On Schur Rings over Cyclic Groups, II

Ka Hin Leung and Shing Hing Man

Department of Mathematics, National University of Singapore,
Singapore 0511, Singapore

Communicated by Alexander Lubotzky

Received November 20, 1994

In this paper, we show that for any Schur ring $S$ over a cyclic group $G$, if every subgroup is an $S$-subgroup, then $S$ is either a wedge product of Schur rings over smaller cyclic groups, or every $S$-principal subset is an orbit of an element under a fixed subgroup of $\text{Aut} G$. With an earlier result proved by us on Schur rings over cyclic groups, preprint, we are able to determine all possible structures of Schur rings over a cyclic group.

1. INTRODUCTION

This paper is a continuation of [LM]. In [LMa], we introduced a method for constructing all Schur rings over a cyclic group of prime power. The idea involved is extending a Schur ring of smaller order to one with larger order. In [LM], we used the notion of dot product and wedge product to formulate this concept of extension. (As we mentioned in [LM], the dot product of Schur rings is not a new notion. However, the wedge product of Schur rings is new and for the convenience of readers, it will be defined later.) It was also shown there that, for any Schur ring $S$ over a cyclic group $G$, if there exists a subgroup $H$ such that $\sum_{g \in H} g \notin S$, then the structure of $S$ can be described by Schur rings over cyclic groups of smaller order. In this paper, we shall look at the remaining case, that is, when $\sum_{g \in H} g \in S$ for all subgroups $H$ of $G$. In this case, we show in Theorems 3.4 and 3.6 that either $S$ can be constructed by Schur rings over smaller cyclic groups, or every $S$-principal subset is an orbit under a fixed subgroup of $\text{Aut} G$. Together with the results in [LM], it is now possible to list all Schur rings over a cyclic group inductively; see Theorem 3.7.

Let $G$ be a finite group. For any subset $A$ of $G$, we denote $\sum_{g \in A} g$ in the group algebra $\mathbb{Z}[G]$ by $\overline{A}$. If $t$ is an integer, we also write $A^{(t)}$ for the set $(g^t : g \in A)$.
Definition 1.1. Let $S$ be a subring of $\mathbb{Z}[G]$. We say $S$ is a Schur ring over $G$ if there exist disjoint subsets $D_1, \ldots, D_t$ in $G$ such that

(i) $G = \bigcup_{i=1}^t D_i$,
(ii) $S = \{\sum a_i D_i : a_i \in \mathbb{Z}\}$,
(iii) for any $i = 1, \ldots, t, D_i^{-1} = D_j$ for some $j$.

We call each $D_i$ an $S$-principal subset of $G$ and define the dimension of $S$ to be $t$. The set of all the $S$-principal subsets is denoted by $\mathcal{D}(S)$. Finally, a subgroup $H$ of $G$ is an $S$-subgroup if $H \in S$.

We first recall some results proved in LM.

Proposition 1.2. Let $G$ be a group, $H$ a normal subgroup of $G$, and $K$ a subgroup containing $H$. Furthermore, let $\rho: G \to G/H$ be the natural surjection. For any Schur ring $S_K$ over $K$, we define $\rho^*(S_K) = \bigoplus_{D \in \mathcal{D}(S_K)} \mathbb{Z}[\rho(D)]$. If $S_{G/H}$ is a Schur ring over $G/H$ with $H \in S_K$ and $\rho^*(S_K) = (\mathbb{Z}[K/H]) \cap S_{G/H}$, then there exists a Schur ring $S$ over $G$ with

$$\mathcal{D}(S) = \mathcal{D}(S_K) \cup \{\rho^{-1}(E) : E \in \mathcal{D}(S_{G/H}) \text{ with } E \nsubseteq K/H\}.$$ 

We denote the Schur ring $S$ over $G$ constructed in Proposition 1.2 by $S_K \wedge S_{G/H}$. We say $S$ is a wedge product of $S_K$ and $S_{G/H}$. Note that the wedge product is defined only when $H \in S_K$ and $\rho^*(S_K) = \mathbb{Z}[K/H] \cap S_{G/H}$. The following result is an easy consequence of Proposition 1.2 and [LMa, Lemma 1.2]. We skip its proof.

Proposition 1.3. Let $S$ be a Schur ring over a group $G$ and $H$ a normal $S$-subgroup of $G$. Suppose there exists an $S$-subgroup $K \supset H$ such that for any $S$-principal subset $D \in K$, $D$ is a union of $H$-cosets. Then $S$ is a wedge product of $S_K$ and $S_{G/H}$, where $S_K$ and $S_{G/H}$ are Schur rings over $K$ and $G/H$, respectively.

Parts (i) and (ii) of the following proposition are special cases of [LM, Lemmas 2.2, 2.6], respectively.

Proposition 1.4. Suppose $S$ is a Schur ring over a cyclic group $G$ and $p$ is a prime divisor of $|G|$ such that the unique subgroup of $G$ of order $p$, denoted by $G(p)$, is an $S$-subgroup. Let $D$ be an $S$-principal subset which is not a union of $G(p)$-cosets. Then

(i) $D^{(p)} = \{dp : d \in D\}$ is a union of $S$-principal subsets,
(ii) $D^{(p)}$ is not a union of $G(p)$-cosets if there exists $d \in D$ with $p^2 \mid \circ(d)$, except for the case when $p = 2$ and $\circ(d) = 2^3k'$, where $k'$ is odd.
2. ORBITS OF AN AUTOMORPHISM SUBGROUP

From now on, we shall assume \( G \) is a cyclic group. Let \( S \) be a Schur ring over \( G \). Our main concern is to study \( S \) when every subgroup of \( G \) is an \( S \)-subgroup. Our first goal is to show that for any \( S \)-principal subset \( D \), there exists a subgroup \( \Omega_D \) in \( \text{Aut} \ G \) such that \( \Omega_D(h) = D \) for all \( h \in D \).

