.5. *Let G be a finite group. Then there is a distributive lattice $\mathcal{L}$ of order no more than 2^{n^2+n} such that* $\mathrm{Aut}(\mathcal{L}) \cong G$.

Proof. This follows immediately from Theorem 7.4, taking $\mathcal{L} = \mathcal{O}(X)$ where X is as in Theorem 7.1. □

Note that in this construction, $\mathcal{L} = \mathcal{O}(X)$ is already a sublattice of a boolean lattice $\mathcal{P}(X)$, which essentially eliminates our dependence on Theorem 6.6 in the proof of the Main Theorem.

8 Automorphisms of S-rings over cyclic groups

In this section, we assume F has characteristic zero.

In [12], Leung and Man give a recursive classification of all S-rings over cyclic groups. We give a brief description of this classification without proof. They give three basic methods of constructing S-rings over a group G:

(I) Given a subgroup $\Omega \leq \mathrm{Aut}(G)$, let $T_1, \ldots, T_n$ be the orbits of Ω acting on G. Then $T_1, \ldots, T_n$ form a Schur partition of G.

(II) Suppose $G = H \times K$ for nontrivial subgroups $H, K \leq G$, and suppose S_H is an S-ring over H with basic sets $C_1, \ldots, C_h$ and S_K is an S-ring over K with basic sets $D_1, \ldots, D_k$. Then the product sets $C_i D_j$, $1 \leq i \leq h, 1 \leq j \leq k$, form a Schur partition of G.

(III) Suppose H and K are nontrivial, proper subgroups of G with $H \leq K$ and $H \trianglelefteq G$, and let S_K be an S-ring over K with basic sets $C_1, \ldots, C_k$ and $S_{G/H}$ be an S-ring over G/H with basic sets $D_1, \ldots, D_k$, and suppose that $\pi(S_K) = F(K/H) \cap S_{G/H}$, where $\pi : G \to G/H$ is the natural projection map, extended to a natural projection map of the group algebra FG onto $F(G/H)$. Then

$$G = C_1 \cup \cdots \cup C_k \cup \{\pi^{-1}(D_i) : i \in \{1, \ldots, k\}, D_i \nsubseteq K/H\}$$

forms a Schur partition of G.

The S-ring constructed in (II) is denoted $S_H \cdot S_K$ and is called the *dot product* of S_H and S_K. The S-ring constructed in (III) is denoted $S_K \wedge S_{G/H}$ and is called the *wedge product* of S_K and $S_{G/H}$. We call an S-ring type (I), (II), or (III) if it can be constructed as in (I), (II), or (III), respectively. The main theorem of Leung and Man ([12, Theorem 3.7]) may then be stated:

Theorem 8.1. *Every nontrivial S-ring over a cyclic group G is type (I), (II), or (III).*

We give a couple of examples of these constructions:

Example 8.2. Over $G = Z_6 = \langle t \rangle$, the S-ring $F\{1, t + t^5, t^2 + t^4, t^3\}$ is type (I) with $\Omega = \langle \phi_{-1} \rangle$ where $\phi_{-1} \in \mathrm{Aut}(G)$ is defined by $\phi_{-1} : t \mapsto t^{-1}$. It is also type (II) with $H = \langle t^2 \rangle$, $K = \langle t^3 \rangle$, $S_H = F\{1, t^2 + t^4\}$ and $S_K = F\{1, t^3\}$.

Example 8.3. Over the same group, $F\{1, t^2, t^4, t + t^3 + t^5\}$ is a type (III) S-ring with $H = K = \langle t^2 \rangle$, $S_K = \{1, t^2, t^4\}$ and $S_{G/K} = \{1, tK\}$.

Note that the constructions (I), (II), and (III) can be used to produce S-rings over an arbitrary group G, but if G is not cyclic then it is not necessarily true that all S-rings can be constructed using these methods.

Theorem 8.4. *Let p be a prime with $p \geq 5$. Then there are S-rings over $Z_p \times Z_p$ which are not type (I), (II), or (III).*

Proof. Let $H_1, \ldots, H_{p+1}$ be the subgroups of $G = Z_p \times Z_p$ of order p, and define $C_i = H_i - \{1\}$ for $i \in \{1, \ldots, p+1\}$, so that the sets $C_1, \ldots, C_{p+1}$ partition the nonidentity elements of the group G. We claim that any partition $\{1\}, T_1, \ldots, T_r$ of G, where each T_i is a union of some C_j's, forms a Schur partition of G. So let $S = F\{1, \overline{T}_1, \ldots, \overline{T}_r\}$. Conditions (ii) and (iii) of an S-ring are clearly satisfied. To check condition (i), we observe that since $H_i \cap H_j = 1$ for $i \neq j$, we have in this case $\overline{H}_i\overline{H}_j = \overline{G}$. So, if we write $T_i = \bigcup_{k=1}^{n_i} C_{ik}$, where each $C_{ik} \in \{C_1, \ldots, C_{p+1}\}$, applying Theorem 2.3(iii) we find that for $i \neq j$

