2016-06-01

Schur Rings Over Projective Special Linear Groups

David R. Wagner
Brigham Young University

Schur Rings Over Projective Special Linear Groups

David R. Wagner

A thesis submitted to the faculty of
Brigham Young University
in partial fulfillment of the requirements for the degree of

Master of Science

Stephen P. Humphries, Chair
Darrin Doud
Paul Jenkins

Department of Mathematics

Brigham Young University

June 2016

ABSTRACT

Schur Rings Over Projective Special Linear Groups

David R. Wagner
Department of Mathematics, BYU
Master of Science

This thesis presents an introduction to Schur rings (S-rings) and their various properties. Special attention is given to S-rings that are commutative. A number of original results are proved, including a complete classification of the central S-rings over the simple groups $\mathrm{PSL}(2, q)$, where q is any prime power. A discussion is made of the counting of symmetric S-rings over cyclic groups of prime power order.

An appendix is included that gives all S-rings over S_4 with basic structural properties, along with code that can be used, for groups of comparatively small order, to enumerate all S-rings and compute character tables for those S-rings that are commutative. The appendix also includes code optimized for the enumeration of S-rings over cyclic groups.

Keywords: Schur Rings, Association schemes, Algebraic combinatorics, Projective special linear groups

Contents

Chapter 1. Introduction

This chapter gives some basic facts about association schemes and defines Schur rings (hereafter S-rings), setting forth some of the properties that will be important in later chapters. On association schemes and algebraic combinatorics, some references include [BI1, D1, BA]. Much of the introductory material on Schur rings is also available in [M1, K1].

1.1 Schur Rings

In what follows, G will be a finite group. We denote the complex group algebra by $\mathbb{C}G$. Given a subset $C \subseteq G$, let $\overline{C} = \sum_{g \in C} 1 \cdot g \in \mathbb{C}G$ and $C^{-1} = \{g^{-1} : g \in C\}$.

Definition 1.1. A subalgebra $\mathfrak{S} \subseteq \mathbb{C}G$ is called a *Schur ring* (or *S-ring*) if it has a generating basis $\{\overline{C_i}\}$ where $\mathcal{K} = \{C_i\}_{i=1}^{r}$ is a partition of G such that the following hold:

(i) $\{1_G\} \in \mathcal{K}$;

(ii) For each $C \in \mathcal{K}$, $C^{-1} \in \mathcal{K}$. $\Diamond$

If $\mathfrak{S}$ satisfies (ii) but not (i), then it is called a *pre-Schur ring*. The set C_i which contains the identity is called its *unit class*.

The fact that the set $\{\overline{C_i}\}$ generates an algebra guarantees that we can write products

$$\overline{C_i} \cdot \overline{C_j} = \sum_k p_{ij}^k \overline{C_k},$$

where the p_{ij}^k are non-negative integer constants and the product on the left is taken in the group algebra. The numbers p_{ij}^k are called the *intersection numbers* or *structure constants* of the algebra. We write $\mathscr{D}(\mathfrak{S}) = \{C_i\}_{i=1}^{r}$ and call these the *principal sets* or the *primitive sets* of $\mathfrak{S}$. The quantities $\overline{C_i}$ are the corresponding *primitive elements*.

Taking the trivial partition $\{\{g_1\}, \{g_2\}, \ldots, \{g_n\}\}$ of the group, we see that the group algebra is an S-ring. Letting the C_i be the conjugacy classes, we also see that the centre of the group algebra is an S-ring. The S-ring given by the 2-element partition

$$\{\{1 = g_1\},\, \{g_2, \ldots, g_n\}\}$$

is called the *trivial* S-ring over G, for which we write $\mathscr{T}(\mathbb{C}G)$ when working over the complex numbers.

As a nontrivial example, consider the partition of S_3:

$$\{\{1\}, \{(12)\},\, \{(123), (321)\},\, \{(13), (23)\}\}.$$

Writing $t_1 = \overline{C_1} = 1$, $t_2 = \overline{C_2} = (12)$, $t_3 = \overline{C_3} = (123) + (321)$, $t_4 = \overline{C_4} = (13) + (23)$, we have a multiplication table

$\cdot$	t_1	t_2	t_3	t_4
t_1	t_1	t_2	t_3	t_4
t_2	t_2	t_1	t_4	t_3
t_3	t_3	t_4	$2t_1 + t_3$	$2t_2 + t_4$
t_4	t_4	t_3	$2t_2 + t_4$	$2t_1 + t_3$

,

confirming that the t_i generate an S-ring.

The following definitions will be of interest:

Definition 1.2. Let $\mathfrak{S}$ be an S-ring with principal sets $\{C_1, \ldots, C_r\}$. Then $\mathfrak{S}$ is called *symmetric* if for all i, $C_i^{-1} = C_i$. An S-ring $\mathfrak{S}$ is called a *central Schur ring* if it is contained as an algebra in the centre of the group algebra.

When $g \mapsto g^{-1}$ is an automorphism, the *symmetric S-ring over G*, denoted $\mathscr{S}(\mathbb{C}G)$, is that given by the partition $\{\{g, g^{-1}\} : g \in G\}$. $\Diamond$

Besides the ordinary multiplication $*$, the group algebra has another useful product, called the *Hadamard product* and written $\circ$, which is linear, associative and commutative.

Given elements of the group algebra $\alpha = \sum_{g \in G} \alpha_g g$, $\beta = \sum_{g \in G} \beta_g g$, this is given by

$$\alpha \circ \beta = \sum_{g \in G} (\alpha_g \beta_g) g.$$

We now give a useful criterion for determining when a subalgebra of $\mathbb{C}G$ is an S-ring. The group inverse $^{-1} : G \to G$ can be extended in its domain to be an endomorphism of $\mathbb{C}G$ by $\sum \alpha_g g \mapsto \sum \overline{\alpha_g} g^{-1}$ with the overline denoting the complex conjugate. Certainly it is bijective and distributes over addition. Moreover,

$$\begin{aligned}\left[\left(\sum_g \alpha_g g\right) \cdot \left(\sum_h \beta_h h\right)\right]^{-1} &= \left(\sum_{gh=k} \alpha_g \beta_h k\right)^{-1} = \sum_{h^{-1}g^{-1}=k^{-1}} \overline{\beta_{h^{-1}} \alpha_{g^{-1}}} k^{-1} \\ &= \left(\sum_h \overline{\beta_{h^{-1}}} h^{-1}\right)\left(\sum_h \overline{\alpha_{g^{-1}}} h^{-1}\right) \\ &= \left(\sum_h \beta_h h\right)^{-1} \cdot \left(\sum_g \alpha_g g\right)^{-1}.\end{aligned}$$

Thus, this operation is an antiautomorphism of $\mathbb{C}G$. Note also that this involution stabilizes any S-ring as it must permute the primitive elements.

Our proof of the following lemma is similar to that of Muzychuk (see [MU1], Lemma 1.3) who gave the same result for $\mathbb{Q}G$:

Lemma 1.3. *A subalgebra $\mathfrak{S}$ of $\mathbb{C}G$ is an S-ring if and only if $\mathfrak{S}$ is closed under $^{-1}$ and $\circ$, and contains 1_G and $\overline{G}$.*

Proof. It is clear that any S-ring is closed under the Hadamard product. Thus, suppose S is a subalgebra closed under the operations of the hypothesis, containing 1_G and $\overline{G}$. Consider the ring $\mathbb{C}G^\circ \cong \mathbb{C}^{|G|}$ with operations $+$ and $\circ$. This is commutative and semisimple; the corresponding matrix decomposition is as $|G|$ 1×1 matrices. Thus, the subring $\mathfrak{S}^\circ$ inherits these properties and so by Wedderburn's Theorem is spanned by orthogonal primitive idempotents. Let e be such an idempotent. Writing $e = \sum_g \alpha_g g$, then $e \circ e = \sum_g \alpha_g^2 g = e$ implies that the α_g are zero or one. Thus each idempotent is of the form $\overline{C_i}$ where $C_i \subset G$.

As $\overline{G} \in \mathfrak{S}$, necessarily $\cup_i C_i = G$ and as $1_G \in \mathfrak{S}$, one of the C_i is $\{1_G\}$. Also, orthogonality implies that

$$\overline{C_i} \circ \overline{C_j} = \delta_{ij} \overline{C_i},$$

where δ_{ij} is the Kronecker delta. Thus $C_i \cap C_j = \emptyset$ when $i \neq j$ and the C_i are a partition of G. Finally, $\overline{C_i}^{-1}$ is also a primitive idempotent contained in $\mathfrak{S}$ by hypothesis ($\mathfrak{S}$ is closed under $^{-1}$). However, the $\overline{C_i}$ are all of the primitive idempotents, so that $C_i^{-1} = C_j$ for some j. This completes the proof. $\square$

We take note of the following theorem due to Wielandt (proved by him for $\mathbb{Q}$ in [W1] while here we give a proof over $\mathbb{C}$). From this we infer that S-rings are semisimple over $\mathbb{C}$. In the next section we will give an alternate proof by showing that S-rings are association schemes, which are semisimple when realized as matrix algebras.

Proposition 1.4. *Every subalgebra of $\mathbb{C}G$ closed under $^{-1}$ is semisimple.*

Proof. Let S be such a subalgebra and not semisimple. Note that the group algebra $\mathbb{C}G$ (and hence S) is Artinian as a finitely generated module over an Artinian ring. Write J for the Jacobson radical, which must be nonzero. Every nonzero ideal of an Artinian ring contains some simple (and necessarily principal) ideal, so we can find a simple ideal $\alpha S \subseteq J$ where $0 \neq \alpha \in J$. As J annihilates simple ideals, $\alpha S \alpha = 0$. Moreover,

$$\begin{aligned} \alpha\alpha^{-1}\alpha &= 0, \text{ so that} \\ \alpha\alpha^{-1}\alpha\alpha^{-1} &= 0, \text{ and} \\ \alpha\alpha^{-1}(\alpha\alpha^{-1})^{-1} &= 0, \end{aligned}$$

where the last implication follows since the involution $^{-1}$ is an antiautomorphism. We now show that $\beta\beta^{-1} = 0$ implies $\beta = 0$ for any $\beta \in S$. This easily implies $\alpha = 0$, a contradiction. Writing $\beta = \sum_g \beta_g g$, the coefficient of 1_G in the product $\beta\beta^{-1}$ is $\sum_g |\beta_g|^2$. Thus $\beta_g = 0$ for all g and $\beta = 0$. $\square$

In the proof, to find the simple ideal (α), we made use of the fact that RG is Artinian when R is an Artinian ring and G is a finite group. In fact, it can be shown (Theorem 1 on page 657 of [C1]) that the converse also holds; for R a ring, G a group, the group ring RG is Artinian if and only if G is finite and R is Artinian.

Leung and Man have given the classification of S-rings over cyclic groups; see [LM1, LM2]. Their theorem is a major accomplishment in the study of S-rings and the proof will not be given here. We state their result:

Theorem 1.5. *Let F be a field of characteristic zero and G be a finite cyclic group. Let S be a Schur ring over the group algebra FG. Then S is one of the following:*

(i) the trivial S-ring;

(ii) an orbit S-ring;

(iii) a dot product of S-rings;

(iv) a semi-wedge product of S-rings. □

We now go about the task of defining the sorts of S-rings spoken of in the theorem. In defining these constructions, G may be any finite group, not necessarily cyclic.

Proposition 1.6. *Let $\mathcal{H} \leq \mathrm{Aut}(G)$ and let $\{\mathcal{O}_i\}$ denote the orbits of G under the action of $\mathcal{H}$. Then the set of orbits generates an S-ring. Such a Schur ring will be called an* orbit S-ring. □

Definition 1.7. The Rational S-ring over G, denoted $\mathscr{R}(\mathbb{C}G)$, is the orbit S-ring over G given by the full automorphism group of G ◊

Proposition 1.8. *Let $G = H \times K$ and let S_H, S_K be S-rings over $H \times 1$ and $1 \times K$ respectively. Then the subalgebra of $\mathbb{C}G$ these S-rings generate is an S-ring, called a* dot product S-ring *and denoted $S_H \cdot S_K$.*

Proof. As $1_G = 1_H 1_K$ and $1_H \in S_H$, $1_K \in S_K$, it follows that 1_G is in the dot product. Clearly $\overline{G} = \overline{H} \cdot \overline{K} \in S_H \cdot S_K$. Let C_i, C_j be principal sets of the dot product. Then we have $C_i = D_i E_i$, $C_j = D_j E_j$, where D_i, D_j are principal sets of S_H, and E_i, E_j are principal sets of S_K. As H commutes with K, we have

$$\overline{C_i} \cdot \overline{C_j} = \overline{D_i} \cdot \overline{E_i} \cdot \overline{D_j} \cdot \overline{E_j} = \overline{D_i} \cdot \overline{D_j} \cdot \overline{E_i} \cdot \overline{E_j},$$

but the products $\overline{D_i} \cdot \overline{D_j}$ and $\overline{E_i} \cdot \overline{E_j}$ are linear combinations of the class sums of their respective S-rings. As the class sums of the dot product are exactly products of class sums for S_H, S_K, we have that $\overline{C_i} \cdot \overline{C_j}$ is in fact a linear combination of class sums. □

Before defining the semi-wedge product, we define the wedge product.

Definition 1.9. Suppose $K \trianglelefteq G$ are finite groups and let $\pi : G \to G/K$ be the quotient map. If S_K and $S_{G/K}$ are S-rings over K, G/K respectively, we define the *wedge product* $S_K \wedge S_{G/K}$ to be the S-ring with principal sets

$$\mathscr{D}(S_K) \cup \{\pi^{-1}(C) : C \in \mathscr{D}(S_{G/K}),\, C \neq \{1\}\}. \qquad \diamondsuit$$

That this is an S-ring is not difficult to show and will follow from Proposition 1.11. The wedge-product construction was generalized as follows by Leung and Man [LM2]. Let K, $H \leq G$ such that $1 < K \leq H < G$ and $K \trianglelefteq G$ with $\pi : G \to G/K$ the quotient map. First, note that π as above extends linearly to give a map $\pi^* : \mathbb{C}G \to \mathbb{C}(G/K)$. In a similar spirit, for some S-ring S_H over H, we write

$$\pi^*(S_H) = \langle \overline{\pi(D)} \rangle_{D \in \mathscr{D}(S_H)}$$

so that π^* sends an S-ring over G to a subalgebra of $\mathbb{C}(G/K)$, generated by the projections of its principal sets.

Definition 1.10. Let G, H, K, π as in the preceding paragraph and let S_H and $S_{G/K}$ be S-rings over H, G/K respectively and assume $\overline{K} \in S_H$ and $\pi^*(S_H) = (\mathbb{C}H/K) \cap S_{G/K}$. The *semi-wedge product* of these S-rings is denoted $S_H \Delta S_{G/K}$. It is generated by S_H and the elements $\sum_{g \in C_i} g\overline{K}$ where C_i are the principal sets of $S_{G/K}$. $\Diamond$

Proposition 1.11. *The semi-wedge product of S-rings is an S-ring.*

Proof. Take the notation of the preceding paragraph and write S for the semi-wedge product. By construction, S is generated by the sums corresponding to the principal sets of S_H and the sets

$$\bigcup_{\substack{g \in C_i \\ C_i \not\subseteq H/K}} gK,$$

where $C_i \in \mathscr{D}(S_{G/K})$. These sets give a partition of the group by construction and so it is clear that 1_G, $\overline{G} \in S$. Denote these sets $\{D_i\}$ in some ordering. We must show that $\{\overline{D_i}\}$ generate an algebra. Without loss of generality, consider the product $\overline{D_1} \cdot \overline{D_2}$. If both D_1 and D_2 are principal sets of H, then the product is certainly a linear combination of the $\{\overline{D_i}\}$ as S_H is an S-ring. Suppose D_1, D_2 are of the form $\cup_{g \in C_i} gK$, where we may suppose the unions are over C_1, C_2 respectively. Then as $K \trianglelefteq G$, we have

$$\begin{aligned}
\overline{D_1} \cdot \overline{D_2} &= \left(\sum_{g \in C_1} g\overline{K} \right) \cdot \left(\sum_{g \in C_2} g\overline{K} \right) \\
&= \left(\sum_{g \in C_1} g \right) \cdot \left(\sum_{g \in C_2} g \right) \overline{K}^2 \\
&= \overline{C_1} \cdot \overline{C_2} \cdot \overline{K}^2 \\
&= |K| \overline{C_1} \cdot \overline{C_2} \cdot \overline{K}.
\end{aligned}$$

Since $S_{G/K}$ is an S-ring, the term $\overline{C_1} \cdot \overline{C_2}$ is a linear combination of the $\overline{C_i}$ and so $\overline{C_1} \cdot \overline{C_2} \cdot \overline{K}$ is a linear combination of the $\overline{D_i}$. As $\overline{K} \in H$, we will be done if we take D_2 to be a principal set of H and D_1 as before. Reasoning similarly, this causes no problems since as in the definition, $\pi^*(S_H) = (\mathbb{C}H/K) \cap S_{G/K}$. $\square$

We will need a definition, with the proposition to follow:

Definition 1.12. Let $\mathfrak{S}$ be an S-ring over G. We say that $\mathfrak{S}$ has *wedge decomposition* $1 < K \leq H < G$ (or is *wedge-decomposable*) if $\mathfrak{S} \cap \mathbb{C}H$ is an S-ring over H and every principal set of $\mathfrak{S}$ is either a principal set of an S-ring over H, or a union of cosets of $K \lhd G$. $\Diamond$

Proposition 1.13. *Suppose $\mathfrak{S}$ has wedge decomposition $1 < K \leq H < G$. Then $\mathfrak{S}$ is a semi-wedge product.*

Proof. Since $\mathfrak{S}$ is an S-ring, the principal sets descend via the natural projection map $\pi : G \to G/K$ to give a partition of K. It is easy to see that this partition yields an S-ring over K since the inverse images of these under the projection map have the requisite properties. $\square$

We conclude the section by giving two notions of isomorphism of S-rings that are more specific than that of $\mathbb{C}$-algebra isomorphism. These are Cayley isomorphism and Schur isomorphism. The Cayley homomorphisms are those derived from group homomorphisms:

Definition 1.14. Let G and H be groups and $A \subseteq \mathbb{C}G$, $B \subseteq \mathbb{C}H$ subalgebras. A $\mathbb{C}$-algebra homomorphism $f : A \to B$ is called a *Cayley homomorphism* if it is the restriction of a map $\varphi : \mathbb{C}G \to \mathbb{C}H$ such that $\varphi|_G$ is a group homomorphism. A bijective Cayley homomorphism is called a *Cayley automorphism.* $\Diamond$

Somewhat trivially, any group automorphism induces a Cayley isomorphism of S-rings. We also have:

Definition 1.15. A *Schur homomorphism* is a linear map $\varphi : S \to T$ of Schur rings that respects the operations $\cdot$, $\circ$ and $^{-1}$. Such a map is a *Schur isomorphism* when it is bijective. $\Diamond$

In general, a Cayley map is not a Schur map. While involution and ordinary multiplication are respected by such a map, the Hadamard product need not be. In particular, consider the augmentation map $\epsilon : \mathbb{C}G \to \mathbb{C}$, which is induced by the map $G \to C_1$ to the trivial group. Taking $\alpha = \sum_g \alpha_g g \in \mathbb{C}G$, we have

$$\epsilon(\alpha \circ \alpha) = \sum_g \alpha_g^2 \quad \text{while} \quad \epsilon(\alpha) \circ \epsilon(\alpha) = \left(\sum_g \alpha_g \right)^2,$$

which are not in general equal. More precisely:

Lemma 1.16. *A Cayley map is a Schur map if and only if it is injective.*

Proof. Let $\varphi : \mathbb{C}G \to \mathbb{C}H$ be a Cayley map. Let $\alpha = \sum_g \alpha_g g$, $\beta = \sum_g \beta_g g \in \mathbb{C}G$. If φ is injective,

$$\begin{aligned}
\varphi(\alpha \circ \beta) = \varphi \left(\sum_g \alpha_g \beta_g g \right) &= \sum_g \alpha_g \beta_g \varphi(g) \\
&= \left(\sum_g \alpha_g \varphi(g) \right) \circ \left(\sum_g \beta_g \varphi(g) \right), \text{ since } \varphi \text{ is injective} \\
&= \varphi(\alpha) \circ \varphi(\beta).
\end{aligned}$$

On the other hand, let $K = \mathrm{Ker}(\varphi|_G)$ be nontrivial. Then

$$\begin{aligned}
&\varphi(\overline{G} \circ \overline{G}) = \varphi(\overline{G}) = |K| \overline{\varphi(G)} \\
\neq &|K|^2 \overline{\varphi(G)} = \left(|K| \overline{\varphi(G)} \right) \circ \left(|K| \overline{\varphi(G)} \right) \\
= &\varphi(\overline{G}) \circ \varphi(\overline{G}).
\end{aligned}$$

□

Proposition 1.17. *Every Cayley isomorphism of S-rings is a Schur isomorphism.*

Note that the converse of this proposition does not hold; consider trivial S-rings over distinct groups G, H of the same order. There is an obvious Schur isomorphism, but if we assume this to be a Cayley isomorphism, it is not hard to see that necessarily $G \cong H$.

