THE GROUP ALGEBRAS OF GROUPS OF ORDER p^4 OVER A MODULAR FIELD

D. S. Passman

Let $\mathfrak{G}$ be a p-group, and let $\Gamma = \Gamma(\mathfrak{G})$ be the group algebra of $\mathfrak{G}$ over $K = GF(p)$, the field with p elements. If $\mathfrak{G} \simeq \mathfrak{H}$, then clearly $\Gamma(\mathfrak{G}) \simeq \Gamma(\mathfrak{H})$. However, it is not known whether the converse is true. We present a partial answer.

THEOREM. *Let* $\mathfrak{G}$ *be a* p-*group of order at most* p^4. *Then* $\Gamma(\mathfrak{G}) \simeq \Gamma(\mathfrak{H})$ *implies* $\mathfrak{G} \simeq \mathfrak{H}$.

For convenience we say that two groups $\mathfrak{G}$ and $\mathfrak{H}$ are *split* if $\Gamma(\mathfrak{G}) \not\simeq \Gamma(\mathfrak{H})$. Since the order of $\mathfrak{G}$ is given by $|\mathfrak{G}| = \dim_K \Gamma(\mathfrak{G})$, we see that $\Gamma(\mathfrak{G}) \simeq \Gamma(\mathfrak{H})$ implies that $|\mathfrak{G}| = |\mathfrak{H}|$. Hence our approach here is to consider the group algebras of all p-groups of order at most p^4 and to show that these are not isomorphic for nonisomorphic groups.

The purpose of this paper is two-fold, first, to offer nontrivial verification for "small" p-groups of the conjecture that every two nonisomorphic p-groups are split, second, to answer a question posed in [2]. In that paper two particular groups of order $81 = 3^4$ were shown to have isomorphic group algebras over all noncharacteristic 3-fields. We show here that their group algebras over GF(3) are not isomorphic.

Our techniques are for the most part based on the results of Jennings in [4].

I. NOTATION AND PRELIMINARY RESULTS

In $\mathfrak{G}$, $(A, B) = A^{-1}B^{-1}AB$, the commutator of elements A and B,

$\mathfrak{G}' = (\mathfrak{G}, \mathfrak{G})$, the commutator subgroup of $\mathfrak{G}$,

$\mathfrak{Z} = \mathfrak{Z}(\mathfrak{G})$, the center of $\mathfrak{G}$,

$\langle \dots \rangle$ = the subgroup of $\mathfrak{G}$ generated by the elements and subgroups indicated within the brackets.

In Γ, $[x, y] = xy - yx$, the Lie product of elements x and y,

$[\Gamma, \Gamma]$ = the commutator subspace of Γ,

N = the radical of Γ,

Z = the center of Γ,

J^n = the nth power of the ideal J of Γ,

$S^{(p)}$ = the set of pth powers of the elements of the subspace S of Γ,

$\langle \dots \rangle$ = the subspace of Γ spanned by the elements and subspaces indicated within the brackets.

Received January 30, 1965.

LEMMA 1. (a) *The center* Z *of* Γ *is the linear space spanned by all class sums of* $\mathfrak{G}$. (b) *The commutator subspace* $[\Gamma, \Gamma]$ *consists of all elements* $x = \sum a_G G$ *with* $\sum_{G\sim H} a_G = 0$ *for all* $H \in \mathfrak{G}$. *Here* $G \sim H$ *signifies that* G *is conjugate to* H.

Proof. Part (a) is well known. We consider part (b). Clearly, the space $[\Gamma, \Gamma]$ is spanned by all Lie products $[A, B]$ with $A, B \in \mathfrak{G}$. Now

$$[A, B] = AB - BA = (AB) - A^{-1}(AB)A.$$

Thus, if $x = \sum a_G G \in [\Gamma, \Gamma]$, then $\sum_{G\sim H} a_G = 0$ for all $H \in \mathfrak{G}$. Conversely, let $G \sim H$, so that $G = T^{-1}HT$. Then

$$G - H = T^{-1}HT - H = [T^{-1}, HT] \in [\Gamma, \Gamma].$$

Therefore the result follows.

The following two results will be used to simplify certain computations.

LEMMA 2. *Let* Ξ *be an algebra over a field of characteristic* p.

