2014-05-01

Algebraic and Combinatorial Properties of Schur Rings over Cyclic Groups

Andrew F. Misseldine
Brigham Young University - Provo

Algebraic and Combinatorial Properties of Schur Rings over Cyclic Groups

Andrew Frank Misseldine

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

Doctor of Philosophy

Stephen Humphries, Chair
Darrin Doud
Tyler Jarvis
William Lang
Pace Nielsen

Department of Mathematics

Brigham Young University

May 2014

ABSTRACT

Algebraic and Combinatorial Properties of Schur Rings over Cyclic Groups

Andrew Frank Misseldine
Department of Mathematics, BYU
Doctor of Philosophy

In this dissertation, we explore the nature of Schur rings over finite cyclic groups, both algebraically and combinatorially. We provide a survey of many fundamental properties and constructions of Schur rings over arbitrary finite groups. After specializing to the case of cyclic groups, we provide an extensive treatment of the idempotents of Schur rings and a description for the complete set of primitive idempotents. We also use Galois theory to provide a classification theorem of Schur rings over cyclic groups similar to a theorem of Leung and Man and use this classification to provide a formula for the number of Schur rings over cyclic p-groups.

Keywords: Schur ring, cyclic group, group ring, primitive idempotent, cyclotomic field, Wedderburn decomposition, representation theory, Galois theory, combinatorics

ACKNOWLEDGMENTS

I first thank my advisor, Dr. Stephen P. Humphries, for the large amount of time, support, wisdom, and patience he gave to me throughout the development of this dissertation. This dissertation would not be what it is without him. I also thank the other members of the committee for their assistance. I thank Brent Kerby, a former student of my advisor, whose MAGMA code, available in [11], was an invaluable tool in the preparation of this dissertation. I thank Dr. Michael Barrus for his suggestions and instructions to me on many topics of combinatorics. I could not have finished Chapter 5 without his guidance. Finally, I also thank my dear wife for all the love and support she has given me and allowing me to go to school for ∞-many years.

Contents

List of Tables

List of Figures

Chapter 1. Introduction

In Finite Group Representation Theory, the group algebra provides a valuable tool, as well as many of its subalgebras. The group algebra is a special example of a class of algebras called Schur rings, as well as many other subalgebras such as the center of the group algebra or double coset subalgebras. In many ways, Schur rings generalize the idea of group algebras and capture many of the critical subalgebras. Loosely speaking, a Schur ring is a subalgebra of the group algebra which is spanned by a partition of the finite group and satisfies other properties (see Definition 2.10). Schur rings were originally developed by Schur and Wielandt in the first half of the 20th century and were used to study permutation groups. In particular, certain properties of a Schur ring can determine properties of a related permutation group, such as 2-transitivity or primitivity. In later decades applications of Schur rings have emerged in combinatorics, graph theory, and design theory [12, 19], such as the study of association schemes. Both Wieldant's and Scott's monographs [35, Chapter 4], [29, Chapter 13] provide an introduction to the subject of Schur rings. Muzychuk and Ponomarenko also offer a recent survey of Schur rings in [22].

Schur rings over cyclic groups have been extremely useful in the study of circulant graphs. For this reason, Schur rings over cyclic groups have been well studied and a surge of papers emerged in the 1980's and 1990's, many of which are included in the bibliography, seeking a complete structure theorem of Schur rings over cyclic groups. This was eventually obtained by Leung and Man around the mid-1990's (Theorem 2.66). The purpose of this dissertation is to provide even more understanding about Schur rings over cyclic groups. When possible, we will try to make the arguments general, but ultimately the focus will be on Schur rings over cyclic groups. There are two main questions about these Schur rings which this dissertation will answer, one algebraic and one combinatorial. First, what are the primitive idempotents of Schur rings over cyclic groups? Second, how many Schur rings over cyclic groups are there?

In Chapter 2, we begin with the basics of Schur rings and their generalizations. This chapter surveys many of the elementary properties of Schur rings with proofs and references

to the original papers in the literature. Here many detailed constructions of Schur rings with examples are included, including new constructions introduced by the author. Chapter 2 provides the fundamental prerequisites for the rest of the dissertation.

In Chapter 3, we introduce a method to construct a complete system of orthogonal central idempotents in Schur rings. This method generalizes methods used by others to build primitive central idempotents in rational group algebras which avoids the use of characters. When the group is cyclic, we will prove that these central idempotents are necessarily primitive (Theorem 3.32). This provides an answer to the algebraic question. Prior to the completion of this dissertation, the contents of this chapter were published in [20].

In Chapter 4, we construct a representation of Schur rings over cyclic groups inside a cyclotomic field. This allows us to use Galois theory to study these Schur rings. One consequence of this work is that we have provided another (simpler) proof of the Leung-Man Classification Theorem of Schur rings over cyclic groups, at least when the order of the group is a power of a prime (Theorem 4.36). A second consequence of this representation is that we provide a Wedderburn decomposition for Schur rings over cyclic groups with rational coefficients (Theorem 4.17). A final consequence is given in Chapter 5, where we give formulas to count the number of Schur rings over specific cyclic groups (Theorem 5.11 and Theorem 5.19). This provides an answer to the combinatorial question.

A few appendices are included for the convenience of the reader. Appendix A provides a basic introduction, including proofs, to semisimple rings and their idempotents. Appendix B includes a quick treatment of subalgebras fixed under groups of automorphisms. These type of subalgebras arise often in Galois theory and with Schur rings, so we have included a few general results. Appendix C contains a description of the lattice of subfields of cyclotomic fields. The shape of these lattices will be useful in Chapter 4 and especially in Chapter 5. Finally, Appendix D includes the author's MAGMA code used for the calculations made in Chapter 5.

All computations made in preparation of this dissertation were accomplished using the computer softwares Maple and Magma [1].

Before closing this introduction, we will declare some common notation used throughout the paper. Unless otherwise specified, G will denote a finite group and F a field with

characteristic zero. Let $Z_n = \langle z_n \rangle$ denote the cyclic group of order n. Since each subgroup of Z_n is necessarily cyclic and is uniquely determined by its order, for each $d \mid n$, we will denote the unique subgroup of Z_n of order d as Z_d.

Throughout, let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ and let $\mathcal{K}_n = \mathbb{Q}(\zeta_n)$. Let $\mathcal{L}_n$ denote the lattice of subfields of $\mathcal{K}_n$. Let $\mathcal{G}_n$ denote the Galois group $\mathcal{G}(\mathcal{K}_n/\mathbb{Q})$. When the context is clear, subscripts may be omitted.

All algebras are associative with unity. Subalgebras will have the same unity as the over algebra. If A is an F-algebra, let $Z(A)$ denote the center of A.

Other commonly used notation and vocabulary will be introduced with boldface font. A list of notation can be found in the index.

Chapter 2. Schur Rings

In this chapter we begin our study of Schur rings, which are subalgebras of a group algebra afforded by certain partitions of the group. The fact that they are subalgebras of group algebras implies that Schur rings inherit many properties from the group algebra and in many ways behave like group algebras. In fact, every group algebra has a Schur ring structure, and hence the theory of Schur rings may be seen as a generalization of the theory of group algebras or of groups themselves.

The purpose of this chapter will be to introduce and familiarize the reader with the fundamental definitions, properties, and examples of Schur rings and to prepare the reader for the more difficult theory which fills the remainder of this dissertation. Section 2.1 begins with group rings themselves and provides definitions and properties of group rings which are pertinent for Schur rings. Section 2.2 will introduce the definition of Schur rings and will present many examples of Schur rings over finite groups. It will also present general constructions of Schur rings, including orbit and dot product Schur rings. This section also contains a collection of elementary properties of Schur rings which are fundamental for calculations in such rings. Most of these elementary properties were known and proven by Wielandt [35]. Section 2.3 focuses on Cayley maps, these being maps on group algebras which are induced from group homomorphisms. It also provides criteria for when the Cayley image of a Schur ring is also a Schur ring. Section 2.4 will generalize the notion of Schur rings in two ways: immersed Schur rings and pre-Schur rings. Both types of rings naturally arise while studying Schur rings and deserve proper attention. Also many properties of Schur rings naturally extend to immersed Schur rings and pre-Schur rings. Certain examples are also included here, including inflated Schur rings. From here we develop the construction of wedge products and their generalizations. Wedge products provide a method of extending Schur rings of normal subgroups by Schur rings of quotient groups. A result by Leung and Man (Theorem 2.66) states that every nontrivial Schur ring over a finite cyclic group is constructible using the methods mentioned in this chapter.

Unless otherwise specified, G will denote a finite group and F a field with characteristic

zero. Let $Z_n = \langle z_n \rangle$ denote the cyclic group of order n.

2.1 Group Rings

Let $F[G]$ denote the group algebra of G with coefficients from F. For $\alpha \in F[G]$, we will often denote the coefficient of the group element g in α by α_g, that is, $\alpha = \sum_{g \in G} \alpha_g g$ with $\alpha_g \in F$.

Definition 2.1. For any $\alpha \in F[G]$ with $\alpha = \sum_{g \in G} \alpha_g g$, we define

$$\boldsymbol{\alpha^*} = \sum_{g \in G} \alpha_g g^{-1}.$$

Similarly, if $C \subseteq G$, then

$$\boldsymbol{C^*} = \{g^{-1} \mid g \in C\}.$$

Proposition 2.2. *Let $\alpha, \beta \in F[G]$ and let $a, b \in F$. Then*

(a) $\alpha^{**} = \alpha$,

(b) $(a\alpha + b\beta)^* = a\alpha^* + b\beta^*$,

(c) $(\alpha\beta)^* = \beta^*\alpha^*$,

Any function $* : A \to A$ on an F-algebra A satisfying Proposition 2.2 is called an **involution** and an algebra equipped with an involution is called a **$*$-algebra**. Thus, every group ring is a $*$-algebra.

Definition 2.3. Let $C \subseteq G$. We define

$$\overline{\boldsymbol{C}} = \sum_{g \in C} g \in F[G].$$

An element $\alpha \in F[G]$ is a **simple quantity** if $\alpha = \overline{C}$ for some $C \subseteq G$. If $C = \emptyset$, then $\overline{C} = 0$.

Proposition 2.4. *Let $D \subseteq C \subseteq G$ be subsets and let $H, K \leq G$ be subgroups.*

(a) $(\overline{C})^* = \overline{C^*}$,

(b) $\overline{C \smallsetminus D} = \overline{C} - \overline{D}$,

(c) $\overline{H} \cdot \overline{K} = |H \cap K| \overline{HK}$.

Let $\boldsymbol{\delta} : F[G] \to F$, called the **augmentation map**, be the linear map given as $\sum_{g \in G} \alpha_g g \mapsto \sum_{g \in G} \alpha_g$.

Proposition 2.5. *Let G be a finite group and let F be a field. Then $\overline{G} \in Z(F[G])$ and for any $\alpha = \sum_{g \in G} \alpha_g g \in F[G]$, we have that $\alpha \overline{G} = \overline{G} \alpha = \delta(\alpha) \overline{G}$.*

Proof. Let $h \in G$. We claim first that $h\overline{G} = \overline{G}h = \overline{G}$, which follows from the straightforward computation

$$h\overline{G} = h \sum_{g \in G} g = \sum_{g \in G} hg = \sum_{h^{-1}g \in G} g = \overline{G}.$$

The last equality holds because if g ranges over all the elements of the group then $h^{-1}g$ also ranges over all the elements. A similar computation shows that $\overline{G}h = \overline{G}$, which proves the claim. This shows also that $\overline{G} \in Z(F[G])$. To finish the proof, let $\alpha \in F[G]$ and we compute

$$\begin{aligned} \alpha \overline{G} &= \left(\sum_{g \in G} \alpha_g g \right) \overline{G} = \sum_{g \in G} (\alpha_g g \overline{G}) \\ &= \sum_{g \in G} (\alpha_g \overline{G}) = \left(\sum_{g \in G} \alpha_g \right) \overline{G} = \delta(\alpha) \overline{G}. \quad \square \end{aligned}$$

Definition 2.6. Define a binary operation $\circ : F[G] \times F[G] \to F[G]$ as follows: if $\alpha, \beta \in F[G]$ with $\alpha = \sum_{g \in G} \alpha_g g$ and $\beta = \sum_{g \in G} \beta_g g$, then

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

The operation $\circ$ is referred to as the **Hadamard product** or the **circle product** on $F[G]$.

Proposition 2.7. *Let $\alpha, \beta, \gamma \in F[G]$, let $r \in F$, $h \in G$, and $C, D \subseteq G$. Then*

(a) $\alpha \circ (\beta \circ \gamma) = (\alpha \circ \beta) \circ \gamma$,

(b) $\alpha \circ (\beta + \gamma) = \alpha \circ \beta + \alpha \circ \gamma$ *and* $(\alpha + \beta) \circ \gamma = \alpha \circ \gamma + \beta \circ \gamma$,

(c) $\overline{G} \circ \alpha = \alpha \circ \overline{G} = \alpha$,

(d) $\alpha \circ \beta = \beta \circ \alpha$,

(e) $(r\alpha) \circ \beta = \alpha \circ (r\beta) = r(\alpha \circ \beta)$,

(f) $\overline{C} \circ \overline{D} = \overline{C \cap D}$.

(g) $\overline{C} \circ \overline{C} = \overline{C}$,

(h) $\overline{C} \circ \overline{D} = 0$ *if and only if* $C \cap D = \emptyset$,

(i) $(\alpha \circ \beta) \cdot h = (\alpha \cdot h) \circ (\beta \cdot h)$,

(j) $(\alpha \circ \beta)^* = \alpha^* \circ \beta^*$.

Proof. Let $\alpha = \sum_{g \in G} \alpha_g g$, $\beta = \sum_{g \in G} \beta_g g$, and $\gamma = \sum_{g \in G} \gamma_g g$. So,

$$\begin{aligned} \alpha \circ (\beta \circ \gamma) &= \alpha \circ \left(\sum_{g \in G} (\beta_g \cdot \gamma_g) g \right) = \sum_{g \in G} [\alpha_g \cdot (\beta_g \cdot \gamma_g)] g \\ &= \sum_{g \in G} [(\alpha_g \cdot \beta_g) \cdot \gamma_g] g = \left(\sum_{g \in G} (\alpha_g \cdot \beta_g) g \right) \circ \gamma = (\alpha \circ \beta) \circ \gamma. \end{aligned}$$

In summary, $\circ$ is associative because the multiplication of F is associative. This proves (a). A similar argument holds also for (b), (d), and (e).

Next, $\overline{G} \circ \alpha = \sum_{g \in G} (1 \cdot \alpha_g) g = \sum_{g \in G} \alpha_g g = \alpha$. Similarly, $\alpha \circ \overline{G} = \alpha$, which gives (c). Suppose that $\alpha = \overline{C}$ and $\beta = \overline{D}$. Thus, $\alpha_g = 1$ if $g \in C$ and $\alpha_g = 0$ if $g \notin C$. Similarly, $\beta_g = 1$ if $g \in D$ and $\beta_g = 0$ if $g \notin D$. Thus, $\alpha_g \beta_g = 1$ if and only if $g \in C \cap D$ and $\alpha_g \beta_g = 0$ if and only if $g \notin C \cap D$. Therefore, (f) holds. Properties (g) and (h) are immediate consequences of (f).

Next,

$$(\alpha \cdot h) \circ (\beta \cdot h) = \left(\sum_{g \in G} \alpha_g gh \right) \circ \left(\sum_{g \in G} \beta_g gh \right) = \sum_{g \in G} (\alpha_g \beta_g) gh = (\alpha \circ \beta) \cdot h,$$

which prove (i).

Lastly,

$$(\alpha \circ \beta)^* = \left(\sum_{g \in G} (\alpha_g \beta_g) g \right)^* = \sum_{g \in G} (\alpha_g \beta_g) g^{-1} = \sum_{g \in G} \alpha_g g^{-1} \circ \sum_{g \in G} \beta_g g^{-1} = \alpha^* \circ \beta^*,$$

which proves (j). □

Note that the previous proposition shows that $(F[G], +, \circ)$ is always a commutative F-algebra with unity $\overline{G}$. In fact, it is easy to check that $(F[G], +, \circ)$ is isomorphic to the $|G|$-fold direct product of F. Furthermore, we have shown that $(F[G], +, \circ)$ is a product of fields. Hence, $(F[G], +, \circ)$ is semisimple. The proposition also shows that $(F[G], +, \circ, *)$ is a $*$-algebra.

We say that two simple quantities $\overline{C}$ and $\overline{D}$ are **disjoint** if $\overline{C} \circ \overline{D} = 0$. In light of Proposition 2.7, $\overline{C}$ and $\overline{D}$ are disjoint if and only if C and D are disjoint.

Definition 2.8. Let $\alpha \in F[G]$, such that $\alpha = \sum_g \alpha_g g$. Let $\mathbf{supp(\alpha)} = \{g \in G \mid \alpha_g \neq 0\}$, which is called the **support** of α.

For a simple quantity, $\text{supp}(\overline{C}) = C$.

We end the section by proving a result due to Wielandt, which shows that all $*$-subalgebras of $\mathbb{Q}[G]$ are semisimple. In particular, Schur rings will be semisimple.

Theorem 2.9 (Wielandt [34])**.** *Every subalgebra of $\mathbb{Q}[G]$ which is closed under $*$ is semisimple.*

Proof. Suppose that S is a $*$-subalgebra of $\mathbb{Q}[G]$ but not semisimple. Let $\mathcal{J}(S)$ denote the Jacobson radical of S. By Theorem A.12, $\mathcal{J}(S) \neq 0$ and contains a simple left ideal $S\alpha$, since S is artinian. But $\alpha \in \mathcal{J}(S)$. So $\alpha(S\alpha) = 0$, and hence $\alpha\alpha^*\alpha = 0$. Then

$$\alpha\alpha^*\alpha\alpha^* = (\alpha\alpha^*)(\alpha\alpha^*)^* = 0.$$

We now claim that the only solution $\beta \in \mathbb{Q}[G]$ to the equation $\beta\beta^* = 0$ is 0 itself. Suppose $\beta = \sum_g \beta_g g$. Then the coefficient of 1 in $\beta\beta^*$ is $\sum_g \beta_g^2$. Now, a sum of squares is 0 in $\mathbb{Q}$ if and only if $\beta_g = 0$ for all $g \in G$. Thus, $\beta\beta^* = 0$ implies that $\beta = 0$.

By the above claim, it must be that $\alpha\alpha^* = 0$. Again using the claim, we conclude that $\alpha = 0$, which contradicts $\mathcal{J}(S) \neq 0$. Therefore, S is semisimple. □

Theorem 2.9 is also true for all fields $F \subseteq \mathbb{R}$ with the same proof. The result is also true for $F = \mathbb{C}$ with the same proof, although we must redefine the involution as $\alpha^* = \sum_{g \in G} \overline{\alpha_g} g^{-1}$, where $\overline{\alpha_g}$ denotes the complex conjugate of α_g.

2.2 Schur Rings

Definition 2.10 (Schur Ring)**.** Let $\{C_1, C_2, \ldots, C_r\}$ be a partition of a finite group G and let S be the subspace of $F[G]$ spanned by $\overline{C_1}, \overline{C_2}, \ldots, \overline{C_r}$. We say that S is a **Schur Ring** over G if

(i) $C_1 = \{1\}$;

(ii) for each i, there is a j such that $C_i^* = C_j$;

(iii) for each i and j, we have $\overline{C_i} \cdot \overline{C_j} = \sum_{k=1}^{r} \lambda_{i,j,k} \overline{C_k}$, for constants $\lambda_{ijk} \in F$.

In the above equation, the $\lambda_{i,j,k}$ are referred to as the **structure constants** of S.

For a Schur ring S over G, let $\boldsymbol{\mathcal{D}(S)} = \{C_1, C_2, \ldots, C_r\}$ denote the partition corresponding to S. We will refer to the sets $C_1, \ldots, C_r$ as the ***S*-classes** or the **primitive sets** of S. We also say that S is the Schur ring **afforded by the partition $\boldsymbol{\mathcal{D}(S)}$**. Finally, the simple quantities $\overline{C_1}, \overline{C_2}, \ldots, \overline{C_r}$ in S will be referred to as the **class sums** of S.

In summary of Definition 2.10, a subalgebra $S \subseteq F[G]$ is a Schur ring if it spanned by a basis of disjoint simple quantities, contains 1 and $\overline{G}$, and is closed under $*$.

Notice that 2.10 (iii) implies that if a partition of G affords a Schur ring, then the product of any two primitive sets is a union of primitive sets.

With respect to the Hadamard product, the class sums of a Schur ring S form an orthogonal basis of primitive central idempotents and $\overline{G}$ acts as unity. These properties characterize Schur rings.

Theorem 2.11 ([24] Lemma 1.3)**.** *Suppose that S is a subalgebra of $F[G]$. Then S is a Schur ring if and only if S is closed under both $*$ and $\circ$ and contains both 1 and $\overline{G}$.*

Proof. Suppose first that S is a Schur ring with partition $\mathcal{D}(S) = \{C_1, C_2, \ldots, C_r\}$. By definition, S is closed under $*$ and $1, \overline{G} \in S$. So we need only show that S is closed under $\circ$. To see this we compute, using Proposition 2.7,

$$\alpha \circ \beta = \left(\sum_{i=1}^{r} \alpha_i \overline{C_i} \right) \circ \left(\sum_{i=1}^{r} \beta_i \overline{C_i} \right) = \sum_{i=1}^{r} \alpha_i \beta_i (\overline{C_i} \circ \overline{C_i}) = \sum_{i=1}^{r} \alpha_i \beta_i \overline{C_i} \in S,$$

which proves the first direction.

Next, suppose that S is closed under $*$ and $\circ$. Now, consider the ring structure $S_\circ = (S, +, \circ)$. Then $S_\circ$ is a subalgebra of $F[G]_\circ = (F[G], +, \circ)$. Clearly, $F[G]$ is isomorphic to a $|G|$-fold product of F. Thus, $F[G]_\circ$ is commutative and semisimple. Since $F[G]_\circ$ is commutative, every subalgebra of $F[G]_\circ$ is commutative and semisimple, including $S_\circ$. Therefore, there exists pairwise-orthogonal primitive idempotents $\tau_i \in S_\circ$ such that

$$S_\circ = (S_\circ \circ \tau_1) \oplus (S_\circ \circ \tau_2) \oplus \ldots \oplus (S_\circ \circ \tau_r). \tag{2.1}$$

Since $\tau_i \circ \tau_i = \tau_i$, it must be that τ_i is a simple quantity, that is, there exist some $C_i \subseteq G$ such that $\tau_i = \overline{C_i}$. Since $\tau_i \circ \tau_j = 0$ for $i \neq j$, we have $C_i \cap C_j = \emptyset$. The primitivity of τ_i requires that $S \circ \tau_i$ is a field extension of F contained in $\prod_{g \in C_i}(F[G]_\circ \circ g)$. Since $F[G]_\circ \circ g \cong F$ for each $g \in G$, it must be that $S_\circ \circ \tau_i \cong F$ for each i. Equation (2.1) then shows that $\{\overline{C_1}, \overline{C_2}, \ldots, \overline{C_r}\}$ is a F-basis for $S_\circ$. Next, since S is closed under $*$, the involution $*$ is a ring automorphism $S_\circ \to S_\circ$ satisfying $(\alpha \circ \beta)^* = \alpha^* \circ \beta^*$ by Proposition 2.7. Thus, $(\overline{C_i})^*$ is also a primitive idempotent. Since $\{\overline{C_1}, \overline{C_2}, \ldots, \overline{C_r}\}$ contains all the primitive idempotents of $S_\circ$, $(\overline{C_i})^* = \overline{C_j}$ for some j.

If additionally $\overline{G} \in S$, then $\{\overline{C_1}, \overline{C_2}, \ldots, \overline{C_r}\}$ must also form a partition of G. Lastly, if $1 \in S$, then S is a Schur ring over G. □

Lemma 2.12. *Let S be a Schur ring over G. Let $g \in G$ such that $\{g\} \in \mathcal{D}(S)$. Then $gC, Cg \in \mathcal{D}(S)$ for all $C \in \mathcal{D}(S)$.*

Proof. Let $\mathcal{D}(S) = \{C_1, C_2, \ldots, C_r\}$. Then $g\overline{C_i} = \sum_k \lambda_k \overline{C_k}$ for S-classes C_k. Now, $g^{-1} = g^* \in S$. Thus, $\overline{C_i} = \sum_k \lambda_k g^{-1}\overline{C_k}$. Since $C_k \cap C_j = \emptyset$ implies that $g^{-1}C_k \cap g^{-1}C_j = \emptyset$, we see that $\overline{C_i} = g^{-1}\overline{C_k}$ for some k. Therefore, $g\overline{C_i} = \overline{C_k}$. □

Proposition 2.13. *Let S be a Schur ring over G. Let $H = \{h \mid \{h\} \in \mathcal{D}(S)\}$. Then $H \leq G$.*

Proof. Clearly, $1 \in H$. Also, if $\{h\} \in \mathcal{D}(S)$, then $\{h^{-1}\} = \{h\}^* \in \mathcal{D}(S)$. So, H is closed under inverses. Lastly, if $\{g\}, \{h\} \in \mathcal{D}(S)$, then $\{gh\} \in \mathcal{D}(S)$ by the previous lemma. So, H is closed under multiplication and hence is a subgroup of G. □

We next provide a few examples of Schur rings.

Example 2.14. Every finite group algebra $F[G]$ is a Schur ring, where each class of $\mathcal{D}(F[G])$ consists of only a single element. For this reason, Schur rings may be thought of as a generalization of group rings. Naturally, $F[G]$ is the largest possible Schur ring over G, that is, it is the unique Schur ring which contains all other Schur rings of G. ∎

Example 2.15. At the other extreme, consider the partition $G = \{1\} \cup (G \setminus \{1\})$ and let S be the subring of $F[G]$ generated by these two class sums. Certainly, $1^* = 1$ and $(\overline{G}-1)^* = \overline{G}-1$. Also, $(\overline{G}-1)^2 = \overline{G}^2 - 2\overline{G}+1 = (|G|-2)\overline{G}+1 = (|G|-2)(\overline{G}-1)+(|G|-1)$. Therefore, S is a Schur ring, which we refer to as the **trivial Schur ring**. The trivial Schur ring is always contained in the center of $F[G]$ and hence is a commutative ring, even if G is nonabelian. The trivial Schur ring will be denoted as $\boldsymbol{F[G]^0}$. A complete multiplication table of $F[G]^0$ can be found in Table 2.1.

Table 2.1: Multiplication Table for $F[G]^0$

	$\tau_1 = 1$	$\tau_2 = \overline{G} - 1$
τ_1	τ_1	τ_2
τ_2	τ_2	$(\lvert G\rvert - 1)\tau_1 + (\lvert G\rvert - 2)\tau_2$

The trivial Schur ring $F[G]^0$ is the unique Schur ring of $F[G]$ of smallest dimension, that is, $F[G]^0$ is the unique Schur ring contained in all Schur rings over G. When $G \neq 1$, $F[G]^0$ is the unique Schur ring of dimension 2. ∎

Example 2.16. Let $G = S_3$, the symmetric group on 3 elements. Let

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

This partition of G affords a Schur ring as shown in Table 2.2. ∎

Example 2.17. Let $G = Z_7 = \langle z \rangle$, the cyclic group of order 7. Let

$$\mathcal{D} = \{\{1\}, \{z, z^2, z^4\}, \{z^3, z^5, z^6\}\}.$$

Table 2.2: Multiplication Table for the Schur Ring in Example 2.16

	$\tau_1 = 1$	$\tau_2 = (12)$	$\tau_3 = (123) + (321)$	$\tau_4 = (13) + (23)$
τ_1	τ_1	τ_2	τ_3	τ_4
τ_2	τ_2	τ_1	τ_4	τ_3
τ_3	τ_3	τ_4	$2\tau_1 + \tau_3$	$2\tau_2 + \tau_4$
τ_4	τ_4	τ_3	$2\tau_2 + \tau_4$	$2\tau_1 + \tau_3$

This partition of G generates a Schur ring as shown in Table 2.3. ∎

Table 2.3: Multiplication Table for the Schur Ring in Example 2.17

	$\tau_1 = 1$	$\tau_2 = z + z^2 + z^4$	$\tau_3 = z^3 + z^5 + z^6$
τ_1	τ_1	τ_2	τ_3
τ_2	τ_2	$\tau_2 + 2\tau_3$	$3\tau_1 + \tau_2 + \tau_3$
τ_3	τ_3	$3\tau_1 + \tau_2 + \tau_3$	$2\tau_2 + \tau_3$

Example 2.18. Let $H \leq G$ and let S be the subspace of $F[G]$ afforded by the partition $\mathcal{D}(S) = \{\{1\}, H \smallsetminus \{1\}, G \smallsetminus H\}$. In particular, $S = \mathrm{Span}_F\langle 1, \overline{H} - 1, \overline{G} - \overline{H}\rangle = \mathrm{Span}_F\langle 1, \overline{H}, \overline{G}\rangle$. Notice that $\overline{H} \cdot \overline{H} = |H| \cdot \overline{H}$, $\overline{H} \cdot \overline{G} = \overline{G} \cdot \overline{H} = |H| \cdot \overline{G}$, and $\overline{G}^2 = |G| \cdot \overline{G}$. Also, $\overline{H}^* = \overline{H}$. Theorem 2.11 then shows that S is a Schur ring.

This kind of Schur ring is our first example of a wedge product of Schur rings and is the simplest kind of wedge product. Wedge products are defined later in Example 2.58. ∎

Example 2.19 (Lattice Schur Rings)**.** Let G be a finite group and $\mathcal{L}$ be a sublattice of the lattice of normal subgroups of G. Then we define

$$\boldsymbol{S(\mathcal{L})} = \mathrm{Span}_F\{\overline{H} \mid H \in \mathcal{L}\}.$$

Since $\overline{H} \circ \overline{K} = \overline{H \cap K}$ and $\overline{H} \cdot \overline{K} = |H \cap K|\overline{HK}$ for $H, K \leq G$, $S(\mathcal{L})$ is a Schur ring, by Theorem 2.11. For this reason, $S(\mathcal{L})$ will be called a **lattice Schur ring**. It should be mentioned that $\mathcal{D}(S) \neq \{\overline{H} : H \in \mathcal{L}\}$.

For any finite group G, the trivial Schur ring is a lattice Schur ring, corresponding to the lattice $\{1, G\}$. The Schur ring from Example 2.18 (in the case that $H \trianglelefteq G$) is another example of a lattice Schur ring, using the lattice $\{1, H, G\}$. ∎

Example 2.20 (Orbit Schur Rings)**.** Let $\mathcal{H} \leq \mathrm{Aut}(G)$. Let

$$\boldsymbol{F[G]^{\mathcal{H}}} = \{\alpha \in F[G] \mid \sigma(\alpha) = \alpha, \text{ for all } \sigma \in \mathcal{H}\},$$

that is, it is the largest subring of $F[G]$ which is fixed by the automorphism group $\mathcal{H}$. We claim that $F[G]^{\mathcal{H}}$ is a Schur ring of G. By Theorem B.3, $F[G]^{\mathcal{H}}$ is an F-subalgebra of $F[G]$ with unity that is generated by the periods of the elements of G with respect to $\mathcal{H}$. In particular, $F[G]^{\mathcal{H}}$ has a basis of disjoint simple quantities whose sum is $\overline{G}$. Since $\sigma(g^{-1}) = \sigma(g)^{-1}$, we have that $C^* \in \mathcal{D}(F[G]^{\mathcal{H}})$ for all primitive sets C. Therefore, $F[G]^{\mathcal{H}}$ is a Schur ring, as claimed, whose partition of G is the $\mathcal{H}$-orbits of G. The Schur ring $F[G]^{\mathcal{H}}$ is called an **orbit Schur ring**.

The group ring $F[G]$ is an orbit Schur ring with respect to $\mathcal{H}$ when $\mathcal{H} = 1 \leq \mathrm{Aut}(G)$, that is, $F[G] = F[G]^{\mathrm{Id}}$. ∎

Example 2.21 (Rational Schur Rings)**.** Let $\boldsymbol{\mathcal{R}(F[G])} = F[G]^{\mathrm{Aut}(G)}$, that is, the Schur ring whose partition is the automorphism classes of G. Any Schur ring contained in $\mathcal{R}(F[G])$ is called a **rational Schur ring** since it is fixed by all group automorphisms. Rational Schur rings have been well studied in the literature, especially in the case of cyclic groups. It was observed by Muzychuk in [23] that for cyclic groups the lattice Schur rings correspond exactly with the rational Schur rings. Understanding the rational Schur rings is useful in developing structure theorems of Schur rings over cyclic groups [15, 23]. ∎

Example 2.22 (Central Schur Rings)**.** Let G be any finite group and consider $S = F[G]^{\mathrm{Inn}(G)}$, where $\mathrm{Inn}(G)$ is the group of inner automorphisms of G. So, S is a Schur ring whose partition $\mathcal{D}(S)$ is the collection of conjugacy classes. In fact, $S = Z(F[G])$, since an element $\alpha \in Z(F[G])$ if and only if $g\alpha = \alpha g$ for all $g \in G$ if and only if $g^{-1}\alpha g = \alpha$

for all $g \in G$ if and only if $\alpha \in F[G]^{\mathrm{Inn}(G)}$. Therefore, the center of a group ring is always a Schur ring. Any Schur ring contained in $Z(F[G])$ is called a **central Schur ring**. The importance of the structure of the group ring $F[G]$ and its center $Z(F[G])$ is readily seen in representation theory. ∎

Example 2.23 (Symmetric Schur Rings)**.** Let G be a finite group. Now, $* \in \mathrm{Aut}(G)$ if and only if G is abelian. Thus, if G is abelian, the subalgebra $F[G]^{\langle * \rangle}$ is a Schur ring of G whose classes are of the form $C_g = \{g, g^{-1}\}$. We will denote this Schur ring by $\boldsymbol{\mathcal{S}(F[G])}$. We say an element α of $F[G]$ is **symmetric** if $\alpha^* = \alpha$. Thus, $\mathcal{S}(F[G])$ is the collection of all symmetric elements of $F[G]$. Any Schur ring contained in $\mathcal{S}(F[G])$ is called a **symmetric Schur ring**. For example, lattice Schur rings are always symmetric. ∎

Example 2.24. When G is a nonabelian group, there is no guarantee that the collection of symmetric elements forms a subring of $F[G]$. For example, let $G = S_3$ and consider the symmetric elements of $\mathbb{Q}[G]$. Since transpositions have order 2, each transposition in S_3 is its own inverse. Thus, $\mathcal{S}(\mathbb{Q}[G])$ contains all transpositions of G. But the product $(12) \cdot (23)$ is a 3-cycle and not contained in $\mathcal{S}(\mathbb{Q}[G])$, since 3-cycles have order 3. So, $\mathcal{S}(\mathbb{Q}[G])$ is not a ring and hence not a Schur ring.

On the other hand, let $G = Q_8$, the quaternion group of 8 elements. For Q_8, the inverse classes of G are the same as the conjugacy classes of G. Thus, $\mathcal{S}(\mathbb{Q}[G])$ is the center of $\mathbb{Q}[G]$, which is always a Schur ring. In particular, if C_x denotes the conjugacy class of $x \in G$, then $\mathcal{D}(S) = \{C_1, C_{-1}, C_i, C_j, C_k\}$ and the multiplication table for the Schur ring is given in Table 2.4. ∎

Proposition 2.25. *Let S and T be Schur rings over G. Then $S \cap T$ is a Schur ring over G.*

Proof. Certainly, $1, \overline{G} \in S \cap T$. If $\alpha \in S$, then $\alpha^* \in S$. Likewise, if $\alpha \in T$, then $\alpha^* \in T$. So, $\alpha^* \in S \cap T$ whenever $\alpha \in S \cap T$. Lastly, suppose $\alpha, \beta \in S \cap T$, then $\alpha \circ \beta \in S, T$ by Theorem 2.11. This implies that $\alpha \circ \beta \in S \cap T$. Therefore, $S \cap T$ is a Schur ring, again by Theorem 2.11. □

The set of all partitions of a finite group G forms a lattice, defined with $\wedge$ and $\vee$ given as follows: if P and Q are partitions of G, then $P \wedge Q$ is the largest partition of G contained

Table 2.4: Multiplication Table of $Z(\mathbb{Q}[Q_8])$

	$\tau_1 = \overline{C_1}$	$\tau_{\text{-}1} = \overline{C_{\text{-}1}}$	$\tau_i = \overline{C_i}$	$\tau_j = \overline{C_j}$	$\tau_k = \overline{C_k}$
τ_1	τ_1	$\tau_{\text{-}1}$	τ_i	τ_j	τ_k
$\tau_{\text{-}1}$	$\tau_{\text{-}1}$	τ_1	τ_i	τ_j	τ_k
τ_i	τ_i	τ_i	$2\tau_1 + 2\tau_{\text{-}1}$	$2\tau_k$	$2\tau_j$
τ_j	τ_j	τ_j	$2\tau_k$	$2\tau_1 + 2\tau_{\text{-}1}$	$2\tau_i$
τ_k	τ_k	τ_k	$2\tau_j$	$2\tau_i$	$2\tau_1 + 2\tau_{\text{-}1}$

both in P and Q and $P \vee Q$ is the smallest partition of G which contains both P and Q. Proposition 2.25 then says that $\mathcal{D}(S \cap T) = \mathcal{D}(S) \wedge \mathcal{D}(T)$. On the other hand, $\mathcal{D}(S) \vee \mathcal{D}(T)$ does not afford a Schur ring in general.

Example 2.26 (Dot Products)**.** Let S and T be Schur rings over G and H, respectively. We naturally can view G and H as subgroups of $G \times H$. Let

$$\mathcal{D} = \{CD \mid C \in \mathcal{D}(S), D \in \mathcal{D}(T)\}, \tag{2.2}$$

that is, $\mathcal{D}$ is the partition of $G \times H$ generated by all the possible products of S- and T-classes. Let

$$\boldsymbol{S \cdot T} = \mathrm{Span}_F\{\overline{CD} \mid C \in \mathcal{D}(S), D \in \mathcal{D}(T)\} = \mathrm{Span}_F\{\overline{C} \cdot \overline{D} \mid C \in \mathcal{D}(S), D \in \mathcal{D}(T)\},$$

the subspace of $F[G \times H]$ afforded by $\mathcal{D}$. Since both $\mathcal{D}(S)$ and $\mathcal{D}(T)$ contain the identity class $\{1\}$, $S \cdot T$ contains an isomorphic copy of S and T and they centralize each other in $S \cdot T$. Furthermore, $1 \in S \cdot T$ and $\overline{G \times H} = \overline{G} \cdot \overline{H} \in S \cdot T$. For any S- and T-classes C and D, respectively, $(\overline{C} \cdot \overline{D})^* = \overline{D}^* \cdot \overline{C}^* = \overline{C}^* \cdot \overline{D}^* \in S \cdot T$. Thus, $S \cdot T$ is closed under $*$. Lastly, if $C_1, C_2 \in \mathcal{D}(S)$ and $D_1, D_2 \in \mathcal{D}(T)$, then $\overline{C_1} \cdot \overline{C_2} \in S$, $\overline{D_1} \cdot \overline{D_2} \in T$ and

$$(\overline{C_1} \cdot \overline{D_1})(\overline{C_2} \cdot \overline{D_2}) = (\overline{C_1} \cdot \overline{C_2})(\overline{D_1} \cdot \overline{D_2}) \in S \cdot T.$$

Therefore, $S \cdot T$ is a Schur ring over $G \times H$. We refer to $S \cdot T$ as the **dot product Schur ring** of S and T or the **direct product Schur ring**. By some authors, $S \cdot T$ is denoted as $S \times T$.

It is a fact that $F[G \times H] \cong F[G] \otimes_F F[H]$, as F-algebras. Using similar reasoning, it is true that $S \cdot T \cong S \otimes_F T$, as F-algebras. Because of this isomorphism, $S \cdot T$ is sometimes referred to as the **tensor product Schur ring** of S and T and denoted as $S \otimes T$.

The Schur ring $S \cdot T$ also has the property that it is the smallest Schur ring of $G \times H$ which contains the subalgebras S and T and hence is the composite or join of the two Schur rings. ∎

Lemma 2.27. *Let G_1, G_2 be finite groups and $\mathcal{H}_i \leq \mathrm{Aut}(G_i)$. Then*

$$\mathbb{Q}[G_1 \times G_2]^{\mathcal{H}_1 \times \mathcal{H}_2} = \mathbb{Q}[G_1]^{\mathcal{H}_1} \cdot \mathbb{Q}[G_2]^{\mathcal{H}_2}.$$

Proof. Let C be the automorphism class of (g_1, g_2) with respect to $\mathcal{H}_1 \times \mathcal{H}_2$. Let C_i be the automorphism class of g_i with respect to $\mathcal{H}_i$, $i = 1, 2$. Then (g_1, g_2) is automorphic to (g_1', g_2') under $\mathcal{H}_1 \times \mathcal{H}_2$ if and only if g_1 is automorphic to g_1' under $\mathcal{H}_1$ and g_2 is automorphic to g_2' under $\mathcal{H}_2$ if and only if $C = C_1 \times C_2$. The result then follows. □

We present now two more constructions of Schur rings which generalize the method of dot products from Example 2.26.

Example 2.28 (Central Products)**.** Let G be a finite group. Let $H, K \leq G$ such that $G = HK$ and H and K centralize each other, that is, $[H, K] = 1$. Then $G = H *_Z K$ is the central product of H and K. As a consequence, $H, K \trianglelefteq G$. Let $L = H \cap K$. Certainly, $L \leq Z(G)$.

Let S and T be Schur rings over H and K, respectively, such that $F[L] \subseteq S \cap T$, that is, the restriction of S and T to the subgroup L is the whole group ring on L. Let

$$\boldsymbol{S *_Z T} = \mathrm{Span}\{\overline{CD} \mid C \in \mathcal{D}(S), D \in \mathcal{D}(T)\}.$$

We claim that $S *_Z T$ is a Schur ring over G.

Let

$$\mathcal{D} = \{CD \mid C \in \mathcal{D}(S), D \in \mathcal{D}(T)\}. \tag{2.3}$$

So, $S *_Z T = \mathrm{Span}_F\{\overline{B} \mid B \in \mathcal{D}\}$. We first show that $\mathcal{D}$ forms a partition of G. Let $g \in G$. Since $G = HK$, there exists $h \in H, k \in K$ such that $g = hk$. Now, there exists some $C \in \mathcal{D}(S)$ and $D \in \mathcal{D}(T)$ such that $h \in C$ and $k \in D$. Thus, $g \in CD$. Suppose next that there exists sets $C_1, C_2 \in \mathcal{D}(S)$ and $D_1, D_2 \in \mathcal{D}(T)$ such that $g \in C_1D_1 \cap C_2D_2$. In particular, there exists elements $h_i \in C_i$, $k_i \in D_i$ such that $g = h_1k_1 = h_2k_2$. Then $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = L$. Since $h_2^{-1}h_1 \in L$, $C_2(h_2^{-1}h_1) \in \mathcal{D}(S)$. This implies that $C_2(h_2^{-1}h_1) = C_1$. Likewise, $(k_2k_1^{-1})^{-1}D_2 = D_1$. Therefore,

$$C_2D_2 = C_2(h_2^{-1}h_1)(k_2k_1^{-1})^{-1}D_2 = C_1D_1.$$

Therefore, $\mathcal{D}$ forms a partition on G.

Since $\{1\} \in \mathcal{D}(S) \cap \mathcal{D}(T)$, $\{1\} \in \mathcal{D}$. Next, if $CD \in \mathcal{D}$, then $(CD)^* = D^*C^* = C^*D^* \in \mathcal{D}$ since $C^* \in \mathcal{D}(S)$ and $D^* \in \mathcal{D}(T)$. To show that $S *_Z T$ is a Schur ring, it remains to prove that $S *_Z T$ is a ring. For this purpose, we will first show that $\overline{C} \cdot \overline{D} = \mu\overline{CD}$, for some positive integer μ.

To prove this claim, consider

$$\begin{aligned} \overline{H} \cdot \overline{K} &= \left(\sum_{C \in \mathcal{D}(S)} \overline{C}\right)\left(\sum_{D \in \mathcal{D}(T)} \overline{D}\right) = \sum_{C,D} \overline{C} \cdot \overline{D} && (2.4) \\ &= |H \cap K|\overline{HK} = |L| \sum_{B \in \mathcal{D}} \overline{B}. && (2.5) \end{aligned}$$

Clearly, $\mathrm{supp}\left(\overline{C} \cdot \overline{D}\right) \subseteq CD$, and, by construction, every $B \in \mathcal{D}$ is of the form $B = CD$ for some $C \in \mathcal{D}(S)$ and $D \in \mathcal{D}(T)$. By comparing coefficients in (2.4) and (2.5), we get

$$|L|\overline{B} = \sum_{CD=B} \overline{C} \cdot \overline{D}.$$

Suppose that $C_1D_1 = B = C_2D_2$. Then there exists some $\ell \in L$ such that $C_1 = C_2\ell$ and $D_1 = \ell^{-1}D_2$, by the work done above. Thus, $\overline{C_2} \cdot \overline{D_2} = (\overline{C_2}\ell) \cdot (\ell^{-1}\overline{D_2}) = \overline{C_2\ell} \cdot \overline{\ell^{-1}D_2} = \overline{C_1} \cdot \overline{D_1}$.

Therefore, if n is the number of terms in the sum $\sum_{CD=B} \overline{C} \cdot \overline{D}$, then

$$|L|\overline{CD} = n(\overline{C} \cdot \overline{D}).$$

Then the previous equation implies that

$$\overline{C} \cdot \overline{D} = \frac{|L|}{n}\overline{CD} = \mu\overline{CD}.$$

Since the coefficients of each group element in $\overline{C} \cdot \overline{D}$ necessarily are positive integers, this proves the claim.