1.2 Association Schemes

The field of algebraic combinatorics has its beginnings with Delsarte [D1]. Preeminent among the objects of study in this branch of mathematics are association schemes, the theory of which will be useful in our investigation of S-rings. These association schemes unify the study of many combinatorial objects; their use has yielded excellent results in combinatorics generally and prompted some of Delsarte's success in coding theory and design theory.

In analogy with S-rings, which are subrings of the group algebra with special combinatorial properties, association schemes can be realized as matrix algebras with a convenient basis. While there are many equivalent definitions and even more general objects, this will be the viewpoint that suits us. Accordingly, we have

Definition 1.18. Let X be a set of size n and $R_i \subset X \times X$, $0 \leq i \leq d$ be relations on X. The pair $\mathscr{X} = (X, \{R_i\}_i)$ is called an *association scheme* if the following five conditions hold.

(i) $R_0 = \{(x,x) : x \in X\}$, the identity relation;

(ii) $R_0 \cup R_1 \cup \cdots \cup R_d = X \times X$ and $R_i \cap R_j = \emptyset$ when $i \neq j$;

(iii) For each $0 \leq i \leq d$, the set $\{(y,x) : (x,y) \in R_i\}$ is equal to $R_{i'}$ for some other i', $0 \leq i' \leq d$;

(iv) Given any triple $0 \leq i,j,k \leq d$, the number

$$|\{z \in X : (x,z) \in R_i \text{ and } (z,y) \in R_j\}|$$

which we name p_{ij}^k is constant for any pair $(x,y) \in R^k$;

(v) $p_{ij}^k = p_{ji}^k$. $\lozenge$

To every association scheme we associate its *Bose-Mesner algebra*, sometimes called the *adjacency algebra*; this is generated by $n \times n$ matrices A_i where

$$(A_i)_{xy} = \begin{cases} 1 \text{ if } (x, y) \in R_i, \\ 0 \text{ otherwise.} \end{cases}$$

These are called the *adjacency matrices* or *A-matrices* of the scheme. Given some pair $(X, \{R_i\}_i)$ where the R_i are relations on X, not necessarily an association scheme, we can form the A_i as above. We have the following easy result, which we state without proof.

Proposition 1.19. *The $n \times n$ 0,1-matrices $\{A_0, \ldots, A_d\}$ are the adjacency matrices of an association scheme if and only if*

(i) $A_0 = I$, *the identity matrix;*

(ii) $\sum_{i=0}^{d} A_i = J$, *the $n \times n$ all-ones matrix;*

(iii) *For each $0 \leq i \leq d$, $A_i^T = A_{i'}$ for some i';*

(iv) $A_i A_j = \sum_{k=0}^{d} p_{ij}^k A_k$, $p_{ij}^k \in \mathbb{Z}$ *for all $i, j \leq d$;*

(v) $A_i A_j = A_j A_i$, *for all $i, j \leq d$.* □

Importantly, the numbers p_{ij}^k of (iv) of either definition, which guarantee that the A_i are a generating basis for a matrix algebra, are called the *intersection numbers* of the association scheme. If $i' = i$ for all i in (iii), the association scheme will be called *symmetric*. In accordance with the literature, matrices A_i satisfying (i) – (iv) are said to give a *non-commutative* association scheme. Given i, the number $k_i = p_{ii'}^0$ will be called the *valency* of A_i and the set of k_i the *valencies of the scheme*

It is immediate that

Proposition 1.20. *Every commutative S-ring is naturally an association scheme.*

Proof. Let G be a finite group of order n and $\mathfrak{S}$ an S-ring over G with principal sets $C_0, \ldots, C_d$. Enumerate the group elements $\{e = g_1, g_2, \ldots, g_n\}$ and let $\{g'_1, \ldots, g'_n\}$ be the corresponding $n \times n$ matrices of the regular representation. Define the matrices $A_0, \ldots, A_d$ by $A_i = \sum_{g_j \in C_i} g'_i$. The resulting algebra is isomorphic to $\mathfrak{S}$. As $C_0 = \{e\}$, point (i) follows. Point (ii) follows from the orbit-stabilizer theorem as each entry of the sum corresponds to a stabilizer sum. Items (iii), (iv) follow from the corresponding properties of the S-ring. Thus a noncommutative S-ring determines a noncommutative association scheme. Finally, (v) holds exactly when we have a commutative S-ring. □

We associate another algebra to each association scheme, called the *intersection algebra* of the scheme. This is generated by the matrices B_i given by $(B_i)_{jk} = (p^k_{ij})$ and which are called the *intersection matrices* or *B-matrices* of the scheme. It is not difficult to show that the intersection algebra is isomorphic to the adjacency algebra defined before.

The identification of commutative S-rings with association schemes allows us to rely on results from algebraic combinatorics to develop their representation theory. In particular, we obtain character tables of commutative S-rings which share many features with the character tables of groups. As we will prove, the method we give below recovers the group character table in the case that the S-ring in question is the class algebra. In fact, this approach has some similarity with Frobenius' original formulation of character theory [F1, F2]. As might be hoped, the character tables of association schemes will have analogous orthogonality relations. A similar inequality concerning the possible number of linear characters for an S-ring as exists for groups may also be obtained.

We exhibit each step of this construction with the commutative S-ring over S_3 given by $\{\{1\}, \{(12)\}, \{(23), (13)\}, \{(123), (132)\}\}$ and principal sets denoted $C_0, \ldots, C_3$ in the same order.

The following matrices generate an algebra isomorphic to the S-ring given above and so are sufficient to extract the intersection numbers:

$$M_0 = \begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \end{pmatrix}, \quad M_1 = \begin{pmatrix} 0&1&0 \\ 1&0&0 \\ 0&0&1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} 1&0&0 \\ 0&0&1 \\ 0&1&0 \end{pmatrix} + \begin{pmatrix} 0&0&1 \\ 0&1&0 \\ 1&0&0 \end{pmatrix},$$
$$M_3 = \begin{pmatrix} 0&1&0 \\ 0&0&1 \\ 1&0&0 \end{pmatrix} + \begin{pmatrix} 0&0&1 \\ 1&0&0 \\ 0&1&0 \end{pmatrix}.$$

We have the relations:

$$M_0 M_i = M_i \text{ for all } i \leq 3,$$
$$M_1 M_1 = M_0,$$
$$M_1 M_2 = M_3,$$
$$M_1 M_3 = M_2,$$
$$M_2^2 = M_3^2 = 2M_0 + M_3,$$
$$M_2 M_3 = 2M_1 + M_2.$$

This gives the B-matrices

$$B_0 = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&1&0 \\ 0&0&0&1 \end{pmatrix}, \quad B_1 = \begin{pmatrix} 0&1&0&0 \\ 1&0&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}, \quad B_2 = \begin{pmatrix} 0&0&1&0 \\ 0&0&0&1 \\ 2&0&0&1 \\ 0&2&1&0 \end{pmatrix}, \quad B_3 = \begin{pmatrix} 0&0&0&1 \\ 0&0&1&0 \\ 0&2&1&0 \\ 2&0&0&1 \end{pmatrix}$$

Recall that a normal matrix is a square matrix A such that $A^\dagger A = AA^\dagger$, where † is the conjugate transpose. The A_i of an association scheme are normal as each is equal to its transpose. As they also commute, a well-known result in linear algebra asserts that these can be simultaneously diagonalized. Thus the B_i can also be simultaneously diagonalized (as they form an isomorphic algebra) to matrices D_i where D_i has j-th diagonal entry D_{ij}.

The P*-matrix* or *character table* of the association scheme is then the $(d+1)\times(d+1)$ matrix

$$P = \begin{pmatrix} D_{00} & D_{01} & \cdots & D_{0d} \\ D_{10} & D_{11} & \cdots & D_{1d} \\ \vdots & \vdots & \ddots & \vdots \\ D_{d0} & D_{d1} & \cdots & D_{dd} \end{pmatrix}.$$

Of course, the character table is only determined up to some permutation of the rows and columns.

In our example, the diagonalization can be done by computer, giving the P-matrix

$$P = \begin{pmatrix} 1 & 1 & 2 & 2 \\ 1 & -1 & -2 & 2 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix}.$$

The Bose-Mesner algebra has an important dual basis of idempotents which is important to further understanding of the P-matrix. Let $A_0, \ldots, A_d$ be the adjacency matrices of some association scheme $\mathscr{X}$ on a set of size n. Write $V_0 \oplus \cdots \oplus V_r$ for the decomposition of $V = \mathbb{C}^n$ into the common eigenspaces of the A_i with their natural action on V. We assume that this decomposition is maximal; that is, when $i \neq j$, V_i and V_j will have distinct eigenvalues on at least one of the A_k. We come to an important definition:

Definition 1.21. With notation as in the preceding paragraph, let E_i be the projection onto V_i, with $m_i = \dim V_i$. Then the matrices E_i are the idempotents of $\mathscr{X}$ and the m_i are called the *multiplicities* of the scheme. ◊

Let $p_i(j)$ be the eigenvalue of A_i on V_j. Using these numbers, we can write

$$A_i = \sum_j p_i(j) E_j.$$

As asserted in the definition above, it is not hard to see that the E_i are also a basis, and so we have $r = d$ and

$$E_i = \frac{1}{n} \sum_j q_i(j) A_j,$$

for some numbers $q_i(j)$.

Definition 1.22. Define matrices P and Q by

$$P_{ij} = p_j(i) \quad \text{and} \quad Q_{ij} = q_j(i).$$

These will be respectively called the *first* and *second eigenmatrices* of $\mathscr{X}$. $\Diamond$

These will also be respectively called the *P-matrix* and the *Q-matrix* of the scheme. It is immediate that $PQ = nI = QP$. The matrix P, equivalently given before as a diagonalization of the B_i, has orthogonality relations in analogy with those of group character tables. As these will be used here and elsewhere, we take time to state them. For a proof, see Theorem 3.5 on page 62 in [BI1]. As usual, the dagger † represents the conjugate transpose.

Theorem 1.23. *Let P_{ij} and Q_{ij} be the eigenmatrices of an association scheme with valences k_i and multiplicities m_i. Then*

(i)

$$Q = \operatorname{diag}(1/k_0, \ldots, 1/k_r) P^\dagger \operatorname{diag}(m_0, \ldots, m_r);$$

(ii)

$$\sum_\ell \frac{1}{k_\ell} P_{i\ell} \overline{P_{j\ell}} = \frac{n}{m_i} \delta_{ij}; \text{ and}$$

(iii)

$$\sum_\ell m_\ell P_{\ell j} \overline{P_{\ell j}} = n k_i \delta_{ij};$$

where all sums are taken over full rows/columns of P. $\square$

Points (ii) and (iii) are called the *first* and *second orthogonality relations* of P and follow easily from (i). The *group-normalized* character table is defined to be:

$$T = \begin{pmatrix} f_0 & & & 0 \\ & f_1 & & \\ & & \ddots & \\ 0 & & & f_d \end{pmatrix} P \begin{pmatrix} \frac{1}{k_0} & & 0 \\ & \ddots & \\ 0 & & \frac{1}{k_d} \end{pmatrix}.$$

Here, the k_i are the valencies as usual and the numbers $f_i = \sqrt{m_i}$ are positive square roots of the multiplicities.

To finish the introduction, it is now our objective to show that when we take as our S-ring the centre of the group algebra, the matrix T is the group character table. We more or less follow [BI1]. First note that rows of the P-matrix for an association scheme are in bijection with 1-dimensional representations of its Bose-Mesner algebra. To be precise,

Proposition 1.24. *Let $\mathscr{X}$ be an association scheme with P-matrix P and intersection algebra $\mathfrak{U}$, having basis given by the B-matrices $B_0, \dots, B_d$. Then there are exactly $d+1$ linear representations ρ_i of $\mathfrak{U}$; these are given by the rows of P as $\rho_i(B_j) = P_{ij}$, $0 \le i \le d$.*

Proof. Say the simultaneous diagonalization that produces P is given by U. Then as the i-th row of P is given by the diagonalization of B_i, $\rho_i(u)$ is the i-th diagonal entry of $U^{-1}uU$ for any $u \in \mathfrak{U}$. This is clearly a homomorphism and thus a linear representation. More generally, any common eigenvector v of the B_i is easily seen to give a 1-dimensional representation of $\mathfrak{U}$ by sending B_i to the eigenvalue of B_i on v.

Now let ρ be any linear representation of $\mathfrak{U}$ and let $v_\rho = (\rho(B_0), \dots, \rho(B_d))^t$. Using $(B_i)_{jk} = (p_{ij}^k)$, where p_{ij}^k are the intersection numbers of $\mathscr{X}$, it is easy to verify that $\rho(B_i)v_\rho = B_i v_\rho$. In other words, v is a common eigenvector of the B_i. Thus there is a bijection between common eigenvectors of the B_i and linear representations. It remains to be shown that the v_{ρ_j} are all the common right eigenvectors.

Let $F_0, \dots, F_d$ be the $(d+1) \times (d+1)$ idempotents of $\mathfrak{U}$ corresponding to the rows of P. Up to reordering, the F_i are exactly the projections onto the common eigenspaces of the B_i, which in turn are each a linear combination of the F_i. The $d+1$ vectors v_{ρ_i} are linearly independent and thus are the common eigenvectors of the F_i. They must also therefore be the common eigenvectors of the B_i, up to a scalar multiple. $\square$

Theorem 1.25. *Let G be a finite group of order n and let P and Q the first and second eigenmatrices of $Z(\mathbb{C}G)$ as an association scheme having multiplicities m_i and valencies k_i. Then the character table T of G is a normalization of P, equal to the group-normalized table defined earlier:*

$$\begin{aligned} T &= \begin{pmatrix} \sqrt{m_0} & & \\ & \ddots & \\ & & \sqrt{m_r} \end{pmatrix} P \begin{pmatrix} \frac{1}{k_0} & & \\ & \ddots & \\ & & \frac{1}{k_r} \end{pmatrix} \\ &= \begin{pmatrix} 1/\sqrt{m_0} & & \\ & \ddots & \\ & & 1/\sqrt{m_r} \end{pmatrix} Q^{\dagger}. \end{aligned}$$

Proof. Denote the classes as $C_0 = \{1_G\}, C_1, \ldots, C_r$. As above, this naturally forms an association scheme with valences $k_i = |C_i|$. Let χ_i denote the characters of G, with degrees $f_i = \chi_i(1)$. Each irreducible character χ is known (see [JL]) to give a distinct linear representation of $Z(\mathbb{C}G)$ by linearly extending the map

$$\overline{C_i} \mapsto \frac{k_i \chi(C_i)}{\chi(1)}.$$

By the previous proposition, the rows of P also give all linear representations of $Z(\mathbb{C}G)$ via

$$\overline{C_i} \mapsto p_i(j)$$

for the j-th row. We equate these (after a possible reordering):

$$\frac{k_i \chi_j(C_i)}{f_j} = p_i(j).$$

In other words, we have

$$P = \begin{pmatrix} \frac{1}{f_0} & & \\ & \ddots & \\ & & \frac{1}{f_r} \end{pmatrix} T \begin{pmatrix} k_0 & & \\ & \ddots & \\ & & k_r \end{pmatrix}.$$

Thus the first equality holds if we can show $f_j = \sqrt{m_j}$. The second equality will then follow as we have $Q = \operatorname{diag}(1/k_0, \ldots, 1/k_r)P^\dagger \operatorname{diag}(m_0, \ldots, m_r)$.

Recall the orthogonality relation for characters: $T \operatorname{diag}(k_0, \ldots, k_r)T^\dagger = nI$. To show $f_j = \sqrt{m_j}$, we have

$$\begin{aligned} nI &= PQ \\ &= P \cdot \operatorname{diag}(\tfrac{1}{k_0}, \ldots, \tfrac{1}{k_r})P^\dagger \operatorname{diag}(m_0, \ldots, m_r) \\ &= \operatorname{diag}(\tfrac{1}{f_0}, \ldots, \tfrac{1}{f_r})T \operatorname{diag}(k_0, \ldots, k_r) \cdot \\ &\qquad \operatorname{diag}(\tfrac{1}{k_0}, \ldots, \tfrac{1}{k_r}) \operatorname{diag}(k_0, \ldots, k_r)T^\dagger \operatorname{diag}(\frac{1}{f_0}, \ldots, \frac{1}{f_r}) \operatorname{diag}(m_0, \ldots, m_r) \\ &= \operatorname{diag}(\tfrac{1}{f_0}, \ldots, \tfrac{1}{f_r})^2 \cdot nI \cdot \operatorname{diag}(m_0, \ldots, m_r), \end{aligned}$$

which completes the proof as we equate the entries of these diagonal matrices. $\square$

Chapter 2. Fusions of the Class Algebra for Projective Special Linear Groups

2.1 The Fusion Condition

Let $\mathcal{A}$ and $\mathcal{B}$ be two partitions of a set $\mathcal{X}$. We write $\mathcal{A} \prec \mathcal{B}$ if every element of $\mathcal{B}$ is a union of elements of $\mathcal{A}$. In this case, we say that $\mathcal{A}$ is *finer* than $\mathcal{B}$ (or equivalently that $\mathcal{B}$ is *coarser* than $\mathcal{A}$).

In this chapter, we give a "fusion condition," with proof, that describes when a partition of a group which yields an S-ring can be made more coarse so as to produce a new S-ring. We say in this case that the S-ring of this coarser partition *fuses* from the first. This technique will be used in the chapter to classify all subrings of the class algebra over the projective special linear groups that are S-rings. Our statement of the fusion condition and its proof will be done in the language of association schemes.

This notion of fusion occurs under multiple names in the literature. For quasigroups in particular, the equivalence of the existence of a subscheme with the fusion condition to follow was given by Johnson and Smith in their series of papers on quasigroup character theory (see [JS1, JS2]). There, fusion is said to occur when certain "magic rectangle conditions" hold given a partition of the characters and classes of a quasigroup. In the case of central S-rings, fusions are in bijection with what are called *supercharacter theories* of the group (for a very readable introduction, see [H1]). In our case, fusion is understood in terms of sub-association schemes. The lemma to follow for association schemes, is given without proof in [B1]. We first give Bannai's fusion condition and then state the magic rectangle condition given by Johnson (as in [J1, HJ]) and then prove the equivalence of these.

