2019-02-01

Schur Rings over Infinite Groups

Cache Porter Dexter
Brigham Young University

Schur Rings over Infinite Groups

Cache Porter Dexter

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

Master of Science

Stephen Humphries, Chair
Nathan Priddis
Pace Nielsen

Department of Mathematics

Brigham Young University

ABSTRACT

Schur Rings over Infinite Groups

Cache Porter Dexter
Department of Mathematics, BYU
Master of Science

A Schur ring is a subring of the group algebra with a basis that is formed by a partition of the group. These subrings were initially used to study finite permutation groups, and classifications of Schur rings over various finite groups have been studied. Here we investigate Schur rings over various infinite groups, including free groups. We classify Schur rings over the infinite cyclic group.

Keywords: Schur ring, permutation group, free group, free abelian group, infinite cyclic group

Acknowledgments

Many thanks to my advisor, Dr. Humphries, for his many hours of helping me understand how to read, write, and think about mathematics.

Contents

Chapter 1. Introduction

1.1 Definitions

In this section we briefly define a Schur ring and provide a few examples. The motivation for constructing and studying Schur rings will be given in the succeeding chapters.

Given a group we can form the *group ring*, which, informally, is the set of formal sums with coefficients in some field. More precisely, if G is a group and F is a field, then all sums of the form

$$\sum_{g\in G} \lambda_g g$$

where $\lambda_g \in F$ and $\lambda_g = 0$ for all but finitely many $g \in G$, form the elements of the group ring $F[G]$. Addition is defined by

$$\sum_{g\in G} \lambda_g g + \sum_{g\in G} \mu_g g = \sum_{g\in G} (\lambda_g + \mu_g) g,$$

and multiplication by

$$\left(\sum_{g\in G} \lambda_g g\right) \left(\sum_{g\in G} \mu_g g\right) = \sum_{g\in G} \nu_g g \quad \text{where} \quad \nu_g = \sum_{h\in G} \lambda_h \mu_{h^{-1}g}.$$

These operations make $F[G]$ a ring that contains a copy of G in its unit group and a copy of F as a subring, identified by $\{\lambda 1 \mid \lambda \in F\}$. This also makes $F[G]$ into a vector space of dimension $|G|$ over F, so in particular $F[G]$ is an F-algebra. We refer to this structure as the group algebra $F[G]$.

For a group G and a finite subset $X = \{x_1, \ldots, x_k\} \subseteq G$, we define

$$\overline{X} = x_1 + \cdots + x_k \in F[G].$$

We also define $X^{-1} = \{x^{-1} : x \in X\}$ and $\overline{X^{-1}} = x_1^{-1} + \cdots + x_k^{-1}$ similarly.

A *Schur ring* over a group G is a subring $\mathfrak{S}$ of $F[G]$ with a basis $\{\overline{P}_i\}_{i\in I}$, with I being an indexing set containing a distinguished element 0, that satisfies the following properties:
(i) the sets $\{P_i\}_{i\in I}$ form a partition of the elements of G into finite sets ($|P_i| < \infty$);
(ii) $P_0 = \{id\}$;
(iii) for all i there is some j such that $P_i^{-1} = P_j$;
(iv) for all i, j there exists a finite subset $K \subset I$ (dependent on i and j) and scalars $\lambda_k \in F$ such that

$$\overline{P}_i\overline{P}_j = \sum_{k\in K} \lambda_k \overline{P}_k.$$

Each set P_i in the partition of G is called a *principal set*, and the corresponding sums $\overline{P}_i, i \in I$ are called *principal elements* of the Schur ring. The principal elements form an F-basis for $\mathfrak{S}$ over F.

In our work here we take F to be a field of characteristic zero unless otherwise stated.

1.2 Examples

If G is a finite group with identity e, then the partition $P_0 = \{e\}, P_1 = G - \{e\}$ gives a basis $\overline{P}_0, \overline{P}_1$ for a Schur ring over G. It is clear that $P_1^{-1} = P_1$ and that $\overline{P}_0\,\overline{P}_1 = \overline{P}_1$ in $F[G]$. The only nontrivial product to check is

$$\begin{aligned}\overline{P}_1^2 = (\overline{G} - e)(\overline{G} - e) = |G|\overline{G} - 2\overline{G} + e &= (|G| - 1)e + (|G| - 2)(\overline{G} - e)\\ &= (|G| - 1)\overline{P}_0 + (|G| - 2)\overline{P}_1,\end{aligned}$$

so $\overline{P}_1^2$ is a linear combination of principal elements. This is called the *trivial* Schur ring over G.

On the other extreme end, for any group G the partition into singleton sets $\{\{g\} : g \in G\}$ gives rise to a basis for the *discrete* Schur ring $\mathfrak{S} = F[G]$.

For a different example, let $G = \langle x \mid x^4 = 1\rangle$ be the cyclic group of order 4. Let $P_0 = \{1\}, P_1 = \{x, x^3\}$, and $P_2 = \{x^2\}$. The subring of $F[G]$ with basis $\{\overline{P}_0, \overline{P}_1, \overline{P}_2\}$ is a

Schur ring over G. For every $i = 0, 1, 2$ the relation $P_i^{-1} = P_i$ holds, and it can be checked that $\overline{P}_2^2 = \overline{P}_0, \overline{P}_1\overline{P}_2 = \overline{P}_1$, and $\overline{P}_1^2 = 2\overline{P}_0 + 2\overline{P}_2$. Schur rings over finite cyclic groups have been studied extensively, see [1].

Other examples of Schur rings over finite groups, such as the Schur ring with a partition given by conjugacy classes in a finite group [2], have been studied. Schur rings were first introduced by Schur and Wielandt to study permutation groups. In the next chapter we show how these Schur rings were initially used to prove results about permutation groups. Since we are expanding the study of Schur rings to include infinite groups, our hope is that some of our results may find eventual use as means to prove results about infinite groups.

Chapter 2. Schur Rings in the Study of Permutation Groups

2.1 Background Information

The group of all bijections from a set Ω to itself under function composition is the *symmetric group* on Ω, denoted $\mathrm{Sym}(\Omega)$. A *permutation group on* Ω is a subgroup of $\mathrm{Sym}(\Omega)$. The usual symmetric group S_n is $\mathrm{Sym}(\{1, 2, ..., n\})$.

If we have a permutation group G on Ω, then we can think of G acting on the set Ω. If $\alpha \in \Omega$ then the (right) action of $x \in G$ on α is the image of α under the permutation x. We will denote this by α^x. The use of this choice of notation will become clear as we want to occasionally identify G with a subset of Ω. We can think of a permutation group as consisting of a group G, a set Ω, and an action $\Omega \times G \to \Omega$.

For an example, let $\Omega = \{1, 2, 3, 4\}$ and consider the alternating group A_4 of even permutations in $S_4 = \mathrm{Sym}(\Omega)$. Using cycle notation to denote $A_4 = \langle (123), (12)(34) \rangle$, this group acts on $\{1, 2, 3, 4\}$ in the natural way. For example, taking $1 \in \Omega$ and $(123) \in A_4$ the action of (123) on 1 is $1^{(123)} = 2$, since the permutation (123) maps 1 to 2. (Since we are using a right action, we compose permutations from left to right. For example, $(12)(13) = (123)$.)

We will use the following definitions to discuss permutation groups. Given a permutation group G acting on a set Ω, the *degree* of G is the cardinality of Ω. The *orbit* of $\alpha \in \Omega$ under G is the set $\alpha^G = \{\alpha^x \mid x \in G\}$. The *stabilizer* of α in G is the subgroup G_α of G:

$$G_\alpha = \{x \in G \mid \alpha^x = \alpha\}.$$

In our continuing example of $G = A_4$ acting on $\Omega = \{1, 2, 3, 4\}$, the orbit of $1 \in \Omega$ is the entire set Ω. This is because the permutations $(12)(34), (13)(24)$, and $(14)(23)$ in particular belong to A_4, so every element of Ω is the image of 1 under some element of G. The stabilizer of $1 \in \Omega$ is $G_1 = \{(1), (234), (243)\} = \langle (234) \rangle$ since these are the elements of A_4 that fix 1.

The set of orbits of Ω under the action of a group G is a partition of Ω. If there is only one orbit, which is to say that given any $\alpha, \beta \in \Omega$ there exists some $x \in G$ such that $\alpha^x = \beta$, then we say that G *acts transitively on* Ω.

The group $G = A_4$ acts transitively on $\Omega = \{1, 2, 3, 4\}$, as seen above by $1^G = \Omega$. (It follows that $2^G = 3^G = 4^G = \Omega$ as well.)

A permutation group $G \leq \mathrm{Sym}(\Omega)$ *acts regularly on* Ω if G acts transitively on Ω and $G_\alpha = 1$ for every $\alpha \in \Omega$.

If G acts on Ω as a permutation group, then any subgroup of G also acts on Ω as a permutation group. Later we will be concerned with subgroups of G that act regularly.

The well-known orbit-stabilizer property states that $|\alpha^G| = [G : G_\alpha]$ for any $\alpha \in \Omega$, so the cardinality of the orbit of α is equal to the index of the stabilizer G_α in G. When G is a finite group, this implies $|\alpha^G| \cdot |G_\alpha| = |G|$. An immediate corollary is that if G acts transitively, then $[G : G_\alpha] = |\Omega|$ for every α. If in addition G is finite, then G acts regularly if and only if G acts transitively and $|G| = |\Omega|$.

The group $G = A_4$ acting on $\Omega = \{1, 2, 3, 4\}$ does not act regularly, since we saw earlier that $G_1 = \{(1), (234), (243)\}$ is not trivial. If $H = \{(1), (12)(34), (13)(24), (14)(23)\}$ is the Klein 4-group in A_4, then H acts transitively and also regularly, since every nontrivial permutation in H fixes no element of Ω.

There is yet another type of permutation group we are interested in, called a *primitive* group. To define a primitive group we first need to define *blocks*. Given a subset $\Delta \subseteq \Omega$, an element $x \in G$ can act on Δ as follows: $\Delta^x = \{\alpha^x \mid \alpha \in \Delta\}$. A *block* is a subset Δ of Ω such that either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \emptyset$, for each $x \in G$.

It's not too hard to see that if Δ is the entire set Ω then $\Delta^x = \Delta$ for every $x \in G$, which makes Ω itself a block. It's also not too hard to see that any singleton set $\{\alpha\}$ in Ω is also a block since $\{\alpha\}^x = \{\alpha^x\}$ is a singleton set that is either $\{\alpha\}$ itself or some other set disjoint from $\{\alpha\}$. These types of blocks, the entire set Ω and the singleton sets, are called *trivial* blocks.

A *primitive* group is a group $G \leq \mathrm{Sym}(\Omega)$ that acts transitively and has no nontrivial blocks in the set Ω. A group that is not primitive (that has nontrivial blocks) is called *imprimitive.*

For $G = A_4$ and $H = \{(1), (12)(34), (13)(24), (14)(23)\} \leq A_4$ acting on $\Omega = \{1, 2, 3, 4\}$ we see that G is primitive but H is imprimitive. Letting $\Delta = \{a, b\}$ be any subset of Ω with two elements, a permutation of the form (abc) in G gives $\Delta^{(abc)} = \{b, c\}$. Thus $\Delta^{(abc)} \neq \Delta$ and $\Delta^{(abc)} \cap \Delta = \{b\} \neq \emptyset$, so Δ is not a block of G. If $\Delta = \{a, b, c\}$ has size 3 then $\Delta^{(ab)(cd)} = \{a, b, d\}$, so Δ is not a block of G either. The only blocks for G are therefore singleton subsets of Ω and Ω itself, so G is primitive.

However, $\{1, 2\}$ is a nontrivial block of H, as seen by directly computing $\{1, 2\}^{(12)(34)} = \{1, 2\}, \{1, 2\}^{(13)(24)} = \{3, 4\}$, and $\{1, 2\}^{(14)(23)} = \{3, 4\}$. The action of any element of H on $\{1, 2\}$ produces either $\{1, 2\}$ or the disjoint set $\{3, 4\}$. This means H is imprimitive.

If G acts on Ω, then we can define an action of G on Ω^k, the Cartesian product of k copies of Ω, as follows:

$$(\alpha_1, \alpha_2, ..., \alpha_k)^x = (\alpha_1^x, \alpha_2^x, ..., \alpha_k^x), \text{ for } \alpha_i \in \Omega, x \in G.$$

The group G acts *k-transitively* if G acts transitively on the set

$$\Omega^{(k)} = \{(\alpha_1, ..., \alpha_k) \in \Omega^k \mid \alpha_i \neq \alpha_j \text{ for all } 1 \leq i < j \leq k\}.$$

Consider $\Omega^2 = \{1, 2, 3, 4\} \times \{1, 2, 3, 4\}$. Eliminating all pairs of the form (a, a) from this set gives the set $\Omega^{(2)}$. Then $G = A_4$ acts on $\Omega^{(2)}$ componentwise, so that for example $(1, 2)^{(123)} = (2, 3)$. It can be verified that $G = A_4$ acts transitively on $\Omega^{(2)}$, as follows. Consider $(1, 2) \in \Omega^{(2)}$ and any other element (a, b) of $\Omega^{(2)}$. It suffices to show that there exists a permutation x in G such that $(1, 2)^x = (a, b)$. If $a = 1$ and $b = 2$ then $x = (1)$ suffices. If $a = 1$ and $b \neq 2$ then $x = (2bc)$ where $c \neq 1$ will do the job. Similarly if $a \neq 1$ and $b = 2$ then take $x = (1ac)$ with $c \neq 2$. If $a = 2$ and $b = 1$ then take $x = (12)$, and if

$a = 2$ and $b \neq 1$ then $x = (12)(bc)$ where $c \in \Omega - \{1, 2, b\}$ suffices. Similarly if $a \neq 2$ and $b = 1$ then take $x = (ac)(12)$ with $c \in \Omega - \{1, 2, a\}$. In every other case where $a \neq 1, 2$ and $b \neq 1, 2$ then take $x = (1a)(2b)$. Since G contains all 3-cycles and 2-2-cycles, this proves $(1, 2)^G = \Omega^{(2)}$, so there is only one orbit of $\Omega^{(2)}$ under G, and hence G acts 2-transitively.