$$\begin{aligned}
\overline{T}_i\overline{T}_j &= \left(\sum_{k=1}^{n_i} \overline{C}_{ik}\right)\left(\sum_{k=1}^{n_j} \overline{C}_{jk}\right) \\
&= \left(\sum_{k=1}^{n_i} \overline{H}_{ik} - 1\right)\left(\sum_{k=1}^{n_j} \overline{H}_{jk} - 1\right) \\
&= \left(\sum_{k=1}^{n_i}\sum_{l=1}^{n_j} \overline{H}_{ik}\overline{H}_{jl}\right) - \overline{T}_i - \overline{T}_j + 1 \\
&= n_i n_j \overline{G} - \overline{T}_i - \overline{T}_j + 1 \in S,
\end{aligned}$$

while likewise

$$\begin{aligned}
\overline{T}_i\overline{T}_i &= \left(\sum_{k=1}^{n_i}\sum_{l=1}^{n_i}\overline{H}_{ik}\overline{H}_{il}\right) - 2\overline{T}_i + 1 \\
&= \sum_{k=1}^{n_i}\sum_{l\neq k}\overline{H}_{ik}\overline{H}_{il} + \sum_{k=1}^{n_i}\overline{H}_{ik}\overline{H}_{ik} - 2\overline{T}_i + 1 \\
&= n_1(n_1-1)\overline{G} + \sum_{k=1}^{n_i} p\overline{H}_{ik} - 2\overline{T}_i + 1 \\
&= n_1(n_1-1)\overline{G} + (p-2)\overline{T}_i + 1 \in S,
\end{aligned}$$

which proves that S is an S-ring.

Up to this point we have described a general method of constructing certain S-rings over $Z_p \times Z_p$ for any prime p. We now show that when $p \geq 5$, this method can be used to construct an S-ring which is not type (I), (II), or (III). We will consider G as a two-dimensional vector space over $\mathbb{F}_p$. Choose a vector $x \in C_1$ and a vector $y \in C_2$. Then $x + y \in G - H_1 - H_2$; without loss of generality, $x + y \in C_3$. Now define an S-ring S on G given by the Schur partition $\{1\}, C_1, C_2, C_3, C_4 \cup \cdots \cup C_{p+1}$.

Suppose S is a type (I) S-ring with $\Omega \leq \mathrm{Aut}(G)$. Now we may identify $\mathrm{Aut}(G)$ with invertible $\mathbb{F}_p$-linear transformations on G. Then given any $\omega \in \Omega$, since C_1 and C_2 are orbits of Ω, we must have $\omega(x) = ax$ and $\omega(y) = by$ for some $a, b \in \mathbb{F}_p^\times$. So with respect to the basis x, y, the matrix of ω is $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$. Moreover, since C_3 is an orbit of Ω, we must have $\omega(x+y) = c(x+y)$ for some $c \in \mathbb{F}_p^\times$. Since we also have $\omega(x+y) = \omega(x) + \omega(y) = ax + by$, this implies $a = b = c$. So Ω consists only of scalar matrices, of which there are only $p-1$. This means that each orbit of Ω has size no greater than $p-1$. But this is a contradiction since $|C_4 \cup \cdots \cup C_{p+1}| = (p-2)(p-1) > p-1$ for $p \geq 5$. So S is not type (I).

Since S has a prime number of basic sets (namely, 5), S cannot be a type (II) S-ring. Suppose S were a type (III) S-ring for proper,nontrivial subgroups $H \leq K$

of G. We must have $|H| = |K| = 5$, so in fact $H = K$. Then every basic set of S not contained in H must consist of a union of cosets of H, hence must have size a multiple of 5. Yet there are three basic sets C_1, C_2, C_3 of size 4 (not a multiple of 5); since it is impossible for all of these to be contained in H, this is a contradiction. So S is not type (III). □

Remark. For $p = 2$ and $p = 3$, exhaustive enumeration shows that all S-rings over $Z_p \times Z_p$ are type (I).

Example 8.5. A computer check shows that every S-ring over $Z_3 \times Z_3 \times Z_3$ is type (I). However, there are examples of S-rings over $G = Z_3 \times Z_3 \times Z_3 \times Z_3 = \langle a \rangle \times \langle b \rangle \times \langle c \rangle \times \langle d \rangle$ which are not type (I), (II), or (III). One is the S-ring with the following basic sets:

$$T_1 = \{1\}$$
$$T_2 = \{bcd^2, b, acd^2, bd^2, d, a^2bd^2, a^2b^2c^2d, abcd, b^2c^2d, bcd, ab^2, b^2c^2d^2,$$
$$b^2, a^2b^2c^2d^2, b^2cd, a^2c^2d, a^2, a, ab^2d, b^2d, bc^2d^2, a^2b, d^2, abcd^2\}$$
$$T_3 = G - T_1 - T_2$$

This example was found using MAGMA. By considering the sizes of the basic sets (1, 24, and 56), it is easy to see that this S-ring is primitive (i.e., there are no nontrivial proper subgroups H of G with $\overline{H}$ in the S-ring) and so is not type (II) or (III). An exhaustive computer search shows that it is also not type (I).

In general, the S-rings over abelian groups, even elementary abelian p-groups, are not well understood. One problem would be explain and generalize the construction given in the preceding example. Another question is the following, an affirmative answer to which we have verified by computer for Z_2^n, $n \leq 4$.

Question 8.6. Is every S-ring over an elementary-abelian 2-group of type (I)?