**Definition 2.1.** Let \( D \) be an \( S \)-principal subset. Define \( V_s = \{ \sigma \in \text{Aut} \ G : \sigma(D) = D \} \).

Clearly, \( V_s \) is a subgroup of \( G \) and \( \{ \sigma(h) : \sigma \in \Omega_D \} \subset D \). To simplify notation, we shall denote the set \( \{ \sigma(h) : \sigma \in \Omega \} \) by \( \Omega(h) \). So, we have \( \Omega_D(h) \subset D \) for all \( h \in D \).

**Proposition 2.2.** Let \( S \) be a Schur ring on \( G \). Suppose every subgroup of \( G \) is an \( S \)-subgroup. Then for any \( S \)-principal subset \( D \), \( V_s \) for any element \( h \in D \).

**Proof.** Let \( D \) be an \( S \)-principal subset and \( H = \langle D \rangle \). We claim that every element in \( D \) generates \( H \). Otherwise, there exists \( d \in D \) with \( \langle d \rangle \not\subset H \). By assumption, \( \langle d \rangle \) is also an \( S \)-subgroup. Therefore, \( \langle d \rangle \) is a union of \( S \)-principal subsets. As \( D \cap \langle d \rangle \neq \emptyset \), \( D \subset \langle d \rangle \). This implies \( H = \langle D \rangle \subset \langle d \rangle \), which is impossible. We have thus proved that every element in \( D \) is a generator of \( \langle D \rangle \). In particular, all elements in \( D \) are of the same order.

To show \( \Omega_D(h) = D \), we only need to show \( D \subset \Omega_D(h) \) for any element \( h \in D \). Suppose \( h, h' \in D \). As \( \sigma(h) = \sigma(h') \), there exists \( \sigma \in \text{Aut} \ G \) such that \( h' = \sigma(h) \). However, \( \sigma(D) \) is also an \( S \)-principal subset containing \( \sigma(h) \). Therefore, \( \sigma(D) = D \). Thus \( \sigma \in \Omega_D \) and \( h' \in \Omega_D(h) \).

The above result leads us to study sets of the form \( \Omega(g) \), where \( \Omega \) is a subgroup in \( \text{Aut} \ G \) and \( g \in G \). Throughout this section, we assume \( \Omega \) is a subgroup of \( \text{Aut} \ G \).

We shall use \( G(k) \) to denote the unique subgroup of \( G \) of order \( k \). It is implicit that \( k \) is a divisor of \( |G| \). First, we want to determine when \( \Omega(g) \) is a union of \( G(p) \)-cosets, where \( p \) is a prime divisor of \( e(g) \).

**Lemma 2.3.** Let \( g \in G \). Suppose \( p^2 \mid e(g) \) for some prime \( p \). Then \( \Omega(g) \) is a union of \( G(p) \)-cosets iff there exists \( \sigma \in \Omega \) such that \( \sigma(g) = gy \) for some \( y \in G(p) \setminus \{ e \} \).

**Proof.** Obviously, we only need to prove the sufficiency. Note that \( \Omega(g) \) is a union of \( G(p) \)-cosets iff \( gG(p) \subset \Omega(g) \). In the following, we show that \( gG(p) \subset \Omega(g) \).

Let \( \sigma \) and \( y \) be as assumed above. Obviously, \( \{ \sigma^i(g) : i \in \mathbb{Z} \} \subset gG(p) \). On the other hand, it is easy to see that \( \sigma \mid \langle g \rangle \) is of order \( p \). Therefore, \( |\{ \sigma^i(g) : i \in \mathbb{Z} \}| = p \) and hence \( \{ \sigma^i(g) : i \in \mathbb{Z} \} = gG(p) \).
Lemma 2.4. Let \( a, b \in G \) with \( \circ(a), \circ(b) \) relatively prime. Suppose \( p^2 \mid \circ(a) \) for some prime \( p \) and \( \Omega(ab) \) is a union of \( G(p) \)-cosets. Then \( \Omega(a) \) is also a union of \( G(p) \)-cosets. Moreover, the converse holds when \( p \nmid \phi(\circ(b)) \). Here \( \phi \) is the Euler function.

Proof. By Lemma 2.3, there exists \( \sigma \in \Omega \) such that \( \sigma(ab) = aby \), where \( y \in G(p) \setminus \{e\} \). As \( \circ(ay) = \circ(a) \) and \( \langle \circ(a), \circ(b) \rangle = 1 \), we have \( \sigma(a) = ay \). With Lemma 2.3 applied again, the first assertion follows.

Let \( l = \phi(\circ(b)) \). We now prove the converse when \( p \nmid l \). Suppose \( \Omega(a) \) is a union of \( G(p) \)-cosets. Then there exists \( \sigma \in \Omega \) such that \( \sigma(a) = ay \), where \( y \in G(p) \setminus \{e\} \). As argued in the proof of Lemma 2.3, \( \sigma^p(a) = a \).

Since \( p \nmid l \), \( \sigma^l(a) = ay^i \), where \( 1 \leq i \leq p - 1 \). On the other hand, \( \sigma^l(b) = b \). Therefore, \( \sigma^l(ab) = \sigma^l(a)b = aby^i \). Our assertion now follows from Lemma 2.3.

Remark. Note that in Lemma 2.4, the condition \( p \nmid \phi(\circ(b)) \) is automatically satisfied if \( p \) is larger than any prime divisor of \( \circ(b) \).

Proposition 2.5. Let \( p \) and \( q \) be distinct prime divisors of \( \circ(g) \). Suppose \( p^2 \mid \circ(g) \). Then \( \Omega(g^p) \) is a union of \( G(q) \)-cosets iff \( \Omega(g) \) is a union of \( G(q) \)-cosets.