One last thing to mention about preliminary definitions. When $\Omega = G$ we can define the action of $x \in G$ on $a \in G$ by $a^x = ax \in G$. For a fixed $x \in G$, the map $a \mapsto ax$ is a bijection from G to G. If we call this bijection σ_x, then the map $x \mapsto \sigma_x$ from G into $\mathrm{Sym}(G)$ is a group homomorphism called the *regular (permutation) representation* of G.

Having concluded the necessary definitions, the next few sections outline some standard results proved about permutation groups using Schur rings.

2.2 Permutation Groups with Subgroups That Act Regularly

The main result of this chapter is an application (due to Schur) of Schur rings to classify permutation groups that contain subgroups that act regularly. Before proving this result, we give some information on permutation groups with such subgroups and introduce the Schur ring construction used.

If R is a group acted upon by G, then we can define an action of G on the group ring $F[R]$. We do this by letting an element x of G act on an element in $F[R]$ by the rule:

$$\left(\sum_{r \in R} \lambda_r r\right)^x = \sum_{r \in R} \lambda_r r^x.$$

It is this case that we are interested in. Let R be a finite group and let G be a subgroup of $\mathrm{Sym}(R)$ such that G contains the image of the regular representation of R. (Meaning if $r \in R$ induces the permutation σ_r of R by right multiplication in R, then G contains σ_r.) Recall that the subgroup $G_1 \leq G$ is the stabilizer of the identity of R. In the group ring $F[R]$ over some field F, define $\mathcal{C}(G_1)$ to be the set of fixed points for the action of G_1 on

$F[R]$:

$$\mathcal{C}(G_1) = \{\alpha \in F[R] \mid \alpha^x = \alpha \text{ for all } x \in G_1\}.$$

We will show that $\mathcal{C}(G_1)$ is a subring of $F[R]$; in fact this will be a Schur ring over R.

As a matter of notation, for an element $c \in F[R]$, where $c = \sum_{r \in R} \lambda_r r$, we define the *support* of c to be the set $\text{supp}(c) = \{r \in R \mid \lambda_r \neq 0\}$. Whenever c is fixed by some $x \in G$ it follows that $\text{supp}(c)$ is invariant under x.

In the main theorem of this chapter, Theorem 2.5, we are concerned with a permutation group with a subgroup R that acts regularly. The following lemma shows that we may restrict our study to subgroups of $\text{Sym}(R)$ that contain the image of the regular representation of R. It introduces the concept of a *permutation homomorphism.* Given two permutation groups $H_1 \leq \text{Sym}(\Omega_1)$ and $H_2 \leq \text{Sym}(\Omega_2)$, a *permutation homomorphism* is a group homomorphism $\psi : H_1 \to H_2$ along with a bijection $\lambda : \Omega_1 \to \Omega_2$ such that

$$\lambda(\alpha^x) = \lambda(\alpha)^{\psi(x)} \qquad \text{for all } \alpha \in \Omega_1 \text{ and } x \in H_1.$$

If ψ above is an isomorphism then we say that ψ is a *permutation isomorphism* and that H_1 and H_2 are *permutation isomorphic.*

Lemma 2.1. *If G is a permutation group on a finite set Ω, where G has a subgroup R that acts regularly, then there exists a permutation homomorphism $\phi : G \to Sym(R)$ such that $\phi|_R$ is the regular representation of R.*

Proof. Fix $\alpha \in \Omega$. Because R acts regularly on Ω, for every $\beta \in \Omega$ there exists a unique element $r_\beta \in R$ such that $\alpha^{r_\beta} = \beta$. Since $|R| = |\Omega|$, this defines a bijection $\lambda : \Omega \to R$ by $\lambda(\beta) = r_\beta$.

Define $\phi : G \to \text{Sym}(R)$ by $\phi(x) = \lambda x \lambda^{-1}$. Since λ is a bijection from Ω into R and x is a permutation of Ω, the function $\lambda x \lambda^{-1}$ is indeed a permutation of R. The function ϕ is a group homomorphism: given $x, y \in G$ we have $\phi(xy) = \lambda xy\lambda^{-1} = (\lambda x \lambda^{-1})(\lambda y \lambda^{-1}) = \phi(x)\phi(y)$.

The homomorphism ϕ is injective, since if $\phi(x) = 1$ then $x = \lambda^{-1}1\lambda = 1 \in G$. Thus ϕ is a permutation homomorphism and G is permutation isomorphic to the image $\phi(G)$.

Let $r \in R$, and consider the permutation $\phi(r) = \lambda r \lambda^{-1} \in \mathrm{Sym}(R)$. We show this permutation is given by right multiplication by r. Given $r_1 \in R$, there is some $\beta \in \Omega$ such that $\lambda(\beta) = r_1$. From the definition of λ this means $\alpha^{r_1} = \beta$. The action of r on β gives $\beta^r \in \Omega$, and $\lambda(\beta^r) = r_2$ for some $r_2 \in R$. This means $\alpha^{r_2} = \beta^r = (\alpha^{r_1})^r = \alpha^{r_1 r}$. By the uniqueness of the elements of R acting on α, this implies $r_2 = r_1 r$. Thus $\lambda r \lambda^{-1}$ permutes R in the same way as right multiplication in R, so $\phi(r)$ is the image of r under the regular representation of R. Thus $\phi|_R$ is the regular representation of R. □

This lemma shows that in our study of permutation groups with subgroups that act regularly, it suffices to study subgroups of $\mathrm{Sym}(R)$ which contain the image of the regular representation of R. This image $\phi(R)$ is an isomorphic copy of R in such a subgroup. In this way we can regard R both as a set of objects that are being permuted (in $\mathrm{Sym}(R)$) and as elements of $\mathrm{Sym}(R)$ themselves. Thus if G is a subgroup of $\mathrm{Sym}(R)$ that contains the image of the regular representation of R then each element of R can be acted on by an element of G, but this action is also simply multiplication inside the group G, viewing $R \leq G$.

If $G = A_4$, acting on $\Omega = \{1, 2, 3, 4\}$, and $R = K_4 = \{(1), (12)(34), (13)(24), (14)(23)\}$, then, as seen previously, R is a subgroup of G that acts regularly. We can label the elements of R as $(1) = r_1, (12)(34) = r_2, (13)(24) = r_3$, and $(14)(23) = r_4$ so that $\beta \mapsto r_\beta$ is a bijection from Ω from R. Furthermore the induced permutation isomorphism $\phi : G \to \mathrm{Sym}(R)$ satisfies $\lambda(\beta^x) = \lambda(\beta)^{\phi(x)}$ for all $\beta \in \Omega$ and $x \in G$, so we can identify each element of G with its image in $\mathrm{Sym}(R)$. The notation translates easily, for example the image of $(123) \in G$ is $(r_1 r_2 r_3) \in \mathrm{Sym}(R)$.

This also illustrates how we can regard R as the set being permuted in $\mathrm{Sym}(R)$ and also as a subgroup of $\mathrm{Sym}(R)$. The image of $r_2 = (12)(34)$ under ϕ is $(r_1 r_2)(r_3 r_4)$. Thus we can act on r_2 by an element of G (regarding $G \leq \mathrm{Sym}(R)$), such as $r_2^{(r_1 r_2 r_3)} = r_3$. But we can also multiply r_2 by $(r_1 r_2 r_3)$ as an element of $\mathrm{Sym}(R)$: $r_2(r_1 r_2 r_3) = (r_1 r_2)(r_3 r_4)(r_1 r_2 r_3) = (r_1 r_3 r_4)$.

We now turn our attention to the first result concerning Schur rings. Recall the definition of the set $\mathcal{C}(G_1)$, the set of elements of the group algebra $F[R]$ fixed under the action of every element of G_1. We have the following lemma.

Lemma 2.2. *Let R be a finite group and G a subgroup of $\mathrm{Sym}(R)$. Let $P_1 = \{1\}, P_2, ..., P_r$ be the orbits in R of the point stabilizer G_1. Then*

(i) $\mathcal{C}(G_1)$ is a vector subspace of $F[R]$, and the elements $c_i = \overline{P}_i = \sum_{u \in P_i} u$ for $i = 1, ..., r$ form an F-basis for $\mathcal{C}(G_1)$;

(ii) $\mathcal{C}(G_1)$ is a subring (and therefore a subalgebra) of $F[R]$.

Proof. (i) Let c be an element of $F[R]$, denoted by $c = \sum_{u \in R} \lambda_u u$ for some $\lambda_u \in F$. If $c \in \mathcal{C}(G_1)$, then by definition, c is fixed by the action of G_1, so $c = c^x$ for every $x \in G_1$. Writing out $c = c^x$ in terms of linear combinations of elements of R gives

$$\sum_{u \in R} \lambda_u u = c = c^x = \sum_{u \in R} \lambda_u (u^x).$$

Whenever $u, v \in R$ are in the same orbit of G_1 then there is some $x \in G_1$ such that $v = u^x$. Since $c = c^x$ holds for all $x \in G_1$, the coefficients λ_u and λ_v must therefore be equal when u and v belong to the same orbit of G_1. Thus given any orbit P_i, every element of P_i must have the same coefficient in the sum representing c. This allows us to write

$$c = \sum_{u \in R} \lambda_u u = \sum_{i=1}^{r} \lambda_i \left(\sum_{u \in P_i} u \right) = \sum_{i=1}^{r} \lambda_i c_i.$$

Conversely, if c is an F-linear combination of the c_i then the coefficients on elements in the same G_1 orbit are equal and c is fixed by every $x \in G_1$, proving that $c \in \mathcal{C}(G_1)$. This shows that every element of $\mathcal{C}(G_1)$ is an F-linear combination of the c_i and that every F-linear combination of the c_i is in $\mathcal{C}(G_1)$. The c_i are linearly independent since each contains only elements from a single orbit and the orbits partition R. Thus the set $\{c_1, ..., c_r\}$ is an F-basis for the vector subspace $\mathcal{C}(G_1)$ of $F[R]$.

(ii) Since it was already shown that $\mathcal{C}(G_1)$ is a vector subspace of $F[R]$, to prove that $\mathcal{C}(G_1)$ is a subring of $F[R]$ it remains to show that the product of two elements of $\mathcal{C}(G_1)$ is again an element of $\mathcal{C}(G_1)$. It suffices to show that the product of any two basis elements c_i, c_j is in $\mathcal{C}(G_1)$. Given $x \in G_1$,

$$\begin{aligned}
(c_i c_j)^x &= \left(\left(\sum_{u \in P_i} u\right) \cdot \left(\sum_{v \in P_j} v\right)\right)^x \\
&= \sum_{v \in P_j} \left(\left(\sum_{u \in P_i} u\right) \cdot v\right)^x \\
&= \sum_{v \in P_j} \left(\sum_{u \in P_i} u\right)^{vx} \\
&= \sum_{v \in P_j} \left(\sum_{u \in P_i} u\right)^{v} = c_i c_j.
\end{aligned}$$

This shows that x fixes the product $c_i c_j$, and because this holds for all $x \in G_1$ we have shown that $c_i c_j$ is fixed by G_1 and is therefore an element of $\mathcal{C}(G_1)$. The product of any number of basis elements for $\mathcal{C}(G_1)$ is therefore in $\mathcal{C}(G_1)$, which makes $\mathcal{C}(G_1)$ a subring of $F[R]$. We note that $\mathcal{C}(G_1)$ is a Schur ring over R. □

2.3 Main Results

We are working toward a theorem that classifies certain permutation groups with subgroups that act regularly using the Schur ring from Lemma 2.2. There are two additional lemmas we will use in the proof of this theorem.

Lemma 2.3. *Let R be a finite group, and let G be a subgroup of* $\mathrm{Sym(R)}$ *that acts transitively. Then G acts 2-transitively on $R^{(2)}$ if and only if the orbits of the stabilizer G_1 are $\{1\}$ and $R - \{1\}$.*

Proof. Suppose that G acts 2-transitively on $R^{(2)}$. Then for any two elements of $R^{(2)}$ of the form $(1, r), (1, s)$ where $r, s \in R$ and $r, s \neq 1$, there is an element $x \in G$ such that

$(1,r)^x = (1,s)$. This means that x fixes 1, so $x \in G_1$. Then $r^x = s$ implies that r and s are in the same orbit of G_1. Since r and s were arbitrary non-identity elements of R this shows that $R - \{1\}$ is an orbit of G_1. Thus G_1 has orbits $\{1\}$ and $R - \{1\}$.

Now suppose that G_1 has orbits $\{1\}$ and $R - \{1\}$. We will use the fact G acting transitively implies that every point stabilizer G_r, $r \in R$, has the same number of orbits. Thus G_r has two orbits, namely $\{r\}$ and $R - \{r\}$, for every $r \in R$.

Let $(1,r)$ be an element of $R^{(2)}$, and let (s,t) be any element of $R^{(2)}$. If $s = 1$, there is an element $x \in G_1$ such that $r^x = t$ because r and t are in the same G_1-orbit $(R - \{1\})$. Then $(1,r)^x = (1,t)$.

Now suppose $t = 1$. There are two sub-cases.