We now turn to the main result of this section:

Theorem 8.7. *If S is an S-ring over a cyclic group Z_n, then* $\mathrm{Aut}(S)$ *is abelian.*

Before proving this, we need a few elementary lemmas. A version of Lemma 8.8 can be found in [20, Theorem 23.9], while more general versions of Lemmas 8.9 and 8.10 can be found in [16, Propositions 3.1, 3.4 and the following Theorem 1.1′].

Lemma 8.8. *Suppose S is an S-ring over an abelian group G and m is an integer relatively prime to $|G|$. If $\overline{C} \in S$, then also $\overline{C}^{(m)} \in S$. Moreover, if $\overline{C}$ is a basic element of S then $\overline{C}^{(m)}$ is also a basic element of S.*

Proof. Since m may be written as a product of primes $m = p_1 \cdots p_k$ and $\overline{C}^{(m)} = (\cdots(\overline{C}^{(p_1)})^{(p_2)} \cdots)^{(p_k)}$, it is sufficient to prove the lemma in the case $m = p$ is prime. Now certainly $\overline{C}^p \in S$. If we write $C = \{c_1, \ldots, c_n\}$, then by the binomial theorem we have

$$\overline{C}^p = \left(\sum_{i=1}^{n} c_i\right)^p = \sum_{i=1}^{n} c_i^p + px = \overline{C}^{(p)} + px,$$

for some $x \in FG$. Now since p is relatively prime to $|G|$, the pth power map is a bijection on G, consequently $\overline{C}^{(p)} = \overline{C^{(p)}}$ is a simple quantity. So $\overline{C}^{(p)}$ has coefficients only 0 and 1; it particular, it has no nonzero coefficients which are multiples of p. Thus $\overline{C}^{(p)} \in S$ by Lemma 1.6.

Now assume $\overline{C}$ is a basic element of S and suppose $\overline{C}^{(p)}$ is not a basic element. Then we may write $\overline{C}^{(p)} = \overline{A} + \overline{B}$ for some disjoint nonempty subsets $A, B \subseteq G$ with $\overline{A}, \overline{B} \in S$. Let p' be the multiplicative inverse of p in $\mathbb{Z}/|G|\mathbb{Z}$. Then $\overline{C} = (\overline{C}^{(p)})^{(p')} = \overline{A}^{(p')} + \overline{B}^{(p')}$ where $A^{(p')}$ and $B^{(p')}$ are disjoint nonempty subsets of G with $\overline{A}^{(p')}, \overline{B}^{(p')} \in S$, contradicting that $\overline{C}$ is a basic element. □

Lemma 8.9. *Suppose S is an S-ring over an abelian group G and $\phi \in \mathrm{Aut}(S)$. Then for any simple quantity $\overline{C} \in S$ and any integer m relatively prime to $|G|$, we have $\phi(C^{(m)}) = \phi(C)^{(m)}$.*

Proof. Again, it is sufficient to prove the lemma in the case where $m = p$ is prime. As above, by the binomial theorem, $\overline{C}^p = \overline{C}^{(p)} + px$ for some $x \in FG$. Hence,

$$\begin{aligned}\phi(\overline{C}^{(p)}) &= \phi(\overline{C}^{(p)} + px - px) = \phi(\overline{C}^p) - p\phi(x) \\ &= \phi(\overline{C})^p - p\phi(x) = \overline{\phi(C)}^p - p\phi(x) \\ &= \overline{\phi(C)}^{(p)} + py - p\phi(x).\end{aligned}$$

for some $y \in FG$, by a second application of the binomial theorem. As above, $\overline{C}^{(p)}$ is a simple quantity. It follows by Theorem 3.7 that $\phi(\overline{C}^{(p)}) = \phi(\overline{C^{(p)}}) = \overline{\phi(C^{(p)})}$ is a simple quantity. Also, $\overline{\phi(C)}^{(p)}$ is a simple quantity. These elements then have coefficients only 0 and 1 (in particular, no nonzero multiple of p can occur as a coefficient), it follows that $py - p\phi(x) = 0$, hence $\phi(\overline{C}^{(p)}) = \phi(\overline{C})^{(p)}$, i.e., $\phi(C^{(m)}) = \phi(C)^{(m)}$, as desired. □

Lemma 8.10. *Suppose S is a type (I) S-ring over Z_n. Let ϕ be an automorphism of S. Then for any basic set T of S, there is an integer m relatively prime to n such that $\phi(T) = T^{(m)}$.*

Remark. This says that in a certain situation, any S-ring automorphism "locally" looks like a strong automorphism. Note that different values of m may be required for different basic sets T of S; for instance this occurs in Example 3.8.

Proof. Since all the elements of T are automorphic, they all have the same order d. If we consider Z_d as a subgroup of Z_n, then we have $\overline{Z}_d \circ \overline{T} = \overline{T}$, since $T \subseteq Z_d$. Now, by Corollary 6.8(ii), $\phi(\overline{Z}_d) = \overline{Z}_d$. So we have

$$\overline{Z}_d \circ \overline{\phi(T)} = \phi(\overline{Z}_d) \circ \phi(\overline{T}) = \phi(\overline{Z}_d \circ \overline{T}) = \phi(\overline{T}) = \overline{\phi(T)},$$

hence $\phi(T) \subseteq Z_d$. This implies $\phi(T) \subseteq Z_d$, so every element of $\phi(T)$ has order dividing

d. On the other hand, for any k properly dividing d, we have $\overline{Z}_k \circ T = 0$, hence

