THE MODULAR GROUP-RING OF A FINITE $p$-GROUP

D. L. JOHNSON

Abstract. For a finite $p$-group $G$ and the field $k$ of $p$ elements, we investigate the embedding of $G$ in the group $G^*$ of elements of the group-ring $kG$ having coefficient-sum equal to 1. Of particular interest is the question of when $G$ has a normal complement in $G^*$, for in this case simple proofs can be given for a number of diverse known results.

Since its inception in [5], the study of modular group-rings of finite $p$-groups has largely centred around the problem (see [1], [3], for example): "When does isomorphism of group-rings imply isomorphism of groups?" A key role in these investigations has been played by the group of units in the group-ring.

Fixing our notation, we let $p$ denote a fixed prime, $G$ a finite $p$-group, $k$ the field of $p$ elements and $kG$ the group-ring of $G$ over $k$. The group of units of $kG$ is simply $kG \setminus U$, where $U$ is the augmentation ideal of $kG$. Furthermore, $kG \setminus U = G^* \times k^*$, where $G^* = 1 + U$, and $k^* = k \setminus \{0\}$. We call $G^*$ the mod $p$ envelope of $G$, and denote the embedding $G \hookrightarrow G^*$ by $\iota_G$, or simply $\iota$.

Note that $G^*$ is also a $p$-group.

Some properties of $\iota$ are as follows:

(1) $Z(G) = Z(G^*) \cap G$,
(2) $N_{G^*}(G) = GC_{G^*}(G)$,
(3) $G' = (G^*)' \cap G$,
(4) $\Phi(G) = \Phi(G^*) \cap G$.

None of these is very hard; (2) and (3) are proved in [2], and (4) in [6]. We have not yet, however, found a proof for

(5) $G^p = (G^*)^p \cap G$.

Incidently, the truth of (2) was established independently by the present author in an (entirely abortive) attempt to find a simple proof of Gaschütz' theorem [4].

We now define the class $\mathcal{C}_p$ of finite $p$-groups to consist of those $G$ which have a normal complement in $G^*$. The properties (1)–(5), along with many others, are immediately obvious for groups in $\mathcal{C}_p$, and it only remains to

Received by the editors October 18, 1973.


The author is grateful to L. E. Moran and R. Tench for their kind permission to include the results embodied in Theorems 2, 4 and 7.

© American Mathematical Society 1978
establish the extent of this class. The purpose of this article is to outline the present state of our knowledge about this problem.

The embedding \( i: G \to G^* \) gives rise to a number of other questions which are beyond the scope of this article. For instance, what (if anything) can be said about the direct limit of the sequence \( G \subseteq G^* \subseteq G^{**} \subseteq \cdots ? \) Can the embedding \( G \subseteq G^* \) be defined by any useful universal property? Are there any significant differences in the theory when \( k \) is replaced by an arbitrary field of characteristic \( p \)? Can we find a formula relating \( \exp G \) and \( \exp G^* \)? While these are equal for abelian groups, equality does not hold in general, as the example of the elementary nonabelian group of order \( p^3 \) shows (see [6]).

It would also be of interest to investigate the relations between the modular representation theory (and also the cohomology) of \( G \) and \( G^* \), for if \( E(G) \) denotes the representation algebra of \( G \) (the vector space over the complex numbers with isomorphism classes of indecomposable \( kG \)-modules as a basis, and multiplication the Kronecker product of representations), then the definition of \( G^* \) ensures that the restriction homomorphism: \( E(G^*) \to E(G) \) splits.

Finally, and perhaps hardest of all, is there an algorithm for finding a presentation for \( G^* \) (in terms of generators and relations) given a presentation of \( G \)?

**Theorem 1.** If \( G \) is cyclic, then \( G \in \mathbb{Q}_p \).

**Proof.** There is an elementary result, which may be thought of as a lemma for the basis theorem or as a consequence of it, to the effect that for any finite abelian \( p \)-group \( G \) and any \( x \in G \) with \( |x| = \exp G \), \( \langle x \rangle \) is a direct factor of \( G \). This, together with the obvious remark that \( \exp G = \exp G^* \) when \( G \) is abelian, proves the result.

We next give a simpler proof of a result in [6].