(i) If $s \neq r$, then there is some $x \in G_r$ such that $1^x = s$ because 1 and s are in the same G_r-orbit. There is also some $y \in G_s$ such that $r^y = 1$ by the same reasoning, so $(1,r)^{xy} = (s,r)^y = (s,1)$.

(ii) If $s = r$, let u be any element of R that is not equal to 1 or r. (If no such u exists, then $R = \{1,r\}$ and since G acts transitively we must have $(1r) \in G$. Thus $(1,r)^{(1r)} = (r,1)$ takes care of this.) There is some $x \in G_r$ such that $1^x = u$, some $y \in G_u$ such that $r^y = 1$, and some $z \in G_1$ such that $u^z = r$. Then $(1,r)^{xyz} = (u,r)^{yz} = (u,1)^z = (r,1)$.

Finally, if $s \neq 1$ and $t \neq 1$, there is some $x \in G_1$ such that $r^x = t$ and some $y \in G_t$ such that $1^y = s$. Then $(1,r)^{xy} = (1,t)^y = (s,t)$.

In every case, there exists some $x \in G$ such that $(1,r)^x = (s,t)$, so the orbit of $(1,r)$ is $R^{(2)}$. This proves that G acts 2-transitively on $R^{(2)}$. □

The proof of the next lemma will use the following result. If S, T are two G_1-invariant subsets of R, then we can show that the subset $ST = \{st \mid s \in S, t \in T\}$ is also G_1-invariant. Given an element $st \in ST$, an element $x \in G_1$ acts on st by $(st)^x = st^x$. Since T is G_1-invariant, t^x runs over T as t runs over T. Then for a particular s the product st^x runs over the products st as t runs over T. Thus as st runs over ST, st^x runs over ST. This is true for each $x \in G_1$, so ST is G_1-invariant.

Lemma 2.4. *Let R be a finite group of order n, and let $G \leq \mathrm{Sym}(R)$ contain the image of the regular representation of R. Again denote by $P_1 = \{1\}, P_2, ..., P_r$ the orbits in R of the stabilizer G_1. For each integer k, define $P_i^{(k)} = \{u^k \mid u \in P_i\}$ for $i = 1, ..., r$.*

(i) G is a primitive group if and only if for each $c \in \mathcal{C}(G_1)$ the subgroup $\langle \mathrm{supp}(c) \rangle$ of R generated by the support of c is either 1 or R.

(ii) If R is abelian and k is relatively prime to n, then the mapping $P_i \mapsto P_i^{(k)}$ defines a permutation of the set of G_1-orbits in R.

(iii) Let G be primitive, R abelian, and p a prime dividing n. Let S be a G_1-invariant subset of R and $c = \sum_{s \in S} s \in F[R]$ where F is a field of characteristic p. Then $c^p = m1$ where m is the number of elements $s \in S$ with $s^p = 1$.

Proof. (i) Recall that a permutation group is primitive if it acts transitively and has only the trivial blocks on the set it permutes. The group R acts on itself by right multiplication, which means that the action of $r \in R$ on a subset S of R will result in the set Sr. This will be a block when Sr is a coset of some subgroup, so the blocks containing 1 are in fact the subgroups of R. Since $G \leq \mathrm{Sym}(R)$ contains the image of the regular representation of R (which is isomorphic to R), the blocks of G acting on R that contain the identity $1 \in R$ will be exactly the G_1-invariant subgroups of R. If G is imprimitive, there exists a nontrivial block containing $1 \in R$; this block must be a subgroup S with $1 < S < R$. Furthermore, this subgroup S is G_1-invariant. This implies that the element $c = \sum_{s \in S} s$ of the group ring $F[R]$ is fixed by the action under G_1. The subgroup generated by the support of c is simply S itself, which is not trivial and not equal to R. This proves the forward implication of (i).

To prove the converse, suppose there exists some $c \in \mathcal{C}(G_1)$ with support T such that the subgroup $S = \langle T \rangle$ generated by T is not trivial nor equal to R. Then $S = \bigcup_{i=0}^{\infty} T^i$. Because T is the support of an element of $\mathcal{C}(G_1)$, T is G_1-invariant. By the result preceding this lemma, each T^i is G_1-invariant, so the union S of these sets is G_1-invariant. This means that S is a G_1-invariant subgroup of R that is neither trivial nor equal to R, so G has a nontrivial block and is therefore imprimitive.

(ii) First consider the case where $k = p$ is a prime that does not divide n. Then p is relatively prime to the order of every element of R. In the group ring $F[R]$ let $F = \mathbb{F}_p$ be the field with p elements. Then for every $c_i = \sum_{u \in P_i} u$ we have $c_i^p = \sum_{u \in P_i} u^p$ because R is abelian. (This follows from the fact that when p is prime, every multinomial coefficient $\binom{p}{k_1,\ldots,k_t}$ not equal to 1 is divisible by p and therefore equal to 0 in $\mathbb{F}_p$.)

The support of c_i^p is therefore the set $P_i^{(p)}$. Since $\mathcal{C}(G_1)$ is a subring of $F[R]$, c_i^p is an element of $\mathcal{C}(G_1)$. Because p is relatively prime to every divisor of n, the mapping $u \mapsto u^p$ is a bijection of R onto itself. (It is a group homomorphism with trivial kernel because R is abelian and finite.) The sets $P_i^{(p)}$ form a partition of R since they are the images of a partition under a bijection. From the fact that each c_i^p is in $\mathcal{C}(G_1)$ it follows that each $P_i^{(p)}$ is G_1-invariant. By assumption there are r orbits of G_1 on R, and there are r sets $P_i^{(p)}$. Thus the sets $P_i^{(p)}$ must be exactly the orbits of G_1 because they are G_1-invariant, so the mapping $P_i \mapsto P_i^{(p)}$ is indeed a permutation of the set of G_1-orbits of R.

We now prove the statement for any integer k relatively prime to n. Factor k into primes as $k = p_1^{a_1} \cdots p_q^{a_q}$. Then we can decompose the map $P_i \mapsto P_i^{(k)}$ into the intermediate maps

$$P_i \mapsto P_i^{(p_1)} \mapsto P_i^{(p_1^2)} \mapsto \cdots \mapsto P_i^{(p_1^{a_1})} \mapsto P_i^{(p_1^{a_1} p_2)} \mapsto \cdots \mapsto P_i^{(p_1^{a_1} \cdots p_q^{a_q})} = P_i^{(k)}.$$

From what we did above, each intermediate map is a permutation of the orbits of G_1 in R, so the composition of these permutations $P_i \mapsto P_i^{(k)}$ is also a permutation of the orbits of G_1.

(iii) For the final statement, consider G to be primitive, R abelian, and p a prime dividing $n = |R|$. Given a G_1-invariant $S \subseteq R$ and $c = \sum_{s \in S} s$ in $F[R]$, we know that $c \in \mathcal{C}(G_1)$ because S is G_1-invariant. Because F has characteristic p, we have $c^p = \sum_{s \in S} s^p$. From the fact that $p \mid |R|$ and R is abelian, the index of the subgroup $\langle \mathrm{supp}(c^p) \rangle$ generated by the s^p in R is divisible by p. Because G is primitive, by (i) we have that the subgroup $\langle \mathrm{supp}(c^p) \rangle$ is either 1 or R. The index of this subgroup is greater than 1, so we must have $\langle \mathrm{supp}(c^p)\rangle = 1$. Thus c^p is the sum of elements s^p where $s^p = 1$, so $c^p = m1$. (We note that there may be elements $s \in S$ that are not of order p, but the coefficients of s^p in the sum c^p will be multiples of p and therefore equal to 0 in $F[R]$.) □

Having detailed all these results, we have built enough to prove the following theorem [3] about certain permutation groups:

Theorem 2.5. *Let G be a permutation group of degree n containing a subgroup R that acts regularly. Suppose that R is abelian and has a nontrivial cyclic Sylow p-subgroup for some prime p with $p < n$. Then G is either imprimitive or acts 2-transitively.*

Proof. Since G has a subgroup R that acts regularly, it is sufficient to prove the result for a group $G \leq \mathrm{Sym}(R)$ that contains the image of the regular representation of R. Because R is abelian, the Sylow p-subgroup is normal and therefore unique. This cyclic Sylow p-subgroup has a unique subgroup P of order p; P is the unique subgroup of R of order p. Assuming that G is primitive, it suffices to show that G must act 2-transitively. We will show that the orbits of the subgroup G_1 acting on R are $\{1\}$ and $R - \{1\}$, which will imply that G acts 2-transitively by Lemma 2.3. To show this, we use calculations in the group ring $\mathbb{F}_p[R]$ and our previous results about the Schur ring $\mathcal{C}(G_1)$ in $\mathbb{F}_p[R]$.

The first order of business is to show that each G_1-orbit Γ of R contains some element of P, and that the set of elements $\Gamma - P$ is a union of cosets of P. Define

$$c = \sum_{u \in \Gamma} u \in \mathbb{F}_p[R].$$

Because Γ is a G_1-orbit, the sum c in the group ring will be fixed by G_1, so $c \in \mathcal{C}(G_1)$. We are assuming that G is primitive, R is abelian, and p must divide $n = |R|$. We can therefore employ Lemma 2.4 (iii), which implies that $c^p = m1$ where m is the number of elements u of Γ such that $u^p = 1$. Because P is the unique subgroup of order p, P contains every element of order p in R. Thus $u^p = 1$ implies $u \in P$, so $m = |\Gamma \cap P|$. Thus we have

$$c^p = \sum_{u \in \Gamma} u^p = |\Gamma \cap P| 1.$$

If $u \in \Gamma - P$ then u^p does not have nonzero coefficient in c^p, which means that there must be other elements $v \in \Gamma$ such that $v^p = u^p$ and the number of these elements is a multiple of p (and therefore 0 in the group ring $\mathbb{F}_p[R]$). Because R is abelian, $v^p = u^p$ if and only if $(vu^{-1})^p = 1$ if and only if $vu^{-1} \in P$. Thus if $v^p = u^p$ then u and v belong to the same coset of P. Each coset of P has p elements, so the fact that the coefficient on u^p for some $u \in \Gamma - P$ in the sum c^p is a multiple of p implies that the entire coset Pu is in Γ. This proves that $\Gamma - P$ is the union of cosets of P.

To prove that $\Gamma \cap P \neq \emptyset$, suppose that this intersection is empty. Then $\Gamma - P = \Gamma$ must itself be a union of cosets of P. If we multiply the elements of a coset Pa by an element $u \in P$, the result is the same coset, since $(Pa)u = (Pu)a = Pa$ because R is abelian. Then for every element $u \in P$ we have $\Gamma u = \Gamma$, since Γ is a union of cosets of P. Defining $H = \{u \in R \mid \Gamma u = \Gamma\}$ we have $P \subset H$. The set H is a subgroup of R and is nontrivial since it contains P. Clearly, H is G_1-invariant: If $x \in G_1$ and $u \in H$, then $\Gamma u^x = (\Gamma u)^x = \Gamma^x = \Gamma$ follows from Γ being G_1-invariant. Thus $u^x \in H$ for all $x \in G_1$, so H is G_1-invariant. Letting $h = \sum_{u \in H} u$ in $\mathbb{F}_p[R]$ gives us $h \in \mathcal{C}(G_1)$. Since G is primitive, Lemma 2.4 (i) implies that the support of h generates a subgroup of R that is either 1 or R. Since H is nontrivial, we must have $H = \langle \mathrm{supp}(h) \rangle = R$. But then for any $r \in R$ we have $\Gamma r = \Gamma$, so $R = \Gamma R = \Gamma$. This shows that there is only one G_1 orbit of R, which is a contradiction because G_1 does not act transitively (every element of G_1 fixes 1). We conclude that $\Gamma \cap P \neq \emptyset$.

Using the two facts that $\Gamma \cap P \neq \emptyset$ and that $\Gamma - P$ is a union of complete cosets of P, we can prove that G acts 2-transitively. We do this by assuming that G does not act 2-transitively and deriving a contradiction. If this is the case, then $R - \{1\}$ is not an orbit of G_1 by Lemma 2.3. This means that the set $R - \{1\}$ must contain at least two orbits. Since there are $p - 1$ non-identity elements of P, this implies the existence of a G_1-orbit Γ that does not contain 1 and satisfies $m = |\Gamma \cap P| \leq \frac{p-1}{2}$. From the fact that $\Gamma \cap P \neq \emptyset$, we also have $m > 0$.

Now we define certain useful elements of the group ring $\mathbb{F}_p[R]$. Let

$$a = \sum_{u \in \Gamma \cap P} u, \qquad b = \sum_{u \in P} u, \qquad \text{and} \qquad c = \sum_{u \in \Gamma} u.$$

We have shown that $\Gamma - P$ is a union of cosets of P, so there exists some $d \in \mathbb{F}_p[R]$ that is the sum of certain coset representatives such that $c = a + bd$. Now if $v \in P$ then naturally $Pv = P$; this implies that $bv = b$ because b is the sum of the elements of P. It follows that when we multiply a and b, the product ab is the sum of m copies of b. This is because there are m summands in a, each of which is in P, so each summand when multiplied by b yields again b. Thus $ab = mb$. We also have $b^2 = |P|b$ by the same reasoning, and since $|P| = p = 0$ in $\mathbb{F}_p$, we have $b^2 = 0$.