Proof. Sufficiency follows easily from Lemma 2.3. To prove necessity, we assume \( \Omega(g^p) \) is a union of \( G(q) \)-cosets. As before, we choose \( \sigma \in \Omega \) such that \( \sigma(g^p) = g^px \), where \( x \in G(q) \setminus \{e\} \). Write \( g = abc \), where \( \circ(a) \) is a \( p \)-power, \( \circ(b) \) is a \( q \)-power, and \( pq \), \( \circ(c) \) are relatively prime. Note that the assumption \( \Omega(g^p) \) is a union of \( G(q) \)-cosets implies \( q^2 \mid \circ(b) \).

As \( \sigma(g^p) = g^px \), we have \( \sigma(a^p) = a^p \), \( \sigma(b^p) = b^px \), and \( \sigma(c) = c \). Consequently, \( \sigma(a) = ay \) for some \( y \in G(p) \). Since \( p, q \) are distinct, \( \sigma(b) = bx^i \) for some \( 1 \leq i \leq q - 1 \). As argued before, \( \sigma^p(a) = a \) and \( \sigma^p(b) = b \). Therefore, \( \sigma^p(abc) = abx^jcx^j = gx^j \) for some \( 1 \leq j \leq q - 1 \). Since \( \sigma^p \in \Omega \), it follows from Lemma 2.3 that \( \Omega(g) \) is a union of \( G(q) \)-cosets.

In the above discussion, we deal with the case when \( \Omega(g) \) is a union of \( G(p) \)-cosets for some prime \( p \). Next, we want to study the case when it is not a union of any \( G(p) \)-cosets.

Definition 2.6. Suppose \( h \in G \). \( \Omega(h) \) is said to be free if it is not a union of \( G(q) \)-cosets for all prime divisors \( q \) of \( \circ(h) \).

To study the case when \( \Omega(g) \) is free, we need some results in number theory.

Proposition 2.7. Let \( G \) be a cyclic group generated by an element \( g \). Suppose \( |G| = p^r \), where \( p \) is a prime and \( r \) a positive integer. Let \( \omega_{p^r} \) be a primitive \( p^r \)th root of unity and \( K \) a field linear disjoint with \( \mathbb{Q}[\omega_{p^r}] \) over \( \mathbb{Q} \).
Define a homomorphism \( \theta : K[G] \rightarrow K[\omega_p] \) such that \( \theta(g) = \omega_p^r \). Then \( \text{Ker } \theta = (G(p)) \).

Proof. Obviously, \( \theta \) is surjective and \( G(p) = \sum_{h \in G(p)} h \in \text{Ker } \theta \). Moreover, as a \( K \)-vector space, the dimension of \( G(p) \) is \( p^{r-1} \). In fact, \( \{gG(p) : 0 \leq i \leq p^{r-1} - 1\} \) is a basis of \( G(p) \) over \( K \). To prove \( \text{Ker } \theta = (G(p)) \), it suffices to show the dimension of \( \text{Ker } \theta \) over \( K \) is also \( p^{r-1} \). Observe that as \( K \) and \( Q[\omega_p] \) are linear disjoint over \( Q \), \( \text{Ker } \theta \) is disjoint in \( Q \), \( \text{Ker } \theta = (G(p)) \) is also \( p^{r-1} \). It follows that the dimension of \( \text{Ker } \theta \) over \( K \) is \( p^{r-1} \). \( \square \)

**Corollary 2.8.** Let \( p, r, m \) be positive integers with \( p \) prime and \( p \neq m \). Let \( \omega_m \) and \( \omega_p \) be primitive \( m \)th root and \( p \)th root of unity. Suppose \( \alpha_1, \ldots, \alpha_l \) are nonzero elements in \( Q[\omega_m] \), \( j_i, s_i \) are integers with \( 0 \leq j_1 < \cdots < j_l \leq p - 1 \), and \( \sum_{i=1}^{l} \alpha_i \omega_p^{j_i} = 0 \). Then \( p \mid l \).

Proof. Let \( K = Q[\omega_m] \) and \( G \) be a cyclic group of order \( p^r \). We define \( \theta \) as in Proposition 2.7. By assumption, we have \( \theta(\sum_{i=1}^{l} \alpha_i \omega_p^{j_i}) = 0 \). It is well known that \( K \) and \( Q[\omega_p] \) are linearly disjoint. Thus, \( \sum_{i=1}^{l} \alpha_i \omega_p^{j_i} \in G(p) \). As all \( \alpha_i \)'s are nonzero, \( p \mid l \). \( \square \)

Let \( g \) be an element in \( G \) and \( p \) the largest prime divisor of \( \phi(g) \). We write \( g = ab \), where \( \phi(a) = p^r \) and \( p \neq \phi(b) \). Set \( \Omega = \{ \sigma \in \Omega : \sigma(a) = a \} \). Write \( \Omega \) as \( \bigcup_{i=1}^{l} \sigma_i \Omega \), where \( \sigma_i \Omega \)'s are disjoint \( \Omega \)'-cosets in \( \Omega \). Clearly,

\[
\Omega(g) = \sigma_1(a)\Omega' = \sigma_2(a)\Omega' \cup \cdots \cup \sigma_l(a)\Omega'
\]

is a disjoint union and \( \Omega(a) = \{ \sigma_1(a), \ldots, \sigma_l(a) \} \). In particular, \( |\Omega(a)| = l \).

**Lemma 2.9.** Keep the notation as defined above. If \( b \neq e \) and \( \Omega(g) \) is free, then \( l \leq p - 1 \) and \( \Omega'(\sigma_i(b)) \) is free for all \( i \).

Proof. Since \( p \) is the largest prime divisor of \( \phi(g) \), \( p \neq \phi(b) \), it follows from Lemma 2.3 that \( \Omega(a) \) is not a union of \( G(p) \)-cosets.