Since S and T are Schur rings, there exists structure constants λ_{ijk} and κ_{rst} such that

$$\overline{C_i} \cdot \overline{C_j} = \sum_k \lambda_{ijk}\overline{C_k} \quad \text{and} \quad \overline{D_r} \cdot \overline{D_s} = \sum_t \kappa_{rst}\overline{D_t}.$$

Then

$$\begin{aligned}\left(\overline{C_i} \cdot \overline{D_r}\right) \cdot \left(\overline{C_j} \cdot \overline{D_s}\right) &= \left(\overline{C_i} \cdot \overline{C_j}\right) \cdot \left(\overline{D_r} \cdot \overline{D_s}\right) = \left(\sum_k \lambda_{ijk}\overline{C_k}\right) \cdot \left(\sum_t \kappa_{rst}\overline{D_t}\right) \\ &= \sum_{k,t} \left(\lambda_{ijk}\kappa_{rst}\right) \overline{C_k} \cdot \overline{D_t} = \sum_{k,t} \left(\lambda_{ijk}\kappa_{rst}\mu_{kt}\right) \overline{C_k D_t} \in S *_Z T.\end{aligned}$$

Therefore, $S *_Z T$ is a Schur ring, which we refer to as the **central product Schur ring** of S and T. By comparing equations (2.2) and (2.3) and recognizing that $H *_Z K = H \times K$ when $L = 1$, we note that $S *_Z T$ generalizes the construction in Example 2.26. Thus, we may also denote $S *_Z T$ as $S \cdot T$. ∎

Example 2.29 (Semi-direct Products)**.** Let G be a finite group. Let $H \trianglelefteq G$, $K \leq G$ such that $G = HK$ and $H \cap K = 1$. Then $G = H \rtimes K$ is the semi-direct product of H and K. As a consequence, conjugation of K on H induces a homomorphism $\varphi : K \to \mathrm{Aut}(H)$.

Let S and T be Schur rings over H and K, respectively, such that $S \cap F[H]^{\varphi(K)} = S$, that is, S is $\varphi(K)$-rational. Let

$$\boldsymbol{S} \rtimes \boldsymbol{T} = \mathrm{Span}\{\overline{CD} \mid C \in \mathcal{D}(S), D \in \mathcal{D}(T)\}.$$

We claim that $S \rtimes T$ is a Schur ring over G.

Let $\mathcal{D} = \{CD \mid C \in \mathcal{D}(S), D \in \mathcal{D}(T)\}$. Since $H \cap K = 1$, we see $\mathcal{D}$ is a partition of G. Since S is $\varphi(K)$-rational, the classes of S commute with the classes of T in $F[G]$. So, as in the case of direct and central products, $1, \overline{G}, (CD)^* \in S \rtimes T$ for all $C \in \mathcal{D}(S)$ and $D \in \mathcal{D}(T)$. Thus, it remains to prove that $S \rtimes T$ is a ring. But as in the case of direct products, $\overline{CD} = \overline{C} \cdot \overline{D} = \overline{D} \cdot \overline{C}$. Thus, $S \rtimes T$ is closed under multiplication. Therefore, $S \rtimes T$ is a Schur ring, which we refer to as the **semi-direct product Schur ring** of S and T. Like the last example, $S \rtimes T$ also generalizes the construction in Example 2.26. Thus, we may also denote $S \rtimes T$ as $S \cdot T$. ∎

We now will end this section by proving some elementary propositions about Schur rings that will be useful in future proofs. All of these results are due to Wielandt [35] and will be built upon a fundamental lemma of Schur rings, Lemma 2.31. This lemma is preceded by a definition.

Definition 2.30. Let S be a Schur ring over G and let $C \subseteq G$. We say that C is an ***S*-set** of G if $\overline{C} \in S$. If C is an S-set and a subgroup of G, then we say that C is an ***S*-subgroup** of G.

The following is clear.

Lemma 2.31. *Let G be a finite group and let S be a Schur ring over G. Let $\alpha \in S$ such that $\alpha = \sum_{g \in G} \alpha_g g$. Then $\{g \in G \mid \alpha_g = c\}$ is an S-set for each $c \in F$.* □

We now begin with the first of the propositions.

Proposition 2.32. *Let S be a Schur ring over G and let $\alpha = \sum_{g \in G} \alpha_g g \in S$. Then* $\mathrm{supp}(\alpha)$ *is an S-set.*

Proof. Let $K_c = \{g \in G \mid \alpha_g = c\}$ for $c \in F$. By Lemma 2.31, $\overline{K_c} \in S$ for all $c \in F$. Then

$$\overline{\mathrm{supp}(\alpha)} = \overline{\bigcup_{g \in \mathrm{supp}(\alpha)} K_{\alpha_g}} = \sum_{\alpha_g : g \in \mathrm{supp}(\alpha)} \overline{K_{\alpha_g}} \in S.$$

Therefore, $\mathrm{supp}(\alpha)$ is an S-set. □

Proposition 2.33. *Let S be a Schur ring over G, let $\alpha \in S$, and let $H = \langle \mathrm{supp}(\alpha) \rangle$. Then $\overline{H} \in S$. In particular, if $C \in \mathcal{D}(S)$, then $\langle C \rangle$ is an S-subgroup.*

Proof. Let $L = \mathrm{supp}(\alpha)$. Since $H = \langle L \rangle$ is finite, there exists some integer n sufficiently large such that $H = \bigcup_{i=1}^{n} L^i$. Since $\mathrm{char}\, F = 0$, $H = \mathrm{supp}\left(\sum_{i=1}^{n} \overline{L}^i\right)$, which is an S-set by Proposition 2.32. □

Proposition 2.34. *Let S be a Schur ring over G, let $\alpha = \sum_{g \in G} \alpha_g g \in S$, and let $f : F \to F$ be any function. Then $f[\alpha] = \sum_{g \in G} f(\alpha_g) g \in S$.*

Proof. Let $K_c = \{g \in G \mid \alpha_g = c\}$. Then $\overline{K_c} \in S$ for each $c \in F$. Now, if $\alpha = \sum c\overline{K_c}$, then $f[\alpha] = \sum f(c)\overline{K_c} \in S$. □

Proposition 2.35. *Let S be a Schur ring over G. Let $\alpha \in S$ and $\mathrm{Stab}(\alpha) = \{g \in G \mid \alpha g = \alpha\}$. Then $\mathrm{Stab}(\alpha)$ is an S-subgroup of G.*

Proof. Let $\alpha = \sum_{g \in G} \alpha_g g \in S$, let $K_c = \{g \in G \mid \alpha_g = c\}$ for $c \in F$, and let $M_c = \{g \in G \mid K_c g = K_c\}$, that is, M_c is the subset of G which permutes K_c. Let $g \in M_c$. Then there exists $|K_c|$ many solutions $(h, k) \in K_c \times K_c$ to the equation $hg = k$. But each solution is also a solution to the equation $g = kh^{-1}$. Thus, the coefficient of g in $\overline{K_c} \cdot \overline{K_c}^*$ is $|K_c|$. Conversely, if the coefficient of g in $\overline{K_c} \cdot \overline{K_c}^*$ is $|K_c|$, then there are $|K_c|$ distinct solutions $(h, k) \in K_c \times K_c$ to $g = kh^{-1}$, i.e. $hg = k$. Thus, $K_c g = K_c$ and $g \in M_c$. Then applying Lemma 2.31 to $\overline{K_c} \cdot \overline{K_c}^*$ and the coefficient $|K_c|$, we conclude that $\overline{M_c} \in S$. Now,

$$\overline{\mathrm{Stab}(\alpha)} = \overline{\bigcap_{g \in \mathrm{supp}(\alpha)} M_{\alpha_g}} = \bigcirc_{g \in \mathrm{supp}(\alpha)} \overline{M_{\alpha_g}} \in S.$$ □

Proposition 2.36. *Let G be an abelian group, let S be a Schur ring over G, and let $\alpha = \sum_g \alpha_g g \in S$. Define $\alpha^{(m)} = \sum_g \alpha_g g^m$ for $m \in \mathbb{Z}$. Then $\alpha^{(m)} \in S$ for every integer m coprime to $|G|$. Furthermore, define $C^{(m)} = \{g^m \mid g \in C\}$ for each $C \subseteq G$ and $m \in \mathbb{Z}$. Then if $C \in \mathcal{D}(S)$, then $C^{(m)} \in \mathcal{D}(S)$ for every integer m coprime to $|G|$.*

Proof. Clearly, the map $^{(m)} : F[G] \to F[G]$ is linear, so it suffices to prove the statement for a simple quantity α. Also, we note that $\alpha^{(-1)} = \alpha^*$ and $\alpha^{(mm')} = (\alpha^{(m)})^{(m')}$. Thus, it suffices to prove the statement for $m = p$, a prime number not dividing $|G|$.

Since α is simple, there exists some subset $C \subseteq G$ such that $\alpha = \overline{C}$. Since G is abelian, $F[G]$ is a commutative ring and the polynomial congruence

$$\left(\sum_{g \in C} g\right)^p \equiv \sum_{g \in C} g^p \pmod{p}$$

holds. Let $f_p : F \to F$ be the function defined as

$$f_p(n) = \begin{cases} n \mod p, & n \in \mathbb{Z} \\ 0, & \text{otherwise.} \end{cases}$$

Thus, $f_p[\alpha^{(p)}] = f_p[\alpha^p] \in S$ by Proposition 2.34. Now, when $p \nmid |G|$, the map $g \mapsto g^p$ is a group automorphism. So, $\alpha^{(p)}$ is a simple quantity and $\alpha^{(p)} = f_p[\alpha^{(p)}] \in S$.

Let C be a primitive set of S. By the above, we see that $C^{(m)}$ is an S-set. If $C^{(m)}$ is not primitive, then let D be one of the primitive subsets of $C^{(m)}$. In particular, $|D| < |C^{(m)}| = |C|$. Let $1 = am + b|G|$ for some integers a, b. Then $D^{(a)}$ is an S-set, but $D^{(a)} \subsetneq C$, which contradicts C being primitive. Therefore, $C^{(m)}$ must also be primitive. □

Proposition 2.37. *Let G be a cyclic group and let S be a Schur ring over G. Let $\sigma \in \mathrm{Aut}(G)$ and $\alpha \in S$. Then $\sigma(\alpha) \in S$. In particular, if $C \in \mathcal{D}(S)$, then $\sigma(C) \in \mathcal{D}(S)$.*

Proof. Since every automorphism σ is of the form $g \mapsto g^m$ for some integer m relatively prime to $|G|$, the result follows immediately from the previous proposition. □

Definition 2.38. A Schur ring S over a finite group G is **primitive** if the only S-subgroups are 1 and G.

For primitive Schur rings, every non-trivial primitive set necessarily generates the whole group. The trivial Schur ring is a typical example of a primitive Schur ring. As Wielandt has shown, for many abelian groups, this is the only example.

Theorem 2.39 (Wielandt)**.** *If G is a finite abelian group not of prime order with a non-trivial, cyclic Sylow subgroup, then the only primitive Schur ring over G is the trivial Schur ring.*

Proof. Its proof can be found in [35] or in [29, Theorem 13.9.1]. □

Example 2.40. Let $G = Z_3 \times Z_3 = \langle a, b \rangle$ and let

$$S = \mathrm{Span}_{\mathbb{Q}}\{1, a + a^2 + b + b^2, ab + a^2b^2 + ab^2 + a^2b\}.$$

Then S is an orbit Schur ring afforded by the automorphism subgroup generated by the automorphism $\sigma : a \mapsto b, b \mapsto a^2$. Now, the set of S-subgroups is simply $\{1, G\}$, that is, S is primitive. Of course, G has no nontrivial, cyclic Sylow subgroup. The multiplication table of S is shown in Table 2.5. ∎

Table 2.5: Multiplication Table for the Schur Ring in Example 2.40

	$\tau_1 = 1$	$\tau_2 = a + a^2 + b + b^2$	$\tau_3 = ab + a^2b^2 + ab^2 + a^2b$
τ_1	τ_1	τ_2	τ_3
τ_2	τ_2	$4\tau_1 + \tau_2 + 2\tau_3$	$2\tau_2 + 2\tau_3$
τ_3	τ_3	$2\tau_2 + 2\tau_3$	$4\tau_1 + 2\tau_2 + \tau_3$

When $G = Z_p$, for some prime p, every Schur ring is necessarily primitive. These Schur rings will be considered in Theorem 4.21.

2.3 Cayley Maps

Now that we have developed many of the elementary properties of Schur rings, it is natural next to compare Schur rings via homomorphisms. Seeing that Schur rings are subalgebras of $F[G]$, it is natural to relate them via ring or algebra homomorphisms. An algebra homomorphism is a map which preserves the ring and linear structure of the Schur ring. More specifically, let S and T be Schur rings over G and H, respectively, and let $\varphi : S \to T$ be an algebra homomorphism. Let $\alpha, \beta \in S$ and let $c \in F$. Then

$$\varphi(\alpha + \beta) \;=\; \varphi(\alpha) + \varphi(\beta),$$

$$\begin{aligned}\varphi(c\alpha) &= c\varphi(\alpha),\\ \varphi(\alpha\cdot\beta) &= \varphi(\alpha)\cdot\varphi(\beta).\end{aligned}$$

Thus, $\varphi(S)$ is a subalgebra of T. Unfortunately, algebra homomorphisms are not sufficient to study Schur rings. For example, for any two finite groups G and H, we have $F[G]^0 \cong F[H]^0$ as F-algebras. To see this, note that $F[G]^0 = (\overline{G}) \oplus \left(1 - \frac{1}{|G|}\overline{G}\right)$ as simple ideals. Now, $(\overline{G}) \cong \left(1 - \frac{1}{|G|}\overline{G}\right) \cong F$, as F-algebras, independent of the group G. For another example, consider the group algebras $\mathbb{C}[Z_4]$ and $\mathbb{C}[Z_2 \times Z_2]$. As $\mathbb{C}$-algebras, $\mathbb{C}[Z_4] \cong \mathbb{C}[Z_2 \times Z_2] \cong \mathbb{C}^4$. Thus, the appropriate homomorphisms of Schur rings need to be stronger than mere algebra homomorphisms.

Although $\varphi(S)$ is an algebra, by Theorem 2.11, $\varphi(S)$ needs to also be closed under $*$ and $\circ$ in order to be a Schur ring. An arbitrary algebra homomorphism need not preserve these two additional operations, as illustrated above. Thus it is natural to define a **Schur homomorphism** to be a linear map $\varphi : S \to T$ between Schur rings S and T such that:

$$\begin{aligned}\varphi(\alpha\cdot\beta) &= \varphi(\alpha)\cdot\varphi(\beta),\\ \varphi(\alpha\circ\beta) &= \varphi(\alpha)\circ\varphi(\beta),\\ \varphi(\alpha^*) &= \varphi(\alpha)^*,\end{aligned}$$

for all $\alpha, \beta \in S$. If $\varphi : S \to T$ is also bijective, then φ is a **Schur Isomorphism**.

An immediate consequence of this type of homomorphism is that the image $\varphi(S)$ is a Schur ring over some T-subgroup, specifically $\mathrm{supp}(\varphi(\overline{G}))$. Schur homomorphisms were studied by Muzychuk in [24], in which it was proven that Schur rings over a cyclic group are Schur isomorphic if and only if they coincide. Tamaschke also considered Schur homomorphisms[2.1] in his attempt to define a category of Schur rings in [31]. These are only a few examples from the literature.

Suppose S is a Schur ring over G. Considering the ring structure $S_\circ = (S, +, \circ)$, $S_\circ \cong \mathbb{Q}^n$, where $n = \dim S$, and hence $S_\circ$ is semisimple. Thus, any homomorphism $\varphi : S_\circ \to T_\circ$ is simply a function from the S-classes into the T-classes. Thus, if φ is a Schur isomorphism,

[2.1] Tamaschke's original definition of a homomorphism of Schur algebras differs from our presentation, although the two definitions are equivalent.

then φ induces a bijection between the primitive sets of S with the primitive sets of T.

From a categorical sense, this class of morphisms is appropriate; that is, Schur maps are exactly the homomorphisms which preserve the operations of Schur rings. On the other hand, Schur rings were originally used to study groups and much of the algebraic structure of Schur rings depends on the group, so it would be useful for the homomorphisms of Schur rings to also relate to the group. It is possible for nonisomorphic groups to have Schur isomorphic Schur rings, e.g. Z_8 and D_4, the dihedral group of order 8, both have isomorphic Schur rings of dimension three. Instead of Schur homomorphisms, we will study maps which preserve the group structure of Schur rings. These maps will be algebra homomorphisms but will not necessarily preserve Hadamard multiplication. Under certain circumstances, the image of a Schur ring will be a Schur ring. Thus, these maps will sometimes provide a class of more useful homomorphism of Schur rings. We introduce now the notion of a Cayley map.

Definition 2.41. Let G and H be groups, let A and B be subalgebras of $F[G]$ and $F[H]$, respectively, and let $f : A \to B$ be an F-algebra homomorphism. If there exists an F-algebra homomorphism $\varphi : F[G] \to F[H]$ such that $\varphi|_A = f$ and $\varphi|_G : G \to H$ is a group homomorphism, then we say that f is a **Cayley homomorphism**. A bijective Cayley homomorphism is a **Cayley isomorphism**.

For example, let G be a group, let H be a subgroup of G, and let $\sigma \in \mathrm{Aut}(G)$. Then the group algebras $F[H]$ and $F[\sigma(H)]$ are Cayley isomorphic in $F[G]$. If S is a Schur ring over G, then S and $\sigma(S)$ are Cayley isomorphic.

Let $\varphi : G \to H$ be a group homomorphism. Let φ also denote its linear extension $\varphi : F[G] \to F[H]$. Let $g \in G$. Then

$$\varphi(g^*) = \varphi(g^{-1}) = \varphi(g)^{-1} = \varphi(g)^*.$$

By linearity, $\varphi(\alpha^*) = \varphi(\alpha)^*$ for all $\alpha \in F[G]$. In particular, a Cayley map is a $*$-algebra homomorphism, that is, Cayley maps always preserve the involution structure of $F[G]$. Likewise, Cayley maps preserve the involution structure of any $*$-subalgebra of $F[G]$, including Schur rings.

Let $\delta : F[G] \to F$ be the augmentation map, which is a Cayley map induced from the

trivial map $\delta : G \to 1$, and let $\alpha \in F[G]$, with $\alpha = \sum_g \alpha_g g$. Then

$$\delta(\alpha \circ \alpha) = \delta\left(\sum_{g\in G} \alpha_g^2 g\right) = \sum_{g\in G} \alpha_g^2$$

and

$$\delta(\alpha) \circ \delta(\alpha) = \left(\sum_{g\in G} \alpha_g\right) \circ \left(\sum_{g\in G} \alpha_g\right) = \left(\sum_{g\in G} \alpha_g\right)^2.$$

This shows that δ does not preserve Hadamard products in general and that Cayley maps are typically not Schur homomorphisms. The next proposition determines a necessary and sufficient condition for when a Cayley map is a Schur map.

Proposition 2.42. *Let $\varphi : F[G] \to F[H]$ be a Cayley map. Then φ is injective if and only if $\varphi(\alpha \circ \beta) = \varphi(\alpha) \circ \varphi(\beta)$ for all $\alpha, \beta \in F[G]$.*

Proof. Suppose that φ is injective. Let $\alpha = \sum_{g\in G} \alpha_g g$ and $\beta = \sum_{g\in G} \beta_g g$. Then

$$\begin{aligned}
\varphi(\alpha \circ \beta) &= \varphi\left(\sum_{g\in G} \alpha_g \beta_g g\right) = \sum_{g\in G} \alpha_g \beta_g \varphi(g) \\
&= \left(\sum_{g\in G} \alpha_g \varphi(g)\right) \circ \left(\sum_{g\in G} \beta_g \varphi(g)\right), \quad \text{since } \varphi(g) \text{ occurs only once in the above sum,} \\
&= \varphi\left(\sum_{g\in G} \alpha_g g\right) \circ \varphi\left(\sum_{g\in G} \beta_g g\right) = \varphi(\alpha) \circ \varphi(\beta).
\end{aligned}$$

Conversely, suppose that φ is not injective. Let $K = \ker(\varphi|_G) \neq 1$. Then

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

which proves the remaining direction. □

Corollary 2.43. *Every Cayley isomorphism is a Schur isomorphism.* □

Cayley isomorphic is a strictly stronger condition than Schur isomorphic. For example,

consider the partition

$$\{1\}, \quad \{z^4\}, \quad \{z, z^2, z^3, z^5, z^6, z^7\}$$

over $Z_8 = \langle z \rangle$. This partition affords a Schur ring over Z_8, which we denote as S. This Schur ring is Schur isomorphic to the Schur ring T over D_4 associated to the partition

$$\{1\}, \quad \{s\}, \quad \{r, r^2, r^3, rs, r^2s, r^3s\}.$$

Here D_4 is the dihedral group of order 8, $D_4 = \langle r, s \mid r^4, s^2, s^{-1}rs = r^{-1} \rangle$. Now, if S is Cayley isomorphic to T, then there exists some group homomorphism $\varphi : Z_8 \to D_4$ such that $\varphi(S) = T$. Since $\varphi(S)$ contains $\overline{D_4}$, φ must be surjective. Considering the orders of the groups, φ must also be injective, that is, $\varphi : Z_8 \to D_4$ is a group isomorphism, which is absurd. Therefore, S and T are Schur isomorphic but not Cayley isomorphic. In particular, Schur isomorphic Schur rings associated to nonisomorphic groups cannot be Cayley isomorphic by this same argument.

The following formula was proven in [24].

Proposition 2.44. *Let $\varphi : G \to H$ be a group homomorphism with $\ker \varphi = K$. Let $\alpha, \beta \in F[G]$. Then*

$$\varphi(\alpha) \circ \varphi(\beta) = \frac{1}{|K|} \varphi((\alpha \cdot \overline{K}) \circ (\beta \cdot \overline{K})).$$

Proof. Suppose that $\alpha = \sum_g \alpha_g g$ and $\beta = \sum_g \beta_g g$. Then, the left hand side is

$$\begin{aligned} \varphi(\alpha) \circ \varphi(\beta) &= \varphi\left(\sum_{g \in G} \alpha_g g\right) \circ \varphi\left(\sum_{g \in G} \beta_g g\right) \\ &= \left[\sum_{h \in \varphi(G)} \left(\sum_{\varphi(g)=h} \alpha_g\right) h\right] \circ \left[\sum_{h \in \varphi(G)} \left(\sum_{\varphi(g)=h} \beta_g\right) h\right] \\ &= \sum_{h \in \varphi(G)} \left[\left(\sum_{\varphi(g)=h} \alpha_g\right)\left(\sum_{\varphi(g)=h} \beta_g\right)\right] h. \end{aligned}$$

The right hand side is

$$\frac{1}{|K|} \varphi((\alpha \cdot \overline{K}) \circ (\beta \cdot \overline{K})) = \frac{1}{|K|} \varphi\left[\left(\sum_{g' \in G} \left(\sum_{g \in g'K} \alpha_g\right) g'\right) \circ \left(\sum_{g' \in G} \left(\sum_{g \in g'K} \beta_g\right) g'\right)\right]$$

$$= \frac{1}{|K|}\varphi\left[\sum_{g'\in G}\left(\sum_{g\in g'K}\alpha_g\right)\left(\sum_{g\in g'K}\beta_g\right)g'\right]$$
$$= \frac{|K|}{|K|}\sum_{h\in\varphi(G)}\left[\left(\sum_{\varphi(g)=h}\alpha_g\right)\left(\sum_{\varphi(g)=h}\beta_g\right)\right]h. \qquad \square$$

Corollary 2.45. *Let $\varphi : G \to H$ be a group homomorphism with $\ker\varphi = K$. Let S be a Schur ring over G such that $\overline{K} \in S$. Then $\varphi(S)$ is a Schur ring over a subgroup of H. Furthermore, if φ is surjective, then $\varphi(S)$ is a Schur ring over H.*

Proof. It is always the case that $\varphi(S)$ is a $*$-subalgebra of $F[H]$ for any Schur ring over G without further assumption. By Proposition 2.44, $\varphi(S)$ is closed under $\circ$. Thus, $\varphi(S)$ is a Schur ring over $\varphi(G)$ by Theorem 2.11. $\square$

Corollary 2.45 was originally proved by Leung and Ma [15] using a different proof.

As an example, if $G = H_1 \times H_2$, $\pi_1 : G \to H_1$ and $\pi_2 : G \to H_2$ are the canonical projections, and S_1 and S_2 are Schur rings over H_1 and H_2, respectively, then $\pi_i(S_1 \cdot S_2) = S_i$ for $i = 1, 2$.

As stated earlier in Example 2.19, for any lattice $\mathcal{L}$ of normal subgroups of a finite group G, $S(\mathcal{L})$ is a Schur ring over G spanned by the elements of $\mathcal{L}$. Let $N \trianglelefteq G$ and let $\varphi : G \to G/N$ be the quotient map. Suppose that $\mathcal{L}$ is a **distributive lattice**, that is,

$$A \cap (BC) = (A \cap B)(A \cap C) \quad \text{and} \quad A(B \cap C) = (AB) \cap (AC),$$

for all $A, B, C \in \mathcal{L}$. Then we claim that $\varphi(S(\mathcal{L}))$ is a Schur ring over G/N, even if $N \notin \mathcal{L}$. As in the proof of Corollary 2.45, it suffices to show that $\varphi(S(\mathcal{L}))$ is closed under $\circ$. If $K_1, K_2 \in \mathcal{L}$, then

$$\begin{aligned}\overline{K_1N} \circ \overline{K_2N} &= \overline{K_1N \cap K_2N} = \overline{(K_1 \cap K_2)N} = \frac{1}{|(K_1 \cap K_2) \cap N|}\overline{K_1 \cap K_2} \cdot \overline{N} \\ &= \frac{1}{|K_1 \cap K_2 \cap N|}(\overline{K_1} \circ \overline{K_2}) \cdot \overline{N},\end{aligned}$$

where the second equality holds by the distributivity of the lattice. Then

$$\begin{aligned}
\varphi(\overline{K_1}) \circ \varphi(\overline{K_2}) &= \frac{1}{|N|}\varphi((\overline{K_1} \cdot \overline{N}) \circ (\overline{K_2} \cdot \overline{N})), \quad \text{by Proposition 2.44,} \\
&= \frac{|K_1 \cap N||K_2 \cap N|}{|N|}\varphi(\overline{K_1 N} \circ \overline{K_2 N}) \\
&= \frac{|K_1 \cap N||K_2 \cap N|}{|N||K_1 \cap K_2 \cap N|}\varphi((\overline{K_1} \circ \overline{K_2}) \cdot \overline{N}) \\
&= |(K_1 \cap N)(K_2 \cap N)|\varphi(\overline{K_1} \circ \overline{K_2}) \in \varphi(S(\mathcal{L})).
\end{aligned}$$

Therefore, $\varphi(S(\mathcal{L}))$ is closed under $\circ$, which proves the claim. This fact is reported in the next proposition.

Proposition 2.46. *Let G be a finite group and let $\mathcal{L}$ be a distributive lattice of normal subgroups of G. Let $\varphi : G \to H$ be a group homomorphism. Then $\varphi(S(\mathcal{L}))$ is a lattice Schur ring over a subgroup of H.* □

Let G be a finite cyclic group. Then the lattice of subgroups of G is distributive, and hence any sublattice is also distributive. Thus, $\varphi(S(\mathcal{L}))$ is a Schur ring for any group homomorphism φ and any lattice $\mathcal{L}$ of subgroups of G. Theorem 2.68 will generalize this for any Schur ring over a cyclic group. On the other hand, the Cayley image of a Schur ring need not be a Schur ring. In fact, it is false even for Schur rings over abelian groups, as illustrated in the following example.

Example 2.47. Let $G = Z_2 \times Z_6 = \langle a, b \rangle$ and let

$$S = \mathrm{Span}_{\mathbb{Q}}\{1, b^3, b^2 + b^4, b + b^5, a + ab^3, ab + ab^2, ab^4 + ab^5\}.$$

Then S is an orbit Schur ring afforded by the subgroup generated by the automorphism $\sigma : a \mapsto ab^3, b \mapsto b^{-1}$. Let $\varphi : G \to Z_6$ be the projection homomorphism onto the subgroup $\langle b \rangle$, that is, $\pi : a \mapsto 1, b \mapsto b$. Then

$$\begin{aligned}
\varphi(S) &= \mathrm{Span}_{\mathbb{Q}}\{1, b^3, b^2 + b^4, b + b^5, 1 + b^3, b + b^2, b^4 + b^5\} \\
&= \mathrm{Span}_{\mathbb{Q}}\{1, b^3, b^2 + b^4, b + b^5, b + b^2\}.
\end{aligned}$$

If $\varphi(S)$ were a Schur ring, then $(b+b^5)\circ(b+b^2)=b\in\varphi(S)$. Since $b\in\varphi(S)$, this implies that $\varphi(S)=\mathbb{Q}[Z_6]$, which is six-dimensional. But $\dim\varphi(S)\leq 5$, which proves that $\varphi(S)$ is not a Schur ring. ∎

2.4 Pre-Schur Rings

This section deals with certain generalizations of Schur rings. According to Theorem 2.11, Schur rings are subalgebras of $F[G]$ which are closed under $\circ$ and $*$ and which contain $\overline{G}$ and 1. We will discuss two generalizations of Schur rings which are defined by removing the elements $\overline{G}$ and 1, respectively.

Definition 2.48. Let S be a subalgebra of $F[G]$ which is closed under $\circ$ and $*$ and $1\in S$. Then S is an **immersed Schur ring** over G. We say that S is a **properly immersed Schur ring** if $\overline{G}\notin S$.

Notice that many results about Schur rings, such as Theorem 2.11, or Corollary 2.45, have natural adaptations to immersed Schur rings.

Certainly, every Schur ring is immersed, but more general immersed Schur rings arise. For example, if $H\leq G$, then the group ring $F[H]$ is an immersed Schur ring in $F[G]$ as well as the trivial S-ring $F[H]^0$. In particular, every Schur ring over H is an immersed Schur ring over G. The next proposition shows that the converse is also true.

Proposition 2.49. *Let S be an immersed Schur ring over G. Then there exists a subgroup $H\leq G$ such that S is a Schur ring over H.*

Proof. By the proof of Theorem 2.11, we know that $(S,+,\circ)$ is a semisimple algebra with a basis of disjoint simple quantities. So, the sum of all these disjoint simple quantities is also a simple quantity corresponding to a subset of G. Call this subset H. Since $1\in S$, we have that $1\in H$. Also, since $H^*=H$, we have that H is closed under inverses. Lastly, let $g,h\in H$. Then there exists primitive sets $C,D\in\mathcal{D}(S)$ such that $g\in C$ and $h\in D$. So, $gh\in CD$. But the product CD is a union of primitive sets. Thus, $gh\in CD\subseteq H$. This proves that $H\leq G$. Since H is a union of the primitive sets of S, we conclude that $\mathcal{D}(S)$ is a partition of H and S is a Schur ring over H. □

Example 2.50. Using a similar argument as Proposition 2.25, we see that the intersection of two immersed Schur rings is also an immersed Schur ring. In particular, let S be a Schur ring over G and let $H \leq G$. Then $S \cap F[H]$ is an immersed Schur ring of G. In fact, it is the largest immersed Schur ring over H contained in S. If H is an S-subgroup, then $S \cap F[H]$ is a Schur ring over H. Let $\boldsymbol{S_H} = S \cap F[H]$. ∎

We now turn to the second generalization of Schur rings.

Definition 2.51. Let S be a subalgebra of $F[G]$ which is closed under $\circ$ and $*$ and $\overline{G} \in S$. Then S is a **pre-Schur ring** over G.

Many results about Schur rings, such as Theorem 2.11, or Corollary 2.45, have natural adaptations to pre-Schur rings.

Example 2.52. For any group G, the ideal $(\overline{G}) \subset F[G]$ is a pre-Schur ring. More generally, if $H \leq G$, then $\mathrm{Span}_F\{\overline{H}, \overline{G \setminus H}\} = \mathrm{Span}_F\{\overline{H}, \overline{G}\}$ is a pre-Schur ring. ∎

If S is a pre-Schur ring, then let the class containing 1 in $\mathcal{D}(S)$ be referred to as the **unit class**. For a Schur ring, the unit class is always the singleton containing the identity, that is, the unit class is always the trivial subgroup. For general pre-Schur rings a similar statement holds.

Proposition 2.53. *Let S be a pre-Schur ring over G and classes $\{C_1, C_2, \ldots, C_r\}$. Let C_1 be the unit class of S. Then $C_1 \leq G$.*

Proof. Certainly, $1 \in C_1$. Also, $C_1^* = C_j$ for some j. Since $1 \in C_1$ and $1^{-1} = 1$, $1 \in C_j$. But $C_1 \cap C_j = \emptyset$ if $j \neq 1$. Thus, $C_1^* = C_1$, which implies that if $g \in C_1$, then $g^{-1} \in C_1$.

Suppose $|C_1| = n$. Then $\overline{C_1}^2 = \sum_k \lambda_{1,1,k} \overline{C_k}$ and $\sum_k \lambda_{1,1,k} |C_k| = n^2$. For all $g \in C_1$, we have $g^{-1} \in C_1$ and thus $gg^{-1} = 1 \in C_1$. So, $\lambda_{1,1,1} \geq n$. But $n|C_1|$ accounts for n^2 many elements. Thus, $\overline{C_1}^2 = n\overline{C_1} = |C_1|\overline{C_1}$, and $C_1^2 = C_1$. Therefore, for all $g, h \in C_1$, we have that $gh \in C_1^2 = C_1$, which finishes the proof. □

Proposition 2.54. *Let S be a pre-Schur ring of $F[G]$, and let C_1 be the unit class of S. Then $\dfrac{1}{|C_1|}\overline{C_1}$ is the identity of S. Furthermore, $\overline{C_1} \cdot \overline{D} = \overline{D} \cdot \overline{C_1} = |C_1|\overline{D}$, for all $D \in \mathcal{D}(S)$.*

Proof. The last statement follows immediately from the fact that $\frac{1}{|C_1|}\overline{C_1}$ is the identity of the ring. By Theorem 2.9, S is semisimple and hence has an identity element, 1_S. In particular, $1_S \cdot \overline{C_1} = \overline{C_1}$. But C_1 is a subgroup of G. Thus, if there exists $g \in \mathrm{supp}(1_S) \setminus C_1$, then $gC_1 \not\subset C_1$, which contradicts 1_S being the identity of S. So, $\mathrm{supp}(1_S) \subseteq C_1$. Since C_1 is a primitive set, it must be that $\mathrm{supp}(1_S) = C_1$. Then $1_S = a\overline{C_1}$, for some $a \in F$. Since $\overline{C_1}^2 = |C_1|\overline{C_1}$, we may solve for a and get that $1_S = \frac{1}{|C_1|}\overline{C_1}$. □

Corollary 2.55. *Let $H \leq G$ and let S be a pre-Schur ring over G such that the unit class of S is H. Then all the primitive sets of S are unions of double cosets of H.*

Proof. Let D be a primitive set of S. By Proposition 2.54, $HDH = D$. On the other hand, $HDH = H\left(\bigcup_{g\in D} g\right)H = \bigcup_{g\in D} HgH$. □

Let S be a pre-Schur ring with unit class H. When $H \trianglelefteq G$, there is essentially only one possible construction for S.

Example 2.56 (Inflated S-rings)**.** Let $H \trianglelefteq G$ and let S be a Schur ring over G/H. Let $\pi : G \to G/H$ be the natural quotient map. Consider the partition of G given by

$$\mathcal{D} = \{\pi^{-1}(C) \mid C \in \mathcal{D}(S)\},$$

that is, if $C = \{g_1H, g_2H, \ldots, g_kH\} \in \mathcal{D}(S)$, then $\pi^{-1}(C) = \bigcup_{i=1}^{k} g_iH \in \mathcal{D}$. Let $\boldsymbol{\pi^{-1}(S)}$ be the subspace of $F[G]$ afforded by $\mathcal{D}$. We claim that $\pi^{-1}(S)$ is a pre-Schur ring over G. First,

$$(\pi^{-1}(C))^* = \left(\bigcup_{i=1}^{k} g_iH\right)^* = \bigcup_{i=1}^{k} g_i^{-1}H = \pi^{-1}(C^*).$$

So, $\pi^{-1}(S)$ is closed under $*$. Next, we note that

$$\pi\left(\overline{\pi^{-1}(C)}\right) = |H|\overline{C}.$$

Therefore, if in S we have

$$\overline{C_i} \cdot \overline{C_j} = \sum_k \lambda_{ijk}\overline{C_k},$$

then in $\pi^{-1}(S)$ we have

$$\overline{\pi^{-1}(C_i)} \cdot \overline{\pi^{-1}(C_j)} = \sum_k |H| \lambda_{ijk} \overline{\pi^{-1}(C_k)}.$$

Therefore, $\pi^{-1}(S)$ is a pre-Schur ring over G, referred to as the **inflated Schur ring** of S over G. Furthermore, the restriction $\pi : \pi^{-1}(S) \to S$ is an isomorphism of F-algebras. ∎

Theorem 2.57. *Let P be a pre-Schur ring over G with unit class H. If $H \trianglelefteq G$, then P is an inflated Schur ring.*

Proof. Let $\pi : G \to G/H$ be the quotient map. We have by Corollary 2.55 that all the primitive sets of P are unions of cosets of H. Then Corollary 2.45 applies, and we have that $\pi(P)$ is a pre-Schur ring over $\pi(G) = G/H$. Also, $\pi(H) = 1$, which implies that $\pi(P)$ is actually a Schur ring over G/H. Clearly, $\pi : P \to \pi(P)$ is surjective. It is also true that this restriction $\pi : P \to \pi(P)$ is injective, since $\ker \pi = H$. Therefore, $P \cong \pi(P)$, as F-algebras. In particular, if $S = \pi(P)$, then $P = \pi^{-1}(S)$. □

Example 2.58 (Wedge Products)**.** Let P be a pre-Schur ring over G. Then let S be the smallest subalgebra of $F[G]$ which contains P and 1. Then S is a Schur ring by Theorem 2.11 and $\dim S = \dim P + 1$. In particular, S is afforded by the same partition of P except the unit class C_1 has been split into two sets: $\{1\}$ and $C_1 \smallsetminus \{1\}$. Notice that $S_{C_1} = F[C_1]^0$, that is, the restricted Schur ring of S onto C_1 is the trivial Schur ring.

This method of constructing a Schur ring from a pre-Schur ring can easily be generalized. Let P be a pre-Schur ring over G with normal unit class H and let N be a Schur ring over H. Now, $\mathcal{D}(P)$ provides a partition of G which contains the primitive set H. Likewise, $\mathcal{D}(N)$ provides a partition of H which contains $\{1\}$. Let $\mathcal{D}$ be the partition of G taken from $\mathcal{D}(P)$ except H has been replaced by $\mathcal{D}(N)$, that is,

$$\mathcal{D} = (\mathcal{D}(P) \smallsetminus \{H\}) \cup \mathcal{D}(N).$$

Let S be the subspace of $F[G]$ afforded by $\mathcal{D}$. Clearly, S contains 1 and is closed under $*$, by construction. Also, since each primitive set outside of H is a union of cosets of H, it is

also clear that S is a subalgebra of $F[G]$. Therefore, S is a Schur ring. This construction is known as the **wedge product** of N and P and is denoted by $\boldsymbol{N \wedge P}$. ∎

Since every pre-Schur ring with normal unit class is an inflated Schur ring, we can construct the wedge product of two Schur rings.

Definition 2.59. Let $H \trianglelefteq G$, and let S and T be Schur rings over H and G/H, respectively. Let $P = \pi^{-1}(T)$ be the inflated Schur ring of T over G. Then

$$\boldsymbol{S \wedge T} = S \wedge P = S + \pi^{-1}(T)$$

and is called the **wedge product** of S and T.

We note that the wedge product operation on Schur rings is associative and has identity F, that is, $F \wedge S = S \wedge F = S$. On the other hand, the operation of taking wedge products is not necessarily commutative as illustrated in the next example.

Example 2.60. Let $G = Z_9$ and pick $H = Z_3$. So, $G/H \cong Z_3$. Then $F[Z_3]^0 \wedge F[Z_3]$ has a basis given by

$$F[Z_3]^0 \wedge F[Z_3] = \text{Span}\{1,\ z^3 + z^6,\ z + z^4 + z^7,\ z^2 + z^5 + z^8\}.$$

Conversely, $F[Z_3] \wedge F[Z_3]^0$ has a basis given by

$$F[Z_3] \wedge F[Z_3]^0 = \text{Span}\{1,\ z^3,\ z^6,\ z + z^2 + z^4 + z^5 + z^7 + z^8\}.$$

Therefore, the operation of taking wedge products of Schur rings is not necessarily commutative. On the other hand, it can be shown that $S \wedge T \cong T \wedge S$, as F-algebras. ∎

Let $H \trianglelefteq G$ and let $\pi : G \to G/H$ be the quotient map. Let S and T be Schur rings over H and G/H respectively. Then $(S \wedge T)_H = S$ and $\pi(S \wedge T) = T$. Thus, the wedge product provides a way of extending two Schur rings, that is, we may build a Schur ring over G with predetermined quotient and restriction. Leung and Man [17, 16] discovered a method to generalize this construction.

Definition 2.61. Let G be a finite group and let S be a Schur ring over G. Then we say that S is **wedge-decomposable** if there exists S-subgroups $1 < K \leq H < G$ such that $K \trianglelefteq G$ and for all $C \in \mathcal{D}(S)$, either $C \subseteq H$ or $C = \bigcup_{g \in X} gK$, for some subset $X \subseteq G \smallsetminus H$. If S is not wedge-decomposable, then S is **wedge-indecomposable**. For a wedge-decomposable Schur ring S, we say that $1 < K \leq H < G$ is a **wedge decomposition** of S over G.

For example, the Schur ring $S \wedge T$ is wedge-decomposable if S and T are both over non-trivial groups. In this case, $H = K$. In fact, a Schur ring with wedge-decomposition $1 < K \leq H < G$ is necessarily a wedge product of Schur rings if $H = K$.

Definition 2.62. Let $1 < K \leq H < G$ be a sequence of finite groups such that $K \trianglelefteq G$. Let S be a Schur ring over H and T a Schur ring over G/K. Let $\pi : G \to G/K$ be the quotient map. Also, assume that H/K is a T-subgroup, K is an S-subgroup, and $\pi(S) = T_{H/K}$. Let $\boldsymbol{S \triangle_K T} = S + \pi^{-1}(T)$ denote the **semi-wedge product** of S and T.

Proposition 2.63. *Let $1 < K \leq H < G$ be a sequence of finite groups with $K \trianglelefteq G$. Let S and T be Schur rings over H and G/K, respectively. Let $\pi : G \to G/K$ be the quotient map. Suppose that H/K is a T-subgroup, K is an S-subgroup, and $\pi(S) = T_{H/K}$. Then $S \triangle_K T$ is a Schur ring over G.*

Proof. Certainly, we have that $1, \overline{G} \in S \triangle_K T$ and $S \triangle_K T$ is closed under $*$ since S and $\pi^{-1}(T)$ are also closed. Next, since H/K is a T-subgroup, $T_{H/K}$ is a Schur ring over H/K. Let $\widehat{K} = \dfrac{1}{|K|}\overline{K}$. Then $\pi(\widehat{K}) = 1$, which implies that $\pi(S \cdot \widehat{K}) = \pi(S) = T_{H/K}$. Also, for all $\alpha \in F[G]$, $\alpha\widehat{K} = 0$ if and only if $\pi(\alpha) = 0$. This implies that the restriction $\pi : S \cdot \widehat{K} \to T_{H/K}$ is an isomorphism. Thus, $\pi^{-1}(T_{H/K}) = S \cdot \widehat{K} \subseteq S$, which implies that

$$\mathcal{D} = (\mathcal{D}(\pi^{-1}(T) \smallsetminus \mathcal{D}(\pi^{-1}(T_{H/K}))) \cup \mathcal{D}(S)$$

is a partition of G. In fact, $S \triangle_K T$ is the subspace afforded by $\mathcal{D}$. Lastly, we must show that $S \triangle_K T$ is a subring of $F[G]$. Certainly, S and $\pi^{-1}(T)$ are closed under multiplication. So it suffices to argue that the product of an element from S and $\pi^{-1}(T)$ is in $S \triangle_K T$. Let $\alpha \in S$ and $\beta \in \pi^{-1}(T)$. Since all the classes of $\mathcal{D}(\pi^{-1}(T))$ are unions of K-cosets, $\widehat{K}$ acts as

the identity on $\pi^{-1}(T)$. Therefore,

$$\alpha\beta = \alpha(\widehat{K}\beta) = (\alpha\widehat{K})\beta \in (S \cdot \widehat{K})\pi^{-1}(T) = \pi^{-1}(T_{H/K})\pi^{-1}(T) \subseteq \pi^{-1}(T).$$

A similar argument shows that $\beta\alpha = \beta\widehat{K}\alpha = \beta(\alpha\widehat{K}) \in \pi^{-1}(T)$, since $\widehat{K}$ is central in $F[G]$. Thus, $S \triangle_K T$ is a ring and $\pi^{-1}(T)$ is an ideal of $S \triangle_K T$. This proves that $S \triangle_K T$ is a Schur ring over G. □

It is important to observe that for a semi-wedge product $S \triangle_K T$, we have that $(S \triangle_K T)_H = S$ and $\pi(S \triangle_K T) = T$. Furthermore, every semi-wedge product naturally has a wedge-decomposition. The converse is also true.