$$\overline{Z}_k \circ \overline{\phi(T)} = \phi(\overline{Z}_k) \circ \phi(\overline{T}) = \phi(\overline{Z}_k \circ \overline{T}) = \phi(0) = 0 \neq \overline{\phi(T)},$$

so that $\phi(T) \not\subseteq Z_k$. So, since all the elements of $\phi(T)$ have the same order (for $\phi(T)$ is a basic set), and this order divides d but not any proper divisor of d, it follows that all the elements of $\phi(T)$ have order d. So, by Lemma 4.2, there is an automorphism $\psi \in \mathrm{Aut}(Z_n)$ mapping some element of T to some element of $\phi(T)$, i.e., there is an m relatively prime to n such that $T^{(m)} \cap \phi(T) \neq \emptyset$. Since, by Lemma 8.8, $T^{(m)}$ and $\phi(T)$ are both basic sets, it follows that $T^{(m)} = \phi(T)$, as desired. □

Proof of Theorem 8.7. If S is a trivial S-ring, then $\mathrm{Aut}(S)$ is also trivial, hence abelian, and we are done. So first consider the case that S is type (I). Each basic set of S then consists of elements of the same order. Let $\mathcal{T}_d$ be the collection of basic sets of S containing elements of order d. We can consider $\mathrm{Aut}(S)$ as a permutation group acting on the basic sets of S, and by Lemma 8.10, for each d, $\mathrm{Aut}(S)$ permutes the basic sets of $\mathcal{T}_d$ among themselves. If we let A_d denote the restriction of $\mathrm{Aut}(S)$ to $\mathcal{T}_d$, then $\mathrm{Aut}(S)$ is a subdirect product of all the A_d's, so it suffices to show that each A_d is abelian. Fix a divisor d of n, and let T be a basic set in $\mathcal{T}_d$. For any k relatively prime to n, $T^{(k)}$ is another basic set of $\mathcal{T}_d$ by Lemma 8.8. By Lemma 4.2, every basic set of $\mathcal{T}_d$ has this form, for if T' is any basic set in $\mathcal{T}_d$, there is an integer l relatively prime to n such that $T^{(l)} \cap T' \neq \emptyset$, hence $T^{(l)} = T'$. Now, by Lemma 8.10, $\phi(T) = T^{(m)}$ for some m relatively prime to n. It follows by Lemma 8.9 that for any basic set $T^{(k)} \in \mathcal{T}_d$,

$$\phi(T^{(k)}) = \phi(T)^{(k)} = (T^{(m)})^{(k)} = (T^{(k)})^{(m)}.$$

Thus $\phi(T') = (T')^{(m)}$ for any basic set $T' \in \mathcal{T}_d$. From this it is evident that A_d is

abelian.

Now suppose $S = S_H \cdot S_K$ is type (II). By induction we may assume $\mathrm{Aut}(S_H)$ and $\mathrm{Aut}(S_K)$ are abelian. Let ϕ be an element of $\mathrm{Aut}(S)$. By Corollary 6.8(ii), $\phi(\overline{H}) = \overline{H}$ and $\phi(\overline{K}) = \overline{K}$. So $\phi(S_H)$ is an S-ring over H which is isomorphic to S_H. By Muzychuk's result cited above in Theorem 3.11, the only such S-ring is S_H itself, so we must have $\phi(S_H) = S_H$ and likewise $\phi(S_K) = S_K$. So $\phi|_{S_H} \in \mathrm{Aut}(S_H)$ and $\phi|_{S_K} \in \mathrm{Aut}(S_K)$. Given another automorphism $\psi \in \mathrm{Aut}(S)$, and any basic set CD of S, where C is a basic set of S_H and D is a basic set of S_K, we have $\phi(\psi(\overline{C})) = \psi(\phi(\overline{C}))$ and $\phi(\psi(\overline{D})) = \psi(\phi(\overline{D}))$ since $\mathrm{Aut}(S_H)$ and $\mathrm{Aut}(S_K)$ are abelian, hence

$$\begin{aligned}\phi(\psi(\overline{CD})) &= \phi(\psi(\overline{C}\ \overline{D})) = \phi(\psi(\overline{C})\psi(\overline{D})) = \phi(\psi(\overline{C}))\phi(\psi(\overline{D})) \\ &= \psi(\phi(\overline{C}))\psi(\phi(\overline{D})) = \psi(\phi(\overline{C})\phi(\overline{D})) = \psi(\phi(\overline{C}\ \overline{D})) = \psi(\phi(\overline{CD}))\end{aligned}$$

which proves that ϕ and ψ commute, so $\mathrm{Aut}(S)$ is abelian.