Let \( \Omega^* = \{ \sigma \in \Omega : \sigma \in \Omega \}. As \ b \neq e, \ p \geq 3 \). It is well known that \( \text{Aut}(a) \) is a cyclic group of order \( (p - 1)p^{r-1} \). Moreover, if \( \tau \) is an element of order \( p \) in \( \text{Aut}(a) \), then \( \tau(a) = ay \) for some \( y \in G(p) \setminus \{e\} \).

Since \( \Omega(a) \) is free, we conclude from Lemma 2.3 that \( \Omega^* \) does not contain an element of order \( p \). Hence \( |\Omega^*| \leq p - 1 \). Since \( \Omega(a) = \Omega^* \), we have \( l \leq p - 1 \).

Suppose \( \Omega'(\sigma_i(b)) \) is a union of \( G(q) \)-cosets for some prime divisor \( q \) of \( \phi(b) \). As \( \text{Aut } G \) is abelian, \( \Omega'(\sigma_i(b)) = \sigma_i \sigma_i^{-1} \Omega'(\sigma_i(b)) \) must then be a union of \( G(q) \)-cosets for all \( 1 \leq j \leq l \). Therefore \( \Omega(g) \) is a union of \( G(q) \)-cosets. This is impossible. \( \square \)
PROPOSITION 2.10. Suppose g is a generator of G and |G| = n. Let \( \omega_n \) be a primitive nth root of unity and \( \chi: \mathbb{Q}[G] \to \mathbb{Q}[\omega_n] \) the homomorphism that maps g to \( \omega_n \). Let \( h \in G \).

(i) \( \Omega(h) \) is free iff \( \chi(\Omega(h)) \neq 0 \).

(ii) If \( \Omega(h) \) is free, then for any \( \tau \in \text{Aut} G \), \( \chi(\Omega(h)) = \chi(\Omega(\tau(h))) \) iff \( \Omega(h) = \Omega(\tau(h)) \).

Proof. By considering the restriction of \( \chi \) on \( \mathbb{Q}[\langle h \rangle] \), we may assume \( h = g \). Let \( t \) be the number of prime divisors of \( n \).

(i) Note that \( \chi(H) = 0 \) for any subgroup \( H \) of \( G \). Therefore, if \( \Omega(g) \) is not free, \( \Omega(g) \) is a union of \( G_q \)-cosets for some prime divisor \( q \) of \( n \). Hence \( \chi(\Omega(g)) = 0 \).

Now suppose \( \Omega(g) \) is free. We shall proceed by induction. Suppose \( t = 1 \). Then \( n \) is a \( p \)-power for some prime \( p \). As \( \Omega(g) \) is not a union of \( G(p) \)-cosets, \( \chi(\Omega(g)) \neq 0 \) follows from Proposition 2.7.

Next, we assume \( t > 1 \). Let \( p \) be the largest prime divisor of \( \sigma(g) \). We now follow the notation used in Lemma 2.9. As before, we have \( \Omega(g) = \bigcup_{i=1}^l \sigma_i(a)\Omega(\sigma_i(b)) \). Clearly,

\[
\chi(\Omega(g)) = \sum_{i=1}^l \chi(\sigma_i(a))\chi(\Omega(\sigma_i(b))).
\]

Note that \( \chi(\sigma_i(a)) \)'s are distinct primitive \( p \)-th roots of unity. By Lemma 2.9, \( l \leq p - 1 \). So by Corollary 2.8, \( \chi(\Omega(g)) = 0 \) iff \( \chi(\Omega(\sigma_i(b))) = 0 \) for each \( i \). Since the number of prime factors in \( \sigma(b) \) is \( t - 1 \) and \( \Omega(\sigma_i(b)) \) is free by Lemma 2.9, we conclude by induction that \( \chi(\Omega(\sigma_i(b))) \neq 0 \). Therefore, \( \chi(\Omega(g)) \neq 0 \).

For (ii), we also proceed by induction on \( t \). Suppose \( \sigma(g) = p^r \), where \( p \) is prime and \( r \geq 1 \). By assumption, \( \Omega(g) = \Omega(\tau(g)) \in \text{Ker} \chi \). It follows from Proposition 2.7 that

\[
\Omega(g) = \Omega(\tau(g)) = \sum_{i=0}^{p^r-1} \alpha_i g^i G(p)
\]

for some integers \( \alpha_i \)'s. If \( \Omega(g) \neq \Omega(\tau(g)) \), then \( \Omega(g) \cap \Omega(\tau(g)) = \emptyset \).

Note that \( g^i G(p) \) and \( g^j G(p) \) are disjoint whenever \( 0 \leq i \neq j \leq p^r-1 - 1 \). By comparing the coefficients of elements in \( \Omega(g) \), we see that \( \Omega(g) \) is the union of the \( g^i G(p) \)'s with \( \alpha_i = 1 \). This contradicts the assumption that \( \Omega(g) \) is free.
Next, we assume \( t > 1 \) and \( \Omega(g) \neq \Omega(\tau(g)) \). We keep the notation used in the proof of (i). Clearly, \( \Omega(\tau(g)) = \tau(\sigma_1(a))\Omega'(\tau(\sigma_1(b))) \cup \cdots \cup \tau(\sigma_l(a))\Omega'(\tau(\sigma_1(b))) \) and
\[
\chi\left(\Omega(g) - \Omega(\tau(g))\right) = \sum_{i=1}^l \chi\left(\Omega'(\sigma_i(b))\right) \cdot \chi(\sigma_i(a)) \\
- \chi\left(\Omega'(\tau(\sigma_i(b)))\right) \cdot \chi(\sigma_i(a)) = 0.
\]
If \( \Omega(a) \neq \Omega(\tau(a)) \), then they are disjoint. Therefore,
\[
\chi(\sigma_1(a)), \ldots, \chi(\sigma_l(a)), \chi(\tau(\sigma_1(a))), \ldots, \chi(\tau(\sigma_l(a)))
\]
are all distinct primitive \( p' \)th roots of unity. But as \( \Omega(g) \) is free, \( \Omega'(\sigma_i(b)) \) and \( \Omega'(\tau(\sigma_i(b))) \) are all free. Let \( m = \varphi(\sigma_i(b)) \). By (i), \( \chi(\Omega'(\sigma_i(b))) \) and \( \chi(\Omega'(\tau(\sigma_i(b))) \) are nonzero elements in \( \mathbb{Q}[\omega_m] \) for all \( i \). As \( p \) is odd and \( p \nmid l \), By Corollary 2.8,
\[
\sum_{i=1}^l \chi\left(\Omega'(\sigma_i(b))\right) \cdot \chi(\sigma_i(a)) - \chi\left(\Omega'(\tau(\sigma_i(b)))\right) \cdot \chi(\tau(\sigma_i(a))) \neq 0.
\]
Next, we assume \( \Omega(a) = \Omega(\tau(a)) \). Since \( \Omega(a) = \Omega(\tau(a)) \), we can think of \( \tau \) as a permutation of \( \{1, 2, \ldots, l\} \). For \( 1 \leq i \leq l \), put \( \tau(\sigma_i(a)) = \sigma_i(a) \).