Theorem 2.64. *Let S be a Schur ring over G with wedge-decomposition $1 < K \leq H < G$. Then S is a semi-wedge product of Schur rings over H and G/K.*

Proof. Let $N = \mathrm{Span}_F\{\overline{C} \mid C \in \mathcal{D}(S), C \subseteq H\}$. Since $N = S \cap F[H]$, N is an immersed Schur ring. Since H is an S-subgroup, N is a Schur ring over H. Next, let $\pi : G \to G/K$ be the quotient map and let $T = \pi(S)$. Since K is an S-subgroup, T is a Schur ring over G/K. Finally, we claim that $S = N \triangle_K T$. Note that $N \triangle_K T = N + \pi^{-1}(T) = N + \pi^{-1}(\pi(S))$. Since N contains all S-classes contained in H, we must argue that $\pi^{-1}(T)$ contains all the S-classes not contained in H. But each class has the form $C = \bigcup_{g \in X} gK$. So, $\pi(C) = \{gK \mid g \in X\}$ and $\pi^{-1}(\pi(C)) = \bigcup_{g \in X} gK = C$. Therefore, $\pi^{-1}(T)$ contains the remaining primitive sets, which implies that $S = N \triangle_K T$. □

Therefore, every semi-wedge product of Schur rings has a wedge-decomposition and every wedge-decomposable Schur ring can be constructed as a semi-wedge product of Schur rings.

Similar to Lemma 2.27, we see when a dot product of Schur rings is wedge-decomposable.

Proposition 2.65. *Let S and T be Schur rings over G and H, respectively. If S is wedge-decomposable, then $S \cdot T$ is wedge decomposable.*

Proof. Since S is wedge-decomposable, there exists a wedge-decomposition $1 < K \leq L < G$ of S. Let $N = S_L$. Naturally, $N \cdot T$ is a Schur ring over $L \times H$ and properly immersed in $S \cdot T$. Let $C \in \mathcal{D}(S) \setminus \mathcal{D}(N)$ and $D \in \mathcal{D}(T)$. Since C is a union of cosets of K, CD is likewise

a union of cosets of $K \times 1 \trianglelefteq G \times H$. Since all primitive sets outside of $N \cdot T$ have the form CD for $C \in \mathcal{D}(S) \setminus \mathcal{D}(N)$ and $D \in \mathcal{D}(T)$, we have that $S \cdot T$ has the wedge-decomposition $1 < K \times 1 \leq L \times H < G \times H$. □

Using only the constructions mentioned in this chapter, Leung and Man [17, 16] have provided a complete classification of Schur rings over cyclic groups.

Theorem 2.66 (Classification of Schur Rings over Finite Cyclic Groups)**.** *Let F be a field of characteristic zero and let G be a finite cyclic group. Let S be a Schur ring over G. Then one of the following holds:*

(a) S is trivial, that is, $S = F[G]^0$.

(b) S is an orbit Schur ring, that is, there exists a subgroup $\mathcal{H} \leq \mathrm{Aut}(G)$ such that $S = F[G]^{\mathcal{H}}$.

(c) S is a dot product of Schur rings, that is, there exist nontrivial subgroups $H, K \leq G$ such that $G = H \times K$ and there exists Schur rings S_H and S_K over H and K, respectively, such that $S = S_H \cdot S_K$.

(d) S is a semi-wedge product of Schur rings, that is, there exist nontrivial, proper subgroups $1 < K \leq H < G$ such that $K \trianglelefteq G$ and there exist Schur rings S_H and $S_{G/K}$ over H and G/K, respectively, such that $S = S_H \triangle_K S_{G/K}$.

Example 2.67. It turns out that lattice Schur rings provide another way to construct Schur rings beyond the three methods used in the Leung and Man classification theorem for non-cyclic groups. For example, let $G = Z_5 \times Z_5 = \langle a, b \rangle$, let $\mathcal{L} = \{1, \langle a \rangle, \langle b \rangle, \langle ab \rangle, G\}$, and let $S = S(\mathcal{L})$. Let $C = G \setminus (\langle a \rangle \cup \langle b \rangle \cup \langle ab \rangle)$, so that $|C| = 12$. Hence, C is one of the S-classes. Since $C \neq G \setminus 1$, S is not trivial. Likewise, S cannot be a dot product of Schur rings since C is not a product of two S-classes contained in proper subgroups of G. Also, S cannot be a wedge product since C is not a union of cosets for any nontrivial subgroup. If S is an orbit Schur ring, it is generated by automorphisms such that $\langle a \rangle$, $\langle b \rangle$, and $\langle ab \rangle$ are invariant subgroups. But there are only three automorphism subgroups with this property, which are all cyclic and are generated by the identity map, by the inversion map, and by the

squaring map. The partitions of G corresponding to these automorphism groups are distinct from S, which implies that S is not an orbit Schur ring. This example then shows that the Leung-Man classification theorem for cyclic groups cannot be extended to arbitrary abelian groups.

A consequence of this classification theorem is the following theorem.

Theorem 2.68. *Let G be a finite cyclic group and S be a Schur ring over G. If $\varphi : G \to L$ is a group homomorphism, then $\varphi(S)$ is a Schur ring over a subgroup of L.*

Proof. Let S be a Schur ring over $G = Z_n$. We proceed by induction on $|G|$. If $|G| = p$, a prime, then the only normal subgroups are 1 and G, which are necessarily S-subgroups. Thus, the property holds for $|G| = p$, by Corollary 2.45.

Suppose now the property holds for all proper divisors of the integer n and let S be a Schur ring over $G = Z_n$. By Theorem 2.66, S is a trivial, orbit, dot product, or semi-wedge product Schur ring. If S is trivial, then it is a lattice Schur ring. So, $\varphi(S)$ is a Schur ring by Proposition 2.46.

If S is an orbit Schur ring, then every subgroup of G is an S-subgroup since every subgroup is characteristic. Thus, $\varphi(S)$ is a Schur ring by Corollary 2.45.

If $S = R \cdot T$ for Schur rings R and T over subgroups H and K, respectively, such that $G = H \times K$, then $\varphi(S) = \varphi(R \cdot T) = \varphi(R) \cdot \varphi(T)$. Since $\varphi(R)$ and $\varphi(T)$ are Schur rings by induction, $\varphi(S)$ is the dot product of Schur rings and hence a Schur ring itself.

Lastly, let $S = R \triangle_K T$ for Schur rings R and T over subgroup H and quotient group G/K, respectively. Let $\pi : G \to G/K$ be the quotient map. Then $S = R \triangle_K T = R + \pi^{-1}(T)$. Without the loss of generality, we may assume that φ is the quotient map $\varphi : G \to G/N$. We likewise define $\pi^* : G/N \to G/KN$ and $\varphi^* : G/K \to G/KN$ to be quotient maps. Then $\varphi(\pi^{-1}(T)) = (\pi^*)^{-1}(\varphi^*(T))$. By induction, $\varphi(R)$ and $\varphi^*(T)$ are Schur rings. Therefore, $\varphi(S) = \varphi(R \triangle_K T) = \varphi(R) + \varphi(\pi^{-1}(T)) = \varphi(R) + (\pi^*)^{-1}(\varphi^*(T)) = \varphi(R) \triangle_{\varphi(K)} \varphi^*(T)$, which is a Schur ring. This then proves the result for arbitrary n. ∎

Chapter 3. Primitive Idempotents of Schur Rings over Cyclic Groups

In representation theory, central idempotents have been a useful tool in the decomposition of associative algebras. In group algebras, for each lattice of normal subgroups of a finite group, there corresponds a family of central idempotents. These lattices of normal subgroups naturally give rise to Schur rings, that is, lattice Schur rings. Furthermore, these systems of idempotents can often capture the primitive idempotents of related Schur rings. This chapter will study the central idempotents of group algebras and of Schur rings. In the case of cyclic groups, it will be shown that the set of central, primitive idempotents of a Schur ring corresponds to the lattice of S-subgroups.

As this chapter deals extensively with properties of idempotents and semisimple rings, the author will remind the reader about some of the important, elementary properties of these objects.

An element ε of a ring R is **idempotent** if $\varepsilon^2 = \varepsilon$ and is **central** in R if $\varepsilon \in Z(R)$. In a semisimple ring such as $\mathbb{Q}[G]$, all two-sided ideals are generated by a central idempotent. We say that a central idempotent is **primitive** if it cannot be expressed as a sum of two nonzero orthogonal central idempotents. A semisimple ring may be expressed as a direct sum of indecomposable two-sided ideals, called a **Wedderburn decomposition**, each of which is principal and generated by a primitive central idempotent. In this situation products of distinct indecomposable ideals are trivial, and hence the primitive central idempotents are pairwise orthogonal. Each central idempotent is a sum of primitive central idempotents. Thus, the primitive central idempotents are the atomic building blocks associated to the ideal structure of $\mathbb{Q}[G]$.

If the sum of a set of orthogonal idempotents is 1, we say that the set of idempotents is **complete**. In particular, the set of all primitive central idempotents is always complete in a semisimple ring. Furthermore, every central idempotent of a semisimple ring is a sum of primitive central idempotents, and the primitive central idempotents **involved** in this sum are precisely the ones whose product with the idempotent is nonzero.

A detailed treatment of semisimple rings can be found in Appendix A.

In the case of complex group algebras, it is well known that the central primitive idempotents can be computed using the irreducible characters of the group. Averaging the Galois conjugates of each primitive central idempotent in $\mathbb{C}[G]$, the idempotents of the group algebra $F[G]$ can be computed for any subfield $F \subseteq \mathbb{C}$. In particular, the primitive central idempotents of $\mathbb{Q}[G]$ can be computed in this way. Although this is possible using the characters, it is often computationally laborious to compute the central idempotents of $\mathbb{Q}[G]$ by this method. Instead, character-free methods have been developed to compute these idempotents using the subgroups of G.

Character-free formulas for the primitive central idempotents of a finite abelian group algebra with rational coefficients are outlined in Chapter VII of [7], which we reproduce below in Corollary 3.19. These formulas were later simplified and extended by Jespers, Leal, and Paques [8] to finite nilpotent groups and by Olivieri, del Río, and Simón [26] to finite abelian-by-supersolvable groups. Other recent papers on the primitive central idempotents of $\mathbb{Q}[G]$ include Olivieri and del Río [25], Broche and del Río [2], Ferraz and Polcino Milies [5], Van Gelder and Olteanu [33], Jespers, Olteanu, and del Río [9], and Jespers, Olteanu, and Van Gelder [10].

Section 3.1 discusses the topic of semilattices and algebras induced from semilattices. Given any semilattice, a complete set of orthogonal primitive idempotents is constructed for a related algebra, called the semilattice algebra. This process of constructing systems of idempotents will be a template for idempotent constructions in subsequent sections.

In Section 3.2 lattices of normal subgroups of finite groups will be used to construct complete systems of orthogonal central idempotents in the group algebra. For abelian groups, a criterion for when these idempotents are primitive is presented. Similarly, in Section 3.3, lattices of normal S-subgroups are used to build complete systems of orthogonal idempotents in Schur rings. They are shown to be primitive idempotents when the group is cyclic.

3.1 Primitive Idempotents of Semilattice Algebras

Throughout this section only, let F be a field of arbitrary characteristic.

Definition 3.1. Let T be a set and let $\cdot : T \times T \to T$ be a binary operation. Then $(T, \cdot)$ is called a **semilattice** if it satisfies the following axioms:

(a) (Associativity Axiom) : For all $r, s, t \in T$, $r \cdot (s \cdot t) = (r \cdot s) \cdot t$,

(b) (Commutativity Axiom) : For all $s, t \in T$, $s \cdot t = t \cdot s$,

(c) (Idempotency Axiom) : For all $t \in T$, $t \cdot t = t$

(d) (Identity Axiom) : There exists an element $1 \in T$, such that for all $t \in T$, $1 \cdot t = t \cdot 1 = t$.

In particular, a semilattice is a commutative monoid for which every element is idempotent.

Let T be a semilattice and let $s, t \in T$. We say $s \leq t$ if $s \cdot t = t$. In particular, $1 \leq t$ for all $t \in T$. Now we show that $\leq$ is a partial ordering on T. If $t \in T$, then $t \cdot t = t$, which implies that $t \leq t$. If $s \leq t$ and $t \leq s$, then $s \cdot t = t$ and $t \cdot s = s$. But $s = t \cdot s = s \cdot t = t$. Lastly, if $r \leq s$ and $s \leq t$, then $r \cdot s = s$ and $s \cdot t = t$. Thus, $r \cdot t = r \cdot (s \cdot t) = (r \cdot s) \cdot t = s \cdot t = t$, that is, $r \leq t$. So, as claimed, $\leq$ is a partial ordering on T.

Lemma 3.2. *Let T be a semilattice and let $r, s \in T$. If $s \cdot t = r$ for some $t \in T$, then $s \leq r$. In particular, if $s \cdot t = 1$, then $s = t = 1$.*

Proof. Suppose $s \cdot t = r$. Then $s \cdot r = s \cdot (s \cdot t) = (s \cdot s) \cdot t = s \cdot t = r$. Thus, $s \leq r$, which proves the first statement. If $s \cdot t = 1$, then $s \leq 1$. But $1 \leq s$, which proves the second statement. □

In particular, the identity of a semilattice T is the unique minimal element of T. If T is finite, then T contains a unique maximal element $\prod_{s \in T} s$.

Definition 3.3. Let T be a semilattice and let $s \in T$. Then let

$$\lceil \boldsymbol{s} \rceil = \{t \in T \mid s \leq t\}$$

be the **principal up-set generated by** s. It is routine to check that $\lceil s \rceil$ is itself a semilattice with identity s.

Definition 3.4. Let T be a semilattice. For $s, t \in T$, we say that t **covers** s if $s \leq t$ and for all $r \in T$ such that $s \leq r \leq t$, either $r = s$ or $r = t$. Let $\boldsymbol{\mathcal{M}(T, s)}$ denote the set of all covers of s in T.

For a finite semilattice, $\mathcal{M}(T, s)$ is nonempty for all $s \in T$ except the maximal element of T.

Definition 3.5. Let F be a field and let T be a monoid. Then $F[T]$ denotes the monoid algebra of T with F-coefficients. If T is also a semilattice, then $F[T]$ is a **semilattice algebra**.

In a semilattice algebra, we will denote the operation of a semilattice by juxtaposition.

Let T be a finite semilattice and F a field. Since T is commutative, the semilattice algebra $F[T]$ is a commutative ring. Hence, all idempotents are central. Now, each semilattice algebra has a basis of central idempotents, the elements of T. We will *orthogonalize* this basis to construct the primitive idempotents. But first, we show that each semilattice algebra is semisimple.

Theorem 3.6. *Let T be a finite semilattice and let F be a field. Then $F[T]$ is a semisimple algebra.*

Proof. Since T is finite, $F[T]$ is a finite dimensional algebra, which implies that $F[T]$ is artinian . Since $\mathcal{J}(F[T])$ is a nilpotent ideal, $\mathcal{J}(F[T]) = 0$ if $F[T]$ contains no nonzero nilpotent elements. To this end, let $\alpha = \sum_{t \in T} \alpha_t t \in F[T]$ such that $\alpha^n = 0$. First, consider the coefficient of 1 in α^n. By Lemma 3.2, the only possible product in α^n which produces 1 is 1^n. So, the coefficient of 1 in α^n is α_1^n. Since $\alpha^n = 0$, it must be that $\alpha_1^n = 0$, which implies that $\alpha_1 = 0$.

Next, let $s \in T$ be a cover of 1 and we consider the coefficient of s in α^n. By Lemma 3.2, in the expansion of α^n the only products which produce s must have factors less than or equal to s. Hence, each factor is 1 or s, which implies that the coefficient of s in α^n is $\sum_{i=1}^{n} \binom{n}{i} \alpha_1^{n-i} \alpha_s^i$. But $\alpha_1 = 0$. So, $\sum_{i=1}^{n} \binom{n}{i} \alpha_1^{n-i} \alpha_s^i = \alpha_s^n = 0$, since $\alpha^n = 0$. As above, this implies that $\alpha_s = 0$. Generalizing this argument, if $t \in T$ and $\alpha_s = 0$ for all $s < t$, then $\alpha_t = 0$. Thus, by induction, $\alpha_t = 0$ for all $t \in T$, so that $\alpha = 0$. Therefore, $F[T]$ is semisimple, by Theorem A.12. □

Definition 3.7. For a finite semilattice T and $s \in T$, let

$$\boldsymbol{\varepsilon(T, s)} = \prod_{m \in \mathcal{M}(T,s)} (s - m) \in F[T].$$

If $\mathcal{M}(T, s) = \emptyset$, let $\varepsilon(T, s) = s$.

Lemma 3.8. *Let T be a finite semilattice with $s, t \in T$. Then*

$$t\varepsilon(T, s) = \begin{cases} \varepsilon(T, s), & t \leq s \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. Suppose that $t \leq s$. For any $m \in \mathcal{M}(T, s)$, $t \leq s < m$. (If $\mathcal{M}(T, s) = \emptyset$, let $m = 0$). Thus, $ts = s$ and $tm = m$, which implies that $t(s - m) = (s - m)$. So, $t\varepsilon(T, s) = \varepsilon(T, s)$.

Suppose $s < t$. Then there exists some cover m of s in T such that $s < m \leq t$. Hence $t(s - m) = ts - tm = t - t = 0$. This implies that $t\varepsilon(T, s) = 0$.

Lastly, suppose that $t \not\leq s$. Then $t\varepsilon(T, s) = t(s\varepsilon(T, s)) = (ts)\varepsilon(T, s) = 0$, where the first equality follows by the first case and the third equality follows by the second case, since $t \not\leq s$ if and only if $ts \neq t$. □

Proposition 3.9. *Let T be a finite semilattice and $s, t \in T$. Then $\varepsilon(T, s)^2 = \varepsilon(T, s)$ and $\varepsilon(T, s)\varepsilon(T, t) = 0$ if $s \neq t$.*

Proof. First, $s\varepsilon(T, s) = \varepsilon(T, s)$ and $m\varepsilon(T, s) = 0$, for all $m \in \mathcal{M}(T, s)$, by Lemma 3.8. Thus, $(s - m)\varepsilon(T, s) = \varepsilon(T, s)$, which implies that $\varepsilon(T, s)^2 = \varepsilon(T, s)$.

Suppose next that $s \neq t$. Then either $t < s$ or $t \not\leq s$. If $t < s$, then $s \not\leq t$. So we may assume without loss that $t \not\leq s$. Then $m \not\leq s$ for all $m \in \mathcal{M}(T, t)$. Thus, $\varepsilon(T, s)(t - m) = 0 - 0 = 0$, which implies that $\varepsilon(T, s)\varepsilon(T, t) = 0$. □

In particular, $\{\varepsilon(T, s) \mid s \in T\}$ is a set of orthogonal idempotents in $F[T]$. Clearly, $\mathrm{Span}_F\{\varepsilon(T, s) \mid s \in T\} \subseteq \mathrm{Span}_F\{s \mid s \in T\} = F[T]$. In fact, we have equality.

Theorem 3.10. *Let T be a finite semilattice and F a field. Then* $\mathrm{Span}_F\{\varepsilon(T, s) \mid s \in T\} = F[T]$.

Proof. The proof will follow by induction on $|T|$. When $|T| = 1$, we have that $T = \{1\}$ and $\varepsilon(T, 1) = 1$. Suppose the statement holds for any semilattice with order less than $|T|$. Let $V = \mathrm{Span}_F\{\varepsilon(T, s) \mid s \in T\}$ and let $s \in T$. If $s \neq 1$, then $S = \lceil s \rceil$ is a semilattice of strictly smaller order than T and $\mathrm{Span}_F\{\varepsilon(S, t) \mid t \in S\} = F[S]$. By Lemma 3.2, the elements of T with nonzero coefficients in $\varepsilon(T, s)$ are contained in S. Thus, $\varepsilon(T, t) = \varepsilon(S, t)$ for all $t \in S$. Therefore, $\mathrm{Span}_F\{\varepsilon(T, t) \mid s \leq t\} = \mathrm{Span}_F\{t \in T \mid s \leq t\}$, by induction. In particular, $s \in \mathrm{Span}_F\{\varepsilon(T, t) \mid t \in T\}$ for all $s \neq 1$. Again by Lemma 3.2, $\varepsilon(T, 1) = 1 + \alpha$, where $\alpha \in \mathrm{Span}_F\{s \in T \mid s \neq 1\}$. Since $\varepsilon(T, 1)$, $\alpha \in \mathrm{Span}_F\{\varepsilon(T, s) \mid s \in T\}$, we conclude that $1 \in \mathrm{Span}_F\{\varepsilon(T, s) \mid s \in T\}$. Therefore, $\mathrm{Span}_F\{\varepsilon(T, s) \mid s \in T\} = F[T]$. □

Corollary 3.11. *Let T be a finite semilattice and F a field. Then $\varepsilon(T, s) \neq 0$ and $\varepsilon(T, s)$ is a primitive central idempotent of $F[T]$ for each $s \in T$.*

Proof. Let $|T| = n$. Then $\dim_F F[T] = n$. If $\varepsilon(T, s) = 0$ for some $s \in T$, then $\mathrm{Span}_F\{\varepsilon(T, t) \mid t \in T, t \neq s\} = \mathrm{Span}_F\{\varepsilon(T, t) \mid t \in T\} = F[T]$, by Theorem 3.10. But

$$\dim F[T] \leq |\{\varepsilon(T, t) \mid t \in T, t \neq s\}| \leq n - 1 < n = \dim F[T],$$

a contradiction. Therefore, each idempotent of the form $\varepsilon(T, s)$ is nonzero.

Next, consider the ideal $(\varepsilon(T, s)) \leq F[T]$. We have that $\sum_{s \in T}(\varepsilon(T, s)) = F[T]$ and $(\varepsilon(T, s)) \cap (\varepsilon(T, t)) = 0$ when $s \neq t$, by Proposition 3.9. Thus,

$$F[T] = \bigoplus_{s \in T}(\varepsilon(T, s)).$$

Since no ideal in this sum is zero, by degree considerations, $\dim(\varepsilon(T, s)) = 1$ for all $s \in T$. Thus, $\varepsilon(T, s)$ is necessarily primitive. □

Corollary 3.12. *Let T be a finite semilattice and F a field. Then, for $s \in T$, we have*

$$\sum_{s \leq t} \varepsilon(T, t) = s.$$

Proof. If $s \in T$, then s is the identity element of $\lceil s \rceil$. Thus, it suffices to prove the claim for

$s = 1$. As in the previous proof,

$$F[T] = \bigoplus_{s \in T} (\varepsilon(T, s)).$$

Thus, $\sum_{t \in T} \varepsilon(T, t)$ is the identity element of $F[T]$. □

In particular, we have shown that for any finite semilattice, the collection $\{\varepsilon(T, s) \mid s \in T\}$ is a complete set of primitive central idempotents for $F[T]$, where F is *any* field.

Let T be a finite semilattice and let S be a subsemilattice of T, not necessarily with the same identity. Then $\varepsilon(S, s)$ is a central idempotent of $F[T]$ for all $s \in S$, and $\varepsilon(S, s)$ can be expressed as a sum of the form $\sum \varepsilon(T, t)$. Let $s \in S$, let $m \in \mathcal{M}(S, s)$, and let $t \in T$. If $s \leq t$ and $m \not\leq t$, then

$$\varepsilon(T, t)(s - m) = \varepsilon(T, t) - 0 = \varepsilon(T, t).$$

If $s \leq t$ and $m \leq t$, then

$$\varepsilon(T, t)(s - m) = \varepsilon(T, t) - \varepsilon(T, t) = 0.$$

And lastly, if $s \not\leq t$, then $m \not\leq t$ and

$$\varepsilon(T, t)(s - m) = 0 - 0 = 0.$$

Therefore, $\varepsilon(T, t)$ is involved in the decomposition of $\varepsilon(S, s)$ if and only if $s \leq t$ and $m \not\leq t$ for all $m \in \mathcal{M}(S, s)$. We have proven the following result.

Theorem 3.13. *Let T be a finite semilattice, S a subsemilattice of T, and $s \in S$. Then*

$$\varepsilon(S, s) = \sum_{t} \varepsilon(T, t)$$

where the sum ranges over all $t \in T$ such that $s \leq t$ and $m \not\leq t$ for all $m \in \mathcal{M}(S, s)$. □

Applications of semilattice algebras will be found in the following sections.

3.2 Primitive Idempotents of Group Algebras

Let G be a finite group and $H \leq G$. Then for all $h \in H$, $h\overline{H} = \overline{H}h = \overline{H}$. Let

$$\widehat{\boldsymbol{H}} = \frac{1}{|H|}\overline{H} \in F[G].$$

Then $\widehat{H}$ is an idempotent in $F[G]$. If $H \trianglelefteq G$, then $\widehat{H}$ is a central idempotent. Note, $(\widehat{G})$ is a one-dimensional ideal in $F[G]$, which implies that $\widehat{G}$ is always primitive in $F[G]$. On the other hand, if $H \lneq G$, then $\widehat{H}$ is not primitive in $F[G]$ since $\widehat{H} = \widehat{G} + (\widehat{H} - \widehat{G})$.

Given any subgroups H and K of G, we have

$$\widehat{H}\widehat{K} = \frac{1}{|H||K|}\overline{H} \cdot \overline{K} = \frac{|H \cap K|}{|H||K|}\overline{HK} = \widehat{HK}.$$

If H is normal, then $HK \leq G$ and $\widehat{HK}$ is an idempotent of $F[G]$. If $H, K \trianglelefteq G$, then HK is also normal in G. So, $\widehat{HK}$ is central in $F[G]$, and the collection of all normal subgroups of G forms a semilattice.

Let G be a finite group and let $\mathcal{L}$ be a subsemilattice of the semilattice of all normal subgroups of G, which we will simply refer to as a semilattice of normal subgroups of G. Since $\mathcal{L}$ must be finite, it contains a maximum element, $\prod_{H \in \mathcal{L}} H$. By shrinking the ambient group G if necessary, we may assume that the maximum element of $\mathcal{L}$ is G. Likewise, $\mathcal{L}$ contains a minimum element, $1_{\mathcal{L}} = K$. By correspondence, the natural quotient map $\pi : G \to G/K$ maps $\mathcal{L}$ onto an isomorphic semilattice $\pi(\mathcal{L})$ of normal subgroups of G/K. In particular, $\pi(K) = 1$. Thus we may assume the minimum element of $\mathcal{L}$ is 1.

Let $H \in \mathcal{L}$ and let $\boldsymbol{\mathcal{M}_{\mathcal{L}}(G, H)} = \mathcal{M}(\mathcal{L}, H)$, the set of all covers of H in the semilattice $\mathcal{L}$. When $\mathcal{L}$ is the whole semilattice of normal subgroups of G, write $\mathcal{M}(G, H) = \mathcal{M}_{\mathcal{L}}(G, H)$.

For every semilattice of normal subgroups of G, there is an associated system of idempotents in $F[G]$ as follows: let

$$\boldsymbol{\varepsilon_{\mathcal{L}}(G, H)} = \prod_{M \in \mathcal{M}_{\mathcal{L}(G,H)}} (\widehat{H} - \widehat{M}) \in F[G].$$

Since each subgroup M is normal, $\widehat{M}$ is central in $F[G]$ and hence the order of the product

is irrelevant and $\varepsilon_{\mathcal{L}}(G,H)$ is central in $F[G]$. When $\mathcal{L}$ is the whole semilattice of normal subgroups, we let $\varepsilon(G,H) = \varepsilon_{\mathcal{L}}(G,H)$. This agrees with the idempotents introduced in [8].

We can naturally extend Example 2.19 to allow $\mathcal{L}$ to be any semilattice of normal subgroups. Then $S(\mathcal{L})$ is a subalgebra of $F[G]$ and is a Schur ring if and only if $\mathcal{L}$ is a lattice. There is a natural algebra homomorphism $\Psi : F[\mathcal{L}] \to S(\mathcal{L})$ from the semilattice algebra generated by $\mathcal{L}$ onto $S(\mathcal{L})$. In particular, $\Psi(H) = \widehat{H}$. Thus, $S(\mathcal{L})$ is the homomorphic image of a semilattice algebra. We utilize this fact below.

Lemma 3.14. *Let $\mathcal{L}$ be a semilattice of normal subgroups of G with $H, K \in \mathcal{L}$. Then*

$$\widehat{K}\varepsilon_{\mathcal{L}}(G,H) = \begin{cases} \varepsilon_{\mathcal{L}}(G,H), & K \leq H \\ 0, & \textit{otherwise.} \end{cases}$$

Proof. For each $H \in \mathcal{L}$, the homomorphism Ψ maps H onto $\widehat{H} \in F[G]$. Likewise, $\varepsilon(\mathcal{L},H) \in F[\mathcal{L}]$ maps onto $\varepsilon_{\mathcal{L}}(G,H) \in S(\mathcal{L})$. The results then follow from Lemma 3.8. □

Proposition 3.15. *Let $\mathcal{L}$ be a semilattice of normal subgroups of G and let $H, K \in \mathcal{L}$. Then $\varepsilon_{\mathcal{L}}(G,H)^2 = \varepsilon_{\mathcal{L}}(G,H)$ and $\varepsilon_{\mathcal{L}}(G,H)\varepsilon_{\mathcal{L}}(G,K) = 0$ if $H \neq K$. Furthermore,*

$$1 = \sum_{H \in \mathcal{L}} \varepsilon_{\mathcal{L}}(G,H).$$

Proof. The result follows from Proposition 3.9 and Corollary 3.12. □

In particular, $\{\varepsilon_{\mathcal{L}}(G,H) \mid H \in \mathcal{L}\}$ is a complete set of orthogonal idempotents in $F[G]$. We note however that $\varepsilon_{\mathcal{L}}(G,H)$ is not necessarily primitive. In fact, $\varepsilon_{\mathcal{L}}(G,H)$ may be zero. For example, let $G = Z_2 \times Z_2 = \langle a, b \rangle$, let $F = \mathbb{Q}$, and let $\mathcal{L}$ be the complete lattice of subgroups of G. Then $\varepsilon_{\mathcal{L}}(G,1) = \frac{1}{8}(1-a)(1-b)(1-ab) = 0$.

On the other hand, when G is cyclic, $\varepsilon_{\mathcal{L}}(G,H) \neq 0$ for all $H \in \mathcal{L}$, as we now show.

Lemma 3.16. *Let G be a finite cyclic group and let $\mathcal{L}$ be a semilattice of subgroups of G. Then $\varepsilon_{\mathcal{L}}(G,H) \neq 0$ for all $H \in \mathcal{L}$.*

Proof. For a cyclic group G, $S(\mathcal{L})$ has for a basis the set $\{\overline{H} \mid H \in \mathcal{L}\}$. This can be seen by examining the generators of each subgroup in $\mathcal{L}$. Thus, $\dim_F S(\mathcal{L}) = |\mathcal{L}|$. Therefore,

the map $\Psi : F[\mathcal{L}] \to S(\mathcal{L})$ is an isomorphism. Thus, $\varepsilon_{\mathcal{L}}(G,H) = \Psi(\varepsilon(\mathcal{L},H)) \neq 0$, since $\varepsilon(\mathcal{L},H) \neq 0$. □

Lemma 3.17. *Let G be an abelian group and let $\mathcal{L}$ be a semilattice of subgroups of G. For all $H \in \mathcal{L}$ such that G/H is cyclic, then $\varepsilon_{\mathcal{L}}(G,H) \neq 0$.*

Proof. Let $\pi : G \to G/H$ be the natural quotient map and let $\pi(\mathcal{L}) = \{\pi(K) \mid K \in \mathcal{L}\}$ denote the quotient semilattice. In fact, $\lceil H \rceil = \{HK \mid K \in \mathcal{L}\}$, and, by the Correspondence Theorem, $\lceil H \rceil \cong \pi(\mathcal{L})$ as semilattices.

Next, let $K \in \mathcal{L}$ such that $H \leq K$. Then

$$\pi(\widehat{K}) = \frac{1}{|K|}\sum_{g\in K} gH = \frac{|H|}{|K|}\sum_{gH\in K/H} gH = \widehat{K/H},$$

and

$$\pi(\varepsilon_{\mathcal{L}}(G,H)) = \pi(\varepsilon_{\lceil H\rceil}(G,H)) = \varepsilon_{\pi(\mathcal{L})}(G/H, H/H) \neq 0,$$

by Lemma 3.16. Thus, $\varepsilon_{\mathcal{L}}(G,H) \not\subseteq \ker\pi$, which implies that $\varepsilon_{\mathcal{L}}(G,H) \neq 0$. □

Let ζ_d denote a primitive dth root of unity in $\mathbb{C}$.

Theorem 3.18 (Perlis-Walker [27])**.** *Let G be a finite abelian group of order n. Then*

$$\mathbb{Q}[G] \cong \bigoplus_{d|n} a_d\mathbb{Q}(\zeta_d),$$

where a_d is the number of cyclic subgroups (or cyclic quotients) of G of order d. In particular, if $G = Z_n$ is a cyclic group of order n, then

$$\mathbb{Q}[Z_n] \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d).$$

Proof. A complete proof of this result may be found in [28] on page 147. □

Corollary 3.19 (Jespers-Leal-Paques [8])**.** *The set $\{\varepsilon(G,H) \mid H \leq G, G/H$ is cyclic$\}$ is a complete set of primitive central idempotents in $\mathbb{Q}[G]$ when G is abelian.*

Proof. Let $\mathcal{S} = \{\varepsilon(G,H) \mid H \leq G,\ G/H \text{ is cyclic}\}$. By Lemma 3.17, each element in $\mathcal{S}$ is nonzero and they are pairwise orthogonal idempotents by Proposition 3.15. Let a denote the number of cyclic quotients of G. Then $\mathcal{S}$ contains a distinct idempotents. By Theorem 3.18, $\mathbb{Q}[G]$ has exactly a primitive idempotents, and since $\mathbb{Q}[G]$ is semisimple, the only set of pairwise orthogonal, nonzero, central idempotents in $\mathbb{Q}[G]$ of size a is the complete set of primitive central idempotents. Therefore, $\mathcal{S}$ is this set. □

Corollary 3.20. *The set $\{\varepsilon(G,H) \mid H \leq G\}$ is a complete set of primitive central idempotents in $\mathbb{Q}[G]$ when G is cyclic.* □

Corollary 3.21. *Let $\varepsilon \in \mathbb{Q}[G]$ be an idempotent, with G abelian. Then*

$$\varepsilon \in \mathrm{Span}_{\mathbb{Q}}\{\overline{H} \mid H \leq G\}.$$ □

Let G be an abelian group. Suppose that $H \leq G$ but G/H is not cyclic. By Corollary 3.19, $\varepsilon(G,H)$ is not a primitive idempotent, but $\varepsilon(G,H)\varepsilon(G,K) = 0$ for all G/K cyclic by Proposition 3.15. Thus, $\varepsilon(G,H) = 0$. Hence, if G is abelian, $\varepsilon(G,H) \neq 0$ if and only if $\varepsilon(G,H)$ is primitive, if and only if G/H is cyclic.

On the other hand, let $G = Z_2 \times Z_2 = \langle a, b\rangle$ and let $\mathcal{L} = \{1, \langle a\rangle, G\}$. Although $G/1$ is not cyclic, $\varepsilon_{\mathcal{L}}(G,1) = 1 - \widehat{\langle a\rangle} = \frac{1}{2}(1-a) \neq 0$. Thus, for general semilattices of abelian groups, nonzero idempotents do not necessarily correspond to cyclic quotients. Of course, $\varepsilon_{\mathcal{L}}(G,1)$ is imprimitive in $F[G]$ since $\varepsilon_{\mathcal{L}}(G,1) = \varepsilon(G,\langle b\rangle) + \varepsilon(G,\langle ab\rangle)$.

When G is a cyclic group of prime power order, the primitive idempotents of $\mathbb{Q}[G]$ can be greatly simplified.

Corollary 3.22. *Let $G = Z_{p^n}$, for a prime p. For each $0 \leq k \leq n$, let Z_{p^k} denote the unique subgroup of G of order p^k. Then the primitive idempotents of $\mathbb{Q}[G]$ are of the form $\widehat{G}$ or $\widehat{Z_{p^k}} - \widehat{Z_{p^{k+1}}}$, for $0 \leq k < n$.* □

A direct consequence of Theorem 3.13 is the following.

Theorem 3.23. *For any semilattice $\mathcal{L}$ of subgroups of an abelian group G and any $H \in \mathcal{L}$,*

$$\varepsilon_{\mathcal{L}}(G,H) = \sum_{K} \varepsilon(G,K)$$

where the sum ranges over all subgroups K of G such that $H \leq K$ and $M \not\leq K$ for all $M \in \mathcal{M}_{\mathcal{L}}(G,H)$. Removing zero idempotents if necessary, this gives a decomposition of $\varepsilon_{\mathcal{L}}(G,H)$ into primitive idempotents in $\mathbb{Q}[G]$.

Let $\mathcal{L}$ be a semilattice of normal subgroups of a finite group G. For any $H \in \mathcal{L}$, set

$$\boldsymbol{\mathcal{N}_{\mathcal{L}}(G,H)} = \{K \trianglelefteq G \mid H \leq K \text{ and } M \not\leq K, \text{ for all } M \in \mathcal{M}_{\mathcal{L}}(G,H)\}.$$

So, $\mathcal{N}_{\mathcal{L}}(G,H)$ is the set of all normal subgroups between H and an $\mathcal{L}$-cover of H. If G is abelian,

$$\varepsilon_{\mathcal{L}}(G,H) = \sum_{K \in \mathcal{N}_{\mathcal{L}}(G,H)} \varepsilon(G,K),$$

by Theorem 3.23. Generalizing the above set, for any $N \in \mathcal{N}_{\mathcal{L}}(G,H)$, put

$$\boldsymbol{\mathcal{N}_{\mathcal{L}}(G,H,N)} = \{K \in \mathcal{N}_{\mathcal{L}}(G,H) \mid K \geq N\}.$$

Also, $\mathcal{N}_{\mathcal{L}}(G,H)$ is closed under intersections and hence is a semilattice (without identity) with respect to $\cap$-products. The set $\mathcal{N}_{\mathcal{L}}(G,H,N)$ is then a subsemilattice.

Theorem 3.24. *Let $\mathcal{L}$ be a semilattice of normal subgroups of a finite group G and let $H \in \mathcal{L}$. Let $N \in \mathcal{N}_{\mathcal{L}}(G,H)$ and let $\pi : G \to G/N$ be the natural quotient map. Then π induces a bijection $\pi : \mathcal{N}_{\mathcal{L}}(G,H,N) \to \mathcal{N}_{\pi(\mathcal{L})}(G/N, N/N)$.*

Proof. First, let $K \in \mathcal{N}_{\mathcal{L}}(G,H,N)$. So, $\pi(K)$ is normal in G/N and clearly $N/N \leq \pi(K)$. Suppose $M' \in \pi(\mathcal{L})$ such that $N/N \leq M' \leq \pi(K)$. Then there exists some $M \in \mathcal{L}$ such that $\pi(M) = M'$. Since $MH \in \mathcal{L}$ and $\pi(MH) = M'$, we may assume that $H \leq M$. Next,

$$H \leq M \leq MN \leq KN \leq K.$$

Since $K \in \mathcal{N}_{\mathcal{L}}(G,H,N)$, the only normal subgroup between K and H contained in $\mathcal{L}$ is H. Thus, $M = H$, which implies

$$M' = \pi(M) = \pi(H) = N/N.$$

Since there are no subgroups in $\pi(\mathcal{L})$ between N/N and $\pi(K)$ other than N/N itself, $\pi(K) \in \mathcal{N}_{\pi(\mathcal{L})}(G/N, N/N)$. Hence, $\pi(\mathcal{N}_{\mathcal{L}}(G, H, N)) \subseteq \mathcal{N}_{\pi(\mathcal{L})}(G/N, N/N)$.

Second, suppose $\pi(K_1) = \pi(K_2)$, for $K_1, K_2 \in \mathcal{N}_{\mathcal{L}}(G, H, N)$. Since $N \leq K_1 \cap K_2$, $K_1 = K_2$, by correspondence. Therefore, $\pi : \mathcal{N}_{\mathcal{L}}(G, H, N) \to \mathcal{N}_{\pi(\mathcal{L})}(G/N, N/N)$ is injective.

Lastly, let $K' \in \mathcal{N}_{\pi(\mathcal{L})}(G/N, N/N)$. Then there exists a unique normal subgroup K of G such that $\pi(K) = K'$ and $N \leq K$. Let $L \in \mathcal{L}$ such that $H \leq L \leq K$. Then $N/N \leq \pi(L) \leq K'$. Since $\pi(L) \in \pi(\mathcal{L})$, it must be that $\pi(L) = N/N$, which implies that $L \leq N$. But $N \in \mathcal{N}_{\mathcal{L}}(G, H)$. Thus, $L = H$, which proves that $K \in \mathcal{N}_{\mathcal{L}}(G, H, N)$, also. This shows that $\pi : \mathcal{N}_{\mathcal{L}}(G, H, N) \to \mathcal{N}_{\pi(\mathcal{L})}(G/N, N/N)$ is surjective. □

Corollary 3.25. *Let G be a finite abelian group with semilattice of subgroups $\mathcal{L}$. Let $H \in \mathcal{L}$ and $N \in \mathcal{N}_{\mathcal{L}}(G, H)$. If $\pi : G \to G/N$ is the quotient map, then $\pi(\varepsilon_{\mathcal{L}}(G, H)) = \varepsilon_{\pi(\mathcal{L})}(G/N, N/N)$.*

Proof. By Theorem 3.23,

$$\varepsilon_{\mathcal{L}}(G, H) = \sum_{K \in \mathcal{N}_{\mathcal{L}}(G,H,N)} \varepsilon(G, K) + \sum_{L \in \mathcal{N}_{\mathcal{L}}(G,H) \setminus \mathcal{N}_{\mathcal{L}}(G,H,N)} \varepsilon(G, L).$$

For each $L \not\geq N$, $\pi(\varepsilon(G, L)) = 0$, and for each $K \geq N$, we have $\pi(\varepsilon(G, K)) = \varepsilon(G/N, K/N)$. Thus,

$$\begin{aligned} \pi(\varepsilon_{\mathcal{L}}(G, H)) &= \sum_{K \in \mathcal{N}_{\mathcal{L}}(G,H,N)} \varepsilon(G/N, K/N) = \sum_{K/N \in \mathcal{N}_{\pi(\mathcal{L})}(G/N,N/N)} \varepsilon(G/N, K/N) \\ &= \varepsilon_{\pi(\mathcal{L})}(G/N, N/N), \end{aligned}$$

where the second equality follows by Theorem 3.24 and the third follows by Theorem 3.23. □

3.3 Primitive Idempotents of Schur Rings

Let S be a Schur ring over G, for some finite group G, not necessarily abelian. Let H, K be normal S-subgroups of G. Then $\overline{H} \cdot \overline{K} = |H \cap K|\overline{HK} \in S$ and $\overline{H} \circ \overline{K} = \overline{H \cap K} \in S$. Thus, the collection of all normal S-subgroups $\mathcal{L}$ forms a lattice of normal subgroups of G. As shown above, associated to this lattice is a complete set of central idempotents in $F[G]$.

Definition 3.26. Let S be a Schur ring over G. Let $\boldsymbol{\varepsilon(S, H)} = \varepsilon(\mathcal{L}, H)$, where $\mathcal{L}$ is the lattice of normal S-subgroups.

Since $\mathcal{L}$ is a lattice, $S(\mathcal{L})$ is a lattice Schur ring contained in S and is maximal with respect to being the largest lattice subring in S. Furthermore, $S(\mathcal{L}) = \mathrm{Span}_F\{\varepsilon(S, H) \mid H \trianglelefteq G \text{ and } \overline{H} \in S\}$, and hence contains many of the central idempotents of S. Under some conditions, $S(\mathcal{L})$ contains all the central idempotents of S, for example when $S = S(\mathcal{L})$.

Theorem 3.27. *Let G be a finite group and let F be a field with characteristic 0. Let $\mathcal{L}$ be a semilattice of normal subgroups of G. Then $\{\varepsilon(\mathcal{L}, H) \neq 0 \mid H \in \mathcal{L}\}$ is a complete set of primitive central idempotents of $S(\mathcal{L})$ and $S(\mathcal{L}) \cong \bigoplus_n F$, where $n = |\{\varepsilon(\mathcal{L}, H) \neq 0 \mid H \in \mathcal{L}\}|$.*

Proof. Let $S = S(\mathcal{L})$. By Theorem 3.10, we have $S = \mathrm{Span}\{\varepsilon(\mathcal{L}, H) \mid H \in \mathcal{L}\}$ and $\{\varepsilon(\mathcal{L}, H) \neq 0 \mid H \in \mathcal{L}\}$ is a basis of S. Thus, this basis must be a complete set of idempotents and the ideal of each idempotent must have dimension 1. Thus, each idempotent is primitive. □

Corollary 3.28. *Let S be a lattice Schur ring over G and let $\varepsilon \in S$ be an idempotent. Then $\varepsilon \in \mathrm{Span}_F\{\overline{H} \mid H \trianglelefteq G \text{ and } \overline{H} \in S\}$.*

We now switch our attention to primitive central idempotents of Schur rings over $G = Z_n$.

Let n be a positive integer with prime factorization given as

$$n = \prod_{i=1}^{r} p_i^{a_i},$$

where the p_i are distinct primes. Set $\lambda(n) = (-1)^{\sum_{i=1}^{r} a_i}$. It is elementary to check that λ and Id, the identity function, are multiplicative functions[3.3]. Let β be the Dirichlet convolution of λ and Id, that is,

$$\beta(n) = (\lambda \sharp \mathrm{Id})(n) = \sum_{d|n} \lambda(d)(n/d).$$

The function β is the alternating-sum-of-divisors function. Since the convolution of multiplicative functions is multiplicative, we have that β is also a multiplicative function. A detailed treatment of β can be found in [32].

[3.3] A function $f : \mathbb{Z}^+ \to \mathbb{R}$ is multiplicative if $f(1) = 1$ and $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.

Definition 3.29. Let $G = Z_n$ be a cyclic group of order n. For each divisor $d \mid n$, let $\boldsymbol{L_d}$ be the set of elements of order d in G. We call L_d the d**th layer** of G.

Since G has a unique subgroup of order d, which is necessarily cyclic, we will abuse notation and refer to this subgroup as Z_d. Thus, L_d is the set of generators of Z_d.