Finally suppose $S = S_K \wedge S_{G/H}$ is type (III). As above, given an automorphism $\phi \in \mathrm{Aut}(S)$, we have $\phi|_{S_K} \in \mathrm{Aut}(S_K)$. Now, the natural projection ϕ^* of ϕ to $S_{G/H}$, given by

$$\phi^*\Big(\sum_{gH \in G/H} r_{gH}(gH)\Big) = \sum_{gH \in G/H} r_{gH}(\phi(g)H),$$

is well-defined since, as above, $\phi(H) = H$. Moreover, by Theorem 3.4, it is easy to see that ϕ^* is an isomorphism of $S_{G/H}$ onto some S-ring over G/H. Since by 3.11 the only such S-ring is $S_{G/H}$ itself, it follows that $\phi^*(S_{G/H}) = S_{G/H}$, which means ϕ^* is an automorphism of $S_{G/H}$. Note that if we define $\pi : FG \to F(G/H)$, the natural

projection map, and $\pi' : F(G/H) \to FG$ by

$$\pi\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g(gH)$$
$$\pi'\left(\sum_{gH\in G/H} a_g(gH)\right) = \sum_{g\in G} a_g(g\overline{H}).$$

then for all $x \in F(G/H)$ we have

$$\pi(\pi'(x)) = |H|x$$

and an equivalent definition of ϕ^* is

$$\phi^*(x) = \frac{1}{|H|}(\pi \circ \phi \circ \pi')(x).$$

By induction we assume $\mathrm{Aut}(S_K)$ and $\mathrm{Aut}(S_{G/H})$ are abelian. Then, given another automorphism $\psi \in \mathrm{Aut}(S)$ and a basic set C of S, we have two cases: If $C \subseteq K$, then

$$\phi(\psi(\overline{C})) = \phi|_{S_K}(\psi|_{S_K}(\overline{C})) = \psi|_{S_K}(\phi|_{S_K}(\overline{C})) = \psi(\phi(\overline{C}))$$

and we are done. Suppose instead that $C \nsubseteq K$. Then C is a union of cosets of H, hence $\pi'(\pi(\overline{C})) = |H|\overline{C}$. Also, $\phi(C)$, $\psi(C)$, $\phi(\psi(C))$, and $\psi(\phi(C))$ are unions of cosets of H, hence

$$(\pi' \circ \pi \circ \phi)(\overline{C}) = \pi'(\pi(\overline{\phi(C)})) = |H|\overline{\phi(C)} = |H|\phi(\overline{C})$$

and likewise

$$(\pi' \circ \pi \circ \psi)(\overline{C}) = |H|\psi(\overline{C})$$
$$(\pi' \circ \pi \circ \phi \circ \psi)(\overline{C}) = |H|(\phi \circ \psi)(\overline{C})$$
$$(\pi' \circ \pi \circ \psi \circ \phi)(\overline{C}) = |H|(\psi \circ \phi)(\overline{C})$$

From all of this it follows that

$$\begin{aligned}(\phi \circ \psi)(\overline{C}) &= \frac{1}{|H|}(\pi' \circ \pi \circ \phi \circ \psi)(\overline{C}) = \frac{1}{|H|^2}(\pi' \circ \pi \circ \phi \circ \pi' \circ \pi \circ \psi)(\overline{C}) \\ &= \frac{1}{|H|^3}(\pi' \circ \pi \circ \phi \circ \pi' \circ \pi \circ \psi \circ \pi' \circ \pi)(\overline{C}) \\ &= \frac{1}{|H|}(\pi' \circ \phi^* \circ \psi^* \circ \pi)(\overline{C}) = \frac{1}{|H|}(\pi' \circ \psi^* \circ \phi^* \circ \pi)(\overline{C}) \\ &= \frac{1}{|H|^3}(\pi' \circ \pi \circ \psi \circ \pi' \circ \pi \circ \phi \circ \pi' \circ \pi)(\overline{C}) \\ &= \frac{1}{|H|^2}(\pi' \circ \pi \circ \psi \circ \pi' \circ \pi \circ \phi)(\overline{C}) = \frac{1}{|H|}(\pi' \circ \pi \circ \psi \circ \phi)(\overline{C}) = (\psi \circ \phi)(\overline{C}),\end{aligned}$$

so that ϕ and ψ commute, as desired. □

We observe that Theorem 8.7 is false if the field F (or more generally, the ring R) has finite characteristic:

Example 8.11. Let R have characteristic n. Set $G = Z_{4n} = \langle t \rangle$ and $H = Z_n \leq G$. Define S_H to be the S-ring $S = S_H \wedge S_{G/H}$ where S_H is the trivial S-ring over H and $S_{G/H}$ is the full group algebra $F(G/H)$. Then S has five basic sets

$$\{1\}, Z_p - \{1\}, T_1, T_2, T_3$$

where $T_i = t^i Z_n$. Then in RG we have $\overline{T}_i\overline{T}_j = nt^{i+j}\overline{Z}_n = 0$ for all $i, j \in \{1, 2, 3\}$ while $(\overline{Z}_n - 1)\overline{T}_i = -\overline{T}_i$. Thus $\mathrm{Aut}(S) \cong \mathrm{Sym}_3$ is non-abelian. Over a ring with characteristic zero, the same Schur partition gives an S-ring with automorphism group

isomorphic to Z_2.