(a) *If* $a_1, \cdots, a_n \in \Xi$, *then*

$$(a_1 + a_2 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p \bmod [\Xi, \Xi].$$

(b) *Let* a *and* b *be elements of* Ξ *that commute with their Lie product* $[a, b]$. *If* $p > 2$, *then*

$$(a + b)^p = a^p + b^p.$$

Proof. Let $a, b \in \Xi$; then [3, page 187]

$$(a + b)^p = a^p + b^p + \sum_{i=1}^{p-1} s_i(a, b),$$

where

$$\underbrace{[\cdots [a, \lambda a + b]\lambda a + b] \cdots]\lambda a + b]}_{p-1} = \sum_{i=1}^{p-1} i s_i(a, b)\lambda^{i-1}$$

and λ is an indeterminate commuting with both a and b. Clearly, $s_i(a, b) \in [\Xi, \Xi]$, and thus

$$(a + b)^p \equiv a^p + b^p \bmod [\Xi, \Xi].$$

Part (a) now follows easily by induction.

Now $[a, \lambda a + b] = [a, b]$. If this term commutes with both a and b, and if $p - 1 \geq 2$, then $s_i(a, b) = 0$ for all i. This yields

$$(a + b)^p = a^p + b^p,$$

and part (b) is proved.

LEMMA 3. *The radical* N *of* Γ *is spanned by the elements* $(P - 1)$ *with* $P \in \mathfrak{G}$. *Let* A *and* B *be elements of* $\mathfrak{G}$ *with* $A - 1 \in N^i$, $B - 1 \in N^j$, *and* $1 \leq i \leq j$. *Then*

(a) $(AB - 1) \equiv (A - 1) + (B - 1) \mod N^{i+1}$,

(b) $(A^{\alpha} - 1) \equiv \alpha(A - 1) \mod N^{i+1}$,

(c) $(B - 1)(A - 1) \equiv (A - 1)(B - 1) + (C - 1) \mod N^{i+j+1}$,

where $C = (B, A) = B^{-1} A^{-1} BA$.

Proof. The first part is a restatement of [4, Theorem 1.2]. If $A, B \in \mathfrak{G}$, then

$$(AB - 1) = (A - 1)(B - 1) + (A - 1) + (B - 1).$$

Since $(A - 1)(B - 1) \in N^{i+1}$, equation (a) follows. Equation (b) is of course a special case of (a).

From the identity

$$(B - 1)(A - 1) = (A - 1)(B - 1) + AB(C - 1)$$

we conclude that $C - 1 \in N^{i+j}$. Since $AB \equiv 1 \mod N$, the above yields equation (c).

The $\mathfrak{M}$-series of $\mathfrak{G}$ (see [4, Section 5]) is defined inductively as follows.

$\mathfrak{M}_1 = \mathfrak{G}$, and $\mathfrak{M}_i = \left\langle (\mathfrak{M}_{i-1}, \mathfrak{G}), \mathfrak{M}^{(p)}_{(i/p)} \right\rangle$ for $i > 1$, where (i/p) is the least integer not less than i/p and $\mathfrak{M}^{(p)}_{\lambda}$ is the set of pth powers of elements of $\mathfrak{M}_{\lambda}$. In [4], Jennings studied the relation between the $\mathfrak{M}$-series of $\mathfrak{G}$ and the radical of $\Gamma(\mathfrak{G})$. He showed that

$$G = \mathfrak{M}_1 \supseteq \mathfrak{M}_2 \supseteq \cdots \supseteq \mathfrak{M}_r = 1$$

and that each $\mathfrak{M}_i$ is normal in $\mathfrak{G}$. Moreover, he proved the following result ([4, Theorems 3.6 and 5.5]).

PROPOSITION 4. *Let* $\mathfrak{G}$ *and* $\mathfrak{H}$ *be two* p-*groups. If* $\Gamma(\mathfrak{G}) \simeq \Gamma(\mathfrak{H})$, *then for all* i

$$\mathfrak{M}_i(\mathfrak{G})/\mathfrak{M}_{i+1}(\mathfrak{G}) \simeq \mathfrak{M}_i(\mathfrak{H})/\mathfrak{M}_{i+1}(\mathfrak{H}),$$

where $\mathfrak{M}_i(\mathfrak{G})$ *is the* i*th term of the* $\mathfrak{M}$-*series of* $\mathfrak{G}$.