Now we use the fact that $\mathcal{C}(G_1)$ is a subring of $\mathbb{F}_p[R]$. The element $c - m1$ is in $\mathcal{C}(G_1)$ because $c, 1 \in \mathcal{C}(G_1)$. This implies that $e = (c - m1)^2 \in \mathcal{C}(G_1)$ also. Using the substitution $c = a + bd$ we obtain

$$e = (a - m1 + bd)^2 = (a - m1)^2 + 2(a - m1)bd + b^2d^2 = (a - m1)^2$$

because $b^2 = 0$ and $(a - m1)bd = (ab - mb)d = 0$. Every summand in a is in P, so the support of the element $e = (a - m1)^2$ is a subset of P.

From the hypothesis that $p < n = |R|$ we have $P \neq R$. Again we can use Lemma 2.4 (i) to say that the subgroup generated by supp(e) is either 1 or R, and, since $\langle \text{supp}(e) \rangle \leq P$, it must be that $\langle \text{supp}(e) \rangle = \{1\}$. This implies that $(a - m1)^2 = \lambda 1$ for some $\lambda \in \mathbb{F}_p$. The condition $m = |\Gamma \cap P| \leq \frac{p-1}{2}$ implies that the coefficient in $(a - m1)^2 = a^2 - 2ma + m^2 1$ of each $u \neq 1$ must be nonzero. (If $m = 1$, then the coefficient of any $u \neq 1$ in $a^2 - 2ma + m^2 1$ is either 1 when $u = a^2$ or -2 when $u = a$. Otherwise, the coefficient k of any particular $u \in \Gamma \cap P$ in a^2 satisfies $0 \leq k \leq m - 1$, since for every $v \in \Gamma \cap P$ there is at most one

$w \in \Gamma \cap P$ such that $u = vw$, and $1 \notin \Gamma \cap P$. The total coefficient ℓ of u in $a^2 - 2ma + m^2 1$ therefore satisfies $-(p-1) \leq -2m \leq \ell \leq -m-1 < 0$, so ℓ is not divisible by p.) It follows that $\Gamma \cap P \subset \{1\}$. In our choice of Γ we selected an orbit that did not contain 1, which implies that $\Gamma \cap P = \emptyset$. This contradicts our previous result about G_1-orbits containing elements of P. We conclude that the orbits of G_1 on R are exactly $\{1\}$ and $R - \{1\}$, so G indeed acts 2-transitively. □

Chapter 3. Primitive Schur Rings

3.1 Primitive Schur Rings

Here we detail a type of Schur ring called a *primitive* Schur ring. Again we will consider the case where R is a finite group and G is a subgroup of $\mathrm{Sym}(R)$ that contains the image of the regular representation of R. Let $\mathfrak{S}$ be a Schur ring in the group algebra $F[R]$ with principal sets $P_0 = \{1\}, P_1, ..., P_n$. We say that $\mathfrak{S}$ is *primitive* if $i > 0$ implies $\langle P_i \rangle = R$. An equivalent characterization of a primitive Schur ring is that $\mathfrak{S}$ over R is primitive if $K = 1$ and $K = R$ are the only subgroups of R such that $\overline{K} \in \mathfrak{S}$.

As with any definition, it is important to consider if such objects even exist. To that end, there is always the trivial primitive Schur ring over any finite group R generated by the partition of R into the sets $\{1\}$ and $R - \{1\}$. Other examples are Schur rings over prime order cyclic groups. If $\mathcal{Z}_p$ is the cyclic group of order p, where p is prime, then every Schur ring over $\mathcal{Z}_p$ is primitive because every principal set (except $P_0 = \{1\}$) contains a generator of $\mathcal{Z}_p$.

In the proof of the second of the following theorems we will use two standard results that we give here without proof. Proofs may be found in [2].

Result 3.1. *A subgroup R of a group G, where G acts transitively on Ω, acts regularly on Ω if and only if $G = G_\alpha R = RG_\alpha$ and $R \cap G_\alpha = 1$ for every stabilizer G_α.*

Result 3.2. *Let $|\Omega| > 1$. If $G \leq Sym(\Omega)$ acts transitively on Ω, then G is primitive if and only if G_α is a maximal proper subgroup of G for each $\alpha \in \Omega$.*

Now for the theorems.

Theorem 3.3. *If $G \leq \mathrm{Sym}(R)$ contains the image of the regular representation of R, then G acts 2-transitively if and only if $\mathcal{C}(G_1)$ is the trivial primitive Schur ring.*

Proof. The group G acts 2-transitively if and only if the orbits of G_1 are $\{1\}$ and $R - \{1\}$ (Lemma 2.3), if and only if the principal sets of $\mathcal{C}(G_1)$ are $\{1\}$ and $R - \{1\}$. □

Theorem 3.4. *Under the hypotheses of Theorem 3.3, G is primitive if and only if $\mathcal{C}(G_1)$ is a primitive Schur ring.*

Proof. If G is not primitive, then there exists a subgroup L with $G_1 < L < G$ by Result 3.2. From the conditions that $G = G_1R$ and $G_1 \cap R = 1$ (Result 3.1), there exists a subgroup K with $1 < K < R$, $G_1 \cap K = 1$, and $L = G_1K = KG_1$. This implies that in the group algebra $F[R]$ we have $\overline{G_1}\,\overline{K} = \overline{L} = \overline{K}\,\overline{G_1}$. (The number of summands in $\overline{G_1}\,\overline{K}$ is equal to the number of summands in $\overline{L}$ since $G_1 \cap K = 1$.) Any element of the group algebra $F[R]$ that commutes with $\overline{G_1}$ is an element of $\mathcal{C}(G_1)$, so this implies that $\overline{K} \in \mathcal{C}(G_1)$.

The sums of principal sets of $\mathcal{C}(G_1)$ form a basis, so $\overline{K}$ is a sum of principal elements. Since K is not trivial, $\overline{K}$ must contain a nontrivial principal set P_i for some $i > 0$. This implies that $\langle P_i \rangle \leq K < R$, so there exists a principal set that does not generate R. Thus $\mathcal{C}(G_1)$ is not a primitive Schur ring, so one implication is proved.

Conversely, suppose that $\mathcal{C}(G_1)$ is not a primitive Schur ring. From the definition of a primitive Schur ring, there exists a nontrivial principal set P of $\mathcal{C}(G_1)$ (a nontrivial orbit of G_1) that generates a subgroup K with $1 < K < R$.

We will show that K is a union of orbits of G_1. Assume to the contrary that this is not the case. Then there exists some orbit U of G_1 with $a \in U \cap K$ and $b \in U - K$. Because P generates K, there is some m such that $\overline{P}^m$ in the group algebra contains a. However, because $\mathcal{C}(G_1)$ is a Schur ring and the expansion of $\overline{P}^m$ contains an element of the orbit U, it must contain all the elements of U. In particular, $\overline{P}^m$ contains b, which implies that $b \in K$. This is a contradiction, so K must be the union of orbits of G_1.

From this it follows that $\overline{K} \in \mathcal{C}(G_1)$. Again we use the fact that an element of $F[R]$ is in $\mathcal{C}(G_1)$ if and only if it commutes with G_1. Thus $\overline{K} \in \mathcal{C}(G_1)$ implies $\overline{G_1}\,\overline{K} = \overline{K}\,\overline{G_1}$, which in turn implies $G_1K = KG_1$. Then G_1K is a nontrivial proper subgroup of G, so G_1 is not a maximal proper subgroup. By Result 3.2 this implies that G is not primitive, completing the proof. □

These theorems show that information about Schur rings can reveal information about the underlying groups. This is partially the motivation for classifying the possible Schur rings over certain groups, which is our concern for the remainder of this work.

Chapter 4. Classification of Schur Rings over Finite Cyclic Groups

4.1 Complete Classification

In this chapter we give the result by Leung and Man [4, 5] that completely classifies Schur rings over finite cyclic groups. There are four types of Schur rings over these groups, and we provide here the necessary definitions before stating the theorem. We include this result because we later provide an extension of it when we classify Schur rings over the infinite cyclic group.

We have already discussed one type of Schur ring over any finite group, the trivial Schur ring afforded by the partition of G into principal sets $\{1\}$ and $G-\{1\}$. Naturally this is one of the types in the classification of finite cyclic groups.

If φ is an automorphism of G, then we can extend φ to be defined on the group algebra $F[G]$ in the natural way. If $\alpha = \sum_{g\in G} \lambda_g g$ is an element of $F[G]$, then we define

$$\varphi(\alpha) = \sum_{g\in G} \lambda_g \varphi(g).$$

If $\mathcal{H}$ is a subgroup of $\mathrm{Aut}(G)$ then the set of elements of $F[G]$ fixed by every element of $\mathcal{H}$ is a Schur ring over G. We denote this as

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

The partition of G that determines this Schur ring is the set of $\mathcal{H}$-orbits of G, which are sets of the form $P_h = \{g \in G \mid \varphi(h) = g \text{ for some } \varphi \in \mathcal{H}\}$. This is called an *orbit Schur ring.*

The next type of Schur ring is a construction of a new Schur ring from two existing ones. If G and H are finite groups with respective Schur rings $\mathfrak{S}$ and $\mathfrak{T}$, then we can form a Schur ring over the group $G \times H$ as follows. Here we view G and H as subgroups of $G \times H$ in the natural way. Let $\mathcal{B}$ be the partition of G that determines $\mathfrak{S}$ and let $\mathcal{C}$ be the partition of H afforded by $\mathfrak{T}$. The collection $\mathcal{D}$ of sets defined by

$$\mathcal{D} = \{BC \mid B \in \mathcal{B}, C \in \mathcal{C}\}$$

is a partition of $G \times H$ because of the uniqueness of products of elements of G and H necessitated by the definition of $G \times H$. This partition $\mathcal{D}$ determines a subring of $F[G \times H]$ with a basis $\{\overline{BC} \mid B \in \mathcal{B}, C \in \mathcal{C}\}$, and this subring is in fact a Schur ring. We denote this Schur ring as $\mathfrak{S} \cdot \mathfrak{T}$, and call this construction the *dot product* of $\mathfrak{S}$ and $\mathfrak{T}$.

The last type of Schur ring in this classification theorem is the *semi-wedge product* of Schur rings, and this is a generalization of the *wedge product* of Schur rings. The construction relies on several new definitions.

For $\alpha \in F[G]$ with $\alpha = \sum_{g \in G} \lambda_g g$, we define

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

We denote this function as $* : F[G] \to F[G]$. We also define a binary operation, denoted $\circ : F[G] \times F[G] \to F[G]$, by

$$\alpha \circ \beta = \sum_{g \in G} (\lambda_g \mu_g) g,$$

where $\alpha = \sum_{g \in G} \lambda_g g$ and $\beta = \sum_{g \in G} \mu_g g$. This is called the *Hadamard product* on $F[G]$. A result by Muzychuk [6] states that a subalgebra S of $F[G]$ is a Schur ring if and only if S is closed under $*$ and $\circ$ and $1 \in S, \overline{G} \in S$.

A *pre-Schur ring* over G is a subalgebra of $F[G]$ that is closed under $*$ and $\circ$ and contains $\overline{G}$. A pre-Schur ring is also determined by a partition of the group G; the difference here being that the principal set containing $1 \in G$ is not a singleton set, and in fact it is a nontrivial subgroup of G.

Let H be a normal subgroup of G, and consider a Schur ring $\mathfrak{S}$ with partition $\mathcal{D}$ over the quotient group G/H. Denoting the natural quotient map by $\pi : G \to G/H$, we can form a partition $\mathcal{C}$ of G by

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

Each set in $\mathcal{C}$ will be the union of cosets of H. We will denote the subalgebra generated by $\mathcal{C}$ by $\pi^{-1}(\mathfrak{S})$, and this subalgebra is in fact a pre-Schur ring over G called the *inflated Schur ring* of $\mathfrak{S}$ over G.

Now we are ready to define a wedge product of Schur rings. Let $H \trianglelefteq G$, and let $\mathfrak{S}$ and $\mathfrak{T}$ be Schur rings over H and G/H, respectively. Then $\pi^{-1}(\mathfrak{T})$ is the inflated Schur ring of $\mathfrak{T}$ over G. The *wedge product* of $\mathfrak{S}$ and $\mathfrak{T}$ is the subalgebra $\mathfrak{S}+\pi^{-1}(\mathfrak{T})$ of $F[G]$, denoted $\mathfrak{S}\wedge\mathfrak{T}$. The wedge product is a Schur ring over G. The principal sets of $\mathfrak{S}\wedge\mathfrak{T}$ are the principal sets of $\mathfrak{S}$ along with the preimages $\pi^{-1}(D)$ for every principal set $D \neq \{1\}$ of $\mathfrak{T}$.

Let $1 < K \leq H < G$ be a sequence of finite groups with $K \trianglelefteq G$. Let $\mathfrak{S}$ and $\mathfrak{T}$ be Schur rings over H and G/K, respectively. Denote the quotient map by $\pi : G \to G/K$. If $\overline{H/K} \in \mathfrak{T}$, $\overline{K} \in \mathfrak{S}$, and $\pi(\mathfrak{S}) = \mathfrak{T}_{H/K}$ (the Schur ring $\mathfrak{T}$ restricted to the subgroup H/K), then the subalgebra $\mathfrak{S}+\pi^{-1}(\mathfrak{T})$ of $F[G]$ is the *semi-wedge product* of $\mathfrak{S}$ and $\mathfrak{T}$. This product is denoted as $\mathfrak{S}\triangle_K\mathfrak{T}$ and is a Schur ring over G.

These constructions are just some of the possible ways to find Schur rings over finite groups, but together they are enough to construct all possible Schur rings over a finite cyclic group. This brings us to the statement of the classification theorem for finite cyclic groups.

Theorem 4.1. *Let G be a finite cyclic group and let $\mathfrak{S}$ be a Schur ring over G. Then one of the following is true:*

(i) $\mathfrak{S}$ is trivial, meaning $\mathfrak{S}$ is given by the partition $\{1\}, G-\{1\}$.