Then
\[
\chi(\Omega(g) - \Omega(\tau(g))) \\
= \sum_{i=1}^l \left[ \chi(\Omega'(\sigma_i(b))) - \chi(\Omega'(\tau(\sigma_i(b)))) \right] \chi(\sigma_i(a)).
\]
As \( \Omega(g) \neq \Omega(\tau(g)) \), \( \Omega'(\sigma_i(b)) \neq \Omega'(\tau(\sigma_i(b))) \) for some \( j \). Note that \( \Omega'(\sigma_i(b)) \) is free as \( \Omega'(\sigma_i(b)) \) is. By induction hypothesis, \( \chi(\Omega'(\tau(\sigma_i(b)))) \neq \chi(\Omega'(\sigma_i(b))) \). As \( p \nmid l \), we can now conclude from Corollary 2.8 that
\[
\chi(\Omega(g) - \Omega(\tau(g))) \neq 0.
\]

3. MAIN RESULTS

Throughout this section, we assume that \( S \) is a Schur ring of \( G \), with the property that every subgroup of \( G \) is an \( S \)-subgroup. The main results are as follows. Suppose \( D \) is an \( S \)-principal subset which contains a generator of \( G \). If \( D \) is a union of \( G(p) \)-cosets for some prime divisor \( p \) of \( |G| \), then \( S \) is a wedge product of Schur rings of smaller cyclic groups. On the other
hand, if $D$ is free, i.e., $D$ is not a union of $G(p)$-cosets for all prime divisors $p$ of $|G|$, then there exists a subgroup $\Omega$ of $\text{Aut} \ G$, such that every $S$-principal subset is of the form $\Omega(h)$ for some $h \in G$.

Recall that we have proved in Proposition 2.2 that every $S$-principal subset $D$ is of the form $\Omega_p(h)$ for any $h \in D$. In particular, there is an $S$-principal subset which contains only elements of order $k$ for each divisor $k$ of $|G|$. For each divisor $k$ of $|G|$, we fix one such $S$-principal subset $D(k)$. Let $D$ be an $S$-principal subset and $d \in D$. If $\sigma(d) = r$, then there exist $h \in D(r)$ and $\sigma \in \text{Aut} \ G$ such that $\sigma(h) = d$. As $D \cap \sigma(D(r)) \neq \emptyset$, $D = \sigma(D(r))$. This shows that every $S$-principal subset is of the form $\sigma(D(k))$, where $\sigma \in \text{Aut} \ G$ and $k$ is a divisor of $|G|$. Clearly, $D(k)$ and $\sigma(D(k))$ share many similar algebraic structures. For example, $\Omega_{D(k)} = \Omega_{\sigma(D(k))}$ and $D(k)$ is a union of $G(p)$-cosets iff $\sigma(D(k))$ is a union of $G(p)$-cosets. Therefore, $S$ is determined once we know all $D(k)$'s. However, $D(k)$'s are not independent of each other. Our task is to determine how $D(k)$'s are related.

For convenience, we introduce the following notation. Recall that $D(k)$ is a fixed $S$-principal subset which contains elements of order $k$. We set $\Omega_k = \{ \sigma \in \text{Aut} \ G : \sigma(D(k)) = D(k) \}$. As we have discussed before, $\Omega_k$ does not depend on the choice of $D(k)$.

**Proposition 3.1.** Suppose $m = kl$, where $k$, $l$ are relatively prime. Let $a \in D(k)$ and $b \in D(l)$.

(i) $D(k) = \Omega_m(a)$ and $D(l) = \Omega_m(b)$. In particular, $\Omega_m \subset \Omega_k$ and $\Omega_m \subset \Omega_l$.

(ii) If $p$ is a prime with $p \mid k$ and $D(m)$ is a union of $G(p)$-cosets, then so is $D(k)$. Furthermore, the converse holds if $p \nmid \phi(l)$.

**Proof.** (i) By the definition of a Schur ring, we have $D(k) \cdot D(l) = \sum \alpha E_j$, where each $E_j$ is an $S$-principal subset. Note that in every $E_j$, any element is of order $m$. Therefore $E_j = \sigma_j D(m)$ for some $\sigma_j \in \text{Aut} \ G$. As $ab \in D(k) \cdot D(l)$, we can assume $ab \in \sigma_j D(m)$. For convenience, we put $D = \sigma_j D(m)$. Clearly, $D = \Omega_m(ab)$.

Let $\rho: G \to G/\langle b \rangle$ be the natural surjection. As $a \in D(k) \cap \Omega_m(a)$, $\rho(a) \in \rho(D(k)) \cap \rho(D)$. By [LMa, Lemma 1.2 (ii)], $\rho(D(k)) = \rho(D)$. On the other hand, it is easy to see that $\rho(D) = \rho(\Omega_m(a))$. Hence we have $\rho(D(k)) = \rho(\Omega_m(a))$. Observe that the restriction of $\rho$ on $\langle a \rangle$ is injective as $\sigma(a) \in \langle b \rangle$ are relatively prime. Since $\rho(D(k)) = \rho(\Omega_m(a))$, we have $D(k) = \Omega_m(a)$. The corresponding result for $D(l)$ follows by a similar argument. The last assertion is obvious.