A Appendix: MAGMA code

```
// Given a subset C of G, returns Aut(G)(C), i.e. the union of
// automorphism classes represented in C.
AutoClass := function(C,G);
  repeat
    oldC := C;
    for g in Generators(AutomorphismGroup(G)) do
      C := C join g(C);
    end for;
  until #oldC eq #C;
  return C;
end function;

// Returns a sequence of sets, the automorphism classes of a group G.
AutoClasses := function(G);
  classes := [ {G!1} ];
  H := Set(G) diff {G!1};
  while H ne {} do
    class := {Random(H)};
    class := AutoClass(class,G);
    classes := Append(classes,class);
    H := H diff class;
  end while;
  return classes;
end function;

// Given a collection 'classes' of subsets of G, returns the sequence of
// subgroups generated by any subcollection of 'classes'.
GenSubgroups := function(classes,G);
  cgroups := [];
  for c in classes do
    Include(~cgroups,sub<G | c>);
  end for;
  newgroups := Set(cgroups);
  repeat
    oldgroups := Set(cgroups);
    for c in newgroups do
      for d in cgroups do
        Include(~cgroups,sub<G | c,d>);
      end for;
    end for;
    newgroups := Set(cgroups) diff oldgroups;
  until newgroups eq {};
  return cgroups;
end function;
```

```
// Returns a sequence of all characteristic subgroups of G
CharSubgroups := function(G);
  return GenSubgroups(AutoClasses(G),G);
end function;

// Given a subset C of a group, returns the sum of the elements of C
// in the group algebra 'alg'.
Bar := function(C,alg);
  return alg ! [(i in C) select 1 else 0 : i in {1 .. Dimension(alg)}];
end function;

// Given an element 'x' of an algebra 'alg', returns x^(-1).
// 'inv' must be a list giving the inverses of the basis elements of 'alg'.
Inv := function(x,alg,inv);
  c := Eltseq(x);
  for i:=1 to #inv do
    if inv[i] gt i then
      a:=c[i];
      c[i]:=c[inv[i]];
      c[inv[i]]:=a;
    end if;
  end for;
  return alg ! c;
end function;

// Given an element 'x' of an algebra 'alg', returns the list of coordinates
// of 'x' with respect to the S-ring 'sring' ('x' must actually be in this S-ring
// or an error will be generated), where 'sring' is represented as a list of
// basic sets, each basic sets being represented as a set of integers
// in the range 1..Dimension(alg).
Coords := function(x,sring,alg);
  coords := [];
  for i:=1 to #sring do
    j := Random(sring[i]);
    Append(~coords,x[j]);
    x := x-x[j]*Bar(sring[i],alg);
  end for;
  if x ne alg!0 then
    error "x not in S-ring.";
  end if;
  return coords;
end function;

// Internal routine used in SRings:
// Given a group 'G', returns the group algebra of G as a structure constant algebra,
// along with several other items:
//   inv: list of integers in the range 1..#G giving the inverse of each element of G
```

```
//   GG:  list of elements of 'G' (in the order used by the preceding 'inv')
//   GI:  associative array giving, for each element 'g' of G, the integer associated
//        with 'g', so that GG[GI[g]] equals g and GI[GG[i]] equals i.
GroupAlg := function(G);
  GG := [G!1] cat Setseq(Set(G) diff {G!1});
  if IsCyclic(G) then
    GG := [G.1^i : i in {0..#G-1}];
  end if;
  GI := AssociativeArray(G);
  for i:=1 to #GG do
    GI[GG[i]] := i;
  end for;
  alg := [];
  inv := [];
  for i:=1 to #GG do
    for j:=1 to #GG do
      Append(~alg,<i,j,GI[GG[i]*GG[j]],1>);
    end for;
    Append(~inv,GI[GG[i]^-1]);
  end for;
  return Algebra<RationalField(),#G | alg>,inv,GG,GI;
end function;

// Internal routine used in RationalAlg:
// Given the set of automorphism classes A of a group G, returns
// the discrete rational S-ring over G as a structure constant algebra.
CAlg := function(A,G);
  inv := [];
  for i:=1 to #A do
    g := Random(A[i]);
    for j:=1 to #A do
      if g in A[j] then
        Append(~inv,j);
        continue i;
      end if;
    end for;
    error "Problem with inv in RationalAlg.";
  end for;

  alg := [];
  for i:=1 to #A do
    for j:=1 to #A do
      for k:=1 to #A do
        g := Random(A[k]);
        S := {g*h : h in A[inv[j]]};
        Append(~alg,#(A[i] meet S));
      end for;
```

```
    end for;
  end for;
  return Algebra<RationalField(),#A | alg>,inv;
end function;

// Returns the discrete rational S-ring over G as an algebra.
RationalAlg := function(G);
  A := AutoClasses(G);
  GA,inv := CAlg(A,G);
  return GA,inv,A;
end function;

// Internal routine used by MergeClasses:
JoinClasses := function(classes,mtab,k1,k2);
  for i:=1 to #classes do
    if i eq k2 then continue; end if;
    mtab[i][k1] +:= mtab[i][k2];
    mtab[k1][i] +:= mtab[k2][i];
  end for;
  mtab[k1][k1] +:= mtab[k2][k2];
  classes[k1] := classes[k1] join classes[k2];
  Remove(~classes,k2);
  Remove(~mtab,k2);
  for i:=1 to #classes do
    Remove(~mtab[i],k2);
  end for;
  return classes,mtab;
end function;

// Internal routine used by SRingsRec:
// Given a sequence 'classes' of disjoint sets of group elements,
// beginning with classes[i] all classes which intersect
// 'class' are merged into a single class.
MergeClasses := procedure(class,~mtab,~classes,~j,~j0,~succ);
  succ := true;
  i := j;
  j := 0;
  for k:=i to #classes do
    if class meet classes[k] ne {} then
      if class eq classes[k] then return; end if;
      classleft := class diff classes[k];
      l:=k+1;
      if k eq i then l:=j0; end if;
      while l le #classes and classleft ne {} do
        if classleft meet classes[l] ne {} then
          classleft := classleft diff classes[l];
          classes,mtab := JoinClasses(classes,mtab,k,l);
```

```
          if l lt j0 then j0 := j0-1; end if;
        else
          l := l+1;
        end if;
      end while;
      succ := classleft eq {};
      j:=k;
      return;
    end if;
  end for;
end procedure;

// Internal routine used in SRings:
forward SRingsRec;
SRingsRec := procedure(classes,mtab,i,j0,alg,inv,~srings);
  j := i;
  while j ne 0 and j lt #classes do
    class := { inv[k] : k in classes[j] };
    j := i;
    MergeClasses(class,~mtab,~classes,~j,~j0,~succ);
    if not succ then return; end if;
    if j lt i and j ne 0 then return; end if;
  end while;

  while i le #classes do
    for j:=j0 to #classes do
      nclasses,nmtab := JoinClasses(classes,mtab,i,j);
      SRingsRec(nclasses,nmtab,i,j,alg,inv,~srings);
    end for;

    for j:=2 to i do