(ii) $\mathfrak{S}$ is an orbit Schur ring: there exists a subgroup $\mathcal{H} \leq \mathrm{Aut(G)}$ such that $\mathfrak{S}$ is given by the partition of G into orbits of $\mathcal{H}$.

(iii) *$\mathfrak{S}$ is a dot product of Schur rings: there exist nontrivial subgroups $H, K \leq G$ such that $G = H \times K$ and Schur rings $\mathfrak{S}_H$ and $\mathfrak{S}_K$ over H and K, respectively, such that $\mathfrak{S} = \mathfrak{S}_H \cdot \mathfrak{S}_K$.*

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

We say that a Schur ring is *traditional* if it is one of these four types: trivial, orbit, dot product, or (semi)-wedge product. In the next few chapters we will explore Schur rings over various infinite groups, thus expanding the work referenced here on finite groups. We will see that there exist nontraditional Schur rings over free groups but that every Schur ring over the infinite cyclic group is traditional.

Chapter 5. Schur Rings over Free Groups

In this section we shift our focus to Schur rings over infinite groups. Every Schur ring encountered so far was over a finite group; the theory of Schur rings was first developed only for such groups. Here we consider infinite groups, since the definition of a Schur ring given in Chapter 1 does not specify that the group G under consideration must be finite. The important thing to keep in mind is that the principal sets in the partition of a group must be finite, regardless of the cardinality of the group.

5.1 A Traditional Example

We denote the free group on n generators by $F_n = \langle x_1, x_2, ..., x_n \mid \emptyset\rangle$. This is the group of "words" that can be formed from the n generators $x_1, ..., x_n$ and their formal inverses. Recall that one of the traditional types of Schur rings is an orbit Schur ring, which has a partition given by orbits of a finite subgroup of the automorphism group. One such example of a subgroup of $\mathrm{Aut}(F_n)$ is the Coxeter group of type B_n.

The Coxeter group of type B_n can be represented as a permutation group on a set of order $2n$. If $\Omega = \{1, 2, ..., 2n\}$ then B_n is the permutation group on Ω generated by the following three permutations: $\alpha = (1, 2)(n + 1, n + 2), \beta = (1, 2, ..., n)(n + 1, n + 2, ..., 2n)$, and $\gamma = (1, n + 1)$. It has order $2^n n!$.

By declaring $\Omega = \{x_1, x_2, ..., x_n, x_1^{-1}, ..., x_n^{-1}\}$ to be the set of generators and inverses of F_n, we naturally see how each element of B_n acts on Ω to produce an automorphism of F_n. For example $\alpha = (x_1, x_2)(x_1^{-1}, x_2^{-1})$ generates the automorphism of F_n given by $x_1 \mapsto x_2, x_2 \mapsto x_1, x_1^{-1} \mapsto x_2^{-1}, x_2^{-1} \mapsto x_1^{-1}$, and all other generators and inverses are fixed.

The partition of F_n into the orbits of B_n (or any subgroup of B_n) will produce a traditional Schur ring over F_n. We illustrate a concrete construction here. Let $n = 2$. (Even stepping up to $n = 3$ makes the group B_n grow to order 48, so we will keep things simple.) With $F_2 = \langle a, b\rangle$ and $\Omega = \{a, b, a^{-1}, b^{-1}\}$, the group B_2 is generated by $\alpha = \beta = (a, b)(a^{-1}, b^{-1})$

and $\gamma = (a, a^{-1})$; B_2 has order 8. We note that B_2 acts transitively on Ω, which means that Ω is a principal set. To find orbits of another element, say ab, we take each $\varphi \in B_2$ and compute $\varphi(ab) = \varphi(a)\varphi(b)$. We note that this implies that $\varphi(ab)$ is itself the product of two generators or inverses. Thus the action of B_n preserves the length of elements of F_n, which we will investigate more in the next section. A few principal sets of the partition of F_2 are

$$\begin{aligned} P_0 &= \{1\}, & P_2 &= \{ab, ab^{-1}, ba, ba^{-1}, a^{-1}b, a^{-1}b^{-1}, b^{-1}a, b^{-1}a^{-1}\}, \\ P_1 &= \{a, b, a^{-1}, b^{-1}\}, & P_3 &= \{a^2, b^2, a^{-2}, b^{-2}\}. \end{aligned}$$

5.2 A Nontraditional Schur Ring over a Free Group

Given an element x of $F_n = \langle x_1, ..., x_n\rangle$, there exists a representation of the element using the fewest number of the given generators and their inverses; the number of letters in this smallest representation is the *length* of x and is denoted by $|x|$. For example, $|x_1^2 x_1^{-1} x_2| = |x_1 x_2| = 2$ and $|x_4^{-2} x_1^3| = 5$.

We can form a Schur ring over F_n in the following way. Partition F_n into principal sets $P_0, P_1, P_2, ...$ defined by $P_i = \{x \in F_n : |x| = i\}$. Each set contains all the elements of F_n having a given length. As an example, consider the free group on two generators, $F_2 = \langle a, b\rangle$. The sets in the partition are

$$\begin{aligned} P_0 &= \{1\}, \\ P_1 &= \{a, b, a^{-1}, b^{-1}\}, \\ P_2 &= \{a^2, b^2, a^{-2}, b^{-2}, ab, a^{-1}b, ab^{-1}, a^{-1}b^{-1}, ba, ba^{-1}, b^{-1}a, b^{-1}a^{-1}\}, \text{ etc.} \end{aligned}$$

Partitioning F_n into these sets satisfies the properties of a Schur ring because

(i) each P_i is finite (there being only finitely many possible words of a given length due to the number of generators being finite),

(ii) $P_0 = \{1\}$ (the only word of length zero is the identity),

(iii) $P_i = P_i^{-1}$ for each i (since the inverse of a word has the same length as the original word), and

(iv) for $k \leq m$,

$$\overline{P_k}\,\overline{P_m} = \lambda_{m-k}\overline{P_{m-k}} + \lambda_{m-k+2}\overline{P_{m-k+2}} + \cdots + \lambda_{m+k}\overline{P_{m+k}};$$

here $\lambda_i \in \mathbb{N}$, as we now show (so the product of principal elements is a linear combination of principal elements.)

In (iv) above, the product of a word of length k and a word of length m is a word of length at most $m+k$ if there is no cancellation. If there is cancellation between the two terms, it occurs in pairs (hence the increments of 2 in the indices); maximum cancellation completely cancels the shorter word (here of length k), so the minimum length is $m-k$. Because each principal element contains *all* the words of that length, all possible words of lengths $m-k$ to $m+k$ in increments of 2 will occur. The coefficients can be determined as $\lambda_{m+k-2\ell} = (2n-1)^{\ell-1}(2n-2)$, as follows.

Consider P_k and P_m with $k \leq m$. Let $0 \leq \ell \leq k$ and $t = m+k-2\ell$. Given any word $w = w_1 \cdots w_t$ of length t, the coefficient of w in the product $\overline{P_k}\,\overline{P_m}$ is the number of ways $w_1 \cdots w_t$ can be written as a product uv of words u and v where $|u| = k$ and $|v| = m$. If $uv = w$, then by comparing the lengths of u, v, and w we must have that the last ℓ letters of u cancel with the first ℓ letters of v to form a word of length $t = m+k-2\ell$.

We can write out $w = w_1 \cdots w_t$ as the product of what remains of u and v after all the inverse pairs have been canceled. We get $w = (w_1 \cdots w_{k-\ell})(w_{k-\ell+1} \cdots w_t)$. We have canceled a word $x_1 \cdots x_\ell$ of length ℓ with its inverse, so when we insert these back in we obtain $(w_1 \cdots w_{k-\ell})(x_1 \cdots x_\ell)(x_\ell^{-1} \cdots x_1^{-1})(w_{k-\ell+1} \cdots w_t)$. Thus the number of ways w can be written as a product uv is the number of words $x_1 \cdots x_\ell$ of length ℓ such that $x_1 \neq w_{k-\ell}$ and $x_1^{-1} \neq w_{k-\ell+1}$. Since $w_{k-\ell}$ and $w_{k-\ell+1}$ are not inverses (otherwise they too would cancel in the end), this puts two restrictions on x_1, namely $x_1 \neq w_{k-\ell}$ and $x_1 \neq w_{k-\ell+1}^{-1}$. Thus there are $2n-2$ possible choices for x_1. There are $2n-1$ possible choices for x_2, since the only restriction is $x_2 \neq x_1^{-1}$. Similarly there are $2n-1$ possible choices for each x_i where $2 \leq i \leq \ell$.

This gives a total of $(2n-1)^{\ell-1}(2n-2)$ distinct words of length ℓ that satisfy these conditions. Because *all* words of length k appear in P_k and *all* words of length m appear in P_m, all of the possible combinations of words $u \in P_k$ and $v \in P_m$ that have these ℓ letters that cancel will occur, so each word of length $t = m+k-2\ell$ appears $(2n-1)^{\ell-1}(2n-2)$ times in the product $\overline{P_k}\,\overline{P_m}$. The case when $k > m$ is similar.

Additionally, the cardinality of P_i can be shown to be $|P_i| = (2n)(2n-1)^{i-1}$ as follows: Given a word of length i, there are $2n$ choices for the first letter, since there are n generators and n inverses of these generators. For the second letter, the inverse of the first letter cannot be chosen because it would cancel the first letter and leave a word of length less than i. However, all other $2n-1$ generating letters (or inverses) are available, and this holds for each successive letter. Thus there are $(2n)(2n-1)^{i-1}$ distinct words of length i, so this is the cardinality of the set P_i.

One final property of this construction to note is that this Schur ring is not an orbit Schur ring for $n \geq 2$. If this were the case, then because the principal set P_2 contains the elements x_1^2 and x_1x_2, there must be some automorphism of F_n such that $x_1^2 \mapsto x_1x_2$. No such automorphism exists, since this would require that x_1x_2 was equal to some square a^2 where $x_1 \mapsto a$. Additionally, the free group F_n has no nontrivial finite subgroups, which are required in the decomposition of a Schur ring into a dot product or wedge product. The trivial Schur ring construction is also impossible, since $F_n - \{1\}$ is not finite. A Schur ring $\mathfrak{S}$ over F_n is therefore traditional if and only if $\mathfrak{S}$ is an orbit Schur ring. This shows that there exist Schur rings over free groups that are nontraditional, since the Schur rings just constructed are not orbit Schur rings.

5.3 Variations on Nontraditional Schur Rings

Once we have a nontraditional Schur ring we can use automorphisms to construct more nontraditional Schur rings. Given a Schur ring with principal sets $\{P_i\}_{i\in I}$ (where I contains a distinguished element 0) over a group G and an automorphism $\varphi \in \operatorname{Aut}(G)$, the sets $\{\varphi(P_i)\}_{i\in I}$ form a partition of G that produces a Schur ring.

This is relatively simple to see. Clearly the sets $\{\varphi(P_0)\}_{i\in I}$ do form a partition of G into finite sets because φ is a bijection and each P_i is finite. The set $\varphi(P_0) = \{\varphi(1)\} = \{1\}$ consists of the identity because φ is a homomorphism. Since $\varphi(g^{-1}) = \varphi(g)^{-1}$ for every $g \in G$, the set consisting of the inverses of the elements of $\varphi(P_i)$ will be the set $\varphi(P_i^{-1})$, which will be an element of the partition. And finally, for each pair P_i, P_j there are scalars $\lambda_k \in F$ indexed by some $K \subset I$ with $|K| < \infty$ so that

$$\overline{P_i}\,\overline{P_j} = \sum_{k\in K} \lambda_k \overline{P_k},$$

and these same scalars will cause the equation

$$\overline{\varphi(P_i)}\ \overline{\varphi(P_j)} = \sum_{k\in K} \lambda_k \overline{\varphi(P_k)}$$

to hold in the group algebra because φ is a homomorphism. These facts together show that φ does produce a new Schur ring from an existing one.

As an example, consider the Schur ring $\mathfrak{S}$ over $F_2 = \langle a, b\rangle$ constructed in the previous section, with principal sets $P_i = \{x \in F_2 : |x| = i\}$. Define a homomorphism $\varphi : F_2 \to F_2$ by

$$\begin{aligned} \varphi : a &\mapsto ab, \\ b &\mapsto b \end{aligned}$$

on the generators. This is an automorphism of F_2, so the images of the principal sets of $\mathfrak{S}$ will produce a partition for a Schur ring. The interesting thing to note here is that this automorphism gives a different Schur ring because it maps a word of length 1 to a word of length 2, which results in sets that no longer contain words of a single length. We can see this in the first few principal sets of the new Schur ring:

$$\varphi(P_0) = \{1\},$$

$$\varphi(P_1) = \{ab, b, b^{-1}a^{-1}, b^{-1}\},$$

$$\varphi(P_2) = \{abab, b^2, b^{-1}a^{-1}b^{-1}a^{-1}, b^{-2}, ab^2, b^{-1}a^{-1}b, a, b^{-1}a^{-1}b^{-1}, bab, a^{-1}, b^{-1}ab, b^{-2}a^{-1}\}.$$

The set $\varphi(P_2)$ contains words of lengths 1, 2, 3, and 4. Naturally this Schur ring over F_2 is not an orbit Schur ring, since that would require some automorphism $\sigma \in \mathrm{Aut}(F_2)$ such that $\sigma(b^2) = a$, and a is not a square in F_n.