COROLLARY 5. *Let* $\mathfrak{G}$ *and* $\mathfrak{H}$ *be two* p-*groups with* $\Gamma(\mathfrak{G}) \simeq \Gamma(\mathfrak{H})$. *Then* $\mathfrak{G}/\mathfrak{G}' \simeq \mathfrak{H}/\mathfrak{H}'$. *In particular, if* $\mathfrak{G}$ *is abelian, then* $\mathfrak{G} \simeq \mathfrak{H}$.

Proof. If $\mathfrak{G}$ is abelian and $\Gamma(\mathfrak{G}) \simeq \Gamma(\mathfrak{H})$, then $\mathfrak{H}$ is also abelian. Since the quotients $\mathfrak{M}_i/\mathfrak{M}_{i+1}$ clearly determine the structure of the abelian group $\mathfrak{G}$, the above proposition implies that $\mathfrak{G} \simeq \mathfrak{H}$ in this case.

Now let $\mathfrak{G}$ be an arbitrary p-group. The kernel of the natural map $\Gamma(\mathfrak{G}) \rightarrow \Gamma(\mathfrak{G}/\mathfrak{G}')$ is easily seen [2, Lemma 1.2] to be the ideal generated by $[\Gamma, \Gamma]$. Hence, if $\Gamma(\mathfrak{G}) \simeq \Gamma(\mathfrak{H})$, then $\Gamma(\mathfrak{G}/\mathfrak{G}') \simeq \Gamma(\mathfrak{H}/\mathfrak{H}')$. Since $\mathfrak{G}/\mathfrak{G}'$ is abelian, the result follows.

COROLLARY 6 (Ward [5]). *If* $\Gamma(\mathfrak{G}) \simeq \Gamma(\mathfrak{H})$, *then* $\mathfrak{Z}(\mathfrak{G}) \simeq \mathfrak{Z}(\mathfrak{H})$.

Proof. We show that $\Gamma(\mathfrak{G})$ determines the isomorphism class of $\mathfrak{Z}(\mathfrak{G})$ in a canonical manner. Let

$$c \in Z \quad \text{and} \quad x = \sum k_i[a_i, b_i] \in [\Gamma, \Gamma].$$

Then $cx = \sum k_i[ca_i, b_i] \in [\Gamma, \Gamma]$. This implies that $Z \cap [\Gamma, \Gamma]$ is an ideal of the algebra Z. Each class sum of $\mathfrak{G}$ is a sum of p^j conjugate group elements. If $j \geq 1$, then by Lemma 1(b) it is an element of $Z \cap [\Gamma, \Gamma]$. On the other hand, by Lemma 1(b) again we see that the elements of $\mathfrak{Z}$ are linearly independent modulo $[\Gamma, \Gamma]$. Thus

$$Z/(Z \cap [\Gamma, \Gamma]) \simeq \Gamma(\mathfrak{Z}).$$

Since $\mathfrak{Z}$ is abelian, the result follows by Corollary 5.

II. GROUPS OF ORDER p^3

In this section we show that the groups of order p, p^2, and p^3 are split by their group algebras. By Corollary 5, we need only consider the nonabelian groups. Thus we need only check the nonabelian groups of order p^3.

In the remainder of this paper we use the list of p-groups of order at most p^4 found in [1, pages 145-146]. We use the numbering of the groups and the particular forms for the generators and relations as given. The only notational change here is the replacing of E by 1 for the identity element of the group.

We first consider $p = 2$. There are two nonabelian groups: (i) the dihedral group and (ii) the quaternion group. There is a natural map $N/N^2 \to N^2/N^3$, defined by mapping each element of N to its square. We compute the size of the kernel in both cases and show that the two values are different (this fruitful technique was suggested by Professor Richard Brauer). Since the map is well-defined, we can compute it by choosing any convenient basis for N/N^2.

The $\mathfrak{M}$-series of the two groups look identical:

$$\mathfrak{M}_1 = \mathfrak{G}, \qquad \mathfrak{M}_2 = \langle P^2 \rangle, \qquad \mathfrak{M}_3 = 1.$$

Thus, in the language of [4], $(P - 1)$ and $(Q - 1)$ have weight 1, and $(P^2 - 1)$ has weight 2. Hence the elements $(P - 1)$ and $(Q - 1)$ form a basis for N/N^2. In the remainder of this paper we assume a knowledge of the techniques of [4], and thus we shall not make further reference to it.

