ON GROUPS OF ORDER p^3

JAMES A. COHN AND DONALD LIVINGSTONE

The simplest example of two non-isomorphic groups with the same character tables is provided by the non-abelian groups of order p^3, $p \neq 2$. Let G_1 be the one of exponent p and let G_2 be the other. If Q denotes the field of rational numbers, then Berman **(2)** has shown that $QG_1 \approx QG_2$, where QG_i denotes the rational group algebra. In this note we shall show that the corresponding statement is false for ZG_i, where Z is the ring of rational integers. More explicitly we shall show that ZG_1 does not contain a unit of order p^2 so that it is impossible to embed ZG_2 in ZG_1.

We represent the elements of G_1 by the ordered triples $[r, s, t]$ of integers (mod p) where

$$[r, s, t][r', s', t'] = [r + r', s + s', t + t' + sr'].$$

It follows that the unit vectors generate G_1, and $[0, 0, 1]$ generates the centre of G_1, which is also its commutator subgroup G_1'. Let ϕ be the homomorphism of ZG_1 onto $Z(G_1/G_1')$, and let Γ denote one of the non-linear irreducible representations of QG_1. Obviously ZG_1 can be embedded in the direct sum of the irreducible representations of QG_1. Since the linear representations of ZG_1 can all be factored through $Z(G_1/G_1')$ and since the non-linear representations are all conjugate, it follows that $\phi \oplus \Gamma$ embeds ZG_1 in $Z(G_1/G_1') \oplus M$, where M is a ring of $p \times p$ matrices with entries from $Z(\omega)$, ω a primitive pth root of unity. In fact we can choose M to consist of matrices with entries from $Z[\omega]$ since the representations are monomial. More explicitly we define

$$\Gamma[1, 0, 0] = \begin{bmatrix} & & & 1 \\ 1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & \cdot & \\ & & 1 & \end{bmatrix}, \quad \Gamma[0, 1, 0] = \begin{bmatrix} 1 & & & & \\ & \omega & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & \omega^{p-1} \end{bmatrix}, \quad \Gamma[0, 0, 1] = \omega I.$$

Since ZG_1 is embedded in $Z(G_1/G_1') \oplus M$, it follows that $U(ZG_1)$, the group of units of ZG_1, is embedded in $U(Z(G_1/G_1')) \times U(M)$. Thus to show that ZG_1 has no unit of order p^2 it suffices to show this for $Z(G_1/G_1')$ and M separately. Since G_1/G_1' is abelian, every unit of finite order in $Z(G_1/G_1')$ is

Received August 31, 1962. The second author's research was supported in part by a fellowship from the Rackham School of Graduate Studies, University of Michigan; and the first author's research was supported in part by NSF-05259.

trivial, i.e., of the form $\pm v$, $v \in G_1/G_1'$ (see **1**). It follows that no unit in $Z(G_1/G_1')$ can have order p^2. Thus we need only consider the units of M.

We next show that in fact we need only consider a certain homomorphic image M_1 of M. Let P be the unique prime ideal dividing p in $Z[\omega]$, so that $P = (1 - \omega)$.

LEMMA. *If $A = (\alpha_{ij}), \alpha_{ij} \in Z[\omega]$ is an $n \times n$ matrix of p-power order such that $A \equiv I \pmod{P^2}$, then $A = I$.*

Proof. Assume $A = I + (1 - \omega)^a B$, where $B = (\beta_{ij})$, $(1 - \omega) \nmid \beta_{ij}$ for some i, j, and $A^t = I$, where $t = p^b$. Then, using the binomial theorem, we have

$$\sum_{i=1}^{t} \binom{t}{i} [(1 - \omega)^a B]^i = 0.$$

If $a \geqslant 2$, then $(1 - \omega)^{2a+p-1}$ divides all the terms from $i = 2$ on, since $(1 - \omega)^{p-1}$ divides p exactly. It follows that $(1 - \omega)^{2a+p-1}$ divides $p(1-\omega)^a\beta_{ij}$ for all i, j. Thus $(1 - \omega)^a$ divides β_{ij} for all i, j, which is a contradiction, and so our lemma is proved.

Using the Lemma we see that if M_1 is the ring obtained by reducing the entries of the matrices in $M \pmod{P^2}$, then this homomorphism preserves the order of units (of p-power order). Thus it suffices to show that M_1 has no unit of order p^2.