      for k:=2 to i do
        try
          c:=Coords(mtab[j][k],classes,alg);
        catch e
          return;
        end try;
      end for;
    end for;

    for j:=2 to i do
      class := { inv[k] : k in classes[j] };
      for k:=2 to #classes do
        if classes[k] eq class then continue j; end if;
      end for;
      return;
    end for;
```

```
    i := i+1;
    j0 := i+1;
  end while;
  Append(~srings,classes);
end procedure;

// Returns a list of all S-rings over a group G (if pseudo is set to 'true', then all
// PS-rings are returned). Each S-ring is represented as a list of basic sets
// (beginning with the identity basic set), where each basic set is represented
// as a set of integers in the range 1..#G; these are indices into the list of group
// elements GG also returned.
SRings := function(G : pseudo:=false);
  GA,inv,GG,GI := GroupAlg(G);
  classes := [ {i} : i in {1 .. #inv} ];
  srings := [];
  a := pseudo select 1 else 2;
  SRingsRec(classes,BasisProducts(GA),a,a+1,GA,inv,~srings);
  return srings,GG;
end function;

// Returns a list of all rational S-rings over a group G. Each S-ring is represented
// as a list of basic sets (beginning with the identity basic set), where each basic
// set is represented as a set of integers which are indices into the list of
// automorphism classes A of G which is also returned.
RationalSRings := function(G);
  GA,inv,A := RationalAlg(G);
  classes := [ {i} : i in {1 .. #inv} ];
  srings := [];
  SRingsRec(classes,BasisProducts(GA),2,3,GA,inv,~srings,false);
  return srings,A;
end function;

// Given an S-ring 'sring' over a group G, returns the list of S-rings over G which
// are strongly isomorphic to 'sring'.
AutoSRings := function(sring,G : A:=AutomorphismGroup(G));
  srings := {sring};
  repeat
    n := #srings;
    newsrings := {};
    for S in srings do
      newsrings join:= {{{(A.i)(g) : g in C} : C in S} : i in
{1..NumberOfGenerators(A)}};
    end for;
    srings join:= newsrings;
  until n eq #srings;
  return srings;
```

```
end function;

// Given a list 'srings' of S-rings over a group G, returns a set of representatives
// from each strong isomorphism class occuring in 'srings'.
AutoReps := function(srings,G);
  reps := {};
  A := AutomorphismGroup(G);
  while #srings gt 0 do
    print #srings;
    sring := Random(srings);
    srings := srings diff AutoSRings(sring,G : A:=A);
    reps join:= {sring};
  end while;
  return reps;
end function;

// ------------------------------------------------------------------------
// The remaining routines deal with S-rings which may be constructed using
// type (I), (II), and (III) constructions. In these routines, the S-rings are
// represented as lists of basic sets, where the basic sets are subsets of the
// group (instead of sets of integer indices into the group as above).
// ------------------------------------------------------------------------

// Given an S-ring 'S', returns whether a subset H of the underlying group is
// an S-set.
IsSSet := function(S,H);
  for C in S do
    if #(C meet H) gt 0 then
      if not C subset H then return false; end if;
      H := H diff C;
    end if;
  end for;
  return true;
end function;

forward SRing0;
forward SRings1;
forward SRings2;
forward SRings3;

// Returns the set of S-rings over a group G which may constructed recursively using
// type (I), (II), and (III) constructions.
SRings123 := procedure(G,~tab,~ans);
  CG := CyclicGroup(#G);
  b,iso := IsIsomorphic(CG,G);
  t := iso(CG.1);
  if IsDefined(tab,#G) then
```

```
    ans := {{{t^i : i in C} : C in S} : S in tab[#G]};
    return;
  end if;
  S0:={SRing0(G)};
  S1:=SRings1(G);
  SRings2(G,~tab,~S2);
  SRings3(G,~tab,~S3);
  ans := S0 join S1 join S2 join S3;
  GI := AssociativeArray();
  for i:=0 to #G-1 do GI[t^i]:=i; end for;
  tab[#G] := {{{GI[g] : g in C} : C in S} : S in ans};
end procedure;

// Returns the trivial S-ring over a group G.
SRing0 := function(G);
  if #G ne 1 then return {{G!1},Set(G) diff {G!1}};
  else return {{G!1}}; end if;
end function;

// Returns the type (I) S-rings over a group G.
// (or rather, a complete set of strong automorphism representatives of
// type (I) S-rings, which, in case G is cyclic, is the complete set
// of type (I) S-rings.)
SRings1 := function(G);
  A := AutomorphismGroup(G);
  map,AA := PermutationRepresentation(A);
  srings := {};
  SS := Subgroups(AA);
  for i:=1 to #SS do
    H := (map^-1)(Generators(SS[i]`subgroup));
    sring := {};
    elts := Set(G);
    while #elts gt 0 do
      C := {Random(elts)};
      repeat
        n := #C;
        C join:= {h(c) : h in H, c in C};
      until #C eq n;
      elts := elts diff C;
      sring join:= {C};
    end while;
    srings join:= {sring};
  end for;
  return srings;
end function;

// Returns the type (II) S-rings over a group G.
```

```
SRings2 := procedure(G,~tab,~srings);
  NN := {N : N in NormalSubgroups(G) | not #N in {1,#G}};
  NN1 := {N : N in NN | (#N)^2 le #G};
  srings := {};
  for N1 in NN1 do
    for N2 in NN do
      if #(N1 meet N2) eq 1 and sub<G|N1,N2> eq G then
        SRings123(N1,~tab,~srings1);
        SRings123(N2,~tab,~srings2);
        for S1 in srings1 do
          for S2 in srings2 do
            srings join:= {{{c*d : c in C,d in D} : C in S1, D in S2}};
          end for;
        end for;
      end if;
    end for;
  end for;
end procedure;

// Returns the type (III) S-rings over a group G.
SRings3 := procedure(G,~tab,~srings);
  KK := {K`subgroup : K in Subgroups(G) | #K`subgroup ne #G};
  HH := {H : H in NormalSubgroups(G) | not #H in {1,#G}};
  srings := {};
  for K in KK do
    for H in HH do
      if not H subset K then continue; end if;
      SRings123(K,~tab,~srings1);
      Q,phi := quo<G|H>;
      SRings123(Q,~tab,~srings2);
      for S1 in srings1 do
        if not IsSSet(S1,Set(H)) then continue; end if;
        for S2 in srings2 do
          SK1 := {{phi(g) : g in C} : C in S1};
          SK2 := {C : C in S2 | C subset phi(K)};
          if SK1 eq SK2 then
            S := S1 join {{(phi^-1)(g)*h : g in C, h in H} : C in S2 |
                          not C subset phi(K)};
            srings join:= {S};
          end if;
        end for;
      end for;
    end for;
  end for;
end procedure;
```