Consider the expansion

$$\begin{aligned}
\varepsilon(G,1) &= \prod_{i=1}^{r}(1-\widehat{Z_{p_i}}) \\
&= 1-\sum_{i\le r}\widehat{Z_{p_i}}+\sum_{i<j\le r}\widehat{Z_{p_ip_j}}-\sum_{i<j<k\le r}\widehat{Z_{p_ip_jp_k}}+\ldots\pm\widehat{Z_m}, \qquad (3.1)\\
&= \sum_{d\mid m}c_d\overline{L_d}, \qquad (3.2)
\end{aligned}$$

where $m = \prod_{i=1}^{r} p_i$ and $c_d \in \mathbb{Q}$. Let a be a divisor of m. By comparing coefficients in (3.1) and (3.2), we have

$$\begin{aligned}
c_a &= \sum_{a\mid d\mid m}\frac{\lambda(d)}{d} = \lambda(a)\sum_{a\mid d\mid m}\frac{\lambda(d/a)}{d} \\
&= \frac{\lambda(a)}{m}\sum_{a\mid d\mid m}\lambda(d/a)(m/d) = \frac{\lambda(a)}{m}\sum_{d'\mid(m/a)}\lambda(d')((m/a)/d') \\
&= \frac{\lambda(a)\beta(m/a)}{m}. \qquad (3.3)
\end{aligned}$$

Also $c_a = 0$ for any $a \nmid m$.

Next, let $H \trianglelefteq G$. Then for all $h \in H$, $h\varepsilon(G,H) = \varepsilon(G,H)$. Thus, the coefficients of $\varepsilon(G,H)$ are constant over cosets of H. Let $\pi : G \to G/H$ be the natural quotient map. Then, as seen above, $\varphi(\varepsilon(G,H)) = \varepsilon(G/H, H/H)$. Let $a \mid n$ and let $g \in G$ be an element of order a. Then $\varphi(g) \in G/H$ is an element of order $a' = \dfrac{a}{\gcd(a,|H|)}$. Finally, let c_a be the coefficient of g in $\varepsilon(G,H)$, let c'_a be the coefficient of $\varphi(g)$ in $\varepsilon(G/H, H/H)$, and let m' be the product of the distinct prime divisors of $n/|H|$. Thus, by (3.3),

$$c_a = \frac{1}{|H|}c'_a = \frac{1}{|H|}\left(\frac{\lambda(a')\beta(m'/a')}{m'}\right) \qquad (3.4)$$

Thus, combining the above formula with Theorem 3.23, it is possible to compute the

coefficients of $\varepsilon(\mathcal{L}, H)$ for any lattice of subgroups of $G = Z_n$.

Now, in a Schur ring, Lemma 2.31 applies, and by examining coefficients of $\varepsilon(G, 1)$ certain S-subgroups can be identified.

Lemma 3.30. *Let S be a Schur ring over G where G is a finite cyclic group. If $\varepsilon(G, 1) \in S$, then $\overline{Z_p} \in S$ for all $p \mid |G|$.*

Proof. Suppose that $|G| = n = \prod_{i=1}^{r} p_i^{a_i}$ is a prime factorization. Let $m = \prod_{i=1}^{r} p_i$. By Proposition 2.33, if $\overline{L_p} \in S$ then $\overline{Z_p} \in S$. So it suffices to show that $\overline{L_p} \in S$ for each $p \mid n$.

As noted in (3.3), the coefficient of $\overline{L_p}$ in $\varepsilon(G, 1)$ is $\dfrac{\lambda(p)\beta(m/p)}{m}$, for each $p \mid m$. Suppose that for some other divisor $d \mid m$,

$$\frac{\lambda(p)\beta(m/p)}{m} = \frac{\lambda(d)\beta(m/d)}{m}. \tag{3.5}$$

Then $\beta(m/p) = \beta(m/d)$, since $\beta(k) > 0$ for all positive k. Since m is square-free and β is multiplicative, this implies that $\beta(p) = \beta(d)$.

Suppose $d = \prod_{i=1}^{s} q_i$, where each q_i is a prime divisor of m. Then $\beta(p) = p - 1$ and

$$\beta(d) = \beta\left(\prod_{i=1}^{s} q_i\right) = \prod_{i=1}^{s}(q_i - 1).$$

Now, if $p \mid d$, then $q_k = p$ for some $1 \leq k \leq s$ and $\prod_{i=1}^{s}(q_i - 1) = q_k - 1$ shows that $(q_1 - 1) \ldots \widehat{(q_k - 1)} \ldots (q_s - 1) = 1$, where here $\widehat{\ }$ denotes an omitted factor. This implies that $d = p$ or $d = 2p$. But if $d = 2p$, then $\lambda(d) = 1$, while $\lambda(p) = -1$, which contradicts (3.5). Therefore, we may assume that $\gcd(p, d) = 1$. Furthermore, since $\prod_{i=1}^{s}(q_i - 1) = p - 1$, we know that $q_i - 1 < p - 1$ and so $q_i < p$ for all primes dividing d.

First, let p be the smallest prime dividing m. Let K be the subset of G consisting of those elements whose coefficient in $\varepsilon(G, 1)$ is equal to $\lambda(p)\beta(m/p)/m$. As above, $L_p \subseteq K$. On the other hand, if any other layer $L_d \subseteq K$, then this implies that $\beta(d) = \beta(p)$, but by the previous paragraph all the prime divisors of d are smaller than p, which is a contradiction. Therefore, $K = L_p$, which implies that $\overline{L_p} \in S$. For induction, suppose that if p is a prime divisor of m which is smaller than k then $\overline{L_p} \in S$. Let p be the smallest prime divisor of m which is greater than or equal to k. Again, let K be the subset of G whose coefficient

in $\varepsilon(G,1)$ is equal to $\lambda(p)\beta(m/p)/m$. Clearly, $L_p \subseteq K$. If $L_d \subseteq K$ for some other divisor d of m, then $d = \prod_{i=1}^{s} q_i$, where q_i is a prime divisor of m strictly smaller than p. By our induction hypothesis, $\overline{L_{q_i}} \in S$ for all divisors of d. Furthermore, $\overline{Z_{q_i}} \in S$ for all i and hence $\overline{Z_{d'}} \in S$ for all $d' \mid d$. Taking differences, this implies that $\overline{L_d} \in S$. So instead, we may set K to be the subset of G whose coefficient in $\varepsilon(G,1) - \frac{\lambda(p)\beta(m/p)}{m}\overline{L_d}$ is equal to $\lambda(p)\beta(m/p)/m$. Repeating this process finitely many times if necessary, eventually we will have that $K = L_p$, which implies that $\overline{L_p} \in S$. Therefore, by induction, $\overline{L_p} \in S$ for all $p \mid |G|$. This implies that $Z_p = \langle L_p \rangle$ is an S-subgroup. □

Lemma 3.31. *Let S be a Schur ring over G where G is a cyclic group. Let $H \trianglelefteq G$. If $\varepsilon(G,H) \in S$, then $\overline{M} \in S$ for all $M \in \mathcal{M}(G,H)$.*

Proof. Now, $\mathrm{Stab}(\varepsilon(G,H)) = H$, which implies $\overline{H} \in S$, by Proposition 2.35. Therefore, the result follows from Corollary 2.45, Corollary 3.25, and Lemma 3.30. □

Theorem 3.32. *Let G be a finite cyclic group and let S be a Schur ring over G. Then $\varepsilon(S,H)$ is primitive for all $\overline{H} \in S$. In particular, $\{\varepsilon(S,H) \mid \overline{H} \in S\}$ is a complete set of primitive idempotents in S.*

Proof. The proof is by induction on $|G|$. If $|G| = p$, a prime, then the lattice of S-subgroups is $\{1, G\}$, the entire lattice of subgroups. Thus, $\varepsilon(S,1) = \varepsilon(G,1)$ and $\varepsilon(S,G) = \widehat{G}$, which are primitive by Corollary 3.20. Next, suppose that the result holds for all cyclic groups with order less than n. Let $G = Z_n$ and let $\overline{H} \in S$. Then consider $\varepsilon(S,H)$. By Theorem 3.23 and Theorem 3.24, if $\pi : G \to G/H$ is the quotient map, then $\varepsilon(S,H)$ is primitive if and only if $\varepsilon(\pi(S), H/H)$ is primitive, where the latter is primitive by our induction hypothesis unless $H = 1$. Thus, it suffices to prove the case for $\varepsilon(S,1)$.

Suppose that

$$\varepsilon(S,1) = \varepsilon_1 + \varepsilon_2 \tag{3.6}$$

decomposes as a sum of nonzero, orthogonal, central idempotents. By Theorem 3.23, $\varepsilon(S,1)$ is a sum of primitive idempotents of the form $\varepsilon(G,H)$, where H does not contain a minimal S-subgroup. So, (3.6) partitions this collection of primitive idempotents. We may assume that $\varepsilon(G,1)$ is involved in ε_1. Suppose that $\varepsilon_1 = \varepsilon(G,1) \in S$. Then by Lemma 3.30, S

contains all the minimal subgroups of G. In particular, $\varepsilon(S,1) = \varepsilon(G,1)$, by Theorem 3.23, and is primitive by Corollary 3.20. So, we may assume that ε_1 involves some other primitive idempotent $\varepsilon(G,H)$, with $H \neq 1$.

Next, suppose that $\varepsilon(G,K)$ is involved in ε_2 and suppose that $H \cap K \neq 1$. Let $\pi : G \to G/(H \cap K)$ be the quotient map. Now, $H, K \in \mathcal{N}(S,1)$, which implies that $H \cap K \in \mathcal{N}(S,1)$. Then both $\pi(\varepsilon(G,H)) \neq 0$ and $\pi(\varepsilon(G,K)) \neq 0$, by Corollary 3.25 and Lemma 3.16. This means that $\pi(\varepsilon(S,1))$ is an imprimitive idempotent of $\pi(S)$. But $\pi(S)$ is a Schur ring by Theorem 2.68 and $\pi(\varepsilon(S,1)) = \varepsilon(\pi(S),1)$ by Corollary 3.25. Thus, $\pi(\varepsilon(S,1))$ is primitive by our induction hypothesis, a contradiction. Hence, $H \cap K = 1$ for all $\varepsilon(G,K)$ involved in ε_2. By this consideration, for all subgroups $1 < L \leq K$, $\varepsilon(G,L)$ must be involved in ε_2 and for all subgroups $1 < L \leq H$, $\varepsilon(G,L)$ must be involved in ε_1. In particular, we may assume that H and K have distinct prime order.

Next, $\varepsilon(G,HK)$ cannot be involved in ε_1 since $HK \cap K \neq 1$ nor ε_2 since $HK \cap H \neq 1$. Thus, $\varepsilon(G,HK)$ is not involved in $\varepsilon(S,1)$, which implies that HK contains a minimal S-subgroup. But the only nontrivial subgroups of HK are H, K, and HK, since H and K have prime order for distinct primes. Thus, HK must be a minimal S-subgroup, that is, $\overline{HK} \in S$.

If $\mathcal{K} = \{K_\alpha \mid \varepsilon(G,K_\alpha) \text{ is involved in } \varepsilon_2\}$ and $\bigcap \mathcal{K} = K \neq 1$, then $\mathrm{Stab}(\varepsilon_2) = K$, which implies that $\overline{K} \in S$. This contradicts Theorem 3.23, since $K \in \mathcal{N}(S,1)$. So, ε_2 must involve at least two distinct primitive idempotents $\varepsilon(G,K_1)$ and $\varepsilon(G,K_2)$ and we may assume that both K_1 and K_2 have prime orders. Using the previous argument, $\overline{HK_1}, \overline{HK_2} \in S$. But then $\overline{HK_1} \circ \overline{HK_2} = \overline{H} \in S$, by the distributivity of the lattice of subgroups of G. But this contradicts Theorem 3.23. Therefore, $\varepsilon(S,1)$ is primitive in S. □

Corollary 3.33. *Let S be a Schur ring over G and let $\varepsilon \in S$ be an idempotent, with G cyclic. Then $\varepsilon \in \mathrm{Span}_{\mathbb{Q}}\{\overline{H} \mid H \trianglelefteq G \text{ and } \overline{H} \in S\}$.*

We now will compute a few examples to illustrate Theorem 3.32.

Example 3.34. Let $G = Z_{12} = \langle z \rangle$. Then the six normal subgroups of G are $Z_1 = 1$, $Z_2 = \langle z^6 \rangle$, $Z_3 = \langle z^4 \rangle$, $Z_4 = \langle z^3 \rangle$, $Z_6 = \langle z^2 \rangle$, and $Z_{12} = G$, and the six primitive idempotents

of $\mathbb{Q}[Z_{12}]$ are

$$\begin{aligned}
\varepsilon(G,1) &= \frac{1}{3} - \frac{1}{3}z^6 - \frac{1}{6}(z^4+z^8) + \frac{1}{6}(z^2+z^{10}) \\
\varepsilon(G,Z_2) &= \frac{1}{6}(1+z^6) - \frac{1}{6}(z^3+z^9) - \frac{1}{12}(z^2+z^4+z^8+z^{10}) + \frac{1}{12}(z+z^5+z^7+z^{11}) \\
\varepsilon(G,Z_3) &= \frac{1}{6}(1+z^4+z^8) - \frac{1}{6}(z^2+z^6+z^{10}) \\
\varepsilon(G,Z_4) &= \frac{1}{6}(1+z^3+z^6+z^9) - \frac{1}{12}(z+z^2+z^4+z^5+z^7+z^8+z^{10}+z^{11}) \\
\varepsilon(G,Z_6) &= \frac{1}{12}(1+z^2+z^4+z^6+z^8+z^{10}) - \frac{1}{12}(z+z^3+z^5+z^7+z^9+z^{11}) \\
\varepsilon(G,G) &= \frac{1}{12}(1+z+z^2+z^3+z^4+z^5+z^6+z^7+z^8+z^9+z^{10}+z^{11})
\end{aligned}$$

As noted before, every subgroup of a cyclic group is characteristic, which implies that every subgroup is an S-subgroup of every orbit Schur ring. Thus, the primitive idempotents of any orbit Schur ring are exactly the primitive idempotents of $\mathbb{Q}[G]$. Consider

$$S = \mathrm{Span}_{\mathbb{Q}}\{1, z^6, z^4+z^8, z^2+z^{10}, z+z^5+z^9, z^3+z^7+z^{11}\},$$

which is not an orbit ring. Then S is a Schur ring over $G = Z_{12}$ and its S-subgroups are 1, Z_2, Z_3, Z_6, and Z_{12}. Therefore, the primitive idempotents of S are

$$\begin{aligned}
\varepsilon(S,1) &= \varepsilon(G,1) \\
\varepsilon(S,Z_2) &= \varepsilon(G,Z_2) + \varepsilon(G,Z_4) = \frac{1}{3}(1+z^6) - \frac{1}{6}(z^2+z^4+z^8+z^{10}) \\
\varepsilon(S,Z_3) &= \varepsilon(G,Z_3) \\
\varepsilon(S,Z_6) &= \varepsilon(G,Z_6) \\
\varepsilon(S,G) &= \varepsilon(G,G).
\end{aligned}$$

We have used Theorem 3.23 to decompose each idempotent into a sum of primitive idempotents over G. We note that $\varepsilon(G,Z_2) \notin S$ since the coefficients of z^9 and z differ. Likewise, $\varepsilon(G,Z_4) \notin S$. Thus, $\varepsilon(S,Z_2)$ is primitive in S. ∎

Example 3.35. For another example, consider the Schur ring T:

$$T = \mathrm{Span}_{\mathbb{Q}}\{1, z^6, z^4 + z^{10}, z^2 + z^8, z + z^3 + z^5 + z^7 + z^9 + z^{11}\}.$$

Then the T-subgroups are 1, Z_2, Z_6, and Z_{12} and the primitive idempotents are

$$\begin{aligned}
\varepsilon(T,1) &= \varepsilon(G,1) + \varepsilon(G,Z_3) = \frac{1}{2} - \frac{1}{2}z^6 \\
\varepsilon(T,Z_2) &= \varepsilon(G,Z_2) + \varepsilon(G,Z_4) \\
\varepsilon(T,Z_6) &= \varepsilon(G,Z_6) \\
\varepsilon(T,G) &= \varepsilon(G,G).
\end{aligned}$$

Since $\varepsilon(G,1), \varepsilon(G,Z_3), \varepsilon(G,Z_2), \varepsilon(G,Z_4) \notin T$, $\varepsilon(T,Z_1)$ and $\varepsilon(T,Z_2)$ are primitive in T. ∎

Example 3.36. We present one last example for Z_{12}. Consider the Schur ring U:

$$U = \mathrm{Span}_{\mathbb{Q}}\{1, z^4, z^8, z^2 + z^6 + z^{10}, z + z^5 + z^9, z^3 + z^7 + z^{11}\}.$$

Then the U-subgroups are 1, Z_3, Z_6, and Z_{12} and the primitive idempotents are

$$\begin{aligned}
\varepsilon(U,1) &= \varepsilon(G,1) + \varepsilon(G,Z_2) + \varepsilon(G,Z_4) \\
&= \frac{2}{3} - \frac{1}{3}(z^4 + z^8) \\
\varepsilon(U,Z_3) &= \varepsilon(G,Z_3) \\
\varepsilon(U,Z_6) &= \varepsilon(G,Z_6) \\
\varepsilon(U,G) &= \varepsilon(G,G).
\end{aligned}$$

Clearly, $\varepsilon(G,1)$, $\varepsilon(G,2)$, and $\varepsilon(G,Z_4) \notin U$. Therefore, $\varepsilon(U,1)$ is primitive in U. ∎

Example 3.37. Let $G = Z_3 \times Z_3 = \langle a, b \rangle$ and let

$$S = \mathrm{Span}_{\mathbb{Q}}\{1, a + a^2 + b + b^2, ab + a^2b^2 + ab^2 + a^2b\},$$

which is the Schur ring mentioned in Example 2.40. Since S is primitive, the lattice of

S-subgroups is $\{1, G\}$. Thus, $\varepsilon(S, 1) = 1 - \widehat{G}$ and $\varepsilon(S, G) = \widehat{G}$. By Theorem 3.23,

$$\varepsilon(S, 1) = [\varepsilon(G, \langle a \rangle) + \varepsilon(G, \langle b \rangle)] + [\varepsilon(G, \langle ab \rangle) + \varepsilon(G, \langle ab^2 \rangle)].$$

But

$$\begin{aligned} \varepsilon(G, \langle a \rangle) + \varepsilon(G, \langle b \rangle) &= \frac{1}{3}(1 + a + a^2) + \frac{1}{3}(1 + b + b^2) - \frac{2}{9}\overline{G} \\ &= \frac{2}{3} + \frac{1}{3}(a + a^2 + b + b^2) - \frac{2}{9}\overline{G} \in S. \end{aligned}$$

Similarly, $\varepsilon(G, \langle ab \rangle) + \varepsilon(G, ab^2) \in S$. Hence, $\varepsilon(S, 1)$ is imprimitive and decomposes as a sum of two nonzero, central idempotents in S. Therefore, Theorem 3.32 may fail when G is non-cyclic. ∎

Chapter 4. Classification of Schur Rings over Cyclic Groups

Any Schur ring is uniquely determined by a partition of the elements of the group, although not every partition determines a Schur ring. An open question in the study of Schur rings is determining which partitions of the group induce a Schur ring and which ones do not. The answer to this question would determine all the possible constructions for Schur rings given a group. Much work has be done to answer this question and some important results have been found. In the case that our group G is cyclic, a complete classification has been found; see Theorem 2.66. In particular, the study of Schur rings over cyclic groups is a very active field with several recent papers being published on this topic: [15], [23], [24], [21], [17], [16], and [13].

A complete classification of Schur Rings over Z_n has already been given in Theorem 2.66 by Leung and Man, which states that all nontrivial Schur rings are of at least one of three constructible types: (1) automorphism orbits, (2) dot products, (3) wedge decompositions. The goal of this chapter will be to provide a new proof for the classification of Schur Rings over cyclic p-groups. This is a weaker result than that of Leung and Man due to the restriction that $|G|$ is a prime power, but the methods used here will be useful in the following chapter. The first section of this chapter will set the stage by outlining exactly how the Schur rings of a cyclic group relate to the subfields of a cyclotomic field, a correspondence which is the essential ingredient in our classification theorem. This approach is fundamentally different from that of Leung and Man. In the second section of this chapter, we will also address Wedderburn decompositions of Schur rings over cyclic groups, which continues the work of the last chapter on idempotents. Even though our goal will be to classify Schur rings over cyclic p-groups, these sections will handle Schur rings over arbitrary cyclic groups. The last section will then be used to classify Schur rings over cyclic p-groups, first in the special case that the cyclic group has prime order and second in the general case of arbitrary prime power order.

Throughout, let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ and let $\mathcal{K}_n = \mathbb{Q}(\zeta_n)$. When the context is clear, subscripts may be omitted.

4.1 A Correspondence Between Schur Rings and Cyclotomic Fields

Every automorphism of Z_n is determined by $z \mapsto z^m$, and every automorphism on $\mathcal{K}_n$ is similarly determined by $\zeta \mapsto \zeta^m$, where m is unique modulo n and $\gcd(n, m) = 1$. Identifying these congruence classes provides an isomorphism between $\mathrm{Aut}(Z_n)$ and the Galois group $\mathcal{G}(\mathcal{K}_n/\mathbb{Q})$.

Lemma 4.1. *The automorphism groups of $\mathcal{K}_n$ and Z_n are isomorphic, that is, $\mathcal{G}(\mathcal{K}_n/\mathbb{Q}) \cong \mathrm{Aut}(Z_n)$. In particular, for $m \in \mathbb{Z}$ such that $\gcd(m, n) = 1$, the map $\zeta \mapsto \zeta^m$ is a field automorphism and $z \mapsto z^m$ is a group automorphism and this correspondence defines an isomorphism of the automorphism groups.*

Proof. This is a standard result whose proof can be found in many graduate texts, including [4, p. 135 and p. 546]. □

By Lemma 4.1, we may identify $\mathcal{G}(\mathcal{K}_n/\mathbb{Q})$ with $\mathrm{Aut}(Z_n)$ and will denote this group as $\boldsymbol{\mathcal{G}_n}$. For each integer m relatively prime to n, let σ_m denote the common automorphism of $\mathrm{Aut}(Z_n)$ and $\mathcal{G}(\mathcal{K}_n/\mathbb{Q})$ which is determined by m. In fact, we may identity $\mathcal{G}_n$ with a set of positive integers. Again, subscripts will be omitted when the context is clear.

Definition 4.2. Let $\boldsymbol{\omega_n} : \mathbb{Q}[Z_n] \to \mathbb{Q}(\zeta_n)$ be the $\mathbb{Q}$-algebra map uniquely defined by the relation $\omega_n(z) = \zeta_n$.

Leung and Man also used this map in their classification of the Schur rings over cyclic groups in [16, Prop 2.7, Cor 2.8, Prop 2.10].

Our current goal will be to prove the Lattice Isomorphism Theorem (Theorem 4.8), which states that there is a lattice-preserving isomorphism between the subfields of the cyclotomic fields and the orbit Schur rings of G. We prove now the necessary prerequisites.

Proposition 4.3. *If A is any subalgebra of $\mathbb{Q}[Z_n]$, then $\omega_n(A)$ is a subfield of $\mathcal{K}_n$.*

Proof. It follows from the definition of ω that $\omega(\mathbb{Q}[Z_n]) = \mathcal{K}_n$ and that $\mathbb{Q}$ is fixed by ω. Consequently, $\omega(\mathbb{Q}) = \mathbb{Q}$. For any subalgebra A such that $\mathbb{Q} \subseteq A \subseteq \mathbb{Q}[G]$, it is clear that $\mathbb{Q} \subseteq \omega(A) \subseteq \mathcal{K}$. Certainly, $\omega(A)$ is a $\mathbb{Q}$-subalgebra of $\mathcal{K}$. Let $\alpha \in \omega(A)$. Since $\mathcal{K}/\mathbb{Q}$ is an

algebraic extension, α is algebraic as well. Thus, there exists a monic irreducible polynomial $f(x) = x^m + a_{m-1}x^{m-1} + \ldots + a_0$ such that $f(\alpha) = 0$. Since f is irreducible, we have that $a_0 \neq 0$. But $f(\alpha) = 0$ gives

$$1 = \alpha \left(\frac{1}{-a_0}\alpha^{m-1} + \frac{a_{m-1}}{-a_0}\alpha^{m-2} + \ldots + \frac{a_1}{-a_0} \right).$$

Therefore, α has an inverse in $\omega(A)$, which implies that $\omega(A)$ is a subfield of $\mathcal{K}$. □

In particular, the proof of Proposition 4.3 actually shows that for any algebraic extension K/F, if A is a ring such that $F \subseteq A \subseteq K$, then A is a field.

Corollary 4.4. *If S is a Schur ring of $\mathbb{Q}[Z_n]$, then $\omega_n(S)$ is a subfield of $\mathbb{Q}(\zeta_n)$.* □

The previous corollary then shows that ω maps the Schur rings of G into the subfields of $\mathcal{K}$. From Galois Theory, we know that the Galois group of the Galois extension $\mathcal{K}/\mathbb{Q}$ determines the structure of the lattice of subfields of $\mathcal{K}$. Likewise, $\mathrm{Aut}(G)$ determines the lattice of orbit Schur rings of $\mathbb{Q}[G]$. Our correspondence exists because these two automorphism groups are essentially the same, as was shown in Lemma 4.1.

Lemma 4.5. *Let $\sigma \in \mathcal{G}_n$. Then $\sigma \circ \omega_n = \omega_n \circ \sigma$.*

Proof. Let $Z_n = \langle z \rangle$ and $\sigma \in \mathcal{G}$. Then there exists an $m \in \mathbb{Z}$ such that $\gcd(m, n) = 1$ and $\sigma(z) = z^m$. Under the identification of Lemma 4.1, we have that $\sigma(\zeta) = \zeta^m$. Therefore,

$$\sigma(\omega(z)) = \sigma(\zeta) = \zeta^m = \omega(z)^m = \omega(z^m) = \omega(\sigma(z)).$$ □

Note that the periods and orbit algebras of a group action are defined in Appendix B.

Lemma 4.6. *Let $\mathcal{H} \leq \mathcal{G}_n$. Then ω respects the periods of $\mathcal{H}$, that is,*

$$\omega_n(\eta_{z^k}) = \eta_{\zeta^k}$$

for every $k \in \mathbb{Z}$.

Proof. Let $\mathcal{H}_{z^k}$ denote the stabilizer of z^k in $\mathcal{H}$. By the correspondence of Lemma 4.1, $\mathcal{H}_{z^k} = \mathcal{H}_{\zeta^k}$, the stabilizer of ζ^k. Let T_{z^k} denote a transversal of the cosets of $\mathcal{H}_{z^k}$ in $\mathcal{H}$. Then

T_{z^k} also denotes a transversal of $\mathcal{H}_{\zeta^k}$. Therefore, the following equation is a consequence of Lemma 4.5:

$$\omega\left(\sum_{\sigma\in T_{z^k}}\sigma(z^k)\right)=\sum_{\sigma\in T_{z^k}}\omega\sigma(z^k)=\sum_{\sigma\in T_{z^k}}\sigma\omega(z^k)=\sum_{\sigma\in T_{z^k}}\sigma(\zeta^k)=\eta_{\zeta^k}. \qquad \square$$

Proposition 4.7. *For each $\mathcal{H}\leq\mathcal{G}_n$, we have $\omega_n(\mathbb{Q}[Z_n]^{\mathcal{H}})=\mathcal{K}_n^{\mathcal{H}}$.*

Proof. We mention that it is a standard result from Galois theory that the subfields of $\mathcal{K}$ are all of the form $\mathcal{K}^{\mathcal{H}}$ for some $\mathcal{H}\leq\mathcal{G}$. Furthermore, Corollary B.4 shows that $\mathcal{K}^{\mathcal{H}}$ is spanned as a $\mathbb{Q}$-algebra by the periods $\{\eta_{\zeta^k}\mid 0\leq k<n\}$. Similarly, $\mathbb{Q}[G]^{\mathcal{H}}=\mathrm{Span}\{\eta_{z^k}\mid 0\leq k<n\}$ by Theorem B.3 and Example 2.20. Then

$$\begin{aligned}\omega(\mathbb{Q}[G]^{\mathcal{H}}) &= \omega\left(\mathrm{Span}\{\eta_{z^k}\mid 0\leq k<n\}\right)\\ &= \mathrm{Span}\{\omega(\eta_{z^k})\mid 0\leq k<n\}\\ &= \mathrm{Span}\{\eta_{\zeta^k}\mid 0\leq k<n\}, \qquad \text{by Lemma 4.6,}\\ &= \mathcal{K}^{\mathcal{H}},\end{aligned}$$

which finishes the proof. $\square$

Proposition 4.7 can also be seen as a consequence of Theorem B.6 after we have determined $\ker\omega_n$.

Theorem 4.8 (The Lattice Isomorphism Theorem)**.** *Let $G=Z_n=\langle z\rangle$ and let $\mathcal{K}=\mathbb{Q}(\zeta_n)$. Then the lattice of orbit Schur rings over G is lattice-isomorphic via ω_n to the lattice of subfields of $\mathcal{K}$.*

We will denote the lattice of subfields of $\mathcal{K}_n$ as $\boldsymbol{\mathcal{L}_n}$.

Proof. Corollary 4.4 shows that ω actually maps the orbit Schur ring lattice into the lattice of subfields of $\mathcal{K}$. Thus, it suffices to show that ω is a bijection between these two lattices.

Let $\mathcal{K}^H$ be the subfield of $\mathcal{K}$ corresponding to $H\leq\mathcal{G}_n$. By Proposition 4.7, $\omega(\mathbb{Q}[G]^H)=\mathcal{K}^H$, which implies that ω is surjective between lattices. Suppose next that $\omega(\mathbb{Q}[G]^H)=\omega(\mathbb{Q}[G]^K)$ for $H,K\leq\mathcal{G}$. Then $\mathcal{K}^H=\mathcal{K}^K$, but the Fundamental Theorem of Galois Theory

implies that $H = K$. Therefore, $\mathbb{Q}[G]^H = \mathbb{Q}[G]^K$. This proves that, in fact, ω induces an isomorphism between these two lattices. □

Corollary 4.9. *Let $H, K \leq \mathcal{G}_n$. Then $\mathbb{Q}[Z_n]^H = \mathbb{Q}[Z_n]^K$ if and only if $H = K$.*

Proof. Only one direction needs to be proven. If H and K are distinct subgroups, then $\omega(\mathbb{Q}[G]^H)$ and $\omega(\mathbb{Q}[G]^K)$ are distinct, which implies that $\mathbb{Q}[G]^H$ and $\mathbb{Q}[G]^K$ are distinct. □

Example 4.10. Corollary 4.9 is not true for arbitrary groups. For example, let

$$G = Z_4 \times Z_2 = \langle a, b \rangle$$

and let

$$S = \mathrm{Span}_{\mathbb{Q}}\{1,\ a^2,\ b + a^2b,\ a + a^3 + ab + ab^3\} \cong \mathbb{Q}Z_2 \wedge \mathbb{Q}Z_2 \wedge \mathbb{Q}Z_2.$$

In fact, $S = \mathcal{R}(\mathbb{Q}[G])$. Furthermore, the automorphism group $\mathrm{Aut}(G) = \mathcal{G}$ is given by

$$\mathcal{G} = \left\langle \sigma : \begin{smallmatrix} a \mapsto a \\ b \mapsto a^2b \end{smallmatrix},\ \tau : \begin{smallmatrix} a \mapsto a^3b \\ b \mapsto a^2b \end{smallmatrix} \right\rangle \cong D_4.$$

Let $\mathcal{H} = \langle \tau \rangle \lneq \mathcal{G}$. It is an exercise to check that $\mathbb{Q}[G]^{\mathcal{H}} = \mathcal{R}(\mathbb{Q}[G]) = \mathbb{Q}[G]^{\mathcal{G}}$, although $\mathcal{H} \neq \mathcal{G}$. ∎

At this point, we change our focus toward understanding the kernel of ω. From Galois theory, if $\Phi_n(x) \in \mathbb{Z}[x]$ denotes the nth cyclotomic polynomial, then $\mathbb{Q}(\zeta_n) \cong \mathbb{Q}[x]/(\Phi_n(x))$. Since $\Phi_n(x) \mid (x^n - 1)$ and $\mathbb{Q}[Z_n] \cong \mathbb{Q}[x]/(x^n - 1)$, the quotient map $\mathbb{Q}[x] \to \mathbb{Q}(\zeta_n)$ factors as the composition $\mathbb{Q}[x] \to \mathbb{Q}[Z_n] \xrightarrow{\omega_n} \mathbb{Q}(\zeta_n)$. In particular, $\ker \omega_n = (\Phi_n(z)) \subseteq \mathbb{Q}[Z_n]$ and, by semisimplicity,

$$\mathbb{Q}[Z_n] \cong \ker \omega_n \oplus \omega_n(\mathbb{Q}[Z_n]) = (\Phi_n(z)) \oplus \mathbb{Q}(\zeta_n).$$

Continuing with this idea, for a Schur ring S over Z_n, we note that

$$\ker \omega|_S = (\ker \omega) \cap S.$$

By Theorem 2.9, S is semisimple and

$$S \cong \ker \omega|_S \oplus \omega(S) = [(\Phi_n(z)) \cap S] \oplus \omega(S). \tag{4.1}$$

More can actually be said about the kernel of ω; it contains all cosets of nontrivial subgroups of Z_n.

Lemma 4.11. *For each prime p dividing n, let Z_p denote the subgroup of Z_n of order p. Then $\ker \omega_n = (\overline{Z_p} : p \mid n$ and p is prime$)$. In particular, a simple quantity of $\mathbb{Q}[Z_n]$ is a kernel element if and only if it is a sum of unions of cosets of some non-trivial subgroups of G.*

Proof. Let $d \mid n$, and let $f_d(x) = \sum_{k=1}^{d} x^{n-kn/d}$. Then, for every prime divisor $p \mid n$,

$$x^n - 1 = (x^{n/p} - 1) f_p(x).$$

Furthermore, since the roots of $x^{n/p} - 1$ consist entirely of n/pth roots of unity, it must be that $\Phi_n(x) \mid f_p(x)$, for all $p \mid n$. Thus, $\Phi_n(x)$ is a common divisor of $\{f_p(x) : p \mid n\}$. Let $g(x) = \gcd\{f_p(x) : p \mid n\}$, and we may assume that g is monic. So, $\Phi_n(x) \mid g(x)$. Certainly, each root of g is an nth root of unity. On the other hand, since $g(x) \mid f_p(x)$ and $x^n - 1 = (x^{n/p} - 1) f_p(x)$, no root of g is a n/pth root of unity for any prime divisor of n. Thus, the roots of g are primitive nth roots of unity. So, $g(x) \mid \Phi_n(x)$, which implies that

$$\Phi_n(x) = \gcd\{f_p(x) : p \mid n\}.$$

Therefore, the ideal generated by the $f_p(x)$ is the principal ideal generated by $\Phi_n(x)$. In particular,

$$\ker \omega_n = (\Phi_n(z)) = (f_p(z) : p \mid n) = (\overline{Z_p} : p \mid n). \qquad \square$$

Theorem 4.12. *Let S be a Schur ring over Z_n. Then $\ker \omega|_S$ is generated as an ideal by the nontrivial S-subgroups, that is, $\ker \omega|_S = (\overline{H} \mid \overline{H} \in S, H \neq 1)$.*

Proof. Let $G = Z_n$. By Lemma 4.11, $(\overline{H} \mid \overline{H} \in S, H \neq 1) \subseteq \ker \omega \cap S$. Recalling the notation introduced in Section 3.2 and Section 3.3, for $1 < K \leq G$, we have that $\varepsilon(G, K) \in$

$(\overline{H} \mid 1 < H \leq G) \subseteq \ker \omega$. Thus, $\omega(\varepsilon(G,K)) = 0$ for all $K \leq G$ except $K = 1$, in which case $\omega(\varepsilon(G,1)) = 1$. By Corollary 3.20,

$$\omega(\mathbb{Q}[G]) \cong \mathbb{Q}[G]\varepsilon(G,1) \quad \text{and} \quad \ker \omega = \mathbb{Q}[G](1 - \varepsilon(G,1)).$$

By Theorem 3.23 and Theorem 3.32,

$$\omega(S) \cong S\varepsilon(S,1) \quad \text{and} \quad \ker \omega|_S = S(1 - \varepsilon(S,1)) = (\overline{H} \mid \overline{H} \in S, H \neq 1). \qquad \square$$

As a consequence of Theorem 4.12,

$$S = S\varepsilon(S,1) \oplus \ker \omega|_S. \tag{4.2}$$

Of course, $S\varepsilon(S,1) \cong \omega(S)$, given by the map $\alpha\varepsilon(S,1) \mapsto \omega(\alpha)$.

We now will collect the various structure properties of Schur rings over cyclic groups which are derived from their interactions with $\omega_n : \mathbb{Q}[G] \to \mathcal{K}$. For example, Proposition 4.7 states that for each $\mathcal{H} \leq \mathcal{G}_n$,

$$\omega_n(\mathbb{Q}[Z_n]^{\mathcal{H}}) = \mathcal{K}_n^{\mathcal{H}}. \tag{4.3}$$

Proposition 4.13. *We have* $\omega_n(\mathbb{Q}[Z_n]^0) = \mathbb{Q}$.

Proof. Since, $\mathbb{Q} \subseteq \mathbb{Q}[Z_n]^0 \subseteq \mathcal{R}(\mathbb{Q}[Z_n])$, Proposition 4.7 implies that

$$\mathbb{Q} = \omega(\mathbb{Q}) \subseteq \omega(\mathbb{Q}[Z_n]^0) \subseteq \omega(\mathcal{R}(\mathbb{Q}[Z_n])) = \mathbb{Q}. \qquad \square$$

Proposition 4.13 also shows that every lattice Schur ring maps onto $\mathbb{Q}$.

Proposition 4.14. *Let* $G = Z_a \times Z_b$ *with* $\gcd(a,b) = 1$. *If* S *is a Schur ring over* Z_a *and* T *is a Schur ring over* Z_b, *then* $\omega_{ab}(S \cdot T) = \omega_a(S) \vee \omega_b(T)$, *the composite of the two fields.*

Proof. Since $S, T \subseteq S \cdot T$, we have that $\omega(S), \omega(T) \subseteq \omega(S \cdot T)$, which implies that $\omega(S) \vee \omega(T) \subseteq \omega(S \cdot T)$. On the other hand, if $x \in \omega(S \cdot T)$, then there exists $s_i \in S$ and $t_i \in T$ such that

$$x = \omega\left(\sum_i s_i t_i\right) = \sum_i \omega(s_i)\omega(t_i) \in \omega(S) \vee \omega(T).$$

Therefore, $\omega(S \cdot T) = \omega(S) \vee \omega(T)$. □

In terms of tensor products, Proposition 4.14 says that $\omega(S \otimes_{\mathbb{Q}} T) = \omega(S) \otimes_{\mathbb{Q}} \omega(T)$.

Proposition 4.15. *Let S be a wedge-decomposable Schur ring of $\mathbb{Q}[Z_n]$ with wedge decomposition $1 < Z_r \leq Z_m < G$. Then $\omega_n(S) = \omega_m(S_{Z_m})$.*

Proof. Let $N = S \cap \mathbb{Q}[Z_m]$. Since $\mathbb{Q}[Z_m] \subseteq \mathbb{Q}[Z_n]$, we have that $\omega_n|_{\mathbb{Q}[Z_m]} = \omega_m$. So, $\omega_m(N) = \omega_n(N)$, where we view N as a subalgebra of $\mathbb{Q}[Z_m]$ and $\mathbb{Q}[Z_n]$, respectively. Since $N \subseteq S \subseteq \mathbb{Q}[Z_n]$, we have that $\omega(N) \subseteq \omega(S)$. Conversely, for any $C \in \mathcal{D}(S) \setminus \mathcal{D}(N)$, we see that $\overline{C}$ is a union of cosets of Z_r and so $\omega(\overline{C}) = 0$, by Lemma 4.11. Therefore, $\omega(S) \subseteq \omega(N)$, which finishes the proof. □

4.2 Wedderburn Decompositions of Schur Rings over Cyclic Groups

In Theorem 3.27, we determined the Wedderburn decomposition of any lattice Schur ring. For cyclic groups, this decomposition characterizes lattice Schur rings.

Proposition 4.16. *Let G be a finite cyclic group and let S be a Schur ring over G. Then $S \cong \bigoplus \mathbb{Q}$ if and only if $S = S(\mathcal{L})$ for some lattice $\mathcal{L}$ of subgroups of G.*

Proof. If $S = S(\mathcal{L})$, then $S \cong \bigoplus \mathbb{Q}$ by Theorem 3.27. Suppose that $S \cong \bigoplus \mathbb{Q}$. Then the complete set of primitive idempotents of S forms a basis. But this set is $\{\varepsilon(S, H) \mid \overline{H} \in S\}$ by Theorem 3.32, and $\mathrm{Span}\{\varepsilon(S, H) \mid \overline{H} \in S\}$ is a lattice Schur ring by Theorem 3.10. □

The next result of this section generalizes the decomposition of Perlis and Walker (Theorem 3.18) to all orbit Schur rings.

Theorem 4.17. *Let $G = Z_n$, a cyclic group of order n, and let $\mathcal{H} \leq \mathrm{Aut}(G)$. Then*

$$\mathbb{Q}[G]^{\mathcal{H}} \cong \bigoplus_{d|n} \mathbb{Q}(\zeta_d)^{\mathcal{H}}.$$

Note that we are using $\mathcal{H}$ to denote a subgroup of $\mathcal{G}_n$ and its restriction in $\mathcal{G}_d$ for each divisor d of n. This notation is used and explained in the paragraph prior to Corollary B.5.

Proof. Let $S = \mathbb{Q}[G]^{\mathcal{H}}$. Since all subgroups of G are characteristic, the primitive idempotents of S are exactly the primitive idempotents of $\mathbb{Q}[G]$, by Corollary 3.20. By Theorem 3.18, each idempotent corresponds to a cyclotomic field and hence to a divisor of n. Let $\varepsilon_d = \varepsilon(G, Z_{n/d})$. Hence, $\mathbb{Q}[G]\varepsilon_d \cong \mathcal{K}_d$. Let $\omega^{(d)} : \mathbb{Q}[G] \to \mathcal{K}_d$ be the representation afforded by $\omega^{(d)}(z) = \zeta_d$ for each $d \mid n$. For each element $x \in \mathcal{K}_d$, there exists some $\alpha \in \mathbb{Q}[G]$ such that $\omega^{(d)}(\alpha) = x$. Define $\varphi_d : \mathcal{K}_d \to \mathbb{Q}[G]\varepsilon_d$ by $\varphi_d(x) = \alpha\varepsilon_d$. It is routine to check that φ_d is an isomorphism. Then

$$S = \bigoplus_{d|n} S\varepsilon_d.$$

Let $\pi_d : G \to G/Z_{n/d}$ be the natural quotient map. Then $\omega^{(d)} = \omega_d \circ \pi_d$. Now, the map $\varphi_d \circ \omega^{(d)}$ is multiplication by ε_d and hence is the natural projection map $\mathbb{Q}[G] \to \mathbb{Q}[G]\varepsilon_d$. Thus, the restriction $\varphi_d \circ \omega^{(d)} : S \to S\varepsilon_d$ is the projection map. Finally,

$$\begin{aligned} S\varepsilon_d &= \varphi_d \circ \omega^{(d)}(S) = \varphi_d \circ \omega_d \circ \pi_d(S) = \varphi_d \circ \omega_d(\mathbb{Q}[Z_d]^{\mathcal{H}}), \quad \text{by Theorem B.6,} \\ &= \varphi_d(\mathcal{K}_d^{\mathcal{H}}), \qquad \text{by Proposition 4.7.} \end{aligned}$$

But $\varphi_d|_{\mathcal{K}_d^{\mathcal{H}}}$ is injective, since $\mathcal{K}_d^{\mathcal{H}}$ is a field. Therefore, $S\varepsilon_d \cong \mathcal{K}_d^{\mathcal{H}}$, which finishes the proof. □

In more generality, let S be a Schur ring over a cyclic group. If $\overline{Z_{n/d}} \in S$, then

$$\omega^{(d)}(\varepsilon(S, Z_{n/d})) = \omega_d \circ \pi_d(\varepsilon(S, Z_{n/d})) = \omega_d(\varepsilon(\pi_d(S), 1)) = 1 \in \mathcal{K}_d.$$

In particular, Schur rings over cyclic groups decompose as sums of subfields of cyclotomic fields, where the degree of each cyclotomic field corresponds to the index of an S-subgroup.

To illustrate this procedure, we provide a few examples over $G = Z_{12}$.