Now, for $a, b \in K$, Lemma 3 implies that

$$\{a(P - 1) + b(Q - 1)\}^2 = a^2(P - 1)^2 + b^2(Q - 1)^2 + ab\{(P - 1)(Q - 1) + (Q - 1)(P - 1)\}$$

$$\equiv (a + ab + \alpha b)(P^2 - 1) \bmod N^3,$$

where $\alpha = 1$ for the quaternions and $\alpha = 0$ for the dihedral group. Since $(P^2 - 1)$ has weight 2, the result is zero if and only if

$$a + ab + \alpha b = 0.$$

Thus the size of the kernel is the number of ordered pairs (a, b) satisfying the above equation. For $\alpha = 0$, there are three such pairs, and for $\alpha = 1$ only one. Since the size of the kernel is an invariant of the algebra Γ, it follows that the two groups are split.

We now consider $p > 2$. Again there are two nonabelian groups, and we show that their respective $\mathfrak{M}$-series do not have isomorphic quotients. The $\mathfrak{M}$-series are as follows:

group (iv): $\mathfrak{M}_1 = \mathfrak{G}, \quad \mathfrak{M}_2 = \langle P^p \rangle = \mathfrak{M}_3 = \cdots = \mathfrak{M}_p, \quad \mathfrak{M}_{p+1} = 1,$

group (v): $\mathfrak{M}_1 = \mathfrak{G}, \quad \mathfrak{M}_2 = \langle P \rangle, \quad \mathfrak{M}_3 = 1.$

Since $p > 2$, we see that the $\mathfrak{M}_2/\mathfrak{M}_3$-quotients are not isomorphic, and the result follows by Proposition 4.

III. GROUPS OF ORDER 2^4

In this section we split the groups of order 2^4. For the nonabelian groups we have the following chart.

Group Number	$\mathfrak{Z}$-type	$\mathfrak{G}/\mathfrak{G}'$-type	Kernel size
(i)	(4)	(4, 2)	
(ii)	(4)	(2, 2, 2)	
(iii)	(2, 2)	(4, 2)	1
(iv)	(2, 2)	(2, 2, 2)	6
(v)	(2, 2)	(4, 2)	2
(vi)	(2, 2)	(2, 2, 2)	2
(vii)	(2)	(2, 2)	3
(viii)	(2)	(2, 2)	3
(ix)	(2)	(2, 2)	3

Here "Kernel size" indicates the number of elements in the kernel of the natural map $N/N^2 \to N^2/N^3$. The computation is straightforward and will be omitted. By Corollaries 5 and 6, we need only show that the group algebras of groups (vii), (viii), and (ix) are nonisomorphic.

To simplify computations, we first work with the dihedral group of order 8 given by

$$P^4 = 1, \quad Q^2 = 1, \quad Q^{-1}PQ = P^{-1}.$$

LEMMA 7. *Let* $\mathfrak{G}$ *be the dihedral group of order* 8. *Then the element* P^2 *can be found canonically in* $\Gamma(\mathfrak{G})$.

Proof. We show first that $\Gamma^{(2)} \cap [\Gamma, \Gamma] = \{0, P + P^{-1}\}$. The elements $(1 + P^2)$, $(P + P^{-1})$, $Q(1 + P^2)$, and $QP(1 + P^2)$ are central and have square zero. Thus, to compute $\Gamma^{(2)}$ we need only consider $x \in \Gamma$ of the form

$$x = a_0 1 + a_1 P + a_2 Q + a_3 QP.$$

Then

$$x^2 = (a_0 + a_2 + a_3)1 + a_1 P^2 + a_2 a_3(P + P^{-1}) + a_1 a_2 Q(P + P^{-1}) + a_1 a_3 QP(P + P^{-1}).$$

By Lemma 1(b), since 1 and P^2 are central elements, $x^2 \in [\Gamma, \Gamma]$ if and only if

$$a_0 + a_2 + a_3 = 0 = a_1 .$$

Hence, in this case $x^2 = a_2 a_3 (P + P^{-1})$, and the result follows. This of course implies that $(P + P^{-1})$ can be found in $\Gamma(\mathfrak{G})$.