Lemma 2.1. *Say that a commutative association scheme has adjacency matrices given by $\{A_0, \ldots, A_d\}$ and idempotents $\{E_0, \ldots, E_d\}$. Let P be the character table of the scheme, so that P_{ij} is the eigenvalue of A_j corresponding to E_i. Let $\mathcal{A}$ be a partition of the A_i and $\mathcal{B}$ be a partition of the E_j. Let the matrices B_i, F_j be the respective sums of the A_i, E_j implied by* *the partition and assume that $B_0 = A_0$, $E_0 = F_0$. Then the B_i give an association scheme with idempotents F_j if and only if for each i, the transpose B_i^t is equal to B_j for some j and the* fusion condition *holds: namely, for each $\alpha \in \mathcal{A}$, $\beta \in \mathcal{B}$, the sum*

$$\sum_{i \in \beta} P_{ji} \text{ is constant for all } j \in \alpha.$$

The association scheme given by the B_i is called a *sub-association scheme* of that given by the A_i. The lemma inspires the following definition:

Definition 2.2. Given partitions of the A_i, E_i such that the fusion condition holds, we will call a pair consisting of one element from each partition a *magic rectangle*. We identify this pair with the corresponding submatrix of the character table as in Lemma 2.1. $\Diamond$

Thus, the fusion condition says merely that row sums are constant in each magic rectangle. Before giving a proof, we first give as an example fusing the S-ring contained in $\mathbb{C}S_3$ given by

$$A_0 = 1, \quad A_1 = (123), \quad A_2 = (132), \quad A_3 = (12) + (23) + (31)$$

to the class algebra. The character table (not normalized) is given by:

$$\left(\begin{array}{c|cc|c} 1 & 1 & 1 & 3 \\ \hline 1 & 1 & 1 & -3 \\ \hline 1 & \omega^2 & \omega & 0 \\ 1 & \omega & \omega^2 & 0 \end{array}\right),$$

where we have used lines within the table to represent the magic rectangles. We denote the central idempotents by $E_0, \ldots, E_3$ given the ordering implied in the rows of the table.

Summing columns 2 and 3 together in this way gives the table

$$\left(\begin{array}{c|c|c} 1 & 2 & 3 \\ \hline 1 & 2 & -3 \\ \hline 1 & -1 & 0 \\ 1 & -1 & 0 \end{array}\right),$$

so that the magic-rectangle condition is implied when we partition the rows of the character table by $\{\{E_0\}, \{E_1\}, \{E_2, E_3\}\}$.

Proof of Lemma 2.1. We know by Proposition **??** that the commuting matrices B_i will form an association scheme if and only if the following hold:

(i) $\sum_i B_i = J$, the all-one matrix;

(ii) for each i, $B_i^T = B_j$ for some j;

(iii) the intersection numbers p_{ij}^k exist; i.e. the B_i form a commutative algebra.

Note that (1) and (2) hold by hypothesis. Suppose that the fusion condition is satisfied. We must show that the B_i form an algebra. When the magic rectangle condition is satisfied, it is clear as above that we have common eigen-spaces for the B_i; these are the sums of the eigen-spaces determined by the partition of the idempotents. This is a complete set of idempotents, and so the Krein parameters exist. From this, we obtain intersection numbers, and so (3) holds.

Suppose now that the B_i form a sub-scheme of that given by the A_i. We must show that the magic-rectangle condition is satisfied. Then rows of the table formed by summing the appropriate columns give a total of $d + 1$ 1-dimensional representations of the algebra formed by the B_i given by the action of the B_i on their eigen-spaces. There can be at most $|\mathcal{B}|$ of these, and so some must be repeated in the table. The partition of the idempotents must be given by grouping these according as the rows of the summed table coincide. The magic rectangle condition is satisfied given this partition. $\square$

In fact, as indicated in the proof, the row sums are the new entries of the fused character table. A similar proof shows that we may replace the row-sum condition on the first eigenmatrix with a row-sum condition on the second eigenmatrix Q:

Proposition 2.3. *The condition that for all $\alpha \in \mathcal{A}$, $\beta \in \mathcal{B}$, the sum $\sum_{j\in\beta} P_{ij}$ be constant for all $i \in \alpha$ in the fusion condition can be equivalently replaced with the condition that $\sum_{j\in\alpha} Q_{ij}$ be constant for all $i \in \beta$. These sums correspond to entries of the fused Q-matrix.*

In [JS1], it is shown that a partition of classes for a finite group (with a compatible partition of characters) gives an S-ring if and only if certain equivalent 'magic rectangle' conditions are satisfied. We repeat these conditions here with a proof of the equivalence:

Let $C_1, C_2, \ldots, C_r$ be the classes in some element of the partition of the classes (with representatives c_i) and $k_1, \ldots, k_r$ let be the conjugacy class sizes. Also take $\chi_1, \ldots, \chi_s$ to be the characters (rows of the group-normalized table) in some element of the partition of the characters, and d_i to be the corresponding degrees. Then these two elements of the partitions determine a magic rectangle if the following condition holds (the partitions of characters and classes are said to satisfy the magic rectangle conditions if this holds for each such pair):

Define the numbers

$$\tau_j = \frac{\sum_{i=1}^{r} k_i \chi_j(c_i)}{d_j \sum_{i=1}^{r} k_i},$$

for each of the χ_j, and

$$\tau'_j = \frac{\sum_{i=1}^{s} d_i \chi_i(c_j)}{\sum_{i=1}^{s} d_i^2},$$

for each of the C_j. These may be seen as a weighted average across rows/columns of the rectangle. Then we require that the numbers τ_j be constant for each j and equal to the numbers τ'_j, which should also be constant for each j. We call this the *Johnson–Smith fusion condition.*

Lemma 2.4. *The Johnson–Smith fusion condition is equivalent to Bannai's magic rectangle condition on row and column sums as given previously.*

Proof. Suppose that Bannai's condition is satisfied. We know by Theorem 1.25 that the P-matrix and the group-normalized character table are related by

$$T = \begin{pmatrix} d_0 & & \\ & \ddots & \\ & & d_r \end{pmatrix} P \begin{pmatrix} \frac{1}{k_0} & & \\ & \ddots & \\ & & \frac{1}{k_r} \end{pmatrix},$$

where the d_i are the degrees of the irreducible characters, and k_i are the conjugacy class sizes. Employing the notation of Johnson yields $\chi_i(c_j) = T_{ij} = \frac{d_i}{k_j} P_{ij}$.

Suppose we have a constant row sum:

$$\sum_j P_{ij} = \frac{\sum_j k_j \chi_i(c_j)}{d_i}.$$

We show that the τ_i, τ_i' are a normalization of the entries of the fused character table. As the new class sizes will be sums of the old, and the degree becomes $\sqrt{\sum_m d_m^2}$, the fused character table will have the value

$$\frac{\sum_j k_j \chi_i(c_j)}{d_i} \cdot \frac{\sqrt{\sum_m d_m^2}}{\sum_j k_j}.$$

The τ_i of Johnson–Smith are obtained by normalizing by a factor of

$$\eta_i = \sqrt{\sum_m d_m^2}.$$

Thus, we have

$$\begin{aligned} \tau_i &= \frac{\sum_j k_j \chi_i(c_j)}{d_i} \cdot \frac{\sqrt{\sum_m d_m^2}}{\sum_j k_j} \cdot \frac{1}{\sqrt{\sum_m d_m^2}} \\ &= \frac{\sum_j k_j \chi_i(c_j)}{d_i \sum_j k_j}. \end{aligned}$$

Thus the τ_i of Johnson are constant, as desired.

If for some submatrix of the second eigenmatrix the sums across rows are constant, as we know

$$T = \operatorname{diag}(1/\sqrt{d_0}, \ldots, 1/\sqrt{d_r})Q^\dagger,$$

we write

$$\sum_j \overline{Q_{ij}} = \sum_j d_j \chi_j(c_i).$$

The new degree corresponding to this entry will be the number $\sqrt{\sum_j d_j^2}$. Normalizing by the η_j factor gives

$$\begin{aligned}\tau_j' &= \sum_i d_i \chi_i(c_j) \cdot \frac{1}{\sqrt{\sum_m d_m^2}} \cdot \frac{1}{\sqrt{\sum_m d_m^2}} \\ &= \frac{\sum_i d_i \chi_i(c_j)}{\sum_i d_i^2},\end{aligned}$$

which is the same for each choice of i, corresponding to a row of Q. $\square$

By uniqueness of the 1-dimensional characters of an association scheme, given some partition of a group determining an S-ring, the characters must fuse uniquely. One can ask how the partition of characters is related to the partition of classes in a fusion. For a cyclic group, this is especially easy to describe. Let G be an abelian group and let $G^* \cong G$ be the dual group of characters. If $\mathfrak{S} \leq \mathbb{Q}G$ is an S-ring over G, the dual S-ring $\mathfrak{S}^* \leq \mathbb{Q}G^*$ is given by sums of partition elements of the characters leading to the fusion. That this is in fact an S-ring is a consequence of Kawada–Delsarte duality and is Theorem II.6.3 of [BI1]:

Theorem 2.5. *Let $\mathfrak{S}$ be an S-ring over a finite abelian group and $\mathfrak{S}^*$ its dual. Then $\mathfrak{S}^*$ is an S-ring with* $\dim \mathfrak{S} = \dim \mathfrak{S}^*$ *and the intersection numbers of $\mathfrak{S}^*$ are the Krein parameters of $\mathfrak{S}$.*

It follows that the double-dual recovers the original S-ring. When the abelian group in question is cyclic, we can use this theorem to give a very clean description of how the primitive sets of $\mathfrak{S}$ and $\mathfrak{S}^*$ relate. For the trivial S-ring or an orbit S-ring, the fusion condition can be used to show that the dual S-ring is Cayley-isomorphic via the isomorphism $G \cong G^*$. The dual of a dot-product of semi-wedge product of S-rings is described in the following lemma:

Lemma 2.6. *Let $G = \mathcal{C}_n$ be a cyclic group. If $G = H \times K$ and $\mathfrak{S} = \mathfrak{S}_H \cdot \mathfrak{S}_K$ is a dot product of S-rings, then*

$$\mathfrak{S}^* = \mathfrak{S}_H^* \cdot \mathfrak{S}_K^*.$$

If $\mathfrak{S} = \mathfrak{S}_H \Delta_K \mathfrak{S}_{G/K}$ is a wedge product of S-rings with wedge decomposition $1 < K \leq H < G$, then the dual S-ring $\mathfrak{S}^*$ has wedge decomposition $1 < (G/H)^* < (G/K)^* < G^*$ and

$$\mathfrak{S}^* = \mathfrak{S}_{G/K}^* \Delta_{(G/H)^*} \mathfrak{S}_H^*.$$

Proof. First let $\mathfrak{S}$ be a dot product of S-rings as described. Since G is a direct product, the character table of G is Kronecker product of the character tables of H and K. If $\psi = \{\psi_1, \ldots, \psi_r\}$ is an element of the partitions of characters of $\mathfrak{S}_H$ and $\omega = \{\omega_1, \ldots, \omega_r\}$ are such for the S-rings $\mathfrak{S}_K$, the fusion condition will be satisfied on rectangles having columns indicated by the dot product and having row $\{\psi_i \cdot \omega_j : \psi_i \in \psi, \omega_j \in \omega\}$ since the Kronecker product of magic rectangles is a magic rectangle. This dictates the principal sets of $(\mathfrak{S}_H \cdot \mathfrak{S}_K)^*$.

Now let $\mathfrak{S}$ be a semi-wedge product as indicated. We treat G/K as a subgroup of G in the wedge product. The compatibility conditions are $\overline{K} \in \mathfrak{S}_H$ and $\pi^*(\mathfrak{S}_H) = (\mathbb{C}H/K) \cap \mathfrak{S}_{G/K}$. It follows that $\overline{G/H} \in \mathfrak{S}_{G/K}$. Now note that the 'inflation' of a magic rectangle is a magic rectangle. Thus we obtain a wedge-decomposable partition of the characters and the indicated wedge product must be valid. □

The next lemma will be relevant in the sections to come.

Lemma 2.7. *Let $G = \mathcal{C}_n$ be a cyclic group with $J \leq G$ and $\mathfrak{S}$ an S-ring over G with $\mathfrak{S}^*$ the dual S-ring over G^*. Then J is an $\mathfrak{S}$-subgroup if and only if G/J is an $\mathfrak{S}^*$-subgroup.*

Proof. If $\mathfrak{S}$ is the trivial S-ring, then note that the only $\mathfrak{S}$-subgroups are the trivial ones. The claim is true for orbit S-rings since every subgroup of a cyclic group is characteristic.

For a dot-product of S-rings, use induction and apply the inductive hypothesis with Lemma 2.6 to $G = H \times K$.

Now let $\mathfrak{S} = \mathfrak{S}_H \Delta_K \mathfrak{S}_{G/K}$ be a semi-wedge product. For J to be an $\mathfrak{S}$-subgroup, one sees by the compatibility condition of the semi-wedge product that it is necessary both that $H \cap J$ be an $\mathfrak{S}_H$-subgroup and that $\pi(C)$ be an $\mathfrak{S}_{G/K}$-subgroup. The analogous statement holds for G/J and the dual S-ring $\mathfrak{S}^*$. Thus the lemma holds for $\mathfrak{S}$ if and only if it holds for $\mathfrak{S}_H$ and $\mathfrak{S}_{G/K}$. $\square$

In particular, if $\mathfrak{S} \leq \mathbb{Q}\mathcal{C}_{2k}$ is an S-ring over a cyclic group of even order, then the character of order 2 fails to fuse exactly when $\mathcal{C}_k$ is an $\mathfrak{S}$-subgroup.

2.2 Fusions of PSL$(2, q)$

In this section, we first give the character table of PSL$(2, q)$, where q is a power of 2. Let $a = e^{2\pi i/(q^2-1)}$. In what follows set $\epsilon = a^{q-1}$, $\delta = a^{q+1}$, and

$$u_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad d_i = \begin{pmatrix} \epsilon^i + \epsilon^{-i} & 0 \\ 0 & \epsilon^i + \epsilon^{-i} \end{pmatrix}, \quad v_i = \begin{pmatrix} \delta^i + \delta^{-i} & 0 \\ 0 & \delta^i + \delta^{-i} \end{pmatrix}.$$

These matrices being conjugacy class representatives, the character table for this group of order $q(q^2 - 1)$ is given in [JL]:

$$
\begin{array}{c||cccccccc}
 & & q & q-1 & \cdots & q-1 & q+1 & \cdots & q+1 \\
 & I & u_1 & d_1 & \cdots & d_{\frac{q-2}{2}} & v_1 & \cdots & v_{\frac{q}{2}} \\
\hline\hline
\lambda_0 & 1 & 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\
\psi_0 & q & 0 & 1 & \cdots & 1 & -1 & \cdots & -1 \\
\psi_{01} & q+1 & 1 & & & & & & \\
\vdots & \vdots & \vdots & & M(\epsilon) & & & 0 & \\
\psi_{0\frac{q-2}{2}} & q+1 & 1 & & & & & & \\
\chi_1 & q-1 & -1 & & & & & & \\
\vdots & \vdots & \vdots & & 0 & & & -M(\delta) & \\
\chi_{\frac{q}{2}} & q-1 & -1 & & & & & &
\end{array}
$$

where the centralizer sizes are given above and the block matrices $M(\epsilon)$, $M(\delta)$ of dimensions $\frac{q-2}{2} \times \frac{q-2}{2}$ and $\frac{q}{2} \times \frac{q}{2}$ respectively have entries

$$M(\epsilon)_{ij} = \epsilon^{ij} + \epsilon^{-ij} \qquad \text{and} \qquad M(\delta)_{ij} = \delta^{ij} + \delta^{-ij}.$$

It is worth noting that each conjugacy class is self-inverse.

Critical to our classification is the observation that the matrices M_δ, M_ϵ are the character tables (neglecting the identity class and character) of the symmetric S-rings over the cyclic groups C_{q-1}, C_{q+1} respectively. Recall that any S-ring containing this one is called *symmetric* so that any symmetric S-ring over a cyclic group is given by a fusion of this one. Thus, fusions of the matrices M_δ, M_ϵ are in bijection with symmetric S-rings over the appropriate cyclic group. This fact will be used in the proof of the following proposition, which leads to the main result of the chapter.

Proposition 2.8. *The following hold for any fusion of the class algebra of* $\mathrm{PSL}(2, 2^q)$*, except in the case of the trivial S-ring:*

(1) in any partition of the characters giving rise to a fusion of the class algebra, ψ_0 is in a singleton set;

(2) in any partition of the classes, u_1 is in a singleton set;

(3) the characters ψ_{0i} do not fuse with the characters χ_i;

(4) the v_i and d_i classes do not fuse.

Proof. (1) Assume to the contrary that ψ_0 fuses with some other character. Take some element of the partition of the classes that contains r of the d_i classes and s of the v_i classes. Since we may discount the trivial S-ring, we may assume this element of the partition does not contain u_1. It will be easy to show that the magic rectangle condition can not be satisfied in this case. In the calculation, note that the number τ_j corresponding to the ψ_0 row in this rectangle is given by

$$\tau_j = \frac{\sum_{i=1}^{r} k_i \psi_0(c_i)}{q\sum_{i=1}^{r} k_i}.$$

Since there are r of the d_i classes and s of the v_i classes and since these have respective class sizes $\frac{q(q^2-1)}{q-1} = q(q+1)$ and $\frac{q(q^2-1)}{q+1} = q(q-1)$, this sum becomes

$$\frac{(q+1)q \cdot 1 \cdot r + (q-1)q \cdot (-1) \cdot s}{q(rq(q+1) + sq(q-1))}.$$

We have two cases to consider; assume first that there is some ψ_{0i} character in the rectangle in addition to ψ_0. With Σ representing the sum across the ψ_{0i} row, equality of magic rectangle numbers along the ψ_{0i} and ψ_0 rows gives the equations

$$\begin{aligned}
\frac{(q+1)q \cdot 1 \cdot r + (q-1)q \cdot (-1) \cdot s}{q(rq(q+1) + sq(q-1))} &= \frac{(q+1)q \cdot \Sigma + (q-1)q \cdot 0}{(q+1)(rq(q+1) + sq(q-1))}, \text{ so that} \\
\frac{q(q+1)r - q(q-1)s}{q} &= \frac{q(q+1)\Sigma}{q+1}, \text{ which gives} \\
(q+1)r - (q-1)s = q\Sigma.
\end{aligned}$$

This shows Σ is rational. However, Σ is an algebraic integer, being a sum of roots of unity. Since the only rational algebraic integers are the integers, Σ is an integer and we have

$r - s + \frac{r+s}{q} = \Sigma \in \mathbb{Z}$ and so $q|(r+s)$. As $r \leq \frac{q-2}{2}$ and $s \leq \frac{q}{2}$, this is achieved only when $r = s = 0$.

In the second case, say there is some χ_i in the same magic rectangle as ψ_0 (again, Σ is the sum of roots of unity across the χ_i row). As before, we assume the rectangle has r of the d_i classes and s of the v_i classes so that the row conditions can be written

$$\begin{aligned}\frac{(q+1)q \cdot 1 \cdot r + (q-1)q \cdot (-1) \cdot s}{q(rq(q+1) + sq(q-1))} &= \frac{(q-1)q \cdot \Sigma + (q-1)q \cdot 0}{(q-1)(rq(q+1) + sq(q-1))}, \text{ so that} \\ \frac{q(q+1)r - q(q-1)s}{q} &= \frac{q(q-1)\Sigma}{q-1}, \text{ which gives} \\ (q+1)r - (q-1)s = q\Sigma, &\end{aligned}$$

leading to the same contradiction as in the previous case.

