INTEGRAL REPRESENTATIONS
OF CYCLIC GROUPS OF ORDER $p^2$

IRVING REINER

Abstract. Let $p$ be an odd prime, either regular or properly irregular, and let $G$ be a cyclic group of order $p^2$. The author determines a full set of inequivalent representations of $G$ by matrices with rational integral entries. This information is used to calculate the ideal class number of the integral group ring $\mathbb{Z}G$.

Let $G$ be a cyclic group of order $p^2$ with generator $x$, where $p$ is an odd prime. We shall determine the number $n(\mathbb{Z}G)$ of nonisomorphic indecomposable $\mathbb{Z}G$-lattices, for the case where $p$ is a regular odd prime (that is, $p$ does not divide the class number of the cyclotomic field $\mathbb{Q}(\sqrt[2]{p})$). We shall also calculate $h(\mathbb{Z}G)$, the number of isomorphism classes of ideals $M$ in $\mathbb{Z}G$ for which $Q_M = QG$. Such problems were considered previously by various authors (see Heller-Reiner [2], for example), but no explicit formulas for $n(\mathbb{Z}G)$ and $h(\mathbb{Z}G)$ were obtained, because of difficulties about units. The methods of Galovich [1] enable one to overcome these difficulties for the case where $p$ is a regular odd prime. We restrict ourselves to this case from now on, unless otherwise stated.

We may write the integral group ring $\mathbb{Z}G$ as $\mathbb{Z}[x]/(x^p - 1)$. Letting $\phi_p(m)(x)$ denote the cyclotomic polynomial of order $p^m$, we now set

$$ R = \mathbb{Z}[x]/(\phi_p(x)), \quad S = \mathbb{Z}[x]/(\phi_p^2(x)), \quad T = \mathbb{Z}[x]/(x^p - 1). $$

Then $R$ is the ring of all algebraic integers in the cyclotomic field $\mathbb{Q}(\sqrt{p^2 - 1})$; let $h_S$ denote its class number. Likewise, $S$ is the ring of integers in $\mathbb{Q}(\sqrt{p^2 - 1})$; let its class number be $h_S$. Finally, $T$ is the integral group ring of a group of order $p$.

We shall set $\lambda = 1 - x$, viewed either as an element of $\mathbb{Z}G$, or else as an element of some quotient ring, such as $R$, $S$, $R/pR$, and so on. Let

$$ \bar{Z} = \mathbb{Z}/p\mathbb{Z}, \quad \bar{R} = R/pR = R/\lambda^{p-1}R \cong \bar{Z}[\lambda]/(\lambda^{p-1}), \quad \bar{T} = T/pT \cong \bar{Z}[\lambda]/(\lambda^p). $$

The subscript $p$ will indicate $p$-adic completion. In order to conform to the notation in [2], we now set

$$ A = Z_p a \cong Z_p, \quad B = R_p b \cong R_p, \quad C = S_p c \cong S_p, \quad E = T_p e \cong T_p, $$

where $A$, $B$, $C$ and $E$ are viewed as $Z_p G$-lattices. For each $\mathbb{Z}G$-lattice $N$, we have
\[
\text{Ext}^1_{ZG}(S, N) \cong \text{Ext}^1_{ZG}(S_0, N_0) \cong \overline{N} = N/pN.
\]

As shown in [2], a full list of nonisomorphic indecomposable \(Z_p G\)-lattices is as follows:

1. \(A, B, C, E\).
2. Extensions of \(C\) by \(A \oplus E\), corresponding to extension classes \(\bar{a} + \lambda \bar{e}\) in \(A \oplus \bar{E}\), \(1 \leq r \leq p - 2\).
3. Extensions of \(C\) by \(E\), corresponding to extension classes \(\lambda \bar{e}\), \(0 \leq r \leq p - 1\).
4. Extensions of \(C\) by \(A \oplus B\); classes \(\bar{a} + \lambda \bar{b}\), \(0 \leq r \leq p - 2\).
5. The extension of \(C\) by \(A\), with extension class \(\bar{a}\).
6. Extensions of \(C\) by \(B\), corresponding to extension classes \(\lambda \bar{b}\), \(0 \leq r \leq p - 2\).