Now, let x satisfy the condition $x(x + P + P^{-1}) = 1$. We show that

$$x(P + P^{-1}) + 1 = P^2 .$$

Since the above equation has at least one solution, namely $x = P$, this will yield the result. The elements $(1 + P^2)$, $(P + P^{-1})$, $Q(1 + P^2)$, and $QP(1 + P^2)$ are central, have square zero, and anhilate $(P + P^{-1})$. Thus, it suffices to assume that x has the form

$$x = a_0 1 + a_1 P + a_2 Q + a_3 QP .$$

Now

$$x(x + P + P^{-1}) = (a_0 + a_1 + a_2 + a_3)1 + (a_0 + a_2 a_3)(P + P^{-1})$$
$$+ (a_1 a_2 + a_2) Q (P + P^{-1}) + (a_1 a_3 + a_3) QP (P + P^{-1}),$$

and this is equal to 1 if and only if

$$a_0 + a_1 + a_2 + a_3 = 1, \quad a_0 + a_2 a_3 = 0, \quad a_2(1 + a_1) = 0, \quad a_3(1 + a_1) = 0 .$$

The only solution is easily seen to be $a_1 = 1$, $a_0 = a_2 = a_3 = 0$. Thus $x = P$ and $x(P + P^{-1}) + 1 = P^2$.

We now consider the groups $\mathfrak{G}$ of order 16. These are as follows.

group (vii): $P^8 = 1, \quad Q^2 = 1, \quad Q^{-1}PQ = P^{-1}$,

group (viii): $P^8 = 1, \quad Q^2 = 1, \quad Q^{-1}PQ = P^3$,

group (ix): $P^8 = 1, \quad Q^2 = P^4, \quad Q^{-1}PQ = P^{-1}$.

For all u in Γ, we write $u = \sum_i a_i P^i + \sum_i b_i QP^i$.

LEMMA 8. *The linear space*

$$T = \{u \mid a_0 = a_4,\ a_2 = a_6,\ a_1 + a_3 + a_5 + a_7 = 0\}$$

can be found canonically in $\Gamma(\mathfrak{G})$.

Proof. We show first that $(N \cap Z)^{(2)} = \{0, P^2 + P^{-2}\}$. The space $(N \cap Z)$ is spanned by $(1 + P^4)$, $Q(1 + P^2 + P^4 + P^6)$, $QP(1 + P^2 + P^4 + P^6)$, and $(P + P^{-1})$, $(P^3 + P^{-3})$ or $(P + P^3)$, $(P^5 + P^7)$. In either case, each basis element has square $(P^2 + P^{-2})$ or zero. Thus we can obtain the element $(P^2 + P^{-2})$.

Let $I = (P^2 + P^{-2})\Gamma = (1 + P^4)\Gamma$. Then Γ/I is the group algebra of the dihedral group of order 8. By Lemma 7, we can find the element P^2 in Γ/I. Thus the coset $P^2 + (1 + P^4)\Gamma$ can be found canonically in Γ. For each $x \in P^2 + (1 + P^4)\Gamma$, set

$$S_x = \{u \in \Gamma \mid ux = (x + P^2 + P^{-2})u\} .$$

We shall show that $T = (N \cap Z) + \sum_x S_x$, and this will yield the result.

Clearly, $T \supseteq N \cap Z$. Let $x \in P^2 + (1 + P^4)\Gamma$, so that $x = P^2 + v(1 + P^4)$, and let $u \in S_x$. Since $(1 + P^4)$ is central, the relation

$$u(P^2 + v(1 + P^4)) = (P^{-2} + v(1 + P^4))u$$

implies that

$$uP^2 + P^{-2}u = (1 + P^4)(uv + vu) \in (1 + P^4)[\Gamma, \Gamma].$$

By Lemma 1(b), the P^i-terms in $[\Gamma, \Gamma]$ are spanned by $(P^2 + P^{-2})$ and $(P + P^{-1})$, $(P^3 + P^{-3})$ or $(P + P^3)$, $(P^5 + P^7)$. Thus in either case the only P^i-term in $(1 + P^4)[\Gamma, \Gamma]$ is $(P + P^3 + P^5 + P^7)$. Hence, for the P^i-terms in $uP^2 + P^{-2}u$,

$$(a_0 1 + a_2 P^2 + a_4 P^4 + a_6 P^6)(P^2 + P^{-2}) = 0,$$

$$(a_1 P + a_3 P^3 + a_5 P^5 + a_7 P^7)(P^2 + P^{-2}) = \delta(P + P^3 + P^5 + P^7),$$

with $\delta = 0$ or 1. This implies that

$$a_0 = a_4, \quad a_2 = a_6, \quad a_1 + a_3 + a_5 + a_7 = 0 .$$

Hence $u \in T$ and $T \supseteq (N \cap Z) + \sum_x S_x$.