(2) By way of contradiction, we assume that some magic rectangle exists containing r of the ψ_{0i} characters and s of the χ_i and where the class u_1 fuses some other class. As in the proof of (1), there are two cases to consider. Say one of the d_i is also in the rectangle. Denote by Σ the column sum of character values of the ϵ^j in that column of the rectangle. Recall that the column sums of the Johnson–Smith magic rectangle condition are

$$\tau_j' = \frac{\sum_{i=1}^{s} d_x \chi_i(c_j)}{\sum_{i=1}^{s} d_i^2}.$$

Thus, the column condition for the u_1 and the d_i row gives

$$\begin{aligned}\frac{r(q+1) - s(q-1)}{r(q+1)^2 - s(q-1)^2} &= \frac{(q+1)\Sigma}{r(q+1)^2 - s(q-1)^2}, \text{ so that} \\ \Sigma &= r - s + \frac{2s}{q+1}.\end{aligned}$$

As Σ is an integer we have $(q+1)|s$, but $s \leq \frac{q}{2}$. This is a contradiction.

Now say one of the v_i is in the rectangle. Similarly, column conditions give

$$\frac{r(q+1)-s(q-1)}{r(q+1)^2-s(q-1)^2} = \frac{(q-1)\Sigma}{r(q+1)^2-s(q-1)^2} \text{ so that}$$
$$\Sigma = r - s + \frac{2r}{q+1}.$$

Similarly, $(q+1)|r$, but $r \leq \frac{q-2}{2}$, a contradiction.

To prove (3), we will first show that a partition of the characters such that some element contains both ψ_{0i} characters and χ_i characters gives a partition where this element is replaced by two elements consisting of those ψ_{0i} and χ_i characters. Suppose we have a magic rectangle with r characters ψ_{0i} and s of the characters χ_i. In a rectangle given by this set and just characters d_i, then the claim is true; likewise when the classes constituting the rectangle are characters v_i. Now suppose we have a classes of type v_i and b classes of type d_i. The column conditions then give:

$$\frac{q(q+1)\Sigma'_\epsilon}{rq^2(q+1)^2+sq^2(q-1)^2} = \frac{q(q-1)\Sigma'_\delta}{rq^2(q+1)^2+sq^2(q-1)^2};$$
$$(q+1)\Sigma'_\epsilon = (q-1)\Sigma'_\delta.$$

The number Σ_δ will therefore be zero exactly when Σ_ϵ is. If these are both nonzero, we compute their ratio to be $\frac{q+1}{q-1} \in \mathbb{Z}$. However, this can not be an integer since we may assume $q > 2$. It follows that both of these columns sums are zero.

By a similar proof, we can show that in any partition of the classes such that some element contains both v_i d_j, row sums are zero and so the Johnson–Smith condition continues to be satisfied if this partition element is split in two — one element containing the v_i and the other containing the d_j.

To finish the demonstrations of (3) and (4), note that we have now shown that in a magic subrectangle of the character table for $\mathrm{PSL}(2,q)$ whose columns are given by both some of the v_i and d_j, the row sums across the v_i (and d_j) must be zero. Splitting these principal sets into their v_i and d_j parts also gives a fusion. We note now that this is not possible; such a situation yields an S-ring character table for a cyclic group with a "cross" of zeros; i.e. all but the uppermost entry of some column is zero, and similarly for some row. Under such conditions, column/row orthogonality conditions cannot be satisfied; the orthogonality condition of the almost zero row and any other will be the product of degrees of those rows, which is a positive number and not equal to zero. For (4), we would similarly obtain a column of zeros. □

The facts (1)–(5) of the previous proposition, together with the fact that fusions of the matrices M_ϵ, M_δ are in bijection with symmetric S-rings over C_{q+1} and C_{q-1}, respectively, give the following theorem:

Theorem 2.9. *Fusions of the class algebra for* $\mathrm{PSL}(2, 2^q)$ *can be understood entirely in terms of the fusions of the* M_ϵ, M_δ *submatrices; aside from the trivial S-ring, the class-algebra fusions are in bijection with pairs of possible fusions of symmetric S-rings over* C_{q-1}, C_{q+1}.

We now consider $\mathrm{PSL}(2, 16)$ as an example. Taking $\epsilon = e^{2\pi i/17}$, we label the columns of $M(\epsilon)$ by i in place of v_i and the rows by j in place of ψ_{0j} so that this matrix is:

	3	6	1	2	4	5	7
5	0	0	5	5	5	5	5
1	3	6	1	2	4	5	7
4	3	6	4	7	1	5	2
6	3	6	6	3	6	0	3
2	6	3	2	4	7	5	1
3	6	3	3	6	3	0	6
7	6	3	7	1	2	5	4

where, in the table, we write i in place of $\epsilon^i + \epsilon^{-i}$. This partition corresponds to the S-ring over C_3 which is the wedge product of the group ring over C_{15} with the orbit S-ring over C_5 given by the partition $\{\{i, i^{-1}\} : i \in C_5\}$. Partition the matrix $-M(\delta)$ trivially (all columns in a single partition element). The fused character table is then seen to be

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 16 & 0 & 1 & 1 & 1 & -1 \\ 17 & 1 & 2 & 2 & -1 & -1 \\ \sqrt{3\cdot 17} & \frac{1}{q+1} & \frac{\epsilon^3+\epsilon^{-3}}{17\sqrt{3}} & \frac{\epsilon^6+\epsilon^{-6}}{17\sqrt{3}} & \frac{-1}{17\sqrt{3}} & 0 \\ \sqrt{3\cdot 17} & \frac{1}{q+1} & \frac{\epsilon^6+\epsilon^{-6}}{17\sqrt{3}} & \frac{\epsilon^3+\epsilon^{-3}}{17\sqrt{3}} & \frac{-1}{17\sqrt{3}} & 0 \\ 2\sqrt{30} & \frac{1}{1-q} & 0 & 0 & 0 & -1 \end{bmatrix},$$

where the columns and rows are arranged as in the group character table given at the start of the section. This computation can be confirmed by hand without difficulty, or by use of the code provided in the appendix of this thesis at §A.3.

Since there are 8 symmetric S-rings over C_{15} and 4 over C_{17}, there are 32 possible fusions of the class algebra of PSL(2, 16) besides this one.

2.3 PSL$(2, p^n)$, $p^n \equiv 1 \bmod 4$

The group character table of PSL$(2, p^n)$ with p an odd prime varies as $q = p^n \equiv \pm 1 \bmod 4$. In both cases, the P-matrices of these are given in [B1], with a small error which we correct here. We first take $q \equiv 1 \bmod 4$. The first eigenmatrix for the class algebra is:

	1	u	u'	v^l	w^m	w^b
1_G	1	$\frac{q^2-1}{2}$	$\frac{q^2-1}{2}$	$q(q-1)$	$q(q+1)$	$\frac{1}{2}q(q+1)$
ψ	1	0	0	$-(q-1)$	$q+1$	$\frac{1}{2}(q+1)$
θ_i	1	$-\frac{q+1}{2}$	$-\frac{q+1}{2}$	$-q(\sigma^{2il}+\sigma^{-2il})$	0	0
χ_j	1	$\frac{q-1}{2}$	$\frac{q-1}{2}$	0	$q(\rho^{2jm}+\rho^{-2jm})$	$q(-1)^j$
ξ_1	1	$(q-1)\lambda^+$	$(q-1)\lambda^-$	0	$2q(-1)^m$	$q(-1)^b$
ξ_2	1	$(q-1)\lambda^-$	$(q-1)\lambda^+$	0	$2q(-1)^m$	$q(-1)^b$

.

Here, the θ_i are indexed from $1 \le i \le a = \frac{q-1}{4}$; the χ_j from $1 \le j < b = a$; the v^l from $1 \le l \le a$ and the w^m from $1 \le m < b$. Also, σ denotes a primitive root of unity of order $q+1$ while ρ is primitive of order $q-1$. We also have $\lambda^{\pm} = \frac{1}{2}(1 \pm \sqrt{q})$. Each class is self inverse, except that $u^{-1} = u'$.

Thus the Q-matrix is

	1_G	ψ	θ_i	χ_j	ξ_1	ξ_2
1	1	q^2	$(q-1)^2$	$(q+1)^2$	$\left(\frac{q+1}{2}\right)^2$	$\left(\frac{q+1}{2}\right)^2$
u	1	0	$-(q-1)$	$q+1$	$\frac{q+1}{2}\lambda^+$	$\frac{q+1}{2}\lambda^-$
u'	1	0	$-(q-1)$	$q+1$	$\frac{q+1}{2}\lambda^-$	$\frac{q+1}{2}\lambda^+$
v^l	1	$-q$	$(q-1)(\sigma^{2il} + \sigma^{-2il})$	0	0	0
w^m	1	q	0	$(q+1)(\rho^{2jm} + \rho^{-2jm})$	$\frac{q+1}{2}(-1)^m$	$\frac{q+1}{2}(-1)^m$
w^b	1	q	0	$2(q+1)(-1)^j$	$\frac{q+1}{2}(-1)^b$	$\frac{q+1}{2}(-1)^b$

Note that the top row gives the multiplicities as expected.

Write M_σ for the square submatrix having rows θ_i and columns v^l. Similarly, write M_ρ for that given by w^m, w^b, χ_j and ξ_1. We begin with a proposition analogous to Proposition 2.8 of the previous section which allows us to classify S-rings contained in the centralizer algebra in terms of fusions of M_σ, M_ρ.

Proposition 2.10. *When $q \equiv 1 \bmod 4$, the following hold except in the case of the trivial S-ring:*

(1) Fusions of the submatrix M_σ are in bijection with symmetric S-rings over $C_{\frac{q+1}{2}}$. Fusions of the submatrix given by M_ρ are in bijection with symmetric S-rings over $C_{\frac{q+1}{2}}$.

(2) The character ψ does not fuse with any other character.

(3) The classes u, u' fuse only with each other. They fuse exactly when ξ_1, ξ_2 fuse.

(4) The characters in the set $\{\chi_j, \xi_1, \xi_2\}$ fuse only among themselves. This also holds for the characters $\{\theta_i\}$, the classes $\{w^m, w^b\}$ and the classes $\{v^l\}$.

Proof. (1) Due the the squaring of σ, ρ in the character table, the proof is the same as in the p even case given previously in this chapter. The row ξ_1 of M_ρ corresponds to the character of order 2 and the column w^b corresponds to the group element of order 2.

(2) We now show that ψ does not fuse with any other character except in the trivial case. Take an element ϵ of the partition of classes that contains r of the v^l and s of the w^m. The sum along the ψ-row of the P-matrix is

$$\begin{cases} q(s-r)+r+s & \text{if } w^b \notin \epsilon; \\ q(s-r+\frac{1}{2})+r+s+\frac{1}{2} & \text{else.} \end{cases}$$

Suppose ψ fuses with one of the θ_i. Writing Σ for the appropriate sum of roots of unity within the matrix M_σ, the row sum for θ_i is

$$\begin{cases} -q\Sigma & u, u' \notin \epsilon; \\ -q\Sigma - \frac{q+1}{2} & \text{one of } u, u' \in \epsilon; \\ -q\Sigma - (q+1) & u, u' \in \epsilon. \end{cases}$$

Each of these six total cases implies that $\Sigma \in \mathbb{Q}$, an integer as Σ is as sum of algebraic integers. Thus each equality leads to q dividing one of

$$\begin{cases} r+s & w^b, u, u' \notin \epsilon; \\ \frac{q}{2}+s+r+\frac{1}{2} & w^b \in \epsilon,\ u, u' \notin \epsilon; \\ \frac{q}{2}+\frac{1}{2}+r+s & \text{one of } u, u' \in \epsilon,\ w^b \notin \epsilon; \\ 1+r+s & \text{one of } u, u' \in \epsilon,\ w^b \in \epsilon; \\ 1+r+s & w^b \notin \epsilon,\ u, u' \in \epsilon; \\ r+s+\frac{3}{2}+\frac{q}{2} & w^b, u, u' \in \epsilon. \end{cases}$$

The fact that $s \leq \frac{q-1}{4} > r$ eliminates the first five possibilities. The last case is only possible if r and s attain their greatest possible values, which leads to the trivial S-ring as all other classes were already included.

Suppose now that ψ fuses with one of the χ_j. The sum along this row is one of

$$-q\Sigma = \begin{cases} \frac{q-1}{2}, \\ \frac{q-1}{2} \pm q, \\ q-1, \\ q-1 \pm q, \end{cases}$$

where Σ is the appropriate sum of roots of unity.

When we assume $w^b \notin \epsilon$, these lead to the following numbers being divisible by q:

$$\begin{cases} r+s-\frac{q-1}{2} & \text{exactly one of } u, u' \in \epsilon; \\ r+s+1 & \text{else,} \end{cases}$$

which are impossibilities based on the restriction on the maximum values of r, s.

If instead $w^b \in \epsilon$, we have q dividing

$$\begin{cases} r+s-\frac{q-1}{2}+\frac{q+1}{2} & \text{if exactly one of } u, u' \in \epsilon; \\ r+s+1+\frac{q+1}{2} & \text{else.} \end{cases}$$

The last case is the only possible one, which yields the trivial S-ring.

It suffices now to show that ψ does not fuse with ξ_1; as the last two rows of the P-matrix are related by a Galois automorphism, ψ will fuse with ξ_1 if and only if it fuses with ξ_2. If just one of u, u' are in ϵ, the possible row sums are $\frac{1}{2}(q-1)(1 \pm \sqrt{q})$ plus a multiple of q. Equating with the row sum for ψ shows that $\sqrt{q}$ is rational, so that q is a square. In fact, we have $\pm\sqrt{q} = s - r + \frac{4s}{q-1} + kq$, where k is a sum of powers of -1 from the bottom right of the P-matrix. When $w^b \notin \epsilon$,

$$\tfrac{1}{2}(q-1)(1 \pm \sqrt{q}) + kq = q(s-r) + r + s, \text{ giving}$$
$$\pm\sqrt{q} = -2k + 4s,$$

where $k = \sum_m (-1)^m \in \mathbb{Z}$, which shows that q is even. When $w^b \in \epsilon$, we obtain $\pm\sqrt{q} = 2 - 2(k+1) + 4s$, again a contradiction.

If $u, u' \notin \epsilon$, we obtain $q|(r+s)$ or $q|(r+s+\frac{q+1}{2})$ which is not possible. Very similar reasoning to the above finishes the demonstration when $u, u' \in \epsilon$ to show that only the trivial S-ring can occur.

(3) Suppose that w^b fuses with one of u, u'. By point (2), there must be a magic rectangle having only r of the θ_i and s of the χ_j characters. The row condition on the Q-matrix shows that we must have

$$-r(q-1) + s(q+1) = 2(q+1)\sum_j (-1)^j.$$

Dividing by $q+1$, we see that $(q+1)|r(q-1)$ so that $r = 0$. Thus we can assume that there exists a magic rectangle containing w^b, one or both of u, u', and only the characters θ_i. Using the row sum on the P-matrix, we see that this can not be. We have shown that w^b does not fuse nontrivially with the classes u, u'.

Now suppose that one of u, u' fuses with some of the v^l and w^m. We can find a magic rectangle with r of the θ_i and s of the χ_j characters. This leads to

$$-\frac{q+1}{2} - q\Sigma_\sigma = q\Sigma_\rho$$

and so $q|(q+1)$, a contradiction. The situation is similar when both of u, u' fuse with some of the v^l and w^m.

If u, u' fuse then ξ_1, ξ_2 take the same values on all fused classes as we see from the first eigenmatrix. This argument reverses.

(4) The proof of this point is similar to the analogous proof for the even-power case. To summarize, suppose that some of the w^m, v^l fuse. If characters θ_i, χ_j fuse, we write Σ_σ, Σ_ρ for appropriate sums of roots of unity of order $|\sigma|$, $|\rho|$ in rows of the Q-matrix. This gives

$$(q-1)\Sigma_\sigma = (q+1)\Sigma_\rho,$$

which implies that $\Sigma_\sigma = \Sigma_\rho = 0$ since Σ_σ and Σ_ρ are algebraic integers and the integers $q-1$, $q+1$ have distinct prime divisors when $q > 3$. If some of the θ_i are in a singleton set, we immediately sum in the P-matrix to obtain zeros. By part (1), this leads to a character table of a symmetric S-ring with a row or column having almost all entries zero. It is impossible for the orthogonality relations to be met in this case. The proof that classes v^l, w^m do not fuse is similar. □

From the proposition, any fusion is determined by a choice of symmetric S-ring over $C_{\frac{q+1}{2}}$ and a symmetric S-ring over $C_{\frac{q-1}{2}}$. If it happens that ξ_1, ξ_2 fuse together with some collection of the χ_j, then this choice determines the fusion as u, u' must fuse. On the other hand, if ξ_1, ξ_2 do not fuse with the χ_j, then this choice allows for two possible fusions as u, u' may be chosen to fuse or not.

Theorem 2.11. *Suppose $q = p^n \equiv 1 \bmod 4$ is a prime power. Let n_+ be the number of symmetric S-rings over $\mathcal{C}_{\frac{q+1}{2}}$, n_- the number of symmetric S-rings over $\mathcal{C}_{\frac{q-1}{2}}$, and n'_- be the number of symmetric S-rings over $\mathcal{C}_{\frac{q-1}{2}}$ such that the character of order 2 does not fuse. Then the number of nontrivial central S-rings over $\mathrm{PSL}(2,q)$ is equal to $n_+(n_- + n'_-)$.* □

2.4 PSL$(2, p^n)$, $p^n \equiv 3 \bmod 4$

The character table for the case $q \equiv 3 \bmod 4$ can also be found in [B1]:

	1	u	u'	v^l	v^a	w^m
1_G	1	$\frac{q^2-1}{2}$	$\frac{q^2-1}{2}$	$q(q-1)$	$\frac{1}{2}q(q-1)$	$q(q+1)$
ψ	1	0	0	$-(q-1)$	$-\frac{1}{2}(q-1)$	$q+1$
θ_i	1	$-\frac{q+1}{2}$	$-\frac{q+1}{2}$	$-q(\sigma^{2il}+\sigma^{-2il})$	$q(-1)^i$	0
χ_j	1	$\frac{q-1}{2}$	$\frac{q-1}{2}$	0	0	$q(\rho^{2jm}+\rho^{-2jm})$
ξ_1	1	$(q+1)\lambda^+$	$(q+1)\lambda^-$	$2q(-1)^l$	$q(-1)^a$	0
ξ_2	1	$(q+1)\lambda^-$	$(q+1)\lambda^+$	$2q(-1)^l$	$q(-1)^a$	0

Here, the numbers σ, ρ, $\lambda^{\pm}$ are defined as for the $q \equiv 1 \bmod 4$ case. By reasoning very similar to that of the previous section, one obtains the result

Theorem 2.12. *The number of nontrivial central S-rings over* $\mathrm{PSL}(2,q)$ *where* $q \equiv 3 \bmod 4$ *is equal to* $n_-(n_+ + n'_+)$ *with* n_-, n_+, n'_+ *defined as in Theorem 2.11.* $\square$

We provide the following table, listing the number of central S-rings over $\mathrm{PSL}(2,q)$ for small values of q:

q	# $\mathrm{PSL}(2,q)$
2	2
3	3
4	3
5	3
7	4
8	7
9	7
11	13
13	13
16	33
17	25
19	34

q	# $\mathrm{PSL}(2,q)$
23	41
25	81
27	45
29	89
31	161
32	37
37	76
41	307
43	100
47	163
49	568
53	169

q	# $\mathrm{PSL}(2,q)$
59	337
61	337
64	1684
67	190
71	1891
73	757
79	2026
81	811
83	571
89	1405
97	2381
101	869

TABLE. *S-rings over the groups* $\mathrm{PSL}(2,q)$.