Chapter 6. Schur Rings over Some Infinite Torsion Groups

6.1 A First Example

We'll start with an example. Consider the additive subgroup $\mathbb{Z}(2^\infty)$ of $\mathbb{Q}/\mathbb{Z}$ consisting of all elements with order 2^k for some $k = 0, 1, 2, \ldots.$ These elements can all be represented as $\frac{a}{2^k}$ for some odd a satisfying $1 \leq a \leq 2^k$.

Let $A_0 = \{0\}$, and for each $k \geq 1$ define

$$A_k = \left\{\frac{a}{2^k} : 1 \leq a \leq 2^k, a \equiv 1 \bmod 4\right\} \qquad \text{and} \qquad B_k = \left\{\frac{b}{2^k} : 1 \leq b \leq 2^k, b \equiv 3 \bmod 4\right\}.$$

Thus

$$\begin{aligned} A_1 = B_1 &= \left\{\frac{1}{2}\right\}, \\ A_2 &= \left\{\frac{1}{4}\right\}, B_2 = \left\{\frac{3}{4}\right\}, \\ A_3 &= \left\{\frac{1}{8}, \frac{5}{8}\right\}, B_3 = \left\{\frac{3}{8}, \frac{7}{8}\right\}, \text{ etc.} \end{aligned}$$

This is a partition of $\mathbb{Z}(2^\infty)$ into finite sets, and we will show that this induces a Schur ring over $\mathbb{Z}(2^\infty)$. For $k \geq 2$, we note that A_k and B_k both contain 2^{k-2} elements, since there are 2^{k-1} odd integers less than 2^k and each set contains elements with half of the odd numerators.

By construction $\{0\}$ is a principal set. We have $A_1 = A_1^{-1}$, and for $k \geq 2$, $a \equiv 1 \bmod 4$ implies that $2^k - a \equiv 3 \bmod 4$ since $4 \mid 2^k$. Thus for a given $\frac{a}{2^k}$ with $a \equiv 1 \bmod 4$ the inverse $\frac{b}{2^k} = \frac{2^k - a}{2^k}$ satisfies $b \equiv 3 \bmod 4$. The inverse of an element of A_k is therefore an element of B_k, and since A_k and B_k have the same number of elements it follows that $A_k^{-1} = B_k$. Taking inverses gives $B_k^{-1} = A_k$.

The last thing to show is that the product of two of these principal elements in the group algebra is a linear combination of principal elements. We will first show that the product of any group element $\frac{s}{2^j}$ and a principal element $\overline{A_k}$ is always a linear combination of principal elements when $j \leq k$.

Set $e = \frac{s}{2^j}$ for some odd s and $j \geq 1$. Consider the product $e\,\overline{A_k}$ in the group algebra. Assume first that $j \leq k-2$. Then

$$\begin{aligned} e\,\overline{A_k} &= \left(\frac{s}{2^j}\right)\left(\frac{1}{2^k} + \frac{5}{2^k} + \cdots + \frac{2^k-3}{2^k}\right) \\ &= \frac{2^{k-j}s+1}{2^k} + \frac{2^{k-j}s+5}{2^k} + \cdots + \frac{2^{k-j}s+2^k-3}{2^k} \\ &= \overline{A_k}. \end{aligned}$$

This is because $2^{k-j} \geq 4$, so $2^{k-j}s$ is 0 mod 4. This makes $2^{k-j}s + a \equiv a \equiv 1$ mod 4. Every element in the sum above is therefore an element of A_k, and because we are adding the same quantity $2^{k-j}s$ to each numerator we will get a permutation of the elements of A_k.

When $j = k-1$ then $2^{k-j} = 2$. This makes every numerator in the sum calculated above congruent to 3 mod 4. Thus every $\frac{2s+a}{2^k}$ is an element of B_k, and adding $2s$ to every $a \equiv 1$ mod 4 gives a permutation of B_k. Thus $e\,\overline{A_k} = \overline{B_k}$ in this case.

Finally assume $j = k \geq 2$. (The cases of $k = 0, 1$ are similar.) Then either $\frac{s}{2^k} \in A_k$ or $\frac{s}{2^k} \in B_k$. In the first case we can reorder the elements of A_k as $\frac{s}{2^k}, \frac{s+4}{2^k}, \frac{s+8}{2^k}, \frac{s+12}{2^k}, \ldots, \frac{s+4(2^{k-2}-1)}{2^k}$. Then

$$\begin{aligned} e\,\overline{A_k} &= \frac{2s}{2^k} + \frac{2s+4}{2^k} + \frac{2s+8}{2^k} + \frac{2s+12}{2^k} + \cdots + \frac{2s+4(2^{k-2}-1)}{2^k} \\ &= \frac{s}{2^{k-1}} + \frac{s+2}{2^{k-1}} + \frac{s+4}{2^{k-1}} + \frac{s+6}{2^{k-1}} + \cdots + \frac{s+2(2^{k-2}-1)}{2^{k-1}} \\ &= \overline{A_{k-1}} + \overline{B_{k-1}}, \end{aligned}$$

because $s + 2m$ for $0 \leq m \leq 2^{k-2}-1$ runs over all odd integers less than 2^{k-1} exactly once.

If $\frac{s}{2^k} \in B_k$, then we can reorder the elements of A_k as $\frac{t}{2^k}, \frac{t+4}{2^k}, \frac{t+8}{2^k}, \frac{t+12}{2^k}, \ldots, \frac{t+4(2^{k-2}-1)}{2^k}$ where $s+t=2^k$, because the inverse of $\frac{s}{2^k}$ is an element of A_k.

This gives us

$$\begin{aligned}
e\,\overline{A_k} &= \frac{s+t}{2^k} + \frac{s+t+4}{2^k} + \frac{s+t+8}{2^k} + \frac{s+t+12}{2^k} + \cdots + \frac{s+t+4(2^{k-2}-1)}{2^k} \\
&= \frac{0}{2^k} + \frac{4}{2^k} + \frac{8}{2^k} + \frac{12}{2^k} + \cdots + \frac{4(2^{k-2}-1)}{2^k} \\
&= 0 + \frac{1}{2^{k-2}} + \frac{2}{2^{k-2}} + \frac{3}{2^{k-2}} + \cdots + \frac{(2^{k-2}-1)}{2^{k-2}} \\
&= \overline{A_{k-2}} + \overline{B_{k-2}} + \overline{A_{k-3}} + \overline{B_{k-3}} + \cdots + \overline{A_1} + \overline{A_0}.
\end{aligned}$$

In every case, $e\,\overline{A_k}$ is a sum of principal elements.

The same type of argument shows that $e\,\overline{B_k}$ is equal to $\overline{B_k}$ (when $j \leq k-2$), $\overline{A_k}$ (when $j = k-1$), $\overline{A_{k-1}} + \overline{B_{k-1}}$ (when $j = k$ and $e \in B_k$), or $\overline{A_0} + \overline{A_1} + \sum_{i=2}^{k-2} \overline{A_i} + \overline{B_i}$ (when $j = k \geq 2$ and $e \in A_k$).

Given two principal sets A_j, A_k we can assume $j \leq k$ and write $\overline{A_j} = e_1 + \cdots + e_{2^{j-2}}$ where the e_i are the individual elements of A_j. Then

$$\overline{A_j}\,\overline{A_k} = \sum_{i=1}^{2^{j-2}} e_i\,\overline{A_k}.$$

Because each $e_i\,\overline{A_k}$ is a linear combination of principal elements, this shows that $\overline{A_j}\,\overline{A_k}$ is a linear combination of principal elements. Because G is abelian, $\overline{A_k}\,\overline{A_j} = \overline{A_j}\,\overline{A_k}$, so any product of two A sets is a linear combination of principal elements.

Similarly, all products of the form $\overline{A_j}\,\overline{B_k}, \overline{B_j}\,\overline{A_k}$, and $\overline{B_j}\,\overline{B_k}$ are linear combinations of principal elements. This proves that this partition of $\mathbb{Z}(2^\infty)$ produces a Schur ring.

6.2 A General Construction

We can extend this construction to $\mathbb{Z}(p^\infty)$ for any prime p. Let $G = \mathbb{Z}(p^\infty) \leq \mathbb{Q}/\mathbb{Z}$, the group of all elements of order p^k for some $k \in \mathbb{N}$. These are represented as rational numbers of the form $\frac{a}{p^k}$ modulo 1. Fix some $n \in \mathbb{N}$, and for each j such that $1 \leq j \leq p^n$ and $\gcd(j, p) = 1$ and each $k \in \mathbb{N}$, define

$$A_{j,k} = \left\{ \frac{a}{p^k} \in \mathbb{Z}(p^\infty) : a \equiv j \bmod p^n \right\}.$$

We claim that $\{A_{j,k}\}$ along with $A_0 = \{0\}$ forms a Schur ring over $\mathbb{Z}(p^\infty)$. (In certain cases it may be that $A_{j,k} = A_{i,k}$ for some $i \neq j$. In these cases we ignore any duplicates and choose one representation for each set. This is important in the upcoming computations, when we leave duplicates out of summations to avoid overcounting.) The sets $A_{j,k}$ form a partition of $\mathbb{Z}(p^\infty)$ because any element $\frac{a}{p^k}$ written in lowest terms is in exactly one of the sets $A_{j,k}$, since the integer a not divisible by p is congruent to exactly one such j between 1 and p^n modulo p^n. Each set $A_{j,k}$ is clearly finite, and $A_0 = \{0\}$ satisfies the identity element condition of the partition.

If $k \leq n$, then $A_{j,k}$ consists of a single element. When $k > n$ there are $\varphi(p^n) = p^{n-1}(p-1)$ sets $A_{j,k}$ since this is the number of positive integers $j \leq p^n$ relatively prime to p^n. There are $\varphi(p^k) = p^{k-1}(p-1)$ positive integers smaller than and relatively prime to p^k, so this is the number of elements of G with denominator p^k in reduced form. Each $A_{j,k}$ has an equal number of elements, which is therefore $\frac{p^{k-1}(p-1)}{p^{n-1}(p-1)} = p^{k-n}$ when $k > n$.

We now show that the partition $\{A_0, A_{j,k}\}$ forms a Schur ring over G. For a given $A_{j,k}$, the integer $i = p^k - j$ is relatively prime to p^n. The (additive) inverse of $\frac{a}{p^k}$ is $\frac{p^k-a}{p^k}$, and $a \equiv j \bmod p^n$ implies that $p^k - a \equiv p^k - j \equiv i \bmod p^n$. Thus $A_{i,k}$ contains the inverse of every element of $A_{j,k}$. The sets $A_{j,k}$ and $A_{i,k}$ have the same number of elements, which implies $A_{j,k}^{-1} = A_{i,k}$.

To prove the product of principal elements is a linear combination of principal elements we use a similar strategy as in the proof of the example preceding this. Let $e = \frac{s}{p^k}$ where $\gcd(s, p) = 1$. Let $A_{i,m}$ be a principal set with $k \leq m$. We note that we can express the elements of $A_{i,m}$ as $\frac{t}{p^m}$, $\frac{t+p^n}{p^m}$, $\frac{t+2p^n}{p^m}$, ..., $\frac{t+(r-1)p^n}{p^m}$ for some t with $\gcd(t, p) = 1$, where $r = p^{m-n}$ is the number of elements in $A_{i,m}$. We assume throughout that $m > n$, otherwise every individual summand in the product $e\,\overline{A_{i,m}}$ has denominator at most $p^m \leq p^n$ and is therefore in its own principal set.

Assume $k \leq m-1$. Then $p^{m-k}s$ is a multiple of p, which implies that $p^{m-k}s+t$ is not divisible by p because $\gcd(t,p)=1$.

Then letting $h = p^{m-k}s+t$ gives

$$\begin{aligned}
e\,\overline{A_{i,m}} &= \left(\frac{s}{p^k}\right)\left(\frac{t}{p^m}+\frac{t+p^n}{p^m}+\frac{t+2p^n}{p^m}+\cdots+\frac{t+(r-1)p^n}{p^m}\right)\\
&= \frac{p^{m-k}s+t}{p^m}+\frac{p^{m-k}s+t+p^n}{p^m}+\frac{p^{m-k}s+t+2p^n}{p^m}+\cdots+\frac{p^{m-k}s+t+(r-1)p^n}{p^m}\\
&= \frac{h}{p^m}+\frac{h+p^n}{p^m}+\frac{h+2p^n}{p^m}+\cdots+\frac{h+(r-1)p^n}{p^m}\\
&= \overline{A_{h,m}}.
\end{aligned}$$

This takes care of the case where $k \leq m-1$.

Now assuming that $k=m$ there are two cases to consider. The first case is $e \in A_{i,m}^{-1}$. This means that we can stipulate that $s+t = p^m \equiv 0 \bmod p$ when we choose t in the representation of $A_{i,m}$.

In this case the product simplifies to

$$\begin{aligned}
e\,\overline{A_{i,m}} &= \left(\frac{s}{p^m}\right)\left(\frac{t}{p^m}+\frac{t+p^n}{p^m}+\frac{t+2p^n}{p^m}+\cdots+\frac{t+(r-1)p^n}{p^m}\right)\\
&= \frac{s+t}{p^m}+\frac{s+t+p^n}{p^m}+\frac{s+t+2p^n}{p^m}+\cdots+\frac{s+t+(r-1)p^n}{p^m}\\
&= \frac{0}{p^m}+\frac{p^n}{p^m}+\frac{2p^n}{p^m}+\cdots+\frac{(r-1)p^n}{p^m}\\
&= 0+\frac{1}{p^{m-n}}+\frac{2}{p^{m-n}}+\frac{3}{p^{m-n}}+\cdots+\frac{r-1}{p^{m-n}}\\
&= 0+\frac{1}{p^{m-n}}+\frac{2}{p^{m-n}}+\frac{3}{p^{m-n}}+\cdots+\frac{p^{m-n}-1}{p^{m-n}}\\
&= \overline{A_0}+\sum_{k=1}^{m-n}\sum_{\substack{1\leq j\leq p^n\\ \gcd(j,p)=1}}\overline{A_{j,k}}.
\end{aligned}$$

Here we note the omission of any duplicate sets in the summation above; each set appears only once in the sum. This finishes this case in which $e \in A_{i,m}^{-1}$.