**Theorem 2.** If \( G, H \in \mathbb{Q}_p \), then \( G \times H \in \mathbb{Q}_p \).

**Proof.** The epimorphisms from \( G \times H \) to \( G \) and \( H \) induce epimorphisms

\[
\begin{array}{ccc}
(G \times H)^* & \xrightarrow{\nu_1} & G^* \\
& \nu_2 & \downarrow \\
& & H^*
\end{array}
\]

If \( N_1 \) and \( N_2 \) are normal complements (which exist by hypothesis) for \( G \) and \( H \) in \( G^* \) and \( H^* \), respectively, then let \( \overline{N}_1 \) and \( \overline{N}_2 \) denote their pre-images in \( (G \times H)^* \) under \( \nu_1 \) and \( \nu_2 \) respectively. \( \overline{N}_1 \) and \( \overline{N}_2 \) are clearly normal subgroups of \( (G \times H)^* \) such that

\[
\overline{N}_1 \cap (G \times H) = H, \quad \overline{N}_2 \cap (G \times H) = G,
\]

so that if we let \( N = \overline{N}_1 \cap \overline{N}_2 \), then \( N \cap (G \times H) = E \). Furthermore,
\[(G \times H)^* : N < \text{Im}(G \times H)^* \rightarrow \overline{N_1} \mid (G \times H)^* : N_2 \]

\[= \mid G^* : N_1 \mid H^* : N_2 \mid = \mid G \mid H = \mid G \times H \mid.\]

Thus \(N\) is the required normal complement.

**Theorem 3.** If \(G\) is abelian, then \(G \in \mathcal{L}_p\).

**Proof.** An immediate consequence of Theorems 1 and 2.

The next result is due to Tench [8], and yields the converse of Theorem 2.

**Theorem 4.** If \(G\) belongs to \(\mathcal{L}_p\), then so does any normally complemented subgroup \(H\) of \(G\).

**Proof.** Let \(\alpha: H^* \rightarrow G^*\) be the inclusion induced by \(H < G\), let \(\beta: G^* \rightarrow G\) be a splitting for \(\iota_G\), and let \(\gamma: G \rightarrow H\) be a splitting for \(H < G\). Then the composite

\[H^* \xrightarrow{\alpha} G^* \xrightarrow{\beta} G \xrightarrow{\gamma} H\]

is clearly a splitting for \(\iota_H\), whose kernel is thus the required normal complement.

**Theorem 5.** For any \(G\), \(G^* \in \mathcal{L}_p\).

**Proof.** Note that \(G^*\), being a subset of \(kG\), is closed under the formation of linear combinations of its elements, provided the coefficient-sum is equal to 1. Now any element of \(G^{**}\) is just a “formal” linear combination of this type, and thus gives rise to a unique element of \(G^*\) (the corresponding “real” linear combination). This mapping is easily seen to be an epimorphism from \(G^{**}\) to \(G^*\) which fixes \(G^*\) elementwise. It is thus a splitting for \(\iota_{G^*}\) and its kernel is the required normal complement.

**Theorem 6.** If \(G_n\) denotes the Sylow \(p\)-subgroup of \(GL(n, p)\), then \(G_n \in \mathcal{L}_p\) for all \(n\).

**Proof.** The embedding \(G_n \rightarrow GL(n, p) \rightarrow M_n(k)\) extends by linearity to a homomorphism of rings \(kG_n \rightarrow M_n(k)\) whose restriction to \(G_n^*\) is such that all its images are units in \(M_n(k)\). We thus obtain a homomorphism \(\alpha: G_n^* \rightarrow GL(n, p)\) which fixes \(G_n\) elementwise. But since \(G_n^*\) is a \(p\)-group and \(G_n\) is a Sylow \(p\)-subgroup of \(GL(n, p)\), we must have \(\text{Im } \alpha = G_n\), so that \(\text{Ker } \alpha\) forms the required normal complement.

**Note.** By examining certain sets of upper triangular matrices with 1’s on the main diagonal, this argument can be extended to show that various other \(p\)-subgroups of \(GL(n, p)\) lie in \(\mathcal{L}_p\). Note further that if we knew \(\mathcal{L}_p\) to be subgroup-closed, it would follow from Theorem 6 (or from Theorem 5) that \(\mathcal{L}_p\) contained all finite \(p\)-groups.

Finally, for the sake of completeness, we list a few groups of small order in \(\mathcal{L}_p\) (see [7] for the proof).

**Theorem 7.** The following groups belong to \(\mathcal{L}_p\):

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
(a) the two nonabelian groups of order 8 \((p = 2)\),
(b) the nonabelian group of exponent \(p\) and order \(p^3\) \((p > 2)\),
(c) the three nonabelian indecomposable groups of exponent 4 and order 16 \((p = 2)\).

Note in conclusion that the “smallest” group not definitely known to belong to \(\mathcal{G}_p\) is the dihedral group \(D_{16}\) of order 16 \((p = 2)\). A programme involving the conjugacy classes of \(D_{16}^p\) is currently in preparation to decide the question using a high-speed computing machine.

REFERENCES


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF NOTTINGHAM, NOTTINGHAM, ENGLAND