These first of these values are all readily checked by computer.

Chapter 3. Counting Symmetric S-rings

Having established a connection between the central S-rings over the projective special linear groups and symmetric S-rings over cyclic groups, we make an attempt to count the latter. We more or less follow Misseldine in our approach; in [M2], he uses similar arguments to count all S-rings over cyclic groups of prime-power order. The idea is to exploit a connection between subalgebras of the group algebra and subfields of a cyclotomic field. This may seem strange in the present context since we are interested in S-rings over groups of order $p^n \pm 1$; however, the formulas we develop may suggest a heuristic in the case that we deal with a cyclic group of arbitrary order. In this chapter, we write $\mathcal{C}_n$ for the cyclic group of order n.

We begin with an obvious corollary to the classification of Leung and Man.

Corollary 3.1. *Let F be a field of characteristic zero, G a finite cyclic group, and S a symmetric Schur ring over $F[G]$. Then one of the following holds:*

(i) S is the trivial S-ring over G.

(ii) S is an orbit Schur ring where the relevant subgroup $H \leq \mathrm{Aut}(G)$ contains the inverse map $g \mapsto g^{-1}$.

(iii) S is a dot product of Schur rings that are symmetric.

(iv) S is a semi-wedge product of Schur rings that are symmetric.

Proof. There are four cases as in the earlier classification, Theorem 1.5. Certainly the trivial S-ring is symmetric.

Suppose S is a symmetric orbit S-ring given by $H \leq \mathrm{Aut}(G)$. Misseldine in [M1] demonstrates the duality between the lattice of orbit Schur rings and subgroups of $\mathrm{Aut}(G)$. As the principal sets of S are certainly unions of orbits of $g \mapsto g^{-1}$, under this correspondence the statement in (ii) of containment of subgroups follows.

Suppose that the symmetric S-ring $S = T \cdot U$ is a dot product of Schur rings T, U over subgroups H, K such that $G = H \times K$. The principal sets of S are all of the form CD where

C, D are principal sets of T, U respectively. If U is not symmetric, we have a principal set C of T such that $C^{-1} \neq C$. Taking $D = \{1_K\}$, a principal set of U, consider the product CD. We see that

$$(CD)^{-1} = C^{-1} \neq C = CD$$

and so S is not symmetric. Similarly, U must be symmetric.

Suppose that $S = T \wedge U$ is a semi-wedge product of Schur rings that is symmetric, where U, T are S-rings over H, G/K. Since T injects into S, if T is not symmetric, S cannot be. Thus, T is symmetric. Suppose U is not symmetric. Take a principal set C of U such that $C^{-1} \neq C$ and the inflation of C is a class of the wedge product. The inflated class has the form $\cup_{g \in C} gK$. The inverse class is $\cup_{g \in C} g^{-1}K$. As each coset has a unique representative $g \in G \setminus H$ and $C^{-1} \neq C$, these cannot be equal. Thus, U is symmetric. $\square$

We now define a canonical map with many applications in the literature:

Definition 3.2. Let $\mathcal{C}_n = \langle g \rangle$ be the cyclic group of order n with g a generator and let ζ_n be a primitive n-th root of unity. We define $\omega : \mathbb{Q}\mathcal{C}_n \to \mathbb{Q}(\zeta_n)$ by requiring $g \mapsto \zeta_n$ and extending linearly.

Thus ω yields an inclusion-preserving set map from the set of S-rings over $\langle g \rangle$ to the subfields of $\mathbb{Q}(\zeta)$ by taking images. We also make use of notation given in the introduction; for finite group G, the rings $\mathscr{R}(\mathbb{Q}G)$, $\mathscr{S}(\mathbb{Q}G)$, $\mathscr{T}(\mathbb{Q}G)$ denote respectively the rational, symmetric and trivial S-rings of G over $\mathbb{Q}G$.

3.1 Counting Orbit S-rings

The correspondence provided above by ω is especially easily to describe for orbit S-rings. We have the following proposition, which relies only on elementary Galois theory.

Proposition 3.3. *The map ω gives a lattice bijection between the orbit S-rings of a cyclic group and the subfield lattice of the corresponding cyclotomic field.*

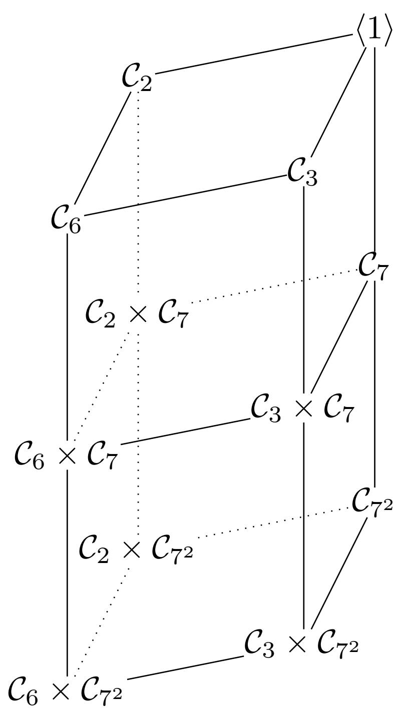
Proof. Subfields of a cyclotomic field are in one-to-one correspondence with fixed fields of the Galois group. These are generated over $\mathbb{Q}$ by orbits of ζ. Under ω, these are in bijection with the orbits giving the principal sets of orbit S-rings. Since ω is covariant, we obtain a lattice isomorphism. $\square$

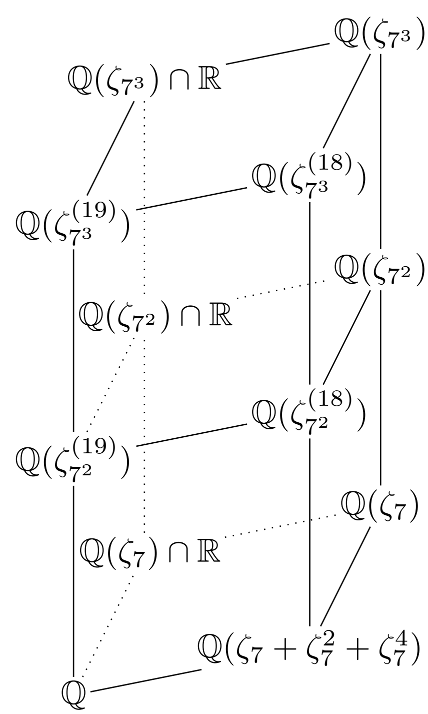
As an immediate corollary, we have

Corollary 3.4. *The map ω gives a bijective correspondence between symmetric orbit S-rings of a cyclic group and real subfields of a cyclotomic field.* $\square$

Now let p be an odd prime. Then as is well-known, the automorphism group of C_{p^n} is cyclic of order $\varphi(p^n) = p^n - p^{n-1} = p^n(p-1)$, where we write φ for the Euler totient. The cyclic group of this order is the Galois group of $\mathbb{Q}(\zeta)$ where ζ is a p^n-th root of unity. The subgroup lattice of $C_{\varphi(p^n)}$ and the dual lattice of subfields are easily described; the subgroup diagram is a lattice-theoretic product of the subgroups lattices of $C_{p^{n-1}}$ and C_{p-1}.

For example, when we take $p = 7$, $n = 3$, we have $\varphi(p^n) = 7^2 \cdot 6$. The subgroup lattice in this case consists of several copies of the subgroup lattice for the cyclic group C_6. The subfield diagram for $\mathbb{Q}(\zeta_{7^3})$ is displayed alongside this:





Here, $\zeta^{(k)}$ is the orbit of ζ under the automorphism $\zeta \mapsto \zeta^k$. In general, we say that the subfield diagram of $\mathbb{Q}(\zeta_{p^n})$ is "layered":

Definition 3.5. For $1 \leq k \leq n$ let $\mathcal{L}^k$ be the sublattice of $\mathbb{Q}(\zeta_{p^n})$ consisting of all subfields of $\mathbb{Q}(\zeta_{p^k})$. We call $\mathcal{L}^k \setminus \mathcal{L}^{k-1}$ the *k-th layer* of $\mathbb{Q}(\zeta_{p^n})$. We call $\mathcal{L}^n$ the *top layer* and $\mathcal{L}^0 = \mathbb{Q}$ the *bottom layer.* $\Diamond$

Abstracting slightly from our example, we can now show:

Proposition 3.6. *Let p be an odd prime. Let $x = d(p-1)$ be the number of divisors of $p-1$. Then there are nx orbit S-rings over C_{p^n}, of which ny are symmetric, where y is the number of even divisors of $p-1$.*

Proof. The first part of the statement is clear. Due to the bijection of Proposition 3.3, we seek the number of real subfields of $\mathbb{Q}(\zeta_{p^n})$. Taking advantage of the layered structure of the subfield lattice, it is enough to prove this when $n = 1$. In this case, $\mathbb{Q}(\zeta_p) \cap \mathbb{R}$ is the fixed field of the order 2 operation of complex conjugation. Since the Galois group $C_{\varphi(p)}$ is cyclic, there is a unique subgroup of order 2 and a given subgroup of $C_{\varphi(p)}$ will contain complex conjugation if and only if it has order divisible by two. Thus the number of symmetric S-rings over C_p is equal to the number of even divisors of $p-1$. Write $p-1 = 2^r k$, where k is odd. By an elementary counting argument, this number is $(r-1)d(k)$ where d is the divisor function. $\square$

Now let $p = 2$. It is known that unless $n = 1$, the multiplicative group $(C_{2^n})^\times$ is $C_2 \times C_{2^{n-2}}$. The subfield lattice of $\mathbb{Q}(\zeta_{2^n})$ can be deduced from the subgroup lattice of $(C_{2^n})^\times$. It is also layered in the same way as the odd prime case. However, we note that the first layer will be empty. The subfield lattice of $\mathbb{Q}(\zeta_{2^5})$ is given below with dots to indicate the diagram for higher powers:

$$\begin{tikzcd}[column sep=small]
 & & \vdots \\
\vdots & & \mathbb{Q}(\zeta_{2^5}) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{Q}(\zeta_{2^5}) \cap \mathbb{R} \arrow[d, dash] & \mathbb{Q}(\zeta_{2^5} - \zeta_{2^5}^{-1}) \arrow[dl, dash] & \mathbb{Q}(\zeta_{2^4}) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{Q}(\zeta_{2^4}) \cap \mathbb{R} \arrow[d, dash] & \mathbb{Q}(\zeta_{2^4} - \zeta_{2^4}^{-1}) \arrow[dl, dash] & \mathbb{Q}(\zeta_{2^3}) \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \\
\mathbb{Q}(\zeta_{2^3}) \cap \mathbb{R} \arrow[d, dash] & \mathbb{Q}(\zeta_{2^3} - \zeta_{2^3}^{-1}) \arrow[dl, dash] & \mathbb{Q}(i) \arrow[dll, dash] \\
\mathbb{Q} & &
\end{tikzcd}.$$

Reasoning as in Proposition 3.6, this leads immediately to

Proposition 3.7. *There are $n-1$ symmetric orbit S-rings over a cyclic group of order C_{2^n}.*

3.2 On the Correspondence ω

We know that any principal element of an S-ring that is a wedge product with decomposition $1 < K \leq H < G$ is either a sum of cosets of K or a principal set of an S-ring over H. Since ω maps cosets of K to zero, this shows:

Proposition 3.8. *Let $\mathfrak{S} = \mathfrak{S}_{G/K} \Delta \mathfrak{S}_H$ be a semi-wedge product of S-rings over a cyclic group. Then $\omega(\mathfrak{S}) = \omega(\mathfrak{S}_H)$.* $\square$

While ω sends symmetric S-rings to real cyclotomic subfields, the converse is not true. Specifically, let $\mathfrak{S}$ be an S-ring with wedge-decomposition $1 < K \leq H < G$, so that $\mathfrak{S} = \mathfrak{S}_{G/K} \Delta_K \mathfrak{S}_H$ where $\mathfrak{S}_{G/K}$ and $\mathfrak{S}_H$ are S-rings over G/K and H respectively. Any principal set of $\mathfrak{S}$ is either a principal set of $\mathfrak{S}_H$ or an inflated principal set of $\mathfrak{S}_{G/K}$. As these inflations are all sent to $\mathbb{Q}$, it follows that $\mathfrak{S}$ will map to a real subfield if and only if $\mathfrak{S}_H$ is symmetric. On the other hand, from Corollary 3.1 we know that $\mathfrak{S} = \mathfrak{S}_{G/K}\Delta_K\mathfrak{S}_H$ is symmetric if and only if the wedge components $\mathfrak{S}_{G/K}$ and $\mathfrak{S}_H$ both are. Thus $\mathfrak{S}$ is symmetric if and only if all of its wedge components (applied recursively to wedge components of wedge components and so forth) map to real subfields.

The classification of S-rings over cyclic p-groups is somewhat simpler than that for arbitrary cyclic groups. One has

Theorem 3.9. *Let $\mathfrak{S}$ be a nontrivial S-ring over a cyclic p-group. Then $\mathfrak{S}$ is an orbit S-ring or a semi-wedge product.* □

The proof of the classification for this special case is simpler than for cyclic groups generally. See [M1, LM1, LM2]. We now give a pair of useful lemmas.

Lemma 3.10. *Suppose $\mathfrak{S}$ is a wedge decomposable S-ring over an abelian group G. Then it has a wedge decomposition $1 < K \leq H < G$ such that $\mathfrak{S} = \mathfrak{S}_{G/K}\Delta\mathfrak{S}_H$ where $\mathfrak{S}_H$ is wedge indecomposable. Additionally, if G has a minimal normal subgroup N (as is the case for a cyclic group of prime-power order), we may independently choose $K = N$.*

Proof. Let $1 < K \leq H < G$ be a wedge decomposition and suppose $\mathfrak{S}_H$ is wedge decomposable with decomposition $1 < K' \leq H' < H$. It is straightforward to show that we can obtain a wedge decomposition $1 < K' \leq H' < G$ of $\mathfrak{S}$. Since G has finite order, this process of refining the decomposition can only be repeated finitely many times.

The second statement follows since any normal subgroup K of G can be written as a union of cosets of N. An inflation of an S-ring over G/K is naturally an inflation of an S-ring over G/N. □

From Theorem 3.9, if we let G of the theorem be a cyclic p-group, it follows that $\mathfrak{S}_H$ of the Lemma is trivial or an orbit S-ring.

Lemma 3.11. *The rational S-ring over $G = \mathcal{C}_{p^n}$ is wedge decomposable as $\mathscr{R}(\mathbb{Q}G) = \bigwedge_{k=1}^{n} \mathscr{T}(\mathbb{Q}\mathcal{C}_{p^k})$.*

Proof. In general, the orbits of the full automorphism group are sets $\{x : x \in G, |x| = d\}$ for each d a divisor of the group order. It follows that the rational S-ring is spanned by cosets of $\overline{\mathcal{C}_p}$ and the identity. Inducting at each step, one sees that the indicated wedge product is spanned by exactly these elements. ☐

We also mention a classical result, whose proof we omit. See [L1] for references and a discussion of related results.

Theorem 3.12. *Let G be a cyclic group of order $\prod_i p_i^{n_i}$. Then*

$$\operatorname{Ker} \omega = \sum_i \overline{P_i},$$

where P_i is the unique group of order p_i in G.

In particular, we see that the rational S-ring over $\mathcal{C}_{p^n}$ is equal to $\operatorname{Ker}\omega + \mathbb{Q}$, so it consists of all elements mapping to $\mathbb{Q}$. From the lemmas, we obtain two theorems.

Theorem 3.13. *Let G be a cyclic p-group and $\mathfrak{S}$ an S-ring over G. If $\omega(\mathfrak{S}) = \mathbb{Q}$, then for some nontrivial $H \leq G$, $\mathfrak{S}$ is a wedge product $\mathscr{T}(\mathbb{Q}H) \wedge \mathfrak{S}_{G/H}$ of the trivial S-ring over H with an S-ring over G/H.*

Proof. We may assume that $\mathfrak{S}$ is nontrivial. Since ω furnishes a bijection between orbit S-rings and fixed fields of a cyclotomic field, the only orbit S-ring mapping to $\mathbb{Q}$ is the rational S-ring, which is of the required form by Lemma 3.11. Assuming now that $\mathfrak{S}$ is not an orbit S-ring, we know that $\mathfrak{S} = \mathfrak{S}_{G/K} \Delta \mathfrak{S}_H$ is wedge decomposable and we can take H minimal as in Lemma 3.10 so that $\mathfrak{S}_H$ is wedge indecomposable. Necessarily $\omega(\mathfrak{S}_H) = \mathbb{Q}$. If we assume $\mathfrak{S}_H$ to be nontrivial, it is the rational S-ring over H. However, by Lemma 3.11 the rational S-ring over a cyclic p-group H is only wedge indecomposable when $H = \mathcal{C}_p$. In this case, the rational S-ring coincides with the trivial one. Now, in the wedge decomposition

$1 < K \leq H = \mathcal{C}_p < G$, K must be a nontrivial $\mathfrak{S}_H$-subgroup which forces so $K = H = \mathcal{C}_p$ and this is a wedge product as required. $\square$

Theorem 3.14. *Let $\mathfrak{S}$ be a nontrivial S-ring over $\mathcal{C}_{p^n}$. If $\mathfrak{S}$ does not map to the top layer under ω, then it is wedge decomposable.*

Proof. Choose $H = \mathcal{C}_{p^k} \leq \mathcal{C}_{p^n}$ minimal so that $\omega(\mathfrak{S}) \subseteq \omega(\mathbb{Q}H) = \mathbb{Q}(\zeta_{p^k})$. By Theorem 3.13 any S-ring mapping to $\mathbb{Q}$ is wedge decomposable, so we can assume $H \neq \{1\}$. Necessarily $\mathfrak{S}$ contains an S-ring over H, which we name $\mathfrak{S}_H$ in typical style. Consider a principal set not contained in H. The map ω sends this principal set to $\mathbb{Q}$ by the minimality of H. Thus, by Theorem 3.12, this principal set is a sum of cosets of nontrivial subgroups of $\mathcal{C}_{p^n}$. Moreover, we can pick K nontrivial so that each such principal set is a sum of cosets of K. Then $1 < K \leq H < \mathcal{C}_{p^n}$ is a wedge decomposition of $\mathfrak{S}$ and $\mathfrak{S}$ is a wedge product by Proposition 1.13. $\square$

Since any wedge decomposable S-ring cannot map to the top layer by Proposition 3.8, it follows immediately that

Corollary 3.15. *Under ω, there is a unique S-ring of $\mathcal{C}_{p^n}$ mapping to each field in the top layer $\mathcal{L}^n \setminus \mathcal{L}^{n-1}$.*

By the theorem to which this is a corollary, this S-ring must be an orbit S-ring.

3.3 A Recursive Formula

We begin with a definition:

Definition 3.16. Let $\Omega(n)$ be the number of S-rings over $\mathcal{C}_{p^n}$ and let $\Omega(n,k)$ be the number of S-rings over $\mathcal{C}_{p^n}$ mapping onto $\mathbb{Q}(\zeta_{p^k})$ under ω.

Also let $\widetilde{\Omega}(n)$ be the number of S-rings over $\mathcal{C}_{p^n}$ mapping onto the real cyclotomic field $\mathbb{Q}(\zeta_{p^n}) \cap \mathbb{R}$ under ω, with $\widetilde{\Omega}(n,k)$ the number mapping onto $\mathbb{Q}(\zeta_{p^k}) \cap \mathbb{R}$.