For each indecomposable \(ZG\)-lattice \(X\), we know from [2] that its completion \(X_p\) is also indecomposable, and hence occurs in the above list. We shall say that \(X\) is of “type \(k\)” if \(X_p\) is listed in the \(k\)th grouping. Corresponding to the \(Z_p G\)-lattice \(A\), the only possible \(X\) is the \(G\)-trivial module \(Z\). Next, the \(h_R\) representatives of the ideal classes of \(R\) give (up to isomorphism) all indecomposable \(ZG\)-lattices \(X\) for which \(X_p = B\). Likewise, there are \(h_S\) ideals of \(S\) which correspond to \(C\). Finally, there are precisely \(h_T\) possible \(X\)’s corresponding to \(T\), namely, the projective ideals of the integral group ring \(T\). (This last assertion follows readily from the discussion below.)

Consider next an \(X\) of type \((6)\), so \(X_p\) is an extension of \(C\) by \(B\). Then \(X\) must be isomorphic to an extension of \(C\) by \(B\), where \(c\) is an ideal of \(S\), and \(b\) is an ideal of \(R\). Now

\[
\text{Ext}^1_{ZG}(c, b) \cong \text{Ext}^1_{ZG}(S, R) \cong \overline{R}.
\]

Furthermore,

\[
\text{Aut } c \cong \text{Aut } S \cong u(S), \quad \text{Aut } b \cong \text{Aut } R \cong u(R),
\]

where \(\text{Aut}\) denotes the group of \(ZG\)-automorphisms, and \(u(\ )\) denotes the group of units. However, the isomorphism class of \(X\) is completely determined by the orbit of its extension class under the action of \(\text{Aut } c\) and \(\text{Aut } b\). It follows at once that in enumerating such orbits, we need only consider the case where \(X\) is an extension of \(S\) by \(R\). The total number of \(X\)’s will then be \(h_R h_S\) times the number of extensions of \(S\) by \(R\).

So now let \(X\) be an extension of \(S\) by \(R\), and let \(\xi \in \overline{R}\) be its class in \(\text{Ext}^1(S, R)\). We may write \(\xi = \lambda \nu\), where \(0 \leq r \leq p - 2\) and where \(\nu\) is a unit in the ring \(R' = \mathbb{Z}[\lambda]/(\lambda^{p-1} - 1)\). We must calculate the number of orbits of \(u(R')\) under the action of \(u(R)\) and \(u(S)\). For each \(w \in u(S)\), its norm \(N(w)\) from \(S\) to \(R\) is a unit of \(R\). It is easily verified that \(w\) acts on \(u(R')\) in the same way that \(N(w)\) acts. Hence it suffices for us to count the orbits of \(u(R')\) under the action of \(u(R)\).

Now \(u(R')\) is the direct product of a cyclic group \(D\) of order \(p - 1\), and an elementary abelian \(p\)-group generated by the units

\[
1 + \lambda, 1 + \lambda^2, 1 + \lambda^3, \ldots, 1 + \lambda^{p-2}.
\]

But for \(p\) regular, Galovich [1] showed that the image of \(u(R)\) in \(u(R')\) is the product of \(D\) and a subgroup generated by units of the form
\begin{equation}
1 + \lambda, 1 + \lambda^2 + \alpha_2 \lambda^3, 1 + \lambda^4 + \alpha_4 \lambda^5, \\
1 + \lambda^6 + \alpha_6 \lambda^7, \ldots, 1 + \lambda^k + \alpha_k \lambda^{k+1},
\end{equation}

where each \( \alpha_i \in R' \), and where \( k \) is the largest even integer \(< p - 2 - r \). The "missing" exponents are 3, 5, 7, \ldots, \( p - 2 - r \), the last term occurring only for even \( r \). The number of such missing exponents is \( \lfloor (p - 3 - r)/2 \rfloor \), where this symbol\(^2\) is interpreted as 0 whenever \( p - 3 - r < 0 \). Consequently, the cokernel of the map \( u(R) \to u(R') \) is an elementary \( p \)-group on \( \lfloor (p - 3 - r)/2 \rfloor \) generators. Hence the total number of indecomposable \( Z \)-\( G \)-lattices of type (6) is given by