(ii) Let $h \in D(m)$. As $\sigma(ab) = m$, $ab = \sigma(h)$ for some $\sigma \in \text{Aut} \ G$. Note that $\Omega_m(h) = D(m)$ is a union of $G(p)$-cosets. Therefore $\Omega_m(\sigma(h))$
is also a union of \( G(p) \)-cosets. By Lemma 2.4 and (i), \( D(k) = \Omega_m(a) \) is also a union of \( G(p) \)-cosets. The converse is also an easy consequence of Lemma 2.4.

Recall that in Definition 2.6, we define the notion of free orbit. As every \( S \)-principal subset is an orbit, this notion also applies to \( S \)-principal subsets.

**Lemma 3.2.** Suppose \( D(k) \) is free and \( p^2 \mid k \), where \( p \) is prime. Then \( D(k/p) \) is also free unless \( p = 2 \) and \( k = 2^2k' \), where \( k' \) is odd.

**Proof.** By Proposition 1.4(i), \( D(k)^{(p)} = \bigcup E_i \) for some \( S \)-principal subsets \( E_i 's \). Note that each element in \( D(k)^{(p)} \) is of order \( k/p \). Therefore, each \( E_i \) is of the form \( \sigma_i(D(k/p)) \), where \( \sigma_i \in Aut \, G \). If \( D(k/p) \) is a union of \( G(p) \)-cosets, so is \( \sigma_i(D(k/p)) \). Therefore, \( D(k)^{(p)} \) is also a union of \( G(p) \)-cosets. This contradicts Proposition 1.4(ii). It follows that \( D(k/p) \) is not a union of \( G(p) \)-cosets.

Let \( g \in D(k) \). As \( D(k) = \Omega_k(g) \) and \( D(k)^{(p)} = \Omega_k(g^p) \). Let \( q \neq p \) be another prime. As \( D(k) = \Omega_k(g) \) is free, it follows from Proposition 2.5 that \( \Omega_k(g^p) \) is not a union of \( G(q) \)-cosets. By an argument similar to that in the previous case, we see that \( D(k/p) \) is not a union of \( G(q) \)-cosets also. This proves \( D(k/p) \) is free.

**Lemma 3.3.** Let \( r, m \) be natural numbers and \( p \) a prime with \( p \nmid m \). Suppose

(i) \( D(mp^t) \) is a union of \( G(p) \)-cosets,

(ii) \( D(m) \) is free,

(iii) every prime divisor of \( m \) is greater than \( p \).

Then, for any \( k \mid m \), \( D(kp^t) \) is a union of \( G(p) \)-cosets.

**Proof.** Let \( k \mid m \) be given. Let \( m = q_1^{s_1}q_2^{s_2} \cdots q_t^{s_t} \) be the prime factorization of \( m \). Write \( k = q_1^{r_1}q_2^{r_2} \cdots q_t^{r_t} \), where \( 0 \leq s_i \leq r_i \) for \( i = 1, 2, \ldots, t \). We first assume all \( s_i \geq 1 \). For \( i = 1, 2, \ldots, t \), let

\[
v_i = \begin{cases} 
1 & \text{if } s_i = r_i = 1 \\
r_i - 1 & \text{if } s_i = r_i \geq 2 \\
r_i & \text{if } s_i < r_i.
\end{cases}
\]

Put \( k' = q_1^{r_1}q_2^{r_2} \cdots q_t^{r_t} \). As each \( q_i > p \geq 2 \), we can apply Lemma 3.2 repeatedly to conclude that \( D(k), D(k') \) are free. By definition of a Schur ring, \( D(k') \cdot D(kp^t) = \sum \alpha_i \sigma_i(D(t_i)) \), where \( \alpha_i \)'s are integers, \( \sigma_i \)'s are in \( Aut \, G \), and \( t_i \)'s are divisors of \( mp^t \). Observe that \( q_i^{t_i} \mid t_i \), for any \( i \) if \( r_i \geq 2 \).

It follows that \( (mp^t/t_i,t_i) = 1 \) for every \( i \). By Proposition 3.1, each \( D(t_i) \) is
a union of $G(p)$-cosets and hence each $\sigma_i(D(t))$ is also a union of $G(p)$-cosets. Let $\chi$ be as defined in Proposition 2.10. Clearly, $\chi(\sigma_i(D(t))) = 0$. Therefore, $\chi(D(k')) \cdot \chi(D(kp')) = 0$. Since $D(k')$ is free, $\chi(D(k')) \neq 0$ by Proposition 2.10. Hence $\chi(D(kp')) = 0$. By the same proposition, $D(kp')$ is then a union of $G(q)$-cosets for some prime divisor $q$ of $kp'$. We claim that $q = p$. Otherwise, we will then conclude that $D(k)$ is a union of $G(q)$-cosets from Proposition 3.1. This contradicts the fact that $D(k)$ is free.

We now go back to the case when some $s_i = 0$. Define $k' = k \cdot \prod_{i=0}^{r} q_i$. As shown above $D(kp')$ is a union of $G(p)$-cosets. Our desired conclusion now follows from Proposition 3.1.

Remark. Let $\rho: G \to G/G(p)$ be the natural surjection. By working with the Schur ring $\rho^*(S)$ of $G/G(p)$, it can be shown by induction that Lemma 3.3 remains valid when “$G(p)$-cosets” is replaced by “$G(p')$-cosets.”

Now, we come back to the study of $S$. As we have seen from the results proved so far, $D(r)$'s are related. As it turns out, the set $D([G])$ determines $S$ when it is free. When it is not, we have the following result.