References

[1] Reinhold Baer. Types of elements and characteristic subgroups of abelian groups. *Proc. London Math. Soc.*, 39(2054):481–514, 1934.

[2] Garrett Birkhoff. Sobre los grupos de automorfismos. *Revista de la Unión Matemática Argentina*, 11:155–157, 1946.

[3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. *J. Symbolic Comput.*, 24(3-4):235–265, 1997.

[4] Richard A. Brualdi. *Introductory Combinatorics*. Pearson Prentice Hall, 2004.

[5] Peter Crawley and Robert P. Dilworth. *Algebraic Theory of Lattices*. Prentice-Hall: Englewood Cliffs, New Jersey, 1973.

[6] B. A. Davey and H. A. Priestley. *Introduction to Lattices and Order, 2nd Ed.* Cambridge University Press, 2002.

[7] David S. Dummit and Richard M. Foote. *Abstract Algebra, Third Edition*. John Wiley and Sons, Inc., 2004.

[8] S. Foldes. On automorphism groups of graphs and distributive lattices. *Algebra Universalis*, 41:115–120, 1999.

[9] G. Grätzer, H. Lakser, and E. T. Schmidt. On a result of Birkhoff. *Periodica Mathematica Hungarica*, 30(3):183–188, 1995.

[10] G. Grätzer, E. T. Schmidt, and D. Wang. A short proof of a theorem of Birkhoff. *Algebra Universalis*, 37(2):253–255, 1997.

[11] H. Hermes. *Einführung in die Verbandstheorie*. Springer-Verlag, 1955.

[12] Ka Hin Leung and Shing Hing Man. On Schur rings over cyclic groups, II. *Journal of Algebra*, 183:273–285, 1996.

[13] G. A. Miller. Determination of all the characteristic subgroups of any abelian group. *American Journal of Mathematics*, 27(2):15–24, 1905.

[14] G. A. Miller, H. F. Blichfeldt, and L. E. Dickson. *Theory and Applications of Finite Groups*. John Wiley and Sons, Inc., 1916.

[15] Mikhail E. Muzychuk. The structure of rational Schur rings over cyclic groups. *European Journal of Combinatorics*, 14:479–490, 1993.

[16] Mikhail E. Muzychuk. On the structure of basic sets of Schur rings over cyclic groups. *Journal of Algebra*, 169:655–678, 1994.

[17] W. R. Scott. *Group Theory*. Englewood Cliffs, New Jersey: Prentice-Hall, 1964.

[18] N. J. A. Sloane. The on-line encyclopedia of integer sequences. http://www.research.att.com/ njas/sequences, 2008.

[19] H. de Vries and A. B. de Miranda. Groups with a small number of automorphisms. *Mathematische Zeitschrift*, 68:450–464, 1957.

[20] Helmut Wielandt. *Finite Permutation Groups*. New York, Academic Press, 1964.