\begin{equation}
\sum_{r=0}^{p-2} \frac{p^{(p-3-r)/2}}{r!}.
\end{equation}

A similar argument shows that the number of lattices of type (4) is also given by formula (7). In this situation, we must count the orbits of \( \mathbb{Z} \oplus \overline{R} \) under the action of \( u(R) \) and \( u(S) \). This action is given by

\[ w(\overline{z} + \overline{r})u = N(w)\overline{z} + N(w)\overline{ru} \]

for \( w \in u(S) \), \( \overline{z} + \overline{r} \in \mathbb{Z} \oplus \overline{R} \), \( u \in u(R) \). We may choose \( w \) so that \( N(w)\overline{z} = \overline{1} \), and then proceed with the remaining term \( N(w)\overline{ru} \) as in the preceding paragraph. This gives formula (7) just as before.

It is easily seen that there are \( h_s \) indecomposable \( Z \)-\( G \)-lattices of type (5), and it remains for us to consider lattices of types (2) and (3). Suppose that \( X \) is of type (3), and is an extension of \( S \) by \( T \). We have seen that

\[ \text{Ext}^1(S, T) \cong \overline{T} \cong \mathbb{Z}[\lambda]/(\lambda^p), \]

and the extension class of \( X \) is of the form \( \lambda^r v \) for some \( r \), \( 0 \leq r \leq p - 1 \), and some \( v \in u(R') \) with \( R' = \mathbb{Z}[\lambda]/(\lambda^{p-r}) \). We wish to count the number of orbits of \( u(R') \) under the action of \( u(S) \) and \( u(T) \).

If \( r > 1 \) then \( R' \) is a quotient of \( R \), and both \( u(S) \) and \( u(T) \) act on \( R' \) via \( u(R) \). Hence by the preceding discussion, the number of orbits equals \( p^{(p-2-r)/2} \). Consider now the case \( r = 0 \), in which \( R' = \mathbb{Z}[\lambda]/(\lambda^p) = \overline{T} \). The group \( u(\overline{T}) \) is the direct product of a cyclic group \( D \) of order \( p - 1 \), and an elementary \( p \)-group with generators

\[ 1 + \lambda, 1 + \lambda^2, 1 + \lambda^3, \ldots, 1 + \lambda^{p-1}. \]

On the other hand, we note that

\[ \overline{T} = \mathbb{Z}[x]/(\phi_{p^2}(x), x^p - 1) \cong S/(x^p - 1) = S/(\lambda^p). \]

By [1], the image of \( u(S) \) in \( u(\overline{T}) \) is the product of \( D \) and the subgroup generated by units of the form

\[ 1 + \lambda, 1 + \lambda^2 + \alpha_2 \lambda^3, 1 + \lambda^4 + \alpha_4 \lambda^5, \ldots, 1 + \lambda^{p-1}, \]

where each \( \alpha_i \in \overline{T} \). The "missing" exponents are 3, 5, \ldots, \( p - 2 \); there are \( (p - 3)/2 \) such exponents. Furthermore, none of them can be recaptured from the action of \( u(T) \) on \( u(\overline{T}) \), since each unit of \( T \) maps onto a unit of \( R \) under the surjection \( T \to R \). Thus the number of orbits for the case \( r = 0 \) is

---

\(^2\)For \( y > 0 \), the symbol \([y]\) denotes the greatest integer \(< y\).
precisely $p^{(p-3)/2}$. It follows at once that the total number of indecomposable $ZG$-lattices of type (3) is given by

$$h_R h_S \beta,$$

where $\beta = \sum_{r=0}^{p-1} p^{(p-2-r)/2}$.

A similar argument shows that the number of lattices of type (2) is given by $(\alpha - 1)h_R h_S$, since in (2) the parameter $r$ ranges from 1 to $p - 2$. We may remark that

$$\beta = \alpha + p^{(p-3)/2},$$

where $\alpha$ is defined in (7).