Finally, let $\Lambda(n)$ be the number of S-rings over $\mathcal{C}_{p^n}$ that map onto the real cyclotomic field $\mathbb{Q}(\zeta_{p^n}) \cap \mathbb{R}$ under ω and are symmetric. Define $\Lambda(n,k)$ analogously. $\lozenge$

The counting is done differently according as p is even or odd. We first consider the case $p = 2$. In this case, it is somewhat simpler to count $\Lambda(n)$ than to count $\Omega(n)$. However, when p is odd, the results necessary to count $\Omega(n)$ apply to $\Lambda(n)$ with only minor modification. Thus, while the proofs in the first part of this section are inspired by [M2], the second half of the section will consist merely in quoting a few results from the same paper. The following proposition holds in either case with a corresponding Λ-version; that is, a similar theorem holds when Ω is replaced with Λ.

Proposition 3.17. *The following equality holds:*

$$\Omega(n, 0) = \sum_{k=0}^{n-1} \Omega(k).$$

Proof. Let $\mathfrak{S}$ be an S-ring over $\mathcal{C}_{p^n}$ such that $\omega(\mathfrak{S}) = \mathbb{Q}$. By Proposition 3.13, we know that $\mathfrak{S}$ has a wedge decomposition $1 < K \leq H < \mathcal{C}_{p^n}$ such that $\mathfrak{S} = \mathscr{T}(\mathbb{Q}H)\Delta\mathfrak{S}_{G/K}$. For the compatibility condition of the semi-wedge product to hold, we see that necessarily $H = K$. Further, any S-ring of this form maps to $\mathbb{Q}$. Thus the S-rings mapping to $\mathbb{Q}$ are in bijection with inflations of S-rings over G/K. □

Requiring that the S-rings over G/K be symmetric in this proof, it is not hard to see that

$$\Lambda(n, 0) = \sum_{k=0}^{n-1} \Lambda(k).$$

We now let $p = 2$. The lattice of cyclotomic fields for $\mathbb{Q}(\zeta_{p^n})$ has no first layer when $p = 2$. Also, the second layer is the imaginary quadratic field $\mathbb{Q}(i)$, so that $\Lambda(n, 2) = 0$. Thus we count $\Lambda(n)$ as

$$\Lambda(n) = \Lambda(n, 0) + \sum_{k=3}^{n} \Lambda(n, k).$$

The numbers $\Lambda(n, k)$ can be computed recursively:

Proposition 3.18. *For $k > 3$,*

$$\Lambda(n,k) = \sum_{j=k-1}^{n-1} \Lambda(n-1,j).$$

When $n > 3$,

$$\Lambda(n,3) = \Lambda(n-2) - \Lambda(n-3,0) + \sum_{j=3}^{n-1} \Lambda(n-1,j).$$

Proof. When $k = n$, then $\Lambda(n,n) = \Lambda(n-1,n-1) = 1$ since there is a single S-ring mapping to each subfield of the top layer (Proposition 3.15). Let $\mathfrak{S}$ be a symmetric S-ring over $\mathcal{C}_{p^n}$ mapping to the k-th layer where $3 < k < n$. By Proposition 3.10, $\mathfrak{S}$ is wedge decomposable as $\mathfrak{S} = \mathfrak{S}_H \Delta \mathfrak{S}_{G/K}$ where we may assume $\mathfrak{S}_H$ is indecomposable with $H = \mathcal{C}_{p^k}$ and $K = \mathcal{C}_p$. If $\mathfrak{S}_H$ were trivial we would have $\omega(\mathfrak{S}_H) = \mathbb{Q}$, so it is instead the orbit S-ring $\mathscr{S}(\mathbb{Q}H)$ given by the inverse map.

It remains to determine which S-rings over G/K can be written as a wedge product in this way. First, K should be a $\mathfrak{S}_H$-subgroup, but this is true for any subgroup of H as a subgroup is closed under taking inverses. Second, we require that H/K be a $\mathfrak{S}_{G/K}$-subgroup and $\pi(\mathfrak{S}_H) = \mathfrak{S}_{G/K} \cap \mathbb{Q}H/K$ where $\pi : G \to G/K$ is the quotient map. Now, $\omega(\pi(\mathfrak{S}_H)) = \omega(\mathscr{S}(\mathbb{Q}H/K))$ is the associated real quadratic field $\mathbb{Q}(\zeta_{|H|/p}) \cap \mathbb{R}$, so we require

$$\begin{aligned}\mathbb{Q}(\zeta_{p^{k-1}} + \zeta_{p^{k-1}}^{-1}) \cap \mathbb{R} &= \omega(\mathfrak{S}_{G/K}) \cap \omega(\mathbb{Q}H/K) \\ &= \omega(\mathfrak{S}_{G/K}) \cap \mathbb{Q}(\zeta_{p^{k-1}})\end{aligned}$$

Thus $\mathfrak{S}_{G/K}$ maps under ω to the j-th real quadratic field for some $k-1 \leq j \leq n-1$. Any such S-ring over G/K mapping to this can be wedged with $\mathfrak{S}_H$, so the counting is complete when $k > 3$.

When $k = 3 < n$, we are interested in the number of symmetric S-rings $\mathfrak{S}$ over $\mathcal{C}_{2^{n-1}}$ such that $\mathfrak{S} \cap \mathbb{Q}\mathcal{C}_4 = \mathscr{S}(\mathbb{Q}\mathcal{C}_4)$. This includes S-rings sent by ω to the j-th real quadratic field for some $3 \leq j \leq n-1$. It remains to count those sent to $\mathbb{Q}$ by ω. If $\omega(\mathfrak{S}) = \mathbb{Q}$, then as usual it is a wedge product $\mathbb{Q}\mathcal{C}_2 \wedge \mathfrak{T}$ where $\mathfrak{T}$ is an S-ring over $\mathcal{C}_{2^{n-2}}$. For the compatibility condition $\mathfrak{S} \cap \mathbb{Q}\mathcal{C}_4 = \mathscr{S}(\mathbb{Q}\mathcal{C}_4)$ of the wedge dictates that $\mathfrak{T} \cap \mathbb{Q}\mathcal{C}_2 = \mathbb{Q}\mathcal{C}_2$. Any symmetric S-ring $\mathfrak{T}$ over $\mathcal{C}_{2^{n-2}}$ (of which there are $\Lambda(n-2)$) has this property except those that are wedge products with $\mathbb{Q}\mathcal{C}_{2^j}$, $1 < j \leq n-2$. There are $\Lambda(n-3, 0)$ of these. $\square$

Since $\Lambda(3,3) = 1$ is known by Proposition 3.15, we now have a recursive method for computing $\Lambda(n)$.

Equation (6.11) of [M2] can be modified using our work here to give the formula

$$\widetilde{\Omega}(n) = \sum_{k=1}^{3} 2^k \widetilde{\Omega}(n-k) - (c_{n-1} + s_{n-1}) + \sum_{k=4}^{n} \left(c_{k-1} + s_{k-1} - \sum_{j=1}^{k-3} (c_j + s_j) \right) \widetilde{\Omega}(n-k),$$

where c_k and s_k are the well-known Catalan and Schröder numbers. Thus, one could also obtain an unwieldy formula for $\widetilde{\Omega}(n) \geq \Lambda(n)$ using only the numbers $\widetilde{\Omega}(k)$, $k < n$.

The following table gives some of the numbers $\Omega(n)$, $\Lambda(n)$. The S-rings in question can be produced using code in [M2] or in section A.6 of the appendix to this thesis.

n	$\Omega(n)$	$\Lambda(n)$
1	1	1
2	3	2
3	10	5
4	37	12
5	151	31
6	657	85
7	2989	246
8	14044	747
9	67626	2361
10	332061	7708

TABLE. *S-rings over cyclic groups of even-power order.*

Now let p be an odd prime. In [M2] Misseldine proves

Proposition 3.19. *The number of S-rings of $\mathcal{C}_{p^n}$ mapping to a given cyclotomic subfield is constant within each layer.*

This justifies our narrow definition of $\Omega(n,k)$; from our combinatorial point of view, the whole layer is described by the subfield $\mathbb{Q}(\zeta_{p^k})$. We also require the following, the proof of which is very similar that of to the non-symmetric result Misseldine gives.

Proposition 3.20. *The number of symmetric S-rings of $\mathcal{C}_{p^n}$ mapping to a given real cyclotomic subfield is constant in each layer.*

We write $x = d(p-1)$ and y for the number of even divisors of $p-1$. In Section 1 of this chapter, we found that there are x subfields in the k-th layer, $k > 1$, y of which are real. The first layer has $x-1$ subfields, $y-1$ of which are real. The 0-th layer, of course, is just $\mathbb{Q}$. This accounting along with the previous proposition gives

Theorem 3.21. *The following recurrences hold:*

$$\Omega(n) = \Omega(n,0) + (x-1)\Omega(n,1) + x\sum_{k=2}^{n}\Omega(n,k),$$

and

$$\Lambda(n) = \Lambda(n,0) + (y-1)\Lambda(n,1) + y\sum_{k=2}^{n}\Lambda(n,k).$$

In the same paper, Misseldine derives recursive relations for the numbers $\Omega(n,k)$ in terms of numbers $\Omega(m,j)$ where $m < n$:

Proposition 3.22. *The following equalities hold when p is odd:*

$$\Omega(n,0) = \sum_{k=0}^{n-1}\Omega(k),$$

$$\Omega(n,1) = \Omega(n-1),$$

$$\Omega(n,k) = \sum_{j=k-1}^{n-1}\Omega(n-1,j),\ \textit{when } 1 < k \leq n \textit{ and } n \geq 2,$$

$$\Omega(n,n) = 1.$$

The proofs that results for $\Omega(n,k)$ descend to results for $\Lambda(n,k)$ are very similar to what we have done previously; most of the necessary arguments have already been demonstrated in this section. These relations allow one to compute $\Omega(n,k)$ as a polynomial of degree $n-1$ in x. Recursively, one obtains polynomials of degree n for $\Omega(n)$, the fullest description of which uses the Catalan numbers. The polynomials for $\Lambda(n)$ are the polynomials for $\Omega(n)$ with y replacing x. The first few such polynomials for $\Omega(n)$ are

$$\begin{aligned}
&\Omega(1) = x\\
&\Omega(2) = x^2 + x + 1\\
&\Omega(3) = x^3 + 2x^2 + 4x + 1\\
&\Omega(4) = x^4 + 3x^3 + 8x^2 + 9x + 2\\
&\Omega(5) = x^5 + 4x^4 + 13x^3 + 23x^2 + 25x + 3\\
&\Omega(6) = x^6 + 5x^5 + 19x^4 + 44x^3 + 72x^2 + 69x + 5\\
&\Omega(7) = x^7 + 6x^6 + 26x^5 + 73x^4 + 152x^3 + 222x^2 + 203x + 8.
\end{aligned}$$

Thus, for example when $p = 3$, $x = 2$ and $y = 1$ so $\Omega(4) = x^4 + 3x^3 + 8x^2 + 9x + 2 = 92$, $\Lambda(4) = y^4 + 3y^3 + 8y^2 + 9y + 2 = 23$, so there are 92 S-rings over C_{81}, 23 of which are symmetric. This is consonant with the table in the Appendix A.6.

A number of nice patterns hold for the coefficients of these polynomials. As might seem apparent from these first examples, $\Omega(n)$ is monic; also, the coefficient of x^{n-1} is in fact $n-1$. The constant terms are given by the Fibonacci numbers. Interested readers are urged to consult [M2] for more combinatorics.

Appendix A. Computer Code

The usefulness of having a large number of examples led me to write up code which gives S-rings for groups of small order (up to order 24 without great difficulty) and character tables for those S-rings that are commutative. All code here is written to be executed in MAGMA and has been run successfully in version V2.21-3. The appendix gives a summary of the S-rings of groups up to order 24 and more detailed information for the S-rings over S_4, finishing with code optimized to generate the S-rings over cyclic groups.

It should be noted that our work of enumeration is surpassed by that of Matan Ziv-Av [Z] whose implementation in COCO and COCO-II has been used to enumerate S-rings for all groups of order up to 63.

A.1 Summary for Groups of Order ≤ 24

The following table gives a summary of all S-rings over groups of order ≤ 24. The columns are labelled as

(i) The SmallGroup MAGMA identifier (first ordinate is the group order);

(ii) Total number of S-rings over this group;

(iii) Total up to conjugacy;

(iv) Number of commutative S-rings (up to conjugacy);

(v) A multiset, giving dimensions of S-rings with multiplicity (up to conjugacy).

(i)	(ii)	(iii)	(iv)	(v)
(3 , 1)	2	2	2	{* 2, 3 *}
(4 , 1)	3	3	3	{* 2, 3, 4 *}
(4 , 2)	5	5	5	{* 2, 3^3, 4 *}
(5 , 1)	3	3	3	{* 2, 3, 5 *}
(6 , 1)	10	6	5	{* 2, 3^2, 4^2, 6 *}
(6 , 2)	7	7	7	{* 2, 3^2, 4^3, 6 *}
(7 , 1)	4	4	4	{* 2, 3, 4, 7 *}
(8 , 1)	10	10	10	{* 2, 3^2, 4, 5^4, 6, 8 *}
(8 , 2)	28	28	28	{* 2, 3^6, 4^9, 5^6, 6^5, 8 *}
(8 , 3)	34	25	24	{* 2, 3^6, 4^9, 5^5, 6^3, 8 *}
(8 , 4)	26	20	19	{* 2, 3^4, 4^4, 5^7, 6^3, 8 *}
(8 , 5)	100	100	100	{* 2, 3^14, 4^49, 5^14, 6^21, 8 *}
(9 , 1)	7	7	7	{* 2, 3, 4^2, 5^2, 9 *}
(9 , 2)	40	40	40	{* 2, 3^7, 4^14, 5^5, 6^12, 9 *}
(10 , 1)	25	9	8	{* 2, 3^2, 4^3, 6^2, 10 *}
(10 , 2)	10	10	10	{* 2, 3^2, 4^3, 6^3, 10 *}
(11 , 1)	4	4	4	{* 2, 3, 6, 11 *}
(12 , 1)	54	29	25	{* 2, 3^4, 4^5, 5^7, 6^4, 7^3, 8^3, 9, 12 *}
(12 , 2)	32	32	32	{* 2, 3^4, 4^6, 5^7, 6^6, 7^3, 8^3, 9, 12 *}
(12 , 3)	52	18	15	{* 2, 3^3, 4^5, 5^4, 6^2, 7, 8, 12 *}
(12 , 4)	120	60	52	{* 2, 3^8, 4^17, 5^12, 6^10, 7^5, 8^5, 9, 12 *}
(12 , 5)	76	76	76	{* 2, 3^8, 4^18, 5^17, 6^12, 7^9, 8^7, 9^3, 12 *}
(13 , 1)	6	6	6	{* 2, 3, 4, 5, 7, 13 *}
(14 , 1)	55	12	10	{* 2, 3^2, 4^3, 5^2, 6, 8^2, 14 *}
(14 , 2)	13	13	13	{* 2, 3^2, 4^3, 5^2, 6, 8^3, 14 *}
(15 , 1)	21	21	21	{* 2, 3^2, 4^5, 5^3, 6^4, 7^2, 8, 9, 10, 15 *}

(i)	(ii)	(iii)	(iv)	(v)
(16 , 1)	37	37	37	{* 2, 3^3, 4^3, 5^3, 6^7, 7^11, 8, 9^4, 10^2, 12, 16 *}
(16 , 2)	537	537	537	{* 2, 3^45, 4^83, 5^93, 6^127, 7^61, 8^57, 9^24, 10^36, 12^9, 16 *}
(16 , 3)	649	379	360	{* 2, 3^31, 4^55, 5^73, 6^79, 7^47, 8^35, 9^26, 10^22, 12^9, 16 *}
(16 , 4)	401	281	268	{* 2, 3^19, 4^29, 5^48, 6^58, 7^41, 8^31, 9^24, 10^20, 12^9, 16 *}
(16 , 5)	163	163	163	{* 2, 3^9, 4^19, 5^21, 6^31, 7^25, 8^29, 9^6, 10^16, 12^5, 16 *}
(16 , 6)	205	149	142	{* 2, 3^12, 4^18, 5^21, 6^33, 7^21, 8^20, 9^5, 10^14, 12^3, 16 *}
(16 , 7)	247	124	110	{* 2, 3^9, 4^19, 5^19, 6^24, 7^18, 8^15, 9^5, 10^10, 12^3, 16 *}
(16 , 8)	287	127	112	{* 2, 3^12, 4^18, 5^18, 6^27, 7^18, 8^15, 9^4, 10^10, 12^3, 16 *}
(16 , 9)	271	128	112	{* 2, 3^7, 4^13, 5^21, 6^34, 7^18, 8^15, 9^5, 10^10, 12^3, 16 *}
(16 , 10)	1121	1121	1121	{* 2, 3^57, 4^115, 5^205, 6^279, 7^141, 8^161, 9^68, 10^68, 12^25, 16 *}
(16 , 11)	1557	959	922	{* 2, 3^65, 4^135, 5^203, 6^251, 7^97, 8^113, 9^36, 10^44, 12^13, 16 *}
(16 , 12)	797	587	550	{* 2, 3^17, 4^51, 5^93, 6^141, 7^85, 8^109, 9^28, 10^48, 12^13, 16 *}
(16 , 13)	607	463	439	{* 2, 3^18, 4^59, 5^91, 6^98, 7^61, 8^79, 9^14, 10^34, 12^7, 16 *}
(16 , 14)	12537	12537	12537	{* 2, 3^513, 4^1891, 5^2205, 6^4151, 7^1085, 8^1505, 9^660, 10^420, 12^105, 16 *}
(17 , 1)	5	5	5	{* 2, 3, 5, 9, 17 *}
(18 , 1)	122	32	24	{* 2, 3^4, 4^5, 5^5, 6^5, 7^4, 8^3, 10^3, 12, 18 *}
(18 , 2)	42	42	42	{* 2, 3^4, 4^6, 5^8, 6^8, 7^4, 8^4, 10^4, 12^2, 18 *}
(18 , 3)	233	112	95	{* 2, 3^7, 4^19, 5^21, 6^20, 7^15, 8^15, 9^5, 10^4, 12^4, 18 *}
(18 , 4)	995	227	166	{* 2, 3^10, 4^35, 5^36, 6^44, 7^32, 8^34, 9^12, 10^6, 12^16, 18 *}
(18 , 5)	297	297	297	{* 2, 3^10, 4^39, 5^44, 6^65, 7^40, 8^46, 9^24, 10^7, 12^20, 18 *}
(19 , 1)	6	6	6	{* 2, 3, 4, 7, 10, 19 *}
(20 , 1)	139	45	41	{* 2, 3^4, 4^6, 5^7, 6^9, 7^5, 8^4, 9, 11^3, 12^3, 15, 20 *}
(20 , 2)	47	47	47	{* 2, 3^4, 4^6, 5^7, 6^8, 7^6, 8^5, 9, 10, 11^3, 12^3, 15, 20 *}
(20 , 3)	154	38	30	{* 2, 3^4, 4^6, 5^8, 6^5, 7^5, 8^4, 9, 11, 12^2, 20 *}
(20 , 4)	313	93	85	{* 2, 3^8, 4^18, 5^17, 6^13, 7^13, 8^8, 9^3, 11^5, 12^5, 15, 20 *}
(20 , 5)	109	109	109	{* 2, 3^8, 4^18, 5^17, 6^14, 7^18, 8^9, 9^3, 10, 11^9, 12^7, 15^3, 20 *}
(21 , 1)	143	23	20	{* 2, 3^3, 4^6, 5^4, 6^4, 8, 9^2, 12, 21 *}
(21 , 2)	27	27	27	{* 2, 3^2, 4^5, 5^5, 6^4, 8^3, 9^3, 11, 12, 14, 21 *}