**Theorem 3.4.** Suppose $|G| = n$ and $D(n)$ is not free. Among all the prime numbers $q$ where $D(q)$ is a union of $G(q)$-cosets, let $p$ be the largest. Then $S$ is a wedge product of $S'$ and $S''$, where $S'$ and $S''$ are Schur rings on $G(n/p)$ and $G/G(p)$, respectively.

**Proof.** By Proposition 1.3, it suffices to show that for any $S$-principal subset $D$, $D$ is a union of $G(p)$-cosets if $D \subseteq G(n/p)$. Write $n = mp'l$, where

(a) $m$, $p$, and $l$ are pairwise relatively prime,
(b) every prime divisor of $mp$ is greater than or equal to $p$,
(c) every prime divisor of $pl$ is smaller than or equal to $p$.

It is enough to show that if $s$ is a divisor of $n$ and $p' \mid s$, then $D(s)$ is a union of $G(p)$-cosets. Write $s = kp'l'$, where $k \mid m$ and $l' \mid l$. Observe that $p \nmid \phi(l)$. By Proposition 3.1(ii), we see that $D(mp')$ is a union of $G(p)$-cosets, and $D(s)$ is a union of $G(p)$-cosets if $D(kp')$ is a union of $G(p)$-cosets. We are done if $m = 1$ as $k$ must be 1 also. If $m \neq 1$, our result will then follow from Lemma 3.3 once we show that $D(m)$ is free. Suppose $D(m)$ is not free. Then $D(m)$ is a union of $G(q)$-cosets for some prime divisor $q$ of $m$. As $q$ is greater than any prime divisors of $p'$, $q \nmid \phi(p')$. By Proposition 3.1(ii), $D(n)$ is a union of $G(q)$-cosets. This contradicts the maximality of $p$. Therefore, $D(m)$ is free.
Finally, we deal with the case when $D(G)$ is free. We need one more lemma.

**Lemma 3.5.** Suppose $D(m)$ is free and $p$ is a prime with $p^2 \not| m$. Then $\Omega_m \subset \Omega_{m/p}$ and $D(m/p) = \Omega_m(h)$ for any $h \in D(m/p)$. Furthermore, $D(m/p)$ is free unless $p = 2$ and $m = 2^3 m'$, where $m'$ is odd.

**Proof.** Let $m = p_1^{e_1} p_2^{e_2} \cdots p_{s-1}^{e_{s-1}} p' e_s^{e_s}$ be the prime factorization of $m$, with $p_1 > p_2 > \cdots > p > \cdots > p_s$. Set $k = p_1 p_2 \cdots p_{s-1} p'$ if $p$ is not the largest prime divisor of $m$. Otherwise, set $k = p'$. Let $s \in \Omega_m$. We claim that $D(k)$ is free and $\sigma(D(k)) = D(k)$. In the case $k = p'$, our claim follows from Proposition 3.1. So we may assume $k = p_1 p_2 \cdots p_{s-1} p'$.

By Proposition 3.1 and the assumption that $D(m)$ is free, we conclude that $\sigma(D(p_1 p_2 \cdots p_{s-1} p')) = D(p_1 p_2 \cdots p_{s-1} p')$ and $D(p_1^{2} p_2^{2} \cdots p_{s-1}^{2} p')$ are free. Note that $p_i$ is odd for $1 \leq i \leq l - 1$. We can thus apply Lemma 3.2 repeatedly to conclude that $D(k)$ is free. As in the proof of Lemma 3.3,

$$D(p_1^{e_1} p_2^{e_2} \cdots p_{s-1}^{e_{s-1}}) \cdot D(k) = \sum \alpha \sigma(D(k)) \cdot D(k).$$

Clearly, $m/k_i$, $k_i$ are relatively prime. It follows from Proposition 3.1 that $\sigma(D(k)) = D(k)$ for all $i$. Applying $\sigma$ to $(*)$, we get

$$D(p_1^{e_1} p_2^{e_2} \cdots p_{s-1}^{e_{s-1}}) \cdot \sigma(D(k)) = \sum \alpha \sigma(D(k)) \cdot \sigma(D(k)).$$

Let $\chi$ be as defined in Proposition 2.10. Then $(*)$ and $(**)$ give

$$\chi(D(p_1^{e_1} p_2^{e_2} \cdots p_{s-1}^{e_{s-1}})) = \chi(D(k)) - \chi(\sigma(D(k))) = 0.$$

Recall that $D(p_1^{e_1} p_2^{e_2} \cdots p_{s-1}^{e_{s-1}})$ is free. Hence by Proposition 2.10, $\chi(D(p_1^{e_1} p_2^{e_2} \cdots p_{s-1}^{e_{s-1}})) \not= 0$. Therefore, $\chi(D(k)) = \chi(\sigma(D(k)))$. As $D(k)$ is free, by Proposition 2.10, $\sigma(D(k)) = D(k)$.

Now, consider $D(k) \cdot D(m/p)$. Suppose $D(m/p)$ is free. Then by using an argument similar to that used before, we get $D(m/p) = \sigma(D(m/p))$. This proves $\Omega_m \subset \Omega_{m/p}$. By Lemma 3.2, $D(m/p)$ is free unless $p = 2$ and $m = 2^3 m'$, where $m'$ is odd. Thus we may assume $p = 2$ and $m = 2^3 m'$, where $m'$ is odd. As argued in the beginning of the proof, $D(m')$ is free. Hence by Proposition 3.1(iii), $D(2^2 m')$ must be a union of $G(2)$-cosets. Let $h \in D(2^2 m')$. We can write $h = ab$, where $\circ(a) = 4$ and $\circ(b) = m'$. As $D(2^2 m')$ is a union of $G(2)$-cosets, we deduce from Proposition 3.1(i) that $D(2^2 m') = \{a, a^2, a^3, \Omega_m(b)\}$. As shown there, $\Omega_{2m}(b)$ and $\Omega_{4m}(b)$ are S-principal subsets containing $b$. Hence they are the same. Thus, $\sigma(\Omega_{4m}(b)) = \Omega_{4m}(b)$. As it is clear that $\sigma(D(4)) = D(4)$, we conclude that $\sigma(D(4m')) = D(4m')$. This completes the proof that $\sigma(D(m/p)) = D(m/p)$. 