The last case to consider is when $e \notin A_{i,m}^{-1}$. In this case it may be that $s + t = p^u v$ for some $0 \leq u \leq m$ and $p \nmid v$. Then

$$\begin{aligned} e\,\overline{A_{i,m}} &= \left(\frac{s}{p^m}\right)\left(\frac{t}{p^m} + \frac{t+p^n}{p^m} + \frac{t+2p^n}{p^m} + \cdots + \frac{t+(r-1)p^n}{p^m}\right) \\ &= \frac{p^u v}{p^m} + \frac{p^u v + p^n}{p^m} + \frac{p^u v + 2p^n}{p^m} + \cdots + \frac{p^u v + (r-1)p^n}{p^m} \\ &= \frac{v}{p^{m-u}} + \frac{v+p^{n-u}}{p^{m-n}} + \frac{v+2p^{n-u}}{p^{m-n}} + \frac{v+3p^{n-u}}{p^{m-n}} + \cdots + \frac{v+(r-1)p^{n-u}}{p^{m-n}}. \end{aligned}$$

The terms $\frac{v+xp^{n-u}}{p^{m-u}}$ will be in distinct principal sets for $0 \leq x < p^u$, since xp^{n-u} are distinct modulo p^n for these values of x. But for the next set of x values $p^u \leq x < 2p^u$ we will get one additional element from each of the principal sets from the first set of x values. This continues up to the last set $(p^{m-n} - p)(p^u) \leq x \leq (p^{m-n} - 1)(p^u)$. Thus we have divided the p^{m-n} terms in the product $e\,\overline{A_{i,m}}$ into p^u sets each with p^{m-n-u} distinct elements. Since the principal sets with denominator p^{m-u} have p^{m-n-u} elements, this accounts for the complete principal sets. Thus $e\,\overline{A_{i,m}}$ is the sum of principal elements in this case also. (In the event that $m - u \leq n$ this breaks down into a sum of singleton principal elements.)

This concludes showing that $e\,\overline{A_{i,m}}$ is a linear combination of principal elements for any $e = \frac{s}{p^k}$ with $k \leq m$. The general result that $\overline{A_{j,k}}\,\overline{A_{i,m}}$ is a linear combination of principal elements when $k \leq m$ follows from writing $\overline{A_{j,k}} = e_1 + \cdots + e_{p^{k-n}}$ and using

$$\overline{A_{j,k}}\,\overline{A_{i,m}} = \sum_{\ell=1}^{p^{k-n}} e_\ell\,\overline{A_{i,m}},$$

since $e_\ell\,\overline{A_{i,m}}$ is a linear combination of principal elements for every ℓ. When $k > m$ we use commutativity, since $\overline{A_{j,k}}\,\overline{A_{i,m}} = \overline{A_{i,m}}\,\overline{A_{j,k}}$. This completes showing that $\{A_0, A_{j,k}\}$ forms a Schur ring over $G = \mathbb{Z}(p^\infty)$.

We have therefore proved

Proposition 6.1. *Let p be prime, and fix some $n \in \mathbb{N}$. The partition of $\mathbb{Z}(p^\infty)$ into sets of the form*

$$A_{j,k} = \left\{ \frac{a}{p^k} \in \mathbb{Z}(p^\infty) : a \equiv j \ mod \ p^n \right\}$$

for each pair j, k where $k \in \mathbb{N}$, $1 \leq j \leq p^n$ and $\gcd(j, p) = 1$, along with $A_0 = \{0\}$, produces a Schur ring over $\mathbb{Z}(p^\infty)$.

Chapter 7. Schur Rings over Free Abelian Groups

In this chapter we introduce Schur rings over groups of the form $\mathcal{Z}^n$, the free abelian groups. Our notation will be multiplicative, with $\mathcal{Z}^n = \langle x_1, x_2, ..., x_n \mid x_ix_j = x_jx_i \text{ for all } i,j\rangle$. Elements of $\mathcal{Z}^n$ will therefore be of the form $x_1^{a_1}\cdots x_n^{a_n}$ where $a_1, ..., a_n \in \mathbb{Z}$.

In this chapter we prove some general results about principal elements of Schur rings over $\mathcal{Z}^n$. We will employ these to completely classify Schur rings over the infinite cyclic group $\mathcal{Z}$ in the next chapter.

7.1 Some General Results

For this section, let n be a positive integer and let $\mathfrak{S}$ be a Schur ring over $\mathcal{Z}^n$. We will call an element $x_1^{a_1}\cdots x_n^{a_n}$ of $\mathcal{Z}^n$ *primitive* if $\gcd(a_1, ..., a_n) = 1$. For brevity, we will usually denote an element of $\mathcal{Z}^n$ by $x^\alpha = x_1^{a_1}\cdots x_n^{a_n}$ where $\alpha = (a_1, a_2, ..., a_n)$. For a given integer m, we will define $m\alpha = (ma_1, ma_2, ..., ma_n)$ so that $x^{m\alpha} = (x^\alpha)^m$, and for given n-tuples $\alpha = (a_1, ..., a_n)$ and $\beta = (b_1, ..., b_n)$ we will define $\alpha + \beta = (a_1 + b_1, ..., a_n + b_n)$ so that $x^{\alpha+\beta} = x^\alpha x^\beta$. Occasionally we will also use the notation x^m to mean $x_1^m \cdots x_n^m$ where m is an integer. The principal set in the partition defining $\mathfrak{S}$ containing the element x^α will be denoted as P_α.

Lemma 7.1. *Let $x^\alpha = x_1^{a_1}\cdots x_n^{a_n}$ be an element of $\mathcal{Z}^n$. Suppose that there is some $r \in \mathbb{N}$ such that $\{(x^\alpha)^r\} = \{x^{r\alpha}\}$ is a principal set. Let $m \in \mathbb{N}$ be the smallest such natural number. Then for all integers $j, k \in \mathbb{Z}$, the equation $P_{(k+jm)\alpha} = (x^\alpha)^{jm}P_{k\alpha}$ holds.*

Proof. For any β, we can write the principal element of $\mathfrak{S}$ containing x^β as $\overline{P_\beta} = x^\beta + \overline{A_\beta}$. Here we simply have $A_\beta = P_\beta - \{x^\beta\}$.

Because $\{x^{m\alpha}\}$ is a principal set, $\{x^{-m\alpha}\}$ is also a principal set. Then for $k \in \mathbb{Z}$, the product of $x^{-m\alpha}$ and $\overline{P_{(m+k)\alpha}}$ in the group algebra is a product of principal elements and is therefore a linear combination of principal elements. Written out, we have

$$x^{-m\alpha}\overline{P_{(m+k)\alpha}} = x^{-m\alpha}(x^{(m+k)\alpha} + \overline{A_{(m+k)\alpha}}) = x^{k\alpha} + x^{-m\alpha}\overline{A_{(m+k)\alpha}}.$$

Since $x^{(m+k)\alpha}$ has coefficient 1 in $P_{(m+k)\alpha}$, the element $x^{k\alpha}$ has coefficient 1 in $x^{-m\alpha}P_{(m+k)\alpha}$. Thus the principal set $P_{k\alpha}$ appears with coefficient 1 in this sum. (All monomials in the sum have coefficient 1.) This allows us to write

$$x^{-m\alpha}\overline{P_{(m+k)\alpha}} = x^{k\alpha} + x^{-m\alpha}\overline{A_{(m+k)\alpha}} = \overline{P_{k\alpha}} + \overline{B_{(m+k)\alpha}} = x^{k\alpha} + \overline{A_{k\alpha}} + \overline{B_{(m+k)\alpha}},$$

where $B_{(m+k)\alpha}$ contains all the elements in the sum that are not in $P_{k\alpha}$. By subtracting $x^{k\alpha}$ and multiplying by $x^{m\alpha}$ we have the equation

$$\overline{A_{(m+k)\alpha}} = x^{m\alpha}(\overline{A_{k\alpha}} + \overline{B_{(m+k)\alpha}}). \tag{7.1}$$

Using this same process we can write

$$x^{m\alpha}\overline{P_{k\alpha}} = x^{m\alpha}(x^{k\alpha} + \overline{A_{k\alpha}}) = x^{(m+k)\alpha} + x^{m\alpha}\overline{A_{k\alpha}} = x^{(m+k)\alpha} + \overline{A_{(m+k)\alpha}} + \overline{C_{(m+k)\alpha}},$$

where again $C_{(m+k)\alpha}$ is simply the set containing all elements in the sum not in $P_{(m+k)\alpha}$. Here we subtract $x^{(m+k)\alpha}$ and multiply by $x^{-m\alpha}$ to obtain $\overline{A_{k\alpha}} = x^{-m\alpha}(\overline{A_{(m+k)\alpha}} + \overline{C_{(m+k)\alpha}})$.

Now we substitute this expression for $\overline{A_{k\alpha}}$ into Equation (7.1), which gives

$$\begin{aligned}\overline{A_{(m+k)\alpha}} &= x^{m\alpha}(\overline{A_{k\alpha}} + \overline{B_{(m+k)\alpha}})\\ &= x^{m\alpha}(x^{-m\alpha}(\overline{A_{(m+k)\alpha}} + \overline{C_{(m+k)\alpha}}) + \overline{B_{(m+k)\alpha}})\\ &= \overline{A_{(m+k)\alpha}} + \overline{C_{(m+k)\alpha}} + x^{m\alpha}\overline{B_{(m+k)\alpha}}.\end{aligned}$$

This implies that the sets $B_{(m+k)\alpha}$ and $C_{(m+k)\alpha}$ are both empty, since the coefficient of every element in the sum is nonnegative. The equation $\overline{A_{(m+k)\alpha}} = x^{m\alpha}(\overline{A_{k\alpha}} + \overline{B_{(m+k)\alpha}})$ then simplifies to $\overline{A_{(m+k)\alpha}} = x^{m\alpha}\overline{A_{k\alpha}}$, so $A_{(m+k)\alpha} = x^{m\alpha}A_{k\alpha}$.

Induction on j using the same argument yields $A_{(k+jm)\alpha} = x^{jm\alpha}A_{k\alpha}$ for all integers k, j. Thus

$$\overline{P_{(k+jm)\alpha}} = x^{(k+jm)\alpha} + x^{jm\alpha}\overline{A_{k\alpha}} = x^{jm\alpha}(x^{k\alpha} + \overline{A_{k\alpha}}) = x^{jm\alpha}\overline{P_{k\alpha}}.$$

It follows that $P_{(k+jm)\alpha} = x^{jm\alpha}A_{k\alpha} = (x^{\alpha})^{jm}P_{k\alpha}$, and this proves Lemma 7.1. □

Lemma 7.2. *Let x^{α} be an element of the group $\mathcal{Z}^n$. If $\{x^{m\alpha}\}$ is a principal set for some m, then $\{x^{\alpha}\}$ is a principal set.*

Proof. Let m be the least positive integer such that $\{x^{m\alpha}\}$ is a principal set of the Schur ring $\mathfrak{S}$ over $\mathcal{Z}^n$. We will show that $m = 1$.

To do this, we impose an ordering on n-tuples of integers. Given n-tuples $\rho = (r_1, ..., r_n)$ and $\sigma = (s_1, ..., s_n)$, we say that $\rho < \sigma$ if $r_1 < s_1$, or if $r_1 = s_1$ and $r_2 < s_2$, and so on. In other words, if there exists some k such that $1 \leq k \leq n$ and $r_i = s_i$ for all $1 \leq i < k$ and $r_k < s_k$, then $\rho < \sigma$. We note that if $\rho < \sigma$, then $k\rho < k\sigma$ for any positive integer k; similarly $k\sigma < k\rho$ for any negative integer k.

We consider the principal set P_{α} containing x^{α}. Here we use a result of Wielandt ([7], Theorem 23.9; see also [8]) extended to infinite abelian groups. The original result states that for a Schur ring $\mathfrak{S}$ over an abelian group of order n and an element $c = \sum \lambda_u u \in \mathfrak{S}$, the element $c^{(m)} = \sum \lambda_u u^m$ is also an element of $\mathfrak{S}$ whenever m and n are relatively prime. Since $\mathcal{Z}^n$ is a torsion-free group, we can extend this theorem to assert that $c^{(m)}$ is an element of $\mathfrak{S}$ for *every* $m \in \mathbb{Z}$ and $c \in \mathfrak{S}$, as follows. From the relations $(\lambda c + \mu d)^{(m)} = \lambda c^{(m)} + \mu d^{(m)}$ and $c^{(mm')} = (c^{(m)})^{(m')}$ in the group ring, it suffices to show that $c^{(p)} \in \mathfrak{S}$ for a prime p and $c = \sum u$. (Note every nonzero coefficient in the sum is 1.) Then $c^p \equiv c^{(p)} \bmod p$ in the group ring, since $\mathcal{Z}^n$ is abelian. From [7] we know that reducing the coefficients of a sum in $\mathfrak{S}$ modulo p again yields an element of $\mathfrak{S}$. Since $c^p \in \mathfrak{S}$, this means that $c^{(p)} \equiv c^p \bmod p$ is an element of $\mathfrak{S}$. Since every element of $\mathcal{Z}^n$ has infinite order, the coefficient of every element in the sum $c^{(p)} = \sum u^p$ is 1. Thus $c^{(p)}$ is equal to $c^{(p)}$ reduced modulo p, so $c^{(p)}$ itself is an element of $\mathfrak{S}$, and the desired result follows.