Example 4.18. Let S be defined as in Example 3.34. Now, S has five primitive idempotents corresponding to the subgroups G, Z_6, Z_3, Z_2, and 1. Thus, S has representations in $\mathbb{Q}$, $\mathcal{K}_2$, $\mathcal{K}_4$, $\mathcal{K}_6$, and $\mathcal{K}_{12}$. Since $\dim \mathbb{Q} = \dim \mathcal{K}_2 = 1$, $S\varepsilon(S, G) \cong S\varepsilon(S, Z_6) \cong \mathbb{Q}$, as $\mathbb{Q}$-algebras. Since $\dim \omega^{(4)}(S) = \dim \mathcal{K}_4 = 2$, we have $S\varepsilon(S, Z_3) \cong \mathcal{K}_4 = \mathbb{Q}(i)$. Also, we have $\dim \omega^{(6)}(S) = 1$, which implies that $S\varepsilon(S, Z_2) \cong \mathbb{Q}$. This accounts for five of the six

dimensions of S. Hence, $S\varepsilon(S,1) = \mathbb{Q}$. Therefore,

$$S \cong \mathbb{Q}^4 \oplus \mathbb{Q}(i).$$ ∎

Example 4.19. Let T be defined as in Example 3.35. So, T has four primitive idempotents corresponding to the subgroups G, Z_6, Z_2, and 1, which gives representations in $\mathbb{Q}$, $\mathcal{K}_2$, $\mathcal{K}_6$, and $\mathcal{K}_{12}$, respectively. Like before, $T\varepsilon(T,G) \cong T\varepsilon(T,Z_6) \cong \mathbb{Q}$. Since $\omega^{(6)}(T) = 2$, it must be that $T\varepsilon(T,Z_2) \cong \mathcal{K}_6 \cong \mathbb{Q}(\zeta_3)$. Since $\dim T = 5$, it follows that $T\varepsilon(T,1) \cong \mathbb{Q}$. Therefore,

$$T \cong \mathbb{Q}^3 \oplus \mathbb{Q}(\zeta_3).$$ ∎

Example 4.20. Let U be defined as in Example 3.36. So, U has four primitive idempotents corresponding to G, Z_6, Z_3, and Z_1. Thus, $U\varepsilon(U,G) \cong U\varepsilon(U,Z_6) \cong \mathbb{Q}$. Since $\omega^{(12)}(z^4) = \zeta_3$, we have that $\mathcal{K}_3 \subseteq \omega^{(12)}(U\varepsilon(U,1))$. But $\dim U\varepsilon(U,1) = 2$, which implies that $U\varepsilon(U,1) \cong \mathcal{K}_3$. By dimension considerations, it must be that $\dim U\varepsilon(U,Z_3) = 2$. This implies that $U\varepsilon(U,Z_3) \cong \mathcal{K}_4$. Therefore,

$$U \cong \mathbb{Q}^2 \oplus \mathbb{Q}(i) \oplus \mathbb{Q}(\zeta_3).$$ ∎

4.3 Schur Rings over Cyclic Groups of Prime Power Order

We switch our attention now to the case when Z_n is a p-group, that is, $G = Z_{p^n}$ for some prime p. Our goal for this section will be to prove the general structure theorem of Schur rings over cyclic p-groups. The structure theorem is given in Theorem 4.36, and it states that over a cyclic p-group, all Schur rings are orbit algebras, trivial, or wedge-decomposable.

As described in Appendix C, the lattice of subfields of $\mathcal{K}_{p^n}$ is naturally *layered* by the powers of the prime. Let $G = Z_{p^n}$ and let $\mathcal{L}_{p^n}$ be the lattice of subfields of $\mathcal{K}_{p^n}$. For $k = 0$, we let the **0th layer**[4.1] of $\mathcal{L}_{p^n}$ be $\mathcal{L}_{p^0} = \mathcal{L}_1 = \{\mathbb{Q}\}$. For $k \geq 1$, the **kth layer** of $\mathcal{L}_{p^n}$ is $\mathcal{L}_{p^k} \smallsetminus \mathcal{L}_{p^{k-1}}$. The **top layer** of $\mathcal{L}_{p^n}$ is the nth layer. In particular, the layers form a partition on $\mathcal{L}_{p^n}$.

[4.1] We mention that this layering differs slightly from the layering used in Appendix C. In the Appendix, the first layer is $\mathcal{L}_p$ but in this Chapter, the first layer is $\mathcal{L}_p \smallsetminus \{\mathbb{Q}\}$. This is because we will need to treat $\mathbb{Q}$ differently than other fields in $\mathcal{L}_p$.

We begin by proving the structure theorem in the special case when $G = Z_p$. This result states that all Schur rings over Z_p are orbit algebras. It is essentially a consequence of Theorem 4.8.

Theorem 4.21 (The Structure Theorem of Schur Rings over a Simple Cyclic Group)**.** *Every Schur ring over Z_p is an orbit algebra for some subgroup of automorphisms of Z_p.*

Proof. Let S and T be Schur rings over G for $G = Z_p$. Suppose also that $\omega(S) = \omega(T)$. Then $S + \ker\omega = T + \ker\omega$. But $\ker\omega = (\overline{G}) \leq S, T$, which implies that $S = T$.

Next, let $\omega(S) = \mathcal{K}^{\mathcal{H}}$ for some $\mathcal{H} \leq \mathcal{G}$. Then $\omega(S) = \omega(\mathbb{Q}[G]^{\mathcal{H}})$, by Proposition 4.7. Therefore, $S = \mathbb{Q}[G]^{\mathcal{H}}$ by above. □

We now examine the case of Z_{p^n}.

Proposition 4.22. *Let $G = Z_{p^n}$ for some prime p and let $\mathcal{R}(\mathbb{Q}[G]) = \mathbb{Q}[G]^{\mathcal{G}}$. Then $\mathcal{R}(\mathbb{Q}[G]) = \bigwedge_{k=1}^{n} \mathbb{Q}[Z_p]^0$.*

Proof. By the definition of the layers of G, $\mathcal{R}(\mathbb{Q}[G]) = \mathrm{Span}_{\mathbb{Q}}\{\overline{L_d} : d \mid p^n\} = \mathrm{Span}_{\mathbb{Q}}\{\overline{L_{p^k}} : 1 \leq k \leq n\}$. For $n = 1$, then $\mathcal{R}(G) = \mathbb{Q}[G]^0$. Assume that the result holds for each $k < n$. For each layer,

$$L_{p^k} = \bigcup_{g \in L_{p^k}} gZ_{p^{k-1}},$$

that is, L_{p^k} is the union of all nontrivial cosets of $Z_{p^{k-1}}$ in Z_{p^k}. Let $\pi : Z_{p^k} \to Z_{p^k}/Z_{p^{k-1}}$ be the natural map. Thus, $\mathrm{Span}\{\overline{Z_{p^{n-1}}}, \overline{L_{p^n}}\} = \pi^{-1}(\mathbb{Q}[Z_p]^0)$. Therefore, $\mathcal{R}(\mathbb{Q}[G]) = \mathrm{Span}\{\overline{L_{p^k}} \mid 0 \leq k \leq n-1\} \wedge \mathbb{Q}[Z_p]^0$. But $\mathrm{Span}\{\overline{L_{p^k}} \mid 0 \leq k \leq n-1\} = \mathcal{R}(\mathbb{Q}[Z_{p^{n-1}}])$. So by induction,

$$\mathcal{R}(G) = \left(\bigwedge_{i=0}^{n-1} \mathbb{Q}[Z_p]^0\right) \wedge \mathbb{Q}[Z_p]^0 = \bigwedge_{k=1}^{n} \mathbb{Q}[Z_p]^0.$$ □

We next address the exceptional case: $p = 2$ and $n = 3$.

Proposition 4.23. *For $p = 2$, $\mathcal{L}_3 \smallsetminus \mathcal{L}_2$ contains 3 fields: $\mathbb{Q}(\zeta_8)$, $\mathbb{Q}(\sqrt{2})$, and $\mathbb{Q}(\sqrt{-2})$, and the only Schur ring over Z_8 which map onto these fields are their respective orbit Schur ring correspondents.*

Proof. The statement about subfields of $\mathbb{Q}(\zeta_8)$ is settled by Proposition C.12, so we will prove that there are only three Schur rings over Z_8 which map to these fields.

Let $G = Z_8$. Let S be a Schur ring over G which maps into the top layer of $\mathcal{L}_8$. Suppose there exists an S-class $C \in \mathcal{D}(S)$ such that $C \cap L_8 \neq \emptyset$ and $C \cap L_2 \neq \emptyset$. Now, $L_2 = \{z^4\}$, which implies that $z^4 \in C$. Since every automorphism of G must map z^4 to itself, we conclude that $\sigma(C) = C$ for all $\sigma \in \mathcal{G}$ by Proposition 2.37. Thus, $L_8 \subseteq C$, but $\omega(\overline{L_8}) = 0$ by Lemma 4.11. So, $\omega(S) \in \mathcal{L}_4$, a contradiction. Thus, no class of S can intersect both L_2 and L_8 nontrivially. Furthermore, suppose that $C \cap L_8 \neq \emptyset$ and $C \cap L_4 \neq \emptyset$. If $L_4 \subseteq C$, then the previous argument leads to contradiction. So we may assume that C contains either z^2 or x^6 but not both. In either case, C must contain exactly two elements from L_8 by Proposition 2.37. Now, L_4 is fixed by the automorphism σ_5. Thus, $\sigma_5(C) = C$ by Proposition 2.37. On the other hand, no element of L_8 is fixed by σ_5. Thus, C must consist of a single element from L_4 and a single orbit of σ_5 from L_8, which contains two elements of L_8. Now, these σ_5-orbits are exactly the cosets of Z_2 in L_8. Thus, $\omega(S) \in \mathcal{L}_4$. Therefore, we may assume that Z_4 is an S-subgroup and that each S-class containing an element of L_8 is contained in L_8.

By Proposition 2.13, if any of the L_8-primitive sets of S are a singleton, then $S = \mathbb{Q}[G]$. On the other hand, if L_8 is partitioned as $\{\{z, z^3, z^5, z^7\}\}$ or $\{\{z, z^5\},\ \{z^3, z^7\}\}$, then $\omega(S) \in \mathcal{L}_4$, which cannot happen. The remaining possibilities are $\{\{z, z^3\},\ \{z^5, z^7\}\}$ and $\{\{z, z^7\},\ \{z^3, z^5\}\}$. Notice that $(z + z^3)(z + z^3) = (z + z^7)(z^3 + z^5) = 2z^4 + (z^2 + z^6)$. So in either of the remaining two cases, $\{z^4\} \in \mathcal{D}(S)$. Lastly, if $L_4 = \{z^2, z^6\}$ is split in S, then it must be that $z^2(z + z^3) = z^3 + z^5$ and $z + z^3$ are in S or $z^2(z + z^7) = z + z^3$ and $z + z^7$ are in S. So, we conclude that $L_4 \in \mathcal{D}(S)$. Thus, the only three partitions of G which result as top layer Schur rings are:

$$1,\ z^4,\ z^2,\ z^6,\ z,\ z^3,\ z^5,\ z^7,$$

$$1,\ z^4,\ z^2 + z^6,\ z + z^3,\ z^5 + z^7,$$

$$1,\ z^4,\ z^2 + z^6,\ z + z^7,\ z^3 + z^5,$$

which correspond to $\mathbb{Q}[Z_8], \mathbb{Q}[Z_8]^{\langle \sigma_3 \rangle}$, and $\mathcal{S}(Z_8)$, respectively. □

In the case that n is a power of a prime, $\ker \omega$ is a pre-Schur ring.

Lemma 4.24. *The kernel of $\omega_{p^n} : \mathbb{Q}[Z_{p^n}] \to \mathcal{K}_{p^n}$ is generated by $\overline{Z_p}$, that is, $\ker \omega_{p^n} = (\overline{Z_p})$. In particular, $\ker \omega_{p^n}$ is a pre-Schur ring. Furthermore, a simple quantity of $\mathbb{Q}[Z_{p^n}]$ is a kernel element if and only if it is a union of cosets of Z_p.*

Proof. This follows immediately from Lemma 4.11. □

Of course, $\ker \omega|_S = \ker \omega \cap S$ is also a pre-Schur ring for any Schur ring S.

Corollary 4.25. *Let S be a Schur ring over Z_{p^n} and let $C \in \mathcal{D}(S)$. If $\overline{C} \in \ker \omega|_S$, then C is a union of cosets for some nontrivial S-subgroup of Z_{p^n}.*

Proof. Let $G = Z_{p^n}$. By Lemma 4.24, $\overline{C} = \sum_{i=1}^{k} \overline{g_i H_i}$, where $g_i \in G$, $1 < H_i \leq G$, and $g_i H_i \cap g_j H_j = \emptyset$ for $i \neq j$. Let $H' = \bigcap_{i=1}^{k} H_i$. Then $g_j H_j$ is a union of H' cosets for all i. Now $H' \neq 1$, since $Z_p \leq H_i$ for all i. Thus, C is a union of cosets of H'. Let $H = \mathrm{Stab}(\overline{C})$, which is an S-subgroup by Proposition 2.35. Now, $H' \leq H$, which shows that $H \neq 1$. Finally, C is a union of cosets of H since $H = \mathrm{Stab}(\overline{C})$. □

Corollary 4.26. *Suppose S is a Schur ring over Z_{p^n} and H is a proper S-subgroup of G such that for all $C \in \mathcal{D}(S)$, either $C \subseteq H$ or C is a union of cosets of an S-subgroup (not necessarily the same subgroup) contained in H. Then S is wedge-decomposable.*

Proof. Let C be an S-class not contained in H. By Corollary 4.25, there is an S-subgroup K_C such that C is a union of K_C cosets. Let K be the intersection of all subgroups K_C, where C ranges over the S-classes outside of H. Then K is an S-subgroup, each class C outside of H is a union of K-cosets, and $K \neq 1$ since $Z_p \leq K_C$ for each C. Therefore, $1 < K \leq H < G$ is a wedge decomposition of S. □

Lemma 4.27. *Let $G = Z_{p^n}$ and let $\mathcal{K} = \mathbb{Q}(\zeta_{p^n})$. Let S be a Schur ring over G such that $\omega(S) = \mathcal{K}^{\mathcal{H}}$ for some $\mathcal{H} \leq \mathcal{G}$. Suppose that $S \not\subseteq \mathbb{Q}[G]^{\mathcal{H}}$. Then S is wedge-decomposable.*

Proof. Let $C \in \mathcal{D}(S)$ such that $\sigma(C) \neq C$ for some $\sigma \in \mathcal{H}$. Then by Proposition 2.37 it follows that $\sigma(C) = D$ for some $D \in \mathcal{D}(S)$. Also,

$$\omega(\overline{D}) = \omega(\sigma(\overline{C})) = \sigma(\omega(\overline{C})) = \omega(\overline{C}),$$

where the second equality follows from Lemma 4.5 and the third equality holds since $\omega(\overline{C}) \in \mathcal{K}^{\mathcal{H}}$. Thus, $0 \neq \overline{C} - \overline{D} \in \ker\omega$. Since $C \cap D = \emptyset$ and $\ker\omega$ is a pre-Schur ring, $\overline{C} \in \ker\omega$ by Lemma 2.31. In particular, every S-class which is not fixed by $\mathcal{H}$ must be in $\ker\omega$.

Let H be an S-subgroup maximal with the property that

$$S \cap \mathbb{Q}[H] \subseteq \mathbb{Q}[G]^{\mathcal{H}}.$$

By above, for all $C \in \mathcal{D}(S)$ such that $S \not\subseteq H$, we have $\overline{C} \in \ker\omega$. By assumption, $H \neq G$. If $H = 1$, then all S-classes are in the kernel of ω except the unit class. Likewise, $\overline{G} \in \ker\omega$. Taking the difference, we have that $1 \in \ker\omega$, a contradiction. Therefore, H is a proper, nontrivial subgroup and S is wedge-decomposable by Corollary 4.25 and Corollary 4.26. □

In the case of prime powers, Theorem 3.32 can be proven without Theorem 2.68.

Theorem 4.28. *Let $G = Z_{p^n}$ and let S be a Schur ring over G with minimal S-subgroup H. Then $\varepsilon(S,1) = 1 - \widehat{H}$ is a primitive idempotent of S.*

Proof. Let $H = Z_{p^h}$. By Theorem 3.23,

$$1 - \widehat{H} = \sum_{K \lneq H} \varepsilon(G, K).$$

By Corollary 3.22,

$$\varepsilon(S,1) = \sum_{k=0}^{h-1} (\widehat{Z_{p^k}} - \widehat{Z_{p^{k+1}}}).$$

If $\varepsilon(S,1)$ is imprimitive in S, then there exists orthogonal, nonzero idempotents ε_1 and ε_2 such that

$$\varepsilon(S,1) = \varepsilon_1 + \varepsilon_2.$$

Suppose $\varepsilon(G,1)$ is involved in ε_1. If $\varepsilon(G, Z_{p^k})$ is involved in ε_1, then either $\varepsilon(G, Z_{p^{k+1}})$ is also involved in ε_1 or $\overline{L_{p^{k+1}}} \in S$ by Lemma 2.31. In the latter case, $\overline{Z_{p^{k+1}}} \in S$ by Proposition 2.33. By the minimality of H, $\varepsilon(G, Z_{p^k})$ is involved in ε_1 for all $0 \leq k < h$. Then $\varepsilon_1 = \varepsilon(S,1)$ and $\varepsilon_2 = 0$, a contradiction. □

Lemma 4.29. *Let S be a Schur ring over Z_{p^n} and suppose $\omega(S) \neq \mathbb{Q}$. Then $\overline{Z_p} \in S$. In particular, $\varepsilon(S,1) = \varepsilon(Z_{p^n},1) = 1 - \widehat{Z_p}$.*

Proof. We will work by contrapositive. Let $G = Z_{p^n}$, let $\omega(S) = \mathcal{K}_{p^n}^{\mathcal{H}}$, and let $H = Z_{p^h}$ be the minimal S-subgroup. If Z_p is not an S-subgroup, then $h > 1$. By assumption, S_H is a primitive Schur ring, which implies that $S_H = \mathbb{Q}[H]^0$, by Theorem 2.39.

Let

$$\eta' = \sum_{\zeta_p^m : m \in \mathcal{H}} \zeta_p^m \in \mathcal{K}_p^{\mathcal{H}},$$

that is, η' is the $\mathcal{H}$-period consisting of primitive pth roots of unity. So, $\eta' \in \omega(S)$. Let $z_{p^k} = z^{p^{n-k}}$, let

$$\eta = \sum_{z_p^m : m \in \mathcal{H}} z_p^m \in \mathbb{Q}[Z_p],$$

and let $\mathcal{T}$ be a transversal of the cosets of Z_p in G. Then there exists some $\alpha \in S$ such that

$$\alpha = \sum_{g \in G} \alpha_g g = \eta + \sum_{t \in \mathcal{T}} c_t t \overline{Z_p},$$

for $c_t \in \mathbb{Q}$. Let $\mathcal{O}$ be the $\mathcal{H}$-orbit containing z_p. If $g \in \mathcal{O}$, then $\alpha_g = 1 + c_1$. If $g \in Z_p \setminus \mathcal{O}$, then $\alpha_g = c_1$. Since $S_H = \mathbb{Q}[H]^0$, every element of $Z_p \setminus 1$ must have the same coefficient in α. Thus, $\mathcal{O} = Z_p \setminus 1$. In particular, this implies that $\omega(S) \cap \mathcal{K}_p = \mathbb{Q}$. By a similar argument, if $g \in Z_{p^k} \setminus Z_{p^{k-1}}$ for $k \leq h$ and $\mathcal{O}$ is the $\mathcal{H}$-orbit containing g, then $\mathcal{O}$ is a union of cosets of Z_p. If η is the corresponding $\mathcal{H}$-period, then $\omega(\eta) = 0$. By induction, $\omega(S) \cap \mathcal{K}_{p^k} = \mathbb{Q}$ for all $k \leq h$. By assumption, $h \geq 2$. If p is an odd prime, $\omega(S) = \mathbb{Q}$ as shown in Appendix C. If $p = 2$ and $h \geq 3$, then we must have $\omega(S) = \mathbb{Q}$.

If $p = 2$ and $h = 2$, then $H = Z_4$. Of course, if $n = 2$, then $S = \mathbb{Q}[Z_4]^0$ and $\omega(S) = \mathbb{Q}$. So, we may suppose that $n \geq 3$. Let $C \in \mathcal{D}(S)$ be the primitive set containing z_8. Since Z_4 is an S-subgroup, $Z_4 \cap C = \emptyset$. Let

$$\mathcal{H}' = \{\sigma_m \in \mathcal{G}_{2^n} \mid m \equiv 1 \pmod 8\}.$$

Then $\mathcal{H}' \leq \mathcal{G}$ and $\sigma(C) = C$ for all $\sigma \in \mathcal{H}'$ by Proposition 2.37. Suppose now that $g \in G \setminus Z_8$ and $g \in C$. Since C is fixed by all elements of $\mathcal{H}'$, the set C must contain the entire $\mathcal{H}'$-orbit

of g, which is necessarily a union of cosets of Z_p. Let $A = C \cap Z_8$, which again by Proposition 2.37 must be one of the five following orbits:

$$\{z_8\}, \quad \{z_8, z_8^3\}, \quad \{z_8, z_8^7\}, \quad \{z_8, z_8^5\}, \quad \{z_8, z_8^3, z_8^5, z_8^7\}. \tag{4.4}$$

Then $\omega(\overline{C}) = \omega(\overline{A})$. In the case A is either of the last two orbits from (4.4), it must be that $\omega(\overline{A}) = 0$. Using Proposition 2.37, we conclude that every class containing an element of order 8 vanishes. We conclude that $\omega(S) \cap \mathcal{K}_8 = \mathbb{Q}$. Like above, this implies that $\omega(S) = \mathbb{Q}$. So, we may assume A is one of the first three orbits from (4.4). In this case, let $B = C \cap (G \smallsetminus Z_8)$, that is, $\overline{C} = \overline{A} + \overline{B}$. The set B contains only elements of order strictly greater than 8. Thus, the product of any element of A and B has order strictly greater than 8. Since B is fixed by $\mathcal{H}'$, the product between any two elements of B has order greater than or equal to 8. Therefore, the coefficients of 1, z_2, and z_4 in $\overline{C}^2$ are the same as their coefficients in $\overline{A}^2$. In all three cases, the coefficients of z_2 and z_4 differ in $\overline{A}^2$, a contradiction since S_H is trivial. Therefore, in all cases either $\omega(S) = \mathbb{Q}$ or a contradiction occurred. This finishes the proof. □

Lemma 4.30. *Let S and T be immersed Schur rings of $\mathbb{Q}[Z_{p^n}]$. If $\omega_n(S) = \omega_n(T)$ and $\varepsilon(S,1) = \varepsilon(T,1)$, then $S\varepsilon(S,1) = T\varepsilon(T,1)$.*

Proof. Let $G = Z_{p^n}$ and let $\varepsilon = \varepsilon(S,1) = \varepsilon(T,1)$. If $\omega(S) = \omega(T) = \mathbb{Q}$, then both $S\varepsilon = T\varepsilon = \mathrm{Span}_{\mathbb{Q}}\{\varepsilon\}$. Otherwise, $\varepsilon = \varepsilon(G,1)$ by Lemma 4.29. Since $\mathbb{Q}[G](1-\varepsilon) = \ker(\omega : \mathbb{Q}[G] \to \mathcal{K}_{p^n})$, the map $\omega : \mathbb{Q}[G]\varepsilon \to \mathcal{K}_{p^n}$ given by $\alpha\varepsilon \mapsto \omega(\alpha)$ is an isomorphism. Let $\alpha \in S\varepsilon \subseteq \mathbb{Q}[G]\varepsilon$. Thus, $\alpha = \alpha\varepsilon$. Since $\alpha \in S$ and $\omega(S) = \omega(T)$, there exists some $\beta \in T$ such that $\omega(\alpha) = \omega(\beta)$. Now, $\beta\varepsilon \in T\varepsilon \subseteq \mathbb{Q}[G]\varepsilon$ and $\omega(\beta\varepsilon) = \omega(\alpha\varepsilon)$. Therefore, $\alpha = \alpha\varepsilon = \beta\varepsilon \in T\varepsilon$. Thus, $S\varepsilon \subseteq T\varepsilon$. A symmetric argument provides the other containment. □

Theorem 4.31. *Let S and T be immersed Schur rings of $\mathbb{Q}[Z_{p^n}]$. Then*

$$\omega(S) \cap \omega(T) = \omega(S \cap T).$$

Proof. Let $G = Z_{p^n}$ and let $\varepsilon = \varepsilon(G,1) = 1 - \widehat{Z_p}$. It is always the case that $\omega(A \cap B) \subseteq$

$\omega(A) \cap \omega(B)$ for any subsets $A, B \subseteq \mathbb{Q}[G]$. Suppose that $\omega(S) = \mathbb{Q}$. Then

$$\mathbb{Q} \subseteq \omega(S \cap T) \subseteq \omega(S) \cap \omega(T) = \mathbb{Q} \cap \omega(T) = \mathbb{Q}.$$

So, $\omega(S \cap T) = \omega(S) \cap \omega(T)$. Similarly, $\omega(S \cap T) = \omega(S) \cap \omega(T)$ if $\omega(T) = \mathbb{Q}$.

If $\omega(S), \omega(T) \neq \mathbb{Q}$, then $\varepsilon(S, 1) = \varepsilon(T, 1) = \varepsilon$, by Lemma 4.29. Let $x \in \omega(S) \cap \omega(T)$. Then there exists some $\alpha \in S$ such that $x = \omega(\alpha)$. In fact, $x = \omega(\alpha\varepsilon)$. Clearly, $\alpha\varepsilon \in S$. Likewise, there exists some $\beta \in T$ such that $x = \omega(\beta\varepsilon)$ and $\beta\varepsilon \in T$. As in the previous proof, $\alpha\varepsilon, \beta\varepsilon \in \mathbb{Q}[G]\varepsilon$ and $\alpha\varepsilon = \beta\varepsilon$ since $\omega(\alpha\varepsilon) = \omega(\beta\varepsilon)$. Therefore, $\alpha\varepsilon \in S \cap T$ and $x \in \omega(S \cap T)$, which implies that $\omega(S) \cap \omega(T) \subseteq \omega(S \cap T)$. □

Corollary 4.32. *Let S be a Schur ring over Z_{p^n}. If $H = Z_d$ is an S-subgroup, then*

$$\omega(S) \cap \mathbb{Q}(\zeta_d) = \omega(S_H).$$

Proof. By Theorem 4.31, $\omega(S) \cap \mathbb{Q}(\zeta_d) = \omega(S) \cap \omega(\mathbb{Q}[H]) = \omega(S \cap \mathbb{Q}[H]) = \omega(S_H)$. □

The structure theorem will be separated into three parts, based upon the image of $\omega(S)$. The first case will be $\omega(S) = \mathbb{Q}$, which we will see by Theorem 4.33 implies that S is a wedge product or trivial. The second case will be $\omega(S) \in \mathcal{L}_{p^{n-1}} \setminus \{\mathbb{Q}\}$, that is, $\omega(S)$ is in the middle of the lattice. We will see that Schur rings in this category are wedge-decomposable. Lastly, the third case addresses $\omega(S) \in \mathcal{L}_{p^n} \setminus \mathcal{L}_{p^{n-1}}$, that is, $\omega(S)$ is in the top layer. We will see that S will necessarily be an orbit algebra and hence will be the unique Schur ring which maps to that particular field. The total of these three parts will prove the structure theorem for cyclic p-groups.

Theorem 4.33. *Let $G = Z_{p^n}$ and let S be a Schur ring over G such that $\omega_n(S) = \mathbb{Q}$. Then there exists a subgroup $K \leq G$ and a Schur ring over G/K such that $S = \mathbb{Q}[K]^0 \wedge T$.*

Proof. We proceed by induction. It is certainly true for Z_p by Theorem 4.21, where $S = \mathbb{Q}[Z_p]^0 \wedge T$ and T is the group algebra over the trivial group.

Suppose $S \not\subseteq \mathcal{R}(\mathbb{Q}[G])$. Then S is wedge-decomposable by Lemma 4.27. Let $1 < K \leq H < G$ be a wedge decomposition of S and let $N = S_H$. Since $\omega(S) = \omega(N) = \mathbb{Q}$, induction gives that $N = \mathbb{Q}[L]^0 \wedge T$ for some Schur ring T over G/L. Since $L \leq H$, each coset of

H is a union of cosets of L. Then S contains an immersed trivial Schur ring over L and all S-classes outside of L are unions of cosets of L. Therefore, S is a wedge product of the desired form.

Let us now assume that $S \subseteq \mathcal{R}(\mathbb{Q}[G]) = \bigwedge_{k=1}^{n} \mathbb{Q}[Z_p]^0$. We notice that all $\mathcal{R}(\mathbb{Q}[G])$-classes outside of the first $\mathbb{Q}[Z_p]^0$ are unions of cosets of Z_p. If L_p is not fused to a larger class in S, then S is wedge-decomposable and $S = \mathbb{Q}[Z_p]^0 \wedge T$. Otherwise, let C be the S-class containing L_p and let $H = \langle C \rangle$. Then $\overline{H} \in S$ by Proposition 2.33. In particular, every class outside of H is a union of cosets of H. So if $N = S_H$, then $S = N \wedge T$ as before. Now, N is a Schur ring over $H \lneq G$. By induction, $N = \mathbb{Q}[K]^0 \wedge T_1$, for $K \leq H$ and some Schur ring T_1. Therefore,

$$S = N \wedge T = (\mathbb{Q}[K]^0 \wedge T_1) \wedge T = \mathbb{Q}[K]^0 \wedge (T_1 \wedge T).$$

Therefore, S is a wedge product of the desired form. □

Theorem 4.34. *Let S be a Schur ring over Z_{p^n} and $\omega(S) \in \mathcal{L}_{p^{n-1}} \setminus \{\mathbb{Q}\}$. Then S is wedge-decomposable.*

Proof. Suppose $\omega(S) \in \mathcal{L}_{p^m} \setminus \mathcal{L}_{p^{m-1}}$. Then there exists an orbit Schur ring T over Z_m such that $\omega(T) = \omega(S)$. Let $N = S \cap T$. By Theorem 4.31, $\omega(N) = \omega(S) \cap \omega(T) = \omega(S)$. Furthermore, $\omega(N) \neq \mathbb{Q}$, which implies that N is not a trivial Schur ring. In particular, N is a Schur ring over a nontrivial subgroup $H \leq G$. Of course, $Z_p \leq H$.

Let $\varepsilon = \varepsilon(S, 1)$. Since the minimal subgroup of S must also be the minimal subgroup of N, we have $\varepsilon = \varepsilon(N, 1)$. By (4.2), we have the decompositions

$$S = S\varepsilon \oplus \ker \omega|_S$$

and

$$N = N\varepsilon \oplus \ker \omega|_N.$$

By Lemma 4.30, $S\varepsilon = N\varepsilon$. Now, $\ker \omega|_S = (\overline{Z_p}) \cap S$ is a pre-Schur ring over G and $\ker \omega|_N = (\overline{Z_p}) \cap N$ is an immersed pre-Schur ring contained in it. Therefore, there exists a $\circ$-ideal V such that

$$(\overline{Z_p}) \cap S = [(\overline{Z_p}) \cap N] \oplus V.$$

Then

$$S = S\varepsilon \oplus [(\overline{Z_p}) \cap S] = S\varepsilon \oplus [(\overline{Z_p}) \cap N] \oplus V = N\varepsilon \oplus [(\overline{Z_p}) \cap N] \oplus V = N \oplus V.$$

Then $\mathcal{D}(S) = \mathcal{D}(N) \cup \mathcal{D}(V)$. Since $V \subseteq (\overline{Z_p})$, $\mathcal{D}(V)$ contains only unions of cosets of Z_p. Therefore, S is wedge-decomposable. □

Theorem 4.35. *Let S be a Schur ring over Z_{p^n} such that $\omega(S)$ is in the top layer of $\mathcal{L}_{p^n}$. Then S is an orbit Schur ring, and hence S is the unique Schur ring over Z_{p^n} which maps to $\omega(S)$.*

Proof. We will proceed by induction. The result is true for $n = 1$ by Theorem 4.21. Also, if $p = 2$ and $n = 3$, then the result follows from Proposition 4.23. So we may assume that $n \geq 2$ and if $p = 2$, then $n \neq 3$.

Let $\omega(S) = F = \mathcal{K}^{\mathcal{H}} \in \mathcal{L}_{p^n} \setminus \mathcal{L}_{p^{n-1}}$, for some $\mathcal{H} \leq \mathcal{G}$. If $S \not\subseteq \mathbb{Q}[G]^{\mathcal{H}}$, then S is wedge-decomposable by Lemma 4.27. But that contradicts $\omega(S) \in \mathcal{L}_{p^n} \setminus \mathcal{L}_{p^{n-1}}$. So, $S \subseteq \mathbb{Q}[G]^{\mathcal{H}}$.

Let $K = F \cap \mathcal{K}_{p^{n-1}}$. As long as $p \neq 2$ or $n \neq 3$, K is in the top layer of $\mathcal{L}_{p^{n-1}}$. By induction, there exists a unique Schur ring T over $Z_{p^{n-1}}$, which is necessarily an orbit ring, such that $\omega(T) = K$. It must be that $T = \mathbb{Q}[Z_{p^{n-1}}]^{\mathcal{H}} = \mathbb{Q}[G]^{\mathcal{H}} \cap \mathbb{Q}[Z_{p^{n-1}}]$. Then

$$\omega(S \cap T) = \omega(S) \cap \omega(T) = F \cap K = K,$$

by Theorem 4.31. By uniqueness, $S \cap T = T$. Thus, S contains an immersed Schur ring over $Z_{p^{n-1}}$ which is identical to $\mathbb{Q}[Z_{p^{n-1}}]^{\mathcal{H}}$. Thus, the classes of S in the lower layers are exactly the same classes of $\mathbb{Q}[G]^{\mathcal{H}}$ on the lower layers. In particular, $\overline{Z_p} \in S$.

Suppose that $S \neq \mathbb{Q}[G]^{\mathcal{H}}$. Then the top layer classes of $\mathbb{Q}[G]^{\mathcal{H}}$ are fused together in some manner to form S. In particular, let $C, D \in \mathcal{D}(\mathbb{Q}[G]^{\mathcal{H}})$ be top layer classes such that there exists some $A \in \mathcal{D}(S)$ and $C, D \subseteq A$. Since C and D are in the same layer, there exists some $\sigma \in \mathcal{G}$ such that σ maps an element of C to an element of D. By Proposition 2.37, $\sigma(C) = D$. Again by Proposition 2.37, we conclude that $\sigma(A) = A$. Since both C and D are automorphism classes with respect to $\mathcal{H}$, it must be that $\sigma \in \mathcal{G} \setminus \mathcal{H}$. Since $\sigma(A) = A$, it must also be that $\sigma(D) \subseteq A$. Continuing in this fashion recursively, we conclude that

A contains the entire $\langle\sigma\rangle$-orbit of C. In particular, if $\mathcal{H}_1 = \langle\mathcal{H}, \sigma\rangle$, then A is a union of $\mathcal{H}_1$-orbits. Again by Proposition 2.37, if $B \in \mathcal{D}(S)$ is another top layer class of S, then there exists an automorphism $\tau \in \mathcal{G}$ such that $\tau(A) = B$, and furthermore,

$$\sigma(B) = \sigma\tau(A) = \tau\sigma(A) = \tau(A) = B,$$

since $\mathcal{G}$ is abelian. Therefore, all the top layer classes of S are unions of $\mathcal{H}_1$-classes and $\mathcal{H} < \mathcal{H}_1$.

Let $\varepsilon = \varepsilon(G, 1)$. Since $\overline{Z_p} \in S$, we have $\varepsilon(S, 1) = \varepsilon$. Furthermore, for any top layer $\mathcal{H}$-period $\eta \in \mathbb{Q}[G]$, we have that $\eta\varepsilon \in \mathbb{Q}[G]^{\mathcal{H}}\varepsilon = S\varepsilon \subseteq S$, by Lemma 4.30. Now, since $L_{p^n} Z_p \subseteq L_{p^n}$, we know that $\mathrm{supp}(\eta\varepsilon) \subseteq L_{p^n}$, which implies that $\eta\varepsilon$ is a linear combination of $\mathcal{H}_1$-periods. In particular, $\eta\varepsilon = \sigma(\eta\varepsilon) = \sigma(\eta)\varepsilon$. Thus, $\omega(\eta) = \omega(\sigma(\eta)) = \sigma(\omega(\eta))$. Since $\omega(\eta)$ is an $\mathcal{H}$-period in $\mathcal{K}$ and fixed under σ, it must be that $\omega(\eta)$ is an $\mathcal{H}_1$-period in $\mathcal{K}$. But the orbit corresponding to this period contains a primitive p^nth root of unity. Hence, every orbit in the lower layers is also $\mathcal{H}_1$-invariant. In particular, the $\mathcal{H}$-orbits and $\mathcal{H}_1$-orbits are identical. By Galois correspondence, it follows that $\mathcal{H} = \mathcal{H}_1$, a contradiction since $\sigma \notin \mathcal{H}$. Therefore, $S = \mathbb{Q}[G]^{\mathcal{H}}$, which finishes the proof. □

Theorem 4.36 (The General Structure Theorem of Schur Rings over a Cyclic p-group)**.** *Let $G = Z_{p^n}$, where p is a prime number. Then every Schur ring over Z_{p^n} is an orbit algebra, trivial, or wedge-decomposable.*

Proof. The result follows from Theorem 4.33, Theorem 4.34, and Theorem 4.35. □

Corollary 4.37. *Let $G = Z_{p^n}$. Then for any wedge-decomposable Schur ring S over G, there exists a wedge-decomposition $1 < K \leq H < G$ such that S_H is an indecomposable orbit algebra or trivial Schur ring over H. In particular, $\omega(S_H) = \omega(S)$.* □

Chapter 5. Counting Schur Rings over Cyclic Groups

In this chapter we consider the problem of counting the number of Schur rings over Z_n. Although a structure theorem is available for Schur rings over cyclic groups, this still proves to be a difficult problem. Specializations of this problem have been considered before. For example, in [13] Kovács determines a formula to count the number of Schur rings over Z_{2^n} which are *wedge-product indecomposable*, that is, those Schur rings which cannot be properly factored as a wedge product of Schur rings. This differs from the notion of wedge-indecomposable introduced above since some Schur rings may be decomposable as semi-wedge products but not as wedge products, for example, $\mathbb{Q}[Z_4] \triangle \mathbb{Q}[Z_4]$ as a Schur ring over Z_8. Kovács formula involves the Catalan and Schröder numbers. We will see these again when we consider Schur rings over cyclic 2-groups below. In [18], Liskovets and Pöschel determine a formula for wedge-product indecomposable Schur rings over Z_{p^n}, where p is an odd prime. This formula depends on the Catalan numbers and the number of divisors of $p-1$. Likewise, we will see these quantities again when we consider Schur rings over cyclic p-groups below.

Using the Galois theoretic methods developed in the previous chapter, we will construct a recursive formula and generating function for the integer sequence counting the number of Schur rings over Z_{p^n}, for p a prime. Section 5.1 will address the case that p is an odd prime. Section 5.2 will address the case that $p = 2$.

Throughout, let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ and let $\mathcal{K}_n = \mathbb{Q}(\zeta_n)$. Let $\mathcal{L}_n$ be the lattice of subfields of $\mathcal{K}_n$. Also, let $\omega_n : \mathbb{Q}[Z_n] \to \mathcal{K}_n$ be the homomorphism determined by $z \mapsto \zeta_n$. When the context is clear, subscripts may be omitted.

This chapter will depend heavily on the shape of $\mathcal{L}_{p^n}$. A detailed treatment of this is included in Appendix C for the interested reader.

5.1 Counting Schur Rings Over Cyclic p-groups, p odd

Throughout this section, let p be an odd prime.

Definition 5.1. Let $\Omega(n)$ denote the number of Schur rings over Z_{p^n} and let $\Omega(n,k)$ denote the number of Schur rings S over Z_{p^n} such that $\omega_n(S) = \mathcal{K}_{p^k}$.

We have that $\Omega(0) = 1$ since there is exactly one Schur ring over $Z_{p^0} = 1$, the group ring itself. Also, if x denotes the number of divisors of $p-1$, then $\Omega(1) = x$ by Theorem 4.21.

Proposition 5.2. *The number of Schur rings over Z_{p^n}, for $n \geq 1$, mapping onto $\mathbb{Q}$ with respect to ω is equal to the sum of the number of Schur rings over Z_{p^k} for $0 \leq k \leq n-1$, that is,*

$$\Omega(n,0) = \sum_{k=0}^{n-1} \Omega(k). \tag{5.1}$$

Proof. Let $G = Z_{p^n}$. By Theorem 4.33, if $\omega(S) = \mathbb{Q}$ then $S = \mathbb{Q}[Z_{p^k}]^0 \wedge T$ for some Schur ring T over G/Z_{p^k}. If we consider the trivial Schur ring on G as a trivial wedge product, that is, $\mathbb{Q}[G]^0 = \mathbb{Q}[G]^0 \wedge \mathbb{Q}[1]$, then every Schur ring descending to $\mathbb{Q}$ has the form

$$S = \mathbb{Q}[Z_{p^k}]^0 \wedge T,$$

where $1 \leq k \leq n$ and T ranges over all the Schur rings of $G/Z_{p^k} \cong Z_{p^{n-k}}$. Since every Schur ring over G of this form maps to $\mathbb{Q}$, the proof is finished. □

Proposition 5.3. *The number of Schur rings over Z_{p^n} mapping to $\mathbb{Q}(\zeta_p)$ with respect to ω is equal to the number of Schur rings over $Z_{p^{n-1}}$, that is,*

$$\Omega(n,1) = \Omega(n-1). \tag{5.2}$$

Proof. Let $G = Z_{p^n}$. If $n = 1$, then $\Omega(n-1) = \Omega(0) = 1$. By Theorem 4.21, there is only one Schur ring which maps to $\mathbb{Q}(\zeta_p)$. So the result follows.

Suppose that $n \geq 2$. Let S be the orbit Schur ring over $G = Z_{p^n}$ which maps onto $\mathbb{Q}(\zeta_p)$. By Theorem 4.34, S is wedge-decomposable. By Corollary 4.37, there is a wedge decomposition of S, $1 < K \leq H < Z_{p^n}$, such that S_H is trivial or an indecomposable orbit Schur ring. By Proposition 4.15, $\omega(S) = \omega(S_H)$. If S_H is trivial, then $\omega(S_H) = \mathbb{Q}$, by Proposition 4.13. Thus, S_H is an indecomposable orbit Schur ring. Now, if $Z_p \neq H$, then S_H is wedge-decomposable by Theorem 4.34. Therefore, $H = Z_p$, which forces $K = H$. In

fact, $S_H = \mathbb{Q}[Z_p]$. This shows that $S = \mathbb{Q}[Z_p] \wedge T$, where T is some Schur ring over G/Z_p. Since every Schur ring over G of this form maps to $\mathbb{Q}(\zeta_p)$, the proof is finished. □

Proposition 5.4. *The number of Schur rings over Z_{p^n} mapping to $\mathbb{Q}(\zeta_{p^n})$ with respect to ω is one, that is,*

$$\Omega(n, n) = 1. \tag{5.3}$$

Proof. Since $\mathbb{Q}(\zeta_{p^n})$ is a field in the top layer, this formula follows immediately from Theorem 4.35. □

Proposition 5.5. *For $n \geq 2$, the number of Schur rings over Z_{p^n} mapping to $\mathbb{Q}(\zeta_{p^k})$ for $1 < k \leq n$ with respect to ω is equal to the sum of the number of Schur rings over $Z_{p^{n-1}}$ mapping onto $\mathbb{Q}(\zeta_{p^j})$ where j ranges between $k-1$ and $n-1$, that is,*

$$\Omega(n, k) = \sum_{j=k-1}^{n-1} \Omega(n-1, j). \tag{5.4}$$

Proof. Let $G = Z_{p^n}$. If $k = n$, then $\Omega(n, n) = 1 = \Omega(n-1, n-1)$, by (5.3). If $1 < k < n$, then each Schur ring mapping onto $\mathcal{K}_{p^n}$ is wedge-decomposable, by Theorem 4.34. In particular, if S is a Schur ring over Z_{p^n} such that $\omega(S) = \mathcal{K}_{p^k}$, then there exists a wedge-decomposition such that $1 < K \leq H = Z_{p^k} < G$ and $S_H = \mathbb{Q}[H]$. Put another way, $S = \mathbb{Q}[H] \triangle_K T$, where T is a Schur ring over G/K. Clearly, $\overline{K} \in \mathbb{Q}[H]$ for any choice of K. If $\pi : G \to G/K$ is the quotient map, then $\pi(\mathbb{Q}[H]) = \mathbb{Q}[H/K]$. Therefore, the semi-wedge product $\mathbb{Q}[H] \triangle_K T$ is possible if and only if H/K is a T-subgroup and $T_{H/K} = \mathbb{Q}[H/K]$. Without the loss of generality, we may assume that $K = Z_p$, since any coset of K is necessarily a coset of Z_p. If we identify π with the map $\pi : Z_{p^n} \to Z_{p^{n-1}}$, then $\pi(H) = Z_{p^{k-1}}$ and we must determine which Schur rings T have the property that $T_{H/K} = \mathbb{Q}[Z_{p^{k-1}}]$. Now, $\omega(T_{H/K}) = \mathbb{Q}(\zeta_{p^{k-1}})$, but by Corollary 4.32, we have $\omega(T_{H/K}) = \omega(T) \cap \mathbb{Q}(\zeta_{p^{k-1}})$. Corollary B.5 then gives that $\omega(T) = \mathbb{Q}(\zeta_{p^j})$ for some $k-1 \leq j \leq n-1$. Since every Schur ring of this type can be wedged to $\mathbb{Q}[H]$, the equality is proven. □

Proposition 5.6. *Let $E, F \in \mathcal{L}_{p^k} \setminus \mathcal{L}_{p^{k-1}}$. Then the number of Schur rings over Z_{p^n} which map onto E with respect to ω is equal to the number of Schur rings over Z_{p^n} which map onto*

F with respect to ω. In particular, the number of Schur rings mapping onto E is equal to $\Omega(n,k)$.

Remember that $\mathbb{Q} \in \mathcal{L}_{p^0}$ and is contained in the 0th layer of $\mathcal{L}_{p^n}$, not the first layer $\mathcal{L}_p \setminus \mathcal{L}_1$.

Proof. Let $\Omega(n,E)$ be the number of Schur rings over Z_{p^n} which map onto E. If $k=0$, then the only fields in this layer is $\mathbb{Q}$. So, $E=\mathbb{Q}$. If $k=1$, we can mimic the proof of (5.2) to get $\Omega(n,E)=\Omega(n-1)=\Omega(n,1)$. So, we may suppose that $k \geq 2$.