We obtain the reverse inclusion by showing that $T = (N \cap Z) + S_{P^2}$. Now

$$S_{P^2} = \{u \mid uP^2 = P^{-2}u\} = \{u \mid a_0 = a_4,\ a_2 = a_6,\ a_1 = a_5,\ a_3 \doteq a_7\} .$$

Thus S_{P^2} is a maximal subspace of T. Since $(N \cap Z) \not\subseteq S_{P^2}$, the result follows.

We are now in a position to split the three groups. We compute the number of $u \in T$ with $u^2 \equiv 1 \bmod [\Gamma, \Gamma]$ and show this is different in the three cases. Lemmas 1(b) and 2(a) are used repeatedly.

Group (vii):
$$u^2 \equiv (a_0 + a_4 + \textstyle\sum b_j)1 + (a_1 + a_5)P^2 + (a_3 + a_7)P^{-2} + (a_2 + a_6)P^4$$
$$\equiv \left(\textstyle\sum b_j\right) 1 \mod [\Gamma, \Gamma],$$

since $u \in T$. Thus $u^2 \equiv 1$ if and only if

$$a_0 = a_4, \quad a_1 = a_3 + a_5 + a_7, \quad a_2 = a_6, \quad b_0 = 1 + \textstyle\sum_1^7 b_j,$$

and there are 2^{12} such u.

Group (viii):
$$u^2 \equiv (a_0 + a_4 + b_0 + b_2 + b_4 + b_6)1 + (a_2 + a_6 + b_1 + b_3 + b_5 + b_7)P^4$$
$$+ (a_1 + a_5)P^2 + (a_3 + a_7)P^{-2}$$
$$\equiv (b_0 + b_2 + b_4 + b_6)1 + (b_1 + b_3 + b_5 + b_7)P^4 \mod [\Gamma, \Gamma],$$

since $u \in T$. Thus $u^2 \equiv 1$ if and only if

$$a_0 = a_4, \quad a_2 = a_6, \quad a_1 = a_3 + a_5 + a_7, \quad b_0 = 1 + b_2 + b_4 + b_6, \quad b_1 = b_3 + b_5 + b_7,$$

and there are 2^{11} such u.

$$\text{Group (ix): } u^2 \equiv (a_0 + a_4)1 + (a_2 + a_6 + \textstyle\sum b_j)P^4 + (a_1 + a_5)P^2 + (a_3 + a_7)P^{-2}$$
$$\equiv \left(\textstyle\sum b_j\right) P^4 \bmod [\Gamma, \Gamma],$$

since $u \in T$. Hence there are no $u \in T$ with $u^2 \equiv 1$. Therefore the three groups are split.

Thus all the groups of order 2^4 are split.

IV. GROUPS OF ORDER p^4 $(p > 2)$

For the nonabelian groups of order p^4 $(p > 2)$ we have the following chart.

Group Number	$\mathfrak{Z}$-type	$\mathfrak{G}/\mathfrak{G}'$-type	$\mathfrak{M}_2/\mathfrak{M}_3$-type	$\mathfrak{M}_3/\mathfrak{M}_4$-type $(p > 3)$	Kernel size $(p = 3)$
(vi)	(p^2)	(p^2, p)			
(vii)	(p^2)	(p, p, p)			
(viii)	(p, p)	(p^2, p)	(1)		
(ix)	(p, p)	(p, p, p)	(1)		
(x)	(p, p)	(p^2, p)	(p)		
(xi)	(p)	(p, p)		(1)	5
(xii)	(p)	(p, p)		(1)	3
(xiii)	(p)	(p, p)		(1)	1
(xiv)	(p, p)	(p, p, p)	(p)		
(xv) $p > 3$	(p)	(p, p)		(p)	
(xv) $p = 3$	(3)	(3, 3)			7

Here "Kernel size" denotes the number of elements in the kernel of the map $N/N^2 \to N^3/N^4$ that sends each element to its cube. This is obtained only for $p = 3$. The computation is straightforward, and we shall omit it. By Proposition 4 and Corollaries 5 and 6, we need only show that the group algebras of groups (xi), (xii), and (xiii) for $p > 3$ are nonisomorphic.