Let b be an integer. This result implies that $\overline{P_\alpha^{(b)}}$ is an element of $\mathfrak{S}$. Thus it must be a linear combination of principal elements. The monomial $x^{b\alpha}$ has coefficient 1 in $\overline{P_\alpha^{(b)}}$, which implies that the principal element $\overline{P_{b\alpha}}$ containing $x^{b\alpha}$ has coefficient 1 in $\overline{P_\alpha^{(b)}}$. Thus $P_{b\alpha} \subseteq P_\alpha^{(b)}$.

For any integer h, the element $x^{hm\alpha} = (x^{m\alpha})^h$ is an element of the Schur ring because it is a power of a principal element. (This is because $\{x^{m\alpha}\}$ is a principal set by assumption.) Therefore the product $x^{hm\alpha}\overline{P_\alpha}$ is an element of the Schur ring, and furthermore by Lemma 7.1 we have the equality

$$x^{hm\alpha} P_\alpha = P_{(1+hm)\alpha}.$$

Taking $b = 1 + hm$ in the previous paragraph gives us

$$x^{hm\alpha} P_\alpha = P_{(1+hm)\alpha} \subseteq P_\alpha^{(1+hm)}.$$

By counting the number of elements we see that the two sets $x^{hm\alpha}P_\alpha$ and $P_\alpha^{(1+hm)}$ have the same number of elements, which implies the equality $x^{hm\alpha}P_\alpha = P_\alpha^{(1+hm)}$.

If we denote the exponents of the elements of P_α by $\alpha_1 < \alpha_2 < \cdots < \alpha_r$, then for $h > 0$ the exponents of the elements of $x^{hm\alpha}P_\alpha$ are

$$\alpha_1 + hm\alpha < \alpha_2 + hm\alpha < \cdots < \alpha_r + hm\alpha.$$

The exponents of $P_{\alpha_1}^{(1+hm)}$ are

$$(1 + hm)\alpha_1 < (1 + hm)\alpha_2 < \cdots < (1 + hm)\alpha_r,$$

and since these two sets are equal the exponents must be equal in the order given above, giving us $\alpha_i + hm\alpha = (1 + hm)\alpha_i$ for all $1 \leq i \leq r$ and all $h > 0$. This implies that $\alpha_i = \alpha$

for all i since $m > 0$. This shows that the exponent of any element of P_α is equal to α, which implies that $P_\alpha = \{x^\alpha\}$. This proves Lemma 7.2. $\square$

Lemma 7.3. *Let $\alpha \neq (0, 0, ..., 0)$. If p is prime and $r > 0$, then $x^{p^r\alpha} \notin P_\alpha$ and*

$$P_{p^r\alpha} \subseteq P_\alpha^{(p^r)} = \{x^{p^r\beta} \mid x^\beta \in P_\alpha\}.$$

Proof. Let p be prime and let r be an integer greater than 0. Assume by way of contradiction that $x^{p^r\alpha} \in P_\alpha$. Denote $P_\alpha = \{x^{\alpha_1}, ..., x^{\alpha_s}\}$ so that the corresponding principal element of the Schur ring is $\overline{P_\alpha} = x^{\alpha_1} + \cdots + x^{\alpha_s}$. We stipulate that $\alpha_1 < \alpha_2 < \cdots < \alpha_s$.

Using the multinomial theorem, raising $\overline{P_\alpha}$ to the power of p^r can be expressed as

$$\overline{P_\alpha}^{p^r} = \sum_{i=1}^{s} x^{p^r\alpha_i} + \sum_{i_1+\cdots+i_s=p^r} \binom{p^r}{i_1, ..., i_s} x^{i_1\alpha_1+\cdots+i_s\alpha_s}$$

where $\binom{p^r}{i_1,...,i_s} = \frac{p^r!}{i_1!i_2!\cdots i_s!}$ are the multinomial coefficients. Each of these multinomial coefficients in the second sum is a multiple of p because when some i_j is nonzero and $i_j < p^r$ for all $1 \leq j \leq s$ the expression $\frac{p^r!}{i_1!i_2!\cdots i_s!}$ will have at least one factor of p that is not canceled by any $i_j!$. Because $x^\alpha \in P_\alpha$, the group element $x^{p^r\alpha}$ appears in the first sum in the above expression. Furthermore, it appears exactly once because the exponents $\alpha_1, ..., \alpha_s$ are distinct. This implies that the coefficient on $x^{p^r\alpha}$ in the entire expansion of $\overline{P_\alpha}^{p^r}$ is congruent to 1 mod p because if it appears in the second sum then it does so with a coefficient divisible by p. From the definition of a Schur ring, the product $\overline{P_\alpha}^{p^r}$ is a linear combination of principal sets. We are assuming that $x^{p^r\alpha}$ is in P_α, so the fact that $x^{p^r\alpha}$ appears with coefficient 1 mod p implies that the every element of P_α appears in the sum $\overline{P_\alpha}^{p^r}$ with coefficient 1 mod p.

There are s elements $x^{\alpha_1}, ..., x^{\alpha_s}$ of P_α and s group elements $x^{p^r\alpha_1}, ..., x^{p^r\alpha_s}$ that appear with coefficient 1 mod p in $\overline{P_\alpha}^{p^r}$, which means that these two sets of s elements must be equal. This is a contradiction, however, since the exponents $\alpha_1, ..., \alpha_s$ in P_α are not the same as the exponents $p^r\alpha_1, ..., p^r\alpha_s$. In particular, $\alpha_1 < p^r\alpha_1 < \cdots < p^r\alpha_s$, so $\alpha_1 \neq p^r\alpha_i$ for all $1 \leq i \leq s$. We conclude that $x^{p^r\alpha}$ cannot be in P_α.

For the second part of the statement of the lemma, we need to show that $P_{p^r\alpha} \subseteq P_\alpha^{(p^r)}$. This follows from the fact that $x^{p^r\alpha} \in P_{p^r\alpha}$ by definition, which implies that $\overline{P_\alpha}^{p^r}$ contains the sum $\overline{P_{p^r\alpha}}$ because $x^{p^r\alpha}$ appears in $\overline{P_\alpha}^{p^r}$. Furthermore, the coefficient on $\overline{P_{p^r\alpha}}$ must be congruent to 1 mod p. This implies that every group element in $P_{p^r\alpha}$ must appear in the first sum in the expansion of $\overline{P_\alpha}^{p^r}$, so every group element in $P_{p^r\alpha}$ is of the form $x^{p^r\alpha_i}$ for some α_i where $x^{\alpha_i} \in P_\alpha$. This exactly proves $P_{p^r\alpha} \subseteq P_\alpha^{(p^r)}$. □

Corollary 7.4. *If x^α is a primitive element and $x^\beta \in P_\alpha$, then x^β is also a primitive element.*

Proof. Suppose to the contrary that x^β is not primitive. Then the greatest common divisor of the nonzero integers in the n-tuple β can be written as $p^r k$ for some prime p and positive integers r, k. This allows us to write $x^\beta = (x^\gamma)^{p^r}$ for some n-tuple γ.

Then by Lemma 7.3 we can write

$$P_\alpha = P_\beta = P_{p^r\gamma} \subseteq P_\gamma^{(p^r)}.$$

All elements in $P_\gamma^{(p^r)}$ are of the form $x^{p^r\delta}$ for some n-tuple δ and are therefore not primitive. This implies that $x^\alpha \in P_\alpha = P_\gamma^{(p^r)}$ is not primitive, a contradiction. We conclude that all elements of P_α are primitive when x^α is primitive. □

Chapter 8. Schur Rings over the Infinite Cyclic Group

8.1 Schur Rings over the Infinite Cyclic Group

In this section we will completely classify all Schur rings over the free group on one generator (the infinite cyclic group). This will extend the earlier classification theorem of Schur rings over finite cyclic groups. The infinite cyclic group is isomorphic to the integers under addition, and we will denote this group multiplicatively by $\mathcal{Z} = \langle x \rangle$. Our result is the following classification:

Proposition 8.1. *Any Schur ring $\mathfrak{S}$ over $\mathcal{Z}$ is given by one of the following partitions:*

$$\big\{\{x^k\} \mid k \in \mathbb{Z}\big\},$$
$$\big\{\{x^k, x^{-k}\} \mid k \in \mathbb{Z}^+ \cup \{0\}\big\}.$$

The Schur ring generated by the partition of $\mathcal{Z}$ into singleton sets is the discrete Schur ring. This partition always yields a Schur ring, so the interesting part of this proposition is that there is only one other Schur ring over $\mathcal{Z}$, generated from the partition of $\mathcal{Z}$ into sets containing pairs of inverses. We note that this partition is the set of orbits of $\mathcal{Z}$ under the automorphism $i : x \mapsto x^{-1}$. We recall that any finite group of automorphisms of a group determines a Schur ring over that group, and that $\mathrm{Aut}(\mathcal{Z}) = \langle i \rangle$.

For the remainder of this section we will use the following notation. Let $\mathfrak{S}$ be a Schur ring over $\mathcal{Z}$. For each $k \in \mathbb{Z}$, let P_k be the principal set containing the group element x^k. To prove the above proposition, we will use Lemmas 7.2 and 7.3. We restate them here using our notation for Schur rings over $\mathcal{Z}$.

Lemma 8.2. *If $\{x^m\}$ is a principal set for any m, then $\{x\}$ is a principal set.*

Lemma 8.3. *If p is prime and $k > 0$, $r > 0$ then $x^{p^r k} \notin P_k$ and $P_{p^r k} \subseteq P_k^{(p^r)} = \{x^{p^r n} \mid x^n \in P_k\}$.*

With these lemmas, the proof of Proposition 8.1 is straightforward. We will investigate the elements of $\mathcal{Z}$ that are in the principal set P_1 containing x, showing that either $P_1 = \{x\}$ or $P_1 = \{x, x^{-1}\}$. Then we will prove that $P_1 = \{x\}$ implies that $\mathfrak{S}$ is the discrete Schur ring and that $P_1 = \{x, x^{-1}\}$ implies that $\mathfrak{S}$ is the Schur ring given by the partition of $\mathcal{Z}$ into sets of the form $\{x^k, x^{-k}\}$.

Proof of Proposition 8.1. Suppose that $x^k \in P_1$ for some $k > 1$. As a consequence, $P_1 = P_k$. Then we can write $k = pm$ for some prime p. By Lemma 8.3, we have $P_1 = P_k = P_{pm} \subseteq P_m^{(p)}$. Every group element in $P_m^{(p)}$ has an exponent that is a multiple of p. However, $x \in P_1$ implies $x \in P_m^{(p)}$, but x does not have an exponent divisible by p. This yields a contradiction, so it must be that no positive power of x is in P_1.

From the definition of a Schur ring, the set $P_1^{-1} = \{x^{-n} \mid x^n \in P_1\}$ is also a principal set. It follows similarly that if $x^k \in P_1$ for some $k < 0$ then we can apply the argument in the previous paragraph to P_1^{-1} to conclude that $k = -1$.

This gives us two possibilities. Either $P_1 = \{x\}$ or $P_1 = \{x, x^{-1}\}$. In the first case, $\mathfrak{S}$ is the discrete Schur ring because any single group element is a power of P_1 in the group algebra. Given x^k with $k > 0$ we can write $x^k = \overline{P_1}^k$, so x^k is a linear combination of principal elements and therefore must be a principal element. This in turn implies x^{-k} is a principal element for every $k > 0$. Thus $\{x^k\}$ is a principal set for every $k \in \mathbb{Z}$, so $\mathfrak{S}$ is the discrete Schur ring.

For the second case, assume $P_1 = \{x, x^{-1}\}$. Then using the binomial theorem for some integer $m > 0$ we have

$$(x + x^{-1})^m = x^m + x^{-m} + \sum_{i=1}^{m-1} \binom{m}{i} x^{m-2i}.$$

This is a power of a principal element and therefore is a linear combination of principal elements. The binomial coefficients $\binom{m}{i}$ in the sum are all greater than 1. Thus the principal set containing x^m appears with coefficient 1 and therefore can only contain x^m alone or x^m and x^{-m}. If $P_m = \{x^m\}$ then by Lemma 8.2 we have $P_1 = \{x\}$, which contradicts our assumption about P_1. We are therefore left with $P_m = \{x^m, x^{-m}\}$ for all $m > 0$, which means that $\mathfrak{S}$ is indeed the Schur ring produced by the partition of $\mathcal{Z}$ into sets of inverse pairs. □

Bibliography

[1] Ka Hin Leung and Siu Lun Ma. The structure of schur rings over cyclic groups. *Journal of Pure and Applied Algebra*, 1990.

[2] W.R. Scott. *Group Theory.* Prentice-Hall, Inc., 1964.

[3] John D. Dixon and Brian Mortimer. *Permutation Groups.* Springer-Verlag New York Inc., 1996.

[4] Ka Hin Leung and Shin Hing Man. On schur rings over cyclic groups ii. *Journal of Algebra*, 1996.

[5] Ka Hin Leung and Shin Hing Man. On schur rings over cyclic groups. *Israel Journal of Mathematics*, 1998.

[6] Mikhail E. Muzychuk. On the structure of basic sets of schur rings over cyclic groups. *Journal of Algebra*, 1994.

[7] Helmut Wielandt. *Finite Permutation Groups.* Academic Press, 1964.

[8] Nicholas Bastian, Jaden Brewer, Stephen Humphries, Andrew Misseldine, and Cache Thompson. On schur rings over infinite groups. *Algebras and Representation Theory*, 2019.