We will now induct on n. Let $n=2$. Then the only k to consider is $k=2$, which represents the top layer. Mimicking the proof of Proposition 5.4, we get $\Omega(n,E)=1=\Omega(n,k)$. Suppose now that the result holds for all integers less than n. Mimicking the the proof of Proposition 5.5 (using here also Proposition C.6), we have

$$\Omega(n,E)=\sum_{j=k-1}^{n-1}\Omega(n-1,E\cap\mathcal{K}_{p^j}).$$

By induction, $\Omega(n-1,E\cap\mathcal{K}_{p^j})=\Omega(n-1,j)$ for each j, which proves $\Omega(n,E)=\Omega(n,k)$. □

Theorem 5.7. *The number of Schur rings over Z_{p^n}, where p is an odd prime and $n \geq 2$, is given by the following equation:*

$$\Omega(n)=\Omega(n,0)+(x-1)\Omega(n,1)+x\sum_{k=2}^{n}\Omega(n,k), \tag{5.5}$$

where x denotes the number of divisors of $p-1$.

Proof. There is exactly one field in the 0th layer, $(x-1)$ fields in the first layer, and x fields in all remaining layers of $\mathcal{L}_{p^n}$. The equation then follows from Proposition 5.6. □

Equation (5.5) provides for us a formula which can calculate the number of Schur rings over Z_{p^n} using $\Omega(n,k)$ for $k \leq n$. This then begs the question, "How does one compute $\Omega(n,k)$?" Equations (5.1), (5.2), and (5.3) provides answers to this question when $k=0$, 1, and n. For example, we can use (5.5) to compute $\Omega(2)$:

$$\Omega(2) \;=\; \Omega(2,0)+(x-1)\Omega(2,1)+x\Omega(2,2)$$

$$
\begin{aligned}
&= (\Omega(0) + \Omega(1)) + (x-1)\Omega(1) + x \\
&= (1+x) + (x-1)x + x \\
&= x^2 + x + 1.
\end{aligned}
$$

Using (5.4), we can compute all remaining values of $\Omega(n,k)$ recursively. We provide a few examples below.

Corollary 5.8. *For $n \geq 2$,*

$$\Omega(n, n-1) = x + (n-2). \tag{5.6}$$

Proof. We proceed by induction on n. For $n = 2$, we have $\Omega(2,1) = \Omega(1) = x = x + (2-2)$. For $n > 2$, we have

$$
\begin{aligned}
\Omega(n, n-1) &= \Omega(n-1, n-2) + \Omega(n-1, n-1) \quad \text{by (5.4)}, \\
&= \Omega(n-1, (n-1)-1) + 1 \quad \text{by (5.3)}, \\
&= x + (n-3) + 1 \quad \text{by induction}, \\
&= x + (n-2). \qquad \square
\end{aligned}
$$

Corollary 5.9. *For $n \geq 3$,*

$$\Omega(n, n-2) = x^2 + (n-2)x + \binom{n-1}{2}. \tag{5.7}$$

Proof. We proceed by induction on n. For $n = 3$, we have $\Omega(3,1) = \Omega(2) = x^2 + x + 1 = x^2 + (3-2)x + \binom{3-1}{2}$. For $n > 3$, we have

$$
\begin{aligned}
\Omega(n, n-2) &= \Omega(n-1, n-3) + \Omega(n-1, n-2) + \Omega(n-1, n-1) \\
&= \Omega(n-1, (n-1)-2) + \Omega(n-1, (n-1)-1) + 1 \\
&= \left(x^2 + (n-3)x + \frac{(n-3)(n-2)}{2}\right) + (x + (n-3)) + 1 \\
&= x^2 + (n-2)x + \binom{n-1}{2}. \qquad \square
\end{aligned}
$$

By a similar induction argument, we can also prove the identity

$$\Omega(n, n-3) = x^3 + (n-2)x^2 + \left(\binom{n-1}{2} + 1\right)x + \left(\binom{n}{3} - 3\right) \tag{5.8}$$

for $n \geq 4$. As in the previous proofs, the base case of the induction argument uses the calculation of $\Omega(3)$, which can be computed using $\Omega(3,3)$, $\Omega(3,2)$, $\Omega(3,1)$ and $\Omega(3,0)$. Thus, $\Omega(n)$ can be computed using $\Omega(n,k)$, which can be computed using $\Omega(j)$ for $j < n$. Therefore, there is a recursive procedure to compute $\Omega(n)$ from $\Omega(j)$ for $j < n$. We now will work to unearth this recursive formula.

Using (5.1) and (5.2), we can rewrite (5.5) as

$$\Omega(n) = x\Omega(n-1) + \sum_{k=0}^{n-2} \Omega(k) + x\sum_{k=2}^{n} \Omega(n,k). \tag{5.9}$$

Thus, we need to expand $\sum_{k=2}^{n} \Omega(n,k)$ using (5.4). This will produce an equation of the following form:

$$\sum_{i=2}^{n} \Omega(n,i) = \sum_{i=1}^{n-1} c_i \Omega(n-i,1) = \sum_{i=2}^{n} c_{i-1}\Omega(n-i) \tag{5.10}$$

for some positive integers c_i. In particular, the jth iteration of (5.4) will produce an equation of the form

$$\sum_{k=2}^{n} \Omega(n,k) = \sum_{i=1}^{j-1} c_i \Omega(n-i,1) + \sum_{k=j+1}^{n} c_{jk}\Omega(n-j,k-j) \tag{5.11}$$

for some positive integers c_{jk}. We note that $c_{i(i+1)} = c_i$ and $c_{0k} = 1$ for all k. Furthermore,

$$c_{jk} = \sum_{\ell=j}^{k} c_{(j-1)\ell} \tag{5.12}$$

by Proposition 5.5. When $0 < j < k-1$, (5.12) can be rewritten recursively to give

$$c_{jk} = c_{(j-1)k} + \sum_{\ell=j}^{k-1} c_{(j-1)\ell} = c_{(j-1)k} + c_{j(k-1)}. \tag{5.13}$$

From (5.13), we can create a triangular array of integers, depicted in Table 5.2, where k indexes the rows ($k \geq 1$) and j indexes the columns ($0 \leq j < k$). The diagonal entries of

Table 5.1: The first several values of $\Omega(n, k)$

n / k	**1**	**2**	**3**	**4**	**5**	**6**
1	1					
2	x	1				
3	$x^2 + x + 1$	$x + 1$	1			
4	$x^3 + 2x^2 + 4x + 1$	$x^2 + 2x + 3$	$x + 2$	1		
5	$x^4 + 3x^3 + 8x^2 + 9x + 2$	$x^3 + 3x^2 + 7x + 7$	$x^2 + 3x + 6$	$x + 3$	1	
6	$x^5 + 4x^4 + 13x^3 + 23x^2 + 25x + 3$	$x^4 + 4x^3 + 12x^2 + 20x + 9$	$x^3 + 4x^2 + 11x + 17$	$x^2 + 4x + 10$	$x + 4$	1

the triangle give the values of c_i.

Table 5.2: The Triangular Array of c_{jk} Coefficients

1							
1	2						
1	3	5					
1	4	9	14				
1	5	14	28	42			
1	6	20	48	90	132		
1	7	27	75	165	297	429	
1	8	35	110	275	572	1001	1430

Lemma 5.10. *Let c_i be the coefficients given in Equation* (5.10)*. Then $c_i = \frac{1}{i+1}\binom{2i}{i}$, that is, c_i is the ith Catalan number.*

Proof. For convenience, we define $c_{00} = 1$ and $c_{jj} = c_{(j-1)j}$ for $j > 0$. This extended triangular array is known as Catalan's Triangle[5.1]. One property of Catalan's Triangle is that the sequence of diagonal entries is the sequence of Catalan numbers [30]. □

Theorem 5.11. *The number of Schur rings over Z_{p^n}, where p is an odd prime and $n \geq 1$, is given by the following recursive equation:*

$$\Omega(n) = x\Omega(n-1) + \sum_{k=2}^{n}(c_{k-1}x + 1)\Omega(n-k), \tag{5.14}$$

where $\Omega(0) = 1$, $\Omega(1) = x$ denotes the number of divisors of $p-1$, and $c_k = \frac{1}{k+1}\binom{2k}{k}$ is the kth Catalan number.

For $n = 1$, we are considering the sum in (5.14) to be empty.

[5.1] Catalan's Triangle is provided in Table 5.3.

Table 5.3: Catalan's Triangle

1															
1	1														
1	2	2													
1	3	5	5												
1	4	9	14	14											
1	5	14	28	42	42										
1	6	20	48	90	132	132									
1	7	27	75	165	297	429	429								
1	8	35	110	275	572	1001	1430	1430							
1	9	44	154	429	1001	2002	3432	4862	4862						
1	10	54	208	637	1638	3640	7072	11934	16796	16796					
1	11	65	273	910	2548	6188	13260	25194	41990	58786	58786				
1	12	77	350	1260	3808	9996	23256	48450	90440	149226	208012	208012			
1	13	90	440	1700	5508	15504	38760	87210	177650	326876	534888	742900	742900		
1	14	104	544	2244	7752	23256	62016	149226	326876	653752	1188640	1931540	2674440	2674440	
1	15	119	663	2907	10659	33915	95931	245157	572033	1225785	2414425	4345965	7020405	9694845	9694845

Proof. The statements $\Omega(0) = 1$ and $\Omega(1) = x$ have already been proven. For $n \geq 2$,

$$\begin{aligned}
\Omega(n) &= x\Omega(n-1) + \sum_{k=0}^{n-2} \Omega(k) + x \sum_{k=2}^{n} \Omega(n,k), \quad \text{by (5.9)}, \\
&= x\Omega(n-1) + \sum_{k=0}^{n-2} \Omega(k) + x \sum_{k=2}^{n} c_{k-1}\Omega(n-k), \quad \text{by (5.10)}, \\
&= x\Omega(n-1) + \sum_{k=2}^{n} (c_{k-1}x + 1)\Omega(n-k).
\end{aligned}$$

Finally, the formula follows from Lemma 5.10. □

By (5.14), $\Omega(n)$ can be computed recursively without reference to $\Omega(n,k)$ and makes for a much more efficient recurrence. The first several values of $\Omega(n)$ are listed in Table 5.4. Now, $\Omega(n)$ is a polynomial of x. Thus, the number of Schur rings over $\mathbb{Z}_{p^n}$ is computed by evaluating this polynomial for a specific value of x which depends on the prime p. Table 5.5 lists the number of Schur rings over Z_{p^n} up to the tenth power for the first seven odd primes.

Table 5.4: The first several Ω-polynomials

$$\begin{aligned}
\Omega(1) &= x \\
\Omega(2) &= x^2 + x + 1 \\
\Omega(3) &= x^3 + 2x^2 + 4x + 1 \\
\Omega(4) &= x^4 + 3x^3 + 8x^2 + 9x + 2 \\
\Omega(5) &= x^5 + 4x^4 + 13x^3 + 23x^2 + 25x + 3 \\
\Omega(6) &= x^6 + 5x^5 + 19x^4 + 44x^3 + 72x^2 + 69x + 5 \\
\Omega(7) &= x^7 + 6x^6 + 26x^5 + 73x^4 + 152x^3 + 222x^2 + 203x + 8 \\
\Omega(8) &= x^8 + 7x^7 + 34x^6 + 111x^5 + 275x^4 + 511x^3 + 703x^2 + 623x + 13 \\
\Omega(9) &= x^9 + 8x^8 + 43x^7 + 159x^6 + 452x^5 + 997x^4 + 1725x^3 + 2272x^2 + 1990x + 21 \\
\Omega(10) &= x^{10} + 9x^9 + 53x^8 + 218x^7 + 695x^6 + 1754x^5 + 3572x^4 + 5854x^3 + 7510x^2 \\
&\qquad +6559x + 34
\end{aligned}$$

Examining Table 5.4, one can recognize a few patterns with these polynomials. First, $\Omega(n)$ is always a monic degree n polynomial. Next, the coefficient of x^{n-1} is always $n-1$. Both of these statements can be easily proven by induction. Other statements about the

Table 5.5: Number of Schur Rings over Z_{p^k}

$k \backslash p$	**3**	**5**	**7**	**11**	**13**	**17**	**19**
1	2	3	4	4	6	5	6
2	7	13	21	21	43	31	43
3	25	58	113	113	313	196	313
4	92	263	614	614	2,288	1,247	2,288
5	345	1,203	3,351	3,351	16,749	7,953	16,749
6	1,311	5,531	18,329	18,329	122,675	50,775	122,675
7	5,030	25,511	100,372	100,372	898,706	324,323	898,706
8	19,439	117,910	550,009	550,009	6,584,443	2,072,078	6,584,443
9	75,545	545,730	3,015,021	3,015,021	48,243,393	13,239,896	48,243,393
10	294,888	2,528,263	16,531,326	16,531,326	353,479,684	84,603,579	353,479,684

coefficients of $\Omega(n)$ can also be stated and proven. Perhaps the most surprising sequence of coefficients is the sequence of constant terms.

Corollary 5.12. *Let p be an odd prime. Then let $f_n(x) = \Omega(n) \in \mathbb{Z}[x]$. Then $f_n(0) = F_{n-1}$, where F_n is the nth term of the Fibonacci sequence.*

Proof. First, we claim that $F_n = 1 + \sum_{k=0}^{n-2} F_k$ for $n \geq 2$. For $n = 2$, we get $F_2 = 1 + F_0 = 1 + 0 = 1$. For $n > 2$, we get $F_n = F_{n-1} + F_{n-2} = \left(1 + \sum_{k=0}^{n-3} F_k\right) + F_{n-2} = 1 + \sum_{k=0}^{n-2} F_k$, which proves the claim.

It is easy enough to see that $f_1(0) = 0 = F_0$ and $f_2(0) = 1 = F_1$. Suppose that $f_k(0) = F_{k-1}$ for all $k < n$. By (5.14),

$$f_n(0) = \sum_{k=2}^{n} f_{n-k}(0) = \sum_{k=0}^{n-2} f_k(0) = 1 + \sum_{k=1}^{n-2} f_k(0) = 1 + \sum_{k=1}^{n-2} F_{k-1} = 1 + \sum_{k=0}^{n-3} F_k = F_{n-1}. \quad \square$$

Let $\mathcal{F}(z) = \sum_{n=0}^{\infty} \Omega(n) z^n$ be the generating function of Ω. Let $\mathcal{C}(z) = \sum_{n=0}^{\infty} c_n z^n = \dfrac{1 - \sqrt{1-4z}}{2z}$ be the generating function for the Catalan numbers. Then by (5.14),

$$\begin{aligned}
\mathcal{F}(z) &= \Omega(0) + \Omega(1)z + \sum_{n=2}^{\infty} \left(x\Omega(n-1) + \sum_{k=2}^{n} (c_{k-1}x + 1)\Omega(n-k) \right) z^n \\
&= 1 + xz + \sum_{n=2}^{\infty} x\Omega(n-1)z^n + \sum_{n=2}^{\infty} \sum_{k=2}^{n} (c_{k-1}x + 1)\Omega(n-k)z^n \\
&= 1 + xz + xz \sum_{n=2}^{\infty} \Omega(n-1)z^{n-1} + \sum_{k=2}^{\infty} \sum_{n=k}^{\infty} (c_{k-1}x + 1)\Omega(n-k)z^n \\
&= 1 + xz + xz \sum_{n=1}^{\infty} \Omega(n)z^n + \sum_{k=2}^{\infty} \sum_{n=0}^{\infty} (c_{k-1}x + 1)\Omega(n)z^{n+k} \\
&= 1 + xz \left(1 + \sum_{n=1}^{\infty} \Omega(n)z^n \right) + \sum_{k=2}^{\infty} (c_{k-1}x + 1)z^k \sum_{n=0}^{\infty} \Omega(n)z^n \\
&= 1 + xzF(z) + F(z) \sum_{k=2}^{\infty} (c_{k-1}x + 1)z^k \\
&= 1 + xz\mathcal{F}(z) + \mathcal{F}(z) \left(xz \sum_{k=1}^{\infty} c_k z^k + z^2 \sum_{k=0}^{\infty} z_k \right) \\
&= 1 + xz\mathcal{F}(z) + \mathcal{F}(z) \left(xz \left(\frac{1 - \sqrt{1-4z}}{2z} - 1 \right) + \frac{z^2}{1-z} \right)
\end{aligned}$$

$$
\begin{aligned}
&= 1 + \mathcal{F}(z)\left(\frac{x - x\sqrt{1-4z}}{2} + \frac{z^2}{1-z}\right) \\
&= 1 + \mathcal{F}(z)\left(\frac{2z^2 - xz + x - x(1-z)\sqrt{1-4z}}{2(1-z)}\right)
\end{aligned}
$$

Solving the above equation for $\mathcal{F}(z)$ then gives the generating function for $\Omega(n)$:

$$
\mathcal{F}(z) = \frac{2(1-z)}{-2z^2 + (x-2)z - (x-2) + x(1-z)\sqrt{1-4z}} \tag{5.15}
$$

Now, one can continue working with the generating function of $\Omega(n)$ using the typical combinatorial methods to produce a non-recursive formula for $\Omega(n)$. Unfortunately, the formula is too complicated to be included in this paper. For example, after rationalizing the denominator of $\mathcal{F}(z)$, one would need to compute the partial fraction decomposition of

$$
\frac{1}{4(z^4 + (x^2 - x + 2)z^3 - (x^2+1)z^2 + (x^2 + 2x - 2)z - (x-1))},
$$

which involves computing the roots of the denominator. Now, the four roots of this polynomial, if written exactly, would take approximately 50 pages to display! For the sake of the dissertation committee, the non-recursive formula of $\Omega(n)$ has been omitted.

5.2 Counting Schur Rings Over Cyclic p-groups, p even

As is common practice, the case $p = 2$ must be treated separately from all other primes as it is the only exceptional[5.2] case. This section is dedicated to the treatment of Schur rings over Z_{2^n}.

As in the odd case, the lattice of subfields of $\mathcal{K}_{2^n}$ is naturally layered by the powers of 2. We define these layers as in the previous section. Likewise, we mention that the notation introduced in Definition 5.1 applies for $p = 2$ also. There are two critical differences between $\mathcal{L}_{2^n}$ and $\mathcal{L}_{p^n}$, for p odd, that should be mentioned. First, there is no first layer on $\mathcal{L}_{2^n}$ since $\mathcal{L}_2 = \mathcal{L}_1 = \{\mathbb{Q}\}$. This will cause our recurrence relation on $\Omega(n)$ to have "extra" initial

[5.2] One might even say that 2 is the oddest prime!

conditions, that is, the recursion does not stabilize until the fourth stage, as opposed to the second stage for odd primes. Second, the Galois group of $\mathcal{K}_{2^n}$ is not cyclic for $n \geq 3$. This gives the lattice $\mathcal{L}_{2^n}$ a different shape than the other lattices we have seen, which translates to different recurrence relations on $\Omega(n,k)$, which we will see below.

Despite these differences, there are still some important similarities between the even and odd cases. For example, it still holds that $\Omega(0) = 1$. Another similarity is the fact that $\Omega(1) = 1$, which is the number of divisors of $2 - 1 = 1$. It also holds that Proposition 5.2, Proposition 5.4, and Proposition 5.5 (for all $n \geq 3$ and $2 < k \leq n$) remain true if $p = 2$ by the same proofs as before. From these, we can compute

$$\Omega(2) = \Omega(2,0) + \Omega(2,2) = (\Omega(0) + \Omega(1)) + 1 = 3.$$

Now, Proposition 5.3 no longer applies since there is no first layer. Instead, we will treat $k = 2$ as the base case in the recurrence relation on $\Omega(n,k)$.

Proposition 5.13. *For $n \geq 3$, the number of Schur rings over Z_{2^n} mapping to $\mathbb{Q}(i)$ with respect to ω is equal to the difference between number of Schur rings over $Z_{2^{n-1}}$ and the number of Schur rings over $Z_{2^{n-2}}$ mapping onto $\mathbb{Q}$, that is,*

$$\Omega(n,2) = \Omega(n-1) - \Omega(n-2,0). \tag{5.16}$$

When $n = 2$, we have $\Omega(2,2) = 1$ by (5.3).

Proof. Let S be a Schur ring over Z_{2^n} such that $\omega(S) = \mathbb{Q}(i)$. Since $n \geq 3$, it must be that S is wedge-decomposable of the form $S = \mathbb{Q}[Z_4] \triangle T$ for some Schur ring T over $Z_{2^{n-1}}$ such that $T \cap \mathbb{Q}[Z_2] = \mathbb{Q}[Z_2]$, by the same reasoning used in Proposition 5.5. Now, every Schur ring over $Z_{2^{n-1}}$ has this property except those of the form $T = \mathbb{Q}[Z_{2^k}]^0 \wedge T'$ for $1 < k \leq n-1$. Now, there are exactly $\Omega(n-2,0)$ such Schur rings by Proposition 5.2. Therefore, the result follows. □

The major consequence of $\mathcal{G}_{2^n}$ not being cyclic is that Proposition 5.6 fails for some of the layers of $\mathcal{L}_{2^n}$. For example, the number of Schur rings over Z_{16} which map onto $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$ is three but the number of Schur rings mapping onto $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\zeta_8) \cap \mathbb{R}$

is four. By Appendix C, for $k \geq 3$, the kth layer of $\mathcal{L}_{2^n}$ contains three fields: $\mathbb{Q}(\zeta_{2^k})$, $\mathbb{Q}(2\cos(\pi/2^{k-1}))$, and $\mathbb{Q}(2i\cos(\pi/2^{k-1}))$. Let $\Omega_{\mathcal{S}}(n,k)$ be the number of Schur rings over Z_{2^n} which map onto $\mathbb{Q}(2\cos(\pi/2^{k-1}))$ via ω. It holds that $\mathcal{S}(Z_{2^n})$ is the unique Schur ring over Z_{2^n} which maps onto $\mathbb{Q}(2\cos(\pi/2^{k-1}))$, by Theorem 4.35. This gives the following formula:

$$\Omega_{\mathcal{S}}(n,n) = 1. \tag{5.17}$$

Likewise, $\mathbb{Q}[Z_{2^n}]^{\langle \sigma_{2^{n-1}-1} \rangle}$ is the unique Schur ring over Z_{2^n} which maps onto $\mathbb{Q}(2i\cos(\pi/2^{k-1}))$. So for the top layer, the number of Schur rings mapping onto a given field is constant. This fact allows use to compute $\Omega(3)$:

$$\Omega(3) = \Omega(3,0) + \Omega(3,2) + 3\Omega(3,3) = (\Omega(0) + \Omega(1) + \Omega(2)) + (\Omega(2) - \Omega(0)) + 3 = 10.$$

Although Proposition 5.6 is false in general for $p = 2$, it is still "mostly" true, as explained in the next proposition.

Proposition 5.14. *The number of Schur rings over Z_{2^n} mapping onto $\mathbb{Q}(2i\cos(\pi/2^{k-1}))$ via ω is the same as the number of Schur rings mapping onto $\mathbb{Q}(2\cos(\pi/2^{k-1}))$.*

Proof. If $\mathbb{Q}(2\cos(\pi/2^{k-1}))$ and $\mathbb{Q}(2i\cos(\pi/2^{k-1}))$ are in the top layer, then there is exactly one Schur ring mapping onto each field by (5.17). Otherwise, each Schur ring mapping onto these fields must be wedge-decomposable. Let $\pi : Z_{2^n} \to Z_{2^{n-1}}$ be the natural quotient map. Then $\pi(\mathcal{S}(Z_{2^k})) = \pi(\mathbb{Q}[Z_{2^k}]^{\langle \sigma_{2^k-1} \rangle}) = \mathcal{S}(Z_{2^{k-1}}) = \pi(\mathbb{Q}[Z_{2^k}]^{\langle \sigma_{2^{k-1}-1} \rangle})$. Since the images are the same, the number of possible semi-wedge products which map on $\mathbb{Q}(2i\cos(\pi/2^{k-1}))$ is the same as the number of possible semi-wedge products which map onto $\mathbb{Q}(2\cos(\pi/2^{k-1}))$. □

Theorem 5.15. *The number of Schur rings over Z_{2^n}, where $n \geq 3$, is given by the following equation:*

$$\Omega(n) = \Omega(n,0) + \Omega(n,2) + \sum_{k=3}^{n} (\Omega(n,k) + 2\Omega_{\mathcal{S}}(n,k)). \tag{5.18}$$

Proof. There is exactly one field in the 0th layer and the second layer of $\mathcal{L}_{2^n}$. Each other layer of $\mathcal{L}_{2^n}$ contains three fields: $\mathbb{Q}(\zeta_{2^n})$, $\mathbb{Q}(2\cos(\pi/2^{n-1}))$, and $\mathbb{Q}(2i\cos(\pi/2^{n-1}))$. The equation then follows from Proposition 5.14. □

A direct consequence of (5.18) and Lemma 5.10 is the following:

$$\Omega(n) = \Omega(n,0) + \sum_{k=0}^{n-2} c_k \Omega(n-k,2) + 2\sum_{k=3}^{n} \Omega_{\mathcal{S}}(n,k) \tag{5.19}$$

Therefore, we seek to express $2\sum_{k=3}^{n} \Omega_{\mathcal{S}}(n,k)$ in terms of the $\Omega(n,k)$.

Proposition 5.16. *For $k > 3$,*

$$\Omega_{\mathcal{S}}(n,k) = \Omega_{\mathcal{S}}(n-1,k-1) + 2\sum_{j=k}^{n-1} \Omega_{\mathcal{S}}(n-1,j) \tag{5.20}$$

Proof. Following the same reasoning as (5.4), we see (5.20) is true for $k = n$ by (5.17) and for $k < n$, it suffices to count the number of Schur rings T over $Z_{2^{n-1}}$ for which $T \cap \mathbb{Q}[Z_{2^{k-1}}] = \mathcal{S}(Z_{2^{k-1}})$. This is exactly the number of Schur rings over $Z_{2^{n-1}}$ which map onto $\mathbb{Q}(2\cos(\pi/2^j))$ for $k-1 \leq j \leq n-1$ or onto $\mathbb{Q}(2i\cos(\pi/2^j))$ for $k-1 < j \leq n-1$. The result then follows from Proposition 5.14. □

Proposition 5.17. *For $n > 3$,*

$$\Omega_{\mathcal{S}}(n,3) = \Omega(n-1,2) + 2\sum_{j=3}^{n-1} \Omega_{\mathcal{S}}(n-1,j) \tag{5.21}$$

Proof. Following the same reasoning as (5.4), it suffices to count the number of Schur rings T over $Z_{2^{n-1}}$ for which $T \cap \mathbb{Q}[Z_4] = \mathbb{Q}[Z_2] \wedge \mathbb{Q}[Z_2]$. This includes the Schur rings over $Z_{2^{n-1}}$ which map onto $\mathbb{Q}(2\cos(\pi/2^j))$ for $3 \leq j \leq n-1$ or onto $\mathbb{Q}(2i\cos(\pi/2^j))$ for $3 \leq j \leq n-1$. On the other hand, no Schur ring which maps onto $\mathbb{Q}(\zeta_{2^j})$ has this property for $j > 1$. It remains to examine which Schur rings that map onto $\mathbb{Q}$ have this property. By Theorem 4.33, any Schur ring over $Z_{2^{n-1}}$ mapping onto $\mathbb{Q}$ has the form $T = \mathbb{Q}[Z_2] \wedge T'$ for some Schur ring T' over $Z_{2^{n-2}}$ such that $T' \cap \mathbb{Q}[Z_2] = \mathbb{Q}[Z_2]$, since $T \cap \mathbb{Q}[Z_4] = \mathbb{Q}[Z_2] \wedge \mathbb{Q}[Z_2]$. As was seen in the proof of Proposition 5.13, the number of choices for T' is $\Omega(n-1,2)$. The result then follows from Proposition 5.14. □

Next, we need to expand $2\sum_{k=3}^{n} \Omega_{\mathcal{S}}(n,k)$ using (5.20) and (5.21). This will produce an

equation of the following form:

$$2\sum_{k=3}^{n}\Omega_{\mathcal{S}}(n,k)=\sum_{i=1}^{n-2}s_i\Omega(n-i,2) \tag{5.22}$$

for some positive integers s_i. In particular, the jth iteration of (5.20) and (5.21) will produce an equation of the form

$$2\sum_{k=3}^{n}\Omega_{\mathcal{S}}(n,k)=\sum_{i=1}^{j-1}s_i\Omega(n-i,2)+\sum_{k=j+1}^{n}s_{jk}\Omega_{\mathcal{S}}(n-j,k-j) \tag{5.23}$$

for some positive integers s_{jk}. We note that $s_{i(i+1)}=s_i$ and $s_{0k}=1$ for all k. Furthermore,

$$s_{jk}=s_{(j-1)k}+2\sum_{\ell=j}^{k-1}s_{(j-1)\ell} \tag{5.24}$$

by (5.20). When $0<j<k-1$, (5.24) can be rewritten recursively to give

$$s_{jk}=s_{(j-1)k}+s_{j(k-1)}+s_{(j-1)(k-1)}. \tag{5.25}$$

From (5.25), we can create a triangular array of integers, depicted in Table 5.6, where k indexes the rows ($k\geq 1$) and j indexes the columns ($0\leq j<k$). The diagonal entries of the triangle give the values of s_i.

Lemma 5.18. *Let s_i be the coefficients given in Equation* (5.22)*. Then $s_i=\sum_{j=0}^{i}\frac{1}{j+1}\binom{2j}{2}\binom{i+j}{2j}$, that is, s_i is the ith Schröder number.*

Proof. Like in Lemma 5.18, we define $s_{00}=1$ and $s_{jj}=s_{(j-1)j}$ for $j>0$. Now, this new triangular array is known as the Super-Catalan Triangle[5.3]. One property of this triangle is that the sequence of diagonal entries is the sequence of super-Catalan numbers, also known as the little Schröder numbers [6]. Multiplying the little Schröder numbers by two and reindexing gives the Schröder numbers. □

[5.3]Catalan's Triangle is provided in Table 5.3.

Table 5.6: The Triangular Array of s_{jk} Coefficients

1							
1	3						
1	5	11					
1	7	23	45				
1	9	39	107	197			
1	11	59	205	509	903		
1	13	83	347	1061	2473	4279	
1	15	111	541	1949	5483	12235	20793

Theorem 5.19. *The number of Schur rings over Z_{2^n}, where $n \geq 2$, is given by the following recursive equation:*

$$\Omega(n) = \sum_{k=1}^{3} 2^k \Omega(n-k) - (c_{n-1} + s_{n-1}) + \sum_{k=4}^{n} \left(c_{k-1} + s_{k-1} - \sum_{j=1}^{k-3} (c_j + s_j) \right) \Omega(n-k) \quad (5.26)$$

where $\Omega(0) = 1$, $\Omega(1) = 1$, $\Omega(2) = 3$, $\Omega(3) = 10$, $c_k = \dfrac{1}{k+1}\dbinom{2k}{k}$ is the kth Catalan number, and $s_k = \sum_{j=0}^{k} \frac{1}{j+1}\binom{2j}{2}\binom{k+j}{2j}$ is the kth Schröder number.

For $n < 4$, we consider the second sum in (5.26) to be empty. Also, we define $\Omega(-1) = 0$, which appear in (5.26) for $n = 2$.

Proof. By (5.19),

$$\Omega(n) = \Omega(n,0) + \sum_{k=0}^{n-2} c_k \Omega(n-k,2) + 2\sum_{k=3}^{n} \Omega_{\mathcal{S}}(n,k),$$

which by Lemma 5.18, can be rewritten as

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

Table 5.7: Super-Catalan's Triangle

1													
1	1												
1	3	3											
1	5	11	11										
1	7	23	45	45									
1	9	39	107	197	197								
1	11	59	205	509	903	903							
1	13	83	347	1061	2473	4279	4279						
1	15	111	541	1949	5483	12235	20793	20793					
1	17	143	795	3285	10717	28435	61463	103049	103049				
1	19	179	1117	5197	19199	58351	148249	312761	518859	518859			
1	21	219	1515	7829	32225	109775	316375	777385	1609005	2646723	2646723		
1	23	263	1997	11341	51395	193395	619545	1713305	4099695	8355423	13648869	13648869	
1	25	311	2571	15909	78645	323435	1136375	3469225	9282225	21737343	43741635	71039373	71039373

$$
\begin{aligned}
&= \Omega(n,0) + \Omega(n,2) + \sum_{k=1}^{n-2}(c_k + s_k)\Omega(n-k,2) \\
&= \Omega(n,0) + \Omega(n,2) + (c_{n-2} + s_{n-2}) + \sum_{k=1}^{n-3}(c_k + s_k)\Omega(n-k,2).
\end{aligned}
$$

We next can apply Proposition 5.13 to the above equation:

$$
\begin{aligned}
\Omega(n) &= \Omega(n,0) + [\Omega(n-1) - \Omega(n-2,0)] + (c_{n-2} + s_{n-2}) \\
&\qquad + \sum_{k=1}^{n-3}(c_k + s_k)[\Omega(n-k-1) - \Omega(n-k-2,0)] \\
&= \Omega(n-1) + \sum_{k=1}^{n-3}(c_k + s_k)\Omega(n-k-1) + (c_{n-2} + s_{n-2}) + \Omega(n,0) \\
&\qquad - \Omega(n-2,0) - \sum_{k=1}^{n-3}(c_k + s_k)\Omega(n-k-2,0) \\
&= \Omega(n-1) + \sum_{k=2}^{n-2}(c_{k-1} + s_{k-1})\Omega(n-k) + (c_{n-2} + s_{n-2}) + \Omega(n,0) \\
&\qquad - \Omega(n-2,0) - \sum_{k=3}^{n-1}(c_{k-2} + s_{k-2})\Omega(n-k,0) \\
&= \Omega(n-1) + \sum_{k=2}^{n-1}(c_{k-1} + s_{k-1})\Omega(n-k) + \Omega(n,0) - \Omega(n-2,0) \\
&\qquad - \sum_{k=3}^{n-1}(c_{k-2} + s_{k-2})\Omega(n-k,0).
\end{aligned}
$$

Next we apply Proposition 5.2 to the above equation:

$$
\Omega(n) = 2\Omega(n-1) + \Omega(n-2) + \sum_{k=2}^{n-1}(c_{k-1} + s_{k-1})\Omega(n-k) - \sum_{k=3}^{n-1}(c_{k-2} + s_{k-2}) \sum_{j=0}^{n-k-1} \Omega(j).
$$

We note that

$$
\begin{aligned}
\sum_{k=3}^{n-1}(c_{k-2} + s_{k-2}) \sum_{j=0}^{n-k-1} \Omega(j) &= \sum_{k=3}^{n-1} \sum_{j=0}^{n-k-1} (c_{k-2} + s_{k-2})\Omega(j) = \sum_{j=0}^{n-4} \sum_{k=3}^{n-j-1} (c_{k-2} + s_{k-2})\Omega(j) \\
&= \sum_{k=0}^{n-4} \sum_{j=3}^{n-k-1} (c_{j-2} + s_{j-2})\Omega(k) = \sum_{k=4}^{n} \sum_{j=3}^{k-1} (c_{j-2} + s_{j-2})\Omega(n-k).
\end{aligned}
$$

Therefore,

$$\begin{aligned}
\Omega(n) &= 2\Omega(n-1) + \Omega(n-2) + \sum_{k=2}^{n-1}(c_{k-1}+s_{k-1})\Omega(n-k) - \sum_{k=4}^{n}\sum_{j=3}^{k-1}(c_{j-2}+s_{j-2})\Omega(n-k) \\
&= 2\Omega(n-1) + 4\Omega(n-2) + 8\Omega(n-3) - (c_{n-1}+s_{n-1}) \\
&\qquad + \sum_{k=2}^{n-1}\left(c_{k-1}+s_{k-1} - \sum_{j=3}^{k-1}(c_{j-2}+s_{j-2})\right)\Omega(n-k) \\
&= \sum_{k=1}^{3} 2^k\Omega(n-k) - (c_{n-1}+s_{n-1}) + \sum_{k=4}^{n}\left(c_{k-1}+s_{k-1} - \sum_{j=1}^{k-3}(c_j+s_j)\right)\Omega(n-k). \quad \square
\end{aligned}$$

Table 5.8 lists the number of Schur rings over Z_{2^n} up to the tenth power.

Table 5.8: Number of Schur Rings over Z_{2^n}

n	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
$\Omega(n)$	1	3	10	37	151	657	2,989	14,044	67,626	332,061

Let $\mathcal{F}(z) = \sum_{n=0}^{\infty}\Omega(n)z^n$ be the generating function of Ω, for $p = 2$. Let

$$\mathcal{C}(z) = \sum_{n=0}^{\infty} c_n z^n = \frac{1-\sqrt{1-4z}}{2z}$$

be the generating function for the Catalan numbers and let

$$\mathcal{S}(z) = \sum_{n=0}^{\infty} s_n z^n = \frac{1-z-\sqrt{1-6z+z^2}}{2z}$$

be the generating function for the Schröder numbers. Then by (5.26),

$$\begin{aligned}
\mathcal{F}(z) &= \Omega(0) + \Omega(1)z + \Omega(2)z^2 + \Omega(3)z^3 + \sum_{n=4}^{\infty}\Bigg(2\Omega(n-1) + 4\Omega(n-2) + 8\Omega(n-3) \\
&\qquad -(c_{n-1}+s_{n-1}) + \sum_{k=4}^{n}\left(c_{k-1}+s_{k-1} - \sum_{j=1}^{k-3}(c_j+s_j)\right)\Omega(n-k)\Bigg)z^n \\
&= 1 + z + 3z^2 + 10z^3 + 2\sum_{n=4}^{\infty}\Omega(n-1)z^n + 4\sum_{n=4}^{\infty}\Omega(n-2)z^n + 8\sum_{n=4}^{\infty}\Omega(n-3)z^n
\end{aligned}$$

$$
\begin{aligned}
& -\sum_{n=4}^{\infty} c_{n-1}z^n - \sum_{n=4}^{\infty} s_{n-1}z^n + \sum_{n=4}^{\infty}\sum_{k=4}^{n}\left(c_{k-1}+s_{k-1}-\sum_{j=1}^{k-3}(c_j+s_j)\right)\Omega(n-k)z^n \\
= \;& 1+z+3z^2+10z^3+2z\sum_{n=3}^{\infty}\Omega(n)z^n+4z^2\sum_{n=2}^{\infty}\Omega(n)z^n+8z^3\sum_{n=1}^{\infty}\Omega(n)z^n \\
& -z\sum_{n=3}^{\infty} c_n z^n - z\sum_{n=3}^{\infty} s_n z^n + \sum_{k=4}^{\infty}\sum_{n=k}^{\infty}\left(c_{k-1}+s_{k-1}-\sum_{j=1}^{k-3}(c_j+s_j)\right)\Omega(n-k)z^n \\
= \;& 1+z+2z\sum_{n=0}^{\infty}\Omega(n)z^n+4z^2\sum_{n=0}^{\infty}\Omega(n)z^n+8z^3\sum_{n=0}^{\infty}\Omega(n)z^n \\
& -z\sum_{n=0}^{\infty} c_n z^n - z\sum_{n=0}^{\infty} s_n z^n + \sum_{k=4}^{\infty}\sum_{n=0}^{\infty}\left(c_{k-1}+s_{k-1}-\sum_{j=1}^{k-3}(c_j+s_j)\right)\Omega(n)z^{n+k} \\
= \;& 1+z+2z\mathcal{F}(z)+4z^2\mathcal{F}(z)+8z^3\mathcal{F}(z)-z\mathcal{C}(z)-z\mathcal{S}(z) \\
& \qquad +\sum_{k=4}^{\infty}\left(c_{k-1}+s_{k-1}-\sum_{j=1}^{k-3}(c_j+s_j)\right)z^k\sum_{n=0}^{\infty}\Omega(n)z^n \\
= \;& 1+z+(2z+4z^2+8z^3)\mathcal{F}(z)-z(\mathcal{C}(z)+\mathcal{S}(z)) \\
& \qquad +\sum_{k=4}^{\infty}\left(c_{k-1}+s_{k-1}-\sum_{j=1}^{k-3}(c_j+s_j)\right)z^k\sum_{n=0}^{\infty}\Omega(n)z^n \\
= \;& 1+z+(2z+4z^2+8z^3)\mathcal{F}(z)-z(\mathcal{C}(z)+\mathcal{S}(z)) \\
& \qquad +\mathcal{F}(z)\sum_{k=4}^{\infty}\left(c_{k-1}+s_{k-1}-\sum_{j=1}^{k-3}(c_j+s_j)\right)z^k.
\end{aligned}
$$

Next, we work to simplify $\mathcal{T}(z)=\sum_{k=4}^{\infty}\left(c_{k-1}+s_{k-1}-\sum_{j=1}^{k-3}(c_j+s_j)\right)z^k$. Note that

$$
\begin{aligned}
\mathcal{T}(z) &= \sum_{k=4}^{\infty} c_{k-1}z^k + \sum_{k=4}^{\infty} s_{k-1}z^k - \sum_{k=4}^{\infty}\sum_{j=1}^{k-3}(c_j+s_j)z^k \\
&= z\sum_{k=3}^{\infty} c_k z^k + z\sum_{k=3}^{\infty} s_k z^k - \sum_{j=1}^{\infty}\sum_{k=j+3}^{\infty}(c_j+s_j)z^k \\
&= -(2z+3z^2+8z^3)+z\mathcal{C}(z)+z\mathcal{S}(z)-\sum_{j=1}^{\infty}(c_j+s_j)\sum_{k=j+3}^{\infty}z^k \\
&= -(2z+3z^2+8z^3)+z\mathcal{C}(z)+z\mathcal{S}(z)-\sum_{j=1}^{\infty}(c_j+s_j)z^{j+3}\sum_{k=0}^{\infty}z^k \\
&= -(2z+3z^2+8z^3)+z\mathcal{C}(z)+z\mathcal{S}(z)-\frac{z^3}{1-z}\sum_{j=1}^{\infty}(c_j+s_j)z^j
\end{aligned}
$$

$$= -(2z + 3z^2 + 8z^3) + z\mathcal{C}(z) + z\mathcal{S}(z) - \frac{z^3}{1-z}(\mathcal{C}(z) + \mathcal{S}(z) - 2).$$

Therefore,

$$\begin{aligned}
\Omega(n) &= 1 + z(1 - \mathcal{C}(z) + \mathcal{S}(z)) + \mathcal{F}(z)\Big(((2z + 4z^2 + 8z^3) - (2z + 3z^2 + 8z^3) \\
&\qquad + z\mathcal{C}(z) + z\mathcal{S}(z) - \frac{z^3}{1-z}(\mathcal{C}(z) + \mathcal{S}(z) - 2)\Big) \\
&= 1 + z(1 - \mathcal{C}(z) + \mathcal{S}(z)) + \mathcal{F}(z)\left(z(\mathcal{C}(z) + \mathcal{S}(z)) + z^2 - \frac{z^3}{1-z}(\mathcal{C}(z) + \mathcal{S}(z) - 2)\right)
\end{aligned}$$

Solving the above equation for $\mathcal{F}(z)$ then gives the generating function for $\Omega(n)$:

$$\begin{aligned}
\mathcal{F}(z) &= \frac{(\mathcal{C}(z) + \mathcal{S}(z) - 1)z(1-z) + z - 1}{z^2(1-z) + (\mathcal{C}(z) + \mathcal{S}(z))z(1-z) + z - 1 + (2 - \mathcal{C}(z) - \mathcal{S}(z))z^3} \\
&= \frac{(2 - z - \sqrt{1-4z} - \sqrt{1-6z+z^2})(1-z) + 2(z^2-1)}{(2 - z - \sqrt{1-4z} - \sqrt{1-6z+z^2})(1-z-z^2) + 2(z^3+z^2+z-1)}. \quad (5.27)
\end{aligned}$$

Appendix A. Semisimple Algebras

Definition A.1. Let R be a ring with unity. Let $x \in R$. We say that x is **nilpotent** if there exists some positive integer n such that $x^n = 0$. If I is a subset of R, we say that I is **nilpotent** if there exists some positive integer n such that $I^n = 0$.

Definition A.2. Let R be a ring and let $\boldsymbol{Z(R)} = \{x \in R \mid xr = rx \text{ for all } r \in R\}$. Then $Z(R)$ is called the **center** of R. We say that $x \in R$ is **central** if $x \in Z(R)$.

It is clear that $Z(R)$ is a subring of R.

Proposition A.3. *Suppose that x is a central element in a ring R such that $x^n = 0$ for some positive integer n. Then Rx is a nilpotent 2-sided ideal of R with $(Rx)^n = 0$.*

Proof. Let $s_i \in R$ for $1 \leq i \leq n$. Then $\prod_{i=1}^n s_i x = \prod_{i=1}^n s_i \cdot \prod_{i=1}^n x = \left(\prod_{i=1}^n s_i\right) x^n = 0$, where the first equality holds since x is central. Therefore, $(xR)^n = 0$. □

Corollary A.4. *Suppose that R is a commutative ring. Then x is nilpotent if and only if xR is nilpotent.* □

Definition A.5. Let R be a ring and M be a left R-module. Then $M \neq 0$ is **simple** if it has no nontrivial, proper submodules.

Definition A.6. Let R be a ring. We define the **Jacobson Radical** of R, denoted by $\boldsymbol{\mathcal{J}(R)}$, to be the intersection of all maximal left (equivalently, right) ideals of R.

Now, a simple left R-module M is of the form $M \cong R/I$, where I is a maximal left ideal of R. Thus, $\mathcal{J}(R)$ is the intersection of all the annihilators of simple left R-modules. In particular, $\mathcal{J}(R)$ is a 2-sided ideal of R since the annihilators of left modules are 2-sided ideals.