Groups (xi), (xii), and (xiii) are given by the relations

$$P^{p^2} = 1, \quad Q^p = 1, \quad Q^{-1}PQ = P^{1+p}, \quad R^{-1}PR = PQ, \quad R^{-1}QR = Q, \quad R^p = P^{\alpha p}$$

with $\alpha = 0, 1$, and any nonresidue modulo p, respectively. They have $\mathfrak{M}$-series

$$\mathfrak{M}_1 = \mathfrak{G}, \quad \mathfrak{M}_2 = \langle P^p, Q\rangle, \quad \mathfrak{M}_3 = \langle P^p\rangle = \cdots = \mathfrak{M}_p, \quad \mathfrak{M}_{p+1} = 1.$$

Thus $(P - 1)$ and $(R - 1)$ have weight 1, $(Q - 1)$ has weight 2, and $(P^p - 1)$ has weight $p > 3$. By Lemma 3 and the fact that $(P^p - 1) \in N^4$,

$$\begin{aligned}
(P - 1)(R - 1) &\equiv (R - 1)(P - 1) + (Q - 1) && \bmod N^3, \\
(P - 1)(Q - 1) &\equiv (Q - 1)(P - 1) && \bmod N^4, \\
(R - 1)(Q - 1) &= (Q - 1)(R - 1) \\
(P^{\alpha p} - 1) &\equiv \alpha(P^p - 1) && \bmod N^{p+1}.
\end{aligned}$$

LEMMA 9. *The natural map* ϕ: $N/N^2 \to N^p/N^{p+1}$ *is given by*

$$\{a(P - 1) + b(R - 1)\}^p \equiv (a + \alpha b)(P^p - 1) \bmod N^{p+1}.$$

Proof. By the above equations,

$$[a(P - 1),\ b(R - 1)] \equiv ab(Q - 1) \bmod N^3,$$

and $a(P - 1)$ and $b(R - 1)$ commute with $ab(Q - 1)$ modulo N^4. It is now clear that in computing $\{a(P - 1) + b(R - 1)\}^p$ we can think of $a(P - 1)$ and $b(R - 1)$ as commuting with their Lie product. Since $p > 3$, Lemma 2(b) yields the relations

$$\begin{aligned}
\{a(P - 1) + b(R - 1)\}^p &\equiv \{a(P - 1)\}^p + \{b(R - 1)\}^p \equiv a(P^p - 1) + b(P^{\alpha p} - 1) \\
&\equiv (a + \alpha b)(P^p - 1) \bmod N^{p+1}
\end{aligned}$$

LEMMA 10. *The subspace* $S = \langle (Q - 1), (Q - 1)^2, \cdots, (Q - 1)^{(p-1)/2}, N^p \rangle$ *can be found canonically in* $\Gamma(\mathfrak{G})$.

Proof. Let $T = \langle P^p - 1, N^{p+1} \rangle$. Since T is the complete inverse image in N^p of $\phi(N/N^2) \subseteq N^p/N^{p+1}$, it can be found canonically in $\Gamma(\mathfrak{G})$. Set

$$U = \{u \in N \mid \forall x \in N,\ xu - ux \in T\}.$$

We show that $S = U$. This will yield the result.

From the identity

$$(P - 1)(Q - 1) = (Q - 1)(P - 1) + (PQ - 1)(P^p - 1) + (P^p - 1)$$

and the fact that $(P^p - 1) \in N^p$ we deduce that

$$(P - 1)(Q - 1) \equiv (Q - 1)(P - 1) + (P^p - 1) \bmod N^{p+1}.$$

Also, $(R - 1)(Q - 1) = (Q - 1)(R - 1)$. These commuting relations and the explicit form of the Jennings basis for N/N^p show immediately that $U \supseteq S$.

We assume by way of contradiction that U properly contains S. Choose $u \in U - S$, and write u in terms of the Jennings basis modulo N^p. We can, of course, assume that no terms of the form $(Q - 1)^j$ with $2j < p$ occur in the representation of u. We prove by induction on t that $u \in N^t$ for $t \leq p$.