Next, we show $D(m/p) = \Omega_m(h)$ for any $h \in D(m/p)$. Let $h \in D(m/p)$. As $\Omega_m \subset \Omega_m/m_p$, $D(m/p) \supset \Omega_m(h)$. Choose an element $g \in G$ such that $g^p = h$. Let $\tau \in \text{Aut } G$ with $\tau(D(m))$ the $S$-principal subset that contains $g$. Since $\tau(D(m)) = \Omega_m(g)$ is free, we can apply an argument similar to that in the proof of Lemma 3.2 to conclude that $\tau(D(m))^{(p)} = \Omega_m(g^p)$ is a union of $S$-principal subsets. Since $h \in \Omega_m(g^p)$, one of those $S$-principal subsets must be $D(m/p)$. Therefore, we have $\Omega_m(g^p) = \Omega_m(h \supset D(m/p))$. This proves $D(m/p) = \Omega_m(h)$. 

We now have all the tools with which to determine the structure of $S$ when $D(G)$ is free.

**Theorem 3.6.** Suppose $|G| = n$ and $D(n)$ is a free $S$-principal subset. Then, any $S$-principal subset is of the form $\Omega_n(h)$ for some $h \in G$.

**Proof.** It suffices to show that for any divisor $n$ and $h \in D(m)$, $\Omega_n(h) = D(m)$. As $D(D(m) = \Omega_m(h)$, we need only show $\Omega_n(h) = \Omega_m(h)$ for any $h \in D(m)$. We shall prove this by induction on $n$. When $n$ is a prime, $m$ must be $n$ and our result is trivial.

We now assume $n$ is not a prime. If $n/m$ and $m$ are relatively prime, then $\Omega_n(h) = D(m)$ follows from Proposition 3.1(i). We may thus assume $(n/m, m) \neq 1$. Let $p$ be a prime divisor of $(n/m, m)$ and $r \in \mathbb{N}$ such that $p^r \parallel n$. Clearly, $r \geq 2$. By Lemma 3.5, $D(n/p) = \Omega_n(g^r)$ for any $g^r \in D(n/p)$. If $p$ is odd or $r \neq 3$, then by Lemma 3.2, $D(n/p)$ is free. By the induction hypothesis on the Schur ring $S \cap \mathbb{Z}[G(n/p)]$, we get $\Omega_{n/p}(h) = D(m)$. Let $g^r \in D(n/p)$. Clearly, $h = g^r$ for some integer $i$. As $\Omega_{n/p}(g^r) = D(n/p) = \Omega_n(g^i)$, $\Omega_n(g^i) = \Omega_{n/p}(g^i)$. Hence, we have $\Omega_n(h) = \Omega_{n/p}(h) = D(m)$.

That leaves us with the case when $2$ is the only prime divisor of $(m, n/m)$ and $r = 3$. In this case, $n = 8k$, where $k$ is odd, and $m = 2k$ or $4k$. If $m = 4k$, our result follows from Lemma 3.5. If $m = 2k$, write $h = ab$, where $\sigma(a) = 2$ and $\sigma(b) = k$. Clearly, $D(2k) = a \cdot \Omega_{2k}(b)$. By Proposition 3.1(i), $\Omega_n(b) = \Omega_{2k}(b)$ and $\Omega_n(b) = \Omega_{8k}(b)$. Since $\sigma(a) = a$ for all $\sigma \in \text{Aut } G$, we easily get $D(2k) = \Omega_n(ab) = \Omega_n(h)$. 

In view of Theorems 3.4 and 3.6 and [LM, 4.3, 4.5, 5.2], we now give a full description of all possible structures of Schur rings over a cyclic group.

**Theorem 3.7.** Let $G$ be a cyclic group of order $n$. Any Schur ring $S$ over $G$ can be constructed as follows:

1. Take a subgroup $\Omega$ of $\text{Aut } G$, set $S = \mathbb{Z}[G]^\Omega$. Here, $\text{Aut } G$ acts naturally on $\mathbb{Z}[G]$ and $\mathbb{Z}[G]^\Omega$ is the subring that is invariant under $\Omega$.

2. Choose a pair of subgroups $H$ and $K$ in $G$ such that $G$ is the direct product of $H$ and $K$. Take any Schur ring $S_H$ and $S_K$ over $H$ and $K$, respectively, and set $S = S_H \cdot S_K$. 

Choose two subgroups $H$ and $K$ with $H \subseteq K$ in $G$. Take any Schur rings $S_{G/H}$ and $S_K$ over $G/H$ and $K$, respectively, such that $H \subseteq S_K$ and $\rho S_K = \mathbb{Z}[K/H] \cap S_{G/H}$. Define $S = S_K \wedge S_{G/H}$. Here $\rho$ and $\rho^*$ are as defined in Proposition 1.2.

As an application of Theorem 3.7, we give an easy proof of [M, Theorem 3.1]. Let $D$ be an $S$-principal subset $D$ having a trivial radical. It is equivalent to saying that $D$ is not a union of $H$-cosets for any nontrivial subgroup $H$. We shall now prove [M, Theorem 3.1] by induction on $|G|$.

There is nothing to be proved if $S$ is of type (I). In particular, our desired result follows when $|G|$ is a prime. If $S$ is of type (II), then we simply apply induction on $H$ and $K$. Finally, if $S$ is of type (III), $K, H$ are as described there. Then clearly, $D \subseteq K$ and we can therefore apply induction to obtain the desired conclusion.

REFERENCES