Lemma A.7 (Nakayama's Lemma)**.** *Let V be a finitely generated, nonzero R-module. Then*

$$\mathcal{J}(R)V \subsetneq V.$$

Proof. Let V' be a maximal submodule of V. The existence of such a maximal submodule is guaranteed by the fact that V is a nonzero, finitely generated module and a typical Zorn's lemma argument. Thus, V/V' is a simple module. So, $\mathcal{J}(R)(V/V') = 0$, which implies that $\mathcal{J}(R)V \subseteq V' \subsetneq V$. □

Proposition A.8. *If I is a nilpotent left ideal of R, then $I \subseteq \mathcal{J}(R)$.*

Proof. Since I is nilpotent, there exists some positive integer m such that $I^m = 0$. Let U be a simple left R-module. If $IU \neq 0$, then by the irreducibility of U, we have $U = IU$. Repeating this process gives

$$U = IU = I^2U = I^3U = \ldots = I^mU = 0,$$

which contradicts U being simple. Thus, $IU = 0$. Since U was an arbitrary simple module, $I \subseteq \mathcal{J}(R)$. □

Theorem A.9. *Let A be a left artinian ring. Then $\mathcal{J}(A)$ is the maximal nilpotent left ideal of A.*

Proof. We will first prove that $\mathcal{J}(A)$ is a nilpotent left ideal of A. Let $\mathcal{J} = \mathcal{J}(A)$. Consider the descending chain of left ideals

$$\mathcal{J} \supseteq \mathcal{J}^2 \supseteq \mathcal{J}^3 \supseteq \ldots$$

Since A is artinian, there exists some n such that $\mathcal{J}^n = \mathcal{J}^{n+1} = \mathcal{J}^{n+2} = \ldots$. But $\mathcal{J}(\mathcal{J}^n) = \mathcal{J}^{n+1} = \mathcal{J}^n$. Since A is artinian, A is also noetherian. This implies that $\mathcal{J}(A)$ is finitely generated. Then by Nakayama's lemma, $\mathcal{J}^n = 0$. So, $\mathcal{J}$ is nilpotent. By Proposition A.8, $\mathcal{J}$ is the maximal nilpotent left ideal. □

Definition A.10. Let R be a ring and M be a left R-module. Then we say M is **semisimple** if it is a direct sum of simple left modules. A ring R is **semisimple** if it is semisimple as a module over itself.

Theorem A.11. *The following are equivalent for a left R-module M.*

(a) M is semisimple.

(b) M is a sum (not necessarily direct) of simple modules.

(c) Every submodule of M is a direct summand of M.

Proof. See [3, Theorem 15.3] or [14, Theorem 2.4]. □

Theorem A.12. *Let A be a left (right) artinian ring. Then A is semisimple if and only if $\mathcal{J}(A) = 0$.*

Proof. Suppose that A is semisimple. Then there exists a left ideal I of A such that $A = I \oplus \mathcal{J}(A)$. If $\mathcal{J}(A) \neq 0$, then I is contained in a maximal left ideal M. But $I, \mathcal{J}(A) \subseteq M$, which implies that $M = R$, a contradiction. Thus, $\mathcal{J}(A) = 0$.

Suppose that $\mathcal{J}(A) = 0$. Let L_1 be a minimal left ideal of A. Since $\mathcal{J}(A) = 0$, there exists a maximal left ideal $M_1 \neq 0$ which does not contain L_1. Thus, $L_1 + M_1 = A$, by the maximality of M_1. By the minimality of L_1, we see $L_1 \cap M_1 = 0$. Therefore,

$$A = L_1 \oplus M_1.$$

Since $M_1 \neq 0$, it too contains a minimal left ideal L_2. Again, there exists a maximal left ideal M_2 which does not contain L_2 and

$$A = L_1 \oplus L_2 \oplus (M_1 \cap M_2).$$

Continuing in this fashion, we may define L_k and M_k recursively so long as $\bigcap_{j=1}^{k-1} M_j \neq 0$. If $\bigcap_{j=1}^{k-1} M_j \neq 0$ for all k, then we have a descending chain of left ideals

$$M_1 \supsetneq M_1 \cap M_2 \supsetneq M_1 \cap M_2 \cap M_3 \supsetneq \ldots,$$

a contradiction. Therefore,

$$A = L_1 \oplus L_2 \oplus \ldots \oplus L_k,$$

for some k, which proves that A is semisimple. □

Corollary A.13. *Let A be a semisimple ring. Then there exists minimal 2-sided ideals U_i, for $1 \leq i \leq r$, such that*

$$A = U_1 \oplus U_2 \oplus \ldots \oplus U_r.$$

Such a decomposition of a semisimple ring is called a ***Wedderburn decomposition****.*

Proof. Let $A = L_1 \oplus L_2 \oplus \ldots \oplus L_k$ be a decomposition of A into a direct sum of minimal left ideals, as in the previous proof. Suppose that there are r isomorphism types amongst the L_i as left A-modules. Reindexing if necessary, we may assume that $L_i \ncong L_j$ for $1 \leq i, j \leq r$. Let $U_j = \sum_{L \cong L_j} L$ for $1 \leq j \leq r$, that is, U_j is the sum of all left ideals of A isomorphic to L_j. In particular, $U_j = \bigoplus_{L_i \cong L_j} L_i$. Thus, $A = U_1 \oplus \ldots \oplus U_r$ and each U_j is a left ideal of A. Now, if $\alpha \in A$, then let $\varphi_\alpha : A \to A$ be the left A-module homomorphism sending $1 \mapsto \alpha$, that is, φ_α is the multiplication on the right by α. Thus, if L is a minimal left ideal of A, then $\varphi_\alpha(L) = L\alpha$ is a left idea and it must be that $L\alpha = 0$ or $L\alpha \cong L$. Thus, multiplication on the right by α permutes the summands of U_j. In particular, U_j is a 2-sided ideal. Let $L \cong L'$ be minimal left ideals. Then there is a left A-module isomorphism ψ which maps L onto L'. Let $\pi : A \to L$ be a projection, which exists by the semisimplicity of A. In particular, $\pi(L) = L$. Let $\mathrm{End}_A(A)$ be the set of all left A-module homomorphisms on A. Then the map $A \to \mathrm{End}_A(A)$ given by $\alpha \mapsto \varphi_\alpha$ is an isomorphism. Thus, $\psi\pi = \varphi_\alpha$ for some $\alpha \in A$ and $L\alpha = L'$. In particular, if I is an ideal of A, it must contain a minimal left ideal L. Since it is also a 2-sided ideal, it must contain $L\alpha$ for all $\alpha \in A$, which implies that $U_j \subseteq I$ for some j such that $L_j \cong L$. Therefore, each U_j is a minimal 2-sided ideal. □

Corollary A.14. *Let A be a semisimple algebra and let T be a finite-dimensional central subalgebra of A. Then T is semisimple.*

Proof. Suppose to the contrary that T is not semisimple. Since T is a finite-dimensional algebra, T is artinian, and it must be that $\mathcal{J}(T) \neq 0$. Let $x \in \mathcal{J}(T)$ be nonzero. Thus, x is a nilpotent element of A. By Proposition A.3, Rx is a nonzero nilpotent ideal of A. Thus, $Rx \subseteq \mathcal{J}(A) \neq 0$, by Proposition A.8. This contradicts Theorem A.12. □

Definition A.15. An element ε of a ring R is **idempotent** if $\varepsilon^2 = \varepsilon$. A pair of central idempotents (δ, ε) is **orthogonal** if $\delta\varepsilon = 0$. We say that a central idempotent is **primitive** if it cannot be expressed as a sum of two nonzero orthogonal central idempotents. If the sum of a set of orthogonal idempotents is 1, we say that the set of idempotents is **complete**.

Every central idempotent of a semisimple ring is necessarily expressed uniquely as a sum of primitive central idempotents.

Theorem A.16. *Let A be a semisimple algebra with Wedderburn decomposition*

$$A = U_1 \oplus U_2 \oplus \ldots \oplus U_r.$$

If

$$1 = \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_r$$

for $\varepsilon_j \in U_j$, then $\{\varepsilon_j \mid 1 \leq j \leq r\}$ is a complete set of pairwise orthogonal, primitive, central idempotents. Furthermore, $U_j = A\varepsilon_j$ for each j.

Proof. Let $E = \{\varepsilon_j \mid 1 \leq j \leq r\}$. Multiplying the above equation by ε_j, we have

$$\varepsilon_j = \varepsilon_1\varepsilon_j + \varepsilon_2\varepsilon_j + \ldots + \varepsilon_r\varepsilon_j.$$

Since $\varepsilon_i\varepsilon_j \in U_i \cap U_j = 0$, the previous equation simplifies to $\varepsilon_j = \varepsilon_j^2$ for each j. Thus, E is a complete set of pairwise orthogonal idempotents.

Let $\alpha \in A$. Then

$$\alpha = \alpha\varepsilon_1 + \alpha\varepsilon_2 + \ldots + \alpha\varepsilon_r = \varepsilon_1\alpha + \varepsilon_2\alpha + \ldots + \varepsilon_r\alpha,$$

where $\alpha\varepsilon_j, \varepsilon_j\alpha \in U_j$. Since α can be uniquely expressed as a sum of elements from the U_j's, it holds that $\alpha\varepsilon_j = \varepsilon_j\alpha$ for all j, that is, ε_j is central. Since U_j is a minimal ideal for each j, we must have that $U_j = A\varepsilon_j A$. Since ε_j is central, we get $U_j = A\varepsilon_j$.

For primitivity, suppose that $\varepsilon_j = \varepsilon + \delta$ for two orthogonal central idempotents and $\varepsilon \neq 0$. Since $\varepsilon = \varepsilon(\varepsilon + \delta) = \varepsilon(\varepsilon_j) \in U_j$, it holds that $A\varepsilon \subseteq U_j$. Since $\varepsilon \neq 0$, the minimality of U_j implies $A\varepsilon = U_j$. In particular, there exists some $\alpha \in A$ such that $\varepsilon_j = \alpha\varepsilon$. Hence,

$$\varepsilon = (\varepsilon + \delta)\varepsilon = \varepsilon_j\varepsilon = \alpha\varepsilon^2 = \alpha\varepsilon = \varepsilon_j.$$

In particular, $\delta = 0$, which shows that ε_j is primitive for each j. □

In particular, each minimal ideal U_j in the Wedderburn decomposition of a semisimple ring A is a simple, artinian ring with identity ε_j. Thus, $U_j \cong M_{n_j}(D_j)$, where D_j is a division

ring and $M_{n_j}(D_j)$ is the ring of $n_j \times n_j$ matrices over D_j. When A is commutative, A is necessarily a finite direct product of fields.

Theorem A.17 (Maschke's Theorem)**.** *Let G be a finite group and let F be any field. Then the group algebra $F[G]$ is semisimple if and only if* $\operatorname{char} F \nmid |G|$.

Proof. Let $p = \operatorname{char} F$. First, suppose that $p \mid |G|$. Then, $\overline{G}^2 = |G| \cdot \overline{G} = 0$ (see Proposition 2.5). So, $\overline{G}$ is nilpotent. Since $\overline{G}$ is central, $(\overline{G})$ is a nilpotent ideal by Proposition A.3. Therefore, $(\overline{G}) \subseteq \mathcal{J}(F[G])$, which implies that $\mathcal{J}(F[G]) \neq 0$. Thus, $F[G]$ is not semisimple by Theorem A.12.

Conversely, suppose $F[G]$ is not semisimple, that is, $\mathcal{J}(F[G]) \neq 0$ (since $F[G]$ is necessarily artinian). Then we may choose a nonzero element $\alpha \in \mathcal{J}(F[G])$ such that $\alpha_1 = 1$. Since $\mathcal{J}(F[G])$ is nilpotent by Theorem A.9, α is also nilpotent. Using the left regular representation of $F[G]$, we may view α as an operator on $F[G]$, that is, the operator which multiplies on the left by α. Thus, α is a nilpotent operator, which implies that all the eigenvalues of α are 0. Thus, $\operatorname{Tr} \alpha = 0$. Alternatively, using the elements of G as a basis for $F[G]$, we see that all the diagonal entries of α are $\alpha_1 = 1$. Thus, $\operatorname{Tr} \alpha = |G|$. Hence, $|G| = 0$ in F, which implies that $p \mid |G|$. □

Appendix B. Orbit Algebras and Cyclotomic Fields

Let F be a field of characteristic zero. Let $\zeta_n = e^{2\pi i/n} \in \mathbb{C}$ and let $\mathcal{K}_n = \mathbb{Q}(\zeta_n) \subseteq \mathbb{C}$. Then, of course, ζ_n is a primitive nth root of unity and a root of the polynomial $x^n - 1 \in \mathbb{Z}[x]$. When the context is clear, the subscripts may be omitted. From Galois theory, we know there is a one-to-one correspondence between the subfields of the cyclotomic field $\mathcal{K}_n$ and the subgroups of the Galois group $\mathcal{G}(\mathcal{K}_n/\mathbb{Q})$. It is our first task to prove that each of these subfields is generated by sums of roots of unity, called **periods**.

Definition B.1. Let A be an algebra over a field F and let $\mathcal{H} \leq \mathrm{Aut}_F(A)$ be finite, where $\mathrm{Aut}_F(A)$ is the group of F-algebra automorphisms of A. Then

$$\boldsymbol{A^{\mathcal{H}}} = \{\alpha \in A \mid \sigma(\alpha) = \alpha, \text{ for all } \sigma \in \mathcal{H}\}.$$

Such a set is referred to as an **orbit algebra**.

Proposition B.2. *Let A be an algebra over a field F and let $\mathcal{H} \leq \mathrm{Aut}_F(A)$. Then the orbit algebra $A^{\mathcal{H}}$ is the largest subalgebra of A that is fixed by all elements of $\mathcal{H}$.*

Proof. Let $\alpha, \beta \in A^{\mathcal{H}}$ and $r, s \in F$. Then $\sigma(r\alpha + s\beta) = r\sigma(\alpha) + s\sigma(\beta) = r\alpha + s\beta$ and $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta$ for each $\sigma \in \mathcal{H}$. Thus, $A^{\mathcal{H}}$ is a subalgebra of A. Since $A^{\mathcal{H}}$ contains every $\mathcal{H}$-fixed element of A, it must contain all $\mathcal{H}$-fixed subalgebras. □

Theorem B.3. *Let A be an algebra over a field F and let $\mathcal{B}$ be a basis (or spanning set) for A. Let $\mathcal{H} \leq \mathrm{Aut}_F(A)$ be a finite subgroup. For each $\alpha \in A$, let $\mathcal{O}_\alpha = \{\sigma(\alpha) \mid \sigma \in \mathcal{H}\} \subseteq A$ denote the orbit of α with respect to $\mathcal{H}$ and let*

$$\boldsymbol{\eta_\alpha} = \sum_{\beta \in \mathcal{O}_\alpha} \beta$$

*denote the **period** of α with respect to $\mathcal{H}$. Then $A^{\mathcal{H}} = \mathrm{Span}_F\{\eta_\alpha \mid \alpha \in \mathcal{B}\}$, that is, $A^{\mathcal{H}}$ is spanned by the periods of a basis of A.*

This theorem is the reason orbit algebras have their name.

Proof. Certainly, for any $\sigma \in \mathcal{H}$,

$$\sigma(\eta_\alpha) = \sum_{\beta \in \mathcal{O}_\alpha} \sigma(\beta) = \sum_{\beta \in \mathcal{O}_\alpha} \beta = \eta_\alpha,$$

since σ permutes the elements of $\mathcal{O}_\alpha$. Thus, $\eta_\alpha \in A^{\mathcal{H}}$ and $\mathrm{Span}_F\{\eta_\alpha \mid \alpha \in \mathcal{B}\} \subseteq A^{\mathcal{H}}$.

Let $\eta'_\alpha = \sum_{\sigma \in \mathcal{H}} \sigma(\alpha)$ for each $\alpha \in A$. If $\mathcal{H}_\alpha = \{\sigma \in \mathcal{H} \mid \sigma(\alpha) = \alpha\}$ is the stabilizer of α in $\mathcal{H}$, then $\eta'_\alpha = |\mathcal{H}_\alpha|\eta_\alpha$.

Suppose $\gamma \in A^{\mathcal{H}}$ and $\gamma = \sum_{\beta \in \mathcal{B}} \gamma_\beta \beta$, where $\gamma_\beta \in F$. So $\gamma = \sigma(\gamma)$ for all $\sigma \in \mathcal{H}$. Then

$$\begin{aligned}
\gamma &= \frac{1}{|\mathcal{H}|} \sum_{\sigma \in \mathcal{H}} \sigma(\gamma) = \frac{1}{|\mathcal{H}|} \sum_{\sigma \in \mathcal{H}} \sigma \left(\sum_{\beta \in \mathcal{B}} \gamma_\beta \beta \right) \\
&= \frac{1}{|\mathcal{H}|} \sum_{\sigma \in \mathcal{H}} \sum_{\beta \in \mathcal{B}} \gamma_\beta \sigma(\beta) = \frac{1}{|\mathcal{H}|} \sum_{\beta \in \mathcal{B}} \sum_{\sigma \in \mathcal{H}} \gamma_\beta \sigma(\beta) \\
&= \frac{1}{|\mathcal{H}|} \sum_{\beta \in \mathcal{B}} \gamma_\beta \left(\sum_{\sigma \in \mathcal{H}} \sigma(\beta) \right) = \frac{1}{|\mathcal{H}|} \sum_{\beta \in \mathcal{B}} \gamma_\beta \eta'_\beta \\
&= \frac{1}{|\mathcal{H}|} \sum_{\beta \in \mathcal{B}} \gamma_\beta |\mathcal{H}_\beta| \eta_\beta \in \mathrm{Span}_F\{\eta_\alpha \mid \alpha \in \mathcal{B}\}.
\end{aligned}$$

Therefore, $A^{\mathcal{H}} \subseteq \mathrm{Span}_F\{\eta_\alpha \mid \alpha \in \mathcal{B}\}$. □

Let $\mathcal{G}_n$ denote the Galois group of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$.

Corollary B.4. *Let $\mathcal{H} \leq \mathcal{G}_n$. Then $\mathbb{Q}(\zeta_n)^{\mathcal{H}} = \mathbb{Q}(\eta_{\zeta_n^i} \mid 0 \leq i < n)$. Furthermore, by Galois correspondence, every subfield of the cyclotomic field is of this form.* □

We make no claim here that the periods form a basis for the orbit algebra. In fact, this is not true in general. In some circumstances, a period may be 0, as is often the case with cyclotomic fields. In the case of group rings, the periods of the group elements always form a basis for the orbit subalgebra.

For each divisor d of n, there is a natural quotient map $\mathcal{G}_n \to \mathcal{G}_d$ given by restriction, that is, each automorphism $\sigma\mathcal{K}_n \to \mathcal{K}_n$ maps to its restriction $\sigma|_{\mathcal{K}_d} : \mathcal{K}_d \to \mathcal{K}_d$. Thus, each subgroup $\mathcal{H} \leq \mathcal{G}_n$ induces a unique subgroup of $\mathcal{G}_d$. By abuse of notation, we will denote

this quotient group also as $\mathcal{H}$. Since $\mathcal{H}$ can be identified as a set of integers modulo n, we may also identify $\mathcal{H}$ with this same set of integers but now modulo d.

Corollary B.5. *Let $\mathcal{H} \leq \mathcal{G}_n$ and let $d \mid n$. Then*

$$\mathcal{K}_n^{\mathcal{H}} \cap \mathcal{K}_d = \mathcal{K}_d^{\mathcal{H}}.$$

Furthermore, $\mathcal{K}_d^{\mathcal{H}}$ is the maximal subfield of $\mathcal{K}_d$ contained in $\mathcal{K}_n^{\mathcal{H}}$.

Proof. By Corollary B.4, both fields are spanned by periods of ζ_d with respect to $\mathcal{H}$. So, they must be equal. □

Let A and B be F-algebras and let $\pi : A \to B$ be a surjective F-homomorphism. Let $\sigma : A \to A$ be an automorphism of A for which $\ker \pi$ is an invariant ideal. Then σ induces an automorphism of B. More specifically, if $\beta \in B$, then there exists some $\alpha \in A$ such that $\pi(\alpha) = \beta$. Then it is easy to check that $\beta \mapsto \pi(\sigma(\alpha))$ is an automorphism of B. We will denote this induced automorphism by σ_*. Thus, $\sigma_*(\pi(\alpha)) = \pi(\sigma(\alpha))$. Of course, all the automorphisms for which $\ker \pi$ is invariant form a subgroup of $\mathrm{Aut}_F(A)$. Furthermore, if $\ker \pi$ is invariant for all automorphisms in $\mathcal{H} \leq \mathrm{Aut}_F(G)$, then $\mathcal{H}_* = \{\sigma_* \mid \sigma \in \mathcal{H}\} \leq \mathrm{Aut}_F(B)$.

Theorem B.6. *Let A and B be F-algebras and $\pi : A \to B$ be a surjective F-algebra homomorphism. Suppose that $\mathcal{H} \leq \mathrm{Aut}_F(A)$ is a finite subgroup and $\ker \pi$ is invariant under $\mathcal{H}$. Then $\pi(A^{\mathcal{H}}) = B^{\mathcal{H}_*}$.*

Proof. Suppose that $\beta, \beta' \in B$ represent the same $\mathcal{H}_*$-orbit, that is, there exists some $\sigma_* \in \mathcal{H}_*$ such that $\sigma_*(\beta) = \beta'$. Now, there exists some $\alpha \in A$ such that $\pi(\alpha) = \beta$. Let $\sigma(\alpha) = \alpha'$, which represents the same $\mathcal{H}$-orbit in A. Now,

$$\begin{aligned} \pi(\alpha') &= \pi(\sigma(\alpha)) = \sigma_*(\pi(\alpha)) \\ &= \sigma_*(\beta) = \beta'. \end{aligned}$$

Next, suppose that $\alpha, \alpha' \in A$ represent the same $\mathcal{H}$-orbit, that is, there exists some $\sigma \in \mathcal{H}$ such that $\sigma(\alpha) = \alpha'$. Then

$$\sigma_*(\pi(\alpha)) = \pi(\sigma(\alpha)) = \pi(\alpha').$$

Thus, $\pi(\alpha)$ and $\pi(\alpha')$ represent that same $\mathcal{H}_*$-orbit in B. This proves that the image of an $\mathcal{H}$-orbit under π is a $\mathcal{H}_*$-orbit.

Let $\mathcal{O}$ be an $\mathcal{H}$-orbit in A and let $\alpha \in \mathcal{O}$, whose image under π is β. Next, we will set $c = |\{\sigma \in \mathcal{H} : \pi(\sigma(\alpha)) = \beta\}|$, that is, c is the number of solutions to the equation $\pi(\sigma(\alpha)) = \beta$, where σ is allowed to vary. Let $\alpha' \in \mathcal{O}$, whose image under π is β'. Let $\rho \in \mathcal{H}$ such that $\rho(\alpha) = \alpha'$. Now, suppose $\pi(\sigma(\alpha)) = \beta$ for some $\sigma \in \mathcal{H}$. Then

$$\begin{aligned} \pi(\rho\sigma(\alpha)) &= \pi \circ \rho(\sigma(\alpha)) = \rho_* \circ \pi(\sigma(\alpha)) \\ &= \rho_*(\beta) = \rho_*(\pi(\alpha)) \\ &= \pi(\rho(\alpha)) = \pi(\alpha') = \beta'. \end{aligned}$$

Thus, every solution to $\pi(\sigma(\alpha)) = \beta$ corresponds to a solution to $\pi(\sigma(\alpha')) = \beta'$. In particular,

$$c = |\{\sigma \in \mathcal{H} : \pi(\sigma(\alpha)) = \beta\}| = |\{\sigma \in \mathcal{H} : \pi(\sigma(\alpha)) = \beta'\}|.$$

If we combine this result with the result from above, $\pi(\mathcal{O})$ is an $\mathcal{H}_*$-orbit and each element of $\pi(\mathcal{O})$ has exactly c pre-images in $\mathcal{O}$. Hence,

$$\begin{aligned} \pi\left(\sum_{\sigma\in\mathcal{H}} \sigma(\alpha)\right) &= \sum_{\sigma\in\mathcal{H}} \pi(\sigma(\alpha)) = \sum_{\sigma\in\mathcal{H}} \sigma_*(\pi(\alpha)) \\ &= c \sum_{\tau\in\mathcal{H}_*} \tau(\beta). \end{aligned}$$

Now, $\sum_\sigma \sigma(\alpha)$ and $\sum_\tau \tau(\beta)$ generate $A^{\mathcal{H}}$ and $B^{\mathcal{H}_*}$, respectively, by Theorem B.3, which proves $\pi(A^{\mathcal{H}}) = B^{\mathcal{H}_*}$. □

Let $\varphi : G \to H$ be a surjective homomorphism between two finite groups such that $\ker\varphi$ is characteristic in G. Then $\varphi : \mathbb{Q}[G] \to \mathbb{Q}[H]$ satisfies the assumptions of Theorem B.6 and maps the orbit subalgebras of $\mathbb{Q}[G]$ onto the orbit subalgebras of $\mathbb{Q}[H]$.

Appendix C. Lattices of Cyclotomic Fields

The purpose of this section is to determine the shape of the lattice of subfields of $\mathcal{K}_n := \mathbb{Q}(\zeta_n)$. We know from Galois theory that this is determined by the Galois group $\mathcal{G}(\mathcal{K}_n/\mathbb{Q})$, that is, the lattice of subfields is lattice anti-isomorphic to the lattice of subgroups of $\mathcal{G}(\mathcal{K}_n/\mathbb{Q})$. By Lemma 4.1, we may identify $\mathcal{G}(\mathcal{K}_n/\mathbb{Q})$ with $\mathrm{Aut}(Z_n)$ and will denote their common isomorphism type as $\mathcal{G}_n$. For each integer m relatively prime to n, let σ_m denote the common automorphism of $\mathrm{Aut}(Z_n)$ and $\mathcal{G}(\mathcal{K}_n/\mathbb{Q})$ which is determined by m. Again, subscripts will be omitted when the context is clear.

By Lemma 4.1, we can calculate $\mathcal{G}_n$ by studying the cyclic group Z_n. The next result classifies the automorphism group of a cyclic group and hence the Galois group of a cyclotomic field.

Proposition C.1.

(a) $\mathrm{Aut}(Z_{2^k}) \cong Z_2 \times Z_{2^{k-2}}$, *for all* $k \geq 2$. *In the case that* $k = 1$, $\mathrm{Aut}(Z_2) = 1$.

(b) $\mathrm{Aut}(Z_{p^k}) \cong Z_{p^{k-1}(p-1)}$, *for* $k \geq 1$ *and* p *is an odd prime.*

(c) Let $n \geq 2$ *be an integer with prime factorization* $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ *and each* p_i *is a distinct prime. Then* $\mathrm{Aut}(Z_n) \cong \mathrm{Aut}(Z_{p_1^{k_1}}) \times \mathrm{Aut}(Z_{p_2^{k_2}}) \times \ldots \times \mathrm{Aut}(Z_{p_r^{k_r}})$.

Proof. See [4, p. 314]. □

Of special interest to our discussion will be the case when n is a power of a prime. In this case, the lattice of subfields is naturally *layered* by the powers of the prime. Let $G = Z_{p^n}$ and let $\mathcal{L}_{p^n}$ be the lattice of subfields of $\mathcal{K}_{p^n}$. For $k = 1$, we let the **first layer** of $\mathcal{L}_{p^n}$ be $\mathcal{L}_p$. For $k > 1$, the k**th layer** of $\mathcal{L}_{p^n}$ is $\mathcal{L}_{p^k} \setminus \mathcal{L}_{p^{k-1}}$. The **top layer** of $\mathcal{L}_{p^n}$ is the nth layer. In particular, the layers form a partition of $\mathcal{L}_{p^n}$.

By Proposition C.1, the Galois groups of powers of 2 behave differently from the Galois groups of powers of an odd prime. Thus, we must consider the two cases separately. We will address the odd prime case first, followed by 2^n.

Let us assume that p is an odd prime. Then, by Proposition C.1, $\mathcal{G}_{p^n}$ is a cyclic group. Galois theory tells us that the subfields of $\mathcal{K}_{p^n}$ correspond to subgroups of $\mathcal{G}$ and group theory tells us that the subgroups of a cyclic group correspond to the divisors of $|\mathcal{G}|$. Now, $|\mathcal{G}| = p^n - p^{n-1} = p^{n-1}(p-1)$. Let x denote the number of divisors of $p-1$. Then $\mathcal{G}$ has nx subgroups. In particular, when $n = 1$, $\mathcal{K}_p$ has x subfields, or in other words, $|\mathcal{L}_p| = x$. This last statement can be generalized, as follows:

Proposition C.2. *Let $\mathcal{K}_{p^n}$ be a cyclotomic field and p an odd prime. Then the kth layer of $\mathcal{L}_{p^n}$ contains x subfields, for all $1 \leq k \leq n$.*

Proof. By the discussion before this proposition, we know that $|\mathcal{L}_p| = x$. Suppose for induction that $|\mathcal{L}_{p^k} \smallsetminus \mathcal{L}_{p^{k-1}}| = x$ for all $k < \ell$. Thus,

$$\begin{aligned} |\mathcal{L}_{p^\ell}| &= \left|\bigcup_{k=1}^{\ell}(\mathcal{L}_{p^k} \smallsetminus \mathcal{L}_{p^{k-1}})\right| = \sum_{k=1}^{\ell} |\mathcal{L}_{p^k} \smallsetminus \mathcal{L}_{p^{k-1}}| \\ &= |\mathcal{L}_{p^\ell} \smallsetminus \mathcal{L}_{p^{\ell-1}}| + \sum_{k=1}^{\ell-1} |\mathcal{L}_{p^k} \smallsetminus \mathcal{L}_{p^{k-1}}| \\ &= |\mathcal{L}_{p^\ell} \smallsetminus \mathcal{L}_{p^{\ell-1}}| + (\ell-1)x, \end{aligned}$$

where the last equality follows by induction. Now, $|\mathcal{L}_{p^\ell}| = \ell x$. So solving for $|\mathcal{L}_{p^\ell} \smallsetminus \mathcal{L}_{p^{\ell-1}}|$ in the above equation, we see that the ℓth layer of $\mathcal{L}_{p^\ell}$ contains x subfields. □

Now that we know each layer contains the same number of fields, we prove that each layer is lattice-isomorphic to $\mathcal{L}_p$. Even more, if we make each layer of $\mathcal{L}_{p^n}$ into a weighted lattice via degrees of extensions, then we show that each layer is weighted-lattice-isomorphic to $\mathcal{L}_p$.

Lemma C.3. *Let p be a prime (even or odd) and $n > 1$. Then $[\mathcal{K}_{p^n} : \mathcal{K}_{p^{n-1}}] = p$.*

Proof. Since $[\mathcal{K}_{p^n} : \mathbb{Q}] = p^{n-1}(p-1)$, we conclude that

$$p^{n-1}(p-1) = [\mathcal{K}_{p^n} : \mathbb{Q}] = [\mathcal{K}_{p^n} : \mathcal{K}_{p^{n-1}}][\mathcal{K}_{p^{n-1}} : \mathbb{Q}] = p^{n-2}(p-1)[\mathcal{K}_{p^n} : \mathcal{K}_{p^{n-1}}].$$

Therefore, $[\mathcal{K}_{p^n} : \mathcal{K}_{p^{n-1}}] = p$. □

Of course, if $n = 1$, then $[\mathcal{K}_{p^1} : \mathcal{K}_{p^{1-1}}] = [\mathcal{K}_p : \mathbb{Q}] = p - 1$.

Proposition C.4. *Let p be an odd prime and let F be a field in the nth layer. Then $p \nmid [\mathcal{K}_{p^n} : F]$.*

Proof. Let $[\mathcal{K}_{p^n} : F] = a$. We will first consider the case $n = 1$. Since $F \in \mathcal{L}_p$, we have that $F \subseteq \mathcal{K}_p$ and $[\mathcal{K}_p : \mathbb{Q}] = p - 1$. Since $[\mathcal{K}_p : \mathbb{Q}] = [\mathcal{K}_p : F][F : \mathbb{Q}] = a[F : \mathbb{Q}]$, it must be that a divides $p - 1$. Since $p \nmid (p - 1)$, we conclude that $p \nmid a$.

Next, let us suppose that $n > 1$. Now, there exists a subgroup $\mathcal{H} \leq \mathcal{G}_{p^n}$ such that $F = \mathcal{K}_{p^n}^{\mathcal{H}}$. Furthermore, $|\mathcal{H}| = a$. Suppose that $p \mid a$. Then $\mathcal{H}$ would contain a subgroup of order p, call it $\mathcal{P}$. Let $E = \mathcal{K}_{p^n}^{\mathcal{P}}$. Then $F \subseteq E$ and $[\mathcal{K}_{p^n} : E] = p$. But $\mathcal{G}_{p^n}$ is cyclic and has a unique subgroup of order p. By the Galois correspondence, $\mathcal{K}_{p^n}$ has a unique subfield E such that $[\mathcal{K}_{p^n} : E] = p$. But $[\mathcal{K}_{p^n} : \mathcal{K}_{p^{n-1}}] = p$. Therefore, $E = \mathcal{K}_{p^{n-1}}$, which implies that $F \in \mathcal{L}_{p^{n-1}}$, a contradiction. Therefore, $p \nmid a$. □

Proposition C.5. *Let p be an odd prime and F be a field in the kth layer. Then for all $n \geq k$, we have $[\mathcal{K}_{p^n} : F] = p^{n-k}a$ for some $a \mid (p - 1)$ determined by F. In particular, if $F = \mathcal{K}_{p^k}^{\mathcal{H}}$, for $\mathcal{H} \leq \mathcal{G}_{p^k}$, then $a = |\mathcal{H}|$.*

Proof. Let $k = n$. Then $[\mathcal{K}_{p^k} : F] = |\mathcal{H}| = p^{k-k}|\mathcal{H}|$ and $|\mathcal{H}| \mid (p - 1)$, by Proposition C.4. Suppose for induction that the statement holds for all $k < \ell$. Then

$$[\mathcal{K}_{p^\ell} : F] = [\mathcal{K}_{p^\ell} : \mathcal{K}_{p^{\ell-1}}][\mathcal{K}_{p^{\ell-1}} : F] = p[\mathcal{K}_{p^{\ell-1}} : F] = p(p^{(\ell-1)-k}|\mathcal{H}|) = p^{\ell-k}|\mathcal{H}|.$$ □

Let $\gcd(m, n) = 1$, so $\sigma_m : \mathcal{K}_n \to \mathcal{K}_n$ is a field automorphism. Now, the restriction of σ_m to $\mathcal{K}_d$, for $d \mid n$, is an automorphism of $\mathcal{K}_d \to \mathcal{K}_d$. Thus, any subgroup $\mathcal{H} \leq \mathcal{G}_n$ also denotes a subgroup $\mathcal{H} \leq \mathcal{K}_d$ for each divisor $d \mid n$.

Proposition C.6. *Let p be an odd prime, let $\mathcal{H} \leq \mathcal{G}_{p^n}$, and let $\mathcal{K}_{p^n}^{\mathcal{H}}$ be in the nth layer. Then $\left[\mathcal{K}_{p^n} : \mathcal{K}_{p^n}^{\mathcal{H}}\right] = \left[\mathcal{K}_{p^k} : \mathcal{K}_{p^k}^{\mathcal{H}}\right]$ for all $1 \leq k \leq n$.*

Proof. Let $E = \mathcal{K}_{p^n}^{\mathcal{H}}$ and $F = \mathcal{K}_{p^k}^{\mathcal{H}}$. Then $F \subseteq E$. By Proposition C.5, there exists $a, b \mid (p-1)$ such that $[\mathcal{K}_{p^n} : E] = a$ and $[\mathcal{K}_{p^n} : F] = p^{n-k}b$. Also,

$$p^{n-k}b = [\mathcal{K}_{p^n} : F] = [\mathcal{K}_{p^n} : E][E : F] = a[E : F].$$

Since $a \mid p^{n-k}b$ and $\gcd(a,p) = 1$, we conclude that $a \mid b$. But a is the order of $\mathcal{H}$ as a subgroup of $\mathcal{G}_{p^n}$ and b is the order of $\mathcal{H}$ as a subgroup of $\mathcal{G}_{p^k}$, also by Proposition C.5. Thus, $b \mid a$, which implies equality. Therefore,

$$[\mathcal{K}_{p^n} : E] = a = b = [\mathcal{K}_{p^k} : F]. \qquad \square$$

By Corollary B.5, $\mathcal{K}_{p^k}^{\mathcal{H}} = \mathcal{K}_{p^n}^{\mathcal{H}} \cap \mathcal{K}_{p^k}$.

Proposition C.7. *Let p be odd and $n > 1$. If F is a field in the nth layer, then there exists a unique subfield K in the $(n-1)$th layer such that $|F : K| = p$. Furthermore, K is the largest field in its layer which is contained in F.*

Proof. Let $\mathcal{H}$ denote the subgroup of $\mathcal{G}_{p^n}$ which corresponds to F. So, $F = \mathcal{K}_{p^n}^{\mathcal{H}}$. Let $K = F \cap \mathcal{K}_{p^{n-1}}$. If $|\mathcal{H}| = a$, then we have that

$$a[F : K] = [\mathcal{K}_{p^n} : F][F : K] = [\mathcal{K}_{p^n} : K] = pa,$$

where the first and last equality follow from Proposition C.5 and Proposition C.6. Thus, $|F : K| = p$. By Corollary B.5, K is the maximal subfield in $\mathcal{L}_{p^{n-1}}$ contained in F. Since $[\mathcal{K}_{p^n} : K] = pa$, it must be that $K \in \mathcal{L}_{p^{n-1}} \setminus \mathcal{L}_{p^{n-2}}$, otherwise Proposition C.5 would be contradicted. $\square$

Proposition C.8. *Suppose p is an odd prime, $n > 1$, and E and F are fields in the nth layer such that $E \subseteq F$. Let E' and F' be the maximal subfields of E and F, respectively, contained in the $(n-1)$th layer, as determined by Proposition C.7. Then $E' \subseteq F'$.*

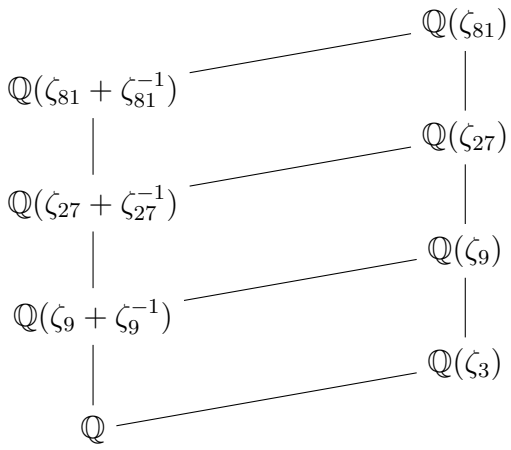
Proof. Let $F = \mathcal{K}_{p^n}^{\mathcal{H}}$. The field E is fixed by $\mathcal{H}$, since $E \subseteq F$, which implies that E' is fixed by $\mathcal{H}$. Thus, $E' \subseteq \mathcal{K}_{p^{n-1}}^{\mathcal{H}}$. But by Proposition C.7, the fields $\mathcal{K}_{p^{n-1}}^{\mathcal{H}}$ and F' are equal, which finishes the proof. $\square$

In summary, Proposition C.7 determines a map between the top two layers of $\mathcal{L}_{p^n}$, which is a one-to-one correspondence by Proposition C.2. Next, Proposition C.8 shows that this correspondence preserves containment of fields and is a lattice-isomorphism. By induction, every layer of $\mathcal{L}_{p^n}$ is lattice isomorphic to $\mathcal{L}_p$. Furthermore, each layer sits on top of the one

before by a degree p extension for each field in the layer. This synopsis gives a complete method to build the lattice of subfields for $\mathcal{K}_{p^n}$. We now will illustrate a few primes below.

Example C.9. Let us begin with $p = 3$. Since $p-1 = 2$, we have that $x = 2$, which implies that each layer of $\mathcal{L}_{3^n}$ contains exactly 2 fields. The two fields contained in $\mathcal{L}_3$ are obvious: $\mathbb{Q}$ and $\mathbb{Q}(\zeta_3)$. For higher layers, the two fields must be $\mathbb{Q}(\zeta_{3^n})$ and $\mathbb{Q}(\zeta_{3^n}) \cap \mathbb{R} = \mathbb{Q}(\zeta_{3^n} + \zeta_{3^n}^{-1})$. The complete lattice of subfields of $\mathbb{Q}(\zeta_{81})$ is given in Figure C.1.

Figure C.1: The Lattice of Subfields of $\mathbb{Q}(\zeta_{81})$.

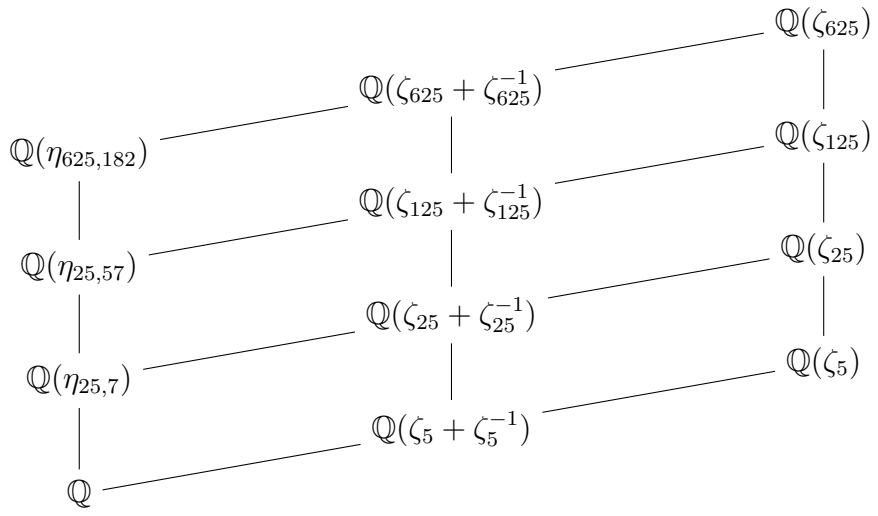


Now, $x = 2$ if and only if $p - 1$ is prime. Since 2 and 3 are the only consecutive prime numbers, $p = 3$ is the only case for which each layer contains exactly 2 fields. ∎

Example C.10. In this example, we will consider $p = 5$. Since $p - 1 = 4$, we have $x = 3$ and thus each layer contains 3 fields. For the first layer, $\mathcal{L}_p$ contains $\mathbb{Q}$ and $\mathbb{Q}(\zeta_5)$ obviously. The remaining field is $\mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\zeta_5 + \zeta_5^{-1})$. For higher layers, $\mathbb{Q}(\zeta_{5^n})$ and $\mathbb{Q}(\zeta_{5^n}) \cap \mathbb{R} = \mathbb{Q}(\zeta_{5^n} + \zeta_{5^n}^{-1})$ are always contained. The third field represents the maximal p-extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_{5^n})$. Let $\eta_{n,a}$ be the period of ζ_n with respect to $\langle \sigma_a \rangle$. With this notion, the complete lattice of subfields of $\mathbb{Q}(\zeta_{625})$ is given in Figure C.2 on page 117.

Now, $x = 3$ if and only if $p - 1 = q^2$ for some prime number q. Thus, $p = q^2 + 1$. For $p = 5$, clearly $q = 2$. If q is an odd prime, then $q^2 + 1$ is even and not a prime number. Therefore, $p = 5$ is the only case for which each layer contains exactly 3 fields. ∎

Figure C.2: The Lattice of Subfields of $\mathbb{Q}(\zeta_{5^4})$.



Example C.11. In this last example, we will consider $p = 7$. Since $p - 1 = 6$, we have $x = 4$ and thus each layer contains four fields. The complete lattice of subfields of $\mathbb{Q}(\zeta_{343})$ is given in Figure C.3 on page 118. Now, for many primes it is true that $x = 4$. For example, $p = 11, 23, 47, 59$, and 83 also satisfy $x = 4$. All of their respective lattices of fields will be isomorphic. ∎

Next, we will switch our attention to the case when $p = 2$. As seen in Proposition C.1, $\mathcal{G}_{2^n} \cong Z_2 \times Z_{2^{n-2}}$ for $n \geq 2$ and $\mathcal{G}_2 = 1$. In particular, $\mathcal{G}_4 \cong Z_2$, and hence $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$ contains two subfields: $\mathbb{Q}(i)$ and $\mathbb{Q}$.

For $\mathbb{Q}(\zeta_8)$, we have that $\mathcal{G}_8 \cong Z_2 \times Z_2$, the Klein 4-group. Thus, $\mathbb{Q}(\zeta_8)$ has 5 subfields: $\mathbb{Q}, \mathbb{Q}(i), \mathbb{Q}(\zeta_8), \mathbb{Q}(\zeta_8+\zeta_8^{-1}), \mathbb{Q}(\zeta_8+\zeta_8^3)$. It is also simple to show that $\mathbb{Q}(\zeta_8+\zeta_8^{-1}) = \mathbb{Q}(\zeta_8)\cap\mathbb{R} = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\zeta_8+\zeta_8^3) = \mathbb{Q}(i\sqrt{2})$, and $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$. Thus, $\mathcal{L}_8$ can be calculated as in Figure C.4 on page 118.

For the fourth layer of the lattice, we notice that $\mathcal{G}_{16} \cong Z_2 \times Z_4$ contains a copy of $Z_2 \times Z_2$ and hence contains three additional subgroups: two subgroups of order 4 and a subgroup of order 8. Thus, $\mathcal{L}_{16}$ contains three additional fields outside of $\mathcal{L}_8$ by Galois correspondence. These fields are in fact $\mathbb{Q}(\zeta_{16}) = \mathbb{Q}\left(i, \sqrt{2+\sqrt{2}}\right)$, $\mathbb{Q}(\zeta_{16}+\zeta_{16}^{-1}) = \mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$, and $\mathbb{Q}(\zeta_{16}+\zeta_{16}^{7}) = \mathbb{Q}\left(i\sqrt{2+\sqrt{2}}\right)$. The complete lattice $\mathcal{L}_{16}$ is depicted in Figure C.5 on page 119.