First, $u \in N$ is given. Now, let us assume that $u \in N^t$ with $t < p$. We show that $u \in N^{t+1}$. Now

$$u \equiv \sum a_{i,j}(P - 1)^i(R - 1)^j(Q - 1)^k \bmod N^{t+1}$$

with $i+j+2k=t$ and $a_{0,0}=0$. Since $u \in U$, it follows that $[(P-1), u] \in T$, $[(R-1), u] \in T$, and

$$[(P-1), u] \in T+N^{t+2}, \quad [(R-1), u] \in T+N^{t+2}.$$

In these equations we need only consider u modulo N^{t+1}, and we conclude that, modulo N^{t+2},

$$[(P-1), u] \equiv -\sum_{j\geq 1} j a_{i,j}(P-1)^i (R-1)^{j-1}(Q-1)^{k+1},$$

$$[(R-1), u] \equiv -\sum_{i\geq 1} i a_{i,j}(P-1)^{i-1}(R-1)^j (Q-1)^{k+1}.$$

If these terms belong to $N^{t+2}+T = \langle N^{t+2}, P^p-1\rangle$, then $j a_{i,j} = 0 = i a_{i,j}$. But since $0 \leq i, j \leq t < p$, this implies that $a_{i,j}=0$, provided not both i and j are zero. On the other hand, $a_{0,0}=0$ by assumption. Hence $u \equiv 0 \mod N^{t+1}$. By induction, we obtain the contradiction $u \in N^p \subseteq S$. Therefore $S=U$, and the result follows.

We are now in a position to split the three groups. Choose an element $x \in N - N^2$ with $\phi(x+N^2)=0$, and choose $y \in N$ with $\phi(y+N^2) \neq 0$. Since P^p-1 has weight p, Lemma 9 implies that

$$x = \lambda\{\alpha(P-1)-(R-1)\}+n,$$

$$y = \rho\{\alpha(P-1)-(R-1)\}+\mu(P-1)+m,$$

with $n, m \in N^2$ and $\lambda, \mu \neq 0$. Since

$$[x, y] = xy - yx \equiv \mu\lambda(Q-1) \mod N^3,$$

there exists $s \in S$ with $[x, y] \equiv s \mod N^3$. Choose any such s. Then

$$s \equiv \mu\lambda(Q-1) + \sum_{i\geq 2} b_i(Q-1)^i \mod N^p.$$

Since $[x, (Q-1)^i] \in N^{p+1}$ for $i \geq 2$ and $[n, s] \in N^{p+1}$, we see that

$$[x, s] \equiv \mu\lambda^2[\{\alpha(P-1)-(R-1)\}, (Q-1)] \equiv \mu\lambda^2\alpha(P^p-1) \mod N^{p+1}.$$

Thus $[x, s] \equiv 0$ modulo N^{p+1} if and only if $\alpha = 0$. Therefore the group for $\alpha = 0$ is split from the other two.

We assume now that $\alpha \neq 0$. By Lemma 9,

$$y^p - [x, s] \equiv (\mu - \mu\lambda^2\alpha)(P^p-1) \mod N^{p+1},$$

and this is congruent to zero if and only if $1-\lambda^2\alpha = 0$. If $\alpha = 1$, there are suitable choices for x to make this expression zero: we need only take $\lambda = \pm 1$. On the other hand, if α is a nonresidue, then there are no such choices for x, since $1-\lambda^2\alpha=0$ implies that $\alpha = (1/\lambda)^2$, a contradiction. Thus the group algebras of these three groups are not isomorphic.

This completes the proof of the theorem.

REFERENCES

1. W. Burnside, *Theory of groups of finite order*, Second Edition, Dover Publications, New York, 1955.

2. D. B. Coleman, *Finite groups with isomorphic group algebras*, Trans. Amer. Math. Soc. 105 (1962), 1-8.

3. N. Jacobson, *Lie algebras*, Interscience Publishers, New York, 1962.

4. S. A. Jennings, *The structure of the group ring of a* p-*group over a modular field*, Trans. Amer. Math. Soc. 50 (1941), 175-185.

5. H. N. Ward, *Some results on the group algebra of a group over a prime field*, Mimeographed notes for the Seminar on Finite Groups and Related Topics at Harvard University, 1960-1961.

University of California, Los Angeles