Let u be a unit of finite order in ZG_1. Then since $\phi(u)$ is a trivial unit in $Z(G_1/G_1')$, we have $\phi(u) = \phi([r, s, t])$, where we can assume that

$$[r, s, t] = [0, 0, 0] = 1$$

or that r and s are not both zero. In the latter case G_1 has an automorphism sending $[r, s, t]$ to $[1, 0, 0]$; and since we are only interested in the order of u, we can assume then that $[r, s, t] = 1$ or $[1, 0, 0]$. Thus either $u - 1$ or $u - [1, 0, 0]$ is in $\ker \phi$.

We shall now give a Z-basis for Γ $(\ker \phi)$ and Γ $(\ker \phi)$ $\pmod{P^2}$. Clearly $\ker \phi$ consists of those elements of ZG_1 which sum to zero on the conjugate classes of G_1, i.e., on the cosets of G_1' in G_1. Let $\alpha_k = 1 - \omega^k$; and let $z = [0, 0, 1]$ so that $G_1' = \langle z \rangle$. Then $\Gamma(1 - z^k) = \alpha_k I$ and so $\{\alpha_k I\}$ is a Z-basis of the elements summing to zero in G_1'.

The elements $[0, s, 0](1 - z^k)$ form a Z-basis for the elements which sum to zero on the $[0, s, 0]$-cosets of G_1'. By means of a unimodular transformation we can take the elements $([0, s, 0] - 1)(1 - z^k)$ as a basis instead. However,

$$\begin{aligned}\Gamma(([0, s, 0] - 1)(1 - z^k)) &= \operatorname{diag}\,(0, (\omega^s - 1)\alpha_k, \ldots, (\omega^{s(p-1)} - 1)\alpha_n) \\ &\equiv 0 \pmod{P^2}\end{aligned}$$

and so these yield nothing new $\pmod{P^2}$, i.e., in M_1.

Finally we turn to the $[r, s, 0]$ cosets. We shall refer to the main diagonal of one of our matrices as the 0-stripe, the elements $\alpha_{21}, \alpha_{32}, \ldots, \alpha_{p,p-1}, \alpha_{1,p}$ as the 1-stripe, etc. Then a basis for the elements which sum to zero on the $[r, s, 0]$-cosets maps under Γ to the matrices with α_k on the r-stripe and 0 elsewhere (mod P^2).

Now recall that $u - 1$ or $u - [1, 0, 0] \in \ker \phi$; hence $\Gamma(u) = A + B$, where $B \in \Gamma(\ker \phi)$, and where either $A = I$ or $A = \Gamma[1, 0, 0]$ and hence has 1 on the 1-stripe and 0 elsewhere. It follows from our description of a Z-basis (mod P^2) for $\Gamma(\ker \phi)$ that B is constant on the various stripes, and hence $AB = BA$ (mod P^2) in either case. Thus

$$(\Gamma(u))^p = (A + B)^p \equiv I \pmod{P^2}.$$

It follows from the lemma that $u^p = 1$ and so ZG_1 has no unit of order p^2.

It may be added that the isomorphism $QG_1 \approx QG_2$ mentioned in the introduction can be realized explicitly by observing that the element xu, where

$$u = 1 - \frac{1}{p}(1 - z^{-1}) \sum y^s$$

and x, y, and z are the elements of G_1 represented in our notation by the unit vectors, is a unit of order p^2 which, with y and z, generates a group isomorphic to G_2. Since u is itself a unit (of order p) in $Z[1/p]\langle y, z\rangle$, it follows that the group rings of G_1 and G_2 are already isomorphic over the coefficient ring $Z[1/p]$.

References

1. S. D. Berman, *On certain properties of integral group rings*, Dokl. Akad. Nauk SSSR(N.S.), *91* (1953), 7–9; M.R. *15*, 99.
2. ——— *On certain properties of group rings over the field of rational numbers*, Užgorod. Gos. Univ. Naučn. Zap. Him. Fiz. Mat., *12* (1955), 88–110; M.R. *20*, No. 3920. (This article was not available to us, and so our knowledge of it is based upon the review.)

University of Michigan,
Ann Arbor, Michigan

https://doi.org/10.4153/CJM-1963-063-1 Published online by Cambridge University Press