Figure C.3: The Lattice of Subfields of $\mathbb{Q}(\zeta_{7^4})$.

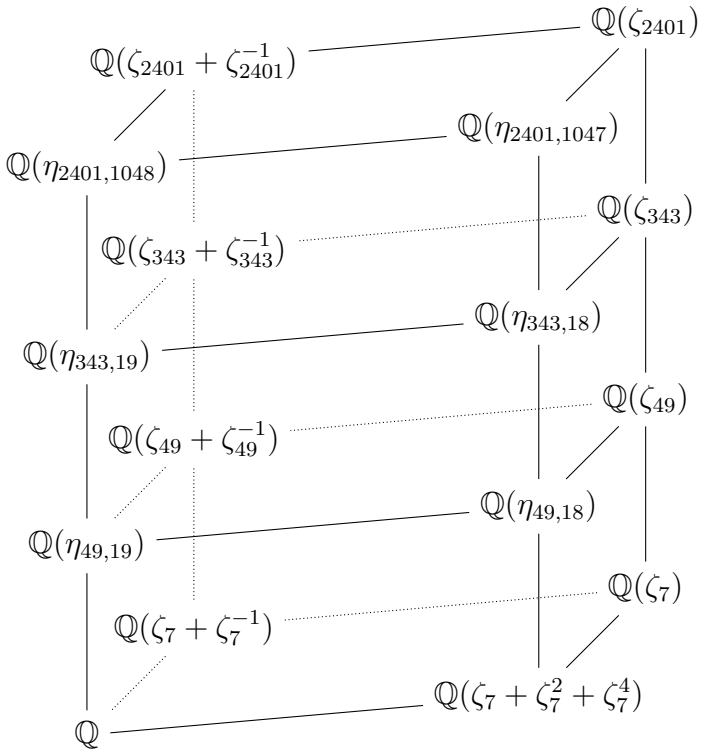


Figure C.4: The Lattice of Subfields of $\mathbb{Q}(\zeta_8)$.

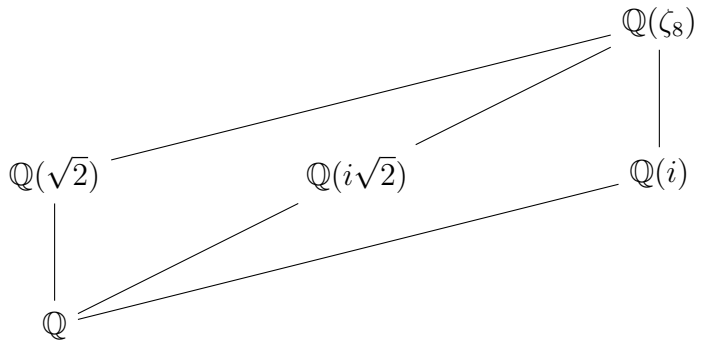
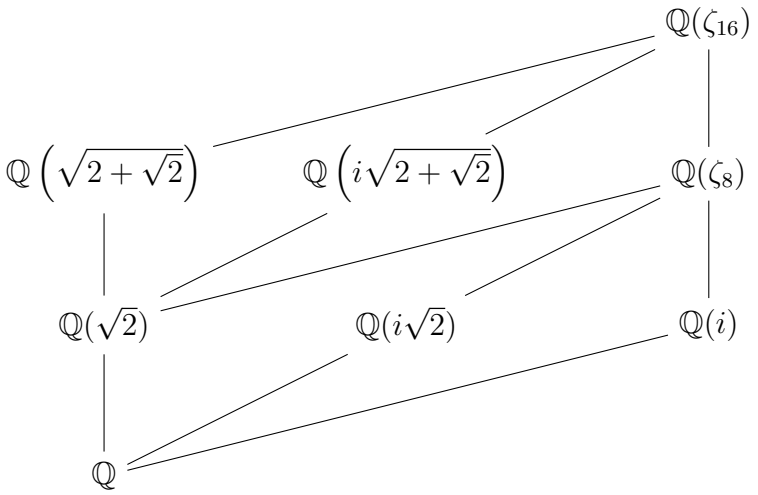


Figure C.5: The Lattice of Subfields of $\mathbb{Q}(\zeta_{16})$.



In general, it is true that $Z_2 \times Z_{2^{n-2}}$ has three more subgroups than $Z_2 \times Z_{2^{n-3}}$, and hence $\mathcal{L}_{2^n}$ has three more fields than $\mathcal{L}_{2^{n-1}}$ for $n \geq 3$. One of the fields is certainly $\mathbb{Q}(\zeta_{2^n})$. Since $\mathcal{G}_{2^n}$ is a 2-group, the remaining two fields must correspond to subgroups of $\mathcal{G}_{2^n}$ of order 2. The group $Z_2 \times Z_{2^{n-2}}$ has three elements of order 2. In particular, $\sigma_{2^n-1}, \sigma_{2^{n-1}-1}$, and $\sigma_{2^{n-1}+1}$ have order 2 in $\mathcal{G}_{2^n}$. But $\zeta^{2^{n-1}} = -1$. So $\zeta + \zeta^{2^{n-1}+1} = \zeta - \zeta = 0$. Hence, $\mathbb{Q}(\zeta_{2^n})^{\langle \sigma_{2^{n-1}+1} \rangle} \subseteq \mathbb{Q}(\zeta_{2^{n-1}})$, which implies that $\mathbb{Q}(\zeta_{2^n})^{\langle \sigma_{2^{n-1}+1} \rangle} = \mathbb{Q}(\zeta_{2^{n-1}})$ by degree considerations. Therefore, the additional two fields are $\mathbb{Q}(\zeta + \zeta^{-1})$ and $\mathbb{Q}(\zeta - \zeta^{-1})$.

Next, we notice that $\mathbb{Q}(\zeta_{2^n})^{\langle \sigma_{2^n-1} \rangle} \cap \mathbb{Q}(\zeta_{2^{n-1}}) = \mathbb{Q}(\zeta_{2^n})^{\langle \sigma_{2^{n-1}-1} \rangle} \cap \mathbb{Q}(\zeta_{2^{n-1}}) = \mathbb{Q}(\zeta_{2^{n-1}})^{\langle \sigma_{2^{n-1}-1} \rangle}$ $= \mathbb{Q}(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1})$, by induction. Also, the automorphisms σ_{2^n-1} and $\sigma_{2^{n-1}-1}$ are contained in exactly one subgroup of order 4 in $\mathcal{G}_{2^n}$, which corresponds to $\mathbb{Q}(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1})$. Furthermore, since

$$(\zeta_{2^n} + \zeta_{2^n}^{-1})^2 = \zeta_{2^n}^2 + 2 + \zeta_{2^n}^{-2} = 2 + (\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1}),$$

by induction we may conclude that

$$\zeta_{2^n} + \zeta_{2^n}^{-1} = \sqrt{2 + \sqrt{2 + \sqrt{\cdots + \sqrt{2}}}} \qquad (n-2) \text{ times}$$

for $n \geq 3$. By a similar argument,

$$\zeta_{2^n} - \zeta_{2^n}^{-1} = \sqrt{-2 + \sqrt{2 + \sqrt{\cdots + \sqrt{2}}}} \qquad (n-2) \text{ times}$$

for $n \geq 3$. In particular, $\mathbb{Q}(\zeta - \zeta^{-1}) = \mathbb{Q}(\zeta^{2^{n-2}}(\zeta - \zeta^{-1})) = \mathbb{Q}(i(\zeta + \zeta^{-1}))$. Furthermore, by the half-angle formula for cosine,

$$\cos(\theta/2) = \pm\sqrt{\frac{1 + \cos(\theta)}{2}},$$

we can write

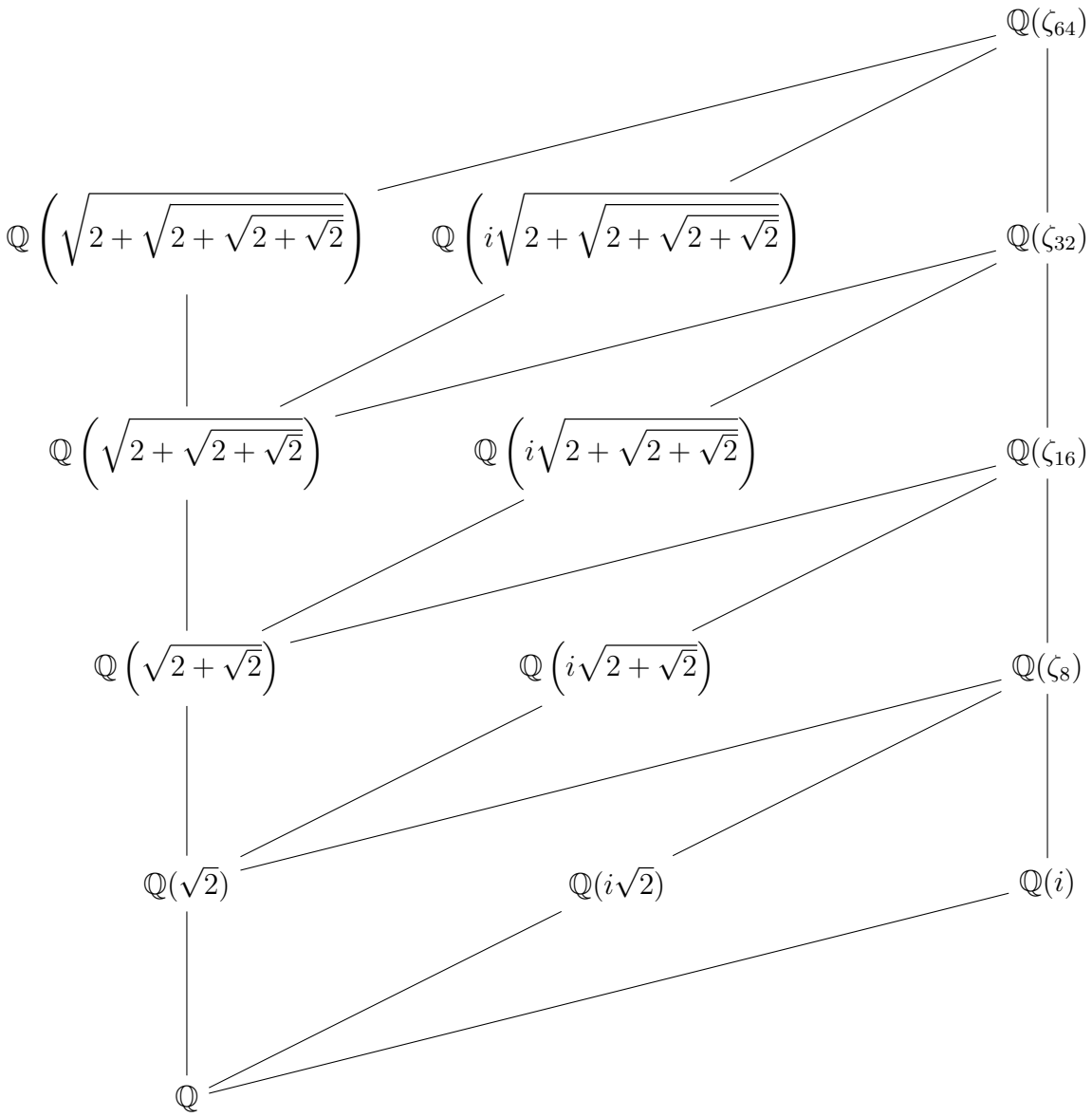
$$\zeta_{2^n} + \zeta_{2^n}^{-1} = 2\cos(\pi/2^{n-1})$$

for $n \geq 3$. We summarize these statements about $\mathbb{Q}(\zeta_{2^n})$ in the following Proposition.

Proposition C.12. *Let $n \geq 3$. Then the lattice $\mathcal{L}_{2^n}$ of subfields of $\mathbb{Q}(\zeta_{2^n})$ is built inductively from $\mathcal{L}_{2^{n-1}}$ by adding three fields: $\mathbb{Q}(2\cos(\pi/2^{n-1}))$, $\mathbb{Q}(2i\cos(\pi/2^{n-1}))$, and $\mathbb{Q}(\zeta_{2^n}) = \mathbb{Q}(i, 2\cos(\pi/2^{n-1}))$. Furthermore, $\mathbb{Q}(\zeta_{2^n})$ is immediately above the other two fields and $\mathbb{Q}(\zeta_{2^{n-1}})$, and the other two fields are only immediately above $\mathbb{Q}(2\cos(\pi/2^{n-2}))$.*

To illustrate Proposition C.12, we construct $\mathcal{L}_{64}$ in Figure C.6 on page 121.

Figure C.6: The Lattice of Subfields of $\mathbb{Q}(\zeta_{64})$.



Appendix D. Magma Code

Many of the examples and counterexamples included in this dissertation were computed using the programing language Magma, as well as many examples not included here. We will now include much of the relevant Magma code that was used in the development of this dissertation. Several collections of code are given below, each prefaced with a short explanation of its purpose.

This first collection of code was written to compute all the Schur rings over the cyclic group Z_{p^n}, where p is any prime. Brent Kerby [11] also has written a Magma program which accomplishes this same task for arbitrary cyclic groups. His code utilizes Leung-Man's classification of Schur rings over cyclic groups. His code was well written and calculated the correct number of Schur rings over Z_{3^6} in 467.810 seconds. Using the techniques of Chapter 4 and Chapter 5, the author was able to write a faster program in the special case of cyclic p-groups.

Following suit from Kerby's code, each Schur ring is denoted in the program by its corresponding partition of Z_{p^n}, instead of the subalgebra itself. The author's first attempt at computing all Schur partitions involved representing each partition as a set of sets of group elements from `CyclicGroup(GrpPC, p^n)`. This approach proved to be faster than Kerby's code, computing the Schur rings over Z_{3^6} in 78.89 seconds, but it was more clumsy than it needed to be. First of all, the cyclic group calculations need not take place in the Magma group object; instead these calculations could be done solely with integers. This modification improved the calculation on Z_{3^6} to 5.200 seconds. The next improvement to the code was the change from sets of sets to arrays of arrays. The set object in Magma uses more memory and is slower to work with than the array object. With this second modification, the program was able to compute the Schur rings over Z_{3^6} in 3.660. This represents the final version of the program. `SRings(p, n)` computes the set of all Schur rings over Z_{p^n}. `SRingsMemory` is an alternative version of `SRings` which takes an additional parameter, the set of all Schur rings over smaller cyclic groups. This speeds up the program by avoiding unnecessary recursion by using data that has already been computed.

```
/////////Set Operations Defined on Arrays////////
ArrayIsSub := function(A, B);
// Given two arrays,
// returns true if everything in A is also contained in B.
     return &and [A[i] in B : i in [1..#A]];
end function;

ArrayDiff := function(A, B);
// Given two arrays A and B without repetition,
// returns the subarray of A which excludes all entries from B.
     for i := 1 to #B do
          Exclude(~A, B[i]);
     end for;
     return A;
end function;

ArrayAppend := procedure(~A, x);
// Given an array and element,
// returns the appended array with element attached
     if not x in A
          then Append(~A, x);
     end if;
end procedure;

ArrayMeet := function(A, B);
// Given two arrays A and B without repetitions,
// returns the intersection of the two arrays.
     AB := [];
     for i := 1 to #A do
          if A[i] in B
```

```
                then Append(~AB, A[i]);
            end if;
        end for;
        return AB;
end function;

ArrayJoin := function(A, B);
// Given two arrays A and B without repetitions,
// returns the union of the two arrays.
        A := ArrayDiff(A, B);
        return A cat B;
end function;

ArrayMultiJoin := function(arrays);
// Iterates ArrayJoin.
        union := [];
        for i := 1 to #arrays do
            union := ArrayJoin(union, arrays[i]);
        end for;
        return union;
end function;

///////Internal Operations for Building and Modifying Schur Rings////////
IncludeSRing := function(sring, p, k, n)
// Given a Schur ring over Z_(p^k) and an integer n larger than k,
// returns sring as an immersed Schur ring of Z_(p^n).
        S := [];
        for i := 1 to #sring do
            S[i] := [a*p^(n-k) : a in sring[i]];
        end for;
```

```
     return S;
end function;

Layer := function(p, k, n);
// Given a cyclic of order p^n and a positive integer k less than n,
// returns the unique subgroup of order p^k.
     return [x*p^(n-k) : x in  [0..p^k-1]];
end function;

ImmersedSRing := function(sring, p, n, k);
// Given a Schur ring over a cyclic group of order p^n and a subgroup K of
// order p^k,
// returns the partition of G containing only classes which intersect K.
     K := Layer(p, k, n);
     return [C : C in sring | ArrayMeet(K,C) ne [] ];
end function;

RemoveSubgroup := function(sring, p, n, k);
// Given a Schur ring over a cyclic group G of order p^n and a subgroup K of
// order p^k,
// returns the partition of G for which every class containing an element of
//  K is removed.
     return ArrayDiff(sring, ImmersedSRing(sring, p, n, k));
end function;

InflatedSRing := function(sring, p, n);
// Given a Schur ring over Z_(p^n),
// returns the inflated S-ring over Z_(p^(n+1)).
     H := Layer(p, 1, n+1);
     return [ &cat[ [x+h : x in C] : h in H] : C in sring];
```

```
end function;

MultiInflatedSRing := function(sring, p, n, r);
// Iterates InflatedSRing r-times.
     for i := 1 to r do
          sring := InflatedSRing(sring, p, n+i-1);
     end for;
     return sring;
end function;

forward SRing0;
DeflatedSRing := function(sring, p, n);
// Given an immersed Schur ring over Z_(p^n),
// returns the deflated Schur ring over Z_(p^(n-1)).
     if #sring eq 2
          then return SRing0(p, n-1);
     else
          S := { {x mod p^(n-1) : x in C} : C in sring};
          return [ Sort(Setseq(C)) : C in S];
     end if;
end function;

AutoClassCyc := function(x, r, n);
// Given an integer x, a modulus, n, and an integer r,
// returns the automorphism class of x with respect to the automorphism
//  group <r> in the ambient cyclic group Z_n.
     C := [x];
     b := (r*x) mod n;
     while b ne x do
          Append(~C, b);
```

```
          b := (r*b) mod n;
     end while;
     return Sort(C);
end function;

//////////////Boolean Operators on Schur Rings/////////////////////
AreSRingsEqual := function(S, T);
// Given two Schur rings,
// returns true if they are the same.
     if #S ne #T
          then return false;
     else
          bool := true;
          for i := 1 to #S do
               bool and:= S[i] in T;
          end for;
          return bool;
     end if;
end function;

IsSset := function(H, sring);
// Given a Schur ring over a group G and a sorted subset H of G,
// returns if true if the sum of H is an element of sring.
     S := &cat [C : C in sring | #ArrayMeet(C,H) ne 0];
     return Sort(S) eq H;
end function;

InverseClass := function(C, p, n);
// Given a subset C of a cyclic group of order p^n,
// returns the inverse class of C.
```

```
     order := p^n;
     return Sort([ (-x) mod order : x in C]);
end function;

ClassProduct := function(C, D, p, n);
// Given two subsets of a cyclic group of order p^n,
// returns the product of sets in the group.
     order := p^n;
     return Sort(ArrayMultiJoin([ [(c + d) mod order : d in D] : c in C]));
end function;

IsSRing := function(sring, p, n);
// Given a partition of a cyclic group of order p^n,
// returns true if the partition affords a Schur ring.
     order := p^n;

     first := [0] in sring;
     second := &and [ InverseClass(C,p,n) in sring : C in sring];

     third := true;
     for C in sring do
          for D in sring do
               S := ClassProduct(C,D,p,n);
               third and:= IsSset(S,sring);
          end for;
     end for;

     return first and second and third;
end function;
```

```
IsCoset := function(C, p, n);
// Given a (sorted) subset of a cyclic group of order p^n,
// returns true if the subset is a coset of the group.
     if (#C) mod p eq 0 then
          order := p^n;
          H := Layer(p,1,n);
          bool := true;

          for x in C do
               bool and:= ArrayIsSub(Sort([(x + h) mod order : h in H]), C);
          end for;
          return bool;
     else
          return false;
     end if;
end function;

IsWedgePossible := function(p, nucleus, h, cloud, k, g);
// Given a Schur ring nucleus over H=Z_(p^h) and a Schur ring cloud
// over K=Z_(p^k),
// returns true if the semi-wedge product is possible over G = Z_(p^n).
// 1 < L < H < G, with K = G/L.
     DN := IncludeSRing(DeflatedSRing(nucleus, p, h),p, h-1, k);
     IC := ImmersedSRing(cloud, p, k, h-1);
     return AreSRingsEqual(IC, DN);
end function;

//////////////Constructing Schur Rings//////////////////////////
AutoSRingCyc := function(p, k, r);
// Given a finite cyclic group Z_{p^k} and an integer r,
```

```
// returns the partition of G corresponding to the orbit
// Schur ring induced by <r> < Aut(G).
     n := p^k;
     Sring := [[0]];
     g := [1..n-1];
     while not IsEmpty(g) do
          C := AutoClassCyc(g[1], r, n);
          Append(~Sring,C);
          for x in C do
               Exclude(~g,x);
          end for;
     end while;
     return Sring;
end function;

SRing0 := function(p, n);
// Given a cyclic group G of order p^n
// returns the trivial Schur ring over G.
     if n eq 0
          then return [ [0] ];
     else
          return [[0], [x : x in [1..p^n-1]] ];
     end if;
end function;


SymmetricSRing := function(p, n);
// Given a cyclic group G of order p^n
// returns the Symmetric S-ring over G.
     order := p^n;
```

```
     if p eq 2 then
          S := [ [0] ] cat [ [x, (-x) mod order] : x in [1..order div 2] ];
          return Prune(S) cat [ [order div 2]];
     else
          return [ [0] ] cat [ [x, (-x) mod order] : x in [1..(order div 2)] ];
     end if;
end function;

TopRationalSRings := function(p, n);
// Given a finite cyclic group G of order p^n,
// returns all the partitions of G which correspond to orbit Schur rings
// which are wedge-indecomposable.
     SRings := [];
     order := p^n;
     if p eq 2 then
          Z := Integers();
          SRings cat:= [ [ [x] : x in [0..order-1]] ];
          if n gt 2 then
               SRings cat:= [SymmetricSRing(p, n)];
               SRings cat:= [AutoSRingCyc(p, n, (p^(n-1)-1) mod order)];
          end if;
          return SRings;
     else
          q := p^(n-1);
          f := order - q;                    // EulerPhi(p^n);
          a := PrimitiveRoot(p^n);          // a generates Aut(G)
          for d in Divisors(p-1) do
               SRings cat:= [AutoSRingCyc(p, n, a^(q*d) mod order)];
          end for;
          return SRings;
```

```
     end if;
end function;

WedgeProduct := function(p, nucleus, h, cloud, k);
// Given two Schur rings, nucleus and cloud, over cyclic groups,
// Z_(p^h) and Z_(p^k), respectively,
// returns the wedge product (S wedge T) and the cyclic group Z_(p^(h+k)).
     g := h+k;
     nucleus := IncludeSRing(nucleus, p, h, g);
     R := MultiInflatedSRing(cloud, p, k, h);
     cloud := Remove(R, 1);
     return nucleus cat cloud;
end function;

TrivialWedgeProducts := function(p, h, srings, k);
// Given a cyclic group H=Z_(p^h) and a set of Schur rings over some cyclic
// group K=Z_(p^k),
// returns all wedge products over G=Z_(p^(h+k)) with nucleus the trivial
// Schur ring over H and clouds from srings.
     trivial := SRing0(p, h);
     return [WedgeProduct(p, trivial, h, cloud, k) : cloud in srings];
end function;

SemiWedgeProduct := function(p, nucleus, h, cloud, k, g);
// Given cyclic subgroups 1 < L < H < G, each cyclic p-groups and K = G/L,
// and given Schur rings nucleus and cloud over H and K, respectively,
// and H, K, and G have orders p^h, p^k, and p^g, respectively,
// returns the semi-wedge product (S wedge T).
     nucleus := IncludeSRing(nucleus, p, h, g);
     R := MultiInflatedSRing(cloud, p, k, g-k);
```

```
     cloud := RemoveSubgroup(R, p, g, h);
     return nucleus cat cloud;
end function;

SemiWedgeProducts := function(p, sring, h, srings, k, g);
// Given cyclic subgroups 1 < L < H < G, each cyclic p-groups and K = G/L,
// and given a Schur ring over H and a set of Schur rings over K,
// and H, K, and G have orders p^h, p^k, and p^g, respectively,
// returns all semiwedge products over G with nucleus sring and clouds
// from srings.
     SR := [];
     for i := 1 to #srings do
          if IsWedgePossible(p, sring, h, srings[i], k, g) then
               SR cat:= [SemiWedgeProduct(p, sring, h, srings[i], k, g)];
          end if;
     end for;
     return SR;
end function;

forward SRings;
SRings := function(p,n);
// Given a cyclic group G of prime power order p^n,
// returns the set of all Schur ring over G.
     if n eq 1
          then return TopRationalSRings(p, 1);
     else
          srings := [SRing0(p, n)];
          srings cat:= TopRationalSRings(p,n);

          sr := [];
```

```
          for i := 1 to n-1 do
               sr[i] := SRings(p, i);
          end for;

          srQ := sr[n-1];               //cloud

          for i := 1 to n-1 do
               srN := TopRationalSRings(p,i); //nucleus
               for s in srN do
                    srings cat:= SemiWedgeProducts(p,s, i, srQ, n-1, n);
               end for;
               if i gt 1 then
                    srH := sr[n-i];
                    srings  cat:= TrivialWedgeProducts(p, i, srH, n-i);
               end if;
          end for;

          return srings;
     end if;
end function;

SRingsMemory := function(p, n, SmallerSRings);
// Given a cyclic group G of prime power order p^n, and the set of all
// Schur rings over cyclic p-groups of smaller order,
// returns the set of all Schur ring over G.
     if n eq 1
          then return TopRationalSRings(p, 1);
     else
          srings := [SRing0(p, n)];
          srings cat:= TopRationalSRings(p, n);
```

```
        srQ := SmallerSRings[n-1];                  //cloud

        for i := 1 to n-1 do
            srN := TopRationalSRings(p, i); //nucleus
            for s in srN do
                srings cat:= SemiWedgeProducts(p, s, i, srQ, n-1, n);
            end for;
            if i gt 1 then
                srH := SmallerSRings[n-i];
                srings  cat:= TrivialWedgeProducts(p, i, srH, n-i);
            end if;
        end for;

        return srings;
    end if;
end function;
```

The next collection of code computes the same information as the previous code except it does so much more efficiently. This new efficiency is obtained by representing each Schur ring as a sequence of wedge-indecomposable Schur rings and integers and hence provides an encoded version of the Schur partition. The trivial Schur ring over Z_{p^n} is encoded as `[p, n, 0]`. Indecomposable orbit Schur rings over Z_{p^n} are afforded by certain cyclic subgroups of Aut(G). Each cyclic subgroup is generated by an integer r. Hence, the indecomposable orbit ring is encoded as `[p, n, r]`. Since $\gcd(r, p) = 1$, we know that $r \neq 0$. Also, we choose r to be the minimal integer which affords the Schur ring. Like in the above code, the functions `SRing0Code` creates the trivial Schur ring and `AutoSRingCycCode` creates the orbit Schur ring corresponding to r. In both case, the output is of the form `[ [p, n, r], [n] ]`. The extra `[n]` is included for the interpretation/decryption process.

Given two Schur ring codes S and T, `WedgeProductCode` and `SemiWedgeProductCode` create the wedge product and semi-wedge product of S and T, respectively. In either case, the encoded wedge product Schur ring $S \wedge T$ will be an array of wedge-indecomposable

factors intermingled with singletons of integers. The singletons `[k]` document the exponent of the order of $K = Z_{p^k}$ in the corresponding wedge decomposition $1 < K \leq H < G$ and act as a postfix binary operator. A few examples are included for clarity.

Example D.1. Let $p = 3$.

(a) The Schur ring $\mathbb{Q}[Z_3] \wedge \mathbb{Q}[Z_3]^0$ has order $3^2 = 9$ and is encoded as

```
[ [3, 1, 1], [3, 1, 0], [2] ].
```

(b) The Schur ring $\mathbb{Q}[Z_3] \wedge \mathbb{Q}[Z_3]^0 \wedge \mathcal{S}(Z_9)$ has order $3^4 = 81$ and is encoded as

```
[ [3, 1, 1], [3, 1, 0], [2], [3, 2, 8], [4] ].
```

(c) The Schur ring $\mathbb{Q}[Z_3] \wedge \mathbb{Q}[Z_3]^0 \wedge \mathcal{S}(Z_9) \wedge \mathbb{Q}[Z_3]^0$ has order $3^5 = 243$ and is encoded as

```
[ [3, 1, 1], [3, 1, 0], [2], [3, 2, 8], [4], [3, 1, 0], [5] ].
```

(d) The Schur ring $\mathcal{S}(Z_9) \triangle_{Z_3} \mathcal{S}(Z_9)$ has order $3^3 = 27$ is encoded as

```
[ [3, 2, 8], [3, 2, 8], [3] ].
```

(e) Finally, the Schur ring $(\mathcal{S}(Z_9) \triangle_{Z_3} \mathcal{S}(Z_9)) \wedge (\mathbb{Q}[Z_9] \triangle_{Z_3} \mathbb{Q}[Z_9])$ has order $3^6 = 729$ is encoded as

```
[ [3, 2, 8], [3, 2, 8], [3], [3, 2, 1], [3, 2, 1], [3], [6] ].
```

■

All the procedures and functions are used and called as the previous collection of code, using the same parameters, except now the additional suffix `Code` is appended to each function call. By comparison, the method of encoded Schur rings was able to compute all the Schur rings over Z_{3^6} in 0.25 seconds. To further emphasis the improvement, `SRings` computed the Schur rings over Z_{3^8} in 717.380 seconds, while `SRingsCode` computed the same

problem in 61.030 seconds. For practical purposes, `SRingDecrypt` was included to translate the encoded Schur rings into partitions of Z_{p^n}.

```
AutoSRingCycCode := function(p, n, r);
// Given a finite cyclic group Z_{p^n} and an integer r,
// returns the partition of G corresponding to the orbit Schur ring induced
// by <r> < Aut(G).
     return [ [p, n, r], [n] ];
end function;

SRing0Code := function(p, n);
// Given a cyclic group G of order p^n
// returns the trivial Schur ring over G.
     return [ [p, n, 0], [n] ];
end function;

TopRationalSRingsCode := function(p, n);
// Given a finite cyclic group G of order p^n,
// returns all the partitions of G which correspond to orbit Schur rings
// which are wedge-indecomposable.
     SRings := [];
     order := p^n;
     if p eq 2 then
          SRings cat:= [ AutoSRingCycCode(p, n, 1) ];
          if n gt 2 then
               SRings cat:= [AutoSRingCycCode(p, n, order-1)];
               SRings cat:= [AutoSRingCycCode(p, n, (p^(n-1)-1) mod order)];
          end if;
          return SRings;
     else
          q := p^(n-1);
```

```
          f := order - q;                    // EulerPhi(p^n);
          a := PrimitiveRoot(p^n);           // a generates Aut(G)
          for d in Divisors(p-1) do
               SRings cat:= [AutoSRingCycCode(p, n, a^(q*d) mod order)];
          end for;
          return SRings;
     end if;
end function;

WedgeProductCode := function(p, nucleus, h, cloud, k);
// Given two Schur rings, nucleus and cloud, over cyclic groups, Z_(p^h)
// and Z_(p^k), respectively,
// returns the wedge product (S wedge T) and the cyclic group Z_(p^(h+k)).
     wedge := [];
     if #nucleus eq 2
     then
          wedge := [nucleus[1]];
     else
          wedge cat:= nucleus;
     end if;
     if #cloud eq 2
     then
          wedge cat:= [cloud[1]];
     else
          wedge cat:= cloud;
     end if;
     wedge cat:= [ [h+k] ];
     return wedge;
end function;
```

```
IsWedgePossibleCode := function(p, nucleus, h, cloud, k, g);
// Given a Schur ring nucleus over H=Z_(p^h) and a Schur ring cloud
// over K=Z_(p^k),
// returns true if the semi-wedge product is possible over G = Z_(p^n).
// 1 < L < H < G, with L = G/K.
     nu := [p, h-1, (nucleus[1,3]) mod p^(h-1)];
     cl := cloud[1];
     if (p eq 2) and (h eq 3) and (nu[3] eq 3) and (#cloud gt 2)
     then
          return ((nu[2] le cl[2]) and ( nu[3] eq ( cl[3] mod p^nu[2]) ))
          or ( (cl eq [2,1,1]) and (cloud[2,3] ne 0) );
     else
          return (nu[2] le cl[2]) and (nu[3] eq (cl[3] mod p^nu[2]));
     end if;
end function;

TrivialWedgeProductsCode := function(p, h, srings, k);
// Given a cyclic group H=Z_(p^h) and a set of Schur rings over some
// cyclic group K=Z_(p^k),
// returns all wedge products over G=Z_(p^(h+k)) with nucleus the
// trivial Schur ring over H and clouds from srings.
     trivial := SRing0Code(p, h);
     return [WedgeProductCode(p, trivial, h, cloud, k) : cloud in srings];
end function;

SemiWedgeProductCode := function(p, nucleus, h, cloud, k, g);
// Given cyclic subgroups 1 < L < H < G, each cyclic p-groups and K = G/L,
// and given Schur rings nucleus and cloud over H and K, respectively,
// and H, K, and G have orders p^h, p^k, and p^g, respectively,
// returns the semi-wedge product (S wedge T).
```

```
     wedge := [];
     if #nucleus eq 2
     then
          wedge := [nucleus[1]];
     else
          wedge cat:= nucleus;
     end if;
     if #cloud eq 2
     then
          wedge cat:= [cloud[1]];
     else
          wedge cat:= cloud;
     end if;
     wedge cat:= [ [g] ];
     return wedge;
end function;

SemiWedgeProductsCode := function(p, sring, h, srings, k, g);
// Given cyclic subgroups 1 < L < H < G, each cyclic p-groups and K = G/L,
// and given a Schur ring over H and a set of Schur rings over K,
// and H, K, and G have orders p^h, p^k, and p^g, respectively,
// returns all semiwedge products over G with nucleus sring and clouds
// from srings.
     SR := [];
     for i := 1 to #srings do
          if IsWedgePossibleCode(p, sring, h, srings[i], k, g) then
               SR cat:= [SemiWedgeProductCode(p, sring, h, srings[i], k,  g)];
          end if;
     end for;
     return SR;
```

```
end function;

forward SRingsCode;
SRingsCode := function(p, n);
// Given a cyclic group G of prime power order p^n,
// returns the set of all Schur rings over G.
     if n eq 1
          then return TopRationalSRingsCode(p, 1);
     else
          srings := [SRing0Code(p, n)];
          srings cat:= TopRationalSRingsCode(p, n);
          sr := [];
          for i := 1 to n-1 do
               sr[i] := SRingsCode(p, i);
          end for;

          srQ := sr[n-1];          //cloud

          for i := 1 to n-1 do
               srN := TopRationalSRingsCode(p, i);          //nucleus

               for s in srN do
                    srings cat:= SemiWedgeProductsCode(p, s, i, srQ, n-1, n);
               end for;

               if i gt 1 then
                    srH := sr[n-i];
                    srings  cat:= TrivialWedgeProductsCode(p, i, srH, n-i);
               end if;
          end for;
```

```
          return srings;
     end if;
end function;

SRingsMemoryCode := function(p, n, SmallerSRings);
// Given a cyclic group G of prime power order p^n, and the set of all
// Schur rings over cyclic p-groups of smaller order,
// returns the set of all Schur ring over G.
     if n eq 1
          then return TopRationalSRingsCode(p, 1);
     else
          srings := [SRing0Code(p, n)];
          srings cat:= TopRationalSRingsCode(p, n);
          srQ := SmallerSRings[n-1];           //cloud

          for i := 1 to n-1 do
               srN := TopRationalSRingsCode(p, i); //nucleus

               for s in srN do
                    srings cat:= SemiWedgeProductsCode(p, s, i, srQ, n-1, n);
               end for;

               if i gt 1 then
                    srH := SmallerSRings[n-i];

                    srings cat:= TrivialWedgeProductsCode(p, i, srH, n-i);
               end if;
          end for;
```

```
          return srings;
     end if;
end function;

AtomicSRingDecrypt := function(sring);
// Given a coded indecomposable Schur ring [p,k,r] sring,
// returns the partition of Z_{p^k}.
     if sring[3] eq 0
          then return SRing0(sring[1], sring[2]);
     else
          return AutoSRingCyc(sring[3], sring[1], sring[2]);
     end if;
end function;

SRingDecrypt := function(sring);
// Given a coded Schur ring sring,
// return the partition for the sring.
     if #sring eq 2
          then return AtomicSRingDecrypt(sring[1]);
     else
          n := Ceiling(#sring/2);
          p := sring[1,1];
          T := AtomicSRingDecrypt(sring[n]);
          k := sring[n,2];
          for i := 1 to (#sring-1) div 2 do
               S := AtomicSRingDecrypt(sring[n-i]);
               T := SemiWedgeProduct(p, S, sring[n-i,2], T, k, sring[n+i,1]);
               k := sring[n+i,1];
          end for;
          return T;
```

```
     end if;
end function;
```

The remainder of the code is a collection of functions and procedures to compute the polynomials $\Omega(n)$ and $\Omega(n,k)$, which appeared in Chapter 5 and hence the number of Schur rings over cyclic p-groups. The value $\Omega(n)$ is computed by the recursive function `Omega` when p is an odd prime and by the recursive function `Omega2` when $p = 2$. The value $\Omega(n,k)$ is computed by the recursive function `omega` when p is an odd prime and by the recursive function `omega2` when $p = 2$. `Omega` and `omega` output polynomials in the variable x, where x is the number of divisors of $p-1$. On the other hand, `Omega2` and `omega2` output integers since there is no variability on the number of divisors of $p-1$ when $p = 2$. In addition to `Omega2` and `omega2`, `omegaS` is a recursive function which counts the number of Schur rings which map onto the maximal real subfield of the cyclotomic field $\mathcal{K}_{2^n}$.

```
forward Omega;
Omega := function(n);
// Given a nonnegative integer n,
// returns the nth Omega-polynomial, that is, the polynomial associated
// with the number of Schur rings over Z_{p^n}.
     P<x> := PolynomialRing(Integers());
     case n:
          when 0: return 1;
          when 1: return x;
          else return (x*Omega(n-1)
                + &+[(Catalan(k-1)*x + 1)*Omega(n-k) : k in [2..n]]);
     end case;
end function;

forward omega;
omega := function(n, k);
// Given a nonnegative integer n and a nonnegative integer k <= n,
// returns the polynomial associated with the number of Schur rings over
```

```
// Z_{p^n} which map onto Q(z_{p^k}).
     P<x> := PolynomialRing(Integers());
     case k:
          when n : return 1;
          when 0:
               if n eq 0 then return 1;
               else return &+[Omega(j) : j in [0..n-1]];
               end if;
          when 1 : return Omega(n-1);
          else return &+[omega(n-1, j): j in [k-1..n-1]];
     end case;
end function;

Schroder := function(n);
// Given a nonnegative integer n,
// returns the nth Schroder number.
     return &+[Catalan(k)*Binomial(n+k,2*k) : k in [0..n]];
end function;

forward Omega2;
Omega2 := function(n);
// Given a nonnegative integer n,
// returns  the number of S-rings over Z_{2^n}.
     case n:
          when 0: return 1;
          when 1: return 1;
          when 2 : return 3;
          when 3 : return 10;
          else return 2*Omega2(n-1)+4*Omega2(n-2) + 8*Omega2(n-3) //
               - (Catalan(n-1) + Schroder(n-1)) + &+[(Catalan(k-1) //
```

```
               + Schroder(k-1) - &+[ Catalan(j) + Schroder(j) //
                : j in [1..k-3]])*Omega2(n-k) : k in [4..n]];
     end case;
end function;

forward omega2;
omega2 := function(n,k);
// Given a nonnegative integer n and a nonnegative integer k <= n,
// returns the the number of Schur rings over  Z_{2^n} which map
// onto Q(z_{2^k}).
     if k gt n then
          return 0;
     else
          case k:
               when n : return 1;
               when 0 :
                    if n eq 0 then return 1;
                    else return &+[Omega2(j) : j in [0..n-1]];
                    end if;
               when 1 : return omega2(n,0);
               when 2 : return Omega2(n-1) - omega2(n-2,0);
               else return &+ [omega2(n-1,j) : j in [k-1..n-1]];
          end case;
     end if;
end function;

forward omegaS;
omegaS := function(n,k);
// Given a nonnegative integer n and a nonnegative integer k <= n,
// returns the the number of Schur rings over  Z_{2^n} which map
```

```
// onto Q(z_{2^k})\cap \R.
     if k gt n then
          return 0;
     else
          case k:
               when 0, 1, 2 : return omega2(n,0);
               when n : return 1;
               when 3 : return  omega2(n-1,2) + 2*&+[omegaS(n-1,j) //
                     : j in [3..n-1]];
               else return omegaS(n-1,k-1) + 2*&+[omegaS(n-1,j) //
                     : j in [k..n-1]];
          end case;
     end if;
end function;
```

Bibliography

[1] 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).

[2] Osnel Broche and Ángel del Río. Wedderburn decomposition of finite group algebras. *Finite Fields and Their Applications*, 13:71–79, 2007.

[3] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. AMS Chelsea Publishing, 2006.

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

[5] Raul Antonio Ferraz and César Polcino Milies. Idempotents in group algebras and minimal abelian codes. *Finite Fields and Their Applications*, 13:382–393, 2007.

[6] Johannes Fischer. Sequence a144944. *The On-Line Encyclopedia of Integer Sequences*.

[7] Edgar G. Goodaire, Eric Jespers, and César Polcino Milies. *Alternative Loop Rings*. North-Holland Mathematics Studies, 184. Noth-Holland Publishing Co., 1996.

[8] Eric Jespers, Guilherme Leal, and Antonio Paques. Central idempotents in rational group algebras of finite nilpotent groups. *J. Algebra Appl.*, 2(no. 1,), 2003.

[9] Eric Jespers, Gabriela Olteanu, and Ángel del Río. Rational group algebras of finite groups: from idempotents to units of integral group rings. *Algebr. Represent. Theory*, 15(no. 2):359–377, 2012.

[10] Eric Jespers, Gabriela Olteanu, and Inneke Van Gelder. Group rings of finite strongly monomial groups: central units and primitive idempotents. *J. Algebra*, 387:99–116, 2013.

[11] Brent Kerby. Rational schur rings over abelian groups. Master's thesis, Brigham Young University, 2008.

[12] M. Kh. Klin and R. Poschel. The konig problem, the isomorphism problem for cyclic graphs and the method of schur rings. *Algebraic Methods in Graph Theory*, 1, 2, 1978.

[13] István Kovács. The number of indecomposable schur rings over a cyclic 2-group. *Séminaire Lotharingien de Combinatoire*, 51:Article B51h, 2005.

[14] Tsit-Yuen Lam. *A First Course in Noncommutative Rings*. Springer-Verlag, 2001.

[15] Ka Hin Leung and Siu Lun Ma. The structure of schur rings over cyclic groups. *Journal of Pure and Applied Algebra*, 66:287–302, 1990.

[16] Ka Hin Leung and Shin Hing Man. On schur rings over cyclic groups ii. *Journal of Algebra*, 183:273–285, 1996.

[17] Ka Hin Leung and Shin Hing Man. On schur rings over cyclic groups. *Israel Journal of Mathematics*, 106:251–267, 1998.

[18] V. Liskovets and R. Poschel. Counting circulant graphs of prime-power order by decomposing into orbit enumeration problems. *Discr. Math.*, 214:173–191, 2000.

[19] S. L. Ma. On association schemes, schur rings, strongly regular graphs and partial difference sets. *Ars Combin.*, 21:211–220, 1989.

[20] Andrew Misseldine. Primitive idempotents of schur rings. *Algebras and Representation Theory*, pages 1–20, 2014.

[21] Mikhail Muzychuk. The structure of schur rings over cyclic groups of square-free order. *Acta Applicandae Mathematicae*, 52:163–181, 1998.

[22] Mikhail Muzychuk and Ilia Ponomarenko. Schur rings. *European Journal of Combinatorics*, 30:1526–1539, 2009.

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

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

[25] Aurora Olivieri and Ángel del Río. An algorithm to compute the primitive central idempotents and the wedderburn decomposition of a rational group algebra. *J. Symbolic Comput.*, 35(no. 6):673–687, 2003.

[26] Aurora Olivieri, Ángel del Río, and Juan Jacobo Simón. On monomial characters and central idempotents of rational group algebras. *Comm. Algebra*, 32(no. 4):1531–1550, 2004.

[27] S. Perlis and G. Walker. Abelian group algebras of finite order. *Trans. Amer. Math. Soc.*, 68:420–426, 1950.

[28] César Polcino Milies and Sudarshan K. Sehgal. *An Introduction to Group Rings*. 2002.

[29] W. R. Scott. *Group Theory*. Dover Publications, Inc., New York, 1987.

[30] N. J. A. Sloane. Sequence a009766. *The On-Line Encyclopedia of Integer Sequences*.

[31] Olaf Tamaschke. On the theory of schur-rings. *Ann. Mat. Pura Appl. (4)*, 81:1–43, 1969.

[32] László Tóth. A survey of the alternating sum-of-divisors function. *ArXiv*, `arXiv:1111.4842 [math.NT]`, 2011.

[33] Inneke Van Gelder and Gabriella Olteanu. Finite group algebras of nilpotent groups: a complete set of orthogonal primitive idempotents. *Finite Fields Appl.*, 17(no. 2):157–165, 2011.

[34] Helmut Wielandt. Zur theorie der einfach transitiven permutationsgruppen II (German). *Math. Z.*, 52:384–393, 1949.

[35] Helmut Wielandt. *Finite Permutation Groups.* Academic Press, New York-London, 1964.