Combining all of these results, we have:

**Theorem.** For $p$ a regular odd prime, the number $n(ZG)$ of isomorphism classes of indecomposable $ZG$-lattices is given by

$$n(ZG) = 1 + 2h_R + 2h_S + (3\alpha - 1)h_R h_S + \beta h_R h_S,$$

where $\alpha, \beta$ are defined in (7) and (8).

We are now in a position to compute $h(ZG)$, the number of isomorphism classes of ideals $M$ in $ZG$ for which $QM = QG$. In the first column below, we list all $M$'s (apart from using ideals in $R$ and $S$, rather than the rings $R$ and $S$ themselves). In the second column, we list the number of $M$'s of each kind, omitting the factor $h_R h_S$ arising from the ideal classes.

<table>
<thead>
<tr>
<th>Classes of ideals in $ZG$</th>
<th>Number of classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>$Z \oplus R \oplus S$</td>
<td>1</td>
</tr>
<tr>
<td>$Z \oplus$ type 6</td>
<td>$\alpha$</td>
</tr>
<tr>
<td>$R \oplus$ type 5</td>
<td>1</td>
</tr>
<tr>
<td>$S \oplus E$</td>
<td>1</td>
</tr>
<tr>
<td>type 3</td>
<td>$\beta$</td>
</tr>
<tr>
<td>type 4</td>
<td>$\alpha$</td>
</tr>
</tbody>
</table>

(Note that type 2 does not give ideals in $ZG$.) We thus obtain:

**Corollary.** The number of ideal classes of $ZG$ is

$$h(ZG) = (3 + 2\alpha + \beta)h_R h_S$$

with $\alpha, \beta$ as in (7) and (8).

When the prime $p$ is irregular, the expressions in the Theorem and its Corollary give lower bounds for $n(ZG)$ and $h(ZG)$, respectively. This follows from our earlier discussion and Galovich's results about units for the case of irregular primes.

The prime $p$ is called properly irregular if $p$ divides $h_R$, but does not divide the class number of the maximal real subfield of $Q(\sqrt[p]{1})$. As pointed out by Galovich, his methods can be applied to the case of properly irregular primes to obtain analogues of the preceding Theorem and its Corollary. For $k \leq (p - 3)/2$, let $\delta(k)$ be the number of Bernoulli numbers among $B_1, B_2, \ldots, B_k$ whose numerators are multiples of $p$. (If $p$ is a regular prime, each
Assuming now that \( p \) is properly irregular, let us consider the orbits of \( u(R') \) under the action of \( u(R) \), where \( R' = \mathbb{Z}[(\lambda^{p-1}-r)] \), with \( 0 < r < p - 2 \). In determining the image of \( u(R) \) in \( u(R') \), we must omit from the list (6a) all those terms \( 1 + \lambda^{2i} + \alpha_i \lambda^{2i+1} \) for which \( p \) divides the numerator of \( B_i \). It follows at once that the number of indecomposable \( ZG \)-lattices of type (6) is given by

\[
h_R h_S \alpha', \quad \text{where} \quad \alpha' = \sum_{r=0}^{p-2} p^{(p-3-r)/2} + \delta((p-2-r)/2).
\]

This also gives the number of indecomposables of type (4).

On the other hand, the image of \( u(S) \) in \( u(T) \) still contains \( 1 + \lambda^{p-1} \), even when \( p \) is properly irregular. It follows easily that the number of indecomposable lattices of type (3) is given by

\[
h_R h_S \beta', \quad \text{where} \quad \beta' = \alpha' + p^{(p-3)/2} + \delta((p-3)/2).
\]

Finally, the number of indecomposables of type (2) is given by \( h_R h_S (\alpha' - 1) \).

Thus, when \( p \) is properly irregular, the analogues of the Theorem and its Corollary are valid, provided that we use \( \alpha' \) in place of \( \alpha \), and \( \beta' \) in place of \( \beta \).

As a concluding remark, it should be mentioned that in all cases known so far, every odd prime is either regular or properly irregular.

References

Department of Mathematics, University of Illinois, Urbana, Illinois 61801