(i)	(ii)	(iii)	(iv)	(v)
(22 , 1)	83	12	10	`{* 2, 3^2, 4^3, 6, 7^2, 12^2, 22 *}`
(22 , 2)	13	13	13	`{* 2, 3^2, 4^3, 6, 7^2, 12^3, 22 *}`
(23 , 1)	4	4	4	`{* 2, 3, 12, 23 *}`
(24 , 1)	365	175	148	`{* 2, 3^6, 4^11, 5^16, 6^21, 7^30, 8^16, 9^27, 10^17, 11^8, 12^6, 13^4, 14^3, 15^4, 16^3, 18, 24 *}`
(24 , 2)	172	172	172	`{* 2, 3^6, 4^12, 5^16, 6^20, 7^28, 8^17, 9^26, 10^16, 11^8, 12^6, 13^4, 14^3, 15^4, 16^3, 18, 24 *}`
(24 , 3)	387	96	76	`{* 2, 3^5, 4^9, 5^15, 6^18, 7^15, 8^10, 9^10, 10^4, 12^2, 13^2, 14^2, 15, 16, 24 *}`
(24 , 4)	1081	389	320	`{* 2, 3^10, 4^25, 5^42, 6^67, 7^54, 8^52, 9^42, 10^42, 11^12, 12^16, 13^5, 14^9, 15^3, 16^5, 18^3, 24 *}`
(24 , 5)	1113	510	437	`{* 2, 3^14, 4^43, 5^68, 6^85, 7^63, 8^79, 9^47, 10^52, 11^8, 12^24, 13^4, 14^11, 15^2, 16^5, 18^3, 24 *}`
(24 , 6)	1341	460	375	`{* 2, 3^14, 4^43, 5^64, 6^78, 7^50, 8^62, 9^46, 10^44, 11^12, 12^20, 13^5, 14^9, 15^3, 16^5, 18^3, 24 *}`
(24 , 7)	1291	604	522	`{* 2, 3^14, 4^43, 5^68, 6^92, 7^69, 8^94, 9^63, 10^69, 11^19, 12^31, 13^9, 14^15, 15^4, 16^7, 18^5, 24 *}`
(24 , 8)	1293	466	387	`{* 2, 3^14, 4^43, 5^66, 6^81, 7^53, 8^65, 9^43, 10^44, 11^11, 12^21, 13^4, 14^9, 15^2, 16^5, 18^3, 24 *}`
(24 , 9)	660	660	660	`{* 2, 3^14, 4^44, 5^76, 6^100, 7^76, 8^101, 9^72, 10^78, 11^20, 12^38, 13^6, 14^15, 15^6, 16^7, 18^5, 24 *}`
(24 , 10)	826	586	550	`{* 2, 3^14, 4^44, 5^76, 6^96, 7^70, 8^89, 9^59, 10^57, 11^18, 12^32, 13^7, 14^9, 15^5, 16^5, 18^3, 24 *}`
(24 , 11)	606	453	425	`{* 2, 3^10, 4^24, 5^46, 6^66, 7^65, 8^60, 9^61, 10^49, 11^18, 12^21, 13^7, 14^9, 15^7, 16^5, 18^3, 24 *}`
(24 , 12)	710	155	119	`{* 2, 3^9, 4^21, 5^29, 6^31, 7^18, 8^16, 9^9, 10^10, 11^2, 12^4, 13, 14, 15, 16, 24 *}`
(24 , 13)	767	236	202	`{* 2, 3^10, 4^25, 5^42, 6^50, 7^29, 8^33, 9^11, 10^18, 11^2, 12^6, 13^2, 14^2, 15^2, 16^2, 24 *}`
(24 , 14)	4819	2094	1840	`{* 2, 3^30, 4^163, 5^288, 6^464, 7^219, 8^380, 9^175, 10^195, 11^27, 12^75, 13^13, 14^39, 15^4, 16^11, 18^9, 24 *}`
(24 , 15)	2876	2876	2876	`{* 2,3^30,4^164,5^308,6^540,7^252,8^525,9^296,10^366,11^84,12^182,13^14,14^63,15^14,16^15,18^21,24 *}`

TABLE. *Summary of S-rings over groups of order less than or equal to 24.*

A.2 Code for Enumeration of S-rings

The following is lightly documented through 'double-slashed' comments. Naively, one might consider all possible partitions of the group and then check each to see if it is an S-ring. This is not likely to be very efficient and eventually becomes impossible. The major optimizations of this code over the naïve approach of considering all partitions of the group is to first find S-rings over a well chosen subgroup.

```
//This function takes a subalgebra of a group algebra
//and outputs true/false acccording as it is an S-ring.
issring:=function(su,ga);g:=Group(ga);
b:=Basis(su);
tf:=Set( Coefficients(&+b)) eq {1} and
{Set(ElementToSequence(x)):x in b} eq {{0,1}};
sb:=[];
for i:=1 to #b do
e:=ElementToSequence(b[i]);ee:={g!ga.k:k in {1..#g}|e[k] eq 1};
sb:=sb cat [ee];
end for;
for i:=1 to #sb do tf:=tf and {x^-1:x in sb[i]} in sb;
end for;
return tf;
end function;


//This function splits elements of a basis.
//Iteratively, it produces the S-ring generated by 'su.'
sring:=function(su,ga);g:=Group(ga);
b:=Basis(su);s:=Set(b);
for i:=1 to #b do
```

```
    x:=b[i];
    ex:=ElementToSequence(x);
    cex:=Set(Coefficients(x)) diff {0};
        for c in cex  do
            h:={i:i in [1..#ex]|ex[i] eq c};
            hh:=&+{ga!ga.i:i in h};
            s:=s join {hh};
hh:=&+{ga!(g!ga.i)^-1:i in h};
s:=s join {hh};
end for;end for;
return sub<ga|s>;
end function;

//This is a simple function which determines all S-rings of a group g.
//It is best suited for a group with few subgroups.
//The previous two functions are relied upon.
simprings:=function(g);
eg:={x:x in g|Order(x) ne 1};
s:={x:x in Subsets(eg)|{y^-1:y in x} eq x or #({y^-1:y in x} meet x) eq 0}
   diff{{}};
rat:=RationalField();
ga:=GroupAlgebra(rat,g:Rep:="Vector");
eg:={ga!y:y in eg};ssr:={};
ssr:={{ga!Id(g),&+eg}};
ssro:={{{h*y*h^-1:y in x}:h in g}:x in ssr};
while #ssr ne 0 do
    ssrs:={};
```

```
    for x in ssr do
        for y in s do
        z:={ga!f:f in y};
        su:=sub<ga|x,&+z>;
        while not issring(su,ga) do
        su:=sring(su,ga);
        end while;
        su:=Basis(su);
        ssrs join:={su};
        end for;
    end for;
    ssr:={{{h*y*h^-1:y in x}:h in g}:x in ssr};
    ssrs:={{{h*y*h^-1:y in x}:h in g}:x in ssrs};
    ssro join:=ssr;
    ssr:=ssrs diff ssro;
    ssr:={Random(x):x in ssr};
    #ssro,#ssr;
end while;
ssro:=[[SetToSequence(y):y in x]:x in ssro];
return ssro;
end function;

//This is a utility that finds the support of an element
//in the group algebra.
fn2:=function(z,ga);
g:=Group(ga);
x:=ElementToSequence(z);
```

```
n:=#x;
x:={i:i in {1..#x}|x[i] ne 0};
x:={g!ga![0^(i-1),1,0^(n-i)]:i in x};
return x;
end function;

//This is the main function; it calls on simprings when
//convenient, but makes significant improvements to
//the algorithm when possible.

givesrings:=function(g);

sg:=Subgroups(g);
sgo:=[x`order:x in sg];
pos:=SetToSequence({Position(sgo,x):x in sgo|x eq Round(#g/2) }) cat
    SetToSequence({Position(sgo,x):x in sgo|x in
    {Round(#g/3)..Round(2*#g/3)} });
if #pos eq 0 or #g le 15 then return simprings(g); end if;
ind:=pos[1];
sg:=[x`subgroup:x in sg];

a4:={g!x:x in sg[ind]};
eg:={x:x in a4|Order(x) ne 1};
s:={x:x in Subsets(eg)|{y^-1:y in x} eq x or #({y^-1:y in x} meet x) eq 0}
    diff{{}};
rat:=RationalField();
ga:=GroupAlgebra(rat,g:Rep:="Vector");
```

```
eg:={ga!y:y in eg};ssr:={};count:=1;
eg1:={ga!x:x in g|x notin a4}diff{Id(g)};


ssr:={{ga!Id(g),&+eg,&+eg1}};
ssro:={{{h*y*h^-1:y in x}:h in g}:x in ssr};


while #ssr ne 0 do
ssrs:={};
for x in ssr do
for y in s do
z:={ga!f:f in y};
su:=sub<ga|x,&+z>;
while not issring(su,ga) do
su:=sring(su,ga);
end while;
su:=Basis(su);
ssrs join:={su};
end for;
end for;
ssr:={{{h*y*h^-1:y in x}:h in g}:x in ssr};
ssrs:={{{h*y*h^-1:y in x}:h in g}:x in ssrs};
ssro join:=ssr;
ssr:=ssrs diff ssro;
ssr:={Random(x):x in ssr};
#ssro,#ssr;
end while;
sa4:=ssro;
```

```
// S-rings S where given subgroup is an S-set.


a4:={g!x:x in sg[ind]};

a4:={x:x in g|x notin a4};

s:={x:x in Subsets(a4)|{y^-1:y in x} eq x or #({y^-1:y in x} meet x) eq 0}

    diff{{}};

eg:={ga!y:y in a4};

ssr:={Random(x):x in sa4};

ssro:={{{h*y*h^-1:y in x}:h in g}:x in ssr};


count:=0;

while #ssr ne 0 do

ssrs:={};

for x in ssr do

count+:=1;if count mod 10 eq 0 then print "ten";end if;

for y in s do

z:={ga!f:f in y};

su:=sub<ga|x,&+z>;

while not issring(su,ga) do

su:=sring(su,ga);

end while;

su:=Basis(su);

ssrs join:={su};

end for;end for;

ssr:={{{h*y*h^-1:y in x}:h in g}:x in ssr};

ssrs:={{{h*y*h^-1:y in x}:h in g}:x in ssrs};
```

```
ssro join:=ssr;
ssr:=ssrs diff ssro;
ssr:={Random(x):x in ssr};
#ssro,#ssr;
end while;

sa4c:=ssro;

// not containing s-rings over subgroup

fn2:=function(z,ga);
g:=Group(ga);
x:=ElementToSequence(z);
n:=#x;
x:={i:i in {1..#x}|x[i] ne 0};
x:={g!ga![0^(i-1),1,0^(n-i)]:i in x};
return x;
end function;

eg:={g!x:x in sg[ind]|Order(x) ne 1};
a4t:=&+{ga!x:x in eg};
s:=[];t:=[];
s[1]:={x:x in Subsets(eg)|{y^-1:y in x} eq x}diff{{}};
s[2]:={x:x in Subsets(eg)|#({y^-1:y in x} meet x) eq 0}diff{{}};
eg:={x:x in g|x notin sg[ind]};
t[1]:={x:x in Subsets(eg)|{y^-1:y in x} eq x}diff{{}};
t[2]:={x:x in Subsets(eg)|#({y^-1:y in x} meet x) eq 0}diff{{}};
```

```
u:={x join y:x in s[1],y in t[1]} join {x join y:x in s[2],y in t[2]};
u:={{{h*y*h^-1:y in x}:h in g}:x in u};
u:={Random(x):x in u};

eg:={x:x in g|Order(g) ne 1};
s:=&join{u,t[1],t[2],s[1],s[2]};

rat:=RationalField();
ga:=GroupAlgebra(rat,g:Rep:="Vector");
st:=&+{ga!x:x in g};

ssr:={};
ssrs:={};
for y in u do
z:={ga!f:f in y};
su:=sub<ga|ga!Id(g),st,&+z>;
while not issring(su,ga) do
su:=sring(su,ga);
end while;
su:=Basis(su);
ssrs join:={su};
end for;
ssr:={{{h*y*h^-1:y in x}:h in g}:x in ssr};
ssr join:={{{h*y*h^-1:y in x}:h in g}:x in ssrs};
ssr:={Random(x):x in ssr};
ssr:={x:x in ssr|a4t notin sub<ga|x>};
```

```
count:=0;
while #ssr ne 0 do
ssrs:={};
for z in ssr do
count +:=1;if count mod 10 eq 0 then print "ten";end if;
for y in {x:x in s|&or{x subset j: j in {fn2(er,ga):er in z}}} do
st:={ga!Id(g),&+{ga!m:m in y}}join z;
su:=sub<ga|st>;
while not issring(su,ga) do
su:=sring(su,ga);
end while;
su:=Basis(su);
ssrs join:={su};
end for;end for;
ssr:={{{h*y*h^-1:y in x}:h in g}:x in ssr};
ssrs:={{{h*y*h^-1:y in x}:h in g}:x in ssrs};
ssro join:=ssr;
ssr:=ssrs diff ssro;
ssr:={Random(x):x in ssr|a4t notin sub<ga|Random(x)>};
#ssro,#ssr;
end while;


s4:=ssro;
s4:=[[SetToSequence(y):y in x]:x in s4];
return s4;


end function;
```

On a dual core 2.66 GHz Intel Xeon without any parallel processing, the function `givesrings()` finds all S-rings over D_8, the dihedral group of order 8, in 0.550 seconds. Performing the same task for C_{20} required about eight minutes. For cyclic groups, one could conceivably find these more quickly by using the classification theorem.

A.3 Code to Compute Character Tables of Commutative S-rings

In the following, the first function `pm` produces the P-matrix of a given association scheme `oo`, with input a basis for a commutative subalgebra of $\mathbb{Q}G$ and a field over which the decomposition occurs (this can generally be chosen to be cyclotomic).

```
set:=function(x);
xx:=ElementToSequence(x);
return {i:i in {1..#g}|xx[i] ne 0};
end function;


pm:=function(oo,F);
ga:=Parent(oo[1]);
g:=Group(ga);
P:=PolynomialRing(F,#oo);
eo:=[Random(set(oo[i])):i in [1..#oo]];
A:=[];
mr:=MatrixRing(P,#oo);
for ii:=1 to #oo do
    m:=mr!0;
    for i:=1 to #oo do
        pp:={* ga.x*ga.y:x in set(oo[i]),y in set(oo[ii]) *};
        for j:=1 to #oo do
        m[i,j]:=Multiplicity(pp,ga.eo[j]);
```

```
        end for;
    end for;
    A[ii]:=m;
end for;
mr2:=MatrixRing(F,#oo);
sr:=sub<mr2|[mr2!x:x in A]>;
rm:=RModule(sr);
c1,c2:=ConstituentsWithMultiplicities(rm);
s1,s2,s3:=CompositionSeries(rm);
if #s2 ne #oo then return [],#s2;end if;
return ElementToSequence(Transpose(mr2!&cat[Diagonal(s3*x*s3^-1):x in A])),
    #s2;
end function;
```

A.4 Running the Code

As an example, after loading all of the above functions, the following

```
ss:=givesrings(SmallGroup(8,3));
a:=ss[4,1];//a rep. of the 4th conjugacy class of S-rings
r,s:=pm(a,CyclotomicField(8));
//entries in the character table are in this field.
```

gives the group-normalized character table

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 \\ \sqrt{2} & \sqrt{2} & -\sqrt{2} & 0 \\ 2 & -2 & 0 & 0 \end{bmatrix}.$$

A.5 S-rings Over S_4

The following is a complete list of the S-rings over S_4 with some structural properties. The columns describe

(i) #: a number after ordering by the dimension multiset (iii);

(ii) dim: the dimension of the S-ring;

(iii) prin. sets: a multiset giving the number k_i associated to each principal set;

(iv) C: left blank if the S-ring is commutative, reading 'F' otherwise;

(v) #: the number of S-rings conjugate to this one;

(vi) SG: For the S-ring $\mathfrak{S}$, this describes which subgroups of S_4 are $\mathfrak{S}$-subgroups.

#	dim.	prin. sets	C	#	SG
1	2	`{* 1, 23 *}`			
2	3	`{* 1^2, 22 *}`			
3	3	`{* 1^2, 22 *}`		6	
4	3	`{* 1, 2, 21 *}`		3	
5	3	`{* 1, 3, 20 *}`		3	
6	3	`{* 1, 3, 20 *}`		3	K_4
7	3	`{* 1, 3, 20 *}`		3	K_4
8	3	`{* 1, 5, 18 *}`		3	S_3
9	3	`{* 1, 7, 16 *}`		12	D_8
10	3	`{* 1, 11, 12 *}`		6	A_4
11	4	`{* 1^3, 21 *}`		3	
12	4	`{* 1^2, 2, 20 *}`		3	K_4
13	4	`{* 1^2, 2, 20 *}`		6	K_4
14	4	`{* 1^2, 2, 20 *}`		4	
15	4	`{* 1^2, 2, 20 *}`		6	K_4
16	4	`{* 1^2, 4, 18 *}`		1	S_3
17	4	`{* 1^2, 6, 16 *}`		1	D_8
18	4	`{* 1^2, 6, 16 *}`		4	D_8
19	4	`{* 1^2, 6, 16 *}`		6	D_8

#	dim.	prin. sets	C	#	SG
20	4	{* 1^2, 10, 12 *}		3	A_4
21	4	{* 1^2, 11^2 *}		3	A_4
22	4	{* 1, 2, 3, 18 *}		6	S_3
23	4	{* 1, 2, 7, 14 *}		3	D_8
24	4	{* 1, 2, 7, 14 *}		4	
25	4	{* 1, 2, 9, 12 *}		3	A_4
26	4	{* 1, 3, 4, 16 *}		6	D_8
27	4	{* 1, 3, 4, 16 *}		4	D_8
28	4	{* 1, 3, 4, 16 *}		1	D_8
29	4	{* 1, 3, 5, 15 *}		6	S_3
30	4	{* 1, 3, 5, 15 *}		12	K_4 S_3
31	4	{* 1, 3, 8, 12 *}		1	
32	5	{* 1^4, 20 *}		6	K_4
33	5	{* 1^4, 20 *}		6	K_4
34	5	{* 1^4, 20 *}		3	
35	5	{* 1^3, 3, 18 *}		4	S_3
36	5	{* 1^3, 9, 12 *}		4	A_4
37	5	{* 1^2, 2^2, 18 *}		6	S_3
38	5	{* 1^2, 2, 4, 16 *}		6	D_8
39	5	{* 1^2, 2, 4, 16 *}		6	D_8
40	5	{* 1^2, 2, 4, 16 *}		6	D_8
41	5	{* 1^2, 2, 4, 16 *}		3	D_8
42	5	{* 1^2, 2, 4, 16 *}		6	D_8
43	5	{* 1^2, 2, 8, 12 *}		3	K_4 A_4
44	5	{* 1^2, 2, 10^2 *}		3	
45	5	{* 1^2, 2, 10^2 *}		3	A_4
46	5	{* 1^2, 2, 10^2 *}		6	
47	5	{* 1^2, 2, 10^2 *}		4	K_4 A_4
48	5	{* 1^2, 3^2, 16 *}		3	D_8
49	5	{* 1^2, 3^2, 16 *}		3	D_8
50	5	{* 1^2, 3^2, 16 *}		3	D_8
51	5	{* 1^2, 3^2, 16 *}		3	D_8
52	5	{* 1^2, 4, 6, 12 *}		3	S_3 D_8
53	5	{* 1^2, 5^2, 12 *}		3	A_4
54	5	{* 1^2, 6, 8^2 *}		6	D_8

#	dim.	prin. sets	C	#	SG
55	5	`{* 1, 2, 3, 6, 12 *}`		1	K_4 A_4
56	5	`{* 1, 2, 3, 9^2 *}`		3	S_3 A_4
57	5	`{* 1, 3, 4^2, 12 *}`		4	K_4 A_4
58	5	`{* 1, 3, 4, 8^2 *}`		3	D_8 A_4
59	5	`{* 1, 3, 6^2, 8 *}`		1	K_4 A_4
60	5	`{* 1, 3, 6^2, 8 *}`		6	K_4 A_4
61	6	`{* 1^4, 4, 16 *}`		6	D_8
62	6	`{* 1^4, 4, 16 *}`		3	D_8
63	6	`{* 1^4, 4, 16 *}`		6	D_8
64	6	`{* 1^4, 8, 12 *}`		6	K_4 A_4
65	6	`{* 1^4, 10^2 *}`		3	K_4 A_4
66	6	`{* 1^4, 10^2 *}`		1	A_4
67	6	`{* 1^3, 3, 9^2 *}`		1	S_3 A_4
68	6	`{* 1^3, 7^3 *}`	F	6	
69	6	`{* 1^2, 2^3, 16 *}`		3	D_8
70	6	`{* 1^2, 2^3, 16 *}`		4	D_8
71	6	`{* 1^2, 2^2, 6, 12 *}`		4	S_3 D_8
72	6	`{* 1^2, 2^2, 9^2 *}`		3	S_3 A_4
73	6	`{* 1^2, 2, 4^2, 12 *}`		3	K_4 A_4
74	6	`{* 1^2, 2, 4^2, 12 *}`		6	K_4 A_4
75	6	`{* 1^2, 2, 4^2, 12 *}`		3	K_4 A_4
76	6	`{* 1^2, 2, 4, 8^2 *}`		3	D_8
77	6	`{* 1^2, 2, 4, 8^2 *}`		3	D_8
78	6	`{* 1^2, 2, 4, 8^2 *}`		3	D_8
79	6	`{* 1^2, 2, 4, 8^2 *}`		3	D_8 A_4
80	6	`{* 1^2, 2, 4, 8^2 *}`		4	D_8
81	6	`{* 1^2, 2, 4, 8^2 *}`		8	D_8 A_4
82	6	`{* 1^2, 2, 5^2, 10 *}`		6	A_4
83	6	`{* 1^2, 2, 5^2, 10 *}`		3	A_4
84	6	`{* 1^2, 2, 5^2, 10 *}`		6	K_4 A_4
85	6	`{* 1^2, 3^2, 4, 12 *}`		1	S_3 D_8
86	6	`{* 1^2, 3^2, 4, 12 *}`		1	S_3 D_8
87	6	`{* 1^2, 3^2, 8^2 *}`		12	D_8 A_4
88	6	`{* 1, 2, 3^2, 6, 9 *}`		12	K_4 S_3 A_4
89	6	`{* 1, 2, 3, 4, 6, 8 *}`		4	D_8 A_4

#	dim.	prin. sets	C	#	SG
90	6	{* 1, 3, 4^2, 6^2 *}		3	K_4 A_4
91	6	{* 1, 3, 4^2, 6^2 *}		3	K_4 A_4
92	7	{* 1^6, 18 *}	F	6	S_3
93	7	{* 1^4, 2^2, 16 *}		1	D_8
94	7	{* 1^4, 2^2, 16 *}		1	D_8
95	7	{* 1^4, 2^2, 16 *}		3	D_8
96	7	{* 1^4, 4^2, 12 *}		3	K_4 A_4
97	7	{* 1^4, 4, 8^2 *}		3	D_8 A_4
98	7	{* 1^4, 4, 8^2 *}		6	D_8
99	7	{* 1^3, 3^3, 12 *}		1	K_4 A_4
100	7	{* 1^2, 2^3, 8^2 *}		3	D_8
101	7	{* 1^2, 2^3, 8^2 *}		3	D_8 A_4
102	7	{* 1^2, 2, 4^3, 8 *}		6	D_8 A_4
103	7	{* 1^2, 2, 4^3, 8 *}		3	D_8 A_4
104	7	{* 1^2, 2, 4^3, 8 *}		3	D_8 A_4
105	7	{* 1^2, 2, 4^3, 8 *}		3	D_8 A_4
106	7	{* 1^2, 2, 4^3, 8 *}		12	D_8 A_4
107	7	{* 1^2, 2, 4^3, 8 *}		6	D_8 A_4
108	7	{* 1, 2, 3^3, 6^2 *}		1	K_4 S_3 A_4
109	7	{* 1, 3, 4^5 *}	F	3	D_8 A_4
110	8	{* 1^6, 9^2 *}	F	1	S_3 A_4
111	8	{* 1^4, 2^2, 8^2 *}		4	D_8
112	8	{* 1^4, 2^2, 8^2 *}		3	D_8 A_4
113	8	{* 1^4, 2^2, 8^2 *}		3	D_8 A_4
114	8	{* 1^4, 2^2, 8^2 *}		3	D_8 A_4
115	8	{* 1^4, 5^4 *}	F	3	A_4
116	8	{* 1^3, 3^4, 9 *}		12	K_4 S_3 A_4
117	8	{* 1^2, 2^5, 12 *}	F	12	K_4 A_4
118	8	{* 1^2, 2^3, 4^2, 8 *}		3	D_8 A_4
119	8	{* 1^2, 2^3, 4^2, 8 *}		3	D_8 A_4
120	8	{* 1^2, 2^3, 4^2, 8 *}		6	D_8 A_4
121	8	{* 1^2, 2^3, 4^2, 8 *}		3	D_8 A_4
122	8	{* 1^2, 2^2, 3^2, 6^2 *}		3	S_3 D_8 A_4
123	8	{* 1^2, 2, 4^5 *}	F	12	S_3 D_8
124	8	{* 1^2, 2, 4^5 *}	F	3	D_8 A_4

#	dim.	prin. sets	C	#	SG
125	8	`{* 1^2, 3^2, 4^4 *}`	F	3	D_8 A_4
126	9	`{* 1^8, 16 *}`	F	4	D_8
127	9	`{* 1^4, 2^4, 12 *}`	F	3	K_4 A_4
128	9	`{* 1^4, 4^5 *}`	F	12	D_8 A_4
129	9	`{* 1^4, 4^5 *}`	F	6	S_3 D_8
130	9	`{* 1^3, 3^3, 4^3 *}`	F	6	D_8 A_4
131	9	`{* 1^2, 2^5, 4, 8 *}`	F	6	D_8 A_4
132	9	`{* 1^2, 2^5, 4, 8 *}`	F	6	D_8 A_4
133	9	`{* 1^2, 2^3, 4^4 *}`	F	12	S_3 D_8
134	9	`{* 1^2, 2^3, 4^4 *}`	F	12	D_8 A_4
135	10	`{* 1^8, 8^2 *}`	F	3	D_8 A_4
136	10	`{* 1^4, 2^2, 4^4 *}`	F	3	D_8 A_4
137	10	`{* 1^4, 2^2, 4^4 *}`	F	3	D_8 A_4
138	10	`{* 1^4, 2^2, 4^4 *}`		4	D_8 A_4
139	10	`{* 1^4, 2^2, 4^4 *}`	F	4	D_8 A_4
140	10	`{* 1^4, 2^2, 4^4 *}`	F	3	S_3 D_8
141	10	`{* 1^4, 2^2, 4^4 *}`		24	D_8 A_4
142	10	`{* 1^4, 2^2, 4^4 *}`	F	3	D_8 A_4
143	10	`{* 1^4, 2^2, 4^4 *}`	F	4	D_8 A_4
144	10	`{* 1^3, 3^7 *}`		1	K_4 S_3 A_4
145	11	`{* 1^4, 2^4, 4^3 *}`	F	3	D_8 A_4
146	11	`{* 1^4, 2^4, 4^3 *}`	F	4	D_8 A_4
147	12	`{* 1^8, 4^4 *}`	F	6	D_8 A_4
148	12	`{* 1^6, 3^6 *}`	F	3	S_3 D_8 A_4
149	12	`{* 1^4, 2^6, 4^2 *}`	F	6	D_8 A_4
150	12	`{* 1^4, 2^6, 4^2 *}`	F	3	D_8 A_4
151	13	`{* 1^12, 12 *}`	F	12	K_4 A_4
152	14	`{* 1^4, 2^10 *}`	F	12	S_3 D_8 A_4
153	15	`{* 1^12, 4^3 *}`	F	3	D_8 A_4
154	16	`{* 1^8, 2^8 *}`	F	4	D_8 A_4
155	24	`{* 1^24 *}`	F	6	S_3 D_8 A_4

TABLE. *Structural properties of S-rings over S_4.*

A.6 S-rings Over Cyclic Groups

Code as in the previous section can be made considerably simpler if the group in question is cyclic. Using the classification theorem for S-rings over cyclic groups and the ease with which integer arithmetic is done on computer, we have the following:

```
triv:=function(n);
return {{0},{1..n-1}}diff{{}};
end function;


auts:=function(n);
g1:=Sym(n);
g2:=sub<g1|{g1![(j*i-1) mod n+1:j in [1..n]]:i in [1..n]|GCD(n,i) eq 1}>;
ss:=[x`subgroup:x in Subgroups(g2)];
orbs:=[Orbits(x):x in ss];
return {{{z mod n: z in x}:x in y}:y in orbs};
end function;


dot:=function(A,B);
a:=(#&join A);b:=(#&join B);n:=a*b;
ap:=Round(n/a);bp:=Round(n/b);
return {{(ap*a+bp*b) mod n:a in x, b in y}:x in A, y in B};
end function;


//A is an S-ring over a subgroup;
//B is an S-ring over a quotient.
swdg:=function(A,B,n);
a:=(#&join A);b:=(#&join B);
ap:=Round(n/a);bp:=Round(n/b);
```

```
ab:=Round(a/bp);
sg:={ab*i:i in {0..bp-1}};
tf1:=sg eq &join{x:x in A|x meet sg ne {}};
sg:={ap*i:i in {0..Round(a/bp)-1}};
tf2:=sg eq &join{x:x in B|x meet sg ne {}};
piA:={{ap*i:i in {0..ab-1}|&or{y mod ab eq i:y in x}}:x in A};
tf3:=piA eq {x:x in B|x meet {ap*i:i in {0..ab-1}} ne {}};
if not (tf1 and tf2 and tf3) then return triv(n);end if;
sg:={b*i:i in {0..bp-1}};
A:={{y*ap:y in x}:x in A};
B:={&join{{y+i:i in sg}:y in x}:x in B};
return A join {x:x in B|x meet &join A eq {}};
end function;

//given a list of S-rings over cyclic groups of smaller order,
//compute recursively the S-rings over C_n.
srcyc:=function(n,prev);
if n le 2 then return {triv(n)};end if;
divs:=[[a,b]:a,b in [2..n-1]|GCD(a,b) eq 1 and a*b eq n and a lt b];
dts:=&join{{dot(x,y):x in prev[z[1]],y in prev[z[2]]}:z in divs};
divs:=[[a,b]:a,b in {2..n-1}|n mod a eq 0 and a mod b eq 0];
wdg:=&join{{swdg(x,y,n):x in prev[z[1]],y in prev[Round(n/z[2])]}
:z in divs};
return {triv(n)} join auts(n) join dts join wdg;
end function;

//returns a list of all S-rings over cyclic groups
```

```
//of order leq n.
cycls:=function(n);
prev:=[];
for i:=1 to n do
i;
prev cat:=[srcyc(i,prev)];
end for;
return prev;
end function;


//does the minimum necessary to produce the S-rings
//over C_n.
cyc:=function(n);
prev:=[];
for i:=1 to n do
if n mod i eq 0 then i;prev cat:=[srcyc(i,prev)];
else prev cat:=[{triv(i)}];
end if;
end for;
return prev[n];
end function;
```

Using the function `cycls`, we obtain the following table counting S-rings over cyclic groups of order up to 100. The third column gives the number of S-rings that are also symmetric. The necessary computation took 54 minutes for the first 100 groups. Of that time, 81% was was spent in doing the computation for C_{96}. We label the columns as

(i) n the group order

(ii) $\Omega(n)$, which we use here for the number of S-rings over $\mathcal{C}_n$, not as in Chapter 3.

(iii) $\Lambda(n)$, here the number of symmetric S-rings over $\mathcal{C}_n$.

n	$\Omega(n)$	$\Lambda(n)$	n	$\Omega(n)$	$\Lambda(n)$	n	$\Omega(n)$	$\Lambda(n)$	n	$\Omega(n)$	$\Lambda(n)$
1	1	1	49	21	7	97	12	10	145	67	33
2	1	1	50	79	42	98	128	42	146	37	28
3	2	1	51	35	14	99	177	47	147	289	68
4	3	2	52	91	41	100	563	195	148	135	60
5	3	2	53	6	4	101	9	6	149	6	4
6	7	4	54	232	68	102	243	102	150	2124	622
7	4	2	55	41	15	103	8	4	151	12	6
8	10	5	56	334	90	104	514	156	152	496	131
9	7	3	57	40	13	105	670	164	153	238	67
10	10	7	58	19	13	106	19	13	154	360	120
11	4	2	59	4	2	107	4	2	155	81	29
12	32	13	60	1103	307	108	2219	470	156	2157	585
13	6	4	61	12	8	109	12	8	157	12	8
14	13	7	62	25	13	110	281	106	158	25	13
15	21	8	63	187	51	111	61	22	159	41	15
16	37	12	64	657	85	112	2030	366	160	11256	1322
17	5	4	65	67	33	113	10	8	161	53	17
18	42	17	66	188	65	114	277	94	162	1224	274
19	6	3	67	8	4	115	41	15	163	10	5
20	47	22	68	77	40	116	91	41	164	121	59
21	27	9	69	27	9	117	291	81	165	670	164
22	13	7	70	281	106	118	13	7	166	13	7
23	4	2	71	8	4	119	69	27	167	4	2
24	172	49	72	2311	471	120	10130	1915	168	12494	2381
25	13	7	73	12	9	121	21	7	169	43	21
26	19	13	74	28	19	122	37	25	170	411	216
27	25	8	75	185	54	123	55	21	171	283	77
28	61	23	76	90	33	124	119	43	172	119	43
29	6	4	77	53	17	125	58	25	173	6	4
30	147	58	78	284	109	126	2099	566	174	284	109
31	8	4	79	8	4	127	12	6	175	363	103
32	151	31	80	1646	315	128	2989	246	176	2030	366
33	27	9	81	92	23	129	53	17	177	27	9
34	16	13	82	25	19	130	457	230	178	25	19
35	41	15	83	4	2	131	8	4	179	4	2
36	284	81	84	1397	361	132	1397	361	180	17888	3513
37	9	6	85	60	31	133	99	33	181	18	12
38	19	10	86	25	13	134	25	13	182	658	244
39	41	15	87	41	15	135	854	177	183	81	29
40	262	82	88	334	90	136	442	148	184	334	90
41	8	6	89	8	6	137	8	6	185	100	49
42	188	65	90	1581	427	138	188	65	186	366	123
43	8	4	91	97	35	139	8	4	187	69	27
44	61	23	92	61	23	140	2142	570	188	61	23
45	140	39	93	53	17	141	27	9	189	1225	280
46	13	7	94	13	7	142	25	13	190	415	154
47	4	2	95	61	22	143	81	29	191	8	4
48	1033	194	96	6719	833	144	21451	3103			

TABLE. *S-rings and symmetric S-rings over cyclic groups of small order.*

Bibliography

[BA] Bailey, R. A. *Association Schemes: Designed Experiments, Algebra and Combinatorics*. Cambridge Unviersity Press, Cambridge UK, 2004.

[B1] Bannai, Eiichi. *Subschemes of Some Association Schemes*. Journal of Algebra 14, 167–188 (1991).

[BI1] Bannai, Eiichi; Ito, Tatsuro. *Algebraic Combinatorics I: Association Schemes*. The Benjamin/Cummings Publishing Company, Inc., Menlo Park, California, 1984.

[BCP] Wieb Bosma, John Cannon, and Catherine Playoust. *The Magma Algebra System. I. The User Language*. J. Symbolic Comput., 24(3-4), 235–265 (1997); Computational algebra and number theory (London, 1993).

[C1] Connell, I. G. *On the Group Ring*, Canad. J. Math. 15, 650–685 (1963).

[D1] Delsarte, P. An algebraic Approach to the Association Schemes of Coding Theory, Philips Research Reports Supplements, No. 10.

[F1] G. Frobenius, *Über die Primfactoren der Gruppendeterminante, Sitzungsber*. Preuss Akad. Wiss Berlin (1896), 1343–1382; Ges Abh. III, 38–77.

[F2] G. Frobenius, *Über einen Fundamentalsatz der Gruppentheorie II*, S'Ber Akad. Wiss. Berlin (1907) 428–437; Ges Abh. III, 394-403.

[G1] Godsil, C. G. *Algebraic Combinatorics*. Chapman Hall, New York, 1993.

[H1] Hendrickson, Anders O. F. *Supercharacter Theory Constructions Corresponding to Schur Ring Products*. Communications in Algebra 40:12, 4420–4438 (2012).

[HJ] Humphries, Stephen P.; Johnson, Kenneth W. *Fusions of Character Tables and Schur Rings of Abelian Groups*. Communications in Algebra, 36:4, 1437–1460 (2008).

[J1] Smith, Jonathan D. H. *An Introduction to Quasigroups and Their Representations.* Chapman & Hall/CRC. Boca Raton, Florida, 2007.

[JK] Johnson, Kenneth W. *Modern Work on Group Matrices, Group Determinants and Related objects: Mathematics Arising from Frobenius' First Papers on Group Representation Theory.* Mathematics Department, The Pennsylvania State University, Abington, PA. Unpublished.

[JL] James, Gordon; Liebeck, Martin. *Representations and Characters of Groups.* Second edition. Cambridge University Press, New York, 2001.

[JS1] Johnson, K. W.; Smith, J. D. H. *Characters of Finite Quasigroups III: Quotients and Fusion.* Europ. J. Combinatorics 10, 47–56 (1989).

[JS2] Johnson, K. W.; Smith, J. D. H. *Characters of Finite Quasigroups.* Europ. J. Combinatorics 5, 43–50 (1984).

[K1] Kerby, Brent. *Rational Schur Rings over Abelian Groups.* Master's Thesis, Brigham Young University, 2008.

[L1] Lam, T. Y., Leung, K. H. *On Vanishing Sums of Roots of Unity.* Journal of Algebra 224, 91–109 (2000).

[LM1] Leung, Ka Hin; Man, Shin Hing. *On Schur Rings Over Cyclic Groups I.* Israeli Journal of Mathematics, 106, 251–267 (1998).

[LM2] Leung, Ka Hin; Man, Shin Hing. *On Schur Rings Over Cyclic Groups II.* Journal of Algebra, 183,273–285 (1996).

[M1] Misseldine, Andrew. *Algebraic and Combinatorial Properties of Schur Rings over Cyclic Groups.* Doctoral Thesis, Brigham Young University, 2014.

[M2] Misseldine, Andrew. *Counting Schur Rings Over Cyclic Groups.* arXiv:1508.03757v1 [math.RA] 15 Aug 2015.

[MU1] Mikhail E. Muzychuk. *On the Structure of Basic Sets of Schur Rings Over Cyclic Groups*. Journal of Algebra, 169:655–678, 1994.

[W1] Helmut, Wielandt. *Zur Theorie der Einfach Transitiven Permutationsgruppen II* (German). Math. Z., 52, 38–393 (1949).

[Z] Ziv-Av, Matan. *Enumeration of Schur Rings Over Small Groups*. Computer Algebra in Scientific Computing. Springer International Publishing